Revista Colombiana de Matemáticas
Volumen 39 (2005), páginas 13–19

On certain closed subgroups of $\mathrm{SL}\,(2, \mathbb{Z}_p[[X]])$

Álvaro Lozano-Robledo
Colby College, Waterville, Maine

Abstract. Let $p > 2$ be a prime number and let $\Lambda = \mathbb{Z}_p[[X]]$ be the ring of power series with p-adic integer coefficients. The special linear group of matrices $\mathrm{SL}(2, \Lambda)$ is equipped with several natural projections. In particular, let $\pi_X\colon \mathrm{SL}(2, \Lambda) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p)$ be the natural projection which sends $X \mapsto 0$. Suppose that G is a subgroup of $\mathrm{SL}(2, \Lambda)$ such that the projection $H = \pi_X(G)$ is known. In this note, different criteria are found which guarantee that the subgroup G of $\mathrm{SL}(2, \Lambda)$ is "as large as possible", i.e. G is the full inverse image of H. Criteria of this sort have interesting applications in the theory of Galois representations.

Keywords and phrases. Closed subgroups, Special linear group, Iwasawa algebra.

2000 Mathematics Subject Classification. Primary: 15A33, 15A54, Secondary: 11F80.

1. Introduction

Let $p > 2$ be a prime number and let $\Lambda = \mathbb{Z}_p[[X]]$ be the ring of power series with p-adic integer coefficients. The special linear group of matrices $\mathrm{SL}(2, \Lambda)$ is equipped with several natural projections. In particular, there is a natural projection onto $\mathrm{SL}(2, \mathbb{Z}_p)$:

$$\pi_X\colon \mathrm{SL}(2, \mathbb{Z}_p[[X]]) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p)\,,$$

induced by the natural ring homomorphism $\Lambda \to \mathbb{Z}_p$ which sends X to 0 and $\mathbb{Z}_p$ is fixed. Suppose that G is a subgroup of $\mathrm{SL}(2, \Lambda)$ such that the projection $H = \pi_X(G)$ is known. In this note we are interested in finding different criteria which guarantee that the subgroup G of $\mathrm{SL}(2, \mathbb{Z}_p[[X]])$ is "as large as possible", i.e. G is the full inverse image of H, or equivalently, $\pi_X(G) = H$ and G contains the kernel of π_X. See Theorem 2.3, Corollary 4.2 and Proposition 5.1 for the precise statements.

Criteria of this sort have interesting applications in the theory of Galois representations (and this was the motivation for this work, [4]). Representations of the p-adic type:

$$\begin{aligned} \rho_0 &: \quad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p) \\ \rho_1 &: \quad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{SL}(2,\Lambda)\,, \end{aligned}$$

appear in several natural ways. For example, the representations associated to: the Tate module of an elliptic curve (or abelian varieties in general); modular forms; certain cohomology groups of algebraic varieties, are all of type ρ_0 (see [9], I-3, for more details on examples). The image of these representations is understood in general (see [10] for the elliptic curve case). More recently, representations of type ρ_1 have also been found ([2], [3], [6]). Notice that by composing ρ_1 with π_X one obtains a representation of type ρ_0. Therefore, any previous knowledge of ρ_0 and appropriate criteria about the subgroups of $\mathrm{SL}(2,\Lambda)$, may yield information about the image of ρ_1 (see [5], [7], [4]).

2. Statement of Results

In [9], IV-23, J.-P. Serre proves the following result:

Lemma 2.1. *Let $p \geq 5$ be a prime and let X be a closed subgroup of $\mathrm{SL}(2,\mathbb{Z}_p)$ whose image in $\mathrm{SL}(2,\mathbb{F}_p)$ is the full group $\mathrm{SL}(2,\mathbb{F}_p)$. Then $X = \mathrm{SL}(2,\mathbb{Z}_p)$.*

Nigel Boston ([1], Prop. 2) generalized Serre's result to the following statement. From now on, $\mathcal{M} = (p, X)$ denotes the maximal ideal of $\Lambda = \mathbb{Z}_p[[X]]$.

