Formes primitives et représentations galoisiennes de type octaédral

Philippe Cassou-Noguès et Arnaud Jehanne

TABLE DES MATIÈRES

Un résultat de Langlands et Weil permet d'associer à toute représentation galoisienne de type octaédral et de déterminant impair du groupe de Galois absolu de $\mathbb{Q}$ une forme primitive de poids 1. En nous appuyant sur les travaux de Bayer et Frey, nous proposons une méthode de construction de formes primitives basée sur ce résultat. Le calcul des coefficients de leur développement de Fourier à l'infini, que nous avons implémenté sur machine, permet la construction de tables. Le cas des formes de niveau pair est étudié avec précision.

It is known by a result of Langlands and Weil that one can associate to each representation of the absolute Galois group of $\mathbb{Q}$ with odd determinant and octahedral type a newform of weight one. Using the work of Bayer and Frey, we provide a method for constructing such newforms. The calculation of the coefficients of their Fourier expansions at infinity can then be computed so as to provide tables. The case of forms of even level is studied in detail.

INTRODUCTION

Soient $\mathbb{Q}^c$ une clôture algébrique de $\mathbb{Q}$ et $G_{\mathbb{Q}}$ le groupe de Galois de $\mathbb{Q}^c/\mathbb{Q}$ muni de sa topologie naturelle de groupe profini.

Langlands a conjecturé l'existence d'une bijection entre d'une part l'ensemble des classes d'isomorphisme des représentations continues et irréductibles de $G_{\mathbb{Q}}$ de degré 2, de conducteur d'Artin M et de déterminant impair χ donnés et, d'autre part, l'ensemble des formes primitives de poids égal à 1 normalisées sur le sous-groupe de congruence $\Gamma_0(M)$, de caractère χ [Deligne et Serre 1974, § 4]. Si ρ est une telle représentation, on introduit sa fonction L d'Artin $L(s,\rho)=\sum_{n\geq 1} a_n n^s$, où $\operatorname{Re} s > 1$, et l'on conjecture que $F_\rho(\tau)=\sum_{n\geq 1} a_n e^{2in\pi\tau}$, où $\operatorname{Im}\tau > 0$, est la forme primitive associée à ρ.

1058-6458/96 \$0.50 per page

Toute représentation ρ du type précédent définit par composition avec l'homomorphisme $\mathrm{GL}_2(\mathbb{C}) \to \mathrm{PGL}_2(\mathbb{C})$ une représentation projective $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$. Nous nous intérèsserons ici au cas où l'image de $\bar{\rho}$ est le groupe octaédral S_4. Les résultats de Langlands et Weil d'une part et de Langlands et Tunnel d'autre part démontrent dans ce cas la conjecture. Un des buts de ce travail est de rendre explicite le procédé de construction de formes primitives associé à ce résultat. Plus précisément, en nous appuyant sur les travaux décrits dans [Bayer et Frey 1991; Jehanne 1995], nous proposons une méthode de construction de formes primitives de niveau donné et le calcul rapide, implémenté sur machine, des coefficients de leurs développements de Fourier à l'infini. Cette méthode permet la construction de tables. Les résultats que nous obtenons complètent ceux de [Bayer et Frey 1991] notamment pour les formes primitives de niveau pair. De plus, ils permettent dans certains cas la construction d'un "relèvement minimal" d'une représentation projective donnée.

I. Schur [1911] a démontré que pour $n \geq 4$, le groupe $H^2(S_n, \{\pm 1\})$ est bicyclique d'ordre 4, c'est-à-dire qu'à isomorphisme près, il existe trois extensions centrales non triviales de S_n par $\{\pm 1\}$. Soit $\widetilde{S}_4$ l'unique extension centrale non triviale de S_4 de degré 2 dans laquelle les transpositions se relèvent en des involutions. On fixe une représentation projective $r : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$, d'image S_4. Soit $\mathcal{R}$ l'ensemble des représentations de $G_{\mathbb{Q}}$ dans $\mathrm{GL}_2(\mathbb{C})$. Un théorème de Tate affirme qu'il existe toujours une représentation ρ de $\mathcal{R}$ telle que $\bar{\rho} = r$ [Serre 1977, seconde partie, théorème 4]. On appelle relèvement de r une telle représentation.

Soit ρ un relèvement de r de déterminant quadratique. La représentation r définit une extension galoisienne $N/\mathbb{Q}$ à groupe de Galois S_4. On note $\widetilde{N}$ le corps des invariants de $\mathbb{Q}^c$ par le noyau de ρ. L'image par ρ de $\mathrm{Gal}(\widetilde{N}/N)$ est un sous-groupe du centre de $\mathrm{GL}_2(\mathbb{C})$ sur lequel $\det(\rho)^2$ est trivial. On en déduit que $\rho\big(\mathrm{Gal}(\widetilde{N}/N)\big)$ est contenu dans le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par $\binom{i\ 0}{0\ i}$. Le groupe de Galois de $\widetilde{N}/N$ est donc nécessairement cyclique d'ordre 2 ou 4. En fait, dans ce cas où $\mathrm{Im}(r) \simeq S_4$, les noyaux de r et de ρ sont égaux. On en déduit que $\mathrm{Gal}(\widetilde{N}/N)$ est cyclique d'ordre 2 et par conséquent que $\mathrm{Gal}(\widetilde{N}/\mathbb{Q}) \simeq \widetilde{S}_4$. L'existence d'un relèvement de r de type $\widetilde{S}_4$ est équivalente à la possibilité de plonger $N/\mathbb{Q}$ dans une extension galoisienne $\widetilde{N}/\mathbb{Q}$ à groupe de Galois $\widetilde{S}_4$. Si K désigne un sous-corps quartique de N, un théorème de Serre ramène ce problème au calcul de l'invariant de Witt de la forme $\mathrm{Tr}_{K/\mathbb{Q}}(x^2)$ [Serre 1984, théorème 1], puis à la vérification de conditions locales en chaque nombre premier impair ramifié dans K. Ces conditions sont décrites dans [Bayer et Frey 1991, Proposition 1.2]. Si l'on souhaite construire des formes de niveau imposé, il est nécessaire de maîtriser la ramification de $N/\mathbb{Q}$. Les courbes elliptiques et leurs points de 2-division sont un outil efficace pour de telles constructions. On retrouve dans ce travail l'une des familles d'extensions introduites dans [Cassou-Noguès et Jehanne 1996] et construites par ce procédé.

Une fois assurée la possibilité de plongement, il s'agit de construire les corps $\widetilde{N}$ qui en sont des réalisations. La nécessité d'obtenir une ramification minimale dans $\widetilde{N}/\mathbb{Q}$ nous conduit à ne construire que des extensions "$\widetilde{S}_4$-pures" dont la définition est rappelée au paragraphe 1. Teresa Crespo [1990] a donné une méthode de construction d'un élément γ de N tel que $\widetilde{N} = N(\sqrt{\gamma})$. Nous en donnons ici une autre dans le paragraphe 1. Cette méthode permet, avec l'aide du système PARI, de donner un générateur de $\widetilde{N}/N$ qui se présente en fait comme la racine carrée d'un élément de K.

L'étape suivante est le calcul du conducteur d'Artin d'une représentation octaédrale de $\mathrm{Gal}(\widetilde{N}/\mathbb{Q})$. Désignons par ρ une telle représentation et pour tout nombre premier p, notons $n_p(\rho)$ la valuation en p du conducteur d'Artin de ρ. Si la détermination de $n_p(\rho)$ est immédiate pour $p \neq 2$, celle de $n_2(\rho)$ exige l'étude précise de la ramification en 2 de N et $\widetilde{N}$. Cette étude théoriquement simple mais techniquement assez longue est faite au paragraphe 2. Les résultats sont regroupés dans les tableaux 2 et 3, qui donnent, suivant la ramification de 2 dans K, les valeurs possibles de $n_2(\rho)$. La plupart des valeurs possibles sont réalisées dans les exemples du paragraphe 4. On remarque que si $p \neq 2$ et si le noyau de ρ fixe un corps "$\widetilde{S}_4$-pur", alors $n_p(\rho)$ est indépendant du choix du relèvement ρ de r. Il n'en est pas de même si $p = 2$. On montre dans un certain nombre de cas l'existence d'un relèvement minimal.

Plus généralement, pour tout nombre premier l, on pose

$$n_l(\rho_m) = \inf\{n_l(\rho) : \rho \in \mathcal{R} \text{ et } \bar{\rho} = r\}.$$

Un relèvement minimal (resp. minimal en p) est défini comme un relèvement ρ de r tel que $n_l(\rho) = n_l(\rho_m)$ pour tout nombre premier l (resp. pour $l = p$).

Grâce aux résultats de Buhler et Kiming, on peut calculer $n_p(\rho_m)$ pour un r donné [Buhler 1978, chapitre 2, théorème 4 ; Kiming 1994, théorèmes 1 et 2]. Si p est impair et si ρ désigne un relèvement $\widetilde{S}_4$-pur de r, on remarque que $n_p(\rho) = n_p(\rho_m)$ si et seulement si soit le groupe de décomposition d'un relèvement premier de p dans N est primitif ou diédral, soit son groupe d'inertie est engendré par une transposition (le groupe bicyclique d'ordre 4 est ici considéré comme diédral). Nous avons calculé $n_2(\rho_m)$ dans chacun des cas du tableau 3. De sa comparaison avec $n_2(\rho)$, nous déduisons que dans un certain nombre de cas que nous déterminons, il existe un relèvement de r de type octaédral minimal en 2 (proposition 2.5 et tableau 3).

Dans le paragraphe 3, nous exposons la méthode utilisée pour le calcul des coefficients de Fourier des formes primitives construites. Cette méthode, différente de celle proposée dans [Bayer et Frey 1991], a été programmée sur machine et fournit les exemples du dernier paragraphe. Ce dernier paragraphe expose les fruits de ce travail puisqu'il regroupe sous forme de tableaux un petit échantillonage des exemples numériques que nous pouvons traiter.

Tous les calculs numériques ont été faits sur le système PARI [Batut et al. 1995].

