This page intentionally left blank

Contemporary Mathematics
Volume 165, 1994

Formes Modulaires et Représentations Galoisiennes à valeurs dans un Anneau Local complet

par

Henri CARAYOL

Introduction.

Cet article est divisé en trois parties : l'objet de la première partie est d'étudier les représentations d'une algèbre à valeurs dans l'algèbre des matrices sur un anneau local A. Nous prouvons qu'il existe une bonne théorie pour celles de ces représentations qui se réduisent modulo l'idéal maximal en une représentation absolument irréductible : nous démontrons que de telles représentations sont déterminées à équivalence près par leur caractère. Dans une version antérieure de ce travail, j'utilisais pour démontrer cela un argument d'approximations successives qui nécessitait de supposer l'anneau A complet. C'est J.-P. Serre qui m'a expliqué comment se débarasser de cette hypothèse, ainsi que de quelques autres parasites. Nous prouvons ensuite que, si l'anneau A est hensélien, les représentations étudiées vérifient des propriétés de type de Schur : il s'agit là d'une généralisation de propriétés déjà établies par Mazur [Ma 2] sous des hypothèses plus particulières. Ici encore je dois à J.-P. Serre des améliorations substantielles par rapport à la première version de ce manuscrit.

Dans une seconde partie, nous expliquons comment les résultats de la première permettent d'attacher de façon univoque des représentations galoisiennes aux formes modulaires (normalisées, vecteurs propres des opérateurs de Hecke) à valeurs dans des anneaux locaux A complets. Faute de références bien précises sur les formes modulaires à coefficients dans des anneaux, nous avons commencé par rappeller des choses bien

1991 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F75.

0271-4132/94 $1.00 + $.25 per page

connues : leur définition du point de vue géométrique (que nous n'utilisons pas par la suite), puis du point de vue arithmétique : de ce dernier point de vue, une forme modulaire (normalisée, vecteur propre des opérateurs de Hecke) est un homomorphisme $\mathbb{T} \longrightarrow A$, où $\mathbb{T} = \mathbb{T}_{k,N}$ désigne l'algèbre de Hecke pour les formes de poids k et de niveau N. Si m est un idéal de $\mathbb{T}$, tel que la représentation résiduelle correspondante du groupe de Galois soit absolument irréductible, tout revient à construire une représentation "universelle" :

$$\rho_m^{\text{univ}} : G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{T}_m) ,$$

où $\mathbb{T}_m$ désigne le complété de $\mathbb{T}$ en m. Cette construction résulte de la construction classique des représentations l-adiques (Eichler - Shimura - Deligne - Serre) et des résultats du premier paragraphe.

Dans le dernier paragraphe enfin, nous considérons la cohomologie $\mathcal{H} = \mathcal{H}_{k,N}$ $(k \geq 2)$ des courbes modulaires $X_1(N)$ à valeurs dans les $\mathbb{Z}_l$-faisceaux habituels (par exemple $\underline{\mathbb{Z}}_l$ si $k = 2$). Si $m \subset \mathbb{T}$ est un idéal maximal de caractéristique résiduelle l, nous pouvons considérer le localisé $\mathcal{H}_m = \mathcal{H} \otimes_{\mathbb{T}} \mathbb{T}_m$. L'objet de la dernière partie est de comparer $\mathcal{H}_m$ et ρ_m^{univ} comme $\mathbb{T}_m[G_{\mathbb{Q}}]$-modules : on trouve une relation du type $\mathcal{H}_m \simeq \rho_m^{\text{univ}} \otimes_{\mathbb{T}_m} J$, avec J un idéal de $\mathbb{T}_m$. Finalement, nous donnons un critère pour que $\mathcal{H}_m \simeq \rho_m^{\text{univ}}$, et nous retrouvons un résultat récent de Boston-Lenstra-Ribet ([B-L-R]), à savoir la semi-simplicité du $G_{\mathbb{Q}}$-module $(\mathcal{H} \otimes \mathbb{F}_l)[m]$.

Je tiens à remercier Ch. Kassel, J.-L. Loday, et bien sûr J.-P. Serre, pour l'intérêt porté à ce travail, et pour leurs utiles suggestions ; de même que R. Livné, pour m'avoir signalé quelques erreurs dans la première version du manuscrit. Ma gratitude va également à l'Université de Caltech où j'ai pu effectuer ce travail (à l'invitation de D. Ramakrishnan). J'ai exposé ces résultats durant l'été 91 lors d'un congrès à Boston, dont je voudrais finalement remercier les organisateurs, B. Mazur et G. Stevens.

1. Représentations d'un groupe à valeurs dans un anneau local.

Dans ce qui suit, A désigne un anneau local de corps résiduel F.

1.1. Une généralisation partielle du théorème de Brauer-Nesbitt au cas d'un anneau local.

Soit R une A-algèbre. Une *représentation* de dimension n de R à valeurs dans A est un homomorphisme $\rho : R \to M_n(A)$ de A-algèbres. Deux telles représentations ρ et ρ' sont *équivalentes* s'il existe $M \in GL_n(A)$ tel que l'on ait $\rho'(r) = M\rho(r)M^{-1}$. Enfin la *représentation résiduelle* associée à ρ est la représentation $\bar{\rho} : R \otimes_A F \longrightarrow M_n(F)$ déduite de ρ par réduction modulo l'idéal maximal de A.

Le cas le plus important pour nos besoins futurs est celui où R est l'algèbre $A[G]$ d'un groupe G. Dans ce cas, la donnée d'une représentation de R correspond clairement à la donnée d'une représentation $G \longrightarrow GL_n(A)$ de G.

THÉORÈME 1. — *Soit A un anneau local, R une A-algèbre, et soient ρ et ρ' deux représentations de R de même dimension n. Faisons l'hypothèse que la représentation résiduelle $\overline{\rho}$ est absolument irréductible. Supposons que ρ et ρ' admettent la même trace : $\forall\ r \in R$, $tr\ \rho(r) = tr\ \rho'(r)$. Alors ρ et ρ' sont équivalentes.*

Remarques :

(i) Le même théorème vaut évidemment pour les représentations d'un groupe G (faire $R = A[G]$).

(ii) Sans hypothèse sur la représentation résiduelle, il ne semble pas y avoir de généralisation raisonnable du théorème de Brauer-Nesbitt : deux représentations peuvent admettre les mêmes polynômes caractéristiques sans avoir de suites de Jordan-Hölder à quotients isomorphes (où l'on entend ici par suite de Jordan-Hölder une extension successive par des A-modules *libres*). Par exemple, soit F un corps fini, et considérons le groupe abélien $G = M_2^0(F)$ constitué des matrices 2×2 de trace nulle à coefficients dans F. On définit deux représentations de G à valeurs dans les nombres duaux $A = F[\varepsilon]/(\varepsilon^2)$:

$$\rho(g) = \mathbf{1} \quad \text{et} \quad \rho'(g) = \mathbf{1} + \varepsilon g\ .$$

Ces deux représentations admettent la même trace et le même déterminant. Pourtant, aucune droite (A-module libre de rang 1 facteur direct dans A^2) n'est invariante sous ρ'.

Nous donnerons de ce théorème deux démonstrations : la première utilise un argument de déformations successives et nécessite donc de supposer l'anneau A complet. La seconde, qui m'a été ensuite communiquée par J.-P. Serre, vaut sans aucune hypothèse sur A.

1.1.1 Commençons par établir que les représentations résiduelles $\bar{\rho}$ et $\bar{\rho}'$ sont équivalentes (c'est, si l'on veut, le cas particulier du théorème 1 où $A = F$). Il suffit ([C-R](29.7)) de le prouver après extension des scalaires à une clôture algébrique, c'est-à-dire que l'on peut supposer F algébriquement clos. Le résultat est bien clair en caractéristique 0. En caractéristique $p > 0$, on utilise ([C-R](27.8)) l'indépendance linéaire des traces des différentes représentations irréductibles de $R \otimes_A F$: exprimant la semi-simplifiée $(\bar{\rho}')^{ss}$ comme une somme $\oplus n_i \pi_i$ de représentations irréductibles deux à deux distinctes π_i apparaissant avec des multiplicités n_i, l'égalité des traces entraîne que ρ figure dans $(\bar{\rho}')^{ss}$ avec une multiplicité $\equiv 1 \ mod.p$ et que les autres multiplicités sont $\equiv 0 \ mod.p$. Comme $\bar{\rho}$ et $\bar{\rho}'$ ont même dimension, il est alors clair qu'elles sont équivalentes.

1.1.2 Première démonstration (où l'anneau A est supposé séparé et complet).

Commençons par supposer qu'une certaine puissance de l'idéal maximal m s'anule, et raisonnons par récurrence sur l'entier λ tel que $m^\lambda \neq (0)$, $m^{\lambda+1} = (0)$. Dans le cas où $\lambda = 0$, notre théorème résulte de 1.1.1. ci-dessus. On peut donc supposer $\lambda \geq 1$, et le théorème déjà établi pour $\lambda - 1$, c'est-à-dire en particulier pour l'anneau $A' = A/m^\lambda$: nos deux représentations sont par suite équivalentes modulo m^λ, et donc coïncident modulo m^λ après conjugaison par un certain élément de $GL_n(A)$. Après cette conjugaison, on peut poser :

$$\rho'(r) = \rho(r) + \delta(r), \qquad \delta(r) \in M_n(m^\lambda) \ .$$

On voit aussitôt que δ se factorise en une application F-linéaire δ : $R \otimes_A F \longrightarrow M_n(m^\lambda)$ qui vérifie l'identité :

$$\delta(r_1 r_2) = \bar{\rho}(r_1)\delta(r_2) + \delta(r_1)\bar{\rho}(r_2) \ ;$$

autrement dit, δ est une *dérivation*. D'autre part, notre hypothèse d'égalité des traces signifie que la trace de δ est identiquement nulle.

