Universität Regensburg
Mathematik

On projective linear groups over finite fields as Galois groups over the rational numbers

Gabor Wiese

Preprint Nr. 14/2006

On projective linear groups over finite fields as Galois groups over the rational numbers

Gabor Wiese

28th June 2006

Abstract

Ideas and techniques from Khare's and Wintenberger's preprint on the proof of Serre's conjecture for odd conductors are used to establish that for a fixed prime l infinitely many of the groups $\mathrm{PSL}_2(\mathbb{F}_{l^r})$, $PGL_2(\mathbb{F}_{l^r})$ (for r running) occur as Galois groups over the rationals such that the corresponding number fields are unramified outside a set consisting of l and only one other prime.

1 Introduction

The aim of this article is to prove the following theorem.

1.1 Theorem. *Let l be a prime and s a positive number. Then there exists a set T of rational primes of positive density such that for each $q \in T$ there exists a modular Galois representation*

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l})$$

which is unramified outside $\{l, q\}$ and whose projective image is isomorphic to either $\mathrm{PSL}_2(\mathbb{F}_{l^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{l^r})$ for some $r > s$.

1.2 Corollary. *Let l be a prime. Then for infinitely many positive integers r the groups $\mathrm{PSL}_2(\mathbb{F}_{l^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{l^r})$ occur as a Galois group over the rationals.* □

Using $\mathrm{SL}_2(\mathbb{F}_{2^r}) \cong \mathrm{PSL}_2(\mathbb{F}_{2^r}) \cong \mathrm{PGL}_2(\mathbb{F}_{2^r})$ one obtains the following reformulation for $l = 2$.

1.3 Corollary. *For infinitely many positive integers r the group $\mathrm{SL}_2(\mathbb{F}_{2^r})$ occurs as a Galois group over the rationals.* □

This contrasts with work by Dieulefait, Reverter and Vila ([D], [RV] and [DV]) who proved that the groups $\mathrm{PSL}_2(\mathbb{F}_{l^r})$ and $\mathrm{PGL}_2(\mathbb{F}_{l^r})$ occur as Galois groups over $\mathbb{Q}$ for fixed (small) r and infinitely many primes l.

In the author's PhD thesis [W] some computational evidence on the statement of Corollary 1.3 was exhibited. More precisely, it was shown that all groups $\mathrm{SL}_2(\mathbb{F}_{2^r})$ occur as Galois groups over $\mathbb{Q}$

for $1 \leq r \leq 77$, extending results by Mestre (see [S2], p. 53), by computing Hecke eigenforms of weight 2 for prime level over finite fields of characteristic 2.

However, at that time all attempts to prove the corollary failed, since it could not be ruled out theoretically that all Galois representations attached to modular forms with image contained in $\mathrm{SL}_2(\mathbb{F}_{2^r})$ for r bigger than some fixed bound and not in any $\mathrm{SL}_2(\mathbb{F}_{2^a})$ for $a \mid r$, $a \neq r$, have a dihedral image.

With the methods from [KW1] and [KW2] one can now find - so called - good-dihedral representations in a given level times an auxiliary prime. These have the property that the image of their associated Galois representation is not dihedral. Moreover, the definition of good-dihedral assures that the image contains an element of order equal to a power of a certain prime which one can make big.

Acknowledgements

The author would like to thank Bas Edixhoven for very useful discussions.

Notations

We shall use the following notations. By $G_{\mathbb{Q}}$ we denote the absolute Galois group of the rational numbers. For a rational prime q we let D_q and I_q be a decomposition group resp. the corresponding inertia group at the prime q. All Galois representations are assumed to be continuous. If $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is an odd Galois representation, we denote by $N(\overline{\rho})$ and $k(\overline{\rho})$ the conductor and the Serre weight of $\overline{\rho}$ (see [S1]). By $S_k(N, \chi)$ we mean the complex vector space of holomorphic modular forms of level N, weight k for the Dirichlet character χ. If χ is trivial, we write $S_k(N)$ for short.

2 Good-dihedral representations

We first state the definition of *good-dihedral* following [KW1].