1. CONSTRUCTION DE $\widetilde{S}_4$-EXTENSIONS

Ce paragraphe contient essentiellement un rappel de certains résultats de [Jehanne 1995]. Nous y énonçons en particulier deux résultats clés pour nos constructions (les propositions 1.4 et 1.5), dont nous illustrons ensuite l'utilisation par un exemple simple. La proposition 1.4, qui découle du théorème 1.2, permet de déceler un nombre fini de candidats $\lambda \in K$ parmi lesquels se trouvera un générateur de $\widetilde{N}/N$ dans chacune de nos constructions alors que la proposition 1.5 donne un critère de vérification facilement testable sur machine. Ce sont ces résultats que nous utilisons dans les exemples du paragraphe 4. On fixe un corps quartique K, de clôture galoisienne N à groupe de Galois S_4 sur $\mathbb{Q}$. On dit que N est *plongeable* s'il existe une extension quadratique $\widetilde{N}$ de N telle que $\widetilde{N}/\mathbb{Q}$ soit galoisienne à groupe de Galois $\widetilde{S}_4$. On dit alors que $\widetilde{N}$ est une *réalisation du plongement*.

J.-P. Serre [1984] a démontré le théorème suivant, qui permet de décider si oui ou non N est plongeable.

Théorème 1.1. *Le corps N est plongeable si et seulement si $\omega_2(\mathrm{Tr}_{K/\mathbb{Q}}(x^2)) = (2, d_K)$, où $\omega_2(q)$ désigne l'invariant de Witt de la forme quadratique q, d_K le discriminant de K et $(\ ,\ )$ le symbole de Hilbert.*

Nous rappelons dans la figure 1 le diagramme de Hasse de l'extension $N/\mathbb{Q}$. Le corps C est cubique non galoisien et L est l'extension quadratique de C contenue dans la composée de K et de C. Soit C' la clôture galoisienne de C. On vérifie que l'extension N/C' est ramifiée si et seulement si l'extension L/C est ramifiée.

Lorsque N est plongeable, le théorème suivant [Jehanne 1995, théorème III.2] précise l'existence d'une réalisation du plongement à "ramification minimale". Il se trouve donc fatalement une réalisation du plongement parmi les extensions quadratiques de N admettant les ramifications qui y sont décrites.

Théorème 1.2. *On suppose N plongeable. Alors :*

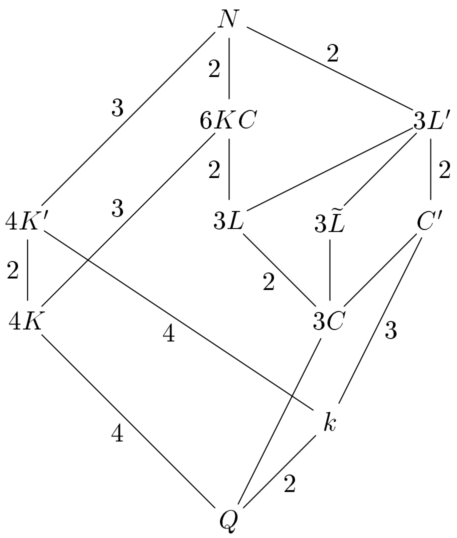

FIGURE 1. Diagramme de Hasse de l'extension $N/\mathbb{Q}$.

1. *Pour toute réalisation $\tilde{N}/\mathbb{Q}$ du plongement, l'extension $\tilde{N}/N$ est ramifiée en tout idéal premier ramifié dans L/C et en tout idéal premier situé au-dessus de 2 si $2\mathcal{O}_K$ est de la forme $\mathfrak{p}_2\mathfrak{p}_1'^2$ (où l'entier placé en indice désigne l'indice résiduel de l'idéal premier), auquel cas $d_k \equiv 4 \bmod 8$.*
2. *Il existe une réalisation du plongement $\tilde{N}$ telle que $\tilde{N}/N$ soit non ramifiée en dehors des idéaux premiers de N qui sont ramifiés dans L/C et des idéaux premiers de N au-dessus de 2 si $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$.*

Définitions 1.3. Si N est plongeable, toute réalisation $\tilde{N}$ du plongement qui vérifie la propriété 2 du théorème 1.2 est dite pure. On dit également que $\tilde{N}$ est un corps $\tilde{S}_4$-pur.

Une représentation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ est dite $\tilde{S}_4$-pure si le corps $(\mathbb{Q}^c)^{\mathrm{Ker}(\rho)}$ est $\tilde{S}_4$-pur.

Supposons maintenant N plongeable et montrons comment l'on peut construire une réalisation $\tilde{N}$ du plongement. L'étude des sous-groupes de $\tilde{S}_4$ montre que le corps $\tilde{N}$ contient une unique extension quadratique $\tilde{K}'$ de K', que l'extension $\tilde{K}'/K$ est galoisienne à groupe de Galois $C_2 \times C_2$ (où C_2 désigne le groupe cyclique d'ordre 2) et que si $\tilde{K}$ désigne l'une des deux extensions quadratiques de K contenues dans $\tilde{K}'$ et distinctes de K', le corps $\tilde{N}$ est clôture galoisienne de $\tilde{K}$. Ainsi la construction de $\tilde{N}$ se ramène-t-elle à la recherche d'un élément γ de K rendant l'extension $N(\sqrt{\gamma})/\mathbb{Q}$ galoisienne à groupe de Galois $\tilde{S}_4$. Si γ est un tel élément, on dit que $K(\sqrt{\gamma})$, tout comme $\tilde{N}$, est une *réalisation du plongement*. Les deux propositions suivantes permettent de trouver une réalisation pure du plongement. La proposition 1.4 décrit les ramifications de l'extension $\tilde{K}/K$, dans le cas où $\tilde{N}$ est $\tilde{S}_4$-pur. Grâce à ce résultat, nous pouvons déterminer un sous-ensemble fini de K contenant nécessairement un élément γ réalisant le plongement. La proposition 1.5 donne un test capable de décider si pour un élément γ donné de K, le corps $K(\sqrt{\gamma})$ réalise ou non le plongement.

Proposition 1.4. *Soit $\tilde{N}$ une réalisation du plongement et soit $\tilde{K}$ l'une des deux extensions quadratiques de K distinctes de K' contenues dans $\tilde{N}$. Le corps $\tilde{N}$ est $\tilde{S}_4$-pur si et seulement si les idéaux premiers de K ramifiés dans $\tilde{K}$ sont exactement ceux qui suivent :*

1. *les idéaux premiers de K qui relèvent un nombre premier p ramifié dans l'extension L/C ;*
2. *les idéaux $\mathfrak{p}_1$ et $\mathfrak{p}_2'$ si $2\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2'$;*
3. *l'un, et seulement l'un des idéaux premiers $\mathfrak{p}_1$ ou $\mathfrak{p}_1'$ pour tout nombre premier p vérifiant $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^2$;*
4. *l'un, et seulement l'un des idéaux premiers $\mathfrak{p}_1$ ou $\mathfrak{p}_1'$ si $3\mathcal{O}_K = \mathfrak{p}_1^3\mathfrak{p}_1'$ et si 3 est ramifié dans k.*

Preuve. Nous décrivons ici comment la proposition 1.4 se déduit du théorème 1.2.

Soit p un nombre premier dont tous les relèvements premiers dans N sont ramifiés dans $\tilde{N}$. Comme $\mathrm{Gal}(\tilde{N}/K')$ est cyclique d'ordre 6, tous les relèvements premiers de p dans K' sont ramifiés dans $\tilde{K}'/K'$. L'extension $\tilde{K}'/K$ étant bicyclique d'ordre 4, on en déduit que tous les relèvements premiers de p dans K sont ramifiés dans $\tilde{K}$. On en déduit que si les idéaux premiers de K ramifiés dans $\tilde{K}$ sont les idéaux de type 1, 2, 3 ou 4 de l'énoncé de la proposition, alors seuls les relèvements dans N des idéaux de type 1 ou 2 sont ramifiés dans $\tilde{N}$. Le corps $\tilde{N}$ est donc $\widetilde{S}_4$-pur.

Supposons maintenant que $\tilde{N}$ soit $\widetilde{S}_4$-pure. On déduit de [Cassou-Noguès et Jehanne 1996, tableau II.1] qu'un idéal premier de K ramifié dans $\widetilde{K}$ qui n'est pas de type 1 ou 2 est soit un relèvement d'un nombre premier p tel que

$$p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'\mathfrak{p}_1'',$$

soit un relèvement de 3, dans le cas où

$$3\mathcal{O}_K = \mathfrak{p}_1^3\mathfrak{p}_1'$$

et où 3 est ramifié dans k. On note que le cas où $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2'$ avec p impair est exclu car N est plongeable. Supposons que $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'\mathfrak{p}_1''$. On déduit également de [Cassou-Noguès et Jehanne 1996, tableau II.1] que l'indice de ramification de p dans N est égal à 2 et que $\mathfrak{p}_1'$ et $\mathfrak{p}_1''$ sont ramifiés dans K'. Soit K'' l'extension quadratique de K contenue dans $\widetilde{K}'$ distincte de K' et de $\widetilde{K}$. Alors l'idéal $\mathfrak{p}_1'$, tout comme l'idéal $\mathfrak{p}_1''$ est ramifié dans l'un, et seulement l'un des corps $\widetilde{K}$ ou K''. Un calcul de conducteur montre que $d_{\widetilde{K}} = d_{K''}$. On en déduit que $\mathfrak{p}_1'$ se ramifie dans $\widetilde{K}$ si et seulement si $\mathfrak{p}_1''$ se ramifie dans K''. Le cas où $3\mathcal{O}_K = \mathfrak{p}_1^3\mathfrak{p}_1'$ se traite de la même façon. $\square$

Proposition 1.5. *Soit γ un élément de $K \setminus \mathbb{Q}$. Le corps $K(\sqrt{\gamma})$ est une réalisation du plongement si et seulement si le polynôme R de degré 24 suivant est réductible sur $\mathbb{Q}$:*

$$R(X) = \prod_{i\neq j}\left(\left(X - \delta_i\delta_j\left(\gamma_i - \gamma_j\right)\right)^2 - d_k\right)$$

où $\{\gamma_i : i \in \{1,2,3,4\}\}$ est l'ensemble des conjugués de γ et où pour tout $i \in \{1,2,3,4\}$, δ_i désigne une racine carrée arbitrairement choisie de γ_i. Dans ce cas, le polynôme R sera égal au produit $F_{+1}F_{-1}$ où pour $\varepsilon \in \{\pm 1\}$, F_ε désigne l'un des huit polynômes de degré 12 définis par :

$$F_\varepsilon(X) = \prod_{i<j}\left(X^2 - \left(\delta_i\delta_j(\gamma_i - \gamma_j) + \varepsilon\varepsilon_{ij}\sqrt{d_k}\right)^2\right)$$

avec $\varepsilon_{ij} \in \{\pm 1\}$ donnés par l'une des lignes du tableau suivant :

