COMPOSITIO MATHEMATICA

A non-solvable extension of $\mathbb{Q}$ unramified outside 7

Luis V. Dieulefait

Compositio Math. **148** (2012), 669–674.

doi:10.1112/S0010437X11007408

https://doi.org/10.1112/S0010437X11007408 Published online by Cambridge University Press

Compositio Math. 148 (2012) 669–674
doi:10.1112/S0010437X11007408

A non-solvable extension of $\mathbb{Q}$ unramified outside 7

Luis V. Dieulefait

Abstract

We consider a mod 7 Galois representation attached to a genus 2 Siegel cusp form of level 1 and weight 28 and using some of its Fourier coefficients and eigenvalues computed by N. Skoruppa and the classification of maximal subgroups of $\mathrm{PGSp}(4, p)$ we show that its image is as large as possible. This gives a realization of $\mathrm{PGSp}(4, 7)$ as a Galois group over $\mathbb{Q}$ and the corresponding number field provides a non-solvable extension of $\mathbb{Q}$ which ramifies only at 7.

1. Introduction

This brief note is concerned with Gross' conjecture about the existence of a non-solvable Galois extension of $\mathbb{Q}$ unramified outside p for any prime p. For primes $p > 7$ such an extension of $\mathbb{Q}$ was constructed by Serre using level 1 classical cuspidal modular forms (cf. [Ser73]) and, because of Serre's conjecture (in its strong form), it is easy to see that this approach cannot solve the cases of small primes. Dembélé, Greenberg, and Voight have solved the problem for $p = 2, 3, 5$ (cf. [Dem09, DGV11]) using Galois representations attached to certain Hilbert modular forms: see [DGV11] for details.

We will give a solution of this problem for the remaining case $p = 7$. The extension will be obtained from a mod 7 representation attached to a level 1 genus 2 Siegel cusp form. The study of the images of these Galois representations was already developed in the author's thesis (see [Die01, ch. 6], and its published version [Die02], which contains fewer computations), where it was shown that the residual images were 'as large as possible' for almost every prime, provided that the form was not a Maass spezialform and under a certain irreducibility condition on one characteristic polynomial. In particular, for a Galois conjugacy class of cusp forms of level 1 and weight 28 it was shown that the image was generically large.

We will consider one of the mod 7 residual representations obtained from such a Siegel cusp form and we will prove that its projective image is $\mathrm{PGSp}(4, 7)$. In this way, we are realizing this non-solvable group as a Galois group over $\mathbb{Q}$ in such a way that the corresponding number field ramifies only at 7.

2. Determination of the image of the mod 7 representation

Let us recall the setup from [Die01] (or [Die02]): we start from a genus 2 Siegel cusp form f of level 1 and weight 28, which is not a Maass spezialform (it is known to have multiplicity one).

Received 2 September 2010, accepted in final form 22 July 2011, published online 24 January 2012.
2010 Mathematics Subject Classification 11F80, 11F46 (primary).
Keywords: Galois theory, Galois representations, Siegel modular forms.

There is a unique conjugacy class, and the field E generated by the eigenvalues of f is the cubic field generated by some root of $P(x) = x^3 - x^2 - 294086x - 59412960$.

Taylor and Weissauer proved the existence of a compatible family of λ-adic symplectic four-dimensional Galois representations $\{\rho_\lambda\}$ attached to f (see [Tay93] and [Wei05, pp. 68 and 76]). This compatible system has conductor 1, that is, each representation ρ_λ ramifies only at ℓ, where ℓ denotes the rational prime such that $\lambda | \ell$. The characteristic polynomial of $\rho_\lambda(\mathrm{Frob}\, p)$ when $\lambda \nmid p$ is

$$\mathrm{Pol}_p(x) = x^4 - a_p x^3 + (a_p^2 - a_{p^2} - p^{2k-4})x^2 - a_p p^{2k-3} x + p^{4k-6},$$

where a_i denotes the ith Hecke eigenvalue of f, for any i, and k denotes the weight of f.

