COMPTES RENDUS

MATHEMATIQUE

Number Theory

A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only

Lassina Dembélé

Institut für Experimentelle Mathematik, Ellernstrasse 29, 45141 Essen, Germany

À la mémoire de ma sœur jumelle Fatouma. Déjà vingt ans que tu es partie

Abstract

In this Note, we show the existence of a non-solvable Galois extension of $\mathbb{Q}$ which is unramified outside 2. The extension K we construct has degree $2\,251\,731\,094\,732\,800 = 2^{19}(3 \cdot 5 \cdot 17 \cdot 257)^2$, it has root discriminant $\delta_K < 2^{\frac{47}{8}} = 58.68\ldots$, and is totally complex. ***To cite this article: L. Dembélé, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Résumé

Une extension galoisienne non résoluble de $\mathbb{Q}$ ramifiée seulement en 2. Dans cette Note, nous démontrons l'existence d'une extension galoisienne non résoluble de $\mathbb{Q}$ ramifiée seulement en 2. L'extension K que nous construisons est de degré $2\,251\,731\,094\,732\,800 = 2^{19}(3 \cdot 5 \cdot 17 \cdot 257)^2$ et de discriminant normalisé $\delta_K < 2^{\frac{47}{8}} = 58,68\ldots$, et est totalement complexe. ***Pour citer cet article : L. Dembélé, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Version française abrégée

La conjecture suivante est proposée dans Gross [6] :

Conjecture 1. *Pour tout nombre premier p, il existe une extension galoisienne non résoluble de $\mathbb{Q}$ ramifiée seulement en p.*

Ce résultat est connu lorsque $p \geqslant 11$. En effet, Serre [17] montre que pour un tel nombre premier p, on trouve $k = 12, 16, 18, 20, 22$ ou 26 tel que la représentation galoisienne résiduelle $\bar{\rho}_{k,p}$ mod p attachée à l'unique forme parabolique de niveau 1 et de poids k, à coefficients entiers, est absolument irréductible. Par [19, Chap. IV], le corps fixe de $\ker \bar{\rho}_{k,p}$ est donc une extension non résoluble de $\mathbb{Q}$ qui est non ramifiée en dehors de p.

Dans cette Note, nous établissons cette conjecture pour $p = 2$. L'extension est construite à partir de représentations galoisiennes attachées aux formes modulaires de Hilbert de niveau 1, de poids parallèle 2 et à coefficients dans $\bar{\mathbb{F}}_2$, sur le sous-corps totalement réel maximal F du corps cyclotomique $\mathbb{Q}(\zeta_{32})$. Nous démontrons le théorème suivant :

E-mail address: lassina.dembele@uni-due.de.

Théorème 2. *Il existe deux* $\mathbf{SL}_2(\mathbb{F}_{2^8})$*-extensions E et E' de F ramifiées en l'unique idéal premier divisant 2. Les extensions E et E' sont galoisiennes sur $\mathbb{Q}(\sqrt{2})$, avec groupe de Galois* $\mathbf{SL}_2(\mathbb{F}_{2^8}) \cdot 4$*, et sont interchangées par* $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

On en déduit :

Corollaire 3. *Il existe une extension galoisienne non résoluble K de $\mathbb{Q}$ qui est ramifiée seulement en 2, de groupe de Galois* $\mathbf{SL}_2(\mathbb{F}_{2^8})^2 \cdot 8$.

Une étude locale des représentations galoisiennes à partir desquelles l'extension K à été construite nous permet de borner son discriminant. On obtient ainsi le résultat suivant. (Le « discriminant normalisé » d'une extension finie E de $\mathbb{Q}$ est $|d_E|^{1/[E:\mathbb{Q}]}$, où d_E est le discriminant de E.)

Proposition 4. *Le discriminant normalisé δ_K de l'extension K est* $< 2^{\frac{47}{8}} = 58{,}68\ldots$.

La Proposition 4 implique que l'extension K ne peut être totalement réelle ; sinon, on aurait $\delta_K > 60{,}83\ldots$, la borne inférieure d'Odlyzko pour un corps totalement réel de ce degré, que nous avons évaluée par les formules de Poitou [5]. Elle est donc totalement complexe, étant donné qu'elle est galoisienne.

