C. R. Acad. Sci. Paris, t. 312, Série I, p. 323-328, 1991

Théorie des groupes/*Group Theory*

Quotients of group rings arising from two-dimensional representations

Nigel Boston, Hendrik W. Lenstra Jr. and Kenneth A. Ribet

Abstract – Suppose that $\rho : G \to \mathrm{Aut}_k V$ is an absolutely irreducible two-dimensional representation of a group G over a field k. Let W be a vector space over k, and $\sigma : G \to \mathrm{Aut}_k W$ a representation such that σg is annihilated by the characteristic polynomial of ρg, for each $g \in G$. Then we prove that the $k[G]$-module W is isomorphic to a direct sum of copies of V. This establishes the semisimplicity of some mod p Galois representations which occur naturally in the Jacobians of Shimura curves.

Quotients d'algèbres de groupes provenant de représentations linéaires de dimension 2

Résumé – *Soit* $\rho : G \to \mathrm{Aut}_k V$ *une représentation absolument irréductible, de dimension deux, d'un groupe* G *sur un corps commutatif* k. *Soit* W *un espace vectoriel sur* k, *et soit* $\sigma : G \to \mathrm{Aut}_k W$ *une représentation avec la propriété suivante : pour tout élément* g *de* G, σg *est annulé par le polynôme caractéristique de* ρg. *Alors, on démontre que* W *est isomorphe, en tant que* $k[G]$*-module, à une somme directe de copies du module* V. *On en déduit la semi-simplicité de certaines représentations modulaires du groupe de Galois* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *qui apparaissent de façon naturelle dans les jacobiennes des courbes de Shimura.*

Version française abrégée – Notre résultat principal est le théorème suivant :

Théorème. – *Soit* $\rho : G \to \mathrm{Aut}_k V$ *une représentation absolument irréductible, de dimension* 2, *d'un groupe* G *sur un corps commutatif* k. *Soit* W *un espace vectoriel sur* k, *et soit* $\sigma : G \to \mathrm{Aut}_k W$ *une représentation ayant la propriété suivante : pour tout élément* g *de* G, σg *est annulé par le polynôme caractéristique de* ρg. *Alors,* W *est isomorphe, en tant que* $k[G]$*-module, à une somme directe de copies du module* V.

Soit k un corps commutatif. Une *involution* d'une k-algèbre E est un homomorphisme de k-espaces vectoriels $* : E \to E$ tel que $x^{**} = x$ et $(xy)^* = y^* x^*$ pour $x, y \in E$.

Soit V un espace vectoriel sur k de dimension 2. Soit $*$ l'involution « principale » de la k-algèbre $\mathrm{End}_k V$, caractérisée par l'équation $f + f^* = \mathrm{tr}\, f$ pour $f \in \mathrm{End}_k V$. (On note tr, det : $\mathrm{End}_k V \to k$ la trace et le déterminant.) On a $ff^* = \det f$, $\mathrm{tr}\, f = \mathrm{tr}\, f^*$, $\det f = \det f^*$, et $f^2 - (\mathrm{tr}\, f) f + \det f = 0$ pour tout $f \in \mathrm{End}_k V$.

La représentation ρ induit un homomorphisme de k-algèbres $k[G] \to \mathrm{End}_k V$, noté encore ρ. On écrira simplement tr, det pour les applications $\mathrm{tr} \circ \rho$, $\det \circ \rho : k[G] \to k$.

Soit J l'idéal bilatère de $k[G]$ engendré par $\{g^2 - (\mathrm{tr}\, g) g + \det g : g \in G\}$, et soit $R = k[G]/J$. On a $J \subseteq \ker \rho$, d'où une application $R \to \mathrm{End}_k V$ que l'on appellera encore ρ. Les applications tr et det induisent des applications tr, det : $R \to k$.

Proposition 1. – *Il existe une involution* $*$ *de* R *telle que*

$$(\rho x)^* = \rho(x^*), \qquad x + x^* = \mathrm{tr}\, x, \qquad xx^* = \det x \quad \textit{pour tout } x \in R.$$

Démonstration. – Pour $g \in G$, soit $g^* = g^{-1} . \det g \in k[G]$. Les équations $(gh)^* = h^* g^*$ et $\det g^* = \det g$ montrent que $*$ se prolonge en une involution $*$ de $k[G]$. On a $\rho(x^*) = (\rho x)^*$ pour tout $x \in k[G]$, comme on voit par linéarité en prenant d'abord $x = g \in G$.

