Vol. 54, No. 1 DUKE MATHEMATICAL JOURNAL © 1987

SUR LES REPRÉSENTATIONS MODULAIRES DE DEGRÉ 2 DE $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$

JEAN-PIERRE SERRE

à Yuri Ivanovich Manin, pour son 50^e anniversaire

Le présent travail reprend, en la précisant, une *conjecture* faite en 1973, dont on trouvera un cas particulier dans [44], §3.

Il s'agit de représentations "modulaires" (au sens de Brauer), de degré 2, du groupe de Galois $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Si ρ: $G_{\mathbf{Q}} \to \mathbf{GL}_2(\overline{\mathbf{F}}_p)$ est une telle représentation, supposée irréductible et de déterminant impair, la conjecture en question affirme que ρ est vraiment "modulaire", i.e. provient d'une forme modulaire parabolique mod p qui est fonction propre des opérateurs de Hecke.

Pour que cet énoncé soit à la fois utilisable et vérifiable numériquement, il est nécessaire de préciser le type de la forme modulaire correspondant à ρ: niveau N, poids k, caractère ε. En ce qui concerne N, les exemples connus suggèrent une réponse simple: N devrait être le *conducteur d'Artin* de ρ (n° 1.2); en particulier, il ne dépendrait que de la ramification de ρ en dehors de p. Une fois N connu, la classe de k mod$(p-1)$, et le caractère ε, s'obtiennent sans difficultés à partir du déterminant de ρ (n° 1.3). Il reste à déterminer la valeur exacte du *poids* k (ou plutôt sa valeur minimale). C'est là une question délicate, qui n'avait pas été abordée dans [44]. Il semble que k ne dépende que de la ramification de ρ en p (exposants des caractères de l'inertie modérée, inertie sauvage, etc); la recette précise que je propose est décrite aux n^{os} 2.2, 2.3 et 2.4.

Les définitions de N, k et ε esquissées ci-dessus font l'objet des §1 et §2. Le §3 contient l'énoncé principal, avec divers compléments. Le §4 explore les conséquences agréables qu'aurait cet énoncé, s'il était vrai: théorème de Fermat, conjecture de Taniyama-Weil, etc. Enfin, le §5 donne un certain nombre d'exemples numériques, pour $p = 2$, 3 et 7.

Ce texte doit beaucoup aux mathématiciens suivants, que j'ai plaisir à remercier:

—John Tate, pour ses nombreuses lettres (notamment en 1973 et 1974) relatives à la conjecture, ainsi qu'aux relations entre poids et inertie en p;

—Jean-Marc Fontaine, dont les résultats sur les représentations locales attachées à la cohomologie ont confirmé les idées de Tate, et ont permis de préciser la valeur du poids k attaché à une représentation;

Received December 5, 1986.

—Gerhard Frey, qui a eu l'idée fondamentale (cf. [17]) que la conjecture de Taniyama-Weil, convenablement complétée, entraîne le théorème de Fermat: i.e., "Weil + epsilon[1] ⇒ Fermat";

enfin, et tout spécialement:

—Jean-François Mestre, qui a réussi à programmer et vérifier un nombre d'exemples suffisant pour me convaincre que la conjecture méritait d'être prise au sérieux.

Table des matières pages

§1. Définitions de N, de ε, et de k mod $(p-1)$

1.1. *Notations.* La lettre p désigne un nombre premier. On note $\overline{\mathbf{F}}_p$ une clôture algébrique du corps $\mathbf{F}_p$, et $\overline{\mathbf{Q}}$ une clôture algébrique du corps $\mathbf{Q}$. On pose $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

On se donne un homomorphisme continu

$$\rho\colon G_{\mathbf{Q}} \to \mathbf{GL}(V),$$

où V est un espace vectoriel de dimension 2 sur $\overline{\mathbf{F}}_p$. L'image de ρ est un groupe fini, noté G; par définition, ce groupe est isomorphe à un sous-groupe de $\mathbf{GL}_2(\mathbf{F}_q)$, où q est une puissance convenable de p. (Si $p \neq 2$, ou si ρ est irréductible, on peut prendre pour $\mathbf{F}_q$ le corps engendré par les *traces* des éléments de G.)

On se propose d'attacher à ρ des entiers positifs N et k, ainsi qu'un caractère de Dirichlet $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$.

1.2. *Définition de N.* L'entier N est simplement le *conducteur d'Artin* de ρ, défini comme en caractéristique 0 (cf. [1], [38]), à cela près que l'on se restreint aux places premières à p.

De façon plus précise, soit l un nombre premier $\neq p$. Choisissons une extension à $\overline{\mathbf{Q}}$ de la valuation l-adique de $\mathbf{Q}$, et soient

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset \cdots$$

la suite des groupes de ramification de G correspondant à cette valuation ([38],

[1]Il semble que Ribet soit récemment parvenu à éliminer entièrement "epsilon"; d'où "Weil ⇒ Fermat".

chap. IV). Notons V_i le sous-espace de V formé des éléments fixés par G_i, et posons

$$n(l,\rho) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim V/V_i. \tag{1.2.1}$$

On peut récrire (1.2.1) sous la forme:

$$n(l,\rho) = \dim V/V_0 + b(V), \tag{1.2.2}$$

où $b(V)$ est "l'invariant sauvage" du G_0-module V, cf. [39], §19.3.

Ces formules entraînent:

(a) $n(l,\rho)$ est un entier $\geqslant 0$;

(b) $n(l,\rho) = 0$ si et seulement si $G_0 = \{1\}$, i.e., si et seulement si ρ est non ramifiée en l;

(c) $n(l,\rho) = \dim V/V_0$ si et seulement si $G_1 = \{1\}$, i.e., si et seulement si ρ est modérément ramifiée en l.

Il résulte de (a) et (b) que l'on peut définir un entier N par la formule

$$N = \prod_{l \neq p} l^{n(l,\rho)}. \tag{1.2.3}$$

Nous appellerons N le *conducteur* de ρ; par construction, N est premier à p.

1.3. *Définition du caractère ε et de la classe de k mod$(p-1)$.* Le *déterminant* de la représentation ρ est un homomorphisme

$$\det \rho : G_{\mathbf{Q}} \to \overline{\mathbf{F}}_p^*.$$

Son image est un sous-groupe cyclique fini de $\overline{\mathbf{F}}_p^*$, d'ordre premier à p. On peut donc regarder $\det \rho$ comme un caractère de $G_{\mathbf{Q}}$. Le conducteur de ce caractère divise pN: cela se voit, par exemple, en comparant les formules donnant les conducteurs de ρ et de $\det \rho$. On peut ainsi identifier $\det \rho$ à un homomorphisme de $(\mathbf{Z}/pN\mathbf{Z})^*$ dans $\overline{\mathbf{F}}_p^*$, ou, ce qui revient au même, à un couple d'homomorphismes

$$\varphi : (\mathbf{Z}/p\mathbf{Z})^* \to \overline{\mathbf{F}}_p^* \tag{1.3.1}$$

et

$$\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*. \tag{1.3.2}$$

Comme $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p-1$, l'homomorphisme φ est de la forme

$$x \mapsto x^h, \text{ avec } h \in \mathbf{Z}/(p-1)\mathbf{Z}. \tag{1.3.3}$$

Ceci peut se récrire:

$$\varphi = \chi^h, \tag{1.3.4}$$

où χ: $G_{\mathbf{Q}} \to \mathbf{F}_p^*$ désigne le p-ième *caractère cyclotomique* de $G_{\mathbf{Q}}$ (celui qui donne l'action de $G_{\mathbf{Q}}$ sur les racines p-ièmes de l'unité).

On peut résumer ces formules en disant que, si l est un nombre premier ne divisant pas pN, et si $\mathrm{Frob}_{l,\rho}$ est l'élément de Frobenius correspondant dans G (défini à conjugaison près), on a

$$\det(\mathrm{Frob}_{l,\rho}) = l^h \varepsilon(l) \quad \text{dans } \overline{\mathbf{F}}_p^*. \tag{1.3.5}$$

Au §2, nous définirons un certain entier k attaché à ρ et nous verrons (n° 2.5) que h est simplement la classe de $k-1$ mod$(p-1)$, de sorte que (1.3.5) peut se récrire:

$$\det(\mathrm{Frob}_{l,\rho}) = l^{k-1} \varepsilon(l) \quad \text{dans } \overline{\mathbf{F}}_p^*. \tag{1.3.6}$$

Remarque. Soit c l'élément d'ordre 2 de $G_{\mathbf{Q}}$ donné par la conjugaison complexe (relativement à un plongement de $\overline{\mathbf{Q}}$ dans $\mathbf{C}$). L'image de c dans $(\mathbf{Z}/pN\mathbf{Z})^*$ est -1. On en conclut que:

$$\det \rho(c) = (-1)^{k-1} \varepsilon(-1). \tag{1.3.7}$$

Dans la suite, on s'intéressera uniquement au cas où $\det \rho$ est *impair*, i.e.

$$\det \rho(c) = -1, \tag{1.3.8}$$

ou encore:

$$\varepsilon(-1) = (-1)^k \quad \text{dans } \overline{\mathbf{F}}_p^*. \tag{1.3.9}$$

Si $p = 2$, cette condition est automatiquement satisfaite, puisque $-1 = 1$. Si $p \neq 2$, elle signifie que $\rho(c)$ est conjuguée de la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

§2. L'entier *k*. Le but de ce § est de définir l'entier k (le "poids") associé à une représentation ρ. Les n^{os} 2.1 à 2.4 contiennent la définition générale; les n^{os} 2.5 à 2.9 en donnent divers exemples.

2.1. *Préliminaires.* L'entier k ne dépend que de la restriction de la représentation ρ au groupe de décomposition en p (et même, en fait, au groupe d'inertie). Aussi, pour le définir, allons-nous partir d'une représentation "locale en p":

$$\rho_p \colon G_p \to \mathbf{GL}(V) \simeq \mathbf{GL}_2(\overline{\mathbf{F}}_p),$$

où $G_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

Nous noterons I le groupe d'inertie de G_p, et I_p le plus grand pro-p-sous-groupe de I (groupe d'inertie *sauvage*). Le quotient $I_t = I/I_p$ est le *groupe d'inertie modérée* de G_p; il s'identifie à $\varprojlim \mathbf{F}_{p^n}^*$, cf. [41], prop. 2. Un caractère de I_t sera dit *de niveau n* s'il se factorise par $\mathbf{F}_{p^n}^*$, et ne se factorise par aucun $\mathbf{F}_{p^m}^*$, où m est un diviseur strict de n.

Si V^{ss} désigne le semi-simplifié de V vis-à-vis de l'action de G_p, le groupe I_p agit trivialement sur V^{ss} ([41], prop. 4), de sorte que I_t opère sur V^{ss}. Cette action de I_t est diagonalisable; elle est donnée par deux caractères

$$\varphi, \varphi' \colon I_t \to \overline{\mathbf{F}}_p^*.$$

PROPOSITION 1. *Les caractères φ et φ' donnant l'action de I_t sur V^{ss} sont de niveau* 1 *ou* 2. *S'ils sont de niveau* 2, *ils sont conjugués*: *on a $\varphi' = \varphi^p$ et $\varphi = \varphi'^p$.*

Soit s un élément de G_p dont l'image dans $G_p/I = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ soit l'automorphisme de Frobenius $x \mapsto x^p$. On vérifie facilement que, si $u \in I$, on a $sus^{-1} \equiv u^p \pmod{I_p}$: la conjugaison par s opère sur $I_t = I/I_p$ par $u \mapsto u^p$. Il en résulte que l'ensemble $\{\varphi, \varphi'\}$ est stable par l'opération de puissance p-ième. D'où deux cas:

(a) on a $\varphi^p = \varphi$, $\varphi'^p = \varphi'$ et les deux caractères φ et φ' sont de niveau 1;

(b) on a $\varphi^p = \varphi'$, $\varphi'^p = \varphi$, $\varphi \neq \varphi'$, et les deux caractères φ et φ' sont de niveau 2.

Cela démontre la prop. 1.

Nous allons maintenant nous occuper séparément de ces deux cas.

2.2 *Définition de k lorsque φ et φ' sont de niveau* 2. Supposons que φ et φ' soient de niveau 2. La représentation V est alors *irréductible*, car si elle contenait un sous-espace stable de dimension 1, l'action de I_t sur ce sous-espace se ferait par un caractère prolongeable à G_p, donc de niveau 1. Appelons ψ et $\psi' = \psi^p$ les deux *caractères fondamentaux de niveau* 2 de I_t ([41], n° 1.7), autrement dit les deux caractères $I_t \to \mathbf{F}_{p^2}^* \to \overline{\mathbf{F}}_p^*$ correspondant aux deux plongements du corps $\mathbf{F}_{p^2}$ dans le corps $\overline{\mathbf{F}}_p$. On peut écrire φ de manière unique sous la forme

$$\varphi = \psi^{a+pb} = \psi^a \psi'^b, \quad \text{avec} \quad 0 \leqslant a, b \leqslant p-1. \tag{2.2.1}$$

On a $b \neq a$, car sinon φ serait égal à $(\psi\psi')^a = \chi^a$, où χ est le caractère cyclotomique (ou plutôt sa restriction à I), et cela contredirait l'hypothèse que φ est de niveau 2. De plus, comme φ' est conjugué de φ, on a

$$\varphi' = \psi^b \psi'^a. \tag{2.2.2}$$

Quitte à permuter φ et φ', on peut donc supposer que:

$$0 \leqslant a < b \leqslant p-1. \tag{2.2.3}$$

Ceci fait, l'entier k attaché à ρ_p est défini par:

$$k = 1 + pa + b. \tag{2.2.4}$$

Remarques

(1) La plus petite valeur possible de k est $k = 2$, qui est obtenue lorsque $a = 0$, $b = 1$, c'est-à-dire lorsque φ et φ' sont égaux aux *caractères fondamentaux* ψ et ψ' de niveau 2.

(2) Dans le cas particulier $a = 0$, on a $(\varphi, \varphi') = (\psi^b, \psi'^b)$, avec $1 \leqslant b \leqslant p - 1$, et la définition de k se réduit à:

$$k = 1 + b \qquad (\text{d'où } 2 \leqslant k \leqslant p).$$

Le cas général se ramène à celui-là par "torsion". En effet, on peut écrire ρ_p sous la forme

$$\rho_p = \chi^a \otimes \rho'_p,$$

où χ est le caractère cyclotomique (vu comme caractère de G_p, et pas seulement de I). Le couple (a, b) attaché à ρ'_p est alors $(0, b - a)$, et l'entier k correspondant est $k' = 1 + b - a$. On peut donc récrire (2.2.4) sous la forme

$$k = k' + a(p + 1). \tag{2.2.5}$$

(Comparer avec la formule donnant la filtration de la forme modulaire "tordue" d'une forme donnée, cf. [24], [42].)

2.3. *Définition de k lorsque φ et φ' sont de niveau* 1, *et que I_p opère trivialement.* On suppose que l'action de I sur V est semi-simple, et qu'elle est donnée par deux caractères (φ, φ') qui sont des puissances χ^a et χ^b du caractère cyclotomique χ:

$$\rho_p | I = \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}.$$

Les entiers a et b sont déterminés mod$(p - 1)$. On les normalise de telle sorte que $0 \leqslant a, b \leqslant p - 2$. De plus, quitte à permuter φ et φ', on peut supposer que $a \leqslant b$. On a donc

$$0 \leqslant a \leqslant b \leqslant p - 2. \tag{2.3.1}$$

L'entier k est alors défini par:

$$k = \begin{cases} 1 + pa + b & \text{si } (a, b) \neq (0, 0) \\ p & \text{si } (a, b) = (0, 0). \end{cases} \tag{2.3.2}$$

Remarques

(1) Ici encore, la plus petite valeur possible de k est $k = 2$, qui correspond à $\varphi = 1$, $\varphi' = \chi$.

(2) Le cas $(a, b) = (0, 0)$ est celui où I opère trivialement sur V, autrement dit où ρ_p est *non ramifiée*. La formule générale $k = 1 + pa + b$ donnerait alors $k = 1$. Comme les formes modulaires de poids 1 ont un comportement quelque peu exceptionnel, j'ai préféré les éviter, et "décaler" k par $p - 1$; d'où la valeur $k = p$ adoptée.

(3) Lorsqu'on tord ρ_p par les puissances successives $\chi, \chi^2, \ldots$ du caractère χ, les entiers k correspondants forment un *cycle de Tate*, cf. [21], [22].

2.4. *Définition de k lorsque I_p n'opère pas trivialement.* On suppose que I_p n'opère pas trivialement, i.e., que l'action de I n'est pas modérée. Les éléments de V fixés par I_p forment alors une droite D, qui est stable par G_p. L'action de G_p sur V/D (resp. sur D) se fait par un caractère θ_1 (resp. θ_2) de G_p:

$$\rho_p = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}. \tag{2.4.1}$$

On peut écrire θ_1 et θ_2 de façon unique sous la forme

$$\theta_1 = \chi^{\alpha}\varepsilon_1, \theta_2 = \chi^{\beta}\varepsilon_2, \qquad (\alpha, \beta \in \mathbf{Z}/(p-1)\mathbf{Z}), \tag{2.4.2}$$

où ε_1 et ε_2 sont des caractères non ramifiés de G_p à valeurs dans $\overline{\mathbf{F}}_p^*$. La restriction de ρ_p à I est donc:

$$\rho_p | I = \begin{pmatrix} \chi^{\beta} & * \\ 0 & \chi^{\alpha} \end{pmatrix}.$$

On normalise les exposants α et β par:

$$0 \leqslant \alpha \leqslant p-2 \quad \text{et} \quad 1 \leqslant \beta \leqslant p-1. \tag{2.4.3}$$

(Noter qu'ici χ^{α} et χ^{β} ne jouent pas des rôles symétriques.) On pose:

$$a = \mathrm{Inf}(\alpha, \beta) \quad \text{et} \quad b = \mathrm{Sup}(\alpha, \beta). \tag{2.4.4}$$

Pour définir k, on distingue deux cas:

(i) *Le cas $\beta \neq \alpha + 1$ (i.e., $\chi^{\beta} \neq \chi \cdot \chi^{\alpha}$).* On pose alors, comme au n° 2.3:

$$k = 1 + pa + b. \tag{2.4.5}$$

(Noter le cas où $\chi^\alpha = \chi^\beta = 1$, $p \geqslant 3$, où (2.4.3) impose $\alpha = 0$, $\beta = p - 1$, de sorte que (2.4.5) donne $k = p$, comme dans (2.3.2).)

(ii) *Le cas* $\beta = \alpha + 1$ (*i.e.*, $\chi^\beta = \chi \cdot \chi^\alpha$).

