HAL
open science

Galois realizations of families of projective linear groups via cusp forms

Luis Victor Dieulefait

To cite this version:

Luis Victor Dieulefait. Galois realizations of families of projective linear groups via cusp forms. 1998. hal-00147919

HAL Id: hal-00147919
https://hal.science/hal-00147919v1

Preprint submitted on 21 May 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Galois realizations of families of Projective Linear Groups via cusp forms

Luis Dieulefait
Dept. d'Algebra i Geometria, Universitat de Barcelona
Gran Via de les Corts Catalanes 585
08007 - Barcelona
Spain

December 14, 2006

1 Introduction

Let S_k be the space of cusp forms of weight k for $SL_2(\mathbf{Z})$ and $S_2(N)$ the one of cusp forms of weight 2 for $\Gamma_0(N)$.

We are going to consider the Galois representations attached to eigenforms in these spaces, whose images have been determined by Ribet and Momose (see [Ri 75] for S_k and [Mo 82], [Ri 85] for $S_2(N)$).

Our purpose is to use these representations to realize as Galois groups over $\mathbf{Q}$ some linear groups of the following form: $PSL_2(p^r)$ if r is even and $PGL_2(p^r)$ if r is odd. In order to ease the notation, we will call both these families of linear groups $PXL_2(p^r)$, so that PXL stands for PSL if r is even and PGL if r is odd.

Extending the results in [Re-Vi], where it is shown that for $r \leq 10$ these groups are Galois groups over $\mathbf{Q}$ for infinitely many primes p, we will cover the cases $r = 11, 13, 17$ and 19, using the representations attached to eigenforms in S_k and again the cases 11 and 17 using the ones coming from $S_2(N)$.

We will give the explicit criterion for the case $r = 3$: for every prime

$p > 3$ such that $p \equiv 2, 3, 4, 5 \pmod 7$ the group $PGL_2(p^3)$ is a Galois group over $\mathbf{Q}$.

Assuming the following conjecture: "The characteristic polynomial $P_{2,k}$ of the Hecke operator T_2 acting on S_k is irreducible over $\mathbf{Q}$, for all k " , we will prove that for every prime exponent $r \geq 3$, $PGL_2(p^r)$ is a Galois group over $\mathbf{Q}$ for infinitely many primes p.

Finally, applying results of [Br 96] we will prove that there exist infinitely many exponents r for which $PXL_2(p^r)$ are Galois groups over $\mathbf{Q}$ for infinitely many primes p.

Remark: This article was written in 1998 and it corresponds to a Research Project advised by Nuria Vila that the author did as part of his PhD at the Universitat de Barcelona, previous to his thesis.

2 Galois representations attached to eigenforms in S_k

Generalizing the result of [Ri 75] for $r = 2$, in [Re-Vi] sufficient conditions are given for $PXL_2(p^r)$ to be a Galois group over $\mathbf{Q}$. They are the following:

Criterion 2.1 : Let k be such that $\dim_{\mathbf{C}} S_k = r$.

Let $P_{2,k}$ be the characteristic polynomial of the Hecke operator T_2 acting on S_k. Let $d_{2,k}$ be its discriminant and λ one of its roots.

Let p be a prime such that $p \notin \Sigma_{k,\lambda}$, where $\Sigma_{k,\lambda}$ is a **finite** set of primes that can be computed in terms of k and λ.

Then if $P_{2,k}$ is irreducible mod$p$,(which implies, in particular, that it is irreducible over $\mathbf{Q}$) $PXL_2(p^r)$ is a Galois group over $\mathbf{Q}$.

Remark 2.2 : The condition $P_{2,k}$ irreducible mod$p$ implies that there are infinitely many inert primes in $\mathbf{Q}(\lambda)$ (besides, $\mathbf{Q}(\lambda) = \mathbf{Q}_f$ for some eigenform f). From this, $PXL_2(q^r)$ is realized as a Galois group over $\mathbf{Q}$ for infinitely many primes q. ([Re-Vi]).

Corollary 2.3 *: Suppose that there is a prime p_0 such that $P_{2,k}$ is irreducible* modp_0. *Then there are infinitely many primes p not in $\Sigma_{k,\lambda}$ satisfying this and for all of them $PXL_2(p^r)$ is a Galois group over $\mathbf{Q}$, where $r = \dim_{\mathbf{C}} S_k$*

Remark 2.4 : The existence of such a prime for $r = 2, 3, 4, ..., 10$ is verified in [Re-Vi], thus 2.3 applies to these exponents.