ε_{12}	ε_{13}	ε_{14}	ε_{23}	ε_{24}	ε_{34}
$+1$	$+1$	$+1$	$+1$	-1	$+1$
-1	$+1$	$+1$	$+1$	-1	-1
$+1$	$+1$	-1	$+1$	$+1$	-1
-1	$+1$	-1	$+1$	$+1$	$+1$
$+1$	$+1$	$+1$	-1	$+1$	-1
-1	$+1$	$+1$	-1	$+1$	$+1$
$+1$	$+1$	-1	-1	-1	$+1$
-1	$+1$	-1	-1	-1	-1

Preuve. Posons $\omega = \gamma_1\gamma_2(\gamma_1 - \gamma_2)^2$. Les tables de classifications des groupes de degré inférieur à 11 établies par G. Butler et J. McKay [1983] et l'action galoisienne de $\mathrm{Gal}(N/\mathbb{Q})$ sur ω permettent de démontrer que l'extension $N(\sqrt{\gamma})$ est galoisienne sur $\mathbb{Q}$ si et seulement si $L(\sqrt{\omega}) = L' = L(\sqrt{d_k})$ et que dans ce cas, $\mathrm{Gal}(N/\mathbb{Q})$ est isomorphe à $\widetilde{S}_4$ [Jehanne 1995, pp. 273–274]. De plus, ω est de degré 6 sur $\mathbb{Q}$. En effet, considérons $\mathrm{Gal}(N/\mathbb{Q})$ comme groupe de permutations agissant sur $\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$ par permutations des indices et posons

$$\tau_1 = (12),\quad \tau_2 = (34),\quad \rho = (1234) \quad \text{et} \quad \sigma = (234).$$

Si $L = N^{\langle\tau_1,\tau_2\rangle}$ et si $C = N^{\langle\tau_1,\rho\rangle}$, alors $\omega \in L$ et $C \subset L$. Supposons que ω appartienne à C. Dans ce cas, $\mathrm{Tr}_{C/\mathbb{Q}}(\omega) = \omega^{1+\sigma+\sigma^2} \in \mathbb{Q}$. On calcule que $\mathrm{Tr}_{C/\mathbb{Q}}(\omega)$ est égal à

$$\gamma_1^3\,\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_1) - 2\gamma_1^2\,\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_1^2) + \gamma_1\,\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_1^3).$$

Comme γ_1 est de degré 4 sur $\mathbb{Q}$, il en ressort que les rationnels $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_1)$, $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_1^2)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_1^3)$ sont nuls et donc que γ_1 est racine de $X^4 - \mathrm{N}_{K/\mathbb{Q}}(\gamma_1)$, ce qui contredit l'hypothèse : $\mathrm{Gal}(N/\mathbb{Q}) \simeq S_4$. On en déduit que $N(\sqrt{\gamma})$ réalise le plongement si et seulement si le polynôme R se factorise.

Tout relèvement dans $\widetilde{S}_4$ d'une transposition de S_4 est d'ordre 2 et transforme $\delta_1\delta_2\delta_3\delta_4$ en $-\delta_1\delta_2\delta_3\delta_4$. Ainsi les relèvements possibles de la transposition (12) sont-ils les suivants (à composition près avec le relèvement de Id_N qui à δ_i associe $-\delta_i$, quelque soit $i \in \{1,2,3,4\}$).

$$a: \begin{cases} \delta_1 \to \delta_2 \\ \delta_2 \to \delta_1 \\ \delta_3 \to \delta_3 \\ \delta_4 \to -\delta_4 \end{cases} \quad \text{ou} \quad a': \begin{cases} \delta_1 \to \delta_2 \\ \delta_2 \to \delta_1 \\ \delta_3 \to -\delta_3 \\ \delta_4 \to \delta_4 \end{cases}$$

De même, les relèvements possibles de (23) sont les applications

$$b: \begin{cases} \delta_1 \to \delta_1 \\ \delta_2 \to \delta_3 \\ \delta_3 \to \delta_2 \\ \delta_4 \to -\delta_4 \end{cases} \quad \text{ou} \quad b': \begin{cases} \delta_1 \to -\delta_1 \\ \delta_2 \to \delta_3 \\ \delta_3 \to \delta_2 \\ \delta_4 \to \delta_4 \end{cases}$$

et ceux de (34) sont

$$c: \begin{cases} \delta_1 \to \delta_1 \\ \delta_2 \to -\delta_2 \\ \delta_3 \to \delta_4 \\ \delta_4 \to \delta_3 \end{cases} \quad \text{ou} \quad c': \begin{cases} \delta_1 \to -\delta_1 \\ \delta_2 \to \delta_2 \\ \delta_3 \to \delta_4 \\ \delta_4 \to \delta_3 \end{cases}$$

On dénombre donc huit actions possibles du groupe $\mathrm{Gal}(\tilde{N}/\mathbb{Q})$ sur $\{\delta_1,\delta_2,\delta_3,\delta_4\}$. Chacune des huit factorisations envisageables du polynôme R données par la proposition 1.5 correspond à l'une de ces actions. □

Notons que l'essai systématique des produits F_1F_{-1} permet une factorisation immédiate du polynôme R et qu'en outre, la connaissance du sextuplet $(\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{14}, \varepsilon_{23}, \varepsilon_{24}, \varepsilon_{34})$ donnant la factorisation de R dévoile l'action de $\mathrm{Gal}(\tilde{N}/\mathbb{Q})$ sur $\{\delta_1,\delta_2,\delta_3,\delta_4\}$.

Nous indiquons sur l'exemple suivant la méthode de construction utilisée.

Exemple. Soit K le corps quartique de discriminant -283. C'est le corps quartique de signature $(2,1)$ de plus petit discriminant en valeur absolue. On peut écrire K sous la forme $K = \mathbb{Q}(\sqrt{\theta})$, où θ est une racine du polynôme $X^4 + X - 1$. Grâce à [Jehanne 1995, proposition I.4], on voit que la clôture galoisienne N de K est plongeable. L'idéal $283\mathcal{O}_K$ est de la forme $\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^2$. Le tableau I.3 de [Jehanne 1995] montre que 283 n'est pas ramifié dans l'extension L/C. Le théorème 1.2 permet donc d'affirmer qu'il existe une réalisation du plongement telle que $\tilde{N}/N$ soit non ramifiée. Soit $\tilde{K}$ une extension quadratique de K dont $\tilde{N}$ est une clôture galoisienne. La proposition 1.4 permet d'affirmer que l'extension $\tilde{K}/K$ est ramifiée en l'un, et l'un seulement des idéaux $\mathfrak{p}_1$ ou $\mathfrak{p}_1'$ et non ramifiée en toute autre place finie. De plus, si $\tilde{K} = K(\sqrt{\gamma})$ et si $\tilde{K}/K$ est ramifiée en $\mathfrak{p}_1$, alors $K(\sqrt{-283\gamma})$ est l'autre extension quadratique de K disctincte de K' contenue dans $\tilde{K}'$; en outre, $K(\sqrt{-283\gamma})$ est ramifiée en $\mathfrak{p}_1'$ et non ramifiée en toute autre place finie. L'élément $\alpha = -3 + 4\theta^2 + 4\theta^3$ de K engendre un idéal premier $\mathfrak{p}_1$ non ramifié de K de norme 283. Nous allons déterminer γ tel que $\mathfrak{p}_1$ soit la seule place finie ramifiée dans l'extension $\tilde{K}/K$. On vérifie que α a pour signature $(1,-1)$. Rappelons que l'élément γ cherché est nécessairement de signature $(1,-1)$ [Jehanne 1995, p. 265]. Il est clair que si ε désigne une unité totalement positive non carrée de K (unique à multiplication par un carré d'une unité de K près), alors l'un des deux corps $K(\sqrt{\alpha})$ et $K(\sqrt{\varepsilon\alpha})$ réalise le plongement. Grâce au test donné par la proposition 1.5, on vérifie sur machine que $K(\sqrt{\alpha})$ réalise le plongement.

2. CALCUL DU CONDUCTEUR

On conserve les notations du paragraphe précédent. On suppose que $N/\mathbb{Q}$ est une extension galoisienne à groupe de Galois S_4 plongeable et que $\tilde{N}$ est une extension de N, $\tilde{S}_4$-pure qui réalise le plongement. On sait que le groupe $\tilde{S}_4$ possède deux représentations de degré 2 fidèles, absolument irréductibles et conjuguées l'une de l'autre. Soit ρ l'une de ces deux représentations. Elle se relève en une représentation galoisienne

$$\rho : \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q}) \to \mathrm{GL}(V),$$

où V est un espace vectoriel sur $\mathbb{C}$ de dimension 2. Pour des raisons de commodité, nous notons par la même lettre ρ ces deux objets liés l'un à l'autre par composition avec une surjection $\pi : \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q}) \to \widetilde{S}_4$ définissant $\widetilde{N}$.

Soit $\mathfrak{F}(\rho)$ le conducteur d'Artin de ρ. Si p est un nombre premier et m un élément de $\mathbb{Z}$, on note $v_p(m)$ la valuation en p de m. Soit $n_p(\rho) = v_p(\mathfrak{F}(\rho))$. Pour tout corps de nombres L, on note $n_p(L) = v_p(d_L)$. On rappelle l'égalité

$$n_p(\rho) = \sum_{i=0}^{\infty} \frac{\widetilde{g}_i}{\widetilde{g}_0} \operatorname{codim}(V^{\widetilde{G}_i}), \tag{2.1}$$

où pour tout entier naturel i, le terme $\widetilde{G}_i$ désigne le $i^{\text{ème}}$ groupe de ramification d'un relèvement de p dans $\widetilde{N}$ et $\widetilde{g}_i$ l'ordre de ce groupe.

Le but de ce paragraphe est de calculer $n_p(\rho)$ pour tout nombre premier p. Si le calcul de cet entier est toujours élementaire, le nombre de cas à considérer lorsque $p = 2$ est important et nécessite une étude minutieuse de la ramification en 2 de l'extension $\widetilde{N}/\mathbb{Q}$. Nos résultats sont regroupés dans les propositions 2.1 et 2.2 et dans le tableau 3.