Remarque 5. *En fait, la borne de la Proposition 4 peut être abaissée à $\delta_K \leqslant 55{,}39\ldots$. À ce sujet, nous référons au complément de Jean-Pierre Serre qui suit.*

1. Introduction

In this Note, we prove that there exists a non-solvable finite Galois extension of $\mathbb{Q}$ which is ramified at 2 only. We construct this extension by using the Galois representations attached to Hilbert modular forms over the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{32})$. This settles the following conjecture, proposed in Gross [6], for the prime $p = 2$:

Conjecture 1. *For any prime number p, there is a finite non-solvable Galois extension K of $\mathbb{Q}$ ramified at p only.*

For primes $p \geqslant 11$, one knows how to construct extensions satisfying Conjecture 1. Indeed, Serre [17] shows that for such a prime p, there is $k = 12, 16, 18, 20, 22$ or 26 such that the residual Galois representation $\bar{\rho}_{k,p}$ mod p associated to the unique cuspidal form of level 1 and weight k, with integral coefficients, is absolutely irreducible. By [19, Chap. IV], the fixed field of $\ker \bar{\rho}_{k,p}$ is then a non-solvable extension of $\mathbb{Q}$ unramified away from p.

As for primes $\leqslant 7$, the first case of the Serre conjecture [15] was proved and later published by Tate [20], for $p = 2$, by simply ruling out the existence of mod 2 irreducible representations of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, unramified away from 2. His results were later extended to the primes 3 and 5 by [18] and [2] respectively, assuming GRH in the latter case. By Khare and Wintenberger [11], this is now true unconditionally for $p = 5, 7$.

However, the general belief is that one can still solve Conjecture 1 by working with automorphic forms over algebraic groups of higher rank; for instance, exceptional groups. Unfortunately, it is not yet clear how to attach Galois representations to such automorphic forms in general. Underscoring this, Gross [7] developed the theory of algebraic modular forms and conjectured the existence of Galois representations attached to irreducible Hecke constituents. Computational results for the exceptional group G_2 over $\mathbb{Q}$ based on his conjectures, led Lansky and Pollack [12] to predict the existence of a $G_2(\mathbb{F}_5)$-extension of $\mathbb{Q}$ that is ramified at 5 only, thus providing further evidence for Conjecture 1.

Our approach, which was suggested to us by Gross, relies on fixing the underlying group and enlarging the base field instead; as for us, it was much easier to study groups of higher rank that are not absolutely simple. The extension K we construct has degree $2^{19}(3 \cdot 5 \cdot 17 \cdot 257)^2 \sim 2 \times 10^{15}$ and has root discriminant $\delta_K < 2^{\frac{47}{8}} = 58.68\ldots$. Thus it is totally complex, being Galois over $\mathbb{Q}$. To the best of our knowledge, this is the largest known totally complex field with such a low root discriminant. It would be interesting to know whether this is an isolated case or if there are infinite towers of totally complex fields with their minimal root discriminant in this magnitude. Indeed, the current

upper bound for such towers is 82.2, which was obtained by Hajir and Maire [8,9]. With the Hilbert Modular Forms Package being currently implemented in Magma [1], we hope to settle the remaining cases of Conjecture 1 in the near future.

2. A non-solvable extension of $\mathbb{Q}$ ramified at 2 only

Let F be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{32})$, and $\mathcal{O}_F$ its ring of integers. It is generated by the element $\beta := \zeta_{32} + \zeta_{32}^{-1}$ with minimal polynomial $x^8 - 8x^6 + 20x^4 - 16x^2 + 2$. We fix the integral basis $1, \beta, \ldots, \beta^7$ of F, and we let σ be the cyclic generator of $\mathrm{Gal}(F/\mathbb{Q})$ given by $(\beta \mapsto -\beta^3 + 3\beta)$. We let α be a cyclic generator of $\mathbb{F}_{2^8}^{\times}$, the unit group in $\mathbb{F}_{2^8}$.

Theorem 2. *There exist two* $\mathbf{SL}_2(\mathbb{F}_{2^8})$*-extensions* E *and* E' *of* F *ramified at the unique prime ideal above* 2 *only. The extensions* E *and* E' *are both Galois over* $\mathbb{Q}(\sqrt{2})$*, with Galois group* $\mathbf{SL}_2(\mathbb{F}_{2^8}) \cdot 4$*, and are interchanged by* $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$*.*