A priori, the representations ρ_λ are not known to be defined over E_λ, even if all characteristic polynomials have coefficients in E. Nevertheless, it was shown in [DKR01] that for the purpose of determining the corresponding residual representation one can proceed as if they were, that is, just formally reduce mod λ by reducing the coefficients of the characteristic polynomials and the resulting residual representation exists and is known to be a quotient of ρ_λ. By construction, this residual representation has coefficients in the residue field $\mathbb{F}_\lambda$ corresponding to the prime λ.

We consider a prime t dividing 7 in E and the corresponding residual representation $\bar{\rho}_t$: for simplicity, let us call this residual representation $\bar{\rho}$. The first Fourier coefficients of f are available at [Sko], and have been quoted and used at [DKR01, Die01]. Moreover, using these coefficients one can compute the first Hecke eigenvalues: $a_2, a_4, a_3, a_9, a_5, a_{25}$ (cf. [DKR01, Die01]). Because we are only interested in a mod 7 representation, let us just give the values of these eigenvalues in the residual representation. Let α be a root of $P(x)$. All Fourier coefficients and eigenvalues are computed in terms of α. If we reduce $P(x)$ mod 7, we obtain

$$P(x) \equiv (x+3)(x+4)(x+6) \pmod 7.$$

Thus, 7 is split in E and we fix a prime t above 7; equivalently, we fix one of the three residual representations with values on $\mathbb{F}_7$. We choose t to be the prime dividing 7 such that α is congruent to 1 modulo t in order to compute, in $\mathbb{F}_7$, the residual values of the eigenvalues and the characteristic polynomials of $\bar{\rho}$. In this way, we obtain

$$a_2 = 4, a_4 = 5, a_3 = 3, a_9 = 2, a_5 = 1, a_{25} = 2.$$

The following are the characteristic polynomials $\mathrm{Pol}_p(x)$ of $\bar{\rho}(\mathrm{Frob}\, p)$ for $p = 2, 3, 5$, factorized over $\mathbb{F}_7$:

$$\begin{aligned}\mathrm{Pol}_2(x) &= x^4 + 3x^3 + 2x^2 + 5x + 2,\\ \mathrm{Pol}_3(x) &= (x+3)(x+4)(x^2+4x+5),\\ \mathrm{Pol}_5(x) &= (x^2+x+3)(x^2+5x+3).\end{aligned}$$

Thus, $\bar{\rho}$ has image in $\mathrm{GSp}(4,7)$ containing three matrices with the above characteristic polynomials, and it cuts an extension of $\mathbb{Q}$ ramifying only at 7. Using some group theory, Galois theory, and number theory, our main result is the determination of the image of this residual representation.

Theorem 2.1. *Let f be the genus 2 Siegel cusp form of level 1 and weight 28 which is not a Maass spezialform (unique up to Galois conjugation). Consider the compatible family of symplectic four-dimensional Galois representations attached to f. Let $\bar{\rho}$ be the residual representation in characteristic 7 just described. Then the projective image of $\bar{\rho}$ is* $\mathrm{PGSp}(4,7)$. *In particular, this non-solvable group corresponds to an extension of $\mathbb{Q}$ ramifying only at 7.*

https://doi.org/10.1112/S0010437X11007408 Published online by Cambridge University Press

Proof. To show that the image is indeed large, we consider the classification of maximal subgroups of $\mathrm{PGSp}(4,q)$ given by Mitchell in geometric language and by Kleidman in group theoretic language (cf. [Mit14, pp. 395–396] and [Kle86, Tables, pp. 191–220]; see also [KL90, Kin05]). For the case of a prime field with $p=7$, this classification reads as follows.

A subgroup of $\mathrm{PGSp}(4,7)$ either contains $\mathrm{PSp}(4,7)$ or is contained in one of the following (see [KL90, p. 3 and ch. 4] for the notation of classes $\mathcal{C}_i$ and the definition of type $\mathcal{S}$):

(1) a maximal parabolic subgroup (class $\mathcal{C}_1$);

(2) a stabilizer of a decomposition of the underlying vector space in two two-dimensional subspaces (class $\mathcal{C}_2$);

(3) a stabilizer of the extension field $\mathbb{F}_{7^2}$ (class $\mathcal{C}_3$);

(4) a group isomorphic to $\mathrm{PGL}(2,7)$ (of type $\mathcal{S}$);

(5) a group isomorphic to $2^4\cdot O_4^-(2)\cdot 2$ (class $\mathcal{C}_6$);

(6) a group isomorphic to $A_7\cdot 2$ (of type $\mathcal{S}$).