Proposition 2.2. *Let H be a closed subgroup of $\mathrm{SL}(2,\Lambda)$ whose projection into $\mathrm{SL}(2,\Lambda/\mathcal{M}^2)$ is the full group. Then $H = \mathrm{SL}(2,\Lambda)$.*

In this note, we intend to prove a generalization of Boston's result. Let $p \neq 2$ be a prime number. We define maps:

$$\begin{aligned} \pi_X &: \quad \mathrm{SL}(2,\Lambda) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p), \quad X \mapsto 0 \\ \pi_X^i &: \quad \mathrm{SL}(2,\Lambda/\mathcal{M}^i) \longrightarrow \mathrm{SL}(2,\mathbb{Z}/p^i\mathbb{Z}), \quad X \mapsto 0 \mod p^i\,, \end{aligned}$$

and projections:

$$\begin{aligned} \tau_X^i &: \quad \mathrm{SL}(2,\Lambda) \longrightarrow \mathrm{SL}(2,\Lambda/\mathcal{M}^i) \\ \tau^i &: \quad \mathrm{SL}(2,\mathbb{Z}_p) \longrightarrow \mathrm{SL}(2,\mathbb{Z}/p^i\mathbb{Z})\,. \end{aligned}$$

For closed subgroups $H \leq \mathrm{SL}(2,\Lambda)$, $G \leq \mathrm{SL}(2,\mathbb{Z}_p)$ we write:

$$H_i = \tau_X^i(H) \leq \mathrm{SL}(2,\Lambda/\mathcal{M}^i), \quad G_i = \tau^i(G) \leq \mathrm{SL}(2,\mathbb{Z}/p^i\mathbb{Z})\,.$$

The main theorem is the following:

Theorem 2.3. *Let $\mathfrak{G}$ be a closed subgroup of $\mathrm{SL}(2,\mathbb{Z}_p)$, and let $\mathfrak{H}$ be a closed subgroup of $\mathrm{SL}(2,\Lambda)$ satisfying:*

(1) $\pi_X(\mathfrak{H}) = \mathfrak{G}$.
(2) *The subgroup* $\mathfrak{H}_2$ *is the full inverse image of* $\mathfrak{G}_2$ *by the map* π_X^2*, i.e.*

$$\mathfrak{H}_2 = (\pi_X^2)^{-1}(\mathfrak{G}_2)\,.$$

Then $\mathfrak{H}$ *is the full inverse image of* $\mathfrak{G}$ *by the map* π_X*, this is,* $\mathfrak{H} = (\pi_X)^{-1}(\mathfrak{G})$.

We present two different proofs of Theorem 2.3, which shed light on different interesting aspects. In section 3 we follow Boston's concise proof of Proposition 2.2, which makes use of Burnside's basis theorem. In section 4 we offer an alternative (longer) proof which explicitly describes the kernel of π_X. Moreover, several corollaries can be deduced from the description of the kernel (see Corollary 4.2). The last section is devoted to an improvement of Proposition 2.2 (see Prop. 5.1).

We end this section with the following remark. In order to prove a theorem like 2.3 one may just consider PSL instead of SL. We make this precise in the form of a lemma.

Lemma 2.4. *Let* $P_{\mathbb{Z}_p}\colon \mathrm{SL}(2,\mathbb{Z}_p) \to \mathrm{PSL}(2,\mathbb{Z}_p)$ *be the natural projection and define similarly* $P_\Lambda\colon \mathrm{SL}(2,\Lambda) \to \mathrm{PSL}(2,\Lambda)$*. Let* C *be a closed subgroup of* $\mathrm{PSL}(2,\mathbb{Z}_p)$*, and let* C' *be the full inverse image of* C *in* $\mathrm{SL}(2,\mathbb{Z}_p)$*. Let* $\mathfrak{X}$ *be the full inverse image of* C *in* $\mathrm{PSL}(2,\Lambda)$*, and let* Y *be a closed subgroup of* $\mathrm{SL}(2,\Lambda)$ *such that* $P_\Lambda(Y) = \mathfrak{X}$ *and* $\pi_X(Y) = C'$*. Then* Y *is the full inverse image of* C' *in* $\mathrm{SL}(2,\Lambda)$*.*

$$\begin{array}{ccc}
\mathrm{SL}(2,\Lambda) \geq Y & \xrightarrow{\ \pi_X\ } & C' \leq \mathrm{SL}(2,\mathbb{Z}_p) \\
{\scriptstyle P_\Lambda}\Big\downarrow & & \Big\downarrow{\scriptstyle P_{\mathbb{Z}_p}} \\
\mathrm{PSL}(2,\Lambda) \geq \mathfrak{X} & \xrightarrow[P\pi_X]{} & C \leq \mathrm{PSL}(2,\mathbb{Z}_p)
\end{array}$$