Proof. Let $S_2(1, \mathbb{F}_2)$ be the space of mod 2 Hilbert cusp forms of level 1 and parallel weight 2 over F. Let $\mathbb{T}$ be the Hecke algebra over $\mathbb{F}_2$ generated by the operator $T(\mathfrak{p})$, where $\mathfrak{p}$ runs over all the primes in F. We computed the space $S_2(1, \mathbb{F}_2)$ and the action of $\mathbb{T}$ on it using the Hilbert Modular Forms Package in Magma [1]. It has two non-zero irreducible Hecke constituents which are both 8-dimensional over $\mathbb{F}_2$. The action of $\mathbb{T}$ is completely determined by the operators $T(\mathfrak{p}_{31}^i)$ at the primes above 31, which splits completely in F into 8 distinct primes $\mathfrak{p}_{31}^i$, $i = 1, \ldots, 8$ (see Table 1 for notations). The common characteristic polynomial of those operators together with the one of $T(\mathfrak{p}_2)$, where $\mathfrak{p}_2$ is the unique prime above 2, are given by

$$\mathrm{charpoly}\big(T(\mathfrak{p}_2)\big) = x^{41}\big(x^2 + x + 1\big)^8 \mod 2,$$
$$\mathrm{charpoly}\big(T(\mathfrak{p}_{31}^1)\big) = x^{41}\big(x^8 + x^4 + x^3 + x + 1\big)\big(x^8 + x^6 + x^5 + x^2 + 1\big) \mod 2.$$

Let f and f' be the newforms whose first few Hecke eigenvalues are listed in Table 1. Their $\mathrm{Gal}(\mathbb{F}_{2^8}/\mathbb{F}_2)$-conjugacy classes determine the two non-zero constituents of $S_2(1, \mathbb{F}_2)$. We recall that to give a newform $f \in S_2(1, \overline{\mathbb{F}}_2)$ is equivalent to giving a maximal ideal $\mathfrak{m}_f \subset \mathbb{T}$; and that the association $(f \mapsto \mathfrak{m}_f)$ is a bijection between $\mathrm{Gal}(\overline{\mathbb{F}}_2/\mathbb{F}_2)$-conjugacy classes of newforms and maximal ideals in $\mathbb{T}$.

Let $\mathfrak{m}_f, \mathfrak{m}_{f'} \subset \mathbb{T}$ be the maximal ideals associated to f and f' respectively, and let $\theta_f : \mathbb{T} \to \mathbb{T}/\mathfrak{m}_f = \mathbb{F}_{2^8}$ and $\theta_{f'} : \mathbb{T} \to \mathbb{T}/\mathfrak{m}_{f'} = \mathbb{F}_{2^8}$ be the corresponding ring homomorphisms. By work of Rogawski–Tunnell, Ohta and Carayol [14,13,4], completed by Taylor and Jarvis [21,10,22], there are Galois representations

$$\bar{\rho}_f, \bar{\rho}_{f'} : \mathrm{Gal}(\overline{F}/F) \to \mathbf{SL}_2(\mathbb{F}_{2^8})$$

such that $\mathrm{Tr}(\bar{\rho}_f(\mathrm{Frob}_{\mathfrak{p}})) = \theta_f(T(\mathfrak{p}))$ and $\mathrm{Tr}(\bar{\rho}_{f'}(\mathrm{Frob}_{\mathfrak{p}})) = \theta_{f'}(T(\mathfrak{p}))$, for all prime $\mathfrak{p}$. From the orders of Frobenii provided in Table 1, we see that $\bar{\rho}_f$ and $\bar{\rho}_{f'}$ are surjective. This proves the first part of Theorem 2 with the two extensions E and E' being the fixed fields of $\ker(\bar{\rho}_f)$ and $\ker(\bar{\rho}_{f'})$, respectively. (We recall that the extensions E and E' only depend on the $\mathrm{Gal}(\mathbb{F}_{2^8}/\mathbb{F}_2)$-conjugacy classes of f and f', or equivalently $\mathfrak{m}_f$ and $\mathfrak{m}_{f'}$, respectively.)