Prenons $k \in Ker \ \bar{\rho}$ et $r \in R \otimes_A F$. On a

$$\delta(rk) = \bar{\rho}(r)\delta(k) \ ,$$

et la trace du produit $\bar{\rho}(r)\delta(k)$ est donc nulle. Or, d'après un théorème bien connu de Burnside ([C-R](27.4)), $\bar{\rho}$, étant absolument irréductible, est surjective. Par suite, on a pour tout $X \in M_n(F) : tr(X\delta(k)) = 0$, d'où $\delta(k) = 0$. Il en résulte que δ se factorise en une dérivation de $M_n(F)$ à valeurs dans $M_n(m^\lambda)$ (lequel n'est rien d'autre qu'une somme de copies de $M_n(F)$). On sait qu'une telle dérivation est nécessairement *intérieure* (résultat vrai plus généralement pour toute algèbre séparable : voir par exemple [K-O] III. 1.4); c'est-à-dire qu'il existe $U \in M_n(m^\lambda)$ tel que l'on ait :

$$\delta(r) = \bar{\rho}(r)U - U\bar{\rho}(r) .$$

Remplaçant alors δ par cette expression dans la formule qui le définit, on trouve finalement :

$$\rho'(r) = (1 - U)\rho(r)(1 + U) ,$$

et notre résultat est donc établi par récurrence. Pour un anneau séparé complet plus général, le raisonnement que l'on vient de faire nous fournit une suite convergente de $M_\lambda \in GL_n(A)$ tels que l'on ait : $\rho'(r) = M_\lambda \rho'(r) M_\lambda^{-1}$ $mod.m^\lambda$, et le théorème en résulte par passage à la limite.

1.1.3 Seconde démonstration.

Elle repose sur les deux faits suivants :

a) Si B est un anneau commutatif unitaire, tout idéal bilatère de la B-algèbre $\mathcal{M} = M_n(B)$ est de la forme $I\mathcal{M} = M_n(I)$ pour un idéal I de B.

b) Si de plus B est local, alors tout automorphisme de la B-algèbre $\mathcal{M}$ est intérieur, i.e. de la forme $X \longrightarrow gXg^{-1}$ pour un élément g de $GL_n(B)$.

Ces deux résultats sont démontrés (dans le cadre plus général des algèbres d'Azumaya) par exemple dans [K-O], III, Cor. 5.2 et IV, Cor. 1.3.

Soient ρ et ρ' comme dans l'énoncé du théorème, et notons Γ l'image de l'application $r \longrightarrow (\rho(r), \rho'(r))$ de R dans le produit $\mathcal{M} \times \mathcal{M}'$ de deux copies de $M_n(A)$. D'après le théorème de Burnside déjà utilisé dans la première démonstration, $\bar{\rho}$ est surjective. Faisant usage du lemme de Nakayama, on en déduit que ρ est surjective. De même, $\overline{\rho}'$ est surjective (car équivalente à $\overline{\rho}$), et par suite ρ' l'est également.

On voit donc que Γ est une sous-algèbre de $\mathcal{M} \times \mathcal{M}'$ telle que sa projection sur chacun des facteurs soit surjective. Posant $J = \Gamma \cap (\mathcal{M} \times$

$\{0\})$, $J' = \Gamma \cap (\{0\} \times \mathcal{M}')$, on en déduit que J (resp. J') est un idéal bilatère de $\mathcal{M}$ (resp. $\mathcal{M}'$); il est immédiat alors de vérifier que la projection de Γ sur $(\mathcal{M}/J) \times (\mathcal{M}'/J')$ est le graphe d'un isomorphisme d'algèbres $\iota : \mathcal{M}/J \xrightarrow{\sim} \mathcal{M}'/J'$. De plus, Γ s'identifie à l'ensemble des couples $(x, x') \in \mathcal{M} \times \mathcal{M}'$ tels que les images de x et x' dans $\mathcal{M}/J$ et $\mathcal{M}'/J'$ se correspondent via ι.

Appliquons maintenant le résultat (a) rappellé ci-dessus. Il existe des idéaux I et I' de A tels que $J = I\mathcal{M}$ et $J' = I'\mathcal{M}'$. Mais I (resp. I') coïncide alors avec l'annulateur du A-module $\mathcal{M}/J$ (resp. $\mathcal{M}'/J'$) et l'existence de l'isomorphisme ι entraîne alors que $I = I'$.

Pour $I = A$, on aurait $\Gamma = \mathcal{M} \times \mathcal{M}'$. Pour $I \neq A$, on peut voir ι comme un automorphisme de l'algèbre $M_n(A/I)$: il est intérieur d'après (b) et provient donc d'un élément g de $GL_n(A/I)$, que l'on peut relever en un élément, noté encore g, de $GL_n(A)$. On a ainsi obtenu dans tous les cas la description suivante de Γ : Γ *est l'ensemble des couples* $(x, x') \in \mathcal{M} \times \mathcal{M}'$ *qui vérifient* $x' \equiv gxg^{-1} mod.I$.

Nous n'avons pas encore à ce stade fait usage de l'hypothèse principale du théorème, à savoir l'égalité des traces de ρ et ρ' : c'est-à-dire que $tr(x) = tr(x')$ pour tout $(x, x') \in \Gamma$. Utilisons maintenant cette hypothèse pour prouver que $I = (0)$. Soit $i \in I$, et prenons pour x la matrice diagonale ayant i comme première composante, les autres étant nulles; prenons d'autre part $x' = 0$. La description de Γ donnée ci-dessus nous dit que $(x, x') \in \Gamma$, et l'égalité des traces signifie que $i = 0$. D'où $I = (0)$. Donc Γ est l'ensemble des couples (x, x') tels que $x' = gxg^{-1}$. Cela revient à dire que g conjugue ρ en ρ', et le théorème est donc démontré.

1.2. Un résultat "à la Schur".

Soit A un anneau local *henselien* d'idéal maximal m tel que le *groupe de Brauer* du corps résiduel $F = A/m$ soit *nul* (par exemple, F peut-être fini). Soit d'autre part $A' \supset A$ une *extension semi-locale* de A : c'est donc un produit fini $A' = \prod A'_i$ d'anneaux locaux A'_i, d'idéaux maximaux m'_i et de corps résiduels $F'_i \supset F$.

Donnons nous une A-algèbre R, et une représentation ρ' à valeurs dans A' :

$$\rho' = \prod \rho'_i : \ R \otimes_A A' \longrightarrow M_n(A') = \prod M_n(A'_i) \ .$$

Nous faisons l'hypothèse que *pour tout* $r \in R$ *la trace de* $\rho'(r \otimes 1)$ (à priori un élément de A') *appartient au sous-anneau* $A \subset A'$. En particulier,

les différentes représentations résiduelles :

$$\overline{\rho}'_i : R \otimes_A F'_i \longrightarrow M_n(F'_i)$$

sont telles que la trace de $\overline{\rho}'_i(r \otimes 1)$ est un élément de F indépendant de i. Notre dernière hypothèse est que l'*une de ces représentations résiduelles est absolument irréductible* (et donc toutes le sont).

THÉORÈME 2. — *Si les hypothèses ci-dessus sont satisfaites, alors ρ' est équivalente à la représentation obtenue, par extension des scalaires de A à A', à partir d'une représentation :*

$$\rho : R \longrightarrow M_n(A) \ .$$

Cette dernière est bien déterminée à équivalence près.

Remarque : Ce théorème s'applique de façon évidente aux représentations d'un groupe G (faire $R = A[G]$).

Preuve : L'unicité de ρ résulte aussitôt du th. 1. Tout revient donc à en prouver l'existence : une forme faible de ce résultat avait été obtenue par Mazur ([Ma 2], 1.8), dans son travail sur les déformations. Dans une première version de cet article, je m'étais placé dans le cadre des représentations continues d'un groupe profini à valeurs dans un anneau complet, et je m'étais servi de la théorie de Mazur. C'est de nouveau J.-P. Serre qui m'a indiqué comment éliminer ces hypothèses superflues. Par souci de généralité, c'est la méthode de Serre que je vais suivre ici.

Considérons l'algèbre de matrices $S' = M_n(A') = \prod M_n(A'_i)$ et soit $S \subset S'$ la sous-A-algèbre de S' constituée des $\rho(r \otimes 1)$: la trace de tout élément $s \in S$ est donc, en vertu de nos hypothèses, un élément de l'anneau A.