Comments/explanations: the image is contained in a group as in (1) if and only if the representation is reducible. If the image is irreducible and is contained in a subgroup as in (2), there is a quadratic number field K such that the restriction to K of $\bar{\rho}$ is reducible, and for primes p that are inert in K the trace of $\bar{\rho}$ at p must be 0 (see [Die01]). Case (3) is similar to the previous two cases, but after extending scalars to $\mathbb{F}_{p^2}$: over this extension a subgroup contained in a maximal subgroup in case (3) is again either reducible or contains a reducible normal subgroup of index 2.

In case (5) the subgroup of order 16 is an elementary abelian 2-group, and the corresponding maximal subgroup of $\mathrm{Sp}(4,7)$ is known to be the normalizer of an extra-special group of order 32 (cf. [Kle86, KL88]).

Therefore, if we call a group as in (2) and (3) imprimitive, our goal is to show that the image of $\bar{\rho}$ is:

(a) absolutely irreducible;

(b) not imprimitive; and

(c) its projectivization is not contained in any of the groups listed in cases (4), (5), and (6).

(a) Assuming that $\bar{\rho}$ is reducible over $\bar{\mathbb{F}}_7$, we semisimplify it. In order to ease the notation, we will call $\bar{\rho}$ the semisimple representation thus obtained. Being reducible and semisimple, $\bar{\rho}$ has either a one-dimensional or a two-dimensional irreducible component, which we will call μ. If μ is one dimensional, it corresponds to a character with values in a finite field of characteristic 7, but, since the representation is unramified outside 7, the character μ must be equal to some power of the mod 7 cyclotomic character χ; thus, it has values in $\mathbb{F}_7$. In particular, all characteristic polynomials must have at least one root in $\mathbb{F}_7$, contradicting the fact that both Pol_2 and Pol_5 do not have any such root. If μ is two dimensional, the representation is the sum of two two-dimensional components μ and ν. We can assume that they are both irreducible because the case of characters has just been taken care of. In this case, the representation cannot be reducible over $\mathbb{F}_7$ as in (1) because the image of $\bar{\rho}$ would be contained in two copies of $\mathrm{GL}(2,7)$, which contradicts the existence of matrices in this image with irreducible characteristic polynomial as Pol_2. On the other hand, if the image is only reducible after extending scalars as in case (3), the representations μ and ν must be conjugate to one another by the generator σ of $\mathrm{Gal}(\mathbb{F}_{49}/\mathbb{F}_7)$. Observe also that μ and ν must have determinants defined over $\mathbb{F}_7$, because these determinants

https://doi.org/10.1112/S0010437X11007408 Published online by Cambridge University Press

are characters of the absolute Galois group of $\mathbb{Q}$ unramified outside 7 and thus powers of χ. This is incompatible with the shape of Pol_3, because by direct computation we see that the only way to factor Pol_3 as a product of two quadratic polynomials such that both have their independent terms in $\mathbb{F}_7$ is by taking these two quadratic factors to be $(x+3)(x+4)$ and (x^2+4x+5); therefore, these polynomials have to be the characteristic polynomials of $\mu(\mathrm{Frob}\, 3)$ and $\nu(\mathrm{Frob}\, 3)$, but this clearly contradicts the fact that μ and ν are σ-conjugates.

(b) If the image of $\bar{\rho}$ were an irreducible imprimitive group, it should contain a normal reducible subgroup H of index 2, and the trace of $\bar{\rho}(\mathrm{Frob}\, p)$ is zero for every prime p that is inert in the quadratic field K that is fixed by H (cf. [Die01, pp. 102–103]). Since $\bar{\rho}$ is unramified outside 7 and K is contained in the field fixed by the kernel of $\bar{\rho}$, the field K must be equal to $\mathbb{Q}(\sqrt{-7})$ and in particular we should have $\mathrm{trace}(\bar{\rho}(\mathrm{Frob}\, 3)) = a_3 = 0$ (because 3 is not a square mod 7), which is not the case.

(c) Using Pol_2, we see that the projective image of $\bar{\rho}$ is not contained in cases (4), (5), or (6), because we easily compute the projective order of a matrix with this characteristic polynomial to be 25. On the other hand, the order of $O_4^-(2)$ is 120.