Proof. It suffices to show that $-I$ belongs to Y. By hypothesis, Y contains an element of the form $g = -I + X \cdot A$ with some 2×2 matrix A over Λ. Since Y is closed, Y also contains $\lim_{n\to\infty} g^{p^n} = -I$ which finishes the proof of the lemma. ☑

3. Proof Using Frattini Quotients

In order to prove Theorem 2.3, we follow an argument due to N. Boston ([1], p. 262, Proposition 2) which makes use of the following well known theorem.

Theorem 3.1 (Burnside's basis theorem)**.** *Let* K *be a pro-p group and let* $\overline{K}$ *be its Frattini quotient, i.e.* $\overline{K} = K/K^pK'$ *where* K^p *is the subgroup of pth powers and* K' *is the subgroup of commutators* $(g,h) = ghg^{-1}h^{-1}$*, for all* $g,h \in K$*. If* J *is a closed subgroup of* K *and if the image of* J *in* $\overline{K}$ *is surjective, then* $J = K$*.*

A proof of the theorem for p-groups can be found in [8], p. 274. Use an inverse limit argument to obtain the one stated here. In our case we let K be the kernel of π_X (which is a pro-p group) and let J be the intersection of K with the subgroup $\mathfrak{H} \leq \mathrm{SL}(2, \Lambda)$. Before we can apply Burnside's theorem, we study the Frattini quotient of K. For every $n \geq 2$ we define groups K_n and $\widetilde{K}$ via the following exact sequences of groups:

$$1 \longrightarrow K_n \longrightarrow \mathrm{SL}(2, \Lambda/(X^n)) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p) \longrightarrow 1$$

$$1 \longrightarrow \widetilde{K} \longrightarrow \mathrm{SL}(2, \Lambda/\mathcal{M}^2) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p/(p^2)) \longrightarrow 1\,.$$

Lemma 3.2. *The kernel of the canonical surjection $\pi_n \colon K_{n+1} \twoheadrightarrow K_n$ lies in K'_{n+1}, the commutator subgroup of K_{n+1}. Thus, the induced homomorphism between the Frattini quotients $\overline{K_{n+1}}$ and $\overline{K_n}$ is an isomorphism.*

Proof. One easily computes the following congruence for a commutator:

$$(1 + XA + X^n B,\ 1 + X^{n-1}C + X^n D) \equiv 1 + X^n(AC - CA) \mod X^{n+1}\,,$$

for arbitrary $A,\ B,\ C,\ D \in M_2^0(\mathbb{Z}_p)$, where M_2^0 denotes the set of all 2×2 trace zero matrices. Moreover, any element in $M_2^0(\mathbb{Z}_p)$ can be written as a finite sum of commutators $AC - CA$ using elementary matrices. Since the kernel of π_n is isomorphic to $(1 + X^n M_2^0(\mathbb{Z}_p))$, the previous argument shows that the kernel of π_n lies in K'_{n+1}. The isomorphism between the Frattini quotients follows immediately. ☑

Corollary 3.3. *The Frattini quotient of K, the kernel of π_X, is isomorphic to $\widetilde{K}$.*

Proof. Notice that $K_2 \cong (1 + XM_2^0(\mathbb{Z}_p)) \cong \mathbb{Z}_p^3$, therefore its Frattini quotient, $\overline{K_2}$, is isomorphic to $\mathbb{F}_p^3$. On the other hand, $\widetilde{K} \cong (1 + XM_2^0(\mathbb{F}_p)) \cong \mathbb{F}_p^3$. Hence, by Lemma 3.2, $\overline{K_n} \cong \widetilde{K}$ for all $n \geq 2$. The corollary follows from the fact that K is the inverse limit of the K_n. ☑

Finally, we are ready to prove the theorem.

