London Mathematical Society ISSN 1461–1570

A POLYNOMIAL WITH GALOIS GROUP $\mathrm{SL}_2(\mathbb{F}_{16})$

JOHAN BOSMAN

Abstract

In this paper we display an explicit polynomial having Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$, filling in a gap in the tables of Jürgen Klüners and Gunter Malle. Furthermore, the polynomial has small Galois root discriminant; this fact answers a question of John Jones and David Roberts. The computation of this polynomial uses modular forms and their Galois representations.

1. *Introduction*

It is a computational challenge to construct polynomials with a prescribed Galois group; see [**15**] for methods and examples. Here, by the Galois group of a polynomial $f \in \mathbb{Q}[x]$ we mean the Galois group of a splitting field of f over $\mathbb{Q}$ together with its natural action on the roots of f in this splitting field. Jürgen Klüners informed me about an interesting group for which a polynomial had not been found yet, namely $\mathrm{SL}_2(\mathbb{F}_{16})$ with its natural action on $\mathbb{P}^1(\mathbb{F}_{16})$. This action is faithful because of $\mathrm{char}(\mathbb{F}_{16}) = 2$. It must be noted that the existence of such a polynomial was already known to Mestre (unpublished). In this paper we will give an explicit example.

PROPOSITION 1. *The polynomial*

$$P(x) := x^{17} - 5x^{16} + 12x^{15} - 28x^{14} + 72x^{13} - 132x^{12} + 116x^{11} - 74x^9 + 90x^8 - 28x^7 - 12x^6 + 24x^5 - 12x^4 - 4x^3 - 3x - 1 \in \mathbb{Q}[x]$$

has Galois group isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$ *with its natural action on* $\mathbb{P}^1(\mathbb{F}_{16})$.

What is still unknown is whether there exists a regular extension of $\mathbb{Q}(T)$ with Galois group isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$; regular here means that it contains no algebraic elements over $\mathbb{Q}$ apart from $\mathbb{Q}$ itself. In Section 2 we will say some words about the calculation of the polynomial and the connection with modular forms. We'll indicate how one can verify that it has the claimed Galois group in Section 3 using computational Galois theory. We will show in Section 4 that this polynomial gives a Galois representation associated to an explicitly given modular form.

1.1. *Further remarks*

In algebraic number theory, the root discriminant of a number field K is defined as $d(K) := |\mathrm{Disc}(\mathcal{O}_K)|^{1/[K:\mathbb{Q}]}$. This way of measuring number fields appears to be very useful in asymptotic analysis on the set of all number fields (inside a fixed algebraic closure of $\mathbb{Q}$, say). An excellent survey paper on this material is [**18**].

This research was partially supported by the Dutch scientific organisation NWO.
Received 14 June 2007, revised 24 September 2007; *published* 27 December 2007.
2000 Mathematics Subject Classification 11Y40, 11F80, 11R29, 12F12
© 2007, Johan Bosman

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

Let us mention some interesting results here as well. For example it is known that the bounds

$$22.38 \approx 4\pi e^{\gamma} \leqslant \liminf_K d(K) \leqslant 82.11$$

hold; see [**19**, Section 7] for the lower bound and [**10**, Section 3.2] for the upper bound. Under the assumption of the Generalised Riemann Hypothesis we even have

$$\liminf_K d(K) \geqslant \Omega := 8\pi e^{\gamma} \approx 44.76,$$

see [**20**]. In view of this lower bound, root discriminants below Ω are called *small* and it is interesting to construct number fields that have small root discriminant. A paper focussing on the construction of Galois number fields with small root discriminant is [**12**]. A question asked in that paper is whether there exists such a field of which the Galois group contains a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$ (see [**12**, Section 13]). The splitting field of the polynomial in Proposition 1 has root discriminant $2^{15/8} \cdot 137^{1/2} \approx 42.93$ and thus answers this question affirmatively.

The example given in Proposition 1 is not the only polynomial that the author could produce. Here are the other examples of polynomials having Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$ computed so far:

$$x^{17} + x^{16} - 4x^{15} - 2x^{14} + 54x^{13} + 6x^{12} - 36x^{11} - 16x^{10} + 714x^9 \\ - 1238x^8 + 484x^7 + 764x^6 - 1084x^5 - 520x^4 + 668x^3 + 776x^2 + 382x + 74$$

and

$$x^{17} + x^{16} + 18x^{15} + 10x^{14} + 194x^{13} + 250x^{12} + 442x^{11} + 1006x^{10} + 1176x^9 \\ - 392x^8 + 1178x^7 + 4490x^6 + 4790x^5 + 1606x^4 + 286x^3 + 38x^2 + 25x + 1.$$

The former polynomial defines a number field that ramifies above 2 and 173 and the number field defined by the latter polynomial ramifies above 2 and 199. The root discriminants of their splitting fields are $2^{15/8}173^{1/2} \approx 48.25$ and $2^{15/8}199^{1/2} \approx 51.74$ respectively, hence they are not small.