La définition de k dépend alors du type de la ramification sauvage. Il y a deux types possibles, que j'appellerai respectivement *peu ramifié* et *très ramifié*. On les définit de la manière suivante:

Soit $K_0 = \mathbf{Q}_{p,\mathrm{nr}}$ l'extension non ramifiée maximale de $\mathbf{Q}_p$; on a $I = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_0)$. Le groupe $\rho_p(I)$ est le groupe de Galois d'une certaine extension totalement ramifiée K de K_0, et le groupe d'inertie sauvage $\rho_p(I_p)$ est le groupe de Galois de K/K_t, où K_t est la plus grande extension modérément ramifiée de K_0 contenue dans K.

$$\begin{array}{c} K \\ | \\ K_t \\ | \\ K_0 \end{array}$$

Du fait que $\beta = \alpha + 1$, on déduit que $\mathrm{Gal}(K_t/K_0) = (\mathbf{Z}/p\mathbf{Z})^*$, donc que $K_t = K_0(z)$, où z est une racine primitive p-ième de l'unité. D'autre part, le groupe $\mathrm{Gal}(K/K_t) = \rho_p(I_p)$ est un groupe abélien élémentaire de type $(p, \ldots, p)$, représentable matriciellement par $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. De plus, l'hypothèse $\beta = \alpha + 1$ entraîne que l'action par conjugaison de $\mathrm{Gal}(K_t/K_0) = (\mathbf{Z}/p\mathbf{Z})^*$ sur $\mathrm{Gal}(K/K_t)$ est l'action évidente. Utilisant la théorie de Kummer, on en déduit que K peut s'écrire sous la forme

$$K = K_t\left(x_1^{1/p}, \ldots, x_m^{1/p}\right), \quad \text{où } p^m = [K : K_t], \tag{2.4.6}$$

les x_i étant des éléments de K_0^*/K_0^{*p}. Si v_p désigne la valuation de K_0, normalisée par $v_p(p) = 1$, nous dirons que l'extension K (ou la représentation ρ_p) est *peu ramifiée* si

$$v_p(x_i) \equiv 0 \pmod{p} \quad \text{pour } i = 1, \ldots, m, \tag{2.4.7}$$

i.e., si les x_i peuvent être choisis parmi les *unités* de K_0. Dans le cas contraire, nous dirons que K et ρ_p sont *très ramifiées*.

Remarques

(1) Le cas très ramifié n'est possible que si les caractères ε_1 et ε_2 définis par (2.4.2) sont égaux, et l'on a alors $m = 1$ ou $m = 2$: cela se voit en utilisant l'action par conjugaison de G_p sur $\rho_p(I_p)$.

(2) Soit π une uniformisante de K_t, par exemple $\pi = 1 - z$ ou $\pi = p^{1/(p-1)}$. Si K/K_t est peu ramifiée, les $p^m - 1$ caractères d'ordre p associés à cette extension

sont tous de conducteur (π^2); dans le cas très ramifié, $p^m - p^{m-1}$ de ces caractères sont de conducteur $(\pi^{p+1}) = (p\pi^2)$ et les $p^{m-1} - 1$ autres sont de conducteur (π^2).

Nous pouvons maintenant définir l'entier k:

(ii_1) *Le cas $\beta = \alpha + 1$, peu ramifié*

La formule est la même que dans le cas $\beta \neq \alpha + 1$:

$$k = 1 + pa + b = 2 + \alpha(p+1). \tag{2.4.8}$$

(ii_2) *Le cas $\beta = \alpha + 1$, très ramifié*

On ajoute $p - 1$ (resp. 2 si $p = 2$) à ce que donnerait (2.4.8):

$$k = \begin{cases} 1 + pa + b + p - 1 = (\alpha+1)(p+1) & \text{si } p \neq 2 \\ 4 & \text{si } p = 2. \end{cases} \tag{2.4.9}$$

Les formules (2.2.4), (2.3.2), (2.4.5), (2.4.8), et (2.4.9) fournissent une définition complète de l'entier k attaché à la représentation ρ_p considérée. Voici quelques propriétés qui résultent de cette définition:

2.5. *Classe de k* mod $(p-1)$.

PROPOSITION 2. *On a.*

$$\det \rho_p | I = \chi^{k-1}. \tag{2.5.1}$$

(Comme χ est d'ordre $p - 1$, cette formule montre que la classe de k mod$(p-1)$ est déterminée par $\det \rho_p$, et même seulement par la restriction de $\det \rho_p$ au groupe d'inertie I.)

Vérifions (2.5.1) dans le cas de hauteur 2 (cf. n° 2.2). On a alors

$$\det \rho_p | I = \varphi \cdot \varphi' = (\psi^a \psi'^b)(\psi^b \psi'^a) = (\psi\psi')^{a+b} = \chi^{a+b}$$

$$= \chi^{k-1},$$

puisque $k - 1 = pa + b \equiv a + b \bmod(p-1)$.

Les autres cas sont analogues.

On peut récrire (2.5.2) sous la forme

$$\det \rho_p = \varepsilon_p \cdot \chi^{k-1}, \tag{2.5.2}$$

où ε_p est un *caractère non ramifié* de G_p à valeurs dans $\overline{\mathbf{F}}_p^*$. Dans le cas où ρ_p provient d'une représentation globale ρ de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, le caractère ε_p n'est autre que la *p-composante* du caractère ε défini au n° 1.3; on a

$$\varepsilon_p(\mathrm{Frob}_p) = \varepsilon(p), \tag{2.5.3}$$

où Frob_p est un élément de Frobenius de G_p.

2.6. *Valeurs de k.* Pour $p \neq 2$, les valeurs possibles de k sont les nombres de l'intervalle $[2, p^2 - 1]$ qui peuvent s'écrire sous la forme

$$k = 1 + a_0 + pa_1, \qquad 0 \leqslant a_0, a_1 \leqslant p - 1,$$

avec $a_1 \leqslant a_0 + 1$. Ainsi, pour $p = 3$, on a $k = 2, 3, 4, 5, 6$ ou 8.

Pour $p = 2$, on a $k = 2$ si l'action de I_p est triviale, ou peu ramifiée, et $k = 4$ si l'action de I_p est très ramifiée.

Exemple. Prenons $p = 2$. Soit u: $G_2 \to \mathbf{Z}/2\mathbf{Z}$ un homomorphisme surjectif, et soit ρ_2: $G_2 \to \mathbf{GL}_2(\mathbf{F}_2)$ la représentation définie par

$$s \mapsto \begin{pmatrix} 1 & u(s) \\ 0 & 1 \end{pmatrix}.$$

Soit $K/\mathbf{Q}_2$ l'extension quadratique correspondant au noyau de u. On a alors:

$k = 2$ si $K/\mathbf{Q}_2$ est non ramifiée, i.e., $K = \mathbf{Q}_2(\sqrt{5})$;

$k = 2$ si $\operatorname{discr}(K/\mathbf{Q}_2) = (4)$, i.e., $K = \mathbf{Q}_2(\sqrt{-1})$ ou $\mathbf{Q}_2(\sqrt{-5})$;

$k = 4$ si $\operatorname{discr}(K/\mathbf{Q}_2) = (8)$, i.e., $K = \mathbf{Q}_2(\sqrt{2}), \mathbf{Q}_2(\sqrt{-2}), \mathbf{Q}_2(\sqrt{10})$ ou $\mathbf{Q}_2(\sqrt{-10})$.

2.7. *Conditions pour que $k \leqslant p + 1$, lorsque $p \neq 2$.* Supposons $p \neq 2$. On a $k \leqslant p + 1$ si et seulement si l'une des deux conditions suivantes est satisfaite:

(2.7.1) Il existe un quotient V/D de V, de dimension 1, sur lequel I opère trivialement (i.e., *V a un quotient étale de dimension* 1); c'est le cas $a = 0$ des n^{os} 2.3 et 2.4.

(2.7.2) L'action de I sur V se fait par deux caractères modérés de la forme (ψ^b, ψ'^b), avec $1 \leqslant b \leqslant p - 1$, où ψ et ψ' sont les deux caractères fondamentaux de niveau 2 de I_t; c'est le cas $a = 0$ du n° 2.2.

Remarques

(1) On a $k = p + 1$ si et seulement si la restriction de ρ_p au groupe d'inertie I est de la forme $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ et est très ramifiée.

(2) Quelle que soit la représentation ρ_p, il existe une "tordue" $\chi^m \otimes \rho_p$ de ρ_p dont l'invariant k est $\leqslant p + 1$ (comparer à [44], th.3).

2.8. *Conditions pour que $k = 2$.*

L'énoncé suivant résulte immédiatement des définitions:

PROPOSITION 3. *Pour que l'invariant k de ρ_p soit égal à 2, il faut et il suffit que $\rho_p|I$ soit de l'un des deux types suivants*:

$$\rho_p|I \simeq \begin{pmatrix} \psi' & 0 \\ 0 & \psi \end{pmatrix}, \tag{2.8.1}$$

où $\psi, \psi' \colon I \to I_t \to \mathbf{F}_{p^2}^*$ *sont les deux caractères fondamentaux de* I *de niveau* 2;

$$\rho_p|I \simeq \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix} \quad ou \quad \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}, \tag{2.8.2}$$

l'action du groupe d'inertie sauvage I_p *étant, soit triviale, soit peu ramifiée.*

On peut donner une autre caractérisation de ce cas, en termes de *schémas en groupes de type* (p, p). Pour l'énoncer, je me bornerai au cas où ρ_p prend ses valeurs dan $\mathbf{GL}_2(\mathbf{F}_p)$, donc définit un schéma en groupes (étale) de type (p, p) sur le corps $\mathbf{Q}_p$ (dans le cas général, il faudrait parler de "schémas en $\mathbf{F}_q$-vectoriels" au sens de Raynaud [35]). On peut se demander si ce schéma en groupes se prolonge en un schéma en groupes fini et plat sur $\mathbf{Z}_p$, cf. [35]; s'il en est ainsi, je dirai (cf. [48]) que la représentation ρ_p est *finie* en p.

PROPOSITION 4. *On a* $k = 2$ *si et seulement si les deux conditions suivantes sont satisfaites*:

$$\det \rho_p|I = \chi; \tag{2.8.3}$$

$$\rho_p \textit{ est finie en } p. \tag{2.8.4}$$

D'après le n° 2.5, la condition (2.8.3) équivaut à:

$$k \equiv 2 \mod(p-1). \tag{2.8.5}$$

Elle est donc nécessaire pour que k soit égal à 2. Montrons qu'elle est suffisante lorsque ρ_p est finie en p. D'après [35], cor. 3.4.4, chacun des caractères φ et φ' de I_t associés à ρ_p peut alors s'écrire sous la forme

$$\psi^n \psi'^{n'}, \quad \text{avec } 0 \leqslant n, n' \leqslant 1,$$

où ψ et ψ' sont comme ci-dessus les deux caractères fondamentaux de niveau 2. Cela fait quatre possibilités

$$1, \psi, \psi' \quad \text{et} \quad \psi\psi' = \chi$$

(qui se réduisent d'ailleurs à trois pour $p = 2$ puisque χ est alors égal à 1). Comme $\varphi\varphi' = \chi$ d'après (2.8.1), deux cas seulement sont possibles:

(i) $$\{\varphi, \varphi'\} = \{\psi, \psi'\}$$

et

(ii) $$\{\varphi, \varphi'\} = \{1, \chi\}.$$

Le cas (i) donne (2.8.1), d'où $k = 2$, comme annoncé. Occupons-nous du cas (ii), en nous bornant, pour simplifier, au cas $p \neq 2$ (le cas $p = 2$ est un peu différent, mais se traite de façon analogue). Soit J le schéma en groupes fini et plat sur $\mathbf{Z}_p$ prolongeant le schéma sur $\mathbf{Q}_p$ défini par ρ_p (d'après [35], prop. 3.3.2, ce schéma est unique). Il résulte de (ii) que ρ_p est réductible, et il en est de même de J. D'où l'existence d'une suite exacte de schémas en groupes finis et plats sur $\mathbf{Z}_p$:

$$0 \to A \to J \to B \to 0, \tag{2.8.6}$$

où A et B sont des schémas en groupes finis et plats d'ordre p. De plus, (ii) impose que l'un de ces schémas soit étale, et que l'autre soit de type multiplicatif. Il existe donc une extension finie étale R de $\mathbf{Z}_p$ sur laquelle A ou B devient isomorphe au schéma étale constant $\mathbf{Z}/p\mathbf{Z}$, et B ou A au schéma μ_p des racines p-èmes de l'unité. Sur R, la suite exacte (2.8.6) devient:

$$0 \to \mathbf{Z}/p\mathbf{Z} \to J \to \mu_p \to 0$$

ou

$$0 \to \mu_p \to J \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

Dans le premier cas, on voit facilement que l'extension J est *scindée* (utiliser la composante connexe de l'élément neutre), i.e., isomorphe sur R à $\mathbf{Z}/p\mathbf{Z} \oplus \mu_p$; d'où (2.8.2), avec action triviale de I_p, ce qui entraîne bien $k = 2$. Dans le second cas, on constate (suite exacte de Kummer) que la classe de l'extension J est donnée par un élément $u \in R^*/R^{*p}$, d'où

$$\rho_p | I \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix},$$

et le corps K du n° 2.4 est égal à $K_t(u^{1/p})$; comme u est une unité, l'extension K/K_t est, soit non ramifiée, soit peu ramifiée, d'où encore $k = 2$ d'après (2.8.2). (Le fait que K/K_t ne soit pas très ramifiée peut aussi se déduire d'un résultat général de Fontaine, cf. [15], th. 1.)

Reste à prouver que $k = 2$ entraîne que ρ_p est finie en p. D'après la prop. 3, il y a deux cas à considérer:

(a) Celui où $\rho_p | I$ est donné par les deux caractères fondamentaux ψ et ψ'. Ce cas est traité dans Raynaud [35], th. 2.4.3.

(b) Celui où $\rho_p | I$ est de la forme $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$, avec action de I_p triviale ou peu ramifiée. On fait alors une construction directe, basée sur la classification des extensions de $\mathbf{Z}/p\mathbf{Z}$ par μ_p, cf. ci-dessus (de façon un peu plus précise, on commence par remplacer $\mathbf{Z}_p$ par une extension finie étale R convenable, on construit l'extension en question sur R, et l'on descend ensuite à $\mathbf{Z}_p$).

2.9. *Exemple de calcul de k: points de p-division d'une courbe elliptique semi-stable.* Soit E une courbe elliptique sur $\mathbf{Q}_p$, d'invariant modulaire j_E, et soit E_p le groupe des points de p-division de E. L'action de G_p sur E_p définit une représentation

$$\rho_p\colon G_p \to \mathrm{Aut}(E_p) \simeq \mathbf{GL}_2(\mathbf{F}_p).$$

Comme $\det \rho_p = \chi$, l'invariant k associé à ρ_p satisfait à:

$$k \equiv 2 \bmod(p-1). \tag{2.9.1}$$

Nous allons déterminer la valeur de k, en nous bornant au cas où E est *semi-stable*, i.e. a, soit bonne réduction, soit mauvaise réduction de type multiplicatif (cf. [41], n^{os} 1.11 et 1.12):

PROPOSITION 5. (i) *Si E a bonne réduction, on a $k = 2$.*
(ii) *Si E a mauvaise réduction de type multiplicatif, on a*

$$k = \begin{cases} 2 & \text{si } v_p(j_E) \text{ est divisible par } p \\ p+1 & \text{sinon.} \end{cases}$$

(Ici, et dans toute la suite, on note v_p la valuation p-adique, normalisée par la condition $v_p(p) = 1$.)

Lorsque E a bonne réduction, ρ_p est évidemment finie en p, et l'assertion (i) résulte de la prop. 4.

Lorsque E a mauvaise réduction de type multiplicatif, on utilise le modèle de Tate ([41], n° 1.12). Celui-ci montre que, après extension quadratique non ramifiée de $\mathbf{Q}_p$, on a une suite exacte de modules galoisiens

$$0 \to \mu_p \to E_p \to \mathbf{Z}/p\mathbf{Z} \to 0$$

d'où

$$\rho_p | I \simeq \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}.$$

Soit de plus q_E l'élément de $\mathbf{Q}_p^*$ défini par l'identité

$$j_E = q_E^{-1} + 744 + 196884 q_E + \ldots$$

On constate que l'extension K/K_t du n° 2.4 est $K = K_t(q_E^{1/p})$. Cette extension est donc très ramifiée si et seulement si $v_p(q_E)$ n'est pas divisible par p; comme $v_p(q_E) = -v_p(j_E)$, on en déduit bien (ii).

Remarques

(1) Supposons que l'on soit dans le cas (ii) avec $k = 2$, i.e. que E ait mauvaise réduction de type multiplicatif et que $v_p(j_E)$ soit divisible par p. Posons $m =$

$-v_p(j_E)/p$ et $u = p^{pm}j_E$, de sorte que u est une unité p-adique et que q_E est égal au produit de u^{-1} par la puissance p-ème d'un élément de K_t. On a alors $K = K_t(u^{1/p})$ et l'on voit que:

(a) si $u^{p-1} \equiv 1 \pmod{p^2}$, on a $K = K_t$ et $\rho_p|I \simeq \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}$;

(b) si $u^{p-1} \not\equiv 1 \pmod{p^2}$, on a $[K : K_t] = p$ et $\rho_p|I \simeq \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$.

Le cas (b) peut effectivement se présenter, contrairement à ce qui est affirmé dans [6], prop. 5.1.(3)(d).

(2) Des calculs analogues à ceux de la prop. 5 (mais plus compliqués) sont possibles lorsque E a mauvaise réduction de type additif. Je me borne à donner le résultat dans un cas particulier typique, celui où $p \equiv 1 \pmod 3$, et où l'équation minimale de E est de la forme

$$y^2 = x^3 + Ax + B,$$

avec $v_p(A) \geqslant 1$ et $v_p(B) = 1$ (type c_1 de Néron).

On trouve alors

$$\rho_p|I \simeq \begin{pmatrix} \chi^\beta & 0 \\ 0 & \chi^\alpha \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix},$$

avec $\alpha = (p-1)/6$ et $\beta = (5p+1)/6$.

Si $p > 7$, cela entraîne $k = 1 + p\alpha + \beta = 2 + (p-1)(p+5)/6$. Par contre, pour $p = 7$, on peut avoir, soit $k = 2 + (p-1)(p+5)/6 = 14$, soit $k = 2$, ce dernier cas survenant si $v_p(A) \geqslant 2$.

§3. Enoncé de la conjecture

3.1. *Rappels sur les formes paraboliques en caractéristique p.* Soient:

N un entier $\geqslant 1$, premier à p;

k un entier $\geqslant 2$;

ε un caractère $(\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$.