Proof of Theorem 2.3. By Burnside basis theorem and Corollary 3.3, it suffices to show that if $\mathfrak{H}$ satisfies hypotheses (1) and (2) then the subgroup $\mathfrak{H}_2$ of $\mathrm{SL}(2, \Lambda/\mathcal{M}^2)$ contains $\widetilde{J} = \overline{J_2} \cong \overline{K}$. By hypothesis (2), $\mathfrak{H}_2$ is the inverse image of $\mathfrak{G}_2$ by π_X^2. Thus, $\mathfrak{H}_2$ contains the kernel of π_X^2, which is $\widetilde{J}$, by definition. ☑

4. **Explicit Proof**

In this section we offer an alternative proof of Theorem 2.3 by analizing, K, the kernel of π_X. Note that $K = \{\gamma \in \mathrm{SL}(2, \Lambda) : \gamma \equiv \mathrm{Id} \mod X\}$. The following lemma is an easy exercise in linear algebra, which proves that K is topologically generated by three elements.

Lemma 4.1. *Let $u, v, w \in \mathbb{Z}_p[[X]]^\times$ be fixed. Let $\widetilde{K}$ be the closed subgroup generated by the three matrices:*

$$T_1 = \begin{bmatrix} 1 & uX \\ 0 & 1 \end{bmatrix}, \; T_2 = \begin{bmatrix} 1 & 0 \\ vX & 1 \end{bmatrix}, \; T_3 = \begin{bmatrix} 1+wX & 0 \\ 0 & (1+wX)^{-1} \end{bmatrix}.$$

Then $\widetilde{K} = K$.

Proof. In order to prove the lemma, one checks that the projection of the matrices $T_i, i = 1, 2, 3$ in $\mathrm{SL}(2, \Lambda/\mathcal{M}^2)$ generate the whole group. Then, an induction argument finishes the proof. ☑

Theorem 2.3 is an immediate consequence of the previous lemma.

Second proof of Theorem 2.3. Let $\mathfrak{G}$ be a closed subgroup of $\mathrm{SL}(2, \mathbb{Z}_p)$, and let $\mathfrak{H}$ be a closed subgroup of $\mathrm{SL}(2, \Lambda)$ satisfying:

(1) $\pi_X(\mathfrak{H}) = \mathfrak{G}$.
(2) The subgroup $\mathfrak{H}_2$ is the full inverse image of $\mathfrak{G}_2$ by the map π_X^2, i.e. $\mathfrak{H}_2 = (\pi_X^2)^{-1}(\mathfrak{G}_2)$.

In order to prove that $\mathfrak{H}$ is the full inverse image of $\mathfrak{G}$ by the map π_X, it suffices to show that $K \leq \mathfrak{H}$, where $K = \mathrm{Ker}\,(\mathrm{SL}(2, \Lambda) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p))$. Let us define $\widetilde{K} = K \cap \mathfrak{H}$. By hypothesis, $\mathfrak{H}_2 = (\pi_X^2)^{-1}(\mathfrak{G}_2)$ which in particular implies that $\pi_X^2(\widetilde{K}) = \pi_X^2(K)$. Hence, there exist matrices $\tilde{T}_i \in \widetilde{K}, \; i = 1, 2, 3$ such that:

$$\tilde{T}_1 \equiv \begin{bmatrix} 1 & X \\ 0 & 1 \end{bmatrix}, \; \tilde{T}_2 \equiv \begin{bmatrix} 1 & 0 \\ X & 1 \end{bmatrix}, \; \tilde{T}_3 \equiv \begin{bmatrix} 1+X & 0 \\ 0 & 1-X \end{bmatrix} \mod (p, X)^2.$$

Therefore, there exist $u, v, w \in \mathbb{Z}_p[[X]]$, with $u, v, w \equiv 1 \mod (p, X)$ (in particular $u, v, w \in \mathbb{Z}_p[[X]]^\times$) such that:

$$\tilde{T}_1 = \begin{bmatrix} 1 & uX \\ 0 & 1 \end{bmatrix}, \; \tilde{T}_2 = \begin{bmatrix} 1 & 0 \\ vX & 1 \end{bmatrix}, \; \tilde{T}_3 = \begin{bmatrix} 1+wX & 0 \\ 0 & (1+wX)^{-1} \end{bmatrix}.$$