Let τ be the cyclic generator of $\mathrm{Gal}(\mathbb{F}_{2^8}/\mathbb{F}_2)$ given by $(\tau : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}, \alpha \mapsto \alpha^2)$. It is not hard to see that, for the primes listed in Table 1,

$$a_{\sigma^2(\mathfrak{p})}(f) = \tau^2\big(a_{\mathfrak{p}}(f)\big) \quad \text{and} \quad a_{\sigma^2(\mathfrak{p})}(f') = \tau^2\big(a_{\mathfrak{p}}(f')\big).$$

Also, since those primes determine f and f', these identities extend to all primes $\mathfrak{p}$. This means that the action of $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{2})) = \langle\sigma^2\rangle$ preserves the $\mathrm{Gal}(\mathbb{F}_{2^8}/\mathbb{F}_2)$-conjugacy classes of f and f'. Or equivalently, that $\sigma^2(\mathfrak{m}_f) = \mathfrak{m}_{\tau^2(f)} = \mathfrak{m}_f$ and $\sigma^2(\mathfrak{m}_{f'}) = \mathfrak{m}_{f'}$. From this, we conclude that E and E' are Galois over $\mathbb{Q}(\sqrt{2})$ with the same Galois group $\mathbf{SL}_2(\mathbb{F}_{2^8}) \cdot 4$. This proves the second part of Theorem 2.

Finally, we observe that $a_{\sigma(\mathfrak{p})}(f) = a_{\mathfrak{p}}(f')$, for any prime $\mathfrak{p}$, which implies that $\sigma(\mathfrak{m}_f) = \mathfrak{m}_{f'}$. Therefore, the action of $\mathrm{Gal}(F/\mathbb{Q})$ permutes the $\mathrm{Gal}(\mathbb{F}_{2^8}/\mathbb{F}_2)$-conjugacy classes of f and f'. Combining this with the observation above, we see that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ interchanges E and E', which concludes the proof of Theorem 2. $\quad\square$

Table 1
Mod 2 Hilbert newforms of weight 2 and level 1 over $F = \mathbb{Q}(\zeta_{32})^+$.

$\mathfrak{p}$	$\mathfrak{p}_{31}^1$	$\mathfrak{p}_{31}^2$	$\mathfrak{p}_{31}^3$	$\mathfrak{p}_{31}^4$	$\mathfrak{p}_{31}^5$	$\mathfrak{p}_{31}^6$	$\mathfrak{p}_{31}^7$	$\mathfrak{p}_{31}^8$
$a_{\mathfrak{p}}(f)$	α^{100}	α^{19}	α^{145}	α^{76}	α^{70}	α^{49}	α^{25}	α^{196}
$\mathrm{ord}(\bar{\rho}_f(\mathrm{Frob}_{\mathfrak{p}}))$	257	255	257	255	257	255	257	255
$a_{\mathfrak{p}}(f')$	α^{196}	α^{100}	α^{19}	α^{145}	α^{76}	α^{70}	α^{49}	α^{25}
$\mathrm{ord}(\bar{\rho}_{f'}(\mathrm{Frob}_{\mathfrak{p}}))$	255	257	255	257	255	257	255	257
$\mathfrak{p}$	$\mathfrak{p}_{97}^1$	$\mathfrak{p}_{97}^2$	$\mathfrak{p}_{97}^3$	$\mathfrak{p}_{97}^4$	$\mathfrak{p}_{97}^5$	$\mathfrak{p}_{97}^6$	$\mathfrak{p}_{97}^7$	$\mathfrak{p}_{97}^8$
$a_{\mathfrak{p}}(f)$	α^{23}	α	α^{92}	α^4	α^{113}	α^{16}	α^{197}	α^{64}
$\mathrm{ord}(\bar{\rho}_f(\mathrm{Frob}_{\mathfrak{p}}))$	257	51	257	51	257	51	257	51
$a_{\mathfrak{p}}(f')$	α^{64}	α^{23}	α	α^{92}	α^4	α^{113}	α^{16}	α^{197}
$\mathrm{ord}(\bar{\rho}_{f'}(\mathrm{Frob}_{\mathfrak{p}}))$	51	257	51	257	51	257	51	257

$$\mathfrak{p}_{31} := \big([1, 2, 0, -4, 0, 1, 0, 0]\big),$$

$$\mathfrak{p}_{31}^i := \sigma^{i-1}(\mathfrak{p}_{31}), \quad i = 1, \ldots, 8.$$

$$\mathfrak{p}_{97} := \big([1, -12, -4, 19, 1, -8, 0, 1]\big),$$

$$\mathfrak{p}_{97}^i := \sigma^{i-1}(\mathfrak{p}_{97}), \quad i = 1, \ldots, 8.$$

Corollary 3. *There exists a finite non-solvable Galois extension K of $\mathbb{Q}$ that is ramified at 2 only, with Galois group* $\mathbf{SL}_2(\mathbb{F}_{2^8})^2 \cdot 8$.

Proof. Let K be the Galois closure of E over $\mathbb{Q}$. By Theorem 2, K is the compositum of E and E', and only ramifies at 2 by construction. So it only remains to find its Galois group.