2. *Computation of the polynomial*

In this section we will briefly indicate how one can find a polynomial like the one in Proposition 1. We will make use of modular forms. For an overview as well as many further references on this subject the reader is referred to [**6**].

Let N be a positive integer and consider the space $S_2(\Gamma_0(N))$ of holomorphic cusp forms of weight 2 for $\Gamma_0(N)$. A newform $f \in S_2(\Gamma_0(N))$ has a q-expansion $f = \sum a_n q^n$ where the coefficients a_n are in a number field. The smallest number field containing all the coefficients is denoted by K_f. To a given prime number ℓ and a place λ of K_f above ℓ one can attach a semi-simple Galois representation $\overline{\rho}_f = \overline{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ unramified outside $N\ell$ satisfying the following property: for each prime $p \nmid N\ell$ and any Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to p we have

$$\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_p)) \equiv a_p \bmod \lambda \quad \text{and} \quad \mathrm{Det}(\overline{\rho}_f(\mathrm{Frob}_p)) \equiv p \bmod \lambda. \tag{1}$$

The representation $\overline{\rho}_f$ is unique up to isomorphism. The fixed field of $\mathrm{Ker}(\overline{\rho}_f)$ in $\overline{\mathbb{Q}}$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathrm{Im}(\overline{\rho}_f)$. For $\ell = 2$ and any λ

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

above ℓ equation (1) together with Chebotarev's density theorem imply that $\mathrm{Im}(\overline{\rho}_f)$ is contained in $\mathrm{SL}_2(\mathbb{F}_\lambda)$. So to show that there is an extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$ it suffices to find an N and a newform $f \in S_2(\Gamma_0(N))$ such that there is a prime λ of degree 4 above 2 in K_f and $\mathrm{Im}(\overline{\rho}_f)$ is the full group $\mathrm{SL}_2(\mathbb{F}_\lambda)$. Using modular symbols we can calculate the coefficients of f, hence traces of matrices that occur in the image of $\overline{\rho}_f$. For a survey paper on how this works, see [**25**]. A subgroup Γ of $\mathrm{SL}_2(\mathbb{F}_{16})$ contains elements of every trace if and only if Γ equals $\mathrm{SL}_2(\mathbb{F}_{16})$; this can be shown in several ways, either by a direct calculation or by invoking a more general classification result like [**27**, Theorem III.6.25]. With this in mind, after a small computer search in which we check the occurring values of $\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_p))$ up to some moderate bound of p, one finds that a suitable modular form f exists in $S_2(\Gamma_0(137))$. It turns out that we have $K_f \cong \mathbb{Q}(\alpha)$ with the minimal polynomial of α equal to x^4+3x^3-4x-1 and that f is the form whose q-expansion starts with

$$f = q + \alpha q^2 + (\alpha^3 + \alpha^2 - 3\alpha - 2)q^3 + (\alpha^2 - 2)q^4 + \cdots .$$

Now the next question comes in: knowing this modular form, how does one produce a polynomial? In general, one can use the Jacobian $J_0(N)$ to construct $\overline{\rho}_f$. In this particular case we can do that in the following way. We observe that K_f is of degree 4 and that the prime 2 is inert in it. Furthermore we can verify that the subspace of $S_2(\Gamma_0(137))$ fixed by the Atkin-Lehner operator w_{137} is exactly the subspace generated by all the complex conjugates of f. These observations imply that $\overline{\rho}_f$ is isomorphic to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Jac}(X_0(137)/\langle w_{137}\rangle)[2]$, where we give this latter space an $\mathbb{F}_{16}$-vector space structure via the action of the Hecke operators. Note that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{SL}_2(\mathbb{F}_{16})$ implies surjectivity of the natural map $\mathbb{T} \to \mathcal{O}_{K,f}/(2) \cong \mathbb{F}_{16}$, where $\mathbb{T}$ is the Hecke algebra attached to $S_2(\Gamma_0(N))$. The methods described in [**8**, Sections 11 & 24] allow us now to give complex approximations of the 2-torsion points of $\mathrm{Jac}(X_0(137)/\langle w_{137}\rangle)$ to a high precision. This part of the calculation took by far the most effort; the author will write more details about how this works in a future paper (or thesis). We use this to give a real approximation of a polynomial with Galois group isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$. The results from [**8**, Sections 14 to 19] do, at least implicitly, give a theoretical upper bound for the height of the coefficients of the polynomial hence an upper bound for the calculation precision to get an exact result. Though this upper bound is small in the sense that it leads to a polynomial time algorithm, it is still far too high to be of use in practice. However it turns out that we can use a much smaller precision to obtain our polynomial, the only drawback being that this does not give us a proof of its correctness, so we have to verify this afterwards.