Utilisons le fait que les représentations résiduelles $\overline{\rho}'_i$ sont absolument irréductibles, et (ayant la même trace) équivalentes entre elles (après extension des scalaires à un sur-corps commun). D'autre part elles sont surjectives, en vertu du théorème de Burnside déjà utilisé dans la preuve du théorème 1. On en déduit qu'il existe une suite $r_1, \ldots, r_{n^2}$ d'éléments de R, telle que, pour tout i, les $\overline{\rho}_i(r_k \otimes 1)$ constituent une base du F_i-espace vectoriel $M_n(F_i)$. Notant $e_k = \rho'(r_k \otimes 1) \in S$, on voit donc en appliquant le lemme de Nakayama que, pour tout i, les projections des e_k sur $S'_i = M_n(A'_i)$ (c'est-à-dire les $\rho'_i(r_k \otimes 1)$) constituent un système

générateur du A_i'-module S_i' (lequel est libre de rang n^2) : ces projections constituent donc une *base*.

On a donc un système $e_1, \ldots, e_{n^2}$ d'éléments de S qui constituent une base du A'-module S'. Prouvons que c'est aussi une *base du* A-module S :

Soit $s \in S$; il s'écrit $s = \Sigma \alpha_k e_k$, avec des α_k à priori dans A' : il nous faut montrer qu'ils appartiennent à A. Pour cela, multiplions par e_l la relation ci-dessus et prenons la trace. On obtient :

$$(*) \qquad \sum_k \alpha_k tr(e_k e_l) = tr(x e_l) \in A \ .$$

Or il est bien connu et facile de vérifier que, pour toute base (e_k) d'une algèbre de matrices, le déterminant de la matrice $tr(e_k e_l)$ est inversible. Ici, les $tr(e_k e_l)$ sont éléments de A, et le déterminant obtenu est inversible dans A (car il l'est dans A'). On voit donc que les relations $(*)$ ci-dessus constituent un *système de Cramer* en les α_k : d'où on déduit qu'ils appartiennent à A. Les (e_k) constituent donc bien une base de S sur A.

Notre algèbre S est donc un A-module libre de rang n^2, et $S \otimes_A A'$ s'identifie à S'. On en déduit en particulier un isomorphisme :

$$(S \otimes_A F) \otimes_F F_i' \simeq S' \otimes_{A_i'} F_i' = M_n(F_i') \ ,$$

et donc l'algèbre $S \otimes_A F$ est centrale simple sur F : par suite, S *est donc une* A*-algèbre d'Azumaya.*

Mais un théorème d'Azumaya ([Az]) affirme que, pour un anneau hensélien, le morphisme de spécialisation du groupe de Brauer $Br(A) \longrightarrow Br(F)$ est un isomorphisme. En vertu de notre hypothèse sur F, $Br(A)$ est donc nul, et par suite S est isomorphe à $M_n(A)$. Si $\varphi : S \xrightarrow{\sim} M_n(A)$ est un tel isomorphisme, on pose pour $r \in R$:

$$\rho(r) = \varphi(\rho'(r \otimes 1)) \ .$$

La représentation ρ ainsi obtenue donne bien par extension des scalaires une représentation équivalente à ρ', car le composé $M_n(A') = S' = S \otimes_A A' \xrightarrow{\varphi \otimes_A A'} M_n(A')$ est d'après (1.1.3.b) un automorphisme intérieur de $M_n(A')$. La preuve de notre théorème est ainsi achevée.

2. Formes modulaires à valeurs dans un anneau local complet et représentations galoisiennes associées.

2.1 Formes modulaires.

Soient $k \geq 1$ et $N \geq 1$ deux entiers; soit d'autre part A un anneau commutatif et unitaire. On dispose de deux définitions possibles de ce que doit être une "forme modulaire de poids k et de niveau N à coefficients dans A" : l'une géométrique, due à Katz, s'exprime en termes du champ classifiant les courbes elliptiques; ellle a un sens pour N inversible dans A. L'autre définition, arithmétique, utilise l'algèbre de Hecke $\mathbb{T}_{k,N}$: pour $A = \overline{\mathbb{F}_l}$, elle revient essentiellement à réduire les formes modulaires depuis la caractéristique 0. Lorsque $k \geq 2$, sauf pour des petites valeurs de N et des caractéristiques résiduelles de A, les formes de Katz se relèvent en caractéristique 0; il en résulte alors que les deux définitions coïncident. Dans la suite, nous n'utiliserons que la définition arithmétique; il nous a semblé utile toutefois de rappeller également la définition géométrique.

2.1.1. La définition géométrique (cf [Gr], [Ka]).

On suppose ici N inversible dans A. Du point de vue de Katz, une forme modulaire à coefficients dans A est une "régle" qui associe à tout couple (E, α) constitué d'une courbe elliptique généralisée E sur un A-schéma S et d'une injection $\alpha : \mu_N \hookrightarrow E_N$ (dont l'image rencontre chaque composante de chaque fibre de E), une section $f(E, \alpha)$ sur S du faisceau $\omega_E^{\otimes k}$: ici, ω_E est le faisceau dual de Lie(E); on impose que f soit compatible au changement de base.

L'ensemble, noté $M_{k,N}(A)$, des tels objets est de façon évidente un A-module. Tout élément $f \in M_{k,N}(A)$ admet un "développement de Fourier" $f(q) \in A[[q]]$ que l'on définit, évaluant f sur la courbe de Tate $G_m/q^{\mathbb{Z}}$ munie du plongement naturel $\mu_N \overset{Id_N}{\hookrightarrow} E_N$, par la formule :

$$f(G_m/q^{\mathbb{Z}}, Id_N) = f(q)\Big(\frac{dt}{t}\Big)^{\otimes k}$$

où $\dfrac{dt}{t}$ est la différentielle canonique de la courbe de Tate.

C'est un résultat bien connu ("q-expansion principle") que l'application $M_{k,N}(A) \longrightarrow A[[q]]$ qui à f associe son développement de Fourier est *injective*. De plus, f provient d'une forme définie sur un sous-anneau $A_0 \subset A$ si et seulement si $f(q) \in A_0[[q]]$.

On dit que f est *parabolique* si elle s'annule aux pointes, c'est à dire sur les courbes elliptiques dégénérées. L'ensemble des formes paraboliques constitue un sous-module $S_{k,N}(A)$ de $M_{k,N}(A)$.

Pour $N > 4$, les couples (E, α) considérés ci-dessus sont classifiés par une courbe algébrique $X_1(N)$ propre et lisse sur $\mathbb{Z}[1/N]$ et munie d'un faisceau ω. On a alors :

$$\begin{aligned} M_{k,N}(A) &= H^0(X_1(N) \bigotimes A,\ \omega^{\otimes k}) , \\ S_{k,N}(A) &= H^0(X_1(N) \bigotimes A,\ \omega^{\otimes k}(-D_\infty)) , \end{aligned}$$

où D_∞ est le diviseur effectif constitué des différentes pointes.

2.1.2. Relèvement en caractéristique 0 (voir toujours [Gr],[Ka]).

PROPOSITION. — *Supposons d'une part $k \geq 2$, et d'autre part que $N > 4$, ou que 6 est inversible dans A. Alors les formes modulaires (resp. les formes modulaires paraboliques) à coefficients dans A se relèvent en caractéristique 0 ; c'est à dire que l'on a :*

$$\begin{aligned} M_{k,N}(A) &= M_{k,N}(\mathbb{Z}[1/N]) \bigotimes A , \\ S_{k,N}(A) &= S_{k,N}(\mathbb{Z}[1/N]) \bigotimes A . \end{aligned}$$

Ebauche de preuve (d'après [Ka] 1.7). Supposons d'abord $N > 4$. L'obstruction à relever à $\mathbb{Z}/l^{n+1}\mathbb{Z}$ une forme à coefficients dans $\mathbb{Z}/l^n\mathbb{Z}$ est un élément de $H^1(X_1(N)_{\mathbb{F}_l}, \omega^k)$, et ce groupe de cohomologie est nul car dual de $H^0(X_1(N)_{\mathbb{F}_l}, \Omega^1\omega^{-k})$. Pour les formes paraboliques, on trouve une obstruction dans le groupe $H^1(X_1(N)_{\mathbb{F}_l}, \omega^k(-D_\infty))$, dual de $H^0(X_1(N)_{\mathbb{F}_l}, \Omega^1\omega^{-k}(D_\infty))$. Ce groupe est nul pour $k > 2$ (rappelons l'isomorphisme $\Omega^1 \simeq \omega^2(-D_\infty)$). Pour $k = 2$, les formes paraboliques s'interprètent comme des formes différentielles régulières sur $X_1(N)$. Si l'on introduit un point P de $X_1(N)$, défini sur $\mathbb{Z}_l$, arbitraire (par exemple une pointe), on peut relever une telle forme différentielle en une forme méromorphe admettant au plus un pôle simple en P (en effet, $H^1(X_1(N)_{\mathbb{F}_l}, \Omega^1(P)) = 0$). Le théorème des résidus entraîne alors que le relèvement obtenu est en fait holomorphe.

Dans le cas où $N \leq 4$ et où 6 est inversible dans A, il existe un problème de modules (on peut par exemple ajouter une "$\Gamma(3)$-structure") représentable par un $\mathbb{Z}[1/6N]$-schéma $\widetilde{X}$, tel que $X_1(N)$ apparaisse comme le quotient de $\widetilde{X}$ par un groupe Γ dont l'ordre n'est divisible que par les nombres premiers 2 et 3 (dans l'exemple ci-dessus $\Gamma = GL_2(\mathbb{Z}/3\mathbb{Z})$, de cardinal 48). L'argument précédent s'applique à $\widetilde{X}$ et prouve que l'on peut relever les sections sur $\widetilde{X}$ de ω^k et $\omega^k(-D_\infty)$. Comme l'ordre de Γ est inversible dans A, on peut aussi relever les sections Γ-invariantes en des sections Γ-invariantes, ce qui prouve le résultat cherché.