Having proved that the properties (a), (b), and (c) are enjoyed by the image of $\bar{\rho}$, we conclude from Mitchell's classification that the image of the projectivization of $\bar{\rho}$ contains $\mathrm{PSp}(4,7)$. Since the residue field is prime (thus it has odd degree) and the multiplier being χ^{2k-3}, it is known (cf. [DKR01]) that this implies that the image must be equal to $\mathrm{PGSp}(4,7)$. This concludes the proof of the theorem.

Remark 1. Reducing modulo the prime ideals above 7 that contain $\alpha - 3$ or $\alpha - 4$, one obtains two more residual mod 7 representations. In these cases the determination of the image is not so easy. In both cases, after computing the characteristic polynomials of the images of $\mathrm{Frob}\, p$ for $p = 2$, 3, and 5, we see that these polynomials are not enough to eliminate directly some cases in Mitchell's classification. What seems achievable is to decide in both cases whether the image is solvable or not, even if the exact group cannot be determined. For example, when we take the prime ideal above 7 that contain $\alpha - 4$, computations suggest that the projective image is either $\mathrm{PGSp}(4,7)$ or a group as in case (5) of the classification. In particular, the image is non-solvable. In order to prove such a claim, we should also consider and eliminate all maximal subgroups of a group as in case (5).

3. An upper bound for the root discriminant

We can give an upper bound for the root discriminant of the extension with Galois group $\mathrm{PGSp}(4,7)$ just constructed using the results of Moon in [Moo00]. In order to do so, since an explicit description of the p-Sylow subgroup of $\mathrm{Sp}(4,p)$ is well known (see for example [Sri68]), it is easy to see that this group has order p^4, is non-abelian, and contains a normal p-elementary subgroup of order p^3.

Proposition 2.4 in [Moo00] then shows that the root discriminant of our extension is bounded by 7^c with $c = 2 + 1 + 2/(7-1) = 10/3$. This gives the bound $7^{10/3} \approx 656.13$.

A better bound can be obtained if we use the explicit description of the p-Sylow subgroup of $\mathrm{PGSp}(4,p)$ in a more subtle way. Let us assume first that we are in the case of 'fundamental characters of level 1', that is, that the image of inertia at 7 is contained in the group of upper-triangular matrices and in the diagonal we have powers of χ. From now on, we consider the mod 7 representation $\bar{\rho}$ without projectivizing: it is easy to see that its image is the group $\mathrm{GSp}(4,7)$.

https://doi.org/10.1112/S0010437X11007408 Published online by Cambridge University Press

We know the determinant and multiplier of $\bar{\rho}$: the multiplier is χ^{-1} and the determinant is χ^{-2}. This implies that the image of the tame inertia group at 7 has order 6. Recall that the structure of the 7-Sylow subgroup of $\mathrm{GSp}(4,7)$ is known: it has order 7^4, length 2, and it contains a 7-elementary normal subgroup of order 7^3. Using this information, we can apply [Moo00, Lemma 2.3] to bound the root discriminant (see also the proof of Proposition 2.4 in [Moo00] for the explanation of why the bound c in Lemma 2.3 is also a bound for the exponent of the p-part of the root discriminant). In the notation of that lemma, we have

$$\begin{gathered} N=2, \quad m_1=1, \quad m_2=3, \\ e_0=6, \quad e_1=6\cdot 7=42, \quad e_2=6\cdot 7^4, \\ \alpha_1=2, \quad \alpha_2=8. \end{gathered}$$

Using this, we easily compute the constant c using the formula in [Moo00, Lemma 2.3]:

$$c=3+\frac{1}{6}+\frac{1}{6}-\left(\frac{1}{7}+\frac{1}{7^3}+\frac{1}{42}+\frac{8}{6\cdot 7^4}\right)\approx 3.1632.$$

Therefore, assuming that we are in the case where tame inertia acts through powers of the cyclotomic character, we obtain the following upper bound for the root discriminant: $7^c \approx 471.21$.