Supposons que:

$$(3.1.1) \qquad \begin{cases} (-1)^k = \varepsilon(-1) & \text{si } p \neq 2 \\ k \text{ est pair} & \text{si } p = 2. \end{cases}$$

Nous aurons à utiliser la notion de *forme parabolique de type* (N, k, ε) *à coefficients dans* $\overline{\mathbf{F}}_p$. Comme plusieurs définitions sont possibles (cf. [23] et [24] par exemple), il convient de préciser ce que nous entendons par là:

Identifions $\overline{\mathbf{Q}}$ à un sous-corps de $\mathbf{C}$, et choisissons une place de $\overline{\mathbf{Q}}$ au-dessus de p. Si $\overline{\mathbf{Z}}$ désigne l'anneau des entiers de $\overline{\mathbf{Q}}$, le choix de la place en question définit

un homomorphisme $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_p$ que nous noterons $z \mapsto \tilde{z}$. Notons enfin

$$\varepsilon_0 \colon (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{Z}}^*$$

le relèvement multiplicatif de ε, i.e., l'unique caractère à valeurs dans les racines de l'unité d'ordre premier à p tel que

$$\varepsilon_0(x)^{\sim} = \varepsilon(x) \quad \text{pour tout } x \in (\mathbf{Z}/N\mathbf{Z})^*.$$

D'après (3.1.1), on a $\varepsilon_0(-1) = (-1)^k$. On peut donc parler des *formes paraboliques de type* (k, ε_0) *sur* $\Gamma_0(N)$, au sens usuel. Rappelons (cf. par exemple [11]) qu'une telle forme est une série

$$F = \sum_{n \geqslant 1} A_n q^n \qquad (q = e^{2\pi i z}), \tag{3.1.2}$$

convergeant dans le demi-plan $\mathrm{Im}(z) > 0$ et satisfaisant aux deux conditions suivantes:

(a) $F((az + b)/(cz + d)) = \varepsilon_0(d)(cz + d)^k F(z)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ et tout $z \in \mathbf{C}$ tel que $\mathrm{Im}(z) > 0$;

(b) F s'annule aux pointes, i.e., pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$, la fonction

$$z \mapsto (cz + d)^{-k} F((az + b)/(cz + d))$$

a un développement en série du type (3.1.2), avec q remplacé par $q^{1/N}$.

Pour abréger, nous dirons qu'une telle forme F est *de type* (N, k, ε_0).

Nous pouvons maintenant définir la notion analogue en caractéristique p:

DÉFINITION. *Une forme parabolique de type* (N, k, ε) *à coefficients dans* $\overline{\mathbf{F}}_p$ *est une série formelle*

$$f = \sum_{n \geqslant 1} a_n q^n, \qquad a_n \in \overline{\mathbf{F}}_p,$$

telle qu'il existe une forme parabolique

$$F = \sum_{n \geqslant 1} A_n q^n, \qquad A_n \in \overline{\mathbf{Z}},$$

de type (N, k, ε_0) *au sens rappelé ci-dessus, qui est telle que* $\tilde{F} = f$, *i.e., que* $\tilde{A}_n = a_n$ *pour tout* n.

(Au lieu de supposer que les A_n appartiennent à $\overline{\mathbf{Z}}$, on pourrait se borner à demander qu'ils appartiennent à l'*anneau local* de la place de $\overline{\mathbf{Q}}$ choisie au début. Cela ne changerait rien.)

Notons $S(N, k, \varepsilon)$ l'espace des f du type ci-dessus. Cet espace jouit des propriétés suivantes:

(3.1.3) $S(N, k, \varepsilon)$ ne dépend pas du choix de la place p-adique de $\overline{\mathbf{Q}}$ utilisée pour le définir. De plus, sa dimension sur $\overline{\mathbf{F}}_p$ est égale à la dimension de l'espace analogue $S(N, k, \varepsilon_0)$ sur $\mathbf{C}$.

Cela résulte de Shimura [51], th. 3.52 (voir aussi [11], prop. 2.7).

(3.1.4) $S(N, k, \varepsilon)$ est stable sous l'action des opérateurs de Hecke:

$$T_l\colon \sum a_n q^n \mapsto \sum a_{ln} q^n + \varepsilon(l) l^{k-1} \sum a_n q^{ln} \qquad (l \nmid pN),$$

$$U_l\colon \sum a_n q^n \mapsto \sum a_{ln} q^n \qquad (l \mid pN).$$

Pour les T_l et les U_l (l premier $\neq p$), cela résulte des propriétés analogues en caractéristique zéro. Pour U_p, il faut noter que c'est la réduction (mod p) de l'opérateur de Hecke

$$T_p\colon \sum a_n q^n \mapsto \sum a_{pn} q^n + \varepsilon_0(p) p^{k-1} \sum a_n q^{pn},$$

grâce à l'hypothèse $k \geqslant 2$.

(3.1.5) Les opérateurs de Hecke commutent entre eux. Si

$$f = \sum a_n q^n, \qquad f \neq 0,$$

est une fonction propre de ces opérateurs, on peut multiplier f par un scalaire non nul de telle sorte que $a_1 = 1$. Une fois f ainsi normalisée, on a $T_l(f) = a_l f$ pour $l \nmid pN$ et $U_l(f) = a_l f$ pour $l \mid pN$: les a_l sont les valeurs propres des T_l et U_l. De plus, la série formelle de Dirichlet

$$L_f(s) = \sum a_n n^{-s} \quad \left(\text{à coefficients dans } \overline{\mathbf{F}}_p\right)$$

est donnée par le produit eulérien usuel:

$$L_f(s) = \prod_{l \mid pN} \left(1 - a_l l^{-s}\right)^{-1} \prod_{l \nmid pN} \left(1 - a_l l^{-s} + \varepsilon(l) l^{k-1} l^{-2s}\right)^{-1}.$$

En particulier, f est déterminée par les a_l.

(3.1.6) Si $f = \sum a_n q^n$ est une fonction propre des opérateurs de Hecke normalisée comme ci-dessus, il existe une forme parabolique $F = \sum A_n q^n$ de type (N, k, ε_0) à coefficients dans $\overline{\mathbf{Z}}$, qui est fonction propre des $T_l (l \nmid N)$ et des $U_l (l \mid N)$ et vérifie:

$$A_1 = 1; \qquad \tilde{F} = f.$$

En effet, du fait que les opérateurs T_l et U_l commutent entre eux, tout système commun de valeurs propres de ces opérateurs dans $\overline{\mathbf{F}}_p$ se relève en caractéristique 0 (cf. par exemple [11], lemme 6.11). On déduit de là qu'il existe une forme parabolique $F = \Sigma\, A_n q^n$, de type (N, k, ε_0), fonction propre des T_l et des U_l, normalisée, et telle que $\tilde{A}_l = a_l$ pour tout nombre premier l. Il est alors immédiat que $\tilde{F} = f$.

(Bien entendu, il n'y a pas unicité de F: deux fonctions propres différentes en caractéristique 0 peuvent avoir la même réduction en caractéristique p.)

(3.1.7) Soit $f = \Sigma\, a_n q^n$ comme ci-dessus. D'après un théorème de Deligne ([11], th. 6.7), il existe une représentation continue semi-simple

$$\rho_f \colon G_{\mathbf{Q}} \to \mathbf{GL}_2\left(\overline{\mathbf{F}}_p\right)$$

caractérisée (à conjugaison près) par la propriété suivante:

(D). Pour tout nombre premier l ne divisant pas pN, la représentation ρ_f est non ramifiée en l, et, si l'on note $\rho_f(\mathrm{Frob}_l)$ l'élément de Frobenius correspondant (défini à conjugaison près), on a

$$\mathrm{Tr}\,\rho_f(\mathrm{Frob}_l) = a_l \tag{3.1.8}$$

et

$$\det \rho_f(\mathrm{Frob}_l) = \varepsilon(l) l^{k-1}. \tag{3.1.9}$$

La formule (3.1.9) peut être récrite avec les notations du n° 1.3 sous la forme

$$\det \rho_f = \varepsilon \cdot \chi^{k-1}. \tag{3.1.10}$$

Compte tenu de (3.1.1) elle entraîne que $\det \rho_f(c) = -1$, autrement dit que $\det \rho_f$ est un caractère *impair*.

Remarque. J'ai supposé au début que le niveau est premier à p. En fait, ce n'est pas nécessaire: tous les résultats énoncés restent vrais dans le cas général. Toutefois, cette généralité accrue ne procure pas de "formes mod p" vraiment nouvelles; on sait en effet que toute forme parabolique à coefficients dans $\overline{\mathbf{F}}_p$ qui est de niveau $p^m N$ est aussi de niveau N, à condition de remplacer le poids par un poids plus grand. Un exemple typique est celui des formes de poids 2 et de niveau p, qui sont aussi de poids $p+1$ et de niveau 1, cf. [43], th. 11.

3.2. *Les diverses variantes de la conjecture.* Revenons aux notations du §1, et soit

$$\rho \colon G_{\mathbf{Q}} \to \mathbf{GL}(V) \simeq \mathbf{GL}_2\left(\overline{\mathbf{F}}_p\right)$$

un homomorphisme continu, V étant un $\overline{\mathbf{F}}_p$-espace vectoriel de dimension 2. On

suppose que:

(3.2.1) ρ *est irréductible*,

et

(3.2.2) $\det \rho$ *est impair*, cf. (1.3.8).

La *conjecture* affirme que ρ est alors du type ρ_f de (3.1.7). Autrement dit:

(3.2.3$_?$) *Il existe une forme parabolique* f (de type convenable) *à coefficients dans* $\overline{\mathbf{F}}_p$ *qui est fonction propre des opérateurs de Hecke, et dont la représentation* ρ_f *associée est isomorphe à la représentation* ρ *donnée.*

Il convient de préciser (3.2.3$_?$) en donnant le type (N, k, ε) de f:

(3.2.4$_?$) *La forme parabolique* f *de* (3.2.3$_?$) *peut être choisie de type* (N, k, ε), *où* N, k *et* ε *sont les invariants de* ρ *définis au* §1 *et au* §2.

Si $f = \sum a_n q^n$ est normalisée ($a_1 = 1$), le fait que ρ_f soit isomorphe à ρ se traduit par les égalités

$$\text{(3.2.5)} \qquad \operatorname{Tr}(\operatorname{Frob}_{l,\rho}) = a_l \quad \text{et} \quad \det(\operatorname{Frob}_{l,\rho}) = \varepsilon(l) l^{k-1},$$

égalités qui doivent être valables pour tout nombre premier l ne divisant pas pN. (Il suffit d'ailleurs que la première égalité de (3.2.5) ait lieu pour un ensemble de l de densité 1.)

En ce qui concerne les a_l, pour l divisant pN, on peut conjecturer ceci:

(3.2.6$_?$) *Supposons que* $f = \sum a_n q^n$ *satisfasse à* (3.2.3$_?$) *et* (3.2.4$_?$) *et soit normalisée. Soit* l *un diviseur premier de* pN. *Alors*:

(a) *Si* $a_l \neq 0$, *il existe une droite* D *de* V *stable par le groupe de décomposition en* l (*relativement à une place* l*-adique donnée de* $\overline{\mathbf{Q}}$) *et telle que le groupe d'inertie en* l *opère trivialement sur* V/D. (*En d'autres termes, la restriction de* ρ *au groupe de décomposition en* l *a un quotient étale de dimension* 1.)

De plus, a_l *est égal à la valeur propre de la substitution de Frobenius en* l, *opérant sur* V/D.

(b) *Si* $a_l = 0$, *il n'existe aucune droite de* V *ayant les propriétés énoncées en* (a).

Remarques sur (3.2.6$_?$)

(1) Si l divise N, il existe au plus une droite D de V satisfaisant à (a). En effet, s'il en existait deux, ρ serait étale en l, et l ne diviserait pas le conducteur N.

On voit donc que, dans ce cas, a_l est déterminé sans ambiguïté par ρ.

[Il n'est pas difficile de prouver que D existe si et seulement si:

ou bien $v_l(N) = 1$, v_l désignant la valuation l-adique;

ou bien $v_l(N) = v_l(\text{cond. } \varepsilon) \geqslant 2$, où cond.$\varepsilon$ désigne le conducteur du caractère ε.

De plus, dans le cas où $v_l(N) = 1$ et $v_l(\text{cond.}\varepsilon) = 0$, on peut montrer que la valeur propre λ de la substitution de Frobenius en l opérant sur V/D est telle

que $\lambda^2 = \varepsilon_{\text{prim}}(l)l^{k-2}$, où $\varepsilon_{\text{prim}}$ est le caractère primitif défini par ε. D'après $(3.2.6_?)$ on aurait alors

$$a_l^2 = \varepsilon_{\text{prim}}(l)l^{k-2},$$

en parfait accord avec [27], th. 3 (iii).]

(2) Si $l = p$ et si ρ est ramifiée en p, la situation est la même que si l divise N: la droite D, si elle existe, est unique; la valeur propre a_p est déterminée sans ambiguïté. D'où *l'unicité* de la forme f dans ce cas; ses coefficients appartiennent au corps de rationalité de ρ, et engendrent ce corps sur $\mathbf{F}_p$.

(3) Si $l = p$ et si ρ est non ramifiée en p (ce qui entraîne $k = p$ d'après nos conventions, cf. n° 2.3), la situation est différente. Il y a alors deux valeurs possibles pour a_p, à savoir les deux valeurs propres λ et μ de la substitution de Frobenius en p; on a d'ailleurs $\lambda\mu = \varepsilon(p)$. Bien entendu, on peut avoir $\lambda = \mu$, auquel cas a_p est déterminé sans ambiguïté. Lorsque $\lambda \neq \mu$, dans tous les cas que je connais, il y a *deux* formes paraboliques f distinctes telles que $\rho_f \sim \rho$, l'une avec $a_p = \lambda$ et l'autre avec $a_p = \mu$. On notera que λ et μ n'appartiennent pas nécessairement au corps de définition de ρ (qui est engendré par les a_l, pour $l \neq p$): ils peuvent être quadratiques sur ce corps; on en verra des exemples au n° 5.1.

(4) Il devrait être possible de préciser $(3.2.6_?)$ en déterminant l'action sur f des opérateurs de symétrie W_l $(l|N)$ d'Atkin-Lehner-Li [3]. Les pseudo-valeurs propres correspondantes (au sens de [3]) peuvent sans doute s'écrire en termes des *constantes locales* de ρ (Deligne [9], §6).

Remarques sur $(3.2.4_?)$

(5) Il est probable que N et k sont *minimaux* pour ρ, autrement dit que, si ρ est isomorphe à $\rho_{f'}$, avec f' de type (N', k', ε'), N' premier à p, $k' \geqslant 2$, alors N' est multiple de N et k' est $\geqslant k$. En particulier, si l'on écrit f sous la forme $\tilde{F}$ comme dans (3.1.6), F doit être une forme *primitive* ("newform" cf. [11], [27]) de type (N, k, ε_0).

(6) Au lieu de définir les formes paraboliques à coefficients dans $\overline{\mathbf{F}}_p$ par réduction à partir de la caractéristique 0, comme nous l'avons fait, nous aurions pu utiliser la définition de Katz [23], qui conduit à un espace *a priori* plus grand,[2] donc donne peut-être davantage de représentations ρ_f. Il serait intéressant de voir si les représentations supplémentaires ainsi obtenues peuvent être irréductibles; je n'en connais aucun exemple (pour $k \geqslant 2$), mais, si cela se produisait, il y aurait lieu de modifier $(3.2.4_?)$ et $(3.2.6_?)$. Il serait également intéressant d'étudier de ce

[2] La définition de Katz jouit de la propriété agréable suivante: toute forme de poids k est aussi de poids $k + p - 1$. Avec la définiton adoptée ici, cet énoncé est vrai pour $p \geqslant 5$, mais est faux pour $p = 2$ ou 3.

point de vue le cas $k = 1$, que nous avons exclu jusqu'ici; peut-être la définition de Katz donne-t-elle alors beaucoup plus de représentations ρ_f?

3.3 *Exemple* $k = 2$. Nous allons appliquer les conjectures du numéro précédent à une représentation

$$\rho\colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_p)$$

telle que:

(a) $\det \rho = \chi$;

(b) ρ est absolument irréductible (i.e., irréductible sur $\overline{\mathbf{F}}_p$);

(c) ρ est finie en p, au sens du n° 2.8.

[Lorsque $p \neq 2$, on peut remplacer (b) par la condition suivante, en apparence plus faible:

(b′) ρ est irréductible (sur $\mathbf{F}_p$).

En effet, (a) entraîne que $\det \rho$ est impair, donc que les valeurs propres de $\rho(c)$ sont $+1$ et -1; du fait que $p \neq 2$, ces valeurs propres sont distinctes. Si alors ρ se décomposait sur $\overline{\mathbf{F}}_p$ en somme directe de deux représentations de dimension 1, cette décomposition ne pourrait être que celle donnée par les vecteurs propres de $\rho(c)$, donc serait rationnelle sur $\mathbf{F}_p$, ce qui contredirait (b′).]

Soient N, k et ε les invariants de ρ. D'après le n° 1.3, on a $\varepsilon = 1$, et d'après la prop. 4 du n° 2.8, on a $k = 2$. La conjecture $(3.2.4_?)$ donne alors:

$(3.3.1_?)$ *Il existe une forme parabolique f de poids 2 et de niveau N, à coefficients dans $\overline{\mathbf{F}}_p$, qui est fonction propre des opérateurs de Hecke et dont la représentation ρ_f associée est isomorphe à ρ.*

D'après $(3.2.6_?)$, cette forme parabolique est à coefficients dans $\mathbf{F}_p$, sauf peut-être si ρ est non ramifiée en p (ce qui ne peut se produire que si $p = 2$).

On peut reformuler $(3.3.1_?)$ en termes de la jacobienne $J_0(N)$ de la courbe modulaire $X_0(N)$ associée au groupe $\Gamma_0(N)$:

$(3.3.2_?)$ *La représentation ρ intervient comme quotient de Jordan-Hölder dans la représentation de $G_{\mathbf{Q}}$ sur les points de p-division de $J_0(N)$.*

3.4. *Questions.* En voici deux, l'une pour pessimistes, l'autre pour optimistes:

(1) Comment construire des contre-exemples aux conjectures du n° 3.2? J'ai fait de nombreux essais dans cette direction. Tous ces essais ont échoué, comme on le verra au §5.

(2) Peut-on reformuler ces conjectures dans le cadre d'une théorie des représentations (mod p) des groupes adéliques? Autrement dit, existe-t-il une "philosophie de Langlands modulo p", comme le demandent Ash et Stevens dans [2]? Si oui, cela permettrait peut-être:

de donner une définition plus naturelle du poids k attaché à ρ;

de remplacer $\mathbf{GL}_2$ par $\mathbf{GL}_N$, ou même par un groupe réductif;

de remplacer $\mathbf{Q}$ par d'autres corps globaux.

§4. Applications. Ces applications concernent:

l'équation de Fermat et ses variantes (n^{os} 4.1 à 4.3);
les discriminants des courbes elliptiques semi-stables (n^{o} 4.4);
la structure des schémas en groupes de type (p, p) sur $\mathbf{Z}$ (n^{o} 4.5);
la conjecture de Taniyama-Weil, et son extension aux variétés abéliennes à multiplications réelles (n^{os} 4.6 et 4.7);
la cohomologie des variétés projectives lisses sur $\mathbf{Q}$ ayant un nombre de Betti égal à 2 en dimension impaire (n^{o} 4.8).