La proposition précédente ramène en un certain sens la connaissance de $M_{k,N}(A)$ (resp. $S_{k,N}(A)$) à celle de $M_{k,N}(\mathbf{Z}[1/N])$ (resp. $S_{k,N}(\mathbf{Z}[1/N])$); d'autre part, en vertu du "q-expansion principle" rappellé plus haut, $M_{k,N}(\mathbf{Z}[1/N])$ (resp. $S_{k,N}(\mathbf{Z}[1/N])$) s'identifie à l'ensemble des formes modulaires (resp. paraboliques) au sens classique, dont tous les coefficients de Fourier sont dans $\mathbf{Z}[1/N]$. On peut aussi introduire les ensembles de formes modulaires, notés $S_{k,N}(\mathbf{Z})$ (resp. $M_{k,N}(\mathbf{Z})$), caractérisés par la propriété que tous leurs coefficients de Fourier sont entiers. Il est clair que l'on a : $S_{k,N}(\mathbf{Z}[1/N]) = S_{k,N}(\mathbf{Z}) \otimes \mathbf{Z}[1/N]$ et l'égalité analogue pour les $M_{k,N}$; de sorte que les égalités de la proposition ci-dessus restent également valides lorsqu'on remplace $S_{k,N}(\mathbf{Z}[1/N])$ (resp. $M_{k,N}(\mathbf{Z}[1/N])$ par $S_{k,n}(\mathbf{Z})$ (resp. $M_{k,N}(\mathbf{Z})$).

Nous allons maintenant donner une interprétation duale, en termes de l'algèbre de Hecke, de ces modules de formes modulaires. Afin de ne pas alourdir inutilement, nous nous bornerons désormais à considérer seulement les formes paraboliques.

2.1.3. Algèbres de Hecke. — L'espace $S_{k,N}(\mathbf{C})$ est muni des opérateurs de Hecke T_p (pour chaque nombre premier p) et diamant $< a >$ pour $a \in (\mathbf{Z}/N\mathbf{Z})^*$. Rappellons en termes modulaires (2.1.1) leur définition :

$$\begin{aligned} (f \mid < a >)(E, \alpha) &= f(E, a\alpha) \\ (f \mid T_p)(E, \alpha) &= \tfrac{1}{p} \sum \varphi^*(f(\varphi E, \varphi\alpha)) \ , \end{aligned}$$

où la somme est prise sur les isogénies $E \xrightarrow{\varphi} \varphi E$ de degré p telles que (dans le cas où $p|N$) leur noyau intersecte trivialement $Im(\alpha)$.

Ces différents opérateurs commutent entre eux et engendrent un anneau (commutatif, unitaire) de type fini sur $\mathbf{Z}$. Cet anneau est *l'algèbre de Hecke*, qu'on note $\mathbb{T}_{k,N}$ (voire $\mathbb{T}_N$ ou même $\mathbb{T}$ lorsque k, ou k et N, sont fixés). Les formules classiques qui expriment les T_n ($n \in \mathbf{N}$) en termes des T_p et $< a >$ montrent d'ailleurs que $\mathbb{T}$ est également l'algèbre engendrée par les $(T_n)_{n \in \mathbf{N}}$.

L'action de $\mathbb{T}_{k,N}$ sur $S_{k,N}(\mathbf{C})$ respecte $S_{k,N}(\mathbf{Z})$: c'est clair pour les opérateurs diamant, et on le vérifie pour les T_p en utilisant par exemple les formules qui décrivent leur action sur le développement de Fourier. Cela permet de définir un accouplement :

$$\begin{aligned} \mathbb{T}_{k,N} \times S_{k,N}(\mathbf{Z}) &\longrightarrow \mathbf{Z} \\ (T, f) &\longrightarrow < T, f > \end{aligned}$$

par la formule $< T, f >= a_1(f|T)$ (premier coefficient de Fourier de $(f|T)$). On vérifie en particulier que $< T_n, f >$ est égal au n-ième coefficient de Fourier de f. On a alors la :

PROPOSITION ([Ri 1] 2.2). — *L'accouplement ci-dessus définit une dualité parfaite entre les deux $\mathbb{Z}$-modules $\mathbb{T}_{k,N}$ et $S_{k,N}(\mathbb{Z})$.*

2.1.4. La définition arithmétique des formes modulaires.

Supposons tout d'abord que l'on est sous les hypothèses de la proposition de (2.1.2), c'est à dire que $k \geq 2$, et que $N > 4$ ou que 6 est inversible dans A. Supposons aussi que N est inversible dans A. Combinant les résultats rappellés en (2.1.2) et (2.1.3), on voit que $S_{k,N}(A) = S_{k,N}(\mathbb{Z}) \otimes A$ est de façon naturelle isomorphe au module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{k,N}, A)$ des homomorphismes de $\mathbb{Z}$-modules de $\mathbb{T}_{k,N}$ dans A : à une forme f correspond un homomorphisme $\lambda_f : \mathbb{T}_{k,N} \longrightarrow A$, tel que l'on ait en particulier $\lambda_f(T_n) = a_n(f)$ (n-ième coefficient de Fourier de f).

La définition arithmétique des formes modulaires consiste à considérer à priori $S_{k,N}(\mathbb{Z}) \otimes A$, ou plutôt (dualement) l'ensemble des homomorphismes $\lambda : \mathbb{T} \to A$. Pour $k = 1$, ou bien pour $N \leq 4$ et 6 non inversible dans A, il peut y avoir davantage de formes modulaires "géométriques" qu'"arithmétiques" : toutes celles qui ne se relèvent pas en caractéristique 0. Noter enfin que la définition arithmétique a encore un sens même si N n'est pas inversible dans A.

L'algèbre de Hecke opère sur $S_{k,N}(\mathbb{Z}) \otimes A$: si f correspond à $\lambda_f : \mathbb{T}_{k,N} \to A$, et si $T_0 \in \mathbb{T}_{k,N}$, la transformée $g = (f|T_0)$ correspond à λ_g défini par : $\lambda_g(T) = \lambda_f(TT_0)$. Il est clair que f est "normalisée" (de premier coefficient de Fourier égal à 1) si et seulement si $\lambda_f(1) = 1$, et on voit que f est alors "vecteur propre des opérateurs de Hecke" si et seulement si λ_f vérifie l'identité $\lambda_f(TT_0) = \lambda_f(T)\lambda_f(T_0)$, i.e. si λ_f est un homomorphisme d'anneaux. La "valeur propre" correspondant à T_0 est alors $\lambda_f(T_0)$.

Dans la suite, nous considérerons toujours de telles formes, définies arithmétiquement, normalisées et vecteurs propres des opérateurs de Hecke, correspondant donc à des homomorphismes d'anneaux $\lambda_f : \mathbb{T} = \mathbb{T}_{k,N} \to A$. Pour nous, A sera toujours un anneau local complet de caractéristique résiduelle l. Se donner λ_f revient alors à se donner $\lambda_f \otimes \mathbb{Z}_l : \mathbb{T} \otimes \mathbb{Z}_l \to A$; l'anneau $\mathbb{T} \otimes \mathbb{Z}_l$ est semi-local complet, produit d'un nombre fini de complétés $\mathbb{T}_{m_i}$ aux différents idéaux maximaux de $\mathbb{T}$ tels que le quotient $\mathbb{T}/m_i$ soit de caractéristique l. Chacun des $\mathbb{T}_{m_i}$ est une

extension finie de $\mathbf{Z}_l$.

2.2. Représentations galoisiennes.

Soit A un anneau local complet, de corps résiduel F de caractéristique l (en pratique, F sera fini, mais il n'y a pas de raison de l'imposer). Soit f une forme modulaire normalisée vecteur propre des opérateurs de Hecke, définie arithmétiquement par un homomorphisme d'anneaux :

$$\lambda_f : T = T_{k,N} \longrightarrow A$$

(on suppose ici fixés, afin d'alléger la notation, le poids k et le niveau N).

On considérera également la *forme résiduelle* $\bar{f}$ à coefficients dans F, correspondant à l'homomorphisme :

$$\lambda_{\bar{f}} = \bar{\lambda}_f : \mathbb{T} \longrightarrow F$$

déduit de λ_f par réduction modulo l'idéal maximal de A. Cette forme résiduelle est en fait à coefficients dans un sous-corps fini $\mathbb{F} \subset F$. Il est bien connu (voir par exemple [D-S] §6) qu'on peut lui associer une représentation résiduelle du groupe Galois $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\rho_{\bar{f}} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}) \subset GL_2(F) \ .$$

Cette représentation (continue) est non ramifiée en les nombres premiers $p \not| Nl$, et vérifie les relations usuelles :

$$\begin{cases} tr\rho_{\bar{f}}(Frob_p) & = \lambda_{\bar{f}}(T_p) \ , \\ det\rho_{\bar{f}}(Frob_p) & = \lambda_{\bar{f}}(< p >)p^{k-1} \ , \end{cases}$$

où $Frob_p$ désigne un élément de Frobenius ("géométrique", pour fixer les normalisations) en p.