Note présentée par Jean-Pierre Serre.

0764-4442/91/03120323 $ 2.00 © Académie des Sciences

De $gg^*=\det g$ et $g^2-(\operatorname{tr} g)g+\det g\in J$, on voit que $g+g^*\equiv \operatorname{tr} g \pmod J$ pour tout $g\in G$. Ceci donne, encore par linéarité, la congruence $x+x^*\equiv \operatorname{tr} x \pmod J$ pour $x\in k[G]$. On a, en particulier, $J^*=J$, d'où une involution * sur R telle que $\rho(x^*)=(\rho x)^*$.

On vient de démontrer la formule $x+x^*=\operatorname{tr} x$, pour $x\in R$. On a, de plus, $xx^*=\det x$ pour tout $x\in R$. En effet, l'identité $(x+y)(x+y)^*=xx^*+yy^*+\operatorname{tr}(xy^*)$ dans R, et l'identité correspondante dans $\operatorname{End}_k V$, montrent que l'ensemble $\{x\in R : xx^*\in k,\ \text{et}\ xx^*=\det x\}$ est stable sous l'addition. Comme cet ensemble contient tout k-multiple d'un élément de G, il coïncide avec R.

Ceci démontre la proposition 1.

Par un calcul évident, la proposition implique l'identité $x^2-(\operatorname{tr} x)x+\det x=0$ pour tout $x\in R$. On remarque également qu'un élément $x\in R$ commute à x^*, puisque $x+x^*=\operatorname{tr} x\in k$. En utilisant l'identité $xx^*=\det x$, et la multiplicativité de det, on voit maintenant que $x\in R$ est une unité de l'algèbre R si et seulement si $\det x$ est non nul; cette dernière condition est satisfaite si et seulement si ρx est une unité de $\operatorname{End}_k V$.

PROPOSITION 2. — *Si l'homomorphisme* $k[G]\to \operatorname{End}_k V$ *est surjectif, alors l'application* $R\to \operatorname{End}_k V$ *qu'il induit est un isomorphisme.*

Démonstration. — Il suffit de démontrer l'injectivité de l'application $R\to \operatorname{End}_k V$, car son image est celle de $k[G]\to \operatorname{End}_k V$.

Soit $x\in R$ tel que $\rho x=0$. On a $x=-x^*$, puisque $\operatorname{tr} x=0$. Pour tout $y\in R$, on en déduit $yx=-yx^*$. Comme on a également $xy^*+yx^*=\operatorname{tr}(xy^*)=0$, on trouve $yx=xy^*$. Ceci donne, pour $y,\ z\in R$, les égalités $yzx=yxz^*=xy^*z^*=x(zy)^*=zyx$, qui entraînent $(yz-zy)x=0$. L'idéal à gauche $\operatorname{Ann} x=\{r\in R : rx=0\}$ de R contient donc l'ensemble $\{yz-zy : y,\ z\in R\}$. Ceci montre que $\operatorname{Ann} x$ est un idéal bilatère de R, et que son image $\rho(\operatorname{Ann} x)$ est un idéal bilatère de $\operatorname{End}_k V$ qui contient $\{ef-fe : e,\ f\in \operatorname{End}_k V\}$. Or, $\operatorname{End}_k V$ est un anneau non commutatif sans idéal bilatère non trivial. On a alors $\rho(\operatorname{Ann} x)=\operatorname{End}_k V$, et, en particulier, on peut trouver $w\in R$ tel que $\rho w=1$ et $wx=0$. Comme on l'a remarqué ci-dessus, w est forcément une unité de R, ce qui implique la nullité de x. La démonstration de la proposition est donc achevée.

On va démontrer maintenant le théorème. Par hypothèse, l'idéal J est contenu dans le noyau de l'homomorphisme $k[G]\to \operatorname{End}_k W$. L'espace vectoriel W est alors, de façon naturelle, un R-module. Comme ρ est absolument irréductible, l'application $k[G]\to \operatorname{End}_k V$ est surjective, et par la proposition 2, elle induit un isomorphisme $R\approx \operatorname{End}_k V$. Il est bien connu que tout $\operatorname{End}_k V$-module est somme directe de sous-modules isomorphes à V. On en déduit le théorème.