The hypothesis of Lemma 4.1 are satisfied, hence $K = \widetilde{K} \leq \mathfrak{H}$, which concludes the proof of the theorem. ☑

The previous proof shows that we can prove the equivalent result:

Corollary 4.2. *Let $\mathfrak{G}$ be a closed subgroup of $\mathrm{SL}(2, \mathbb{Z}_p)$, and let $\mathfrak{H}$ be a closed subgroup of $\mathrm{SL}(2, \Lambda)$ satisfying:*

(1) $\pi_X(\mathfrak{H}) = \mathfrak{G}$.
(2) *There exist matrices $T_i \in \mathfrak{H}, \; i = 1, 2, 3$ such that:*

$$T_1 \equiv \begin{bmatrix} 1 & uX \\ 0 & 1 \end{bmatrix}, \; T_2 \equiv \begin{bmatrix} 1 & 0 \\ vX & 1 \end{bmatrix}, \; T_3 \equiv \begin{bmatrix} 1+wX & 0 \\ 0 & 1-wX \end{bmatrix},$$

modulo $(p, X)^2$, for some $u, v, w \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Then $\mathfrak{H}$ is the full inverse image of $\mathfrak{G}$ by the map π_X, this is, $\mathfrak{H} = (\pi_X)^{-1}(\mathfrak{G})$.

5. **A Different Improvement**

In this final section, we come back to the case of the full group $\mathrm{SL}(2,\Lambda)$.

Proposition 5.1. *Let $p \geq 5$ be a prime and let H be a closed subgroup of $\mathrm{SL}(2,\Lambda)$. For $i = 1,2$, let H_i be the projection of H into $\mathrm{SL}(2,\Lambda/\mathcal{M}^i)$. If $H_1 = \mathrm{SL}(2,\mathbb{F}_p)$ and there exist $k \in H \cap \mathrm{Ker}(\pi_X)$ such that $k \neq \mathrm{Id} \mod \mathcal{M}^2$ but $k \equiv \mathrm{Id} \mod (p^2, X)$, then $H = \mathrm{SL}(2,\Lambda)$.*

Proof. By Boston's Proposition 2.2, it suffices to show that

$$H_2 = \mathrm{SL}(2,\Lambda/\mathcal{M}^2).$$

For simplicity, let us denote $G = \mathrm{SL}(2,\Lambda/\mathcal{M}^2)$, $G_2 = \mathrm{SL}(2,\mathbb{Z}/p^2\mathbb{Z})$ and $G_1 = \mathrm{SL}(2,\mathbb{F}_p)$. Also, let $\mathcal{A} = (p^2, X)$ and define $\Gamma(\mathcal{A})$, $\Gamma(\mathcal{M})$ to be the following kernels:

$$\Gamma(\mathcal{A}) = \mathrm{Ker}(G \to G_2), \quad \Gamma(\mathcal{M}) = \mathrm{Ker}(G \to G_1).$$

In particular, $\Gamma(\mathcal{A}) \subseteq \Gamma(\mathcal{M})$. We claim that $\Gamma(\mathcal{M})$ is abelian. Indeed, if $\mathcal{F}_1, \mathcal{F}_2 \in \Gamma(\mathcal{M})$, then there exist matrices F_1, F_2 with coefficients in $\mathcal{M}/\mathcal{M}^2$ such that $\mathcal{F}_1 = \mathrm{Id} + F_1, \mathcal{F}_2 = \mathrm{Id} + F_2$. Thus: $\mathcal{F}_1 \cdot \mathcal{F}_2 = \mathrm{Id} + F_1 + F_2 = \mathcal{F}_2 \cdot \mathcal{F}_1$. Hence, $\Gamma(\mathcal{M})$ is an abelian normal subgroup of G, and so is $\Gamma(\mathcal{A})$. Furthermore the fact that $H_1 = G_1$ implies by Lemma 2.1 that the subgroup H surjects onto G_2. Thus, $G = H_2 \cdot \Gamma(\mathcal{A})$, and so, in order to prove the proposition, it is enough to show that $\Gamma(\mathcal{A})$ is included in H_2.