En vertu des théorèmes de Brauer-Nesbitt et de Čebotarev, ces relations déterminent de façon unique la semi-simplifiée de $\rho_{\bar{f}}$, et donc $\rho_{\bar{f}}$ elle-même si on la suppose irréductible, ce que nous allons faire dans la suite.

THÉORÈME 3. — *Soit f comme ci-dessus, telle que la représentation résiduelle associée $\rho_{\bar{f}}$ soit absolument irréductible. Il existe alors une représentation continue à valeurs dans A :*

$$\rho_f : G_{\mathbb{Q}} \longrightarrow GL_2(A) \ ,$$

qui est non ramifiée en dehors de Nl, et qui vérifie les relations :

$$(*) \qquad \text{pour } p \not| Nl : \begin{cases} tr\rho_f(Frob_p) & = \lambda_f(T_p) \ , \\ det\rho_f(Frob_p) & = \lambda_f(< p >)p^{k-1} \ . \end{cases}$$

Cette représentation est unique à équivalence près.

Preuve : L'unicité résulte du théorème 1 et du théorème de Čebotarev (noter que la réduction $\bar{\rho}_f$ de ρ_f est équivalente à $\rho_{\bar{f}}$). Pour l'existence, notons $m = Ker\bar{\lambda}_f$ l'idéal maximal de $\mathbb{T}$ où notre forme est localisée. L'homomorphisme λ_f se factorise à travers le complété $\mathbb{T}_m$:

$$\lambda_f : \mathbb{T} \xrightarrow{\lambda_{f_m^{\text{univ}}}} \mathbb{T}_m \xrightarrow{\mu_f} A \ ,$$

où $\lambda_{f_m^{\text{univ}}}$ est une notation compliquée pour désigner simplement l'homomorphisme canonique de $\mathbb{T}$ vers son complété $\mathbb{T}_m$; cette notation met en évidence que cet homomorphisme est associé à une forme modulaire "universelle" (tautologique, si on ne regarde que le point de vue arithmétique) à coefficients dans $\mathbb{T}_m$. Il est clair que tout revient alors à construire la représentation galoisienne associée à f_m^{univ}, soit : $\rho_m^{\text{univ}} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{T}_m)$.

On sait que l'algèbre de Hecke $\mathbb{T}$, et donc aussi $\mathbb{T}_m$, peut avoir des éléments nilpotents non nuls, lesquels proviennent des "mauvais" opérateurs de Hecke $T_p(p|N)$. Notons $\mathbb{T}'$ le sous-anneau de $\mathbb{T}$ engendré par les "bons" opérateurs $T_p(p \not| N)$, et $\mathbb{T}'_m$ l'adhérence dans $\mathbb{T}_m$ de l'image de $\mathbb{T}'$. Alors, ni $\mathbb{T}'$ ni $\mathbb{T}'_m$ ne contiennent d'éléments nilpotents non nuls ; en fait $\mathbb{T}'$ (resp. $\mathbb{T}'_m$) se plonge dans un produit de corps de nombres (resp. de corps l-adiques) : cela résulte du fait que les bons opérateurs de Hecke se diagonalisent simultanément ; en particulier, le normalisé $\widehat{\mathbb{T}}'_m \supset \mathbb{T}'_m$ de $\mathbb{T}'_m$ est le produit d'un nombre fini d'anneaux d'entiers O_i de corps l-adiques E_i.

Le morphisme composé $\mathbb{T}' \longrightarrow \mathbb{T}'_m \longrightarrow \widehat{\mathbb{T}}'_m \longrightarrow E_i$ se relève à l'extension finie $\mathbb{T} \supset \mathbb{T}'$, quitte à peut-être étendre E_i en une extension finie E'_i, d'où une forme modulaire (normalisée, vecteur propre des opérateurs de Hecke) à coefficients dans E'_i ; à cette dernière la théorie d'Eichler-Shimura-Deligne-Serre associe une représentation galoisienne ρ'_i, à valeurs dans E'_i, vérifiant les relations $(*)$ ci-dessus. Cette représentation galoisienne peut être réalisée sur E_i (les relations $(*)$ montrent que la trace de ρ'_i est à valeurs dans E_i, et il est bien connu et facile de vérifier que les représentations galoisiennes impaires sont non obstruées, i.e. réalisables sur le corps

de définition de leur caractère). Choisissant un réseau invariant, on peut même supposer que l'image de ρ'_i est contenue dans $GL_2(\mathcal{O}_i)$. Le produit ρ' des ρ'_i est alors une représentation :

$$\rho' : G_{\mathbb{Q}} \longrightarrow GL_2(\widehat{\mathbb{T}}'_m) .$$

Les relations $(*)$ et le théorème de Čebotarev montrent que la trace et le déterminant de ρ' sont à valeurs dans $\mathbb{T}'_m$. On peut alors appliquer le théorème 2 : on en déduit que ρ' provient d'une représentation :

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{T}'_m) .$$

La représentation ρ_m^{univ} cherchée en résulte, par composition avec l'inclusion de $GL_2(\mathbb{T}'_m)$ dans $GL_2(\mathbb{T}_m)$.

3. La cohomologie entière l-adique des courbes modulaires.

3.1. Les faisceaux $\mathcal{F}_k$ et leur cohomologie.

3.1.1. Fixons désormais un niveau $N > 4$ et un poids $k \geq 2$. Soit $Y_1(N)$ l'ouvert de la courbe modulaire $X_1(N)$ complémentaire des pointes. Cet ouvert est la base d'une courbe elliptique universelle $\mathcal{E} \xrightarrow{\pi} Y_1(N)$. On en déduit un $\mathbb{Z}_l$-faisceau lisse de rang 2 sur $Y_1(N) \otimes \mathbb{Z}[1/Nl]$: $\mathcal{F}_3 \overset{\text{def}}{=} R^1\pi_*(\mathbb{Z}_l)$. Nous notons $\mathcal{F}_k$ la puissance symétrique $(k-2)$-ième de $\mathcal{F}_3$: en particulier $\mathcal{F}_2$ est le faisceau constant $\underline{\mathbb{Z}}_l$; le rang de $\mathcal{F}_k$ est $(k-1)$.

Nous allons nous intéresser dans ce qui suit au groupe de cohomologie parabolique :

$$H^1_p(Y_1(N) \otimes \overline{\mathbb{Q}},\ \mathcal{F}_k) = H^1(X_1(N) \otimes \overline{\mathbb{Q}},\ j_*\mathcal{F}_k) ,$$

où j désigne l'inclusion de $Y_1(N)$ dans $X_1(N)$; si on préfère, ce groupe est l'image de la cohomologie à support propre dans la cohomologie . Nous notons $\mathcal{H} = \mathcal{H}_{k,N}$ ce groupe de cohomologie parabolique quotienté par son éventuelle torsion ; ce dernier point est d'ailleurs sans importance, dans la mesure où nous allons localiser par la suite $\mathcal{H}$ en un idéal de l'algèbre de Hecke correspondant à une représentation résiduelle irréductible de Galois, tandis que ce groupe de Galois opère sur la torsion, liée au H^0, par son quotient abélien : la torsion disparaîtrait donc de toute façon par localisation.

Un argument analogue s'appliquerait aussi à la "différence" entre cohomologie à support propre et cohomologie : comme cette différence

provient des séries d'Eisenstein, elle disparaît par notre localisation. De sorte que ce que nous allons démontrer pour la cohomologie parabolique serait aussi valide pour la cohomologie elle-même, ou la cohomologie à support propre, en prenant garde toutefois d'utiliser alors l'algèbre de Hecke engendrée par l'action des opérateurs T_p et $< a >$ sur l'espace de toutes les formes modulaires, non nécessairement paraboliques : celle que nous utilisons ici en est le quotient qui correspond aux formes paraboliques.

3.1.2. Opérateurs de Hecke.

On sait définir l'action des opérateurs de Hecke sur la cohomologie à partir de correspondances sur les couples $(Y_1(N), \mathcal{F}_k)$: cf. [De], [Hi], [Sh]. Rappellons comment sont définies ces correspondances sur $Y_1(N) \otimes \mathbb{Q}$: fixons un nombre premier p, et considérons le foncteur qui associe à chaque $\mathbb{Q}$-schéma S l'ensemble des classes d'isomorphie de diagrammes commutatifs de S-schémas :

(*)

$$\begin{array}{ccc} & \mu_N & \\ \swarrow^{\alpha_1} & & \searrow^{\alpha_2} \\ E_{1,N} & \longrightarrow & E_{2,N} \\ \downarrow & & \downarrow \\ E_1 & \xrightarrow{\varphi} & E_2 \end{array}$$

où φ est une p-isogénie entre les deux courbes elliptiques E_1 et E_2, et α_i un homomorphisme de μ_N dans la N-torsion de E_i. Noter qu'il résulte de la commutativité du diagramme et de l'injectivité de α_2 que : $\mathrm{Im}\ \alpha_1 \cap \mathrm{Ker}\ \varphi = (0)$.