By Galois theory and the fact that $E \cap E'$ is Galois over F, we have

$$\mathrm{Gal}(K/E) = \mathrm{Gal}(EE'/E) \cong \mathrm{Gal}(E/E \cap E') = \mathrm{Gal}(E'/E \cap E')$$

$$\lhd \mathrm{Gal}(E/F) = \mathbf{SL}_2(\mathbb{F}_{2^8}).$$

Since E is not Galois over $\mathbb{Q}$ and the only normal subgroups of $\mathbf{SL}_2(\mathbb{F}_{2^8})$ are 1 and itself, we must have $E \cap E' = F$ and $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/E') = \mathbf{SL}_2(\mathbb{F}_{2^8})$. Thus, the fields E and E' are disjoint over F and $\mathrm{Gal}(K/F) = \mathbf{SL}_2(\mathbb{F}_{2^8})^2$, which implies that

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K/F)^2 \cdot 8 = \mathbf{SL}_2(\mathbb{F}_{2^8})^2 \cdot 8. \qquad \square$$

3. An estimate for the root discriminant

In this section, we use the modularity of the Galois representations from which our extension K of Section 2 was constructed in order to obtain an estimate for its root discriminant.

Proposition 4. *The root discriminant δ_K of the extension K is* $< 2^{\frac{47}{8}} = 58.68\ldots$.

Proof. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the primes in $\mathcal{O}_K$ above $\mathfrak{p}_2$ so that

$$\mathfrak{p}_2 = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}.$$

Since K is Galois over F, the group $\mathrm{Gal}(K/F)$ acts transitively on the set of those primes. We let e and s be the common ramification index and residue field degree, respectively, so that $e_i = e$ and $esg = [K : F]$. Let $\mathfrak{P}$ be any of the primes above $\mathfrak{p}_2$, and $\mathfrak{p} = \mathcal{O}_E \cap \mathfrak{P}$ and $\mathfrak{p}' = \mathcal{O}_{E'} \cap \mathfrak{P}$. Let $E_{\mathfrak{p}}$, $E'_{\mathfrak{p}'}$ and $K_{\mathfrak{P}}$ be the completions of E, E' and K at $\mathfrak{p}$, $\mathfrak{p}'$ and $\mathfrak{P}$, respectively. Then $K_{\mathfrak{P}}$ is the compositum of $E_{\mathfrak{p}}$ and $E'_{\mathfrak{p}'}$. The eigenvalue of f at $\mathfrak{p}_2$ is $a_{\mathfrak{p}_2}(f) = \alpha^{170} \in \mathbb{F}_4^{\times}$,

thus f is ordinary at $\mathfrak{p}_2$. By Wiles [23, Theorem 2] it follows that the restriction of $\bar\rho_f$ to the decomposition group at $\mathfrak{p}_2$ is of the form

$$\bar\rho_f|D_{\mathfrak{p}_2} \sim \begin{pmatrix} \chi & * \\ 0 & \chi^{-1} \end{pmatrix},$$

where χ is an unramified character of order 3. It also follows that

$$\bar\rho_f|I_{\mathfrak{p}_2} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

From this and the fact that the extensions $E_{\mathfrak{p}}$ and $E'_{\mathfrak{p}'}$ are *peu ramifiées* in the sense of Serre [15, Section 2] (see also [3] for a group scheme theoretic definition), it follows that $K_{\mathfrak{P}} = L(\sqrt{x_1}, \ldots, \sqrt{x_{2m}})$, where $e = 2^{2m}$, L is the unique unramified extension of degree 3 of $F_{\mathfrak{p}_2}$ contained in $K_{\mathfrak{P}}$ and $x_i \in \mathcal{O}_L^{\times}/(\mathcal{O}_L^{\times})^2$. And so, the Galois group $\mathrm{Gal}(K_{\mathfrak{P}}/L)$ has $2^{2m} - 1$ quadratic characters, whose conductors divide $\mathfrak{p}_L^{16}$. Therefore, by the discriminant-conductor formula [16, Chap. VI], we get that the local discriminant $d_{K_{\mathfrak{P}}/L}$ divides $\mathfrak{p}_L^{16(2^{2m}-1)}$. Equivalently, this means that $d_{K_{\mathfrak{P}}/F_{\mathfrak{p}_2}}$ divides $\hat{\mathfrak{p}}_2^{16(2^{2m}-1)}$, where $\hat{\mathfrak{p}}_2$ is the maximal ideal in $F_{\mathfrak{p}_2}$. Taking the product over all primes then yields that the global discriminant $d_{K/F}$ divides $\mathfrak{p}_2^{16gs(2^{2m}-1)} = \mathfrak{p}_2^{2[K:\mathbb{Q}](1-1/2^{2m})}$. From the relation