Excepté la dernière, ces applications n'utilisent la conjecture $(3.2.4_?)$ que dans le cas où $\varepsilon = 1$, $k = 2$, cf. n^{o}. 3.3.

4.1. *Rappels sur certaines courbes elliptiques sur* $\mathbf{Q}$. Soient A, B, C trois entiers non nuls, premiers entre eux deux à deux, et tels que

$$A + B + C = 0.$$

Choisissons des nombres entiers x_1, x_2, x_3 tels que

$$x_1 - x_2 = A,\ x_2 - x_3 = B,\ x_3 - x_1 = C.$$

La courbe elliptique d'équation

$$y^2 = (x - x_1)(x - x_2)(x - x_3)$$

est indépendante du choix des x_i, à isomorphisme près. Pour fixer les idées, nous prendrons $x_1 = A$, $x_2 = 0$, $x_3 = -B$, de sorte que l'équation ci-dessus s'écrit

$$y^2 = x(x - A)(x + B). \tag{4.1.1}$$

Nous noterons $E_{A,B,C}$, ou simplement E, la courbe ainsi définie.

Remarque. Une permutation de A, B, C de signature 1 (resp. -1) ne change pas E (resp. change E en sa "tordue" par l'extension quadratique $\mathbf{Q}(\sqrt{-1})/\mathbf{Q}$).

Donnons maintenant quelques propriétés de *mauvaise réduction* de E (cf. Frey [17]).

(4.1.2) *Mauvaise réduction en* $l \neq 2$. Soit l un nombre premier $\neq 2$. La courbe E a mauvaise réduction en l si et seulement si l divise ABC, et cette mauvaise réduction est alors *de type multiplicatif*.

C'est immédiat sur (4.1.1). On notera également que cette équation fournit un *modèle minimal* de E en l, cf. Tate [4], p. 47.

(4.1.3) *Mauvaise réduction en* 2. Nous nous bornerons au cas où:

$$A \equiv -1 \pmod 4 \quad \text{et} \quad B \equiv 0 \pmod{32}. \tag{4.1.4}$$

En faisant le changement de variables

$$x = 4X, \qquad y = 8Y + 4X,$$

on transforme (4.1.1) en l'équation

(4.1.5)

$$Y^2 + XY = X^3 + cX^2 + dX, \quad \text{avec } c = (B - 1 - A)/4,\ d = -AB/16,$$

dont la réduction (mod 2) est:

$$Y^2 + XY = \begin{cases} X^3 & \text{si } A \equiv 7 \pmod 8 \\ X^3 + X^2 & \text{si } A \equiv 3 \pmod 8. \end{cases}$$

On obtient ainsi une cubique sur $\mathbf{F}_2$ qui a un point double en $(0,0)$ à tangentes distinctes (ces tangentes étant rationnelles sur $\mathbf{F}_2$ si et seulement si $A \equiv 7 \pmod 8$). Il en résulte que E a *mauvaise réduction de type multiplicatif en* 2 (Tate, *loc. cit.*) et que (4.1.5) est une *équation minimale* en 2, donc aussi sur $\mathrm{Spec}(\mathbf{Z})$ d'après ce qu'on vient de voir. Le discriminant Δ correspondant est:

$$\Delta = 2^{-8}A^2B^2C^2. \tag{4.1.6}$$

Ainsi, E a partout, soit bonne réduction, soit mauvaise réduction de type multiplicatif: c'est une courbe *semi-stable*. Son *conducteur* est donné par:

$$\mathrm{cond}(E) = \mathrm{rad}(ABC), \tag{4.1.7}$$

où $\mathrm{rad}(X)$ désigne le produit des nombres premiers qui divisent X (i.e., le plus grand diviseur sans facteur carré de X).

L'invariant modulaire j_E de E est:

$$j_E = 2^8(C^2 - AB)^3/A^2B^2C^2. \tag{4.1.8}$$

Si l divise ABC, on a:

$$v_l(j_E) = -v_l(\Delta) = \begin{cases} -2v_l(ABC) & \text{si } l \neq 2 \\ 8 - 2v_2(ABC) & \text{si } l = 2. \end{cases} \tag{4.1.9}$$

Points de p-division de E. Soit p un nombre premier $\geqslant 5$. Nous nous intéresserons à la représentation

$$\rho_p^E \colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_p)$$

fournie par les points de p-division de E.

On a tout d'abord:

PROPOSITION 6. *La représentation ρ_p^E est irréductible.*

(Comme son déterminant est égal au caractère cyclotomique χ, cette représentation est même *absolument irréductible*, cf. n° 3.3.)

Supposons que ρ_p^E soit réductible, i.e. que E contienne un sous-groupe X d'ordre p qui soit rationnel sur $\mathbf{Q}$. Du fait que E est semi-stable, l'action de $G_{\mathbf{Q}}$ sur X se fait, soit par le caractère unité, soit par le caractère χ ([41], p. 307). Dans le premier cas, E a un point d'ordre p rationnel sur $\mathbf{Q}$; comme les points d'ordre 2 de E sont également rationnels sur $\mathbf{Q}$, l'ordre du groupe de torsion de $E(\mathbf{Q})$ est $\geqslant 4p \geqslant 20$, ce qui contredit un théorème de Mazur ([28], th. 8). Dans le second cas, la courbe $E' = E/X$ a un point d'ordre p rationnel sur $\mathbf{Q}$, et on lui applique le même argument que ci-dessus.

Remarque. Au lieu d'utiliser le th. 8 de [28], on aurait pu se servir des résultats plus généraux de Mazur [29].

On va maintenant déterminer les *invariants* (N, k, ε) attachés à ρ_p^E:

(4.1.10) Comme $\det \rho_p^E = \chi$, on a $\varepsilon = 1$.

(4.1.11) *On a $k = 2$ si $v_p(\Delta)$ est divisible par p* (i.e., si $v_p(ABC)$ est divisible par p), *et $k = p + 1$ dans le cas contraire.* Cela résulte de la prop. 5 du n° 2.9, compte tenu du fait que E est semi-stable.

(4.1.12) *Le conducteur N de ρ_p^E est égal au produit des nombres premiers $l \neq p$ tels que $v_l(\Delta)$ ne soit pas divisible par p.*

C'est là une propriété générale des courbes semi-stables, qui se vérifie immédiatement sur les modèles de Tate "$\mathbf{G}_m/q^{\mathbf{Z}}$".

Remarque. Vu (4.1.6), la condition "$v_l(\Delta)$ n'est pas divisible par p" est équivalente à:

$$(4.1.13) \qquad v_l(ABC) \not\equiv \begin{cases} 0 & (\mathrm{mod}\ p) \quad \text{si } l \neq 2 \\ 4 & (\mathrm{mod}\ p) \quad \text{si } l = 2. \end{cases}$$

4.2. *Le théorème de Fermat.* Soit p un nombre premier $\geqslant 5$.

THÉORÈME 1. *Admettons* (3.3.1$_?$). *L'équation*

$$a^p + b^p + c^p = 0$$

n'a alors aucune solution avec $a, b, c \in \mathbf{Z}$, $abc \neq 0$.

Soit (a, b, c) une telle solution. Quitte à faire une homothétie, ainsi qu'une permutation, on peut supposer que a, b et c sont premiers entre eux, et que $b \equiv 0 \pmod 2$, $a \equiv -1 \pmod 4$. Si l'on pose

$$A = a^p, \qquad B = b^p, \qquad C = c^p,$$

les conditions (4.1.4) du n° 4.1 sont satisfaites. Soit $E = E_{A,B,C}$ la courbe elliptique correspondante, et soit ρ_p^E la représentation de $G_{\mathbf{Q}}$ fournie par ses points de p-division. Par construction, on a

$$v_l(ABC) \equiv 0 \pmod{p} \quad \text{pour tout } l \text{ premier.}$$

Il en résulte, d'après (4.1.11) et (4.1.13), que les invariants k et N attachés à ρ_p^E sont égaux à 2. De plus ρ_p^E est irréductible (prop. 6). La conjecture $(3.3.1_?)$ affirme alors que ρ_p^E est isomorphe à la représentation ρ_f associée à une forme parabolique normalisée f, de poids 2 et de niveau 2, à coefficients dans $\overline{\mathbf{F}}_p$. Mais une telle forme n'existe pas: la courbe modulaire $X_0(2)$ est de genre 0. D'où le théorème.

Remarque. La relation existant entre "solutions de l'équation de Fermat" et "points de p-division de certaines courbes elliptiques" figure déjà dans un travail de Hurwitz ([20]) datant de 1886.

Elle a été utilisée depuis par différents auteurs, notamment Hellegouarch [19], Vélu [54] et Frey [16], [17]. La méthode suivie ici est tirée de Frey [17].

4.3. *Variantes du théorème de Fermat.* Soit p un nombre premier $\geqslant 11$.

THÉORÈME 2. *Admettons* $(3.3.1_?)$. *Soit L un nombre premier $\neq p$ appartenant à l'ensemble*

$$S = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\},$$

et soit α un entier $\geqslant 0$. L'équation

$$a^p + b^p + L^\alpha c^p = 0 \tag{4.3.1}$$

n'a alors aucune solution avec $a, b, c \in \mathbf{Z}$ et $abc \neq 0$.

On procède comme pour le th. 1. Tout d'abord, on peut évidemment supposer que $0 < \alpha < p$. Soit alors (a, b, c) une solution de l'équation (4.3.1), avec a, b, c premiers entre eux. On prend pour A, B, C les trois entiers a^p, b^p, $L^\alpha c^p$ (qui sont premiers entre eux, comme on le vérifie tout de suite), à une permutation près choisie de telle sorte que B soit pair (donc divisible par 2^p et *a fortiori* par 32) et $A \equiv -1 \pmod 4$. On considère la représentation ρ_p^E attachée à la courbe elliptique $E = E_{A,B,C}$. D'après (4.1.11) et (4.1.13) les invariants k et N de cette représentation sont $k = 2$ et $N = 2L$ (noter que L a été supposé distinct de p). D'après $(3.3.1_?)$, il existe alors une forme parabolique

$$f = q + a_2(f)q^2 + \cdots + a_n(f)q^n + \cdots$$

à coefficients dans $\overline{\mathbf{F}}_p$, de poids 2 et de niveau $2L$, fonction propre des opérateurs de Hecke, et telle que la représentation ρ_f associée soit isomorphe à ρ_p^E. Nous

allons voir que ceci est impossible. C'est clair pour $L = 3, 5$ puisqu'aucune f n'existe dans ce cas: les courbes modulaires $X_0(6)$ et $X_0(10)$ sont de genre 0. On peut donc supposer $L \geqslant 7$.

LEMME 1. (*a*) *La forme f est la réduction en caractéristique p d'une forme primitive F de niveau $2L$ en caractéristique* 0.

(b) *On a* $a_3(f) = 0$ *ou* ± 4.

(c) *On a* $a_5(f) = \pm 2$ *ou* ± 6.

D'après (3.1.6), on a $f = \tilde{F}$, où F est une forme parabolique de poids 2 et de niveau $2L$, à coefficients dans $\overline{\mathbf{Z}}$, qui est fonction propre normalisée des opérateurs de Hecke. Si F n'était pas primitive, elle proviendrait du niveau L et la représentation ρ_f ne serait pas ramifiée en 2. Or ρ_p^E est ramifiée en 2, puisque son conducteur est $2L$. D'où (a).

Pour prouver (b) on distingue deux cas:

(b_1) *La courbe E a bonne réduction en* 3, *i.e.*, $ABC \not\equiv 0 \pmod 3$.

Soit $\tilde{E}$ la réduction de E en 3. C'est une courbe elliptique sur $\mathbf{F}_3$ dont les points d'ordre 2 sont rationnels. Le nombre de points rationnels de $\tilde{E}$ est donc divisible par 4. Comme ce nombre est compris entre $1 + 3 - 2\sqrt{3}$ et $1 + 3 + 2\sqrt{3}$, il est égal à 4. Cela signifie que la trace de l'endomorphisme de Frobenius de $\tilde{E}$ est égale à 0. D'où $a_3(f) = 0$ (dans $\mathbf{F}_p$), d'après (3.1.8).

(b_2) *La courbe E a mauvaise réduction en* 3.

On a vu que cette mauvaise réduction est de type multiplicatif. Si elle est déployée (i.e., si E est isomorphe sur $\mathbf{Q}_3$ à une courbe de Tate), le $G_{\mathbf{Q}_3}$-module galoisien E_p est extension de $\mathbf{Z}/p\mathbf{Z}$ par μ_p; les valeurs propres de l'endomorphisme de Frobenius en 3 sont donc 1 et 3; leur somme est 4. D'où $a_3(f) = 4$ dans ce cas. Lorsque la réduction est non déployée, il y a une "torsion" quadratique, et l'on obtient $a_3(f) = -4$.

La démonstration de (c) est analogue à celle de (b): on trouve que $a_5(f) = \pm 2$ lorsque E a bonne réduction en 5, et $a_5(f) = \pm 6$ sinon.

LEMME 2. *Soit $L \in S$, avec $L \geqslant 7$, et soit*

$$F = q + A_2 q^2 + \cdots + A_n q^n + \cdots, \qquad A_n \in \overline{\mathbf{Z}},$$

une forme primitive normalisée de poids 2 *et de niveau $2L$. On a alors*:

$$A_3 = \pm 1, \pm 2 \text{ ou } \pm 3 \text{ si } L \neq 23$$

et

$$A_5 = 4 \text{ si } L = 23.$$

Cela se vérifie cas par cas:

L	7	13	17	19	29	53	59
valeurs de A_3	-2	$1, -3$	-2	$1, -1$	$-1, -3$	$1, -1, 2, -2$	$-1, -1, 2, 2.$

($L = 11$ ne figure pas dans ce tableau, car il n'y a pas de forme primitive de poids 2 pour le niveau 22.)

On peut maintenant achever la démonstration du th. 2. Tout d'abord, pour $L = 23$, la comparaison des lemmes 1 et 2 montre que l'on a

$$\pm 2 \text{ ou } \pm 6 \equiv 4 \pmod{p},$$

ce qui est impossible pour $p \geqslant 7$. De même, si $L \neq 23$, $L \in S$ et $L \geqslant 7$, on a

$$0 \text{ ou } \pm 4 \equiv \pm 1, \pm 2 \text{ ou } \pm 3 \pmod{p},$$

ce qui est impossible pour $p \geqslant 11$.

Remarques

(1) L'hypothèse $p \neq L$ n'est pas essentielle; elle a seulement servi à assurer que le poids k est égal à 2, ce qui a permis d'appliquer $(3.3.1_?)$. Si $p = L$, on a $k = p + 1$, $N = 2$, et les arguments utilisés ci-dessus restent valables, à condition d'admettre $(3.2.4_?)$ pour $k = p + 1$ et non plus pour $k = 2$.

(2) Il est possible que le th. 2 reste vrai pour $p = 5$ et $p = 7$. La question devrait pouvoir se traiter, sans utiliser aucune conjecture, par les méthodes traditionnelles de factorisation et de descente (cf. par exemple Dénes [12]).

(3) La plus petite valeur de L ne figurant pas dans l'ensemble S du th. 2 est $L = 31$ (qui est un nombre de Mersenne–cf. ci-dessous). Pour cette valeur, la méthode suivie conduit à une représentation ρ_p^E qui pourrait, par exemple, être isomorphe à celle fournie par la forme primitive F de niveau 62 suivante:

$$F = q + q^2 + q^4 - 2q^5 + q^8 + \ldots$$

Je ne vois pas comment tirer de là une contradiction, d'autant plus que l'équation $a^5 + b^5 + 31c^5 = 0$ a effectivement une solution, à savoir $(1, -2, 1)$ [cette solution conduit à la courbe E d'équation $y^2 = x(x + 1)(x - 32)$, qui est une courbe de Weil de niveau 62 correspondant à F.]

Je ne vois pas non plus comment attaquer les équations

$$a^p + b^p + 15c^p = 0 \quad \text{et} \quad a^p + 3b^p + 5c^p = 0,$$

pour lesquelles le conducteur N est égal à 30.

(4) Si l'on fixe L, on peut se demander ce qui se passe pour p assez grand. Dans cette direction, Mazur m'a signalé le résultat suivant:

Admettons $(3.3.1_?)$. *Soit L un nombre premier* $\neq 2$ *qui ne soit ni un nombre de Fermat ni un nombre de Mersenne* (i.e. L ne peut pas s'écrire sous la forme

$2^n \pm 1$). *Il existe alors une constante C_L telle que, si $p \geqslant C_L$ et $\alpha \geqslant 0$, l'équation*

$$a^p + b^p + L^\alpha c^p = 0$$

n'a aucune solution avec $a, b, c \in \mathbf{Z}$ et $abc \neq 0$.

La démonstration est analogue à celle du th. 2; l'hypothèse faite sur L est utilisée pour montrer qu'il n'existe aucune courbe elliptique de conducteur $2L$ dont les trois points d'ordre 2 soient rationnels sur $\mathbf{Q}$.

4.4 *Discriminants des courbes elliptiques semi-stables.* La conjecture $(3.3.1_?)$ permettrait de répondre affirmativement à des questions de Brumer-Kramer ([6], §9):

PROPOSITION 7. *Admettons* $(3.3.1_?)$. *Soit E une courbe elliptique semi-stable sur $\mathbf{Q}$, et soit Δ le discriminant de son modèle minimal. Supposons que $|\Delta|$ soit une puissance p-ème. Alors E possède un sous-groupe d'ordre p rationnel sur $\mathbf{Q}$, et l'on a $p \leqslant 7$.*

Pour $p = 2$, on remarque que l'extension de $\mathbf{Q}$ engendrée par les points d'ordre 2 de E est non ramifiée en dehors de 2; son groupe de Galois ne peut donc être ni $\mathfrak{S}_3$ ni $\mathfrak{A}_3$, et cela montre que l'un de ces points est rationnel sur $\mathbf{Q}$. Pour $p = 3$, 5 ou 7, on applique un argument analogue (cf. [6], prop. 9.2). Il reste à prouver que le cas $p > 7$ est impossible. Or, si $p > 7$, la représentation ρ_p^E est irréductible (Mazur [29], th. 4). D'autre part, les hypothèses faites sur E entraînent que les invariants (N, k, ε) de ρ_p^E sont égaux à $(1, 2, 1)$. D'après $(3.3.1_?)$, ρ_p^E provient donc d'une forme parabolique normalisée de poids 2 et de niveau 1. Il y a contradiction: une telle forme n'existe pas.