On vérifie sans peine que le foncteur précédent est représentable par un $\mathbb{Q}$-schéma $Y_1(N,p)_{\mathbb{Q}}$; d'où une correspondance sur $Y_1(N)_{\mathbb{Q}}$:

$$\begin{array}{ccc} & Y_1(N,p)_{\mathbb{Q}} & \\ \swarrow^{q_1} & & \searrow^{q_2} \\ Y_1(N)_{\mathbb{Q}} & & Y_1(N)_{\mathbb{Q}} \end{array}$$

où q_i est le morphisme qui associe à un diagramme $(*)$ comme ci-dessus le couple (E_i, α_i) : c'est un revêtement fini étale. De plus, on dispose

sur $Y_1(N,p)_{\mathbb{Q}}$ d'un diagramme $(*)$ universel, avec des isomorphismes $E_i \simeq q_i^*\mathcal{E}$, où $\mathcal{E}$ désigne toujours la courbe elliptique universelle sur $Y_1(N)$. On obtient ainsi une p-isogénie $\varphi : q_1^*\mathcal{E} \to q_2^*\mathcal{E}$, d'où un morphisme de faisceaux $\mathrm{Sym}^{k-2}(\varphi^*) : q_2^*\mathcal{F}_k \to q_1^*\mathcal{F}_k$. Finalement, on peut définir l'action de l'opérateur de Hecke T_p sur $H_p^1(Y_1(N)_{\overline{\mathbb{Q}}}, \mathcal{F}_k)$, et donc sur $\mathcal{H}$, comme le composé :

$$H_p^1(Y_1(N)_{\overline{\mathbb{Q}}}, \mathcal{F}_k) \xrightarrow{q_2^*} H_p^1(Y_1(N,p)_{\overline{\mathbb{Q}}}, q_2^*\mathcal{F}_k) \xrightarrow{\mathrm{Sym}^{k-2}(\varphi^*)} H_p^1(Y_1(N,p)_{\overline{\mathbb{Q}}}, q_1^*\mathcal{F}_k) \xrightarrow{q_{2*}} H_p^1(Y_1(N)_{\overline{\mathbb{Q}}}, \mathcal{F}_k) .$$

L'action des opérateurs diamant $< a >$ est plus évidente, car ils induisent des automorphismes de $(Y_1(N)_{\mathbb{Q}}, \mathcal{F}_k)$. Il est bien connu que ces actions définissent au bout du compte une action sur $\mathcal{H}$ de l'algèbre de Hecke $\mathbb{T} = \mathbb{T}_{k,N}$ (voir pour s'en convaincre, au paragraphe suivant, *l'isomorphisme de Shimura).*

3.1.3. Pour chaque idéal maximal m de $\mathbb{T}$, tel que $\mathbb{T}/m$ soit de caractéristique l, on notera $\mathcal{H}_m$ la composante correspondante de $\mathcal{H}$, image de l'idempotent associé à la composante $\mathbb{T}_m$ de $\mathbb{T} \otimes \mathbb{Z}_l$.

Le groupe de Galois $G_{\mathbb{Q}}$ opère sur $\mathcal{H}$ (une action compatible avec la structure de $\mathbb{T}$-module), et donc sur les $\mathcal{H}_m$, qui apparaissent ainsi comme des $\mathbb{T}_m[G_{\mathbb{Q}}]$-modules.

Dans la suite, nous allons nous intéresser surtout aux idéaux maximaux m tels que la *représentation résiduelle* $\overline{\rho}_m$, associée à la forme résiduelle $\mathbb{T} \to \mathbb{T}/m$ (cf. 2.2.), soit *absolument irréductible.* Notre but est de comparer alors $\mathcal{H}_m$ au $\mathbb{T}_m[G_{\mathbb{Q}}]$-module associé à la représentation universelle ρ_m^{univ} (i.e. $\mathbb{T}_m^2$ où $G_{\mathbb{Q}}$ opère via ρ_m^{univ}).

3.1.4. Dualité.

Supposons que $k \leq l+1$: l'accouplement de Weil sur la courbe elliptique universelle $\mathcal{E}$ identifie le $\mathbb{Z}_l$-dual $\mathcal{F}_3^\vee$ de $\mathcal{F}_3$ à $\mathcal{F}_3(-1)$, et par suite $\mathcal{F}_k^\vee$ est isomorphe à $\mathcal{F}_k(2-k)$ [en effet, notre hypothèse fait que $(k-2)!$ est inversible dans $\mathbb{Z}_l$, et le dual de $Sym^{k-2}(\mathcal{F}_3)$ est donc naturellement isomorphe à $Sym^{k-2}(\mathcal{F}_3^\vee)$]. La dualité de Poincaré définit alors un accouplement sur $\mathcal{H}$ à valeurs dans $\mathbb{Z}_l(1-k)$. On prendra garde au fait que ce dernier n'est pas compatible à l'action de $\mathbb{T}$, autrement dit que les opérateurs de Hecke ne sont pas autoadjoints. Pour rendre cet accouplement compatible, on le modifie par l'involution ω_ξ associée à une racine primitive N-ième ξ de l'unité (pour tout ceci, voir [MW1] ou [MW2]) : l'accouplement tordu $[\ ,\ ]$ ainsi obtenu est alors compatible à la

structure de $\mathbb{T}$-module; mais il n'est plus équivariant sous l'action de $G_{\mathbb{Q}}$, car ω_ξ n'est pas définie sur $\mathbb{Q}$, mais sur l'extension cyclotomique $\mathbb{Q}(\xi)^+$. Sa variance suivant $G_{\mathbb{Q}}$ est donnée par la formule :

$$\text{pour } g \in G_{\mathbb{Q}} : \ [g.x, < a_g > g.y] = g.[x, y] \ ,$$

où $g \to a_g \in (\mathbb{Z}/N\mathbb{Z})^*$ désigne le caractère modulo N qui donne l'action de $G_{\mathbb{Q}}$ sur μ_N.

De tout cela on déduit (cf. la remarque finale de 3.1.1.) que le $\mathbb{Z}_l$-dual $\mathcal{H}_m^\vee$ de $\mathcal{H}_m$ est isomorphe comme $\mathbb{T}_m[G_{\mathbb{Q}}]$-module à $\mathcal{H}_m \otimes_{\mathbb{T}_m} \Delta_{m,k,N}$, où $\Delta_{m,k,N}$ désigne un $\mathbb{T}_m$-module libre de rang 1 sur lequel Galois opère via

$$\begin{array}{ll} G_{\mathbb{Q}} & \to \mathbb{T}_m^* \\ g & \to < a_g > \chi_l^{k-1}(g) \ , \end{array}$$

avec $\chi_l : G_{\mathbb{Q}} \to \mathbb{Z}_l^*$ le caractère cyclotomique.

Sans l'hypothèse $k \leq l+1$, tous ces résultats sont vrais rationnellement, c'est-à-dire après extension des scalaires de $\mathbb{Z}_l$ à $\mathbb{Q}_l$.

3.2. La comparaison entre $\mathcal{H}_m$ et ρ_m^{univ}.

3.2.1. Comparons tout d'abord $\mathcal{H}_m \otimes \mathbb{Q}$ et $\rho_m^{\text{univ}} \otimes \mathbb{Q}$.

LEMME. — *Soit m comme ci-dessus (tel que la représentation résiduelle $\overline{\rho}_m$ soit absolument irréductible). Alors les $(\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)[G_{\mathbb{Q}}]$-modules $\mathcal{H}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ et $(\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)^2$, où $G_{\mathbb{Q}}$ opère via $\rho_m^{\text{univ}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, sont isomorphes.*

Preuve :

(a) Commençons par oublier l'action de $G_{\mathbb{Q}}$, et vérifions que $\mathcal{H}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ est un $(\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)$-module libre de rang 2. Il suffit pour cela de vérifier que $\mathcal{H} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ est un $(\mathbb{T} \otimes \mathbb{Q}_l)$-module libre de rang 2, et il revient encore au même de voir que $H_p^1(Y_1(N)_{\mathbb{C}}, \mathcal{F}_k(\mathbb{C}))$ est $(\mathbb{T} \otimes \mathbb{C})$-libre de rang 2 (où $\mathcal{F}_k(\mathbb{C}) = Sym^{k-2}(R^1\pi_*(\mathbb{C}))$. Or l'isomorphisme de Shimura ([De] §3).

$$H_p^1(Y_1(N)_{\mathbb{C}}, \mathcal{F}_k(\mathbb{C})) \simeq S_{k,N}(\mathbb{C}) \oplus \overline{S_{k,N}(\mathbb{C})}$$

décompose $H_p^1(Y_1(N)_{\mathbb{C}}, \mathcal{F}_k(\mathbb{C}))$ en deux sous-espaces qui sont à la fois $\mathbb{T}$-isomorphes (car échangés par la conjugaison complexe) et $\mathbb{T}$-duaux l'un de l'autre; en termes classiques, on peut réaliser l'autodualité hermitienne de $S_{k,N}(\mathbb{C})$ en composant celle associée au produit scalaire de Petersson avec l'opérateur W_N (de façon analogue à (3.1.4)).

D'autre part, il découle d'un résultat de Ribet rappelé en (2.1.4) que $S_{k,N}(\mathbb{C})$ et $\mathbb{T} \otimes \mathbb{C}$ sont en dualité. On en déduit donc bien que $H^1_p(Y_1(N)_{\mathbb{C}}, \mathcal{F}_k(\mathbb{C}))$ est $(\mathbb{T} \otimes \mathbb{C})$-libre de rang 2.