The polynomial P' obtained in this way has coefficients of about 200 digits so we want to find a polynomial of smaller height defining the same number field K. To do this, we first compute the ring of integers $\mathcal{O}_K$ of K. In [**2**, Section 6] an algorithm to do this is described, provided that one knows the squarefree factorisation of $\mathrm{Disc}(f)$ [**2**, Theorem 1.4] and even if we don't know the squarefree factorisation of the discriminant, the algorithm produces a 'good' order in K [**2**, Theorem 1.1]. Assuming that our polynomial P' is correct we know that K is unramified outside $2 \cdot 137$ so we can easily calculate the squarefree factorisation of $\mathrm{Disc}(f)$ and hence apply the algorithm. Having done this we obtain an order in K with a discriminant small enough to be able to factor and hence we know that this is indeed the maximal

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

order $\mathcal{O}_K$. Explicitly, the discriminant is equal to

$$\mathrm{Disc}(\mathcal{O}_K) = 2^{30} \cdot 137^8. \tag{2}$$

We embed $\mathcal{O}_K$ as a lattice into $\mathbb{C}^{[K:\mathbb{Q}]}$ in the natural way and use lattice basis reduction, see [**16**, (1.15)], to compute a short vector $\alpha \in \mathcal{O}_K - \mathbb{Z}$. The minimal polynomial of α has small coefficients. In our particular case $[K : \mathbb{Q}]$ is equal to 17, which is a prime number, hence this new polynomial must define the full field K. This method gives us also a way of expressing α as an element of $\mathbb{Q}(x)/(P'(x))$.

3. *Verification of the Galois group*

Now that we have computed a polynomial $P(x)$, we want to verify that its Galois group $\mathrm{Gal}(P)$ is really isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$ and that we can identify the set $\Omega(P)$ of roots of P with $\mathbb{P}^1(\mathbb{F}_{16})$ in such a way that the action of $\mathrm{Gal}(P)$ on $\Omega(P)$ is identified with the action of $\mathrm{SL}_2(\mathbb{F}_{16})$ on $\mathbb{P}^1(\mathbb{F}_{16})$.

For completeness let us remark that it is easy to verify that $P(x)$ is irreducible since it is irreducible modulo 5. The irreducibility of P implies that $\mathrm{Gal}(P)$ is a transitive permutation group of degree 17. The transitive permutation groups of degree 17 have been classified, see for example [**22**, Section 5]. From [**27**, Theorem III.6.25] it follows that up to conjugacy there is only one subgroup of index 17 in $\mathrm{SL}_2(\mathbb{F}_{16})$, namely the group of upper triangular matrices. This implies that up to conjugacy there is exactly one transitive $G < S_{17}$ that is isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$. Hence if $\mathrm{Gal}(P) \cong \mathrm{SL}_2(\mathbb{F}_{16})$ is an isomorphism of groups then there is an identification of $\Omega(P)$ with $\mathbb{P}^1(\mathbb{F}_{16})$ such that the group actions become compatible.

It follows from the classification in [**22**, Section 5] that if the order of a transitive $G < S_{17}$ is divisible by 5, then G contains a transitive subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_{16})$. To show $5 \mid \#\mathrm{Gal}(P)$ we use the fact that for a prime $p \nmid \mathrm{Disc}(P)$ the decomposition type of P modulo p is equal to the cycle type of any Frobenius element in $\mathrm{Gal}(P)$ attached to p. One can verify that modulo 7 the polynomial P has an irreducible factor of degree 15, showing that indeed $5 \mid \#\mathrm{Gal}(P)$ holds, hence $\mathrm{Gal}(P)$ contains $\mathrm{SL}_2(\mathbb{F}_{16})$ as a subgroup.

To show that $\mathrm{Gal}(P)$ cannot be bigger than $\mathrm{SL}_2(\mathbb{F}_{16})$ it seems inevitable to use heavy computer calculations. We will use ideas from [**9**], in particular [**9**, Algorithm 6.1], which combines the absolute resolvent method from [**23**] with an improved version of the relative resolvent method from [**24**]. It would be interesting to see how $\mathrm{Gal}(P) \cong \mathrm{SL}_2(\mathbb{F}_{16})$ can be proven without using heavy calculations.