PROPOSITION 8. *Admettons* $(3.3.1_?)$. *Soit E une courbe elliptique sur $\mathbf{Q}$ dont le conducteur est un nombre premier P. Soit $\Delta = \pm P^m$ le discriminant du modèle minimal de E. On a alors $m = 1$, sauf si E est une courbe de Setzer-Neumann, ou si $P = 11, 17, 19$ ou 37.*

Supposons $m > 1$. Il existe alors un nombre premier p qui divise m, et l'on peut appliquer la prop. 7. On en conclut d'abord que $p \leqslant 7$. Si $p = 2$, E a un point rationnel d'ordre 2, et c'est une courbe de Setzer-Neumann ([33], [50]), à moins que P ne soit égal à 17. Si $p = 3$, 5 ou 7, il existe une courbe isogène à E sur $\mathbf{Q}$ qui possède un point rationnel d'ordre p ([41], p. 307); d'après Miyawaki [32], cela est impossible pour $p = 7$ et cela entraîne $P = 11$ pour $p = 5$, et $P = 19$ ou 37 pour $p = 3$.

4.5. *Schémas en groupes de type (p, p) sur $\mathbf{Z}$.* Soit p un nombre premier $\geqslant 3$.

THÉORÈME 3. *Admettons* $(3.3.1_?)$. *Tout schéma en groupes fini et plat sur $\mathbf{Z}$, de type (p, p), est alors isomorphe à l'un des trois suivants*:

$$\mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}, \qquad \mathbf{Z}/p\mathbf{Z} \oplus \mu_p, \qquad \mu_p \oplus \mu_p.$$

Soit J un schéma en groupes fini et plat sur $\mathbf{Z}$, de type (p, p). On sait que J est étale sur $\mathrm{Spec}(\mathbf{Z}) - \{p\}$, donc définit une représentation

$$\rho: G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_p)$$

qui est non ramifiée en dehors de p. Comme $p \neq 2$, la connaissance de ρ détermine celle de J (Raynaud [35], prop. 3.3.2).

LEMME 3. *Si ρ est réductible, J est isomorphe à $\mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z} \oplus \mu_p$ ou $\mu_p \oplus \mu_p$.*

La réductibilité de ρ équivaut à l'existence d'une suite exacte

$$0 \to A \to J \to B \to 0,$$

où A et B sont des schémas en groupes finis et plats sur $\mathbf{Z}$, d'ordre p. D'après Oort-Tate [34], A et B sont isomorphes, soit à $\mathbf{Z}/p\mathbf{Z}$, soit à μ_p. Le lemme résulte alors de ce que toute extension de B par A est scindée (Fontaine [15], n° 3.4.3).

LEMME 4. *Si ρ est irréductible, on a* $\det \rho = \chi$.

Le caractère $\det \rho: G_{\mathbf{Q}} \to \mathbf{F}_p^*$ est non ramifié en dehors de p, donc de la forme χ^i, avec $0 \leqslant i \leqslant p-2$. Les résultats locaux de Raynaud [35] (cf. n° 2.8, démonstration de la prop. 4) montrent que les seules possibilités pour i sont $i = 0$, 1 et 2. De plus (*loc. cit.*) le cas $i = 0$ n'est possible que si J est étale en p, auquel cas ρ est non ramifiée partout, d'où $\rho = 1$ d'après Minkowski, ce qui contredit l'hypothèse que ρ est irréductible. De même, le cas $i = 2$ n'est possible que si le dual de J est étale en p, ce qui conduit à une contradiction par le même argument. On a donc $i = 1$, d'où le lemme.

Le th. 3 est maintenant immédiat. En effet, si ρ est réductible, on applique le lemme 3. Et, si ρ est irréductible, le lemme 4, joint à la prop. 4 du n° 2.8, montre que les invariants (N, k, ε) attachés à ρ sont $(1, 2, 1)$; d'où une contradiction avec $(3.3.1_?)$ par le même argument que celui utilisé dans la démonstration de la prop. 7.

Remarques

(1) Pour $p = 3$, 5, 7, 11, 13 ou 17, Fontaine [15] a démontré (sans utiliser aucune conjecture) un résultat plus général que le th. 3: tout schéma en groupes fini et plat sur $\mathbf{Z}$, de type $(p, \ldots, p)$, est somme directe de copies de $\mathbf{Z}/p\mathbf{Z}$ et de μ_p.

(2) Le th. 3 ne s'étend pas au cas $p = 2$: outre $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mu_2$ et $\mu_2 \oplus \mu_2$, il y a une quatrième possibilité, à savoir une certaine extension non scindée de $\mathbf{Z}/2\mathbf{Z}$ par μ_2. La représentation ρ correspondante s'écrit

$$\rho = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

où u: $G_{\mathbf{Q}} \to \mathbf{Z}/2\mathbf{Z}$ est l'homomorphisme de noyau $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(i))$. Ce schéma en groupes de type $(2,2)$ peut se réaliser comme celui des points de 2-division de la courbe elliptique

$$y^2 + xy + y = x^3 - x^2 - x - 14,$$

de conducteur 17 et de discriminant -17^4.

4.6. *La conjecture de Taniyama-Weil.* Soit E une courbe elliptique sur $\mathbf{Q}$, soit j_E son invariant modulaire, et soit N son conducteur.

THÉORÈME 4. *Admettons* $(3.3.1_?)$. *Alors E est une courbe de Weil de niveau N.*

(En particulier, E est isomorphe à un quotient de la jacobienne $J_0(N)$ de la courbe modulaire $X_0(N)$.)

Pour tout nombre premier p, notons ρ_p^E: $G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_p)$ la représentation de $G_{\mathbf{Q}}$ fournie par les points de p-division de E. On a

$$\det \rho_p^E = \chi. \tag{4.6.1}$$

De plus:

LEMME 5. *Il existe une constante C_E telle que, pour tout $p \geqslant C_E$, on ait:*
(4.6.2) *ρ_p^E est irréductible;*
(4.6.3) *le conducteur de ρ_p^E est égal à N.*

C'est là un résultat connu. En effet, d'après Mazur [29], (4.6.2) est vrai dès que $p > 163$. D'autre part la définition du conducteur de E en termes de représentations l-adiques (cf. [18], [40], [49]) montre que le conducteur N_p de ρ_p^E *divise* N (ce qui d'ailleurs suffirait pour la suite). De plus, si $p \geqslant 5$, on vérifie que $N_p = N$ si et seulement si p satisfait aux deux conditions suivantes:

(a) p ne divise pas N;

(b) pour tout l tel que $v_l(N) = 1$, p ne divise pas $v_l(j_E)$.

(Noter, à propos de b), que l'hypothèse $v_l(N) = 1$ signifie que E a mauvaise réduction de type multiplicatif en l, et l'on a donc $v_l(j_E) < 0$.)

Bornons-nous maintenant aux nombres premiers $p \geqslant C_E$. D'après $(3.3.1_?)$, ρ_p^E est isomorphe à la représentation ρ_{f_p} associée à une forme parabolique de poids 2 et de niveau N

$$f_p = \sum a_{n,p} q^n,$$

à coefficients dans $\overline{\mathbf{F}}_p$, qui est fonction propre normalisée des opérateurs de Hecke.

D'après (3.1.6), f_p se relève en caractéristique 0: il existe une forme parabolique de poids 2 et de niveau N

$$F = \sum A_n q^n,$$

à coefficients dans $\overline{\mathbf{Z}}$, qui est fonction propre normalisée des opérateurs de Hecke, et telle que $\tilde{F} = f_p$. *A priori*, F dépend de p. Mais il n'y a qu'un nombre fini de F

possibles, puisque le poids et le niveau sont fixés. On en conclut qu'il existe un choix de F tel que l'on ait

$$\tilde{F} = f_p$$

pour tout $p \in P$, où P est un ensemble infini de nombres premiers. Soit alors l un nombre premier ne divisant pas N. La courbe E a bonne réduction en l. Soit a_l la trace de l'endomorphisme de Frobenius correspondant. On a

$$a_l \equiv a_{l,p} \pmod{p} \quad \text{pour tout } p \neq l.$$

Il en résulte que l'entier algébrique $A_l - a_l$ *a une image dans* $\bar{\mathbf{F}}_p$ *qui est égale à* 0 *pour tout* $p \in P$, $p \neq l$. Comme P est infini, cela entraîne

$$A_l = a_l \quad \text{pour tout } l \nmid N. \tag{4.6.4}$$

En particulier, les A_l appartiennent à $\mathbf{Z}$. Ils définissent une *courbe de Weil* E_F de niveau un diviseur de N; d'après (4.6.4), les représentations l-adiques attachées à E et E_F sont isomorphes, et l'on sait (Faltings [13], [14]) que cela entraîne que E et E_F sont isogènes sur $\mathbf{Q}$. D'où le th. 4.

Remarques

(1) Le th. 4 m'a été suggéré par P. Colmez au Colloque de Luminy, en juin 1986. Jusque là, je ne m'étais pas rendu compte de l'étendue (à la fois intéressante et inquiétante) des conséquences des conjectures du §3.

(2) La forme F construite dans la démonstration ci-dessus est *primitive*; cela résulte d'un théorème de Carayol [8].

(3) La méthode suivie ici s'applique à d'autres questions du même genre. En voici un exemple, tiré de [52]:

Soit $K = \mathbf{Q}(\sqrt{D})$ un corps quadratique réel; notons σ l'involution de K. Soit E une courbe elliptique sur K, soit E^σ sa conjuguée, et soit λ: $E \to E^\sigma$ une isogénie telle que $\lambda^\sigma \circ \lambda = -c$, où c est un entier > 0. Shimura pose alors la question suivante ([52], p. 184): est-il vrai que E provienne (par la construction donnée dans [52]) d'une forme primitive de type $(N, 2, \varepsilon)$, où N est un entier convenable, et ε est le caractère quadratique associé à K? On peut montrer que la réponse est "oui" si l'on admet la conjecture $(3.2.4_?)$. La démonstration est analogue à celle du th. 4 (on travaille avec un système de représentations l-adiques qui est rationnel sur $\mathbf{Q}(\sqrt{-c})$, et dont le déterminant est le produit de ε et du caractère cyclotomique).

Pour d'autres exemples, voir les n^{os} 4.7 et 4.8 ci-après.

4.7. *Variétés abéliennes à multiplications réelles.* Soit X une variété abélienne sur $\mathbf{Q}$ de dimension $n \geqslant 1$. On dit que X est *à multiplication réelles* (cf. Ribet

[36]) si la $\mathbf{Q}$-algèbre $K_X = \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(X)$ est un corps de nombres algébriques totalement réel de degré n. On sait que de telles variétés apparaissent lorsqu'on décompose les jacobiennes $J_0(N)$ sous l'action des opérateurs de Hecke, cf. Shimura [51], §7.5. Réciproquement:

THÉORÈME 5. *Admettons* $(3.3.1_7)$. *Alors toute variété abélienne X sur $\mathbf{Q}$, à multiplications réelles, de dimension n, est isomorphe à un quotient de $J_0(N)$, où N est la racine n-ème du conducteur de X.*

La démonstration est analogue à celle du th. 4 (que l'on retrouve pour $n = 1$). Je me bornerai à en indiquer les grandes lignes. Tout d'abord:

(4.7.1) *La variété abélienne X définit un "système de représentations λ-adiques" de $G_{\mathbf{Q}}$, de degré 2, rationnel sur K_X; le déterminant de ce système est le caractère cyclotomique.*

Cela est expliqué dans Ribet [36].

Si X a bonne réduction en l, on notera a_l la trace de l'endomorphisme correspondant (dans le système λ-adique ci-dessus); c'est un entier du corps K_X.

(4.7.2) *Le conducteur de X est de la forme N^n, avec N entier $\geqslant 1$.*

La définition du conducteur donnée dans [18], exposé IX, §4 (voir aussi [40], n° 2.1) fait intervenir certains caractères locaux de degré $2n$, à valeurs dans $\mathbf{Q}$. Or on constate (comme pour (4.7.1) ci-dessus) que ces caractères peuvent s'écrire comme sommes des n conjugués de caractères de degré 2 à valeurs dans K_X. L'assertion (4.7.2) résulte facilement de là.

Fixons maintenant un plongement de K_X dans $\overline{\mathbf{Q}}$. Pour tout nombre premier p, on a choisi au n° 3.1 une place p-adique de $\overline{\mathbf{Q}}$, d'où une place λ_p de K_X. Si l'on suppose *p complètement décomposé* dans K_X, le corps résiduel de λ_p est $\mathbf{F}_p$; par réduction (mod λ_p), la représentation λ_p-adique correspondante définit une représentation

$$\rho_p^X \colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_p).$$

Les ρ_p^X jouissent des propriétés suivantes:

$$\det \rho_p^X = \chi. \tag{4.7.3}$$

Cela résulte de (4.7.1).

(4.7.4) *Si p est assez grand, ρ_p^X est irréductible.*

Cela résulte d'un théorème de Faltings ([14], p. 204), et cela peut aussi se voir par un argument élémentaire, analogue à celui que nous utiliserons au n° suivant pour démontrer le th. 6.

(4.7.5) *Si p est assez grand, le conducteur de ρ_p^X est N.*

Cela se vérifie au moyen des propriétés des modèles de Néron décrites dans [18], *loc. cit.* (Le fait que le conducteur de ρ_p^X soit un *diviseur* de N est nettement plus facile à démontrer, et serait suffisant pour la suite.)

(4.7.6) *Si p est assez grand, l'invariant k de ρ_p^X est égal à* 2.

Cela résulte de la prop. 4 du n° 2.8.

Une fois (4.7.3), ..., (4.7.6) établis, on peut appliquer ($3.3.1_?$). D'où, pour tout p assez grand et complètement décomposé dans K_X, une forme parabolique de poids 2 et de niveau N:

$$f_p = \sum a_{n,p} q^n,$$

à coefficients dans $\overline{\mathbf{F}}_p$, fonction propre normalisée des opérateurs de Hecke, telle que $\rho_p^X \simeq \rho_{f_p}$; on a en particulier

$$a_{l,p} = \tilde{a}_l \quad \text{pour tout } l \nmid N,\ l \neq p.$$

En relevant f_p en caractéristique zéro grâce à (3.1.6) on en déduit une forme parabolique de poids 2 et de niveau N:

$$F = \sum A_n q^n,$$

à coefficients dans $\overline{\mathbf{Z}}$, fonction propre normalisée des opérateurs de Hecke, et telle que $\tilde{F} = f_p$ pour tout $p \in P$, où P est un ensemble infini de nombres premiers complètement décomposés dans K_X. Si $l \nmid N$, on a donc

$$\tilde{A}_l = a_{l,p} = \tilde{a}_l \quad \text{pour tout } p \in P,\ p \neq l,$$

d'où $A_l = a_l$ puisque P est infini. Les systèmes de représentations λ-adiques définis par X et par F sont donc isomorphes. Le théorème en résulte d'après Faltings [13].

Remarque. Ici encore, F est *primitive*, cf. Carayol [8].

4.8. *Variétés projectives ayant un nombre de Betti égal à* 2 *en dimension impaire.* Soient:

X une variété projective lisse sur $\mathbf{Q}$;
$X_{\mathbf{C}} = X(\mathbf{C})$ la variété complexe définie par X;
m un entier impair $\geqslant 1$;
$H^m(X_{\mathbf{C}}, \mathbf{C})$ le m-ème groupe de cohomologie de $X_{\mathbf{C}}$, à coefficients complexes.

Faisons les deux hypothèses suivantes:

(4.8.1) $\dim H^m(X_{\mathbf{C}}, \mathbf{C}) = 2$ (i.e., le m-ème nombre de Betti de $X_{\mathbf{C}}$ est égal à 2);
(4.8.2) La décomposition de Hodge de $H^m(X_{\mathbf{C}}, \mathbf{C})$ est de type $(m, 0) + (0, m)$.

Choisissons un ensemble fini S de nombres premiers assez grand pour que X ait bonne réduction en dehors de S. Si $l \notin S$, on peut définir une réduction

modulo l de X, qui est une variété $\tilde{X}_l$ lisse sur $\mathbf{F}_l$. Soient π_l et π_l' les valeurs propres de l'endomorphisme de Frobenius de $\tilde{X}_l$, opérant sur la cohomologie de dimension m. D'après Deligne, π_l et π_l' sont des entiers d'un corps quadratique imaginaire, et l'on a

$$\pi_l' = \bar{\pi}_l \quad \text{et} \quad \pi_l \bar{\pi}_l = l^m. \tag{4.8.3}$$

On posera

$$a_l(X) = \pi_l + \bar{\pi}_l. \tag{4.8.4}$$

On a $a_l(X) \in \mathbf{Z}$ et $|a_l(X)| \leqslant 2l^{m/2}$.

(Noter qu'il n'y a pas en général unicité de $\tilde{X}_l$, contrairement à ce qui se passe pour les variétés abéliennes. Toutefois, deux choix différents de $\tilde{X}_l$ conduisent au même $a_l(X)$, cf. [40], n° 1.2.)

THÉORÈME 6. *Admettons* (3.2.4$_?$). *Il existe alors*:
(a) *un entier* $N \geqslant 1$ *dont tous les facteurs premiers appartiennent à* S,
(b) *une forme parabolique de type* $(N, m+1, 1)$:

$$F = q + \cdots + A_n q^n + \ldots,$$

fonction propre normalisée des opérateurs de Hecke, tels que:

$$A_l = a_l(X) \quad \textit{pour tout } l \notin S. \tag{4.8.5}$$

(En d'autres termes, les $a_l(X)$ sont les valeurs propres associées à une forme de poids $m+1$ dont le niveau ne fait intervenir que les nombres premiers de S.)

Il y a intérêt à reformuler le th. 6 en termes de représentations galoisiennes: Soit $\overline{X}$ la $\overline{\mathbf{Q}}$-variété déduite de X par extension des scalaires de $\mathbf{Q}$ à $\overline{\mathbf{Q}}$, et soit $H^m_{\text{et}}(\overline{X}, \mathbf{Q}_p)$ le m-ème groupe de cohomologie étale de $\overline{X}$ à coefficients dans $\mathbf{Q}_p$. Notons H_p le $\mathbf{Q}_p$-*dual* de $H^m_{\text{et}}(\overline{X}, \mathbf{Q}_p)$. Le groupe $G_{\mathbf{Q}}$ opère sur H_p. On obtient ainsi une représentation p-adique de $G_{\mathbf{Q}}$ de dimension 2; son déterminant est la puissance m-ème du caractère cyclotomique $G_{\mathbf{Q}} \to \mathbf{Z}_p^*$. Lorsque p varie, ces représentations forment un système rationnel de représentations p-adiques compatibles entre elles, les traces des substitutions de Frobenius étant les a_l. (Noter qu'il s'agit ici de substitutions de Frobenius "arithmétiques", et non "géométriques"; c'est ce qui explique le passage au dual.) Le th. 6 équivaut à dire que *ce système de représentations est isomorphe à celui fourni par une forme parabolique de poids* $k = m+1$.