It remains to consider the complementary cases, where at least one fundamental character of order greater than 1 appears in the action of tame inertia. But, in all such cases, using the explicit description of the 7-Sylow subgroup of $\mathrm{GSp}(4,7)$, suitably conjugated in $\mathrm{GL}(4,7)$ so that it is contained in the subgroup of upper-triangular matrices, we easily check that in these complementary cases the image of wild inertia must be contained in the 7-elementary subgroup of order 7^3 of the 7-Sylow subgroup. Thus, the 7-length of the inertia subgroup is 1. The bound c in Lemma 2.3 of [Moo00], as noted by Moon, is smaller than $N+1+(N/(7-1))$, where N denotes the length of the inertia subgroup. So, having $N=1$, we obtain $c<13/6$ and this gives the upper bound for the root discriminant: $7^c=7^{13/6}\approx 67.77$.

In particular, we conclude that, in any case, the root discriminant of the extension determined by $\bar{\rho}$ is smaller than 471.22.

Proposition 3.1. *Let $\bar{\rho}$ be the residual representation considered in the previous section. Let F be the fixed field of the kernel of $\bar{\rho}$, a Galois number field with Galois group* $\mathrm{GSp}(4,7)$ *unramified outside* 7. *Then the root discriminant of $F/\mathbb{Q}$ is smaller than* 471.22.

Acknowledgements

This research was partially supported by grant MTM2009-07024 and by an ICREA Academia prize. I want to thank Lassina Dembélé, Sara Arias de Reyna, John Voight, and Dick Gross for useful explanations, comments, and corrections.

References

Dem09 L. Dembélé, *A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only*, C. R. Math. Acad. Sci. Paris **347** (2009), 111–116.

DGV11 L. Dembélé, M. Greenberg and J. Voight, *Nonsolvable number fields ramified only at 3 and 5*, Compositio Math. **147** (2011), 716–734.

DKR01 M. Dettweiler, U. Kuhn and S. Reiter, *On Galois realizations via Siegel modular forms*, Math. Res. Lett. **8** (2001), 577–588.

https://doi.org/10.1112/S0010437X11007408 Published online by Cambridge University Press

Die01 L. Dieulefait, *Modular Galois realization of linear groups*, PhD thesis, Universitat de Barcelona (2001), available at: wstein.org/people/dieulefait/lvdtesis.ps.

Die02 L. Dieulefait, *On the images of the Galois representations attached to genus 2 Siegel modular forms*, J. Reine Angew. Math. **553** (2002), 183–200.

Kin05 O. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, in *Surveys in Combinatorics, 2005*, ed. B. S. Webb (Cambridge University Press, Cambridge, 2005), 29–56.

Kle86 P. Kleidman, *The subgroup structure of some finite simple groups*, PhD thesis, Cambridge (1986).

KL88 P. Kleidman and M. Liebeck, *A survey of the maximal subgroups of the finite simple groups*, Geom. Dedicata **25** (1988), 375–389.

KL90 P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129 (Cambridge University Press, Cambridge, 1990).

Mit14 H. Mitchell, *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc. **15** (1914), 379–396.

Moo00 H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165.

Ser73 J.-P. Serre, *Congruences et formes modulaires [d'après H.P.F. Swinnerton-Dyer]*, in *Séminaire Bourbaki, Vol. 1971/1972*, Lecture Notes in Mathematics, vol. 317 (Springer, New York, 1973), 319–338 Exp. No. 416.

Sko N. Skoruppa, *Siegel modular forms of genus 2: eigenforms of level 1*, tables available at: http://wotan.algebra.math.uni-siegen.de/∼modi/.

Sri68 B. Srinivasan, *The characters of the finite symplectic group* $\mathrm{Sp}(4, q)$, Trans. Amer. Math. Soc. **131** (1968), 488–525.

Tay93 R. Taylor, *On the ℓ-adic cohomology of Siegel threefolds*, Invent. Math. **114** (1993), 289–310.

Wei05 R. Weissauer, *Four dimensional Galois representations*, in *Formes automorphes (II), Le cas du groupe* GSp(4), Astérisque, Vol. 302 (Société Mathématique de France, 2005), 67–150.

Luis V. Dieulefait ldieulefait@ub.edu
Departament d'Álgebra i Geometria, Universitat de Barcelona,
Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

https://doi.org/10.1112/S0010437X11007408 Published online by Cambridge University Press