Note that the action of $\mathrm{SL}_2(\mathbb{F}_{16})$ on $\mathbb{P}^1(\mathbb{F}_{16})$ is sharply 3-transitive. So first we show that $\mathrm{Gal}(P)$ is not 4-transitive to prove that it does not contain A_{17}. To do this we start with calculating the polynomial

$$Q(x) := \prod_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\} \subset \Omega(P)} (X - \alpha_1 - \alpha_2 - \alpha_3 - \alpha_4), \tag{3}$$

where the product runs over all subsets of $\{1, \ldots, 17\}$ consisting of exactly 4 elements. This implies $\deg(Q) = 2380$. One can calculate $Q(x)$ using symbolic methods (see [**5**, Section 2.1]). Suppose that $\mathrm{Gal}(P)$ acting on $\Omega(P)$ is 4-transitive. Then the action on $\Omega(Q)$ is transitive hence if $Q(x)$ is squarefree it is irreducible. So if we can show that $Q(x)$ is reducible and squarefree, we have shown that $\mathrm{Gal}(P)$ is not 4-transitive.

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

We have two ways to find a nontrivial factor of $Q(x)$: the first way is use a factorisation algorithm and the second way is to produce a candidate factor ourselves. An algorithm that works very well for our type of polynomial is Van Hoeij's algorithm [**11**, Section 2.2]. One finds that $Q(x)$ is the product of 3 distinct irreducible polynomials of degrees 340, 1020 and 1020 respectively. A more direct way to produce a candidate factorisation is as follows. The calculation of the 2-torsion in the Jacobian mentioned in Section 2 gives a bijection between the set of complex roots of P' and the set $\mathbb{P}^1(\mathbb{F}_{16})$ such that the action of $\mathrm{Gal}(P')$ on $\Omega(P')$ corresponds to the action of $\mathrm{SL}_2(\mathbb{F}_{16})$ on $\mathbb{P}^1(\mathbb{F}_{16})$, assuming the outcome is correct. From the previous section we know how to express the roots of P as rational expressions in the roots of P hence this gives us a bijection between $\Omega(P)$ and $\mathbb{P}^1(\mathbb{F}_{16})$, conjecturally compatible with the group actions of $\mathrm{Gal}(P)$ and $\mathrm{SL}_2(\mathbb{F}_{16})$ respectively. A calculation shows that the action of $\mathrm{SL}_2(\mathbb{F}_{16})$ on the set of unordered four-tuples of elements of $\mathbb{P}^1(\mathbb{F}_{16})$ has 3 orbits, of size 340, 1020 and 1020 respectively. Using approximations to a high precision of the roots, we use these orbits to produce sub-products of (3), round off the coefficients to the nearest integer and verify afterwards that the obtained polynomials are indeed factors of $Q(x)$.

Let us remark that the group $\mathrm{SL}_2(\mathbb{F}_{16}).4 := \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes \mathrm{Aut}(\mathbb{F}_{16})$ with its natural action on $\mathbb{P}^1(\mathbb{F}_{16})$ is a transitive permutation group of degree 17, and the same holds for its normal subgroup $\mathrm{SL}_2(\mathbb{F}_{16}).2 := \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes \langle \mathrm{Frob}_2^2 \rangle$. Furthermore, it is well-known that $\mathrm{SL}_2(\mathbb{F}_{16}).4$ is isomorpic to $\mathrm{Aut}(\mathrm{SL}_2(\mathbb{F}_{16}))$ (where $\mathrm{SL}_2(\mathbb{F}_{16})$ acts by conjugation and $\mathrm{Aut}(\mathbb{F}_{16})$ acts on matrix entries) and actually inside S_{17} this group is the normaliser of both $\mathrm{SL}_2(\mathbb{F}_{16})$ and itself. According to the classifiation of transitive permutation groups of degree 17 in [**22**, Section 5] these two groups are the only ones that lie strictly between $\mathrm{SL}_2(\mathbb{F}_{16})$ and A_{17}. Once we have fixed $\mathrm{SL}_2(\mathbb{F}_{16})$ inside S_{17}, these two groups are actually unique subgroups of S_{17}, not just up to conjugacy.

From $A_{17} \not< \mathrm{Gal}(P)$ we can thus conclude $\mathrm{Gal}(P) < \mathrm{SL}_2(\mathbb{F}_{16}).4$. To proceed we consult [**9**, Theorem 2.17], which gives a good computational method to move down over small steps in a lattice of transitive permutation groups. Using this method we can easily go from $\mathrm{Gal}(P) < \mathrm{SL}_2(\mathbb{F}_{16}).4$ to $\mathrm{Gal}(P) < \mathrm{SL}_2(\mathbb{F}_{16}).2$ and from there to $\mathrm{Gal}(P) < \mathrm{SL}_2(\mathbb{F}_{16})$. So indeed we have $\mathrm{Gal}(P) \cong \mathrm{SL}_2(\mathbb{F}_{16})$.