Démonstration du th. 6. On reprend la méthode utilisée pour le th. 4. Notons T l'ensemble des p tels que, soit $H^m_{\text{et}}(\overline{X}, \mathbf{Z}_p)$, soit $H^{m+1}_{\text{et}}(\overline{X}, \mathbf{Z}_p)$, ait une composante de torsion non nulle; c'est un ensemble fini. Si $p \notin T$, on a $\dim H^m_{\text{et}}(\overline{X}, \mathbf{F}_p) = 2$; l'action de $G_{\mathbf{Q}}$ sur le dual de $H^m_{\text{et}}(\overline{X}, \mathbf{F}_p)$ définit alors une

représentation

$$\rho_p\colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_p),$$

qui est non ramifiée en dehors de S et de p (c'est une réduction modulo p de la représentation de $G_{\mathbf{Q}}$ sur H_p considérée plus haut; en particulier, on a $\det \rho_p = \chi^m$). Il est essentiel pour la suite de connaître le comportement de ρ_p en p, et, plus précisément, son invariant k au sens du §2. D'après un théorème de J-M. Fontaine (démontré en utilisant certains de ses résultats récents obtenus en collaboration avec W. Messing), on a:

(4.8.6) (Fontaine–non publié). *Si p est assez grand, l'invariant k de la représentation ρ_p est égal à $m+1$.*

(C'est ici que sert l'hypothèse faite sur la décomposition de Hodge de $H^m(X_{\mathbf{C}}, \mathbf{C})$.)

On va maintenant s'intéresser au conducteur N_p de ρ_p. Il est clair que N_p est de la forme

$$N_p = \prod_{l \in S} l^{n(l,p)}, \qquad \text{avec } n(l,p) \geqslant 0.$$

Il nous faut majorer les exposants $n(l,p)$, pour l fixé et p variable. Si l'on admettait la conjecture C_3 de [40], on saurait que les $n(l,p)$ sont *bornés* quand l varie (en fait, il est vraisemblable que $n(l,p)$, pour p assez grand, est *égal* à l'exposant du conducteur défini dans [40], formule (11)). Comme C_3 n'est pas démontrée, nous allons nous restreindre aux nombres premiers p satisfaisant aux congruences suivantes:

$$(4.8.7) \qquad \begin{cases} p \not\equiv \pm 1 \pmod{2^3} & \text{si } 2 \in S, \\ p \not\equiv \pm 1 \pmod{3^2} & \text{si } 3 \in S, \\ p \not\equiv \pm 1 \pmod{l} & \text{pour tout } l \in S,\ l \geqslant 5. \end{cases}$$

On peut alors majorer les $n(l,p)$:

(4.8.8) *Si p satisfait à* (4.8.7), *et si $l \in S$, $l \neq p$, on a*:

$$n(l,p) \leqslant 9 \quad \text{pour } l = 2,$$
$$n(l,p) \leqslant 5 \quad \text{pour } l = 3,$$
$$n(l,p) \leqslant 2 \quad \text{pour } l \geqslant 5.$$

En effet, soit $I_{l,p}$ le sous-groupe d'inertie en l de $\rho_p(G_{\mathbf{Q}})$. Comme $\det \rho_p$ n'est pas ramifiée en l, $I_{l,p}$ est contenu dans $\mathbf{SL}_2(\mathbf{F}_p)$, et son ordre est un diviseur de

$p(p^2-1)$. Si $l \geqslant 5$, l'hypothèse (4.8.7) entraîne que $I_{l,p}$ est d'ordre premier à l; la représentation ρ_p est donc modérée en l, et d'après le n° 1.2, on a $n(l, p) \leqslant 2$. Lorsque $l = 3$ (resp. $l = 2$), les l-sous-groupes de Sylow de $\mathbf{SL}_2(\mathbf{F}_p)$ sont cycliques d'ordre 3 (resp. quaternioniens d'ordre 8); en appliquant une majoration de conducteurs que l'on trouvera au n° 4.9 ci-après, on en déduit $n(3, p) \leqslant 5$ (resp. $n(2, p) \leqslant 9$).

Notons P l'ensemble des nombres premiers p satisfaisant aux conditions de (4.8.6) et (4.8.7). C'est un ensemble infini.

(4.8.9) *Si $p \in P$, et si p est assez grand, la représentation ρ_p est irréductible.*

Soit P' l'ensemble des $p \in P$ tels que ρ_p soit réductible. Si $p \in P'$, la semi-simplification de ρ_p est donnée par deux caractères

$$\alpha, \beta\colon G_{\mathbf{Q}} \to \mathbf{F}_p^*, \quad \text{avec } \alpha\beta = \chi^m.$$

Il résulte de (4.8.6) que l'un de ces caractères, disons α, est non ramifié en p. Le conducteur de α est alors un diviseur de N_p, et l'on a

$$a_l(X) \equiv \alpha(l) + \alpha(l)^{-1} l^m \pmod{p} \tag{4.8.10}$$

pour tout $l \notin S$, $l \neq p$.

Soit $\alpha_0\colon (\mathbf{Z}/N_p\mathbf{Z})^* \to \overline{\mathbf{Z}}^*$ le relèvement multiplicatif de α, cf. n° 3.1. D'après (4.8.8), N_p ne prend qu'un nombre fini de valeurs. Il n'y a donc qu'un nombre fini de possibilités pour α_0. Si P' était infini, il y aurait alors un α_0 qui interviendrait pour un sous-ensemble infini P'' de P'. Si $l \notin S$, posons:

$$b_l = \alpha_0(l) + \alpha_0(l)^{-1} l^m.$$

D'après (4.8.10), $a_l(X)$ et b_l ont même image dans $\overline{\mathbf{F}}_p$ pour tout $p \in P''$, $p \neq l$. Comme P'' est infini, cela entraîne

$$a_l(X) = b_l \quad \text{pour tout } l \notin S,$$

donc aussi

$$\{\pi_l, \bar{\pi}_l\} = \{\alpha_0(l), \alpha_0(l)^{-1} l^m\},$$

ce qui est absurde. D'où (4.8.9).

En combinant (4.8.6), (4.8.8) et (4.8.9), on voit que l'on peut trouver un ensemble infini P_1 de nombres premiers, et un entier N de la forme $\prod_{l \in S} l^{n(l)}$, tels que, pour tout $p \in P_1$, la représentation ρ_p jouisse des propriétés suivantes:

(a) ρ_p est irréductible, de déterminant χ^m;

(b) le conducteur de ρ_p est égal à N;

(c) l'invariant k de ρ_p est égal à $m + 1$.

Comme m est impair, (a) entraîne que ρ_p est absolument irréductible si $p \in P_1$, $p \neq 2$. On peut alors appliquer $(3.2.4_?)$. D'où, pour tout $p \in P_1$, $p \neq 2$, l'existence d'une forme parabolique de poids $k = m + 1$ et de niveau N:

$$f_p = \sum a_{n,p} q^n,$$

à coefficients dans $\overline{\mathbf{F}}_p$, qui est fonction propre normalisée des opérateurs de Hecke, et telle que $\rho_p \simeq \rho_{f_p}$. On conclut alors comme dans la démonstration du th. 4, en relevant f_p en caractéristique 0, et en remarquant qu'il n'y a qu'un nombre fini de possibilités.

Remarques

(1) On trouvera dans Schoen [37] un exemple où les conditions (4.8.1) et (4.8.2) sont satisfaites, avec $m = \dim X = 3$, $k = 4$, $S = \{5\}$, $N = 5^2$. Il s'agit d'une variété X qui est une désingularisation de l'hypersurface de l'espace projectif $\mathbf{P}_4$ d'équation

$$X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 - 5X_0X_1X_2X_3X_4 = 0.$$

On peut alors expliciter la forme parabolique F et démontrer la relation (4.8.5) sans utiliser aucune conjecture: il suffit d'appliquer la méthode de Faltings ([13], p. 362–363—voir aussi [47]) aux représentations 2-adiques définies par X et par F.

(2) Comme l'a remarqué S. Bloch [5], la conclusion du th. 6 peut aussi se déduire des conjectures "archimédiennes" (et non plus modulo p) sur les fonctions L attachées aux motifs (Deligne [10]), combinées avec la caractérisation des formes modulaires due à Weil [55]. De ce point de vue, l'hypothèse (4.8.2) sert à assurer que le facteur à l'infini de la fonction L est bien $(2\pi)^{-s}\Gamma(s)$.

(3) Si l'on supprime l'hypothèse (4.8.2) en question, la décomposition de Hodge de $H^m(X_{\mathbf{C}}, \mathbf{C})$ est de type $(m - r, r) + (r, m - r)$, avec $0 \leqslant r < m/2$. En admettant $(3.2.4_?)$, on peut alors démontrer l'existence d'une forme parabolique normalisée

$$F = \sum A_n q^n,$$

de poids $m - 2r$, telle que $a_l(X) = l^r A_l$ pour tout $l \notin S$: la représentation de $G_{\mathbf{Q}}$ sur H_p se déduit de celle associée à F par une "torsion de Tate" d'amplitude r. La démonstration est essentiellement la même.

4.9. *Une majoration de conducteurs.* La question étant *locale*, nous utiliserons les notations standard suivantes:

K est un corps complet pour une valuation discrète;

v_K: $K^* \to \mathbf{Z}$ est la valuation normalisée de K;

$\overline{K}$ est une clôture algébrique de K;

$G_K = \mathrm{Gal}(\overline{K}/K)$ est le groupe de Galois de $\overline{K}$ sur K.

On suppose que K est de caractéristique 0, et que son corps résiduel est parfait de caractéristique $p > 0$. On note

$$e_K = v_K(p)$$

l'indice de ramification absolu de K.

(Attention au changement de notation: au n° précédent, la caractéristique résiduelle était notée l.)

Soit maintenant V un espace vectoriel de dimension finie sur un corps Ω de caractéristique $\neq p$, et soit ρ: $G_K \to \mathbf{GL}(V)$ un homomorphisme continu. *L'exposant du conducteur de* ρ est un entier $n(\rho) \geqslant 0$, que l'on définit comme au n° 1.2:

si $(G_i)_{i \geqslant 0}$ est la suite des groupes de ramification du groupe fini $G = \rho(G_K)$, on a

$$n(\rho) = \sum_{i \geqslant 0} \frac{g_i}{g_0} \dim V/V_i, \tag{4.9.1}$$

où g_i est l'ordre de G_i, et V_i est le sous-espace de V fixé par G_i.

Il y a intérêt à récrire cette définition sous la forme

$$n(\rho) = \dim V/V_0 + b(\rho), \tag{4.9.2}$$

où

$$b(\rho) = \sum_{i \geqslant 1} \frac{g_i}{g_0} \dim V/V_i$$

est *l'invariant sauvage* de ρ ([39], §19.3).

La majoration que nous avons en vue est la suivante:

PROPOSITION 9. *Soit p^c l'ordre du groupe d'inertie sauvage G_1, et soit N la dimension de V sur Ω. On a*

$$b(\rho) \leqslant N e_K \left(c + \frac{1}{p-1} \right). \tag{4.9.3}$$

De plus, si G_1 n'est pas cyclique, cette inégalité est stricte.

Vu (4.9.2), ceci entraîne:

COROLLAIRE. *On a*

$$n(\rho) \leqslant N(1 + e_K c + e_K/(p-1)), \tag{4.9.4}$$

avec inégalité stricte si G_1 n'est pas cyclique.

Démonstration de la prop. 9. Soit I le plus grand indice $i \geqslant 1$ tel que $G_i \neq \{1\}$. On majore $\dim V/V_i$ par N si $i \leqslant I$, et par 0 si $i > I$. D'où:

$$(4.9.5) \qquad b(\rho) \leqslant \frac{N}{g_0}(g_1 + \cdots + g_I) \leqslant \frac{N}{g_0}(I + \sum_{i \geqslant 1}(g_i - 1)).$$

D'après un résultat élémentaire sur les groupes de ramification ([38], p. 79, exerc. 3), on a:

$$(4.9.6) \qquad I \leqslant g_0 e_K/(p-1),$$

avec inégalité stricte si G_1 n'est pas cyclique.

D'autre part, l'entier

$$d = \sum_{i \geqslant 0}(g_i - 1)$$

est égal à la valuation de la différente de l'extension L/K de groupe de Galois G ([38], p. 72). D'après une majoration due à Hensel (reproduite dans [38], p. 67), on a

$$d \leqslant g_0 - 1 + g_0 e_K c,$$

d'où:

$$(4.9.7) \qquad \sum_{i \geqslant 1}(g_i - 1) \leqslant g_0 e_K c.$$

En combinant (4.9.5), (4.9.6) et (4.9.7), on obtient l'inégalité à démontrer (4.9.3), et l'on voit aussi que cette inégalité est stricte si G_1 n'est pas cyclique.

Remarque. Lorsque G_1 est *abélien* d'exposant p^h, on peut montrer que

$$b(\rho) \leqslant N e_K \left(h + \frac{1}{p-1}\right).$$

Comme $h \leqslant c$, cela améliore (4.9.3).

Application à (4.8.8). Dans la situation de (4.8.8), il y a deux cas à considérer:

(a) *Caractéristique résiduelle* 3. Avec les notations de la prop. 9 (qui diffèrent de celles du n° 4.8, comme on l'a signalé plus haut), on a $p = 3$, $N = 2$, $e_K = 1$ et $c \leqslant 1$, d'où $n(\rho) \leqslant 5$ d'après (4.9.4). Cette borne est optimale: il existe des courbes elliptiques de conducteur 3^5.

(b) *Caractéristique résiduelle* 2. On a alors $p = 2$, $N = 2$, $e_K = 1$ et $c \leqslant 3$, avec G_1 non cyclique si $c = 3$; d'où $n(\rho) \leqslant 9$ d'après (4.9.4). En fait, une analyse plus détaillée montre que l'on a même $n(\rho) \leqslant 8$, ce qui est une majoration optimale: il existe des courbes elliptiques de conducteur 2^8.

§5. Exemples. Ce § rassemble un certain nombre d'exemples sur lesquels on peut vérifier, au moins en partie, les conjectures du §3. La plupart des vérifications ont nécessité l'emploi d'un ordinateur; elles ont été programmées et réalisées par J-F. Mestre.

Les valeurs de p considérées sont:
$p = 2$ (nos 5.1 et 5.2),
$p = 3$ (nos 5.3 et 5.4),
$p = 7$ (n° 5.5).

5.1. *Exemples provenant de* $\mathbf{GL}_2(\mathbf{F}_2) \simeq \mathfrak{S}_3$. Soit K un corps cubique non abélien, et soit K^{gal} sa clôture galoisienne. Le groupe $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q})$ est isomorphe au groupe symétrique $\mathfrak{S}_3$, lui-même isomorphe à $\mathbf{GL}_2(\mathbf{F}_2)$. On obtient ainsi une représentation

$$\rho^K\colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_2),$$

qui est absolument irréductible, et à laquelle on peut appliquer les conjectures du §3.

Les invariants (N, k, ε) de ρ^K sont faciles à déterminer. Si l'on écrit le discriminant D du corps K sous la forme

$$D = \pm 2^m N, \text{ avec } N \text{ impair } > 0, \text{ et } m = 0, 2 \text{ où } 3,$$

on constate que:
le conducteur de ρ^K est égal à N;
le caractère ε est égal à 1;
le poids k de ρ^K est égal à 2 (resp. 4) si $m = 0, 2$ (resp. si $m = 3$).

La conjecture $(3.2.4_?)$ prédit alors l'existence d'une forme parabolique f à coefficients dans $\mathbf{F}_2$ (ou dans $\mathbf{F}_4$ si $m = 0$, i.e., si K est non ramifié en 2), de type $(N, k, 1)$, fonction propre normalisée des opérateurs de Hecke, et telle que ρ^K soit isomorphe à ρ_f. Le tableau suivant donne une liste de cas où ceci a été vérifié sur ordinateur:

$D < 0$	k = poids	N = niveau	$D > 0$	k = poids	N = niveau
− 23	2	23	148	2	37
−31	2	31	229	2	229
−44	2	11	257	2	257
−59	2	59	316	2	79
−76	2	19			
−104	4	13			

(Dans les cas $D = -23$, $D = -31$ et $D = 257$, l'idéal (2) reste premier dans K, et la valeur propre de U_2 est une racine cubique primitive de l'unité, i.e., un élément de $\mathbf{F}_4 - \mathbf{F}_2$, conformément à $(3.2.6_?)$. Pour les autres valeurs de D, la valeur propre de U_2 est 0 ou 1, et tous les coefficients de f appartiennent à $\mathbf{F}_2$.)

Dans le cas général, je ne sais démontrer qu'un résultat un peu plus faible que $(3.2.4_?)$:

PROPOSITION 10. *Il existe une forme f de type $(N, k', 1)$, avec k' convenable, telle que ρ^K soit isomorphe à ρ_f.*

(En particulier, ρ^K satisfait à $(3.2.3_?)$.)

Démonstration. On utilise le plongement évident $\mathfrak{S}_3 \to \mathbf{GL}_2(\mathbf{Z})$, ce qui fournit une représentation

$$\rho_0^K \colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{C}),$$

qui "relève" ρ^K en caractéristique 0. Le déterminant de ρ_0^K est le caractère quadratique

$$\varepsilon_D \colon G_{\mathbf{Q}} \to \mathfrak{S}_3 \xrightarrow{\text{sgn}} \{\pm 1\}$$

qui correspond au corps $\mathbf{Q}(\sqrt{D})$. Distinguons alors deux cas:

(i) $D < 0$, *i.e., K est un corps cubique imaginaire.*

Le caractère $\varepsilon_D = \det \rho_0^K$ est alors *impair*. Comme l'image de ρ_0^K est $\mathfrak{S}_3$, qui est un groupe diédral, on en conclut (cf. [11], [45]), que ρ_0^K est la représentation associée à une forme parabolique F_1 de poids 1, de caractère ε_D et de niveau $|D|$; on peut d'ailleurs écrire explicitement F en termes de fonctions thêta de formes quadratiques binaires de discriminant D. Soit E_D la série d'Eisenstein de poids 1 et de caractère ε_D (qui est aussi une fonction thêta). Le produit $F = F_1 \cdot E_D$ est une forme parabolique de poids 2, de caractère 1, et de niveau $|D|$. Si $f = \tilde{F}$ est la réduction (mod 2) de F, on a $f = \tilde{F}_1$, car $\tilde{E}_D = 1$. La forme f est la forme cherchée; en effet, par construction f est de type $(2^m N, 2, 1)$, donc aussi de type $(N, k', 1)$, pour k' convenable.

(Il devrait être possible de préciser cette démonstration, et d'obtenir la valeur exacte de k'. Je ne l'ai fait que pour $m = 0$, i.e., $D = -N$, où l'on obtient bien $k' = 2$, comme annoncé.)