(b) L'algèbre $\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ est un produit d'extensions artiniennes de corps l-adiques. En vertu de (a) et du théorème 1, il nous suffit maintenant de vérifier les relations

$$\text{pour } p \not| Nl \begin{cases} tr_{\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l}(Frob_p \mid \mathcal{H}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = T_p, \\ det_{\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l}(Frob_p \mid \mathcal{H}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = < p > p^{k-1} . \end{cases}$$

Or ces relations résultent classiquement de la relation de congruence d'Eichler-Shimura (comme dans [De]). Cette dernière entraîne en effet l'égalité :

$$T_p = Frob_p + p^{k-1} < p > Frob_p^{-1} ,$$

que l'on peut écrire, introduisant une indéterminée X :

$$1 - T_p X + p^{k-1} < p > X^2 = (1 - Frob_p X)(1 - p^{k-1} < p > Frob_p^{-1} X) .$$

D'autre part, $Frob_p$ et $p^{k-1} < p > Frob_p^{-1}$ sont transposés l'un de l'autre par rapport à l'accouplement $[\ ,\ ]$ de 3.1.4. On peut donc écrire, prenant les déterminants des deux membres de l'égalité ci-dessus (vus comme endomorphismes $(\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)$-linéaires de $\mathcal{H}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$) :

$$det_{\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l}(1 - Frob_p X)^2 = det_{\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l}(1 - T_p X + p^{k-1} < p > X^2) .$$

Enfin, l'isomorphisme de Shimura nous permet d'exprimer le membre de droite : on trouve que c'est le carré de $(1 - T_p X + p^{k-1} < p > X^2)$. D'où la formule :

$$det_{\mathbb{T}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l}(1 - Frob_p X \mid \mathcal{H}_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_m) = 1 - T_p X + p^{k-1} < p > X^2 ,$$

qui prouve les relations annoncées.

3.2.2. Venons-en maintenant à la comparaison entre $\mathcal{H}_m$ et ρ_m^{univ}. On conserve les notations et les hypothèses en vigueur jusqu'ici : en particulier m est un idéal maximal de caractéristique résiduelle l de $\mathbb{T} = \mathbb{T}_{k,N}$ tel que la représentation résiduelle associée soit absolument irréductible ; $\mathcal{H}_m$ a été défini en (3.1.3), et ρ_m^{univ} dans le cours de la démonstration du théorème 3 (2.2).

THÉORÈME 4. — *Il existe un idéal J de $\mathbb{T}_m$ tel que $\mathcal{H}_m$ soit isomorphe comme $\mathbb{T}_m[G_{\mathbb{Q}}]$-module à $\rho_m^{\mathrm{univ}} \otimes_{\mathbb{T}_m} J$, c'est à dire à J^2 où $G_{\mathbb{Q}}$ opère via ρ_m^{univ}.*

Démonstration : Le lemme ci-dessus entraîne l'existence d'une injection $\mathbb{T}_m[G_{\mathbb{Q}}]$-équivariante $\mathcal{H}_m \hookrightarrow \rho_m^{\mathrm{univ}}$; de sorte que tout revient à démontrer le fait suivant : *Soit $\mathcal{R} \subset \mathbb{T}_m^2$ un sous $\mathbb{T}_m$-module, $G_{\mathbb{Q}}$-stable ($G_{\mathbb{Q}}$ opérant sur $\mathbb{T}_m^2$ par ρ_m^{univ}). Alors $\mathcal{R}$ est de la forme J^2 pour $J \subset \mathbb{T}_m$ un idéal.*

Prouvons ceci : désignons par J un idéal de $\mathbb{T}_m$, maximal parmi les idéaux J' tels que $(J')^2 \subset \mathcal{R}$. Il nous faut voir que l'inclusion $J^2 \subset \mathcal{R}$ est en fait une égalité. Raisonnons par l'absurde, en supposant le contraire : il existe $x \in \mathcal{R}$, $x \notin J^2$. On peut supposer de plus que $m.x \subset J^2$ (sinon, il existe un plus petit $n \geq 1$ tel que $m^n.x \subset J^2$ et on remplace x par $x' \in m^{n-1}.x$, $x' \notin J^2$).

Notons alors J' l'idéal de $\mathbb{T}_m$ engendré par J et par les coordonnées x_1 et x_2 de x : J' contient strictement J, et le quotient $Q = J'/J$ est un $\mathbb{F}_m (= \mathbb{T}_m/m)$-espace vectoriel de dimension 1 ou 2.

Dans $Q^2 = (J')^2/J^2$, on a un sous-espace $G_{\mathbb{Q}}$-invariant $W = ((J')^2 \cap \mathcal{R})/J^2$ qui est non nul (car il contient la classe de x). Or, comme représentation de $G_{\mathbb{Q}}$, $Q^2 = Q \otimes_{\mathbb{F}_m} \overline{\rho}_m$, et l'irréductibilité de $\overline{\rho}_m$ entraîne que les sous-espaces invariants dans Q^2 sont de la forme $W = Q_1^2 = Q_1 \otimes_{\mathbb{F}_m} \overline{\rho}_m$, avec Q_1 un sous-espace de Q.

Ici, Q_1 est non nul, et correspond à un idéal J_1 tel que $J' \supset J_1 \supsetneq J$ et que $Q_1 = J_1/J$. On a par définition de W et Q_1 : $(J')^2 \cap \mathcal{R} = J_1^2$. Le fait que $\mathcal{R}$ contienne J_1^2 contredit alors la maximalité de J. Cette contradiction prouve le fait annoncé, et donc le théorème 4.

3.2.3. Quelques remarques.

(i) Si on fait l'hypothèse supplémentaire que $k \leq l+1$, alors l'idéal J qui apparaît dans l'énoncé du théorème 4 est *autodual*, c'est à dire isomorphe comme $\mathbb{T}_m$-module à $J^\vee = Hom_{\mathbb{Z}_l}(J, \mathbb{Z}_l)$. Pour voir ceci, on utilise le fait (3.1.4) que le dual $\mathcal{H}_m^\vee$ est isomorphe à $\mathcal{H}_m$ muni de l'action de Galois tordue par le caractère $g \to < a_g > \chi_l^{k-1}(g)$. D'autre part, le $\mathbb{Z}_l$-dual de $\rho_m^{\mathrm{univ}} \otimes_{\mathbb{T}_m} J \simeq J^2$ s'identifie à $(J^\vee)^2$ où $G_{\mathbb{Q}}$ opère par ${}^t(\rho_m^{\mathrm{univ}})^{-1}$, ce qui est équivalent à $\rho_m^{\mathrm{univ}} \otimes det(\rho_m^{\mathrm{univ}})^{-1}$. Comme $det(\rho_m^{\mathrm{univ}})^{-1}$ est précisément le caractère $g \to < a_g > \chi_l^{k-1}(g)$, on obtient ainsi un $\mathbb{T}_m$-isomorphisme $J^2 \simeq (J^\vee)^2$ compatible avec l'action de $G_{\mathbb{Q}}$ agissant sur les deux membres par la représentation ρ_m^{univ}. Écrivons ce dernier isomorphisme sous la forme d'une matrice $\Phi = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, $A, B, C, D \in \mathrm{Hom}_{\mathbb{T}_m}(J, J^\vee)$. La

réduction modulo m : $\overline{\Phi} = \begin{pmatrix} \overline{A} & \overline{B} \\ \overline{C} & \overline{D} \end{pmatrix}$, de cette matrice est la matrice d'un isomorphisme entre $(J \otimes_{\mathbf{T}_m} \mathbf{F}_m)^2$ et $(J^\vee \otimes_{\mathbf{T}_m} \mathbf{F}_m)^2$, où $\mathbf{F}_m$ désigne le corps résiduel de $\mathbf{T}_m$. Appliquant le lemme de Schur à la réduction (irréductible) $\overline{\rho}_m$ de ρ_m^{univ}, on voit que $\overline{A} = \overline{D}$, et que $\overline{B} = \overline{C} = 0$. La même chose vaut pour l'inverse $\Phi^{-1} = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ de Φ, et par suite $A'A$ (resp. AA'), de réduction l'identité, est un automorphisme de J (resp. de $J^\vee$). Finalement, A établit bien un isomorphisme entre J et $J^\vee$.

(ii) L'idéal J est *bien déterminé en tant que $\mathbf{T}_m$-module* : utilisant en effet le même raisonnement que celui que l'on vient de faire dans la remarque précédente, on voit que l'existence d'un $\mathbf{T}_m$-isomorphisme $G_{\mathbf{Q}}$-équivariant entre $\rho_m^{\mathrm{univ}} \otimes_{\mathbf{T}_m} J$ et $\rho_m^{\mathrm{univ}} \otimes_{\mathbf{T}_m} J'$ entraîne que J et J' sont $\mathbf{T}_m$-isomorphes.