4. *Does P indeed define $\overline{\rho}_f$?*

So now that we have shown $\mathrm{Gal}(P) \cong \mathrm{SL}_2(\mathbb{F}_{16})$ we can wonder whether we can prove that P comes from the modular form f we used to construct it with. Once an isomorphism of $\mathrm{Gal}(P)$ with $\mathrm{SL}_2(\mathbb{F}_{16})$ is given, the polynomial P defines a representation $\overline{\rho}_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{SL}_2(\mathbb{F}_{16})$. Above we mentioned that that $\mathrm{Out}(\mathrm{SL}_2(\mathbb{F}_{16}))$ is isomorphic to $\mathrm{Aut}(\mathbb{F}_{16})$ acting on matrix entries. Hence, up to an automorphism of $\mathbb{F}_{16}$, the map sending $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to the characteristic polynomial of $\overline{\rho}_P$ in $\mathbb{F}_{16}[x]$ is determined by P and in fact the isomorphism class of $\overline{\rho}_P$ is well-defined up to an automorphism of $\mathbb{F}_{16}$. More concretely, we have to show that the splitting field of P, which we will denote by L, is the fixed field of $\mathrm{Ker}(\overline{\rho}_f)$.

A continuous representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ has a *level*, denoted by $N(\overline{\rho})$, and a *weight*, denoted by $k(\overline{\rho})$. Instead of repeating the full definitions here, which are lengthy (at least for the weight) and can be found in [**21**, Sections 1.2 and 2] (see also [**7**, Section 4] for a discussion on the definition of the weight), we will just

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

say that they are defined in terms of the local representations $\overline{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ obtained from $\overline{\rho}$. The level is defined in terms of the representations $\overline{\rho}_p$ with $p \neq \ell$ and the weight is defined in terms of $\overline{\rho}_\ell$. The following conjecture is due to Serre:

Conjecture 1 (Serre's strong conjecture, [**21**, Conjecture 3.2.4]). *Let ℓ be a prime and let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be a continuous odd irreducible Galois representation (a representation is called odd if the image of a complex conjugation has determinant -1). Then there exists a modular form f of level $N(\overline{\rho})$ and weight $k(\overline{\rho})$ which is a normalised eigenform and a prime $\lambda \mid \ell$ of K_f such that $\overline{\rho}$ and $\overline{\rho}_{f,\lambda}$ become isomorphic after a suitable embedding of $\mathbb{F}_\lambda$ into $\overline{\mathbb{F}}_\ell$.*

In 2006, Khare and Wintenberger proved the following part of Serre's strong conjecture:

Theorem 1 (Khare & Wintenberger [**14**, Theorem 1.2]). *Conjecture 1 holds in each of the following cases:*

- *$N(\overline{\rho})$ is odd and $\ell > 2$.*
- *$\ell = 2$ and $k(\overline{\rho}) = 2$.*

With Theorem 1 in mind it is sufficient to prove that a representation $\overline{\rho} = \overline{\rho}_P$ attached to P has level 137 and weight 2, which are the level and weight of the modular form f we used to construct it with and that of all eigenforms in $S_2(\Gamma_1(137))$, the form f is one which gives rise to $\overline{\rho}_P$. Therefore, in the remainder of this section we will verify the following proposition.

Proposition 2. *Let f be the cusp form from Section 2. Up to an automorphism of $\mathbb{F}_{16}$, the representations $\overline{\rho}_P$ and $\overline{\rho}_{f,(2)}$ are isomorphic. In particular, the representation $\overline{\rho}_P$ has Serre-level* 137 *and Serre-weight* 2.

Let us argue that it is not clear how to prove the modularity of $\overline{\rho}_P$ using only results that are older than Theorem 1. The older results deal with cases that are 'small' in some sense. For example, [**17**, Thms 1 & 2] deal with $\overline{\rho}$ that satisfy $N(\overline{\rho}) = 1$ or $k(\overline{\rho}) = 1$ and focus on proving *non-existence* of Galois representations. Also, the group $\mathrm{SL}_2(\mathbb{F}_{16})$ is too big to apply other results. It is a non-solvable group and in that case there are some old results dealing with $\mathrm{Im}\,\overline{\rho} \subset \mathrm{GL}_2(\mathbb{F}_q)$ for $q \in \{2^2, 3^2, 5, 7\}$, but not for $q = 16$ (see [**13**, Section 1.3] for a survey). Neither is it clear how to do a computer search of whichever kind that will eliminate the possibility that $\overline{\rho}_P$ is not isomorphic to $\overline{\rho}_{f,(2)}$, as the group $\mathrm{SL}_2(\mathbb{F}_{16})$ and the degree 17 are simply too big.

4.1. *Verification of the level*

The level is the easiest of the two to verify. Here we have to do local computations in p-adic fields with $p \neq 2$. According to the definition of $N(\overline{\rho})$ in [**21**, Section 1.2] it suffices to verify that $\overline{\rho}$ is unramified outside 2 and 137, tamely ramified at 137 and the local inertia subgroup I at 137 leaves exactly one line of $\mathbb{F}_{16}^2$ pointwise fixed. That $\overline{\rho}_P$ is unramified outside 2 and 137 follows immediately from (2).