On considère S_4 comme l'ensemble des permutations du quadruplet $\{1, 2, 3, 4\}$. On note $\{1, \omega\}$ le centre de $\widetilde{S}_4$ et pour toute permutation σ de S_4, on fixe un représentant $\widetilde{\sigma}$ de σ dans $\widetilde{S}_4$. Soit

$$R = \{1, \omega, \widetilde{(12)}, \widetilde{(12)(34)}, \widetilde{(123)}, \omega\widetilde{(123)}, \widetilde{(1234)}, \omega\widetilde{(1234)}\}$$

un ensemble de représentants des huit classes de conjugaisons de $\widetilde{S}_4$. La représentation ρ que nous considérons a pour déterminant le caractère signature du groupe S_4. Les valeurs prises par le caractère $\mathrm{Tr}(\rho)$ de ρ sur chacune des classes de conjugaison de $\widetilde{S}_4$ sont décrites dans [Dornhoff 1971, § 28]. Puisque ρ est de degré 2, nous en déduisons immédiatement pour tout s de $\widetilde{S}_4$ le polynôme caractéristique de $\rho(s)$, qu'on note $P_s(x)$, et la codimension de l'espace propre associé à la valeur propre 1, qu'on note $V^{\langle s \rangle}$.

On commence par calculer $n_p(\rho)$ lorsque p est modérément ramifié dans $\widetilde{N}$ ou égal à 3.

Proposition 2.1. *Soit p un nombre premier modérément ramifié dans $N/\mathbb{Q}$. Alors $n_p(\rho) = 1$ si $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'\mathfrak{p}_1''$ et $n_p(\rho) = 2$ sinon.*

Preuve. Le résultat se déduit immédiatement de l'égalité (2.1) et du tableau 1. L'égalité $n_p(\rho) = 1$ se produit lorsque le groupe d'inertie d'un relèvement premier de p dans N est engendré par une transposition. Puisque $N/\mathbb{Q}$ est plongeable cette condition équivaut à l'égalité $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'\mathfrak{p}_1''$ [Jehanne 1995, lemme III.3 ; Cassou-Noguès et Jehanne 1996, tableau II.1]. □

Proposition 2.2. *Le nombre premier 3 est sauvagement ramifié dans N si et seulement si $3\mathcal{O}_K = \mathfrak{p}_1^3\mathfrak{p}_1'$. Dans ce cas, on a l'égalité $n_3(\rho) = n_3(K)$. Ainsi, $n_3(\rho) = 3$ ou 5 si 3 est ramifié dans k et $n_3(\rho) = 4$ sinon.*

Preuve. Le tableau 2.1 de [Cassou-Noguès et Jehanne 1996] nous donne l'équivalence souhaitée. Comme $\widetilde{N}/\mathbb{Q}$ est une extension $\widetilde{S}_4$-pure, ce tableau indique également que le groupe $\widetilde{G}_0$ est d'ordre 3 ou diédral d'ordre 6. Le résultat se déduit alors de [Serre 1980, chapitre 4]. □

Nous nous intéressons maintenant au calcul de $n_2(\rho)$. La connaissance de la ramification de 2 dans N et $\widetilde{N}$ étant fondamentale pour ce calcul, nous débutons cette étude en donnant le tableau 2, qui exhibe toutes les ramifications possibles de 2 dans une réalisation pure $\widetilde{N}$ du plongement.

s	1	ω	$\widetilde{(12)(34)}$	$\widetilde{(123)}$	$\omega\widetilde{(123)}$	$\widetilde{(12)}$	$\widetilde{(1234)}$	$\omega\widetilde{(1234)}$
$\mathrm{Tr}(\rho)(s)$	2	-2	0	-1	1	0	$i\sqrt{2}$	$-i\sqrt{2}$
$P_s(x)$	$(x-1)^2$	$(x+1)^2$	x^2+1	x^2+x+1	x^2-x+1	x^2-1	$x^2-i\sqrt{2}x-1$	$x^2+i\sqrt{2}x-1$
$\dim(V/V^{\langle s \rangle})$	0	2	2	2	2	1	2	2

TABLEAU 1. Ce tableau fournit un représentant s de chaque classe de conjugaison du groupe $\widetilde{S}_4$, la valeur de $\mathrm{Tr}(\rho)(s)$, le polynôme caractéristique de $\rho(s)$ et la codimension de l'espace invariant par $\rho(s)$.

Cas	C	L	k	K	K'	G_{-1}	G_0	$\widetilde{G}_0$
1	$\mathfrak{p}_1\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1\mathfrak{p}''_2$	$\mathfrak{p}_1\mathfrak{p}'_1$	$\mathfrak{p}_2^2$	$\mathfrak{p}_2^2\mathfrak{p}'^2_2$	$D_4 \subset A_4$	C_2	C_4
2	$\mathfrak{p}_1\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1\mathfrak{p}''_1\mathfrak{p}'''_1$	$\mathfrak{p}_1\mathfrak{p}'_1$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1$	$\prod_{i=1}^4 \mathfrak{p}_1^{(i)2}$	$C_2 \subset A_4$	C_2	C_4
3	$\mathfrak{p}_1\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1\mathfrak{p}''^2_1$	$\mathfrak{p}_1\mathfrak{p}'_1$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}'^4_1$	$D_4 \subset A_4$	D_4	H_8
4	$\mathfrak{p}_2\mathfrak{p}'_1$	$\mathfrak{p}_2^2\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_2$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1$	$\mathfrak{p}_2^2\mathfrak{p}'^2_2$	$D_4 \not\subset A_4$	$C_2 \subset A_4$	C_4
5	$\mathfrak{p}_2\mathfrak{p}'_1$	$\mathfrak{p}_2^2\mathfrak{p}'_2$	$\mathfrak{p}_2$	$\mathfrak{p}_2^2$	$\mathfrak{p}_2^2\mathfrak{p}'^2_2$	C_4	C_2	C_4
6	$\mathfrak{p}_2\mathfrak{p}'_1$	$\mathfrak{p}_2^2\mathfrak{p}'^2_1$	$\mathfrak{p}_2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_2^4$	D_8	$D_4 \subset A_4$	H_8
7	$\mathfrak{p}_3$	$\mathfrak{p}_3^2$	$\mathfrak{p}_1\mathfrak{p}'_1$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}'^4_1$	A_4	D_4	H_8
8	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_1^4\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1$	$\mathfrak{p}_1^4\mathfrak{p}'^4_1$	$D_4 \not\subset A_4$	D_4	D_8
9	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_1^4\mathfrak{p}'_2$	$\mathfrak{p}_1^2$	$\mathfrak{p}_2^2$	$\mathfrak{p}_2^4$	D_8	D_4	D_8
10	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_1^4\mathfrak{p}'^2_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}'^4_1$	C_4	C_4	C_8
11	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_1^4\mathfrak{p}'^2_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_2^4$	D_8	C_4	C_8
12	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_1^4\mathfrak{p}'^2_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^8$	D_8	D_8	$\widetilde{D}_8$
13	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_1^2\mathfrak{p}'_1\mathfrak{p}''^2_1\mathfrak{p}'''_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^2\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_1^2\mathfrak{p}'^2_1\mathfrak{p}''^2_1\mathfrak{p}'''^2_1$	$C_2 \not\subset A_4$	C_2	C_2
14	$\mathfrak{p}_1^2\mathfrak{p}'_1$	$\mathfrak{p}_2^2\mathfrak{p}'_1\mathfrak{p}''_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^2\mathfrak{p}'_2$	$\mathfrak{p}_2^2\mathfrak{p}'^2_2$	$D_4 \not\subset A_4$	$C_2 \not\subset A_4$	D_4
15	$\mathfrak{p}_1^3$	$\mathfrak{p}_1^6$	$\mathfrak{p}_1\mathfrak{p}'_1$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}'^4_1$	A_4	A_4	$\widetilde{A}_4$
16	$\mathfrak{p}_1^3$	$\mathfrak{p}_1^6$	$\mathfrak{p}_2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_2^4$	S_4	A_4	$\widetilde{A}_4$

TABLEAU 2. Ce tableau décrit les différentes possibilités de ramification de 2 dans certains sous-corps d'une S_4 extension de $\mathbb{Q}$ plongeable, les groupes G_{-1}, G_0 et le group $\widetilde{G}_0$ correspondant à un plongement pur de cette extension.

Le premier résultat obtenu est le suivant.

Proposition 2.3. *On a* $n_2(\rho) = \frac{1}{2}\big(n_2(\widetilde{K}) - n_2(K)\big)$.

Preuve. Soient E, F' et F des corps de nombres tels que $E \subset F' \subset F$, soit χ un caractère de $\mathrm{Gal}(F/F')$, on désigne par χ^* le caractère de $\mathrm{Gal}(F/E)$ induit par χ. Rappelons la formule d'induction des conducteurs : $\mathfrak{F}(\chi^*) = N_{F'/E}(\mathfrak{F}(\chi)) \cdot \mathfrak{d}_{F'/E}^{\chi(1)}$, où $\mathfrak{d}_{F'/E}$ désigne le discriminant relatif de F'/E.

Le corps $\widetilde{K}$ introduit au paragraphe 1 est l'une des sous-extensions de $\widetilde{N}$ telle que $\mathrm{Gal}(\widetilde{N}/\widetilde{K})$ soit diédral de degré 6. En appliquant successivement la formule d'induction aux caractères triviaux de $\mathrm{Gal}(\widetilde{N}/\widetilde{K})$ et $\mathrm{Gal}(\widetilde{N}/K)$, puis en décomposant dans chacun de ces deux cas le caractère de $\mathrm{Gal}(\widetilde{N}/\mathbb{Q})$ obtenu par induction en une somme de caractères irréductibles, on obtient que $\mathfrak{d}_{\widetilde{K}} = \mathfrak{d}_K \cdot \mathfrak{F}(\rho')$, où $\mathfrak{d}_K = d_K\mathbb{Z}$ et où ρ' est l'unique représentation de degré 4 de $\widetilde{S}_4$. La Führerdiskriminantenproduktformel fournit l'égalité $\mathfrak{d}_{\widetilde{N}} = \mathfrak{d}_N \cdot \mathfrak{F}(\rho)^4 \cdot \mathfrak{F}(\rho')^4$ et les formules de transitivité de la différente nous donnent : $\mathfrak{d}_{\widetilde{N}} = N_{\widetilde{K}/\mathbb{Q}}(\mathfrak{d}_{\widetilde{N}/\widetilde{K}}) \cdot \mathfrak{d}_{\widetilde{K}}^6$ et $\mathfrak{d}_N = N_{K/\mathbb{Q}}(\mathfrak{d}_{N/K}) \cdot \mathfrak{d}_K^6$. On en déduit :

$$\mathfrak{F}(\rho)^4 = \left(\frac{d_{\widetilde{K}}}{d_K}\right)^2 \cdot \frac{N_{\widetilde{K}/\mathbb{Q}}(\mathfrak{d}_{\widetilde{N}/\widetilde{K}})}{N_{K/\mathbb{Q}}(\mathfrak{d}_{N/K})}.$$