Lemma 5.2. *$H_2 \cap \Gamma(\mathcal{A})$ is a non-trivial normal subgroup of G.*

Proof. The existence of an element k as in the statement of the proposition ensures that $H_2 \cap \Gamma(\mathcal{A})$ is non-trivial. Let $g \in G$ and $h \in H_2 \cap \Gamma(\mathcal{A})$. Since $h \in \Gamma(\mathcal{A})$, $ghg^{-1} \in \Gamma(\mathcal{A})$ and $G = H_2 \cdot \Gamma(\mathcal{A})$ implies that $g = h_0 \cdot \gamma$ for some $h_0 \in H_2$ and $\gamma \in \Gamma(\mathcal{A})$. Thus:

$$ghg^{-1} = h_0 \gamma h \gamma^{-1} h_0^{-1} = h_0 h h_0^{-1} \in H_2\,,$$

and so $ghg^{-1} \in H_2 \cap \Gamma(\mathcal{A})$. ☑

Since $\Gamma(\mathcal{A})$ is normal in G and $H_2 \leq G$, there is a well defined representation:

$$\rho\colon H_2 \longrightarrow \mathrm{Aut}(\Gamma(\mathcal{A})), \quad h \mapsto (\mathcal{F} \to h\mathcal{F}h^{-1}).$$

Moreover, $H_2 \cap \Gamma(\mathcal{M})$ is included in the kernel of ρ (because $\Gamma(\mathcal{M})$ is abelian). Thus, ρ factors through $H_2/H_2 \cap \Gamma(\mathcal{M}) \cong \mathrm{SL}(2,\mathbb{F}_p) = G_1$. The induced representation of $\mathrm{SL}(2,\mathbb{F}_p)$ into $\mathrm{Aut}(\Gamma(\mathcal{A}))$ is the adjoint representation (because $\Gamma(\mathcal{A}) \cong M_2^0(\mathbb{F}_p)$, the set of zero trace matrices), which is irreducible. By Lemma 5.2, $H_2 \cap \Gamma(\mathcal{A})$ is normal and abelian, thus it is an invariant subspace for ρ and therefore for the adjoint representation of $\mathrm{SL}(2,\mathbb{F}_p)$. By the irreducibility of the latter and the fact that $H_2 \cap \Gamma(\mathcal{A})$ is non-trivial, we conclude that $H_2 \cap \Gamma(\mathcal{A}) = \Gamma(\mathcal{A})$, as desired. ☑

Acknowledgment. The author would like to thank the Revista Colombiana de Matemáticas and its editors for making the contents of the journal available for free to the public. *El autor quisiera agradecer y congratular a la Revista Colombiana de Matemáticas y a sus editores por mantener sus contenidos en internet de manera gratuita para el público.*

References

[1] N. Boston, Appendix to [5], *Compositio Mathematica* **59** (1986), 261–264.

[2] H. Hida, Iwasawa modules attached to congruences of cusp forms, *Annales Scientifiques de l'École Normale Supérieure*, Quatrième Série (4) **19** no. 2 (1986), 231–273.

[3] H. Hida, Galois representations into $\mathrm{GL}_2(Z_p[[X]])$ attached to ordinary cusp forms, *Inventiones Mathematicae* **85** no. 3 (1986), 545–613.

[4] A. Lozano-Robledo, On elliptic units and p-adic Galois representations attached to elliptic curves, To appear in the Journal of Number Theory.

[5] B. Mazur & A. Wiles, On p-adic analytic families of Galois representations, *Compositio Mathematica* **59** (1986), 231–264.

[6] D.E. Rohrlich, A deformation of the Tate module, *Journal of Algebra* **229** (2000), 280–313.

[7] D.E. Rohrlich, Modular units and the surjectivity of a Galois representation, *Journal of Number Theory* **107** (2004), 8–24.

[8] J.S. Rose, *A Course on Group Theory*, Dover Publications, Inc., New York, 1994.

[9] J-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, W.A. Benjamin, Inc., New York, 1968.

[10] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones Mathematicae* **15** (1972), 259–331.

(Recibido en abril de 2005. Revisado en mayo de 2005)

Department of Mathematics
Colby College, Waterville
Maine 04901, USA
e-mail: alozano@colby.edu