2.1 Definition. *Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l})$ be a continuous representation.*

- *A prime $q \neq l$ is called* good-dihedral *for $\overline{\rho}$ if both of the following two statements hold:*
  - *(i) The restriction of $\overline{\rho}$ to I_q is of the form $\left(\begin{smallmatrix} \psi & 0 \\ 0 & \psi^q \end{smallmatrix}\right)$ for a character $\psi : I_q \to \overline{\mathbb{F}_l}^*$ of order p^s for some $s > 0$ and some odd prime p which divides $q+1$ and is greater than l, 5 and greater than all prime divisors of $N(\overline{\rho})$ different from q.*
  - *(ii) $q \equiv 1 \mod 8$ and $q \equiv 1 \mod r$ for every prime $r \neq q$ smaller than or equal to the maximum of l and the greatest prime divisor of $N(\overline{\rho})$ different from q.*
- *If a good-dihedral prime q exists for $\overline{\rho}$, then $\overline{\rho}$ is called* good-dihedral *or q-*dihedral*. In that case we will say that the number p^s of (i) is the q-*order of *$\overline{\rho}$.*

If $\overline{\rho}$ is q-dihedral, the ramification at q is tame and the local conductor at q is equal to q^2, since no line is fixed.

The following is [KW1], Lemma 6.3(i). It already shows the usefulness of the definition of good-dihedral in our context.

2.2 Lemma. *Any q-dihedral representation has non-solvable image.* □

We will not repeat the proof here. Let us just say that (ii) in the above definition assures that the prime q cannot be inert in any quadratic field whose discriminant only contains primes dividing $N(\overline{\rho})$. As $p \nmid q-1$, the restriction of the representation to D_q is irreducible which then suffices to rule out the dihedral case.

We next state the definition of a strictly compatible system of Galois representations following [KW1].

2.3 Definition. *Let E be a number field. An E-*rational 2-dimensional strictly compatible system of representations (ρ_λ) of $G_{\mathbb{Q}}$ *is the data of: For each finite place λ of E a continuous semi-simple representation*

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(E_\lambda)$$

such that:

(i) For each rational prime q and each place λ of E of residue characteristic different from q, the Frobenius-semi-simplification of the Weil-Deligne parameter of $\rho_\lambda|_{D_q}$ is independent of λ, and for almost all primes q this parameter is unramified.

(ii) For almost all places λ of E, the representation ρ_Λ is crystalline at l (if Λ divides l) with integral Hodge-Tate weights (a, b) that are independent of l.

2.4 Theorem. (Khare, Wintenberger) *Let $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be an odd continuous representation with non-solvable image for a prime $p > 5$ such that $p \equiv 1 \mod 4$ and p is greater than any prime divisor of $N(\overline{\rho}_p)$. We suppose $k(\overline{\rho}_p) = 2$.*

Then there exists a set of primes T of positive density such that for any $q \in T$ the following statement holds:

> *There exists a number field E and an E-rational compatible system of representations (ρ_λ) lifting $\overline{\rho}_p$ such that the residual representations $\overline{\rho}_l$ for all primes $l < p$ are q-dihedral of order a power of p and are unramified outside l, q and the primes dividing $N(\overline{\rho}_p)$.*

Proof. This follows from [KW1], Lemma 8.2, and [KW1], Theorem 5.1(4), which is proved in [KW2], and proceeds analogously to the couple of lines below the proof of [KW1], Lemma 8.2.

Let us be more precise. We take T to be the set of primes provided by an application of [KW1], Lemma 8.2, to $\overline{\rho}_p$. That is, T consists of primes q which are unramified in $\overline{\rho}_p$ and satisfy

(i) $\overline{\rho}_{p,\text{proj}}(\text{Frob}_q)$ is the conjugacy class of $\overline{\rho}_{p,\text{proj}}(c)$ where c denotes a complex conjugation and $\overline{\rho}_{p,\text{proj}}$ stands for the projectivisation,

(ii) $q \equiv 1 \mod r$ for all primes $r < p$ and $q \equiv 1 \mod 8$, and

(iii) $q \equiv -1 \mod p$.

Let now $q \in T$. Conditions (i) and (iii) assure that one may appeal to [KW1], Theorem 5.1(4), with the prime q. For, one needs that $\overline{\rho}_p|_{D_q}$ is of the form $\begin{pmatrix} \overline{\chi}_p & * \\ 0 & 1 \end{pmatrix}$ up to unramified twists. But, due to $q \equiv -1 \mod p$ this becomes $\begin{pmatrix} -1 & * \\ 0 & 1 \end{pmatrix}$. The conjugacy class of a complex conjugation takes the form $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Condition (i) now gives that this coincides with $\overline{\rho}_p|_{D_q}$ up to a scalar, which in turn corresponds to an unramified twist.

Consequently, [KW1], Theorem 5.1(4), yields a strictly compatible system (ρ_λ) lifting $\overline{\rho}_p$ such that $\rho_p|_{I_q}$ is of the form $\begin{pmatrix} \psi & * \\ 0 & \psi^q \end{pmatrix}$ for a character ψ of I_q of order a power of p.