(iii) L'idéal J doit être un réseau dans $\mathbf{T}_m$ (en tant que $\mathbf{Z}_l$-module), c'est à dire que $J \otimes_{\mathbf{Z}_l} \mathbf{Q}_l \simeq \mathbf{T}_m \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$: en effet, $\mathcal{H}_m \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$ et $(\mathbf{T}_m \otimes_{\mathbf{Z}_l} \mathbf{Q}_l)^2$ sont isomorphes d'après le lemme 3.2.1.

En particulier, si J est *principal* engendré par un élément j_0, ce dernier doit être non diviseur de 0 dans $\mathbf{T}_m$, et J est alors libre de rang 1 sur $\mathbf{T}_m$.

3.3. Conséquence : où l'on retrouve un résultat de Boston-Lenstra-Ribet. Un critère pour que $\mathcal{H}_m \simeq \rho_m^{\mathrm{univ}}$.

3.3.1. Nous nous intéressons maintenant à la réduction modulo l de $\mathcal{H}_m$, c'est à dire $\mathcal{H}_m \otimes \mathbf{F}_l$. Cet espace coïncide avec la localisation en m de la cohomologie modulo l : $H^1_p(Y_1(N)_{\overline{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)_m$; en effet, de même que pour la torsion de la cohomologie (3.1.1), le groupe $G_{\mathbf{Q}}$ opère via son quotient abélien sur le conoyau (lié au H^2) de l'injection de $H^1_p(Y_1(N)_{\mathbf{Q}}, \mathcal{F}_k) \otimes \mathbf{F}_l$ dans $H^1_p(Y_1(N)_{\overline{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)$, de sorte que ce conoyau est tué par localisation en m. L'espace $H^1_p(Y_1(N)_{\overline{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)_m$ n'est rien d'autre que le sous-espace propre généralisé dans $H^1_p(Y_1(N)_{\overline{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)$, constitué des éléments annulés par une certaine puissance m^n de l'idéal maximal.

Notons $(\mathcal{H}_m \otimes \mathbf{F}_l)[m] = H^1_p(Y_1(N)_{\overline{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)[m]$ le sous-espace de $\mathcal{H}_m \otimes \mathbf{F}_l$ constitué des éléments annulés par m lui-même : c'est un $\mathbf{F}_m (= \mathbf{T}_m/m)$-espace vectoriel, muni d'une action de $G_{\mathbf{Q}}$. Il est commode de considérer plutôt le $\mathbf{F}_l$-dual de $(\mathcal{H}_m \otimes \mathbf{F}_l)[m]$, lequel s'identifie au quotient de $\mathcal{H}_m^\vee \otimes \mathbf{F}_l$ par le sous-espace engendré par les images des $T \in m$, autrement dit à :

$$\mathcal{H}_m^\vee \otimes \mathbf{F}_l / m(\mathcal{H}_m^\vee \otimes \mathbf{F}_l) = \mathcal{H}_m^\vee / m\mathcal{H}_m^\vee = \mathcal{H}_m^\vee \otimes_{\mathbf{T}_m} \mathbf{F}_m \ .$$

Or, si on utilise le théorème 4, on voit que ce dernier espace est isomorphe à $(J^\vee)^2 \otimes_{\mathbf{T}_m} \mathbf{F}_m = (J^\vee/mJ^\vee)^2$ où $G_{\mathbf{Q}}$ agit par la contragrédiente de la représentation résiduelle $\overline{\rho}_m$. Désignons par ν *la dimension du* $\mathbf{F}_m$*-espace vectoriel* $J^\vee/mJ^\vee$*, c'est à dire le nombre minimal de générateurs du module* $J^\vee$: alors $\mathcal{H}_m^\vee \otimes_{\mathbf{T}_m} \mathbf{F}_m$ est la somme de ν copies de $\mathbf{F}_m^2$, sur chacune desquelles $G_{\mathbf{Q}}$ agit par $({}^t\overline{\rho}_m)^{-1}$. Redualisant, on obtient finalement :

THÉORÈME 5. — [*rappelons que la représentation résiduelle* $\overline{\rho}_m$ *est supposée absolument irréductible*].

Le $\mathbf{F}_m$*-espace* $H^1_p(Y_1(N)_{\bar{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)[m]$ *se décompose en la somme de* ν *sous-espaces* $G_{\mathbf{Q}}$*-stables de dimension 2 isomorphes (comme représentations de* $G_{\mathbf{Q}}$*) à* $\overline{\rho}_m$*.*

On retrouve ainsi un résultat de semi-simplicité que Boston, Lenstra et Ribet ([B-L-R]) ont récemment établi par de toutes autres méthodes; ils obtiennent d'ailleurs, plus généralement, le résultat analogue pour les courbes de Shimura.

3.3.2. Un critère pour que $\mathcal{H}_m \simeq \rho_m^{\mathrm{univ}}$.

On se place ici sous l'hypothèse que $k \leq l+1$, et donc ((3.2.3)(i)) $J^\vee$ est isomorphe à J. D'après ce qui précède, le théorème 4 et les remarques (3.2.3)(ii) et (iii) qui le suivent, on voit que $\mathcal{H}_m$ est $\mathbf{T}_m[G_{\mathbf{Q}}]$-isomorphe à ρ_m^{univ} si et seulement si J est un idéal principal, c'est à dire *si et seulement si l'entier* ν *introduit ci-dessus est égal à* 1. Compte tenu du théorème 5, cela revient encore à exiger que la représentation résiduelle $\overline{\rho}_m$ n'intervienne qu'une seule fois dans $H^1_p(Y_1(N)_{\overline{\mathbf{Q}}}, \mathcal{F}_k/l\mathcal{F}_k)[m]$.

Cette condition de multiplicité 1 a été souvent été étudiée, la première fois par Mazur ([Ma 1]); elle constituait un ingrédient essentiel de la preuve par Ribet ([Ri 2]) du fait que la conjecture de Taniyama-Weil entraîne celle de Fermat, bien que des travaux récents du même auteur ([Ri 3]) permettent de s'en dispenser partiellement. On renvoie à ([M-R]) pour une discussion de cette question. Bornons-nous simplement ici à dire que la condition est satisfaite, en poids 2, si l est supérieur ou égal à 3 et ne divise par N; plus généralement, en poids $k \geq 3$, elle est en principe satisfaite (on devrait trouver une démonstration complète de ce fait dans un article en préparation de Faltings et Jordan) si $l > k$, $l \nmid N$. On prouve cela par un argument de comparaison entre cohomologie étale modulo l et cohomologie de De Rham modulo l : voir [Ma 1], [Ri 2], [J-L]; ce résultat est énoncé généralement plutôt pour $X_0(N)$ que pour $X_1(N)$, mais les arguments utilisés valent aussi pour $X_1(N)$.

Si la condition est satisfaite, il résulte alors de la remarque (3.2.3)(i) que $\mathbb{T}_m^\vee = Hom_{\mathbb{Z}_l}(\mathbb{T}_m, \mathbb{Z}_l)$ est $\mathbb{T}_m$-libre de rang 1 : l'anneau $\mathbb{T}_m$ est donc un *anneau de Gorenstein.*

Lorsque la condition n'est pas satisfaite, j'ignore comment réaliser géométriquement la représentation ρ_m^{univ}.

Références

[Az] G. AZUMAYA, *On maximally central algebras*, Nagoya Math. J. Vol. **2** (1951), p. 119-150.

[B-L-R] N. BOSTON, H.W. LENSTRA, Jr., K.A. RIBET, *Quotients of group rings arising from two-dimensional representations*, C.R. Acad. Sci. Paris, t. **312**, Ser. I, Fev. 1991, p. 323-328.

[C-R] C.W. CURTIS, I. REINER, *Representation theory of finite groups and associative algebras*, Pure and Applied Math. **11**, New-York, Interscience 1962.

[De] P. DELIGNE, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki, exposé 355, Février 1969, Springer Lecture Notes in Math. **179**, 1971, p. 139-172.

[D-S] P. DELIGNE, J.-P. SERRE, *Formes modulaires de poids 1*, Ann. Sci. E.N.S. 4^e Ser. t. **7**, 1974, p. 507-530.

[Gr] B.H. GROSS, *A tameness criterion for Galois representations associated to modular forms (mod. p)* Duke Math. J., Vol. **61**, $n^o 2$, 1990, p. 445-517.

[Hi] H. HIDA, *Galois representations into* $GL_2(\mathbb{Z}_p[[X]])$ *attached to ordinary cusp forms*, Invent. Math. **85**, 1986, p. 545-613.

[J-L] B.W. JORDAN, R. LIVNÉ, *Conjecture "epsilon" for weight* $k > 2$, Bull. A.M.S., Vol. **21**, $n^o 1$, July 1989, p. 51-56.

[Ka] N.M. KATZ, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable III (W. Kuyk and J.-P. Serre, ed.), Springer Lecture Notes in math. **350**, 1972, P. 69-190.

[K-O] M.-A. KNUS, M. OJANGUREN, *Théorie de la Descente et Algèbres d'Azumaya*, Springer Lecture Notes in Math. **389**, 1974.

[La] S.LANG, *Algebra*, Addison-Wesley publishing company, 1971.

[Lo] J.-L. LODAY, *Cyclic Homology*, livre en préparation à paraître dans Grundl. Math. Wiss. (Springer).

[Ma 1] B. MAZUR, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES n^o **47**, 1977, p. 33-186.

[Ma 2] B. MAZUR, *Deforming Galois Representations*, Galois Groups over