Si I et J sont des idéaux fractionnaires d'un corps de nombres, nous notons $I \sim J$ si l'idéal IJ^{-1} est premier avec 2. Pour achever la démonstration, il suffit de vérifier l'équivalence

$$N_{\widetilde{K}/\mathbb{Q}}(\mathfrak{d}_{\widetilde{N}/\widetilde{K}}) \sim N_{K/\mathbb{Q}}(\mathfrak{d}_{N/K}).$$

Supposons que $\widetilde{G}_0$ soit un 2-groupe, ce qui exclut les cas 15 et 16 du tableau 2. Comme $\widetilde{N}/\widetilde{K}'$ et N/K' sont non ramifiées au-dessus de 2, il suffit de montrer que $N_{\widetilde{K}/\mathbb{Q}}(\mathfrak{d}_{\widetilde{K}'/\widetilde{K}}) \sim N_{K/\mathbb{Q}}(\mathfrak{d}_{K'/K})$. Soit K'' la sous-extension quadratique de $\widetilde{K}'/K$ distincte de $\widetilde{K}$ et de K'. On déduit alors l'équivalence souhaitée des deux égalités

$$\mathfrak{d}_{K'/K} \cdot \mathfrak{d}_{K''/K} = N_{\widetilde{K}/K}(\mathfrak{d}_{\widetilde{K}'/\widetilde{K}}) \cdot \mathfrak{d}_{\widetilde{K}/K}$$

et $N_{K/\mathbb{Q}}(\mathfrak{d}_{\widetilde{K}/K}) = N_{K/\mathbb{Q}}(\mathfrak{d}_{K''/K})$. La démonstration dans le cas où $\widetilde{G}_0 \simeq \widetilde{A}_4$, qui est analogue, est laissée au lecteur. □

Nous terminons ce paragraphe en regroupant dans le tableau 3 les valeurs $n_2(\rho)$ et $n_2(K)$ obtenues dans les seize cas du tableau 2. Ce calcul, qui passe par la détermination des groupes de ramification possibles de l'extension $\widetilde{N}/\mathbb{Q}$, s'appuie sur [Serre 1980, chapitre 4, § 2 et § 3]. Après avoir remarqué l'égalité $n_2(K) = n_2(\theta)$, où θ est le caractère de la représentation de permutation de degré 4 du groupe $\mathrm{Gal}(N/\mathbb{Q})$ isomorphe à S_4, nous utilisons comme dans le cas impair l'égalité 2.1 pour le calcul de $n_2(\rho)$ et $n_2(\theta)$. Parmi les valeurs ainsi obtenues, certaines sont à éliminer pour diverses raisons : les relations entre les discriminants des corps contenus dans N (voir par exemple [Jehanne 1995, p. 263]) qui impliquent les congruences de $n_2(K)$, $n_2(k)$ et $n_2(C)$ modulo 2, la proposition 2.3 dont on déduit la parité de $n_2(\widetilde{K}) - n_2(K)$, les conditions à satisfaire données dans [Jehanne 1995] pour que N soit plongeable et enfin les formules données par Kiming dans [Kiming 1994, théorème 1 et proposition 2]. De ces formules de Kiming, on déduit en effet que lorsque le groupe de décomposition d'un relèvement premier de 2 dans N est soit diédral, soit égal à A_4 ou S_4 — ce qui est respectivement le cas pour les lignes 1, 3, 4, 6, 8, 9, 11, 12, 14, et pour les lignes 7, 15 et 16 du tableau 2 — alors, soit $n_2(\rho)$ est la valuation en 2 du conducteur d'un “relèvement minimal” de la représentation projective $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ associée à ρ, soit $n_2(\rho)$ est pair. Nous avons calculé dans chaque cas cette valuation minimale notée $n_2(\rho_m)$ et nous l'avons comparée à $n_2(\rho)$. Signalons enfin que la théorie de Kummer nous a permis à plusieurs reprises de majorer $v_2(d_{\widetilde{K}})$. Le résultat utilisé est le lemme suivant (voir par exemple [Hecke 1981]).

Lemme 2.4. *Soient F une extension finie de $\mathbb{Q}_2$ et $E = F(\sqrt{\gamma})$ une extension quadratique de F, où $\gamma \in F^* \smallsetminus F^{*2}$ vérifie : $v_F(\gamma) = 0$ ou 1. On note $\mathfrak{p}_F$ l'idéal de valuation de F, v_F la valuation normalisée associée et $e = v_F(2)$.*

1. *Si $v_F(\gamma) = 1$, l'extension E/F est ramifiée et $v_F(d_{E/F}) = 2e + 1$.*
2. *Si $v_F(\gamma) = 0$, on note n le plus grand entier tel que la congruence $\gamma \equiv x^2 \bmod \mathfrak{p}_F^n$ ait une solution dans F. Alors $n \le 2e$. En outre, si $n = 2e$, l'extension E/F est non ramifiée et si $n \ne 2e$, cette extension est ramifiée, n est impair et si l'on écrit $n = 2a + 1$, alors $v_F(d_{E/F}) = 2(e - a)$.*

La détermination dans chacun des cas des valeurs possibles de $n_2(K)$ et $n_2(\rho)$ est élémentaire mais technique. Nous choisissons d'expliquer nos méthodes en traitant en détail deux des cas du tableau 2.

Supposons que $\widetilde{G}_0 \simeq D_4$. Puisque $N/\mathbb{Q}$ est plongeable, nous savons grâce à [Jehanne 1995, lemme III.3] que $n_2(k)$ et donc $n_2(K)$ sont pairs. On en déduit l'égalité $n_2(K) = 2$. L'étude des sauts de ramification possibles pour l'extension $\widetilde{N}/\mathbb{Q}$ nous conduit à considérer cinq cas. Le calcul de la valeur de $n_2(K)$ pour chaque cas implique que seuls les deux premiers sont à conserver.

$$\widetilde{G}_0 = \widetilde{G}_1, \qquad \widetilde{G}_2 = \{1\}, \tag{2.2}$$

$$\widetilde{G}_0 = \widetilde{G}_1 \supset \widetilde{G}_2 = \widetilde{G}_3 = \langle\omega\rangle, \quad \widetilde{G}_4 = \{1\}. \tag{2.3}$$

Par l'égalité (2.1), on calcule $n_2(\rho) = 4$ dans le cas (2.2) et $n_2(\rho) = 6$ dans le cas (2.3).

On suppose maintenant que $\widetilde{G}_0 = D_8$. Par le tableau 2, nous savons qu'alors $2\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'^2$ ou $\mathfrak{p}_2^2$. Le lemme 2.4 conduit à la majoration $n_2(K) \le 6$. Nous avons alors quatre possibilités pour les suites de ramifications

$$\widetilde{G}_0 = \widetilde{G}_1 \supset \widetilde{G}_2 = \widetilde{G}_3 = \cdots = \widetilde{G}_t = \langle\omega\rangle, \quad t \in \{3, 5, 7\}, \tag{2.4}$$

$$\widetilde{G}_0 = \widetilde{G}_1 \supset \widetilde{G}_2 = \widetilde{G}_3 = \langle\omega, \tilde{\tau}\rangle \supset \widetilde{G}_4 = \cdots = \widetilde{G}_t = \langle\omega\rangle, \quad t \in \{5, 7\}, \tag{2.5}$$

$$\widetilde{G}_0 = \widetilde{G}_1 \supset \widetilde{G}_2 = \widetilde{G}_3 = \langle\tilde{\sigma}\rangle \supset \widetilde{G}_4 = \cdots = \widetilde{G}_t = \langle\omega\rangle, \quad t \in \{5,7\}, \qquad (2.6)$$

$$\widetilde{G}_0 = \widetilde{G}_1 = \widetilde{G}_2 \supset \widetilde{G}_3 = \widetilde{G}_4 = \cdots = \widetilde{G}_t = \langle\omega\rangle, \quad t \in \{4,6,8\}, \qquad (2.7)$$

où $\tilde{\sigma}$ est d'ordre 4, et où dans tous les cas $\widetilde{G}_{t+1} = \{1\}$. La formule (2.1) donne pour chacune de ces suites les valeurs de $n_2(K)$ et $n_2(\rho)$ indiquées dans le tableau suivant.

Cas	(2.4)	(2.5)	(2.6)	(2.7)
$n_2(K)$	4	5	6	6
$n_2(\rho)$	$4+\frac{1}{2}(t-1)$	$6+\frac{1}{2}(t-3)$	$6+\frac{1}{2}(t-3)$	$6+\frac{1}{2}(t-2)$

De la proposition 2.3 on déduit que $2n_2(\rho) = n_2(K)+v_2(N_{K/\mathbb{Q}}(d_{\widetilde{K}/K}))$. Si $n_2(K)$ est impair, alors $v_2(N_{K/\mathbb{Q}}(d_{\widetilde{K}/K}))$ est impair. C'est donc que $2\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'^2$. On en déduit l'égalité : $2n_2(\rho) = n_2(K) + v_{\mathfrak{p}_1}(d_{\widetilde{K}/K}) + v_{\mathfrak{p}_1'}(d_{\widetilde{K}/K})$. Le lemme 2.4 implique que $v_{\mathfrak{p}_1}(d_{\widetilde{K}/K})$ (tout comme $v_{\mathfrak{p}_1'}(d_{\widetilde{K}/K})$) est soit pair et inférieur ou égal à 4, soit égal à 5. On en déduit que $n_2(K) \le 7$, ce qui interdit la valeur t=7 dans le cas (2.5). Le calcul de $n_2(\rho_m)$, par les formules de [Kiming 1994, théorème 1], nous permet d'éliminer la valeur t= 7 dans le cas (2.4) et les valeurs t= 4 et t= 8 dans le cas (2.7).

Comme nous l'avons déjà indiqué, étant donnée une représentation projective r, l'entier $n_2(\rho)$ peut dépendre du choix du relèvement $\widetilde{S}_4$-pur ρ de r choisi. Nous avons répondu à cette question par la proposition 2.5 suivante et avons porté les résultats obtenus dans le tableau 3.