Let now l be any prime smaller than p. The next step is to show that $\overline{\rho}_l$ is q-dihedral of q-order a power of p. Condition (ii) of the definition of q-dihedral is met due to Condition (ii) provided above, using that $\overline{\rho}_l$ is unramified outside l, q and the prime divisors of $N(\overline{\rho}_p)$, still by [KW1], Theorem 5.1(4). For $l = 2$ this is not explicitly stated in [KW1], but follows from the independence of the Weil-Deligne parameters and the fact that a Weil-Deligne representation is unramified if and only if its Frobenius-semi-simplification is.

Part (i) in the definition of q-dihedral is fulfilled by construction and by the fact that the inertial Weil-Deligne parameter at q is the same for any member of (ρ_λ), whence we get that the q-order is a power of p in these cases. □

3 On images of Galois representations

In order to determine which projective images can occur we quote the following well-known group theoretic result due to Dickson (see [Hu], II.8.27).

3.1 Proposition. (Dickson) *Let l be a prime and H a finite subgroup of $\text{PGL}_2(\overline{\mathbb{F}_l})$. Then a conjugate of H is isomorphic to one of the following groups:*

- *finite subgroups of the upper triangular matrices,*
- $\text{PSL}_2(\mathbb{F}_{l^r})$ *or* $\text{PGL}_2(\mathbb{F}_{l^r})$ *for* $r \in \mathbb{N}$,
- *dihedral groups D_r for $r \in \mathbb{N}$ not divisible by l,*
- A_4, A_5 *or* S_4.

We next quote two results of Ribet showing that the images of Galois representations of the type we are interested in are in general not solvable.

3.2 Proposition. (Ribet) *Let $f \in S_2(N, \chi)$ be an eigenform of level N and some character χ which is not a CM-form. Then for almost all primes p, the image of the representation*

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

attached to f restricted to a suitable open subgroup $H \leq G_{\mathbb{Q}}$ is $\{g \in \mathrm{GL}_2(\mathbb{F}) | \det(g) \in \mathbb{F}_p^*\}$ for some finite extension $\mathbb{F}$ of $\mathbb{F}_p$.

Proof. Reducing modulo a suitable prime above p, this follows from Theorem 3.1 of [R1], where the statement is proved for the p-adic representation attached to f. □

3.3 Proposition. (Ribet) *Let N be a square-free integer and $f \in S_2(N)$ a newform for the trivial character. Then for all primes $p > 2$, the image of the Galois representation*

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

attached to f contains the group $\mathrm{SL}_2(\mathbb{F}_p)$ if $\overline{\rho}_p$ is irreducible.

Proof. The representation $\overline{\rho}_p$ is semi-stable (see [R2], p. 278). As it is assumed to be irreducible, the proposition is just a restatement of [R2], Corollary 2.3. □

We will use these two results by Ribet in order to establish the simple fact that for a given prime l there exists a modular form of level a power of l whose mod p Galois representations have non-solvable images for almost all p.

The following lemma can be easily verified using e.g. William Stein's modular symbols package which is part of MAGMA ([Magma]).

3.4 Lemma. *In any of the following spaces there exists a newform without CM: $S_2(2^7)$, $S_2(3^4)$, $S_2(5^3)$, $S_2(7^3)$, $S_2(13^2)$.*

3.5 Lemma. *Let $l \geq 11$, $l \neq 13$ be a prime and $f \in S_2(l)$ a newform. Then for almost all primes p, the image of the Galois representation*

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

attached to f contains the group $\mathrm{SL}_2(\mathbb{F}_p)$.

Proof. Due to the assumption on l the existence of a newform in $S_2(l)$ is guaranteed. By Proposition 3.3 it suffices to prove that $\overline{\rho}_p$ is irreducible for almost all p.

Since its Frobenius traces are given by reductions of the Fourier coefficients of f, it is clear that $\overline{\rho}_p$ is non-trivial for almost all p. Non-triviality, however, implies that the conductor of $\overline{\rho}_p$ is l. For, it can only be 1 or l. If it were 1, then level lowering would imply that $\overline{\rho}_p$ comes from an eigenform in $S_2(1) = 0$, contradicting the non-triviality.