(ii) $D > 0$, *i.e., K est un corps cubique totalement réel*

Le corps $\mathbf{Q}(\sqrt{D})$ est alors un corps quadratique réel, et la représentation ρ_0^K est induite par un caractère ψ d'ordre 3 de $\mathbf{Q}(\sqrt{D})$. Choisissons un caractère auxiliaire α de $\mathbf{Q}(\sqrt{D})$ ayant les propriétés suivantes:

(ii_1) l'ordre de α est une puissance de 2;

(ii_2) α a pour signatures $+$ et $-$ en les deux places à l'infini de $\mathbf{Q}(\sqrt{D})$;

(ii_3) α est non ramifié en toute place finie de $\mathbf{Q}(\sqrt{D})$ de caractéristique résiduelle $\neq 2$.

(L'existence d'un tel caractère est facile à démontrer.)

Soit $\rho_0' = \text{Ind}(\psi\alpha)$ la représentation de $G_{\mathbf{Q}}$ *induite* par le caractère $\psi\alpha$ du corps $\mathbf{Q}(\sqrt{D})$. C'est une représentation irréductible de degré 2. D'après (ii_1), sa

réduction en caractéristique 2 est isomorphe à $\mathrm{Ind}(\psi) \simeq \rho^K$. D'après (ii_2), son déterminant est impair, et d'après (ii_3) son conducteur est de la forme $2^M N$, avec M entier. On peut donc appliquer à ρ_0' l'argument utilisé dans le cas (i) pour ρ_0^K: cette représentation est associée à une forme parabolique F' de poids 1 et de niveau $2^M N$; par réduction en caractéristique 2, F' donne la forme f cherchée. (Noter qu'ici F' est combinaison linéaire de fonctions thêta de formes binaires indéfinies.)

Remarque. Le même genre d'argument s'applique à toute représentation

$$\rho_p \colon G_{\mathbf{Q}} \to \mathbf{GL}_2\left(\overline{\mathbf{F}}_p\right), \qquad p \neq 2,$$

à déterminant impair, et telle que l'image de $\rho_p(G_{\mathbf{Q}})$ dans $\mathbf{PGL}_2(\overline{\mathbf{F}}_p)$ soit un groupe *diédral*; en particulier, la conjecture faible $(3.2.3_?)$ est vraie pour une telle représentation.

5.2. *Exemples provenant de* $\mathbf{SL}_2(\mathbf{F}_4) \simeq \mathfrak{A}_5$. Soit K un corps de degré 5 sur $\mathbf{Q}$ dont la clôture galoisienne K^{gal} ait pour groupe de Galois le groupe alterné $\mathfrak{A}_5$. Comme $\mathfrak{A}_5$ est isomorphe à $\mathbf{SL}_2(\mathbf{F}_4)$, on déduit de là un homomorphisme surjectif $G_{\mathbf{Q}} \to \mathbf{SL}_2(\mathbf{F}_4)$, d'où une représentation absolument irréductible

$$\rho^K \colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_4),$$

avec $\det \rho^K = 1$.

Ici encore, on désire tester sur ρ^K les conjectures du §3. Comme le conducteur N de ρ^K est le plus souvent très grand, les calculs ne sont praticables que si N est un nombre premier, et si le poids k est égal à 2, car cela permet alors d'appliquer la "méthode des graphes" ([30], [31]). Le tableau suivant indique les différents cas étudiés par Mestre; on a noté D la racine carrée du discriminant de K, avec le signe + si K est réel et le signe − si K est imaginaire.

$D < 0$	N = niveau	$D > 0$	N = niveau
− 2083	2083	$2^3 887$	887
−2707	2707	8311	8311
−3203	3203	$2^2 8447$	8447
−3547	3547	13613	13613
−4027	4027	$2^2 24077$	24077

Les exemples avec $D < 0$ sont extraits d'une table de J. Buhler ([7], p. 136–141); ceux avec $D > 0$ proviennent de [31], n° 4.2.

Remarques

(1) Dans chacun des cas considérés, Mestre obtient une forme parabolique f à coefficients dans $\mathbf{F}_4$ (ou, parfois, dans $\mathbf{F}_{16}$), du type $(N, 2, 1)$ voulu, fonction propre des opérateurs de Hecke $U_2, T_3, T_5, \ldots$, les valeurs propres des trois premiers opérateurs étant les bonnes. Il est donc vraisemblable que la représenta-

tion ρ_f associée à f est isomorphe à ρ^K; toutefois, une démonstration complète demanderait un travail considérable, qui n'a pas été entrepris.

(2) Le cas $D < 0$ n'est pas très surprenant. En effet, la représentation ρ^K peut se relever en caractéristique 0, son image étant alors une certaine extension centrale de $\mathfrak{A}_5$ par un groupe cyclique d'ordre une puissance de 2 (utiliser un plongement de $\mathfrak{A}_5$ dans $\mathbf{PGL}_2(\mathbf{C})$ et appliquer les résultats de Tate reproduits dans [45], §6). Si $D < 0$, cette représentation est de déterminant impair, et provient donc (si l'on admet la conjecture d'Artin sur les fonctions L) d'une forme parabolique F de poids 1. En réduisant F en caractéristique 2, on obtient une forme f telle que $\rho_f \simeq \rho^K$ (cf. démonstration de la prop. 10), ce qui montre que ρ^K satisfait à la conjecture faible ($3.2.3_?$).

Le cas $D > 0$ est plus étonnant: on ne voit *a priori* aucun moyen de rattacher ρ^K à une quelconque forme modulaire.

5.3. *Exemples provenant de* $\mathbf{GL}_2(\mathbf{F}_3) \simeq \tilde{\mathfrak{S}}_4$. Le groupe $\mathbf{PGL}_2(\mathbf{F}_3)$ agit sur la droite projective $\mathbf{P}_1(\mathbf{F}_3)$, qui a 4 points, et cela définit un isomorphisme $\mathbf{PGL}_2(\mathbf{F}_3) \simeq \mathfrak{S}_4$. Comme le noyau de $\mathbf{GL}_2(\mathbf{F}_3) \to \mathbf{PGL}_2(\mathbf{F}_3)$ est $\{\pm 1\}$, on en conclut que $\mathbf{GL}_2(\mathbf{F}_3)$ est une extension centrale de degré 2 de $\mathfrak{S}_4$; en fait, c'est l'extension notée $\tilde{\mathfrak{S}}_4$ dans [46], n° 1.5.

Il est bien connu que $\tilde{\mathfrak{S}}_4$ peut se plonger dans $\mathbf{GL}_2(\mathbf{Z}[\sqrt{-2}])$, et que ce plongement donne par réduction (mod 3) l'isomorphisme $\tilde{\mathfrak{S}}_4 \simeq \mathbf{GL}_2(\mathbf{F}_3)$ ci-dessus. Ceci permet d'associer à toute représentation

$$\rho\colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_3),$$

son *relèvement*

$$\rho_0\colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{Z}[\sqrt{-2}]) \subset \mathbf{GL}_2(\mathbf{C})$$

en caractéristique 0. Supposons que ρ satisfasse aux conditions du n° 3.2, i.e., soit irréductible et de déterminant impair. Il en est alors de même de ρ_0, et l'on peut appliquer les résultats de Langlands [26] et Tunnell [53]. On en déduit que ρ_0 provient d'une forme parabolique de poids 1 et de niveau le conducteur de ρ_0, conducteur que l'on peut écrire sous la forme $3^m N_0$, avec N_0 premier à 3. D'où, comme au n° 5.1:

PROPOSITION 11. *Il existe une forme f de type (N_0, k', ε), avec k' convenable, telle que ρ soit isomorphe à ρ_f.*

(Ici, ε est le caractère $G_{\mathbf{Q}} \to \{\pm 1\}$ défini à partir de $\det \rho$ comme on l'a expliqué au n° 1.3.)

En particulier ρ *satisfait à la conjecture faible* ($3.2.3_?$).

Remarque. Le conducteur $3^m N_0$ de ρ_0 est étroitement lié au conducteur N de ρ défini au §1. Si l'on pose

$$N = \prod_{l \neq 3} l^{n(l)} \quad \text{et} \quad N_0 = \prod_{l \neq 3} l^{n_0(l)},$$

on constate en effet que:

(5.3.1) Si le groupe d'inertie en l de $\rho(G_{\mathbf{Q}}) \simeq \rho_0(G_{\mathbf{Q}})$ est cyclique d'ordre 3, on a $n(l) = 1$ et $n_0(l) = 2$.

(5.3.2) Dans tout autre cas, on a $n(l) = n_0(l)$.

En particulier, N *divise* N_0, et les facteurs premiers de N et de N_0 sont les mêmes. La conjecture $(3.2.4_\gamma)$ affirme donc (entre autres choses) que le niveau N_0 intervenant dans la prop. 11 peut être abaissé à N. Voici deux exemples où cet abaissement a bien lieu:

Exemples tirés de courbes elliptiques. Soit E une courbe elliptique sur $\mathbf{Q}$. Supposons qu'il y ait un nombre premier $l > 3$ en lequel E a mauvaise réduction de type c_3 ou c_6 au sens de Néron (types IV ou IV* de Kodaira). Avec les notations de [41], n° 5.6, cela équivaut à dire que E a potentiellement bonne réduction en l, et que le groupe Φ_l correspondant est cyclique d'ordre 3. Prenons pour ρ la représentation

$$\rho^E\colon G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_3)$$

définie par les points de 3-division de E. D'après (5.3.1), l'exposant de l dans N (resp. N_0) est 1 (resp. 2). On doit donc constater un abaissement. Effectivement:

Exemple (5.3.3). *La courbe* 121_F (cf. [4], p. 97). L'équation de E est

$$y^2 + xy = x^3 + x^2 - 2x - 7.$$

Il y a bonne réduction en dehors de $l = 11$, et mauvaise réduction de type c_3 en 11, d'où $N_0 = 11^2$ et $N = 11$. De plus, la représentation ρ^E est irréductible. La conjecture $(3.2.4_\gamma)$ prédit que ρ^E provient d'une forme de poids 2 et de niveau $N = 11$. Mais il n'y a qu'une telle forme (à homothétie près): celle qui correspond à la courbe E' de conducteur 11 et d'équation

$$y^2 + y = x^3 - x^2.$$

On en conclut que les représentations ρ^E et $\rho^{E'}$ doivent être isomorphes, ou encore que les traces a_l et a'_l de leurs endomorphismes de Frobenius doivent être telles que:

$$a_l \equiv a'_l \pmod 3 \quad \text{pour tout } l \neq 3, 11.$$

La table suivante (extraite de [4], p. 117–119) montre que c'est bien le cas, au moins pour $l < 50$:

l	2	5	7	13	17	19	23	29	31	37	41	43	47
a_l	1	1	−2	1	−5	6	2	9	−2	−3	−5	0	2
a'_l	−2	1	−2	4	−2	0	−1	0	7	3	−8	−6	8

Exemple (5.3.4). *La courbe* 147_I (cf. [4], p. 103). L'équation de E est

$$y^2 + y = x^3 + x^2 - 114x + 473.$$

Son conducteur est $147 = 3.7^2$. Il y a mauvaise réduction de type multiplicatif en 3, et mauvaise réduction de type c_6 en 7, d'où $N_0 = 7^2$, $N = 7$. La représentation ρ^E a pour conducteur 7; comme elle est très ramifiée en 3, son poids k est égal à 4. La conjecture $(3.2.4_?)$ prédit que ρ^E provient d'une forme parabolique de poids 4 et de niveau 7. Or, ici encore, il n'y a qu'une seule telle forme (normalisée):

$$F = q + \sum_{n \geqslant 2} A_n q^n$$

$$= q - q^2 - 2q^3 - 7q^4 + 16q^5 + 2q^6 - 7q^7 + 15q^8 + \cdots .$$

(Pour le calcul des coefficients de F, voir ci-après.)

Si a_l désigne la trace de l'endomorphisme de Frobenius de E en l, on doit donc avoir

$$a_l \equiv A_l \pmod 3 \quad \text{pour tout } l \neq 3, 7.$$

C'est bien ce qui se passe, au moins pour $l < 50$:

l	2	5	11	13	17	19	23	29	31	37	41	43	47
a_l	2	−2	−2	1	0	1	0	4	9	3	−10	5	−6
A_l	−1	16	−8	28	54	−110	48	−110	12	−246	182	128	324

Calcul de F. Soit L l'anneau des entiers du corps $\mathbf{Q}(\sqrt{-7})$. Les séries

$$f_1 = \sum_{z \in L} q^{z\bar{z}} = 1 + 2q + 4q^2 + 6q^4 + 2q^7 + \cdots$$

$$f_2 = \frac{1}{2} \sum_{z \in L} z^2 q^{z\bar{z}} = q - 3q^2 + 5q^4 - 7q^7 - 3q^8 + \cdots$$

sont des formes modulaires de poids 1 et 3 respectivement, de niveau 7 et de caractère le caractère de Legendre mod 7. Leur produit $f_1 \cdot f_2$ est la forme F considérée plus haut; d'où le calcul des coefficients de F.

5.4. *Exemples provenant de* $\mathbf{SL}_2(\mathbf{F}_9) \simeq \tilde{\mathfrak{A}}_6$. Soit G le sous-groupe de $\mathbf{GL}_2(\mathbf{F}_9)$ formé des éléments de déterminant ± 1. On a

$$G = \{\pm 1, \pm i\} \cdot \mathbf{SL}_2(\mathbf{F}_9) = \mathbf{SL}_2(\mathbf{F}_9) \cup i \cdot \mathbf{SL}_2(\mathbf{F}_9),$$

où i désigne un élément d'ordre 4 de $\mathbf{F}_9^*$. L'image de ce groupe dans $\mathbf{PGL}_2(\mathbf{F}_9)$

est égale à $\mathbf{PSL}_2(\mathbf{F}_9)$, qui est isomorphe au groupe alterné $\mathfrak{A}_6$. D'où une projection φ: $G \to \mathfrak{A}_6$. Le couple $(\varphi, \det)$ définit un homomorphisme surjectif $G \to \mathfrak{A}_6 \times \{\pm 1\}$, de noyau $\{\pm 1\}$. On a donc une suite exacte:

$$(*) \qquad \{1\} \to \{\pm 1\} \to G \to \mathfrak{A}_6 \times \{\pm 1\} \to \{1\}.$$

Donnons-nous maintenant un corps K de degré 6 sur $\mathbf{Q}$, avec $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}) \cong \mathfrak{A}_6$, ainsi qu'un corps quadratique $\mathbf{Q}(\sqrt{D})$. On en déduit des homomorphismes

$$\alpha^K\colon G_{\mathbf{Q}} \to \mathfrak{A}_6 \quad \text{et} \quad \varepsilon_D\colon G_{\mathbf{Q}} \to \{\pm 1\},$$

d'où

$$\alpha\colon G_{\mathbf{Q}} \to \mathfrak{A}_6 \times \{\pm 1\}.$$

Cherchons à *relever* α en un homomorphisme

$$\rho\colon G_{\mathbf{Q}} \to G.$$

Vu $(*)$, il y a une *obstruction* à ce relèvement, qui est une classe de cohomologie

$$\mathrm{obs}(\alpha) \in H^2(G_{\mathbf{Q}}, \{\pm 1\}) \simeq \mathrm{Br}_2(\mathbf{Q}),$$

cf. [46], n° 1.1. Le lemme suivant donne un moyen de calculer cette classe:

LEMME 6. *Soit* $w \in \mathrm{Br}_2(\mathbf{Q})$ *l'invariant de Witt de la forme quadratique* $\mathrm{Tr}_{K/\mathbf{Q}}(x^2)$, *cf.* [46]. *On a*:

$$(5.4.1) \qquad \mathrm{obs}(\alpha) = w + (-1)(D).$$

(Rappelons, *loc. cit.*, que $(-1)(D)$ est l'élément de $\mathrm{Br}_2(\mathbf{Q})$ qui correspond à l'algèbre de quaternions $(-1, D)$.)

D'après le th. 1 de [46], w est l'obstruction à relever

$$\alpha^K\colon G_{\mathbf{Q}} \to \mathfrak{A}_6 \simeq \mathbf{PSL}_2(\mathbf{F}_9)$$

en un homomorphisme

$$G_{\mathbf{Q}} \to \tilde{\mathfrak{A}}_6 \simeq \mathbf{SL}_2(\mathbf{F}_9).$$

D'autre part, $(-1)(D)$ est l'obstruction à relever

$$\varepsilon_D\colon G_{\mathbf{Q}} \to \{\pm 1\}$$

en un homomorphisme:

$$G_{\mathbf{Q}} \to \{\pm 1, \pm i\}.$$

Le lemme résulte de ces deux faits, par un argument facile.

Fixons maintenant les choix de K et de D. Nous prendrons:
$D = -3$;
K = corps sextique défini par une équation

$$X^6 + aX + b = 0, \qquad a, b \in \mathbf{Z},$$

le couple (a, b) étant choisi de telle sorte que l'équation soit irréductible et de groupe de Galois $\mathfrak{A}_6$.

[Voici quelques choix possibles de (a, b), obtenus par Mestre: $(a, b) = (24, -20)$; $(30, 25)$; $(240, 400)$; $(240, -400)$; $(48, -80)$; $(432, 720)$; $(480, -400)$.]

D'après [46], n° 3.3, le fait que K soit défini par une telle équation entraîne

$$w = (3)(-d) + (-1)(-1),$$

où d est le discriminant de K. Comme $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q})$ est isomorphe à $\mathfrak{A}_6$, d est un carré, et l'on a

$$w = (3)(-1) + (-1)(-1) = (-1)(-3),$$

d'où

$$\mathrm{obs}(\alpha) = 0$$

en vertu du lemme 6. On peut donc relever α en un homomorphisme

$$\rho\colon G_{\mathbf{Q}} \to G \subset \mathbf{GL}_2(\mathbf{F}_9).$$

Bien entendu, la représentation ρ ainsi obtenue n'est pas unique: elle n'est définie qu'à torsion quadratique près. Comme dans la théorie de Tate (exposée dans [45], §6), on peut utiliser cette torsion pour rendre les invariants k et N de ρ aussi petits que possible; en particulier, on peut choisir ρ de telle sorte que $k = 2$ ou 4, et que N ne soit divisible que par les facteurs premiers du discriminant d qui sont $\neq 3$ (i.e., $l = 2$ et 5 dans les exemples donnés plus haut). Ceci fait, les conjectures du §3 affirment l'existence d'une forme parabolique $f = \Sigma a_n q^n$ de type $(N, k, 1)$, à coefficients dans $\mathbf{F}_9$, fonction propre normalisée des opérateurs de Hecke, et telle que $\rho \simeq \rho_f$. Cette dernière relation entraîne un lien étroit entre les a_l (pour $l \nmid 3N$), et la décomposition de l dans le corps K. De façon plus précise, notons $\mathrm{ord}(l)$ *l'ordre* de la substitution de Frobenius attachée à l dans $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}) \simeq \mathfrak{A}_6$. On doit avoir:

$$\mathrm{ord}(l) = 1 \text{ ou } 3 \iff a_l^2 = \left(\frac{l}{3}\right);$$

$$\mathrm{ord}(l) = 2 \iff a_l = 0;$$

$$\mathrm{ord}(l) = 4 \iff a_l^2 = -\left(\frac{l}{3}\right);$$

$$\mathrm{ord}(l) = 5 \iff a_l^4 = -1.$$

(Rappelons que les a_l sont des éléments du corps $\mathbf{F}_9$.)