Le texte anglais contient une application aux courbes modulaires et donne quelques exemples complémentaires.

---

1. INTRODUCTION. — In this Note we prove the following theorem.

THEOREM 1. — *Suppose that* $\rho : G\to \operatorname{Aut}_k V$ *is an absolutely irreducible two-dimensional representation of a group* G *over a field* k. *Let* W *be a vector space over* k, *and let* $\sigma : G\to \operatorname{Aut}_k W$ *be a representation such that* σg *is annihilated by the characteristic polynomial of* ρg, *for each* $g\in G$. *Then the* $k[G]$*-module* W *is isomorphic to a direct sum of copies of* V.

The theorem becomes false if the hypotheses are relaxed in various ways, for example if three-dimensional representations are considered instead of two-dimensional representations (§ 5).

Representations satisfying our annihilation condition occur naturally in the study of division points of Jacobians of modular curves (§ 3). For example, let J be the Jacobian of the Shimura curve over $\mathbf{Q}$ which is associated to a maximal order in a rational quaternion algebra whose discriminant is the product of two prime numbers. This abelian variety comes equipped with a commuting family of Hecke operators $T_n \in \operatorname{End}(J)$, indexed by the positive integers. These operators generate a subring $\mathbf{T}$ of End (J) which has finite index in End (J) and which is free of rank dim J over $\mathbf{Z}$. To each maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ we may attach: (i) a canonical two-dimensional semisimple representation V of $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ over the field $\mathbf{T}/\mathfrak{m}$, and (ii) the kernel $W = J[\mathfrak{m}]$ of $\mathfrak{m}$ on $J(\bar{\mathbf{Q}})$. The Eichler-Shimura relation for J shows that the characteristic polynomial condition of the theorem is satisfied. Hence the representation W is a direct sum of copies of V whenever V is absolutely irreducible. In [5], the third author constructs a series of examples where V is absolutely irreducible and W has dimension 4. In that case, we have an isomorphism of representations $W \approx V \oplus V$.

2. Principle of the proof. — The action of G on W may be interpreted as a homomorphism $k[G] \to \operatorname{End}_k W$. The hypothesis on W states that this homomorphism is trivial on the two-sided ideal J of $k[G]$ generated by $\{g^2 - (\operatorname{tr} \rho g) g + \det \rho g : g \in G\}$. Hence W is naturally a module over the ring $R = k[G]/J$.

Analogously, the action of G on V may be interpreted as a homomorphism $\lambda : R \to \operatorname{End}_k V$. Since the representation V is assumed to be absolutely irreducible, λ is surjective. We prove that λ is in fact an isomorphism, so that W may be viewed as a module over $\operatorname{End}_k V$. Since all $\operatorname{End}_k V$-modules are isomorphic to direct sums of copies of V, the theorem then follows.

To prove that λ is injective, we consider the involution of $k[G]$ whose restriction to G is the map $g \mapsto (\det \rho g) g^{-1}$. We show that this involution descends to an involution * of R which mimics the main involution of $\operatorname{End}_k V$ in the sense that we have $x + x^* = \operatorname{tr} \lambda x$ and $x x^* = \det \lambda x$ for $x \in R$. Using this involution, and the surjectivity of λ, we prove that λ is injective. For more details, *see* the "Version française abrégée".

3. Jacobians of modular curves. — Let N be a positive integer. Let $X_0(N)$ be the modular curve over $\mathbf{Q}$ associated with the subgroup $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, c \equiv 0 \pmod{N} \right\}$ of $\mathbf{SL}(2, \mathbf{Z})$. For $n \geqq 1$, let T_n denote the nth Hecke correspondence on $X_0(N)$. Abusing notation, we write again T_n for the induced endomorphism T_n^* of the Jacobian $J_0(N)$ of $X_0(N)$.

Let R be the subring of $\operatorname{End}(J_0(N))$ generated by the Hecke operators T_n with n prime to N. The theory of newforms shows that $E = R \otimes \mathbf{Q}$ is a product of totally real algebraic numbers fields E_α and that the degree $[E : \mathbf{Q}]$ is the number of (normalized) newforms of weight 2, trivial character, and level dividing N. The ring R itself is an "order" in E; it is a subring of finite index in the product $\mathcal{O} = \prod \mathcal{O}_\alpha$ of the integer rings of the E_α.

