COLLÈGE
DE
FRANCE

CHAIRE D'ALGÈBRE ET GÉOMÉTRIE

Paris, le 27 mai 79

cher Fontaine,

Voici un résumé du fourbi modulaire qui paraît nécessaire (ou plutôt : suffisant) pour les questions d'inertie modérée que tu sais.

Le fourbi en question se coupe assez nettement en deux morceaux :

a) Représ. mod p fournies par les points de division de la jacobienne $J_1(p)$ de la courbe modulaire $X_1(p)$;

b) Passage des formes modulaires de poids qqe sur $SL_2(\mathbb{Z})$ aux formes de poids 2 sur $\Gamma_1(p)$.

La partie qui te concerne le plus directement est la partie a)

a) Le courbe $X_1(p)$ et sa jacobienne

a.1. Notations

Comme dans Deligne-Serre, je considère que $X_1(p)$ classifie les courbes elliptiques E munies d'un sous-groupe C d'ordre p et d'un isomorphisme $\alpha : \mu_p \xrightarrow{\sim} C$. C'est peu différent du point de vue classique où $X_1(p)$ classifie les courbes munies d'un point d'ordre p, mais c'est plus commode, car la courbe de Tate est munie de façon naturelle d'un sous-groupe μ_p, mais pas d'un point d'ordre p.

Je note $X_0(p)$ la courbe qui classifie les (E, C), où C est seulement un sous-groupe d'ordre p. Bien sûr, $X_1(p)$ est un revêtement de $X_0(p)$ (de degré $(p-1)/2$, et non $p-1$ comme on pourrait naïvement s'y attendre).

Je note $J_1(p)$ et $J_0(p)$ les jacobiennes correspondantes. Et je note $T J_{1/0}(p)$ le noyau (ou la comp.connexe du noyau) de $J_1(p) \to J_0(p)$. C'est surtout sur A que l'on travaillera : ce sont les points d'ordre fini de A qui nous intéressent. $A = T$

a.2. Opérateurs

Il y a tout une série d'opérateurs sur $X_1(p)$, $J_1(p)$ et A qui vont jouer un rôle essentiel dans la suite. Ils vérifient de jolies formules que je ne te garantis pas entièrement (vu les "signes" possibles). Voici ces opérateurs :

Opérateur R_d $(d \in F_p^*/\{\pm 1\})$

Il consiste en remplacer (E,C,α) par $(E,C,d\alpha)$, avec des notations évidentes. L'automorphisme $x \mapsto -x$ de E montre que $R_d = R_{-d}$. On obtient ainsi une action de $(Z/pZ)^*/\{\pm 1\}$ sur $X_1(p)$; le quotient est $X_0(p)$. D'où des opérateurs analogu sur $J_1(p)$ et A ; sur A, on a $\sum_d R_d = 0$: on a éliminé des points fixes.

Opérateur T_ℓ (ℓ premier, $\ell \neq p$)

Il associe à (E,C,α) les $\ell+1$ systèmes $(E/C_i,C,\alpha)$, où C $(i = 0,\ldots,\ell)$ désigne les $\ell+1$ sous-groupes d'ordre ℓ de E et où j'ai noté C et α les sous-groupes et isomorphismes évidents. Ce sont les opérateurs de Hecke. (Tu peux les oublier : tu n'auras pas à t'en servir. Mais ce sont eux qui m'intéressent le plus !)

Opérateur U

C'est presque l'opérateur T_p : il associe à (E,C,α) les $(E/C_i,C,\alpha)$ comme ci-dessus, où C_i $(i = 1,\ldots,p)$ désigne les p sous-groupes d'ordre p de E distincts du groupe C lui-même.

Ces opérateurs sont définis sur Q. Ils commutent entre eux. Quand on les fait opérer sur les formes de 1ère espèce sur $X_1(p)$ (i.e. sur les formes invariantes sur $J_1(p)$), et qu'on identifie ces formes à des formes modulaires de poids 2, on trouve les opérateurs habituellement notés de cette manière.

Opérateurs W_z

Soit z une racine primitive p-ème de 1. Si (E,C,α) est comme d'habitude, la courbe E/C se trouve muni d'un sous-groupe d'ordre p (à savoir E_p/C) qui (par dualité de Weil) est canoniquement Z/pZ. Grâce à z, je peux identifier ce sous-groupe à μ_p. D'où un automorphisme W_z de $X_1(p)$, qui est d'ordre 2. On a

$$W_z R_d = R_{d^{-1}} W_z \qquad \text{si } d \in F_p^* .$$

En particulier, $W_z = W_{z'}$ si et seulement si $z' = z^{\pm 1}$.

Bien sûr, les W_z ne sont définis que sur le corps $Q(\mu_p)^+$, plus grand sous-corps réel de $Q(\mu_p)$. De plus, ils ne commutent pas aux R_d, T_p, U mais ont avec eux des relations qui sont essentielles pour la suite:

Notons $\underline{H}$ (pour Hecke) l'algèbre d'opérateurs (sur Q) engendrée par les R_d, T_ℓ, U ; c'est une algèbre commutative (je la considère comme une sous-algèbre de l'algèbre des endomorphismes de $J_1(p)$, pour fixer les idées - cela revient aussi à la considérer comme algèbre de classes de correspondances sur la courbe $X_1(p)$). Si T est une correspondance, je note T' la correspondance transposée (autom. de Rosatti, dit Weil, à moins que ce ne soit Rosati). Ceci étant, il me semble que l'on a :

<u>Théorème</u> (?) - (i) <u>L'algèbre</u> $\underline{H}$ <u>est stable par l'involution</u> $T \longmapsto T'$.