From (2) and the fact that $137^8 \| \mathrm{Disc}(P)$ it follows that the monogeneous order defined by P is maximal at 137. Modulo 137, the polynomial P factors as

$$\overline{P} = (x+14)(x^2+6x+101)^2(x^2+88x+97)^2(x^2+106x+112)^2(x^2+133x+110)^2.$$

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

Let v be any prime above 137 in L. From the above factorisation it follows that the prime 137 decomposes in K as a product of 5 primes; one of them has its inertial and ramification degree equal to 1 and the other four ones have their inertial and ramification degrees equal to 2. Thus $\deg(v)$ is a power of 2, as L is obtained by successively adjoining roots of P and in each step the relative inertial and ramification degrees of the prime below v are both at most 2. In particular, $\mathrm{Gal}(L_v/\mathbb{Q}_{137})$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_{16})$ whose order is a power of 2. Now, $\{\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\}$ is a Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_{16})$, so $\mathrm{Gal}(L_v/\mathbb{Q}_{137})$ is, up to conjugacy, a subgroup of $\{\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\}$. Hence I is also conjugate to a subgroup of $\{\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\}$ and it is actually nontrivial because 137 ramifies in L (so I is of order 2 since the tame inertia group of any finite Galois extension of local fields is cyclic).

It is immediate that $\overline{\rho}$ is tamely ramified at 137 as no power of 2 is divisible by 137. Also, it is clear that I leaves exactly one line of $\mathbb{F}_{16}^2$ pointwise fixed since $\{\binom{*}{0}\}$ is the only pointwise fixed line of any nontrivial element of $\{\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\}$. This establishes the verification of $N(\overline{\rho}) = 137$.

4.2. *Verification of the weight*

Because the weight is defined in terms of the induced local representation $\overline{\rho}_2$, we will try to compute some relevant properties of the splitting field L_v of P over $\mathbb{Q}_2$, where v is any place of L above 2. In p-adic fields one can only do calculations with a certain precision, but this does not give any problems since practically all properties one needs to know can be verified rigorously using a bounded precision calculation and the error bounds in the calculations can be kept track of exactly.

The polynomial P does not define an order which is maximal at the prime 2. Instead we use the polynomial

$$\begin{aligned} R = {} & x^{17} - 11x^{16} + 64x^{15} - 322x^{14} + 916x^{13} + 276x^{12} - 5380x^{11} + 2748x^{10} \\ & + 6904x^9 - 23320x^8 + 131500x^7 - 140744x^6 - 16288x^5 - 39752x^4 \\ & - 48840x^3 + 102352x^2 + 234466x - 1518, \end{aligned}$$

which is the minimal polynomial of

$$\begin{aligned} & \big(36863 + 22144\alpha + 123236\alpha^2 + 154875\alpha^3 - 416913\alpha^4 + 436074\alpha^5 + 229905\alpha^6 \\ & - 1698406\alpha^7 + 1857625\alpha^8 - 467748\alpha^9 - 2289954\alpha^{10} + 2838473\alpha^{11} - 1565993\alpha^{12} \\ & + 605054\alpha^{13} - 263133\alpha^{14} + 112104\alpha^{15} - 22586\alpha^{16}\big)/8844, \end{aligned}$$

where α is a root of P. We can factor R over $\mathbb{Q}_2$ and see that it has one root in $\mathbb{Q}_2$ which happens to be odd, and an Eisenstein factor of degree 16, which we will call E. This type of decomposition can be read off from the Newton polygon of R and it also shows that the order defined by R is indeed maximal at 2. From the oddness of the root and (2) we see

$$v_2(\mathrm{Disc}(E)) = 30. \tag{4}$$

For the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ on $\mathbb{P}^1(\mathbb{F}_{16})$ the factorisation means that there is one fixed point and one orbit of degree 16. If we adjoin a root β of E to $\mathbb{Q}_2$ and factor E over $\mathbb{Q}_2(\beta)$ then we see that it has an irreducible factor of degree 15; in [**4**, Section 6] one can find methods for factorisation and irreducibility testing that can be used to verify this. This means that $[L_v : \mathbb{Q}_2]$ is at least 240.