Proposition 2.5. *Soit N une S_4-extension de $\mathbb{Q}$ plongeable et soit r une représentation projective telle que $N = (\mathbb{Q}^c)^{\mathrm{Ker}(r)}$. Soit $\mathcal{R}_r(\widetilde{S}_4)$ l'ensemble des relèvements $\widetilde{S}_4$-purs de r.*

Dans les cas 3, 11, 13 *et* 22 *du tableau* 3 *toutes les valeurs de $n_2(\rho)$ indiquées sont atteintes quand ρ parcourt $\mathcal{R}_r(\widetilde{S}_4)$. Dans chacun de ces cas, $\mathcal{R}_r(\widetilde{S}_4)$ contient donc un relèvement minimal en* 2.

Dans les cas 8, 10, 12, 18 *et* 23 *du tableau* 3, *$n_2(\rho)$ est constant quand ρ parcourt $\mathcal{R}_r(\widetilde{S}_4)$. De plus, dans le cas* 20, *$n_2(\rho) = 6$ si et seulement si $p\mathcal{O}_K = \mathfrak{p}_2^2$.*

Preuve. Nous nous contentons de démontrer ce résultat dans les cas 22 et 23 du tableau 3. Les autres cas se résolvent de la même façon.

On suppose donc que $2\mathcal{O}_K = \mathfrak{p}^4$. Si $\widetilde{K} = K(\sqrt{\gamma})$ désigne la réalisation du plongement correspondant à ρ, la proposition 2.3 donne l'égalité : $n_2(\rho) = \frac{1}{2}(n_2(K) + v_{\mathfrak{p}}(\mathfrak{d}_{\widetilde{K}/K}))$. Comme $n_2(K)$ est pair, on peut supposer que $v_{\mathfrak{p}}(\gamma) = 0$. On utilise le lemme 2.4 pour calculer la valuation $v_{\mathfrak{p}}(\mathfrak{d}_{\widetilde{K}/K})$). Soit π une uniformisante du complété $K_{\mathfrak{p}}$ de K en $\mathfrak{p}$. On écrit dans $K_{\mathfrak{p}}$: $2 = \varepsilon\pi^4$, où ε désigne une unité de $K_{\mathfrak{p}}$. Soit $X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ le polynôme minimal de π. C'est un polynôme d'Eisenstein. Pour tout $i \in \{1,2,3,4\}$, on pose $a_i' = a_i/2$. On obtient :

$$-a_0'\varepsilon = 1 + a_1'\varepsilon\pi + a_2'\varepsilon\pi^2 + a_3'\varepsilon\pi^3.$$

Si $n_2(K) = 4$, alors $v_2(a_1) = 1$ et $\varepsilon \equiv 1 + \pi \bmod \mathfrak{p}^2$. Ainsi ε n'est-il pas un carré modulo $\mathfrak{p}^2$. Comme $(\mathcal{O}_K/\mathfrak{p}^2)^*$ est d'ordre 2, on en déduit que si $\gamma \notin (\mathcal{O}_K/\mathfrak{p}^2)^{*2}$, c'est-à-dire si $n_2(\rho) = 6$, alors $\varepsilon\gamma \equiv 1 \bmod \mathfrak{p}^2$. La réalisation du plongement donnée par $K(\sqrt{2\gamma})$ fournit donc un relèvement $\widetilde{S}_4$-pur de r tel que $n_2(\rho) = 3$ ou 4. Si $n_2(\rho) = 3$ ou 4, alors dans $K_{\mathfrak{p}}$, on peut écrire $\gamma = x^2 + u\pi^5$ et $-\gamma = y^2 + v\pi^5$, où x et y désignent des unités de $K_{\mathfrak{p}}$ et où u et v appartiennent à l'anneau de valuation de $K_{\mathfrak{p}}$. On a alors $(x+y)^2 = 2xy - \pi^5(u+v)$ et donc $v_{\mathfrak{p}}(x+y) = 2$. Un calcul supplémentaire montre que $(u+v)\pi \equiv 1 + \varepsilon \bmod \mathfrak{p}^2$. Or on a montré que $1 + \varepsilon \notin \mathfrak{p}^2$. On en déduit que $u + v \notin \mathfrak{p}$ et donc que l'on passe de l'une à l'autre des valeurs $n_2(\rho) = 3$ et 4 en substituant $-\gamma$ à γ.

Si $n_2(K) = 8$, alors $v_2(a_1) = 2$ et $v_2(a_3) \ge 2$. On en déduit que $\varepsilon \equiv 1 \bmod \mathfrak{p}^2$. On voit en outre qu'on ne modifie pas $n_2(\rho)$ en multipliant γ par un entier relatif impair. $\square$

Théorème 2.6. *Quand ρ parcourt les représentations de $\mathcal{R}$ dont le noyau fixe une $\widetilde{S}_4$-extension de $\mathbb{Q}$, le plus petit conducteur $\mathfrak{F}(\rho)$ est égal à* 283, *et le plus petit conducteur pair est* 344.

Preuve. Le conducteur $\mathfrak{F}(\rho) = 283$ (resp. 344) correspond au corps quartique de discriminant -283 (resp. -688). Les propositions 2.1 et 2.5 et le tableau ci-dessous permettent de majorer les valeurs absolues des discriminants susceptibles de correspondre à une représentation ρ de conducteur im-

Ramification dans K	G_{-1}	G_0	$\widetilde{G}_0$	$n_2(K)$	$n_2(\rho_m)$	$n_2(\rho)$	Cas
$\mathfrak{p}_1^2\mathfrak{p}'\mathfrak{p}''$	$C_2 \not\subseteq A_4$	C_2	C_2	2	2	2	1
				3	3	3	2
$\mathfrak{p}_1^2\mathfrak{p}_2'$	$D_4 \not\subseteq A_4$	$C_2 \not\subseteq A_4$	D_4	2	4	4 et 6	3
$\mathfrak{p}_1^2\mathfrak{p}_1'^2$	$D_4 \not\subseteq A_4$	$C_2 \subset A_4$	C_4	4	4	6	4
				6	6	8	5
$\mathfrak{p}_1^2\mathfrak{p}_1'^2$ ou $\mathfrak{p}_2^2$	$C_2 \subset A_4$ ou C_4	C_2	C_4	4	2	6	6
				6	3	8	7
$\mathfrak{p}_1^2\mathfrak{p}_1'^2$ ou $\mathfrak{p}_2^2$	$D_4 \not\subseteq A_4$ ou D_8	$D_4 \not\subseteq A_4$	D_8	4	5	5 ou 6	8
				5	7	7	9
				6	7	7 ou 8	10
$\mathfrak{p}^4$	$D_4 \subset A_4$ ou D_8	$D_4 \subset A_4$	H_8	6	5	5 et 6	11
				8	7	7 ou 8	12
$\mathfrak{p}^4$	A_4	D_4	H_8	6	5	5 et 6	13
$\mathfrak{p}^4$	C_4	C_4	C_8	8	3	8	14
				11	4	10	15
$\mathfrak{p}^4$	D_8	C_4	C_8	8	8	8	16
				11	10	10	17
$\mathfrak{p}^4$	D_8	D_8	$\widetilde{D}_8$	8	7	7 ou 8	18
				9	9	9	19
				10	8	8	20
				11	4	10	21
$\mathfrak{p}^4$	A_4 ou S_4	A_4	$\widetilde{A}_4$	4	3	$3, 4$ et 6	22
				8	7	7 ou 8	23

TABLEAU 3. Pour chaque possibilité de ramification de 2 dans un sous-corps quartique K d'une S_4 extension plongeable associée à une représentation galoisienne projective r, ce tableau rappelle les groupes G_{-1}, G_0 et le groupe $\widetilde{G}_0$ correspondant à un plongement pur. Il donne les valuations en 2, notées $n_2(K)$, $n_2(\rho_m)$ et $n_2(\rho)$, du discriminant de K, du conducteur d'un relèvement minimal de r et du conducteur du relèvement ρ de r de type octaédral associé à ce plongement. La mention "et" dans la colonne $n_2(\rho)$ indique que chacune des valeurs est réalisée, tandis que "ou" indique qu'il n'y a qu'une valeur réalisée (proposition 2.5).

pair inférieur à 283 ou de conducteur pair et inférieur à 344. L'examen d'une table de corps quartiques de signature mixte permet alors de conclure. □

3. COEFFICIENTS DE FOURIER

Nous reprenons les notations des paragraphes précédents et décrivons la méthode utilisée dans les exemples du paragraphe 4 pour calculer les coefficients a_p de la série L associée à ρ

$$L(s,\rho)=\sum_{n=1}^{\infty} a_n n^{-s},$$

où p parcourt l'ensemble $\mathcal{E}_\rho$ des nombres premiers ne divisant pas le conducteur $\mathfrak{F}(\rho)$ de ρ. Soit p un tel nombre premier. La valeur de a_p, dont le calcul se ramène en fait à un calcul de substitution de Frobenius, dépend fortement de la décomposition de p dans K et $\tilde{K}$. Les résultats utilisés dans les exemples du paragraphe 4 sont décrits dans le tableau 4 et les lemmes 3.1 et 3.2.

Dans tout ce paragraphe, p désigne un nombre premier de $\mathcal{E}_\rho$.

Par définition de L, on a :

$$a_p = \operatorname{Tr}\left(\rho(\tilde{\pi}_p)\right),$$

où $\tilde{\pi}_p$ désigne la substitution de Frobenius (définie à conjugaison près) de $\mathrm{Gal}(\tilde{N}/\mathbb{Q})$ associée à l'un quelconque des idéaux premiers de $\tilde{N}$ divisant p. C'est donc la classe de conjugaison de cet élément $\tilde{\pi}_p$ — appelée également substitution de Frobenius en p associée à l'extension $\tilde{N}/\mathbb{Q}$ — qu'il nous faut calculer.

Soit π_p la substitution de Frobenius de p associée à l'extension $N/\mathbb{Q}$. Le tableau 4 montre que sa classe de conjugaison est uniquement déterminée par la décomposition de p dans K. Cette décomposition permet donc le calcul de $\tilde{\pi}_p$ à un éventuel facteur ω près. Comme $\rho(\omega) = -\mathrm{Id}$, on en déduit la valeur de a_p^2 (voir le tableau 2.1).