$$d_K = d_F^{[K:F]} \mathrm{N}_{F/\mathbb{Q}}(d_{K/F}),$$

it then follows that d_K divides $2^{31[K:F]} \times 2^{2[K:\mathbb{Q}](1-1/2^{2m})}$, and hence

$$\delta_K \leqslant \delta_F 2^{2(1-1/2^{2m})} = 2^{31/8} 2^{2(1-1/2^{2m})} = 2^{47/8 - 1/2^{2m-1}} < 2^{47/8}. \qquad \square$$

From Proposition 4, we see that K cannot be totally real; otherwise, we would have $\delta_K > 60.83$, the Odlyzko bound for a totally real field of this degree, estimated using Poitou's formulas in [5]. Therefore it must be totally complex, being Galois over $\mathbb{Q}$.

Remark 5. The bound in Proposition 4 can be lowered to $\delta_K \leqslant 55.39 \ldots$. To this end, we refer to the supplement written by Jean-Pierre Serre.

Acknowledgements

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[2] S. Brueggeman, The nonexistence of certain Galois extensions unramified outside 5, J. Number Theory 75 (1999) 47–52.
[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, J. Amer. Math. Soc. 14 (4) (2001) 843–939.
[4] H. Carayol, Sur les représentations l-adiques associées aux formes modulaires de Hilbert, Ann. Sci. Ecole Norm. Sup. 19 (1986) 409–468.
[5] F. Diaz y Diaz, Tables minorant la racine n-ième du discriminant d'un corps de degré n, Publications Mathématiques d'Orsay 80, Université de Paris-Sud, Département de Mathématique, Orsay, 1980, 59 pp.
[6] B. Gross, Modular forms (mod p) and Galois representations, Int. Math. Res. Notices 16 (1998) 865–875.
[7] B. Gross, Algebraic modular forms, Israel J. Math. 113 (1999) 61–93.
[8] F. Hajir, C. Maire, Tamely ramified towers and discriminant bounds for number fields. II, J. Symbolic Comput. 33 (4) (2002) 415–423.
[9] F. Hajir, C. Maire, Tamely ramified towers and discriminant bounds for number fields, Compositio Math. 128 (1) (2001) 35–53.
[10] F. Jarvis, On Galois representations associated to Hilbert modular forms of low weight, J. Reine Angew. Math. 491 (1997) 199–216.

[11] C. Khare, J.-P. Wintenberger, On Serre's conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals, Ann. of Math., in press.

[12] J. Lansky, D. Pollack, Hecke algebras and automorphic forms, Compositio Math. 130 (1) (2002) 21–48.

[13] M. Ohta, Hilbert modular forms of weight one and Galois representations, Progr. Math. 46 (1984) 333–353.

[14] J. Rogawski, J. Tunnell, On Artin L-functions associated to Hilbert modular forms of weight 1, Invent. Math. 74 (1983) 1–42.

[15] J.-P. Serre, Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), Duke Math. J. 54 (1) (1987) 179–230.

[16] J.-P. Serre, Corps locaux, Deuxième édition, in : Publications de l'Université de Nancago, vol. VIII, Hermann, Paris, 1968, p. 245.

[17] J.-P. Serre, Congruences et formes modulaires [d'après H.P.F. Swinnerton-Dyer], Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, in: Lecture Notes in Math., vol. 317, Springer, Berlin, 1973, pp. 319–338.

[18] J.-P. Serre, Oeuvres III, Springer-Verlag, 1986, Note 229.2 on p. 710.

[19] J.-P. Serre, Abelian *l*-Adic Representations and Elliptic Curves, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1997.

[20] J. Tate, The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2, Contemp. Math. 174 (1994) 153–156.

[21] R. Taylor, On Galois representations associated to Hilbert modular forms, Invent. Math. 98 (2) (1989) 265–280.

[22] R. Taylor, On the meromorphic continuation of degree two *L*-functions, Doc. Math. Extra Vol. (2006) 729–779.

[23] A. Wiles, On ordinary λ-adic representations associated to modular forms, Invent. Math. 94 (3) (1988) 529–573.