In [Bu 96] it is proved that for $r = 11, 13, 17, 19,$ $P_{2,12r}$ is irreducible *mod* $479, 353, 263, 251$ respectively. Then applying 2.3 we obtain:

Corollary 2.5 *: $PGL_2(p^r)$ is a Galois group over $\mathbf{Q}$ for $r = 11, 13, 17, 19,$ for infinitely many primes p in each case.*

The following conjecture is widely believed:

Conjecture 2.6 *: For every k, the characteristic polynomial $P_{2,k}$ of the Hecke operator T_2 acting on S_k is irreducible over $\mathbf{Q}$.*

Even assuming 2.6 we are not in condition of applying 2.3 for other values of r. However, in case r is prime we can use the following :

Lemma 2.7 *: Let K be a number field of prime degree p over $\mathbf{Q}$. Then there exist infinitely many rational primes inert in K.*

Proof: Let N be the normal closure of K and $G = Gal(N/\mathbf{Q})$. It is clear that $\#G = [N : \mathbf{Q}]$ satisfies:

$$p \mid \#G, \qquad \#G \mid p! \tag{2.1}$$

Let H be a $p-$Sylow subgroup of G, whose order is p, and let L be its fixed field, so that $H = Gal(N/L)$. Being N/L a cyclic extension of degree p, we can apply class field theory ([Ne], pag. 85) to see that there are infinitely many primes Q of L inert in N/L. Applying this fact, together with the multiplicativity of the residual degree and (2.1), we see that there are infinitely many inert primes q in K.

Theorem 2.8 *: Assume the truth of 2.6. Then for every prime exponent r, there exist infinitely many primes p such that $PGL_2(p^r)$ is Galois over $\mathbf{Q}$*

Proof: Let $k = 12r$. If $P_{2,k}$ is irreducible over $\mathbf{Q}$, calling λ one of its roots we have: $\mathbf{Q}(\lambda) = \mathbf{Q}_f$, for some eigenform f and $\dim_{\mathbf{C}} S_k = r = [\mathbf{Q}_f : \mathbf{Q}]$. The previous lemma implies that there are infinitely many inert primes in $\mathbf{Q}_f$ / $\mathbf{Q}$ and we can apply 2.3 .

3 Galois representations attached to newforms in $S_2(N)$

Let f be a newform of weight 2 in $\Gamma_0(N)$. We apply the following theorem, ([Ri 85], [Re 95]):

Theorem 3.1 *: Let N be squarefree and P_2 be the characteristic polynomial of T_2 acting on $S_2(N)$. Let λ be a simple root of P_2* ***such that*** *there exists a newform $f \in S_2(N)$ verifying $\mathbf{Q}(\lambda) = \mathbf{Q}_f$ (this always holds in the case of prime level). Then for every rational prime p outside a finite set $\Sigma_{N,\lambda}$ inert in $\mathbf{Q}_f$, $PXL_2(p^r)$ is a Galois group over $\mathbf{Q}$, where $r = [\mathbf{Q}_f : \mathbf{Q}]$.*

Remark 3.2 : The fact that the nebentypus $\varepsilon = 1$ and N is squarefree implies that f does not have neither complex multiplication nor inner twists. This is used to obtain the surjectivity of the Galois representations.

In [Wa 73], a table of P_2 polynomials, we see that for $N = 229, 239$ there are simple factors of degree $11, 17$ respectively.

These are prime levels, so that there are no old forms around. Invoking again 2.7 we can apply 3.1 and conclude:

Corollary 3.3 *: $PGL_2(p^r)$ is Galois over $\mathbf{Q}$ for $r = 11, 17$ and infinitely many primes p in both cases.*

In the case of prime level N the exceptional set $\Sigma_{N,\lambda}$ can be 'removed' by using the following new result [Ri 97]:

Proposition 3.4 *: Let $\mathbf{T}$ be the Hecke ring, the ring of endomorphisms over $\mathbf{Q}$ of $J_0(N)$, for prime N . Let $\Re$ be a maximal ideal of $\mathbf{T}$ of residual characteristic $p \geq 5$, and with $\mathbf{T}/\Re = \mathbf{F}_{p^r}$. Then if $\Re$ is not Eisenstein, $PXL_2(p^r)$ is Galois over $\mathbf{Q}$.*

Remark 3.5 : 1- In the prime level case there are no oldforms, and we have the identification:

$$\mathbf{T} \otimes \mathbf{Q} \cong \prod_{f \in \Sigma} \mathbf{Q}_f$$

where Σ is a set of representatives of all newforms modulo the action of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$.

2- The Eisenstein ideal $\Im \subseteq \mathbf{T}$ is the one generated by the elements: $1 + l - \mathbf{T}_l$ $(l \neq N)$, $1 + \omega$. An Eisenstein prime is a prime ideal $\beta \subseteq \mathbf{T}$ in the support of $\Im$. Let $n = num(\frac{N-1}{12})$. We have a one-to-one correspondence between Eisenstein primes β and prime factors p of n, given by:

$$Prime \quad factors \quad of \quad n \leftrightarrow Eisenstein \quad primes$$

$$p \leftrightarrow (\Im, p)$$

Besides, for every Eisenstein prime β, $\mathbf{T}/\beta = \mathbf{F}_p$. In particular, whenever the inertia is nontrivial (and these are the cases we are interested in) the involved prime will not be Eisenstein.