So, we suppose that the conductor of $\overline{\rho}_p$ is l. The definition of the conductor shows that there exists a $\sigma \in I_l$ such that $\overline{\rho}_p(\sigma) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ for some $a \neq 0$. This yields that $\overline{\rho}_p$ is irreducible. □

3.6 Corollary. *Let l be a prime. Then for almost all primes p there exists a modular Galois representation*

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

such that $k(\overline{\rho}_p) = 2$, the conductor of $\overline{\rho}_p$ is a power of l and the image of $\overline{\rho}_p$ is non-solvable.

Proof. If $l \in \{2, 3, 5, 7, 13\}$ we appeal to Lemma 3.4 together with Proposition 3.2 in order to obtain the claim. For the other l we may use Lemma 3.5. We use that $\mathrm{SL}_2(\mathbb{F}_p)$ is non-solvable for $p > 2$. □

4 Proof and remarks

In this section we prove the main theorem of this note and comment on possible generalisations.

Proof of Theorem 1.1. Corollary 3.6 provides us with a prime $p > l$ and a modular Galois representation $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ satisfying

(i) $p \equiv 1 \mod 4$,

(ii) no group $\mathrm{GL}_2(\mathbb{F}_{l^a})$ contains an element of order p for any $a \leq s$, and

(iii) $\overline{\rho}_p$ has non-solvable image, its conductor is a power of l and $k(\overline{\rho}_p) = 2$.

From Theorem 2.4 we obtain a set of primes T of positive density such that for all $q \in T$ there exists a compatible system (ρ_λ) such that $\overline{\rho}_l$ is q-dihedral of order a power of p and $\overline{\rho}_l$ is unramified outside $\{l, q\}$. Lemma 2.2 tells us that the image of $\overline{\rho}_l$ is non-solvable. Consequently, Assumption (ii) made on p implies that the image of $\overline{\rho}_l$ is not conjugate to a subgroup of $\mathrm{GL}_2(\mathbb{F}_{l^a})$ for any $a \leq s$.

Composing $\overline{\rho}_l$ with the natural projection $\mathrm{GL}_2(\overline{\mathbb{F}_l}) \to \mathrm{PGL}_2(\overline{\mathbb{F}_l})$, the image is of the claimed form by Proposition 3.1. □

4.1 Remark. *The author is intending to develop the basic idea used here further, in particular, in order to try to establish an analogue of Theorem 1.1 such that the representations ramify at a given finite set of primes S and are unramified outside $S \cup \{l, q\}$.*

4.2 Remark. *It is desirable to remove the ramification at l. For that, one would need that $\overline{\rho}_l$ is unramified at l. This, however, seems difficult to establish.*

References

[Magma] W. Bosma, J.J. Cannon, C. Playoust. *The Magma Algebra System I: The User Language.* J. Symbolic Comput. **24** (1997), 235–265.

[D] L. V. Dieulefait. *Newforms, inner twists, and the inverse Galois problem for projective linear groups.* Journal de Théorie des Nombres de Bordeaux **13** (2001), 395–411.

[DV] L. V. Dieulefait, N. Vila. *Projective linear groups as Galois groups over $\mathbb{Q}$ via modular representations.* J. Symbolic Computation **30** (2000), 799–810.

[Hu] B. Huppert. *Endliche Gruppen I*. Grundlehren der mathematischen Wissenschaften **134**. Springer-Verlag, 1983.

[KW1] C. Khare, J.-P. Wintenberger. *Serre's modularity conjecture: the case of odd conductor (I)*. Preprint, 2006.

[KW2] C. Khare, J.-P. Wintenberger. *Serre's modularity conjecture: the case of odd conductor (II)*. Preprint, 2006.

[RV] A. Reverter, N. Vila. *Some projective linear groups over finite fields as Galois groups over $\mathbb{Q}$*. Contemporary Math. **186** (1995), 51–63.

[R1] K. A. Ribet. *On l-adic representations attached to modular forms II*. Glasgow Math. J. **27** (1985), 185–194.

[R2] K. A. Ribet. *Images of semistable Galois representations*. Pacific Journal of Mathematics **181** No. 3 (1997), 277–297.

[S1] J.-P. Serre. *Sur les représentations modulaires de degré 2 de Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$*. Duke Math. J. **54** No. 1 (1987), 179–230.

[S2] J.-P. Serre. *Topics in Galois theory.* Research Notes in Mathematics **1**. Jones and Bartlett Publishers, Boston, MA, 1992.

[W] G. Wiese. *Modular Forms of Weight One Over Finite Fields*. PhD thesis, Universiteit Leiden, 2005.

Gabor Wiese

NWF I - Mathematik, Universität Regensburg, D-93040 Regensburg, Germany

E-mail: `gabor@pratum.net`, Web page: `http://maths.pratum.net/`