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

A subgroup of $\mathrm{SL}_2(\mathbb{F}_{16})$ that fixes a point of $\mathbb{P}^1(\mathbb{F}_{16})$ has to be conjugate to a subgroup of the group

$$H := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{F}_{16}),$$

which is the stabiliser subgroup of $[\binom{*}{0}]$. But we have $\#H = 240$ so $\mathrm{Gal}(L_v/\mathbb{Q}_2)$ is isomorphic to H and from now on we will identify these two groups with each other. We can filter H by normal subgroups:

$$H \supset I \supset I_2 \supset \{e\},$$

where I is the inertia subgroup and I_2 is the wild ramification subgroup, which is the unique Sylow 2-subgroup of I. We wish to determine the groups I and I_2. Let $k(v)$ be the residue class field of L_v. The group H/I is isomorphic to $\mathrm{Gal}(k(v)/\mathbb{F}_2)$ and I/I_2 is isomorphic to a subgroup of $k(v)^*$. In particular $[I : I_2] \mid (2^{[H:I]} - 1)$ follows. The group H has the nice property

$$[H, H] = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \cong \mathbb{F}_{16},$$

which is its unique Sylow 2-subgroup. As H/I is abelian, we see that $[H, H] \subset I$. We conclude that $I_2 = [H, H]$, since above we remarked that I_2 is the unique Sylow 2-subgroup of I. The restriction $[I : I_2] \mid (2^{[H:I]} - 1)$ leaves only one possibility for I, namely $I = I_2$.

Let L_v' be the subextension of $L_v/\mathbb{Q}_2$ fixed by I. Then L_v' is the maximal unramified subextension as well as the maximal tamely ramified subextension. It is in fact isomorphic to $\mathbb{Q}_{2^{15}}$, the unique unramified extension of $\mathbb{Q}_2$ of degree 15 and the Eisenstein polynomial E from above, being irreducible over any unramified extension of $\mathbb{Q}_2$, is a defining polynomial for the extension $L_v/\mathbb{Q}_{2^{15}}$. According to [**17**, Theorem 3] we can relate the discriminant of L_v to $k(\overline{\rho})$ as follows:

$$v_2(\mathrm{Disc}(L_v)) = \begin{cases} 240 \cdot \frac{15}{8} = 450 & \text{if } k(\overline{\rho}) = 2 \\ 240 \cdot \frac{19}{8} = 570 & \text{if } k(\overline{\rho}) \neq 2 \end{cases}$$

It follows from (4) that $v_2(\mathrm{Disc}(L_v/\mathbb{Q}_2)) = 30 \cdot 15 = 450$, so indeed $k(\overline{\rho}) = 2$.

4.3. *Verification of the form f*

Now we know $N(\overline{\rho}_P) = 137$ and $k(\overline{\rho}_P) = 2$ Theorem 1 shows that there is an eigenform $g \in S_2(\Gamma_1(137))$ giving rise to $\overline{\rho}_P$. Using [**3**, Corollary 2.7] we see that if such a g exists, then there actually exists such a g of trivial Nebentypus, i.e. $g \in S_2(\Gamma_0(137))$ (as $\mathrm{SL}_2(\mathbb{F}_{16})$ is non-solvable $\overline{\rho}_P$ cannot be an induced Hecke character from $\mathbb{Q}(i)$).

A modular symbols calculation shows that there exist two Galois orbits of newforms in $S_2(\Gamma_0(137))$: the form f we used for our calculations and another form, g say. The prime 2 decomposes in K_g as a product $\lambda^3\mu$, where λ has inertial degree 1 and μ has inertial degree 4. So it could be that $g \bmod \mu$ gives rise to $\overline{\rho}_P$. We will show now that $f \bmod (2)$ and $g \bmod \mu$ actually give the same representation. The completions of $\mathcal{O}_{K_f}$ and $\mathcal{O}_{K_g}$ at the primes (2) and μ respectively are both isomorphic to $\mathbb{Z}_{16}$, the unramified extension of $\mathbb{Z}_2$ of degree 4. After a choice of embeddings of $\mathcal{O}_{K_f}$ and $\mathcal{O}_{K_g}$ into $\mathbb{Z}_{16}$ we obtain two modular forms f' and g' with coefficients in $\mathbb{Z}_{16}$ and we wish to show that a suitable choice of embeddings exists such that they are congruent modulo 2. According to [**26**, Theorem 1], it suffices to

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

check there is a suitable choice of embeddings that gives $a_n(f') \equiv a_n(g') \bmod 2$ for all $n \leqslant [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(137)]/6 = 23$ (in [**26**] this theorem is formulated for modular forms with coefficients in the ring of integers of a number field, but the proof also works for p-adic rings). Using a modular symbols calculation, this can be easily verified. The bound on the indices up to which one has to check such a congruence is usually referred to as the *Sturm bound* or *Hecke bound*.

Appendix A. Magma *code used for computations*

All the calculations were done using Magma (see [**1**]); for most of them the author used the Medicis cluster (see http://medicis.polytechnique.fr). The Magma code used for the computation of the polynomials, together with a short instruction on how to use it, has been included as an add-on to this paper and may be found at

http://www.lms.ac.uk/jcm/10/lms2007-024/appendix-a

Acknowledgements. I would like to thank Jürgen Klüners for proposing this computational challenge and explaining some computational Galois theory to me. Furthermore I want to thank Bas Edixhoven for teaching me about modular forms and the calculation of their coefficients. Thanks also go to David Roberts, for making me aware of the small root discriminant problem and the fact that this polynomial provides an example for it. For being able to make use of the Medicis cluster I want to thank Marc Giusti and Pierre Lafon.