Corollary 3.6 *: $PSL_2(p^2)$ is Galois over $\mathbf{Q}$, for every*

$$p \equiv \pm 2 \pmod 5, \quad p \geq 7.$$

Proof: Consider level $N = 23$. In this case $\mathbf{T} \otimes \mathbf{Q} \cong \mathbf{Q}(\sqrt{5})$, $n = 11$. If $\Re$ is Eisenstein, $\mathbf{T}/\Re = \mathbf{F}_{11}$. In $\mathbf{Q}(\sqrt{5})$ the inert primes are the $p \equiv \pm 2 \pmod 5$. The result follows from 3.4.

Remark 3.7 : The same result is obtained in [Me 88] by a different approach.

Corollary 3.8 *: $PSL_2(p^2)$ is Galois over $\mathbf{Q}$, for every*

$$p \equiv \pm 3 \pmod 8, \quad p \geq 5.$$

Proof: Consider level $N = 29$. Here $\mathbf{T} \otimes \mathbf{Q} \cong \mathbf{Q}(\sqrt{2})$, $n = 7$. If $\Re$ is Eisenstein, $\mathbf{T}/\Re = \mathbf{F}_7$. The inert primes are the $p \equiv \pm 3 \pmod 8$. Apply 3.4.

Remark 3.9 : This same result is obtained in [Re 95] using 3.1 where the exceptional set is explicitated and proved to be disjoint from the set of inert primes.

Corollary 3.10 : *$PGL_2(p^3)$ is Galois over $\mathbf{Q}$, for every*

$$p \equiv 2, 3, 4, 5 \pmod 7, \quad p \geq 5.$$

Proof: Consider level $N = 97$. We found in [Wa 73] that for this level there is a newform f with $\mathbf{Q}_f$ equal to the splitting field of the polynomial:

$$x^3 + 4\ x^2 + 3 - 1$$

This field is the real cyclotomic field: $\mathbf{Q}(\zeta_7 + \zeta_7^{-1})$. The inert primes in this field are the primes that when reduced mod7 give a generator of the group $(\mathbf{Z}/7\mathbf{Z})^*$ or the square of such a generator; corresponding to the cases of residual degree 6 and 3 in $\mathbf{Q}(\zeta_7)$, respectively. These are the following: $p \equiv 2, 3, 4, 5 \pmod 7$. Applying 3.4 and 3.5-1 (and once again the fact that Eisenstein primes are not inert) we obtain the desired result.

We now consider the case of arbitrary level N, again with trivial nebentypus. We still need the assumption that f is a newform without CM (complex multiplication). In this general case, we can apply the surjectivity result of [Ri 85], after replacing $\mathbf{Q}_f$ by the field $F_f \subseteq \mathbf{Q}_f$ defined as follows (we give three equivalent definitions, see [Ri 80]):

Definition 3.11 : Let A_f be the abelian variety associated to f, and $E = End\ A_f \otimes \mathbf{Q}$ its algebra of endomorphisms. We define F_f to be the centre of E. Equivalently, if Γ is the set of all immersions $\gamma : \mathbf{Q}_f \to \mathbf{C}$ such that there exists a Dirichlet character χ with: $\gamma(a_p) = \chi(p)a_p$ for almost every p, where $\sum a_n q^n = f$; then $F_f = \mathbf{Q}_f^\Gamma$, the fixed field of Γ. This coincides with the field generated over $\mathbf{Q}$ by the a_p^2 , p ranging through almost every prime.

The following theorem can be deduced from the results in [Ri 85]:

Theorem 3.12 : *Let f be a newform in $S_2(N)$ without CM. Let p be a rational prime outside a finite set $\Sigma_{N,f}$ and let i be the residual degree in F_f /$\mathbf{Q}$ of some $P \mid p$. Then $PXL_2(p^i)$ is Galois over $\mathbf{Q}$.*

In order to obtain Galois realizations, we need some information about the fields F_f. The best result is the following ([Br 96]):

Theorem 3.13 *: Let f be as in 3.12. Suppose that $p^{r_p} \parallel N$. Let $s_p = \left\lceil \frac{r_p}{2} - 1 - \frac{1}{p-1} \right\rceil$ and ζ a primitive p^{s_p}-root of unity. Then $F_f \supseteq \mathbf{Q}(\zeta + \zeta^{-1})$ if $p > 2$ (resp. $\mathbf{Q}(\zeta^2 + \zeta^{-2})$ if $p = 2$)*

As a particular case, let $p > 3$, $p^3 \parallel N$. Then $s_p = \left\lceil \frac{1}{2} - \frac{1}{p-1} \right\rceil = 1$. If f does not have CM, $F_f \supseteq \mathbf{Q}(\zeta_p + \zeta_p^{-1})$. If q is a rational prime inert in $\mathbf{Q}(\zeta_p)$, that is to say: $q \pmod p$ generates the multiplicative group $\mathbf{F}_p^*$, and if Q is a prime over q in O_{F_f} ,the ring of integers of F_f, we have: $\frac{p-1}{2} \mid f_Q(F_f : \mathbf{Q})$.