Il reste à déterminer le signe de a_p dans les cas 1, 4 et 5 du tableau 4. Dans les cas 1 et 4, l'ordre de $\tilde{\pi}_p$

Cas	$p\mathcal{O}_K$	π_p	$\tilde{\pi}_p$	a_p^2
1	$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''\mathfrak{p}_1'''$	1	1 ou ω	4
2	$\mathfrak{p}_2\mathfrak{p}_2'$	(12)(34)	$\widetilde{(12)(34)}$	0
3	$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_2''$	(12)	$\widetilde{(12)}$	0
4	$\mathfrak{p}_1\mathfrak{p}_3'$	(123)	$\widetilde{(123)}$ ou $\omega\widetilde{(123)}$	1
5	$\mathfrak{p}_4$	(1234)	$\widetilde{(1234)}$ ou $\omega\widetilde{(1234)}$	−2

TABLEAU 4. Si K est un corps quartique de type S_4, de clôture galoisienne $\tilde{N}$, pour chaque nombre premier impair p non ramifié dans K, ce tableau fournit selon la décomposition de p dans K les substitutions de Frobenius π_p et $\tilde{\pi}_p$, définies à conjugaison près dans $\mathrm{Gal}(N/\mathbb{Q})$ et $\mathrm{Gal}(\tilde{N}/Q)$, ainsi que la valeur du carré de la trace a_p de l'image de $\tilde{\pi}_p$ par une représentation octaédrale ρ associée à $\tilde{N}$.

permet de trancher et la décomposition de p dans $\tilde{K}$ donne la valeur de a_p.

Lemme 3.1. *Dans le cas* 1 *du tableau* 4 :

- $a_p = 2$ *si et seulement si* $p\mathcal{O}_{\tilde{K}} = \prod_{i=1}^{8}\mathfrak{p}_1^{(i)}$.
- $a_p = -2$ *si et seulement si* $p\mathcal{O}_{\tilde{K}} = \prod_{i=1}^{4}\mathfrak{p}_1^{(i)}$.

Dans le cas 4 *du tableau* 4 :

- $a_p = 1$ *si et seulement si* $p\mathcal{O}_{\tilde{K}} = \mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_3''\mathfrak{p}_3'''$.
- $a_p = -1$ *si et seulement si* $p\mathcal{O}_{\tilde{K}} = \mathfrak{p}_2\mathfrak{p}_6'$.

Dans le cas 5, l'élément $\tilde{\pi}_p$ peut être égal à $\widetilde{(1234)}$ ou à $\omega\widetilde{(1234)}$, qui engendrent des groupes conjugués. Par conséquent, la connaissance du groupe de décomposition est insuffisante pour distinguer les deux possibilités. Il faut donc être plus précis et déterminer la substitution de Frobenius $\tilde{\pi}_{\tilde{\mathfrak{p}}}$, d'un idéal premier $\tilde{\mathfrak{p}}$ de $\tilde{N}$ relevant p donné.

Pour ce faire, on pose $\tilde{N} = N(\sqrt{\gamma})$, où $\gamma \in K$, et $s = (1234)$. Comme l'extension $\tilde{N}/\mathbb{Q}$ est galoisienne, il existe un élément $b \in N^*$ tel que $s(\gamma) = b^2\gamma$. Soit δ une racine carrée arbitraire de γ, on suppose que $\tilde{s}(\delta) = b\delta$. Soit $\mathfrak{p}$ un idéal premier de N relevant p, de substitution de Frobenius égale à s, on note $\tilde{\mathfrak{p}}$ l'unique idéal premier de $\tilde{N}$ relevant $\mathfrak{p}$. Le lemme suivant donne, pour un nombre premier p tel que $p\mathcal{O}_K = \mathfrak{p}_4$, le coefficient a_p de la représentation ρ qui vérifie : $\operatorname{Tr}(\rho)(\tilde{s}) = i\sqrt{2}$. Comme $v_{\mathfrak{p}}(\gamma)$

est pair, on peut se ramener en multipliant γ par un carré de K au cas où γ est premier à $\mathfrak{p}$. On démontre alors le résultat suivant.

Lemme 3.2. *On suppose p impair. Soit L le corps inclus dans N fixé par s. Alors $p\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_1'\mathfrak{P}_4''$. De plus, dans le cas 5 du tableau 4 :*

- *$a_p = i\sqrt{2}$ si et seulement si $N_{N/L}(\delta^{p-1} - b) \in \mathfrak{P}_1 \cup \mathfrak{P}_1'$.*
- *$a_p = -i\sqrt{2}$ si et seulement si $N_{N/L}(\delta^{p-1} + b) \in \mathfrak{P}_1 \cup \mathfrak{P}_1'$.*

Preuve. Comme $\widetilde{\pi}_{\widetilde{\mathfrak{p}}}(\delta) \equiv \delta^p \bmod \widetilde{\mathfrak{p}}$, on a $\widetilde{\pi}_{\widetilde{\mathfrak{p}}} = \widetilde{s}$ si et seulement si $\delta^{p-1} \equiv b \bmod \mathfrak{p}$ et $\widetilde{\pi}_{\widetilde{\mathfrak{p}}} = \omega\widetilde{s}$ si et seulement si $\delta^{p-1} \equiv -b \bmod \mathfrak{p}$. Comme le groupe de décomposition de $\mathfrak{p}$ est égal à $\langle s\rangle = \mathrm{Gal}(N/L)$, son indice résiduel dans l'extension N/L est égal à 4, ce qui montre que $\mathfrak{p}$ relève $\mathfrak{P}_1$ ou $\mathfrak{P}_1'$. Soit $\alpha_\varepsilon = N_{N/L}(\delta^{p-1} - \varepsilon b)$, où $\varepsilon \in \{\pm 1\}$, on a : $\delta^{p-1} \equiv \varepsilon b \bmod \mathfrak{p}$ si et seulement si $\alpha_\varepsilon \in \mathfrak{P}_1$ ou $\mathfrak{P}_1'$. On en déduit que $\widetilde{\pi}_{\widetilde{\mathfrak{p}}} = \widetilde{s}$ si et seulement si $N_{N/L}(\delta^{p-1} - b) \in \mathfrak{P}_1 \cup \mathfrak{P}_1'$ et que $\widetilde{\pi}_{\widetilde{\mathfrak{p}}} = \omega\widetilde{s}$ si et seulement si $N_{N/L}(\delta^{p-1} + b) \in \mathfrak{P}_1 \cup \mathfrak{P}_1'$. □

4. RÉSULTATS NUMÉRIQUES

Ce paragraphe regroupe les résultats numériques annoncés dans l'introduction : on trouve dans le tableau 5 des réalisations de plongements $\widetilde{S}_4 \to S_4$, avec le conducteur de la représentation ρ correspondante. Les tableaux 6, 7 et 8 donnent un certain nombre de coefficients de Fourier à l'infini des formes primitives correspondant à trois de ces réalisations. Ces tableaux ont été obtenus grâce aux méthodes exposées dans les paragraphes précédents, lesquelles pourraient permettre d'établir des tables étendues regroupant de tels résultats.

	$\Delta(K)$	Pol. de rupture de K	Cas	Cond. ρ	Polynôme de rupture de $\widetilde{K}$
1	$-688 = -2^4.43$	X^4-2X-1	16	$2^3.43$	$X^8+12X^6-22X^4+96X^2-43$
				$2^4.43$	$X^8-12X^6-22X^4-96X^2-43$
				$2^6.43$	$X^8+24X^6-88X^4+768X^2-688$
2	$-1588 = -2^2.397$	$X^4+X^3-3X^2+2$	14	$2^4.397$	$X^8-21X^6+222X^4-341X^2-397$
				$2^6.397$	$X^8-42X^6+888X^4-2728X^2-6352$
3	$-3424 = -2^5.107$	X^4-3X^2+2X+2	8	$2^7.107$	$X^8+12X^6-363X^4+2474X^2-214$
4	$-3776 = -2^6.59$	X^4+2X^3-2	6	$2^5.59$	$X^8+32X^6+224X^4-1536X^2-15104$
				$2^6.59$	$X^8+16X^6+56X^4-192X^2-944$
5	$-4864 = -2^8.19$	X^4+4X+2	16	$2^7.19$	$X^8+16X^6+88X^4+128X^2-304$
6	$-5184 = -2^6.3^4$	$X^4+2X^3-3X^2-2X-1$	9	$2^8.3^4$	$X^8-8X^6-18X^4-16X^2-4$
7	$-6848 = -2^6.107$	$X^4+2X^3-5X^2+2X-1$	5	$2^8.107$	$X^8-20X^6-114X^4+264X^2-428$
8	$-7492 = -2^2.1873$	$X^4+X^3-2X^2+2X-4$	13	$2^2.1873$	$X^8+38X^6-1152X^4+7722X^2-1873$
9	$-7744 = -2^6.11^2$	$X^4+2X^3-3X^2+2$	8	$2^8.11^2$	$X^8-8X^6+16X^4-16X^2-4$
10	$-8392 = -2^3.1049$	$X^4+X^3-5X^2+X-2$	13	$2^3.1049$	$X^8+7X^6-47X^4-535X^2-2098$
11	$-8752 = -2^4.547$	$X^4+2X^3+4X^2+2X-2$	4	$2^6.547$	$X^8+2X^6+46X^4-152X^2-547$
12	$-8896 = -2^6.139$	$X^4+2X^3-3X^2+4X-2$	4	$2^8.139$	$X^8+16X^6+68X^4+320X^2-556$

TABLEAU 5. Quelques corps quartiques K de type S_4 dont la clôture galoisienne N est plongeable dans une $\widetilde{S}_4$-extension, avec des réalisations de plongements $\widetilde{S}_4 \to S_4$, le conducteur d'une représentation ρ associée au plongement et le cas correspondant dans le tableau 2.

Pour chaque corps K dans le tableau 5, la méthode décrite au paragraphe 2 nous a permis de construire une extension quadratique $\tilde{K}$ de K dont la clôture galoisienne $\tilde{N}$ est une réalisation pure du plongement. Nous donnons le conducteur de la représentation galoisienne ρ (définie au paragraphe 2) associée à $\tilde{N}$. De plus, lorsque la valuation $n_2(\rho)$ en 2 de ce conducteur peut atteindre différentes valeurs selon la réalisation $\tilde{N}$ choisie, nous avons également construit des corps $\tilde{K}$ correspondant à ces valeurs. Le tableau 5 regroupe ces résultats en sept colonnes qui donnent de gauche à droite, le numéro de ligne dans le tableau, le discriminant de K, la factorisation de ce discriminant en produit de facteurs premiers, un polynôme de rupture de K, le numéro du cas correspondant dans le tableau 2, les conducteurs de ρ possibles et des polynômes de rupture des corps $\tilde{K}$ associés à chacun de ces conducteurs.