Suppose that $\mathfrak{p}$ is a maximal ideal of the ring R and let $F = R/\mathfrak{p}$ be its residue field. Thus F is a finite field, say of characteristic p. As is well known, there is a semisimple two-dimensional F-linear representation $\rho_\mathfrak{p}$ of $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, characterized up to isomorphism by the following properties:

(i) The representation $\rho_\mathfrak{p}$ is unramified outside p and the prime numbers dividing N;

(ii) For l a prime not dividing Np, and $\varphi_l \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ a Frobenius element for l, the element $\rho_\mathfrak{p}(\varphi_l)$ has trace $T_l \,(\mathrm{mod}\ \mathfrak{p})$ and determinant $l \,(\mathrm{mod}\ \mathfrak{p})$.

To construct $\rho_\mathfrak{p}$, one may note that the ring R operates faithfully on the abelian variety $A := \prod_{M \mid N} J_0(M)_{\mathrm{new}}$, where $J_0(M)_{\mathrm{new}}$ is the new subvariety of $J_0(M)$. The dimension of A is the degree [E : **Q**], and the decomposition of E into the product ΠE_α decomposes A, up to isogeny, as a product of abelian varieties with "real multiplication" by the factors E_α. In particular, the $\mathbf{Q}_p$-adic Tate module $\mathscr{V}_p$ of A is free of rank 2 over $E \otimes \mathbf{Q}_p$. Choose an extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\mathcal{O}$, and let $E_\mathfrak{P}$ be the completion of E at $\mathfrak{P}$. The vector space $\mathscr{V}_\mathfrak{P} := \mathscr{V}_p \otimes_{E \otimes \mathbf{Q}_p} E_\mathfrak{P}$ is a two-dimensional representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ over $E_\mathfrak{P}$, unramified outside pN, which has a property similar to (ii) above. Namely, the $E_\mathfrak{P}$-linear trace (resp. determinant) of φ_l acting on $\mathscr{V}_\mathfrak{P}$ is T_l (resp. l), for l prime to Np. This follows from the Eichler-Shimura relation for T_l ([7], 7.5.1), together with the invariance of T_l under the Rosati involution on $\mathrm{End}(J_0(N))$. (For more details on this latter point, *see* for example [7], Chapter 7.)

By "reducing" this representation mod $\mathfrak{P}$, one obtains a semisimple representation $\rho_\mathfrak{P}$ of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ over $\mathcal{O}/\mathfrak{P}$ with properties analogous to (i) and (ii). More precisely, choose a model for the representation $\mathscr{V}_\mathfrak{P}$ over the completion of $\mathcal{O}$ at $\mathfrak{P}$, reduce mod $\mathfrak{P}$, and then semisimplify. The Brauer-Nesbitt Theorem implies that the resulting object does not depend on the model chosen (*cf.* [6], § 3.6). Since the traces and determinants of $\rho_\mathfrak{P}$ are elements of the subfield F of $\mathcal{O}/\mathfrak{P}$, and since the Brauer group of a finite field is trivial, $\rho_\mathfrak{P}$ has a model over F (*cf.* [1], Lemme 6.13). This is the desired representation $\rho_\mathfrak{p}$.

The Brauer-Nesbitt Theorem and the Čebotarev Density Theorem imply that $\rho_\mathfrak{p}$ is unique up to isomorphism.

Suppose now that **T** is the commutative subring of $\mathrm{End}(J_0(N))$ generated by all T_n with $n \geqq 1$. We have $\mathbf{T} \supseteq \mathrm{R}$. Let $\mathfrak{m}$ be a maximal ideal of **T**, let k be the residue field of $\mathfrak{m}$, and let p be the characteristic of k. Let $\mathfrak{p} = \mathrm{R} \cap \mathfrak{m}$. Then the representation $\rho_\mathfrak{m} := \rho_\mathfrak{p} \otimes_F k$ is a semisimple two-dimensional representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ over k with properties analogous to (i) and (ii). Our aim is to compare $\rho_\mathfrak{m}$ with the "kernel" of $\mathfrak{m}$ on $J = J_0(N)$, *i.e.*, the group $J[\mathfrak{m}] := \{x \in J_0(N)(\bar{\mathbf{Q}}) \mid \mu x = 0 \text{ for all } \mu \in \mathfrak{m}\}$ of p-division points on J. The Eichler-Shimura relation for J shows that each Frobenius element φ_l (with l prime to Np) is annihilated by the polynomial $X^2 - T_l X + l$ on W, *i.e.*, by the characteristic polynomial of φ_l in the representation $\rho_\mathfrak{p}$. Accordingly, by Theorem 1, we have