All these residual degrees are bounded by $[F_f : \mathbf{Q}]$, then between the infinitely many primes congruent with generators of $\mathbf{F}_p^*$ we can pick out an infinite subset of primes $\{q_i\}_{i \in \mathbf{N}}$ such that for all of them there exists a prime Q_i in O_{F_f} over q_i with:

$$f_{Q_i}(F_f : \mathbf{Q}) = l \cdot \frac{p-1}{2}, \qquad l \quad \textit{independent} \quad \textit{of} \quad i$$

Combining this with 3.12 we get:

Theorem 3.14 *: Let $p > 3$ be a prime and let N be such that $p^3 \parallel N$. Then if there is a newform $f \in S_2(N)$ without CM, there exists a number $l = l(p)$ such that for infinitely many primes q : $PXL_2(q^{l(p-1)/2})$ is a Galois group over $\mathbf{Q}$. The primes q can all be chosen congruent modp to generators of $\mathbf{F}_p^*$.*

Remark 3.15 : 1-There is always an exceptional set $\Sigma_{N,f}$ that has to be eluded in order to apply 3.12.

2-The values of $l = l(p)$ are bounded by:

$$l \leq [F_f : \mathbf{Q}(\zeta_p + \zeta_p^{-1})] < [\mathbf{Q}_f : \mathbf{Q}] \leq \dim S_2^{new}(N)$$

Remark 3.16 In order to apply this result we need to ensure that: "For every odd prime p there exist a positive integer N with $p^3 \parallel N$ and such that every newform $f \in S_2(N)$ does not have complex multiplication." Taking $N = p^3 \cdot t$, t odd prime, $t \neq p$, it is well-known that this holds, in fact if a newform f of this level has CM the corresponding abelian variety A_f, factor of $J_0(N)$, would also have CM ,contradicting the fact that it has multiplicative reduction at t, as can be seen looking at its Néron model.

We see from the remark above that 3.14 applies for every prime $p > 3$ (take $N = p^3 \cdot t$) so that we have:

Corollary 3.17 *: Let $p > 3$ be a prime. Then there exists a positive integer $l = l(p)$ such that for infinitely many primes q : $PXL_2(q^{l(p-1)/2})$ is a Galois group over* $\mathbf{Q}$.

The fact that 3.17 holds for every prime $p > 3$ implies the following:

Corollary 3.18 *: There exist infinitely many positive integers n such that for every one of them there are infinitely many primes q with $PXL_2(q^n)$ being a Galois group over* $\mathbf{Q}$. *Moreover, an infinite number of these exponents n is even.*

4 Bibliography:

[Br 96]- Brumer, A., *The rank of $J_0(N)$,* S.M.F. Astérisque **228** (1995) 41-68

[Bu 96]- Buzzard, K., *On the eigenvalues of the Hecke operator T_2*, J. of Number Theory **57** (1996) 130-132

[Me 88]- Mestre, J.F., *Courbes hyperelliptiques à multiplications réelles*, C.R. Acad. Sci. Paris **307** (1988) 721-724

[Mo 81]- Momose, F., *On the l-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo, Sect. IA Math. **28**:1 (1981) 89-109

[Ne]- Neukirch, J.,*Class Field Theory*, Springer Verlag (1986)

[Re 95]- Reverter, A.,*Construccions arithmètico-geomètriques de grups de Galois*, (thesis) Universitat de Barcelona (1995)

[Re-Vi]- Reverter, A. and Vila, N., *Some projective linear groups over finite fields as Galois groups over* $\mathbf{Q}$, Contemporary Math. **186** (1995) 51-63

[Ri 75]- Ribet, K.A., *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975) 245-275

[Ri 77]- _____, *Galois representations attached to eigenforms with nebentypus*, LNM 601 (1977), Springer-Verlag

[Ri 80]- _____, *Twists of modular forms and endomorphisms of Abelian Varieties*, Math. Ann. **253** (1980) 43-62

[Ri 85]- _____, *On l-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985) 185-194

[Ri 97]- _____, *Images of semistable Galois representations*, Pacific J. of Math. **181**, 3 (1997)

[Wa 73]- Wada, H., *A table of Hecke operators II*, Proc. Japan Acad. **49** (1973) 380-384