L'exemple situé ligne 1 de ce tableau 5 fait partie de la famille de corps donnée dans la proposition IV.5 de [Cassou-Noguès et Jehanne 1996] : il s'agit des corps de rupture K_n des polynômes $X^4 - 2nX - 1$, où n désigne un nombre entier impair. Soient E_n la courbe elliptique d'équation $y^2 = x^3 + 4x + 4n^2$ et P le point de coordonnées affines $P = (0, 2n)$. Le corps N_n obtenu par adjonction à $\mathbb{Q}$ des points de 2-division de E et de $\frac{1}{2}P$ est une clôture galoisienne de K_n. On vérifie que le groupe d'inertie de $N_n/\mathbb{Q}$ en 2 est isomorphe au groupe alterné A_4 et que la valuation $n_2(K_n)$ du discriminant d_{K_n} est égale à 4. Pour tout n impair, nous sommes donc dans le cas 22 du tableau 3. Nous obtenons le résultat suivant.

Proposition 4.1. *On suppose que $16 + 27n^4$ soit un nombre premier p. Alors il existe une extension galoisienne $\tilde{N}$ de $\mathbb{Q}$ à groupe de Galois $\tilde{S}_4$ contenant N et une représentation galoisienne irréductible $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ telle que $(\mathbb{Q}^c)^{\mathrm{Ker}(\rho)} = \tilde{N}_n$ et dont la forme primitive associée soit de niveau $8p$.*

Remarques. 1. Le tableau IV.6 de [Cassou-Noguès et Jehanne 1996] laisse penser qu'il existe une infinité d'entiers n vérifiant l'hypothèse de la proposition.

2. La représentation ρ de la proposition est un relèvement primitif minimal de la représentation projective $r = \bar{\rho}$.

Les tableaux 6, 7 et 8 se rapportent respectivement aux lignes 1, 2 et 3 du tableau 5, sachant que pour les lignes 1 et 2, on considère la réalisation du plongement correspondant au plus petit conducteur $\mathfrak{F}(\rho)$. Les coefficients de Fourier a_p, où p parcourt les nombres premiers non ramifiés dans K ont été calculés pour $p < 5000$, mais pour des raisons de place, nous nous sommes limités dans la présentation des résultats à une ligne de nombres premiers p pour chacune des huit valeurs que peut prendre a_p.

p	$\tilde{\pi}_p$	a_p
$487, 619, 719, 1013, 1669, 1987, 2207, 3011, 3041, 4657$	1	2
$173, 827, 857, 1543, 1831, 2347, 3089, 3191, 3583, 3779, 4357, 4409$	ω	-2
$47, 59, 79, 107, 181, 197, 239, 293, 367, 397, 443, 461, 613, 643, 701, 769, 787, 797, 809, 977$	$\widetilde{(12)(34)}$	0
$19, 37, 71, 113, 131, 137, 149, 157, 191, 199, 211, 227, 233, 241, 263, 373, 383, 389, 421, 467$	$\widetilde{(12)}$	0
$11, 17, 53, 67, 97, 101, 103, 127, 193, 251, 271, 311, 379, 431, 509, 541, 563, 569, 599, 617$	$\widetilde{(123)}$	-1
$13, 23, 31, 41, 83, 109, 139, 167, 229, 269, 281, 283, 307, 317, 337, 353, 359, 401, 439, 479$	$\omega\widetilde{(123)}$	1
$3, 5, 73, 151, 163, 257, 313, 331, 347, 349, 409, 419, 433, 449, 523, 577, 641, 751, 773, 811$	$\widetilde{(1234)}$	$i\sqrt{2}$
$7, 29, 61, 89, 179, 223, 277, 457, 463, 491, 499, 521, 571, 593, 673, 691, 839, 937, 983, 991$	$\omega\widetilde{(1234)}$	$-i\sqrt{2}$

TABLEAU 6. Forme primitive associée à une représentation ρ de conducteur $\mathfrak{F}(\rho) = 2^3.43$. Le caractère quadratique χ est défini sur $(\mathbb{Z}/344\mathbb{Z})^*$ par le symbole de Legendre $\left(\frac{-43}{\cdot}\right)$, avec la convention habituelle.

p	$\widetilde{\pi}_p$	a_p
$419, 461, 811, 1553, 2099, 3769, 4357, 4751$	1	2
$211, 463, 563, 883, 1181, 1877, 1931, 2029, 3109, 3299, 3643$	ω	-2
$199, 223, 239, 283, 311, 379, 401, 433, 541, 593, 619, 653, 743, 797, 881, 1039, 1123, 1297$	$\widetilde{(12)(34)}$	0
$19, 23, 47, 53, 61, 67, 83, 89, 107, 113, 163, 181, 191, 233, 241, 269, 313, 373, 431, 479, 487$	$\widetilde{(12)}$	0
$7, 29, 37, 59, 71, 97, 103, 137, 139, 229, 251, 263, 281, 293, 331, 409, 659, 701, 769, 787, 829$	$\widetilde{(123)}$	-1
$73, 173, 227, 257, 277, 347, 349, 353, 359, 443, 467, 491, 521, 547, 557, 569, 571, 607, 673$	$\omega\widetilde{(123)}$	1
$5, 17, 31, 101, 149, 151, 167, 179, 271, 337, 421, 457, 499, 509, 599, 601, 733, 773, 827, 1019$	$\widetilde{(1234)}$	$i\sqrt{2}$
$3, 11, 13, 41, 43, 79, 109, 127, 131, 157, 193, 197, 307, 317, 367, 383, 389, 439, 449, 587, 613$	$\omega\widetilde{(1234)}$	$-i\sqrt{2}$

TABLEAU 7. Forme primitive associée à une représentation ρ de conducteur $\mathfrak{F}(\rho) = 2^4.397$. Le caractère quadratique χ est défini sur $(\mathbb{Z}/6352\mathbb{Z})^*$ par le symbole de Legendre $\left(\frac{-1588}{\cdot}\right)$.

p	$\widetilde{\pi}_p$	a_p
$223, 937, 1013, 1481, 1697, 1931, 2677, 2803, 3253, 3413, 3463, 3593, 4723$	1	2
$109, 743, 839, 1091, 1303, 2767, 2917, 3323, 3449, 4133, 4243, 4337, 4987$	ω	-2
$139, 157, 179, 239, 263, 269, 307, 349, 383, 439, 499, 503, 557, 619, 829, 857, 881, 907, 971$	$\widetilde{(12)(34)}$	0
$19, 31, 37, 53, 101, 103, 163, 191, 227, 257, 281, 331, 373, 397, 401, 409, 433, 461, 487, 521$	$\widetilde{(12)}$	0
$5, 23, 43, 59, 79, 89, 151, 173, 181, 193, 199, 229, 233, 241, 277, 313, 347, 389, 419, 431, 457$	$\widetilde{(123)}$	-1
$41, 47, 67, 131, 137, 211, 271, 317, 337, 379, 443, 541, 563, 569, 577, 599, 613, 727, 739, 757$	$\omega\widetilde{(123)}$	1
$3, 11, 29, 71, 73, 83, 97, 127, 149, 167, 197, 283, 311, 421, 449, 467, 479, 641, 677, 719, 883$	$\widetilde{(1234)}$	$i\sqrt{2}$
$7, 13, 17, 61, 113, 251, 293, 353, 359, 367, 509, 617, 631, 661, 811, 983, 1009, 1033, 1087$	$\omega\widetilde{(1234)}$	$-i\sqrt{2}$

TABLEAU 8. Forme primitive associée à une représentation ρ de conducteur $\mathfrak{F}(\rho) = 2^7.107$. Le caractère quadratique χ est défini sur $(\mathbb{Z}/13696\mathbb{Z})^*$ par le symbole de Legendre $\left(\frac{-856}{\cdot}\right)$.

BIBLIOGRAPHIE

[Batut et al. 1995] C. Batut, D. Bernardi, H. Cohen, et M. Olivier, *User's Guide to Pari-GP* 1.39, ftp://megrez.math.u-bordeaux.fr/pub/pari, 1995.

[Bayer et Frey 1991] P. Bayer et G. Frey, "Galois representations of octahedral type and 2-coverings of elliptic curves", *Math. Z.* **207** (1991), 395–408.

[Buhler 1978] J. P. Buhler, *Icosahedral Galois representations*, Lecture Notes in Math. **654**, Springer, Berlin, 1978.

[Butler et McKay 1983] G. Butler et J. McKay, "The transitive groups of degree up to eleven", *Comm. Algebra* **11** (1983), 863–911.

[Cassou-Noguès et Jehanne 1996] P. Cassou-Noguès et A. Jehanne, "Parité du nombre de classes des S_4-extensions de $\mathbb{Q}$ et courbes elliptiques", *J. Number Theory* **57** (1996), 366–384.

[Crespo 1990] T. Crespo, "Explicit construction of $2S_n$ Galois extensions", *J. Algebra* **129** (1990), 312–319.

[Deligne et Serre 1974] P. Deligne et J.-P. Serre, "Formes modulaires de poids 1", *Ann. Sci. École Norm. Sup.* (4) **7** (1974), 507–530.

[Dornhoff 1971] L. Dornhoff, *Group representation theory*, Dekker, New York, 1971.

[Hecke 1981] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Math. **77**, Springer, New York, 1981.

[Jehanne 1995] A. Jehanne, "Sur les extensions de $\mathbb{Q}$ à groupe de Galois S_4 et $\widetilde{S}_4$", *Acta Arith.* **69** (1995), 259–276.

[Kiming 1994] 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 $\mathbb{Q}$”, pp. 1–36 dans *On Artin's conjecture for odd 2-dimensional representations*, édité par G. Frey, Lecture Notes in Math. **1585**, Springer, Berlin, 1994.

[Schur 1911] I. Schur, “Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen”, *J. reine angew. Math.* **139** (1911), 155–250.

[Serre 1977] J.-P. Serre, “Modular forms of weight one and Galois representations”, pp. 193–268 dans *Algebraic number fields*, édité par A. Fröhlich, Academic Press, London, 1977.

[Serre 1980] J.-P. Serre, *Corps locaux* (3ème éd.)., Hermann, Paris, 1980.

[Serre 1984] J.-P. Serre, “L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$”, *Comment. Math. Helv.* **59** (1984), 651–676.

Philippe Cassou-Noguès, Laboratoire de Mathématiques Pures de Bordeaux, Université Bordeaux I, cours de la Libération, 33405 Talence cedex, France (phcassou@math.u-bordeaux.fr)

Arnaud Jehanne, Laboratoire d'Algorithmique Arithmétique, Université Bordeaux I, cours de la Libération, 33405 Talence cedex, France (jehanne@math.u-bordeaux.fr)

Received January 2, 1996 ; accepted in revised form September 14