THEOREM 2. — *Suppose that* $\rho_\mathfrak{m}$ *is an absolutely irreducible representation of* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *over* $\mathbf{T}/\mathfrak{m}$. *Then the representation* $J[\mathfrak{m}]$ *is isomorphic to a direct sum of copies of* $\rho_\mathfrak{m}$.

Remarks. — 1. Theorem 2 strengthens a result of B. Mazur ([2], p. 115) to the effect that the *semisimplification* of $J[\mathfrak{m}]$ is a direct sum of copies of $\rho_\mathfrak{m}$, when the latter representation is irreducible. It is to be noted in this connection that if $\rho_\mathfrak{m}$ is irreducible and p is odd, then $\rho_\mathfrak{m}$ is absolutely irreducible. Indeed, this implication follows from the fact that the image under ρ_m of a complex conjugation in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ has the $\mathbf{F}_p$-rational eigenvalues $+1$ and -1, which are distinct if p is odd.

2. Under an assortment of mild hypotheses, $J[\mathfrak{m}]$ is in fact of dimension two ([2], [4], [3]). Whenever this is so, Mazur's result shows that $J[\mathfrak{m}]$ and $\rho_\mathfrak{m}$ are isomorphic,

provided that the latter representation is simple. Hence Theorem 2 gives no new information in such cases. When we replace J by the Jacobian of a modular curve other than $X_0(N)$, however, we find a larger class of instances where Theorem 2 gives new information. For example, Theorem 2 generalizes immediately to the situation where $\Gamma_0(N)$ is replaced by its analogue in the group of norm-1 elements in a maximal order in an indefinite rational quaternion algebra of discriminant prime to N. The case where $N=1$ and where the quaternion algebra ramifies at exactly two primes is discussed in [5] and alluded to in Section 1 above. As we mentioned in Section 1, [5] exhibits a class of maximal ideals $\mathfrak{m}$ for which $\rho_{\mathfrak{m}}$ is absolutely irreducible, but where $J[\mathfrak{m}]$ has dimension 4 over $T/\mathfrak{m}$. The result of Mazur cited in Remark 1 implies in those cases that $J[\mathfrak{m}]$ can be written, up to isomorphism, as an extension of $\rho_{\mathfrak{m}}$ by $\rho_{\mathfrak{m}}$. The analogue of Theorem 2 implies that the extension is in fact *trivial.*

Similarly, a variant of Theorem 2 holds in the case where $X_0(N)$ is replaced by the modular curve $X_1(N)$.

4. $\mathfrak{P}$-ADIC REPRESENTATIONS. — The discussion of Section 3 suggests abstracting some of its arguments to the following situation.

Let $\mathscr{V}$ be a two-dimensional continuous representation over a finite extension E of $\mathbf{Q}_p$ of a compact group G. Let $\mathcal{O}$ be the "integer ring" of E, and let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}$. Then there exist $\mathcal{O}$-lattices in $\mathscr{V}$ which are G-stable. This implies, for each g in G, that the characteristic polynomial $P_g(X)$ associated to the E-linear action of g on $\mathscr{V}$ has coefficients in $\mathcal{O}$. Further, if $\mathscr{L}$ is a G-stable $\mathcal{O}$-lattice in $\mathscr{V}$, the vector space $\mathscr{L}/\mathfrak{P}\mathscr{L}$ is a two-dimensional representation of G over $\mathcal{O}/\mathfrak{P}$, whose semisimplification is independent of the choice of $\mathscr{L}$. Let V′ be this semisimplification. Thus V′ is the "reduction" of $\mathscr{V}$ mod $\mathfrak{P}$, and the characteristic polynomials associated to this representation are the reductions $\bar{P}_g(X)$ of the $P_g(X)$ mod $\mathfrak{P}$.