References

1. W. Bosma, J. J. Cannon, C. E. Playoust, 'The magma algebra system I: the user language', *J. Symbolic Comput.* 24 (1997) no. 3/4, 235–265.

2. J. A. Buchmann and H. W. Lenstra, Jr., 'Approximating rings of integers in number fields', *J. Théor. Nombres Bordeaux* 6 (1994) no. 2, 221–260.

3. K. Buzzard, 'On level-lowering for mod 2 representations', *Math. Research Letters* 7 (2000) 95–110.

4. D. G. Cantor and D. M. Gordon, 'Factoring polynomials over p-adic fields', Proceedings of the 4th International Symposium on Algorithmic Number Theory, 2000, 185–208.

5. D. Casperson and J. McKay, 'Symmetric functions, m-sets, and Galois groups', *Math. Comp.* 63 (1994) 749–757

6. F. Diamond and J. Im, 'Modular forms and modular curves', in: Seminar on Fermat's Last Theorem (Toronto, ON, 1993-1994), CMS Conf. Proc. 17, Amer. Math. Soc., Providence, RI, 1995, 39–133.

7. S. J. Edixhoven, 'The weight in Serre's conjectures on modular forms', *Invent. Math.* 109 (1992) no. 3, 563–594.

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

8. S. J. Edixhoven *et al.*, 'On the computation of coefficients of a modular form', eprint, 2006, arXiv reference math.NT/0605244v1.

9. K. Geissler and J. Klüners, 'Galois group computation for rational polynomials', *J. Symbolic Comput.* 30 (2000) 653–674.

10. F. Hajir and C. Maire, 'Tamely ramified towers and discriminant bounds for number fields II', *J. Symbolic Comput.* 33 (2002) 415–423.

11. M. van Hoeij, 'Factoring polynomials and the knapsack problem', *J. Number Theory* 95 (2002) 167–189.

12. J. W. Jones and D. P. Roberts, 'Galois number fields with small root discriminant', *J. Number Theory* 122 (2007) 379–407.

13. C. Khare, 'Serre's modularity conjecture: a survey of the level one case', to appear in *L-functions and Galois representations* (Durham, UK, 2004).

14. C. Khare and J.-P. Wintenberger, 'Serre's modularity conjecture: the odd conductor case (I, II)', preprint, 2006, available at http://www.math.utah.edu/~shekhar/papers.html

15. J. Klüners and G. Malle, 'Explicit Galois realization of transitive groups of degree up to 15', *J. Symbolic Comput.* 30 (2000) no. 6, 675–716.

16. A. K. Lenstra, H. W. Lenstra, Jr., L. Lovász, 'Factoring polynomials with rational coefficients', *Math. Ann.* 261 (1982) no. 4, 515–534.

17. H. Moon and Y. Taguchi, 'Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations', *Documenta Math.* Extra Volume Kato (2003) 641–654.

18. A. M. Odlyzko, 'Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey or recent results', *Sém de Théorie des nombres, Bordeaux* 2 (1990) 119–141.

19. G. Poitou, 'Minoration de discriminants (d'après A. M. Odlyzko)', *Lecture notes in mathematics* 567 (1977) 136–153.

20. J.-P. Serre, 'Minoration de discriminants', note of October 1975, published in *Œuvres*, Vol. III (Springer, 1986) 240–243.

21. J.-P. Serre, 'Sur les représentations modulaire de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$', *Duke Math. J.* 54 (1987) no. 1, 179–230.

22. C. C. Sims, 'Computational methods for permutation groups', in: *Computational problems in abstract algebra* (J. Leech, ed.; Pergamon, Elmsforth, N.Y., 1970) 169–184.

23. L. Soicher and J. McKay, 'Computing Galois groups over the rationals', *J. Number Theory* 20 (1985) 273–281.

24. R. P. Stauduhar, 'The determination of Galois groups', *Math. Comp.* 27 (1973) 981–996.

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press

25. W. A. Stein, 'An introduction to computing modular forms using modular symbols', eprint, downloadable at
http://modular.fas.harvard.edu/papers/msri-stein-ant/

26. J. Sturm, 'On the congruence of modular forms', Lecture Notes in Mathematics 1240 (1987) 275–280.

27. M. Suzuki, *Group theory I*, Grundlehren der mathematischen Wissenschaften 247 (Springer, New York, 1982).

Johan Bosman jgbosman@math.leidenuniv.nl

Mathematisch Instituut
Postbus 9512
2300 RA Leiden
The Netherlands

https://doi.org/10.1112/S1461157000001467 Published online by Cambridge University Press