En particulier, si $l \neq 3$ ne divise pas le discriminant de $X^6 + aX + b$, le *nombre de solutions dans* $\mathbf{F}_l$ de la congruence

$$x^6 + ax + b \equiv 0 \pmod{l}$$

doit être égal à 1 (resp. 2) si et seulement si a_l est un élément d'ordre 8 de $\mathbf{F}_9^*$ (resp. si $a_l = 0$).

La recherche d'une telle forme f a été effectuée par J.-F. Mestre dans chacun des cas $(a, b) = (24, -20), \ldots, (480, -400)$ cités plus haut, ainsi que dans quelques autres. Le conducteur N est alors égal à $2^m 5^n$, où m et n dépendent de (a, b). La détermination de n n'est pas difficile: lorsqu'il y a ramification sauvage en 5 (ce qui est le cas dans les exemples), n est égal à l'exposant de 5 dans $d^{1/2}$. Par contre, la détermination de m est un exercice dyadique que je n'ai pas fait; cela a obligé Mestre à essayer les différents niveaux possibles: 2.5^n, $2^2 5^n$, $2^3 5^n, \ldots$, jusqu'à ce qu'il en trouve un ayant une forme f du type voulu. Ses résultats sont résumés dans le tableau suivant:

a	b	$d^{1/2}$	k = poids	niveau
24	-20	$2^3 3^3 5^3$	2	$2^3 5^3 = 1000$
30	25	$2^3 3^3 5^4$	2	$\geqslant 20000$?
240	400	$2^2 3^3 5^4$	2	$2^2 5^4 = 2500$
240	-400	$2^3 3^3 5^4$	2	$2^3 5^4 = 5000$
48	-80	$2^3 3^3 5^3$	2	$2^3 5^3 = 1000$
432	720	$2^2 3^5 5^3$	4	$2^2 5^3 = 500$
480	-400	$2^3 3^2 5^4$	2	$2^3 5^4 = 5000$

Noter le cas $a = 30$, $b = 25$, où aucun niveau $\leqslant 10000$ ne convient: il semble que le conducteur N soit alors de la forme $2^m 5^4$, avec $m \geqslant 5$, d'où $N \geqslant 20000$, ce qui est un peu trop grand pour la méthode employée (basée sur la formule des traces d'Eichler-Selberg). Dans tous les autres cas, on trouve bien une forme parabolique ayant les propriétés cherchées, au moins pour l assez petit.

5.5. *Un exemple utilisant le groupe simple* $\mathbf{PSL}_2(\mathbf{F}_7)$ *d'ordre* 168. L'extension de $\mathbf{Q}$ de degré 7 définie par l'équation

$$X^7 - 7X + 3 = 0 \tag{5.5.1}$$

a pour groupe de Galois le groupe $\mathbf{PSL}_2(\mathbf{F}_7)$ (W. Trinks–cf. [25]). Nous allons l'utiliser pour construire une représentation de $G_{\mathbf{Q}}$ en caractéristique 7. La méthode est analogue à celle du n° précédent:

Soit G le sous-groupe de $\mathbf{GL}_2(\mathbf{F}_{49})$ défini par:

$$G = \{\pm 1, \pm i\} \cdot \mathbf{SL}_2(\mathbf{F}_7) = \mathbf{SL}_2(\mathbf{F}_7) \cup i \cdot \mathbf{SL}_2(\mathbf{F}_7),$$

où i est un élément d'ordre 4 de $\mathbf{F}_{49}^*$. On a $\det G = \{\pm 1\}$, et l'image de G dans $\mathbf{PGL}_2(\mathbf{F}_{49})$ est égale à $\mathbf{PSL}_2(\mathbf{F}_7)$. D'où une suite exacte:

$$(*) \qquad \{1\} \to \{\pm 1\} \to G \to \mathbf{PSL}_2(\mathbf{F}_7) \times \{\pm 1\} \to \{1\}.$$

Soit K le corps de degré 7 défini par (5.5.1), et soit α^K: $G_{\mathbf{Q}} \to \mathbf{PSL}_2(\mathbf{F}_7)$ l'homomorphisme correspondant. Soit d'autre part

$$\varepsilon: G_{\mathbf{Q}} \to \{\pm 1\}$$

le caractère quadratique associé au corps $\mathbf{Q}(\sqrt{-3})$. Le couple (α^K, ε) définit un homomorphisme

$$\alpha: G_{\mathbf{Q}} \to \mathbf{PSL}_2(\mathbf{F}_7) \times \{\pm 1\}.$$

Soit $\mathrm{obs}(\alpha) \in \mathrm{Br}_2(\mathbf{Q})$ l'obstruction à relever α en un homomorphisme

$$\rho: G_{\mathbf{Q}} \to G \subset \mathbf{GL}_2(\mathbf{F}_{49}).$$

Un calcul analogue à celui du lemme 6 montre que

$$\mathrm{obs}(\alpha) = w + (-1)(-3),$$

où w est l'invariant de Witt de la forme quadratique $\mathrm{Tr}_{K/\mathbf{Q}}(x^2)$. D'après [46], n° 3.3, on a $w = (-1)(-3)$, d'où $\mathrm{obs}(\alpha) = 0$. Cela démontre l'existence de la représentation

$$\rho: G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_{49})$$

cherchée. Par construction, on a $\det \rho = \varepsilon$.

Ici encore, on choisit ρ de telle sorte que son conducteur soit le plus petit possible. Le discriminant du polynôme $X^7 - 7X + 3$ est $3^8 7^8$ et celui du corps K est $3^6 7^8$. Il en résulte que le conducteur de ρ peut être choisi égal à 3^n, et un calcul de ramification en 3 montre que $n = 3$. D'autre part, l'étude de la ramification en 7 montre que l'action de l'inertie en 7 est:

$$\text{soit } \begin{pmatrix} \chi & * \\ 0 & \chi^{-1} \end{pmatrix}, \qquad \text{soit } \begin{pmatrix} \chi^4 & * \\ 0 & \chi^{-4} \end{pmatrix},$$

où χ est le caractère cyclotomique.

En faisant le produit tensoriel de ρ par χ, ou χ^4, on obtient une nouvelle représentation ρ' où l'action de l'inertie en 7 est donnée par:

$$\begin{pmatrix} \chi^2 & * \\ 0 & 1 \end{pmatrix},$$

ce qui conduit à un poids k égal à 3, cf. n^{os} 2.3 et 2.4. On a

$$\det \rho' = \varepsilon \cdot \chi^2.$$

[Noter que ρ' prend ses valeurs dans un groupe un peu plus grand que G: on a

$$\mathrm{Im}\, \rho' = \mathbf{GL}_2(\mathbf{F}_7) \cup i \cdot \mathbf{GL}_2(\mathbf{F}_7).]$$

Les conjectures du §3 affirment que ρ' est de la forme ρ_f, où $f = \Sigma a_n q^n$ est une forme parabolique de type $(3^3, 3, \varepsilon)$, à coefficients dans $\mathbf{F}_{49}$ et fonction propre normalisée des opérateurs de Hecke. Le lien entre les a_l ($l \neq 3, 7$) et la décomposition de l dans K est le suivant:

si l'on note $\mathrm{ord}(l)$ *l'ordre* de la substitution de Frobenius attachée à l dans $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}) \simeq \mathbf{PSL}_2(\mathbf{F}_7)$, on doit avoir:

$$\begin{aligned}
&\mathrm{ord}(l) = 1 \text{ ou } 7 \quad &&\Leftrightarrow \quad a_l^2 = 4l^2\varepsilon(l) \quad \text{dans } \mathbf{F}_7\\
&\mathrm{ord}(l) = 2 \quad &&\Leftrightarrow \quad a_l = 0 \quad \text{dans } \mathbf{F}_7\\
&\mathrm{ord}(l) = 3 \quad &&\Leftrightarrow \quad a_l^2 = l^2\varepsilon(l) \quad \text{dans } \mathbf{F}_7\\
&\mathrm{ord}(l) = 4 \quad &&\Leftrightarrow \quad a_l^2 = 2l^2\varepsilon(l) \quad \text{dans } \mathbf{F}_7,
\end{aligned}$$

avec $\varepsilon(l) = \left(\frac{l}{3}\right)$.

Effectivement, on trouve bien une forme f ayant ces propriétés, au moins pour l assez petit. C'est la réduction (mod 7) d'une forme parabolique primitive F en caractéristique 0:

$$\begin{aligned}
F &= q + \sum_{n \geqslant 2} A_n q^n\\
&= 9 + 3iq^2 - 5q^4 - 3iq^5 + 5q^7 - 3iq^8 + \cdots
\end{aligned}$$

Cette forme est à coefficients dans $\mathbf{Z}[i]$. Elle se calcule sans difficulté, cf. ci-dessous. Le tableau suivant donne les valeurs des $\mathrm{ord}(l)$ et des A_l pour $l \leqslant 37$:

l	2	5	11	13	17	19	23	29	31	37
$\mathrm{ord}(l)$	7	7	7	4	3	3	3	7	7	4
A_l	$3i$	$-3i$	$-15i$	-10	$18i$	-16	$-12i$	$30i$	-1	20

(Par exemple, pour $l = 17$, on a $a_l^2 \equiv A_l^2 \equiv -2 \pmod 7$, $\varepsilon(l) = -1$, $l^2 \equiv 2 \pmod 7$, d'où $a_l^2 = l^2\varepsilon(l)$ dans $\mathbf{F}_7$, conformément au fait que $\mathrm{ord}(l) = 3$.)

Calcul de F. Soit θ_1 la fonction thêta associée au corps $\mathbf{Q}(\sqrt{-3})$:

$$\theta_1 = \sum_{x,\, y \in \mathbf{Z}} q^{x^2+xy+y^2} = 1 + 6(q + q^3 + q^4 + 2q^7 + q^9 + \cdots).$$

C'est une série d'Eisenstein de poids 1, de niveau 3 et de caractère ε. Si l'on pose

$$\theta_2 = \theta_1(3z) = 1 + 6(q^3 + q^9 + q^{12} + \cdots)$$

$$\theta_3 = \theta_1(9z) = 1 + 6(q^9 + q^{27} + q^{36} + \cdots),$$

on obtient des formes de niveaux 3^2 et 3^3.

D'autre part, la série

$$g = q \prod_{n \geqslant 1} (1 - q^{3n})^2 (1 - q^{9n})^2 = q - 2q^4 - q^7 + 5q^{13} + \cdots$$

est l'unique forme parabolique normalisée de poids 2, de niveau 3^3 et de caractère unité (elle correspond à la courbe elliptique $y^2 + y = x^3 - 3$, de conducteur 3^3).

Les produits $g\theta_1$, $g\theta_2$ et $g\theta_3$ sont des formes de poids 3, de niveau 3^3 et de caractère ε. Ils forment une *base* de l'espace des formes paraboliques de type $(3^3, 3, \varepsilon)$. Les fonctions propres normalisées des opérateurs de Hecke s'obtiennent, par exemple, en diagonalisant l'opérateur T_2. On trouve:

$$F = \frac{1}{2} ig\theta_1 - \frac{1}{2}(1 + i) g\theta_2 + \frac{3}{2} g\theta_3 = q + 3iq^2 - 5q^4 + \cdots,$$

$$\bar{F} = -\frac{1}{2} ig\theta_1 - \frac{1}{2}(1 - i) g\theta_2 + \frac{3}{2} g\theta_3 = q - 3iq^2 - 5q^4 + \cdots,$$

$$G = g\theta_2 = q + 4q^4 - 13q^7 + \cdots$$

La série G est de type (CM): elle correspond à un caractère de Hecke du corps $\mathbf{Q}(\sqrt{-3})$.

La série F est la forme parabolique cherchée.

Bibliographie

1. E. Artin, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*, Hamb. Abh. **8** (1930), 292–306 (= Coll. P., 165–179).
2. A. Ash et G. Stevens, *Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues*, J. Crelle **365** (1986), 192–220.
3. A. O. L. Atkin et W. Li, *Twists of Newforms and Pseudo-Eigenvalues of W-Operators*, Invent. Math. **48** (1978), 221–243.
4. B. J. Birch et W. Kuyk (édit.), *Modular Forms of One Variable* IV, Lect. Notes in Math. **476**, Springer-Verlag, 1975.

5. S. BLOCH, *Algebraic cycles and values of L-functions*, II, Duke Math. J. **52** (1985), 379–397.
6. A. BRUMER ET K. KRAMER, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–742.
7. J. P. BUHLER, *Icosahedral Galois Representations*, Lect. Notes in Math. **654**, Springer-Verlag, 1978.
8. H. CARAYOL, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. E.N.S. **19** (1986), 409–468.
9. P. DELIGNE, *Les constantes des équations fonctionnelles des fonctions L*, Lect. Notes in Math. **349**, 501–597, Springer-Verlag, 1973.
10. _____, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Symp. Pure Math. **33**, Amer. Math. Soc. (1979), vol. 2, 313–346.
11. P. DELIGNE ET J-P. SERRE, *Formes modulaires de poids* 1, Ann. Sci. E.N.S. **7** (1974), 507–530 (= J-P. Serre, *Oe.* 101).
12. P. DÉNES, *Über die Diophantische Gleichung* $x^l + y^l = cz^l$, Acta Math. **88** (1952), 241–251.
13. G. FALTINGS, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366; *Erratum*, ibid. **75** (1984), 381.
14. G. FALTINGS, G. WÜSTHOLZ ET AL., *Rational Points*, Vieweg, 1984.
15. J-M. FONTAINE, *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math **81** (1985), 515–538.
16. G. FREY, *Rationale Punkte auf Fermatkurven und getwisteten Modulkurven*, J. Crelle **331** (1982), 185–191.
17. _____, *Links between stable elliptic curves and certain Diophantine equations*, Ann. Univ. Saraviensis, Ser. Math. **1** (1986), 1–40.
18. A. GROTHENDIECK, *Groupes de Monodromie en Géométrie Algébrique* (SGA 7 I), Lect. Notes in Math. **288**, Springer-Verlag, 1982.
19. Y. HELLEGOUARCH, *Courbes elliptiques et équation de Fermat*, Thèse, Besançon, 1972.
20. A. HURWITZ, *Über endliche Gruppen linearer Substitutionen, welche in der Theorie der elliptischen Transzendenten auftreten*, Math. Ann. **27** (1886), 183–233 (= Math. W. **XI**).
21. N. JOCHNOWITZ, *A study of the local components of the Hecke algebra* mod *l*, Trans. Amer. Math. Soc. **270** (1982), 253–267.
22. _____, *Congruences between systems of eigenvalues of modular forms*, Trans. Amer. Math. Soc. **270** (1982), 269–285.
23. N. KATZ, *p-adic properties of modular schemes and modular forms*, Lect. Notes in Math. **350**, 69–190, Springer-Verlag, 1973.
24. _____, *A result on modular forms in characteristic p*, Lect. Notes in Math. **601**, 53–61, Springer-Verlag, 1976.
25. S. LAMACCHIA, *Polynomials with Galois group* **PSL**(2, 7), Comm. in Algebra **8** (1980), 983–992.
26. R. P. LANGLANDS, *Base Change for* **GL**(2), Princeton Univ. Press, 1980.
27. W. LI, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.
28. B. MAZUR, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33–186.
29. _____, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
30. J-F. MESTRE, *Courbes de Weil et courbes supersingulières*, Sém. de Théorie des Nombres, Bordeaux (1984–1985), exposé 23.
31. _____, *La méthode des graphes. Exemples et applications*, Taniguchi Symp., Kyoto, 1986, à paraître.
32. I. MIYAWAKI, *Elliptic curves of prime power conductor with* **Q***-rational points of finite order*, Osaka Math. J. **10** (1973), 309–323.
33. O. NEUMANN, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten* II, Math. Nach. **56** (1973), 269–280.
34. F. OORT ET J. TATE, *Group schemes of prime order*, Ann. Sci. E.N.S. **3** (1970), 1–21.
35. M. RAYNAUD, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. S.M.F. **102** (1974), 241–280.
36. K. RIBET, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. of Math. **98** (1976), 751–804.
37. C. SCHOEN, *On the geometry of a special determinantal hypersurface associated to the Mumford-Horrocks vector bundle*, J. Crelle **364** (1986), 85–111.

38. J-P. SERRE, *Corps Locaux*, 3ème édition, Hermann, Paris, 1980.
39. _____, *Représentations linéaires des groupes finis*, 3ème edition, Hermann, Paris, 1978.
40. _____, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Sém. Delange-Pisot-Poitou 1969/1970, exposé 19 (= *Oe.* 87).
41. _____, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15**, (1972), 259–331 (= *Oe.* 94).
42. _____, *Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer)*, Sém. Bourbaki 1971/1972, exposé 416 (= *Oe.* 95).
43. _____, *Formes modulaires et fonctions zêta p-adiques*, Lect. Notes in Math. **350**, 191–268, Springer-Verlag, 1973 (= *Oe.* 97).
44. _____, *Valeurs propres des opérateurs de Hecke modulo l*, Journées arith., Bordeaux, 1974, Astérisque **24–25** (1975), 109–117 (= *Oe.* 104).
45. _____, *Modular forms of weight one and Galois representations*, Algebraic Number Fields (A. Fröhlich édit.), Acad. Press, 1977, 193–268 (= *Oe.* 110).
46. _____, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comm. Math. Helv. **59** (1984), 651–676 (= *Oe.* 131).
47. _____, *Résumé des cours de* 1984–1985, Annuaire du Collège de France (1985), 85–90.
48. _____, *Lettre à J-F. Mestre*, Arith. Alg. Geo. (K. Ribet édit.), Contemporary Math. Series, Amer. Math. Soc., 1986.
49. J-P. SERRE ET J. TATE, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517 (= J-P. Serre, *Oe.* 79).
50. C. B. SETZER, *Elliptic curves of prime conductor*, J. London Math. Soc. **10** (1975), 367–378.
51. G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan, vol. **11**, Princeton Univ. Press, 1971.
52. _____, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. **95** (1972), 130–190.
53. J. TUNNELL, *Artin's conjecture for representations of octahedral type*, Bull. A.M.S. **5** (1981), 173–175.
54. J. VÉLU, *Courbes modulaires et courbes de Fermat*, Sém. de Théorie des Nombres, Bordeaux (1975–1976), exposé 16.
55. A. WEIL, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156 (= *Oe. Sci.* [1967a]).

COLLÈGE DE FRANCE, F-75231 PARIS CEDEX 05, FRANCE.