Suppose now that $R \subseteq \mathcal{O}$ is a $\mathbf{Z}_p$-subalgebra of $\mathcal{O}$ which contains the coefficients of all polynomials $P_g(X)$, and let $\mathfrak{p}=R\cap\mathfrak{P}$. Then $R/\mathfrak{p}$ is a subfield of the finite field $\mathcal{O}/\mathfrak{P}$ which contains the coefficients of the polynomials $\bar{P}_g(X)$. Accordingly, by the argument mentioned above, V′ has a model V over $R/\mathfrak{p}$; this is a two-dimensional representation of G over $R/\mathfrak{p}$.

Finally, suppose that $\mathscr{M}$ is an R[G]-submodule of $\mathscr{V}$, and let $W=\mathscr{M}/\mathfrak{p}\mathscr{M}$. By the Cayley-Hamilton Theorem, $\mathscr{M}$ is annihilated by the operators $P_g(g)$. Therefore, W is annihilated by each $\bar{P}_g(g)$. From Theorem 1, we conclude:

THEOREM 3. — *In the situation described above, suppose that* V *is absolutely irreducible. Then* W *is a direct sum of copies of* V.

5. COMPLEMENTS. — Theorem 1 becomes false if three-dimensional representations are considered instead of two-dimensional representations. To see this, we note that the alternating group A_4 of order 12 has, over any field k of characteristic different from 2, exactly one absolutely irreducible three-dimensional representation $\rho : G \to \mathrm{Aut}_k V$, up to isomorphism. The characteristic polynomials of the elements of order 1, 2, 3 of A_4 in this representation are $(X-1)^3$, $(X^2-1)(X+1)$, X^3-1, respectively. Therefore *any* k[G]-module W satisfies the hypothesis of the theorem, but not every W is isomorphic to a direct sum of copies of V.

Furthermore, Professor R. Solomon has pointed out to us that Theorem 1 becomes false if one allows the dimension of V to be arbitrary, but requires the semisimplification of W to be isomorphic to a sum of copies of V. Indeed, let $G=\mathbf{PSL}(2, \mathbf{F}_{11})$ and let H be a subgroup of G of index 11 in G. Consider the permutation representation of G on G/H over the field $k=\mathbf{F}_2$, and let V be the trace-zero subrepresentation of this permutation representation. Thus V has dimension 10 over k.

The representation V is the unique irreducible in a 2-block of defect 1 for G. This means that the principal indecomposable module for this block is a *nonsplit* extension W of V by itself. However, W satisfies the annihilation hypothesis of Theorem 1 relative to the characteristic polynomials of V. Indeed, let g be an element of G, and let n be the order of g. If n is odd, W splits as a $k[\langle g \rangle]$-module by Maschke's theorem. If n is even (*i.e.*, $n=2$ or 6), a direct check shows that X^n-1 divides the characteristic polynomial of g on V.

The authors are grateful to Professor R. Solomon for helpful correspondence concerning counterexamples to possible generalizations of Theorem 1. The second author was supported by NSF contracts DMS 87-06176 and DMS 90-02939. The third author was supported by NSF contract DMS 88-06815.

Note remise et acceptée le 24 septembre 1990.

REFERENCES

[1] P. DELIGNE and J.-P. SERRE, Formes modulaires de poids 1, *Ann. Sci. Ecole Norm. Sup.*, 7, 1974, pp. 507-530.

[2] B. MAZUR, Modular curves and the Eisenstein ideal, *Publ. Math. I.H.E.S.*, 47, 1977, pp. 33-186.

[3] B. MAZUR and K. A. RIBET, Two-dimensional representations in the arithmetic of modular curves, *Astérisque* (to appear).

[4] K. A. RIBET, On modular representations of Gal ($\bar{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms, *Invent. Math.*, 100, 1990, pp. 431-476.

[5] K. A. RIBET, Multiplicities of Galois representations in Jacobians of Shimura curves (to appear).

[6] J.-P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, 15, 1972, pp. 259-331.

[7] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton 1971.

Department of Mathematics, University of California, Berkeley, CA 94720, *U.S.A.*;

N. B. : Current address: *Department of Mathematics, University of Illinois, Urbana IL* 61801, *U.S.A.*