(ii) <u>Si</u> $T \in \underline{H}$, <u>on a</u> $T' = W_z T W_z$ <u>pour tout</u> z.

(iii) $R_d' = R_{d^{-1}}$, $T_\ell' = R_\ell^{-1} T_\ell$.

(iv) <u>Sur</u> A, <u>on a</u> $U' = p.U^{-1}$; <u>sur</u> $J_0(p)$, $U = U' = -W_z$ (qui est alors indépendant de z, et qu'on note W).

Je n'ai pas rédigé une démonstration détaillée de ce th., mais je me suis essentiellement convaincu qu'il était vrai(*)... Il est sûrement dans les papiers de Shimura quelque part (encore faudrait-il savoir les déchiffrer).

Pour la suite, la formule $U'U = p$ sera particulièrement importante.

(Note une façon peu fatigante de <u>vérifier</u> les formules du th. ci-dessus : on remarque que deux endom. de A (par exemple) sont égaux s'ils opèrent de la même façon sur les formes de 1ère espèce, i.e. sur les formes modulaires de poids 2; on applique alors les formules standard, cf. par exemple thèse de W.Li.)

(Référence pour les W_z : Mazur-Tate, Invent. 22 (1973), p.41-49., qui ont regardé le cas $p = 13$. Dans ce cas, $A = J_1(p)$ est de dim.2 ; on a $\underline{H} = Q(\sqrt{-3}) = Q(\mu_6)$ et l'algèbre engendrée par $\underline{H}$ et W_z est $M_2(Q)$; d'où le fait que A est isogène(sur une extension de Q) au produit d'une courbe elliptique par elle-même; toutefois A est simple sur Q. C'est un exemple qui m'a beaucoup servi à comprendre la situation.)

(*) et facile !

a.3. Réduction modulo ℓ (avec $\ell \neq p$, bien sûr)

La situation se réduit parfaitement bien : c'est lisse et tout. On obtient donc une var. abélienne $J_1(p)$, resp. $J_0(p)$, resp. A sur le corps F_ℓ ; on peut parler de son endomorphisme de Frobenius $F = F_\ell$ et de son Verschiebung V_ℓ. On a

Théorème (Eichler-Shimura) - $T_\ell = R_\ell F_\ell + V_\ell$.

(Je rappelle que $F_\ell V_\ell = \ell$, et aussi que $(F_\ell)' = V_\ell$, ce qui ~~~~ redonne d'ailleurs la formule donnant $(T_\ell)'$.) .)

Note aussi la formule $W_z F_\ell = F_\ell R_\ell W_z$, équivalente à $F_\ell W_z F_\ell^{-1} = W_{z\ell}$, qui est évidente par transport de structure.

a.4. Construction des représentations ℓ-adiques (ou p-adiques) associées aux formes modulaires de poids 2 sur $\Gamma_1(p)$

Occupons-nous des représentations de l'algèbre $\underline{H}$. Cette algèbre opère sur des tas de choses :

(i) (dual de) l'espace tangent à $J_1(p)$;

(ii) homologie (à coef. dans Q) de $J_1(p)$;

(iii) homologie ℓ-adique (i.e. module de Tate) de $J_1(p)$.

La théorie transcendante montre que la repr. (i) est la représentation régulière de $\underline{H}$ (c'est le fait qu'une forme est connue quand on connait les val.propres des opérateurs de Hecke - Note que toutes les formes sont ici des "newforms" du fait qu'on est en poids 2 et que le niveau p est un nombre premier.) Les fourbis généraux sur les courbes montrent que les repr. (ii) et (iii) sont équivalentes entre elles et sont équivalentes à (i) + transposée de (i), c'est-à-dire à 2 copies de la repr. régulière.

(J'ai oublié de faire une remarque sur $\underline{H}$, qui est parfois utile : $\underline{H}$ est engendrée par les T_ℓ tous seuls, ce n'est pas la peine d'y mettre les R_d et U; il est même engendré par les T_ℓ où ℓ parcourt n'importe quel ensemble de densité 1.

La façon dont on ~~~~~~~ construit les repr. ℓ-adiques est maintenant claire : disons qu'on veut construire la repr. ℓ-adique associée à un facteur K de l'algèbre $Q_\ell \otimes \underline{H}$. Si

25/5/79

l'on note π le projecteur de $Q_\ell \otimes \underline{H}$ sur K, on prend dans le module de Tate V_ℓ le morceau découpé par π ; c'est un K-espace vectoriel de dimension 2, où opère Galois. Il est peut-être plus commode de prendre les choses un peu autrement, i.e. d'étendre les scalaires à une extension finie assez grande Ω_ℓ de Q_ℓ, et de considérer un <u>caractère</u> $a : \underline{H} \to \Omega_\ell$. On prend alors le sous-espace propre de $\Omega_\ell \otimes V_\ell$ correspondant à a; c'est un Ω_ℓ-espace vectoriel de dimension 2.

(La notation " a " pour un caractère t'intrigue peut-être ? C'est que je veux rappeler que l'image par a de $T_q \in \underline{H}$ est a_q, q-ème valeur propre de Hecke; et l'image de R_d par a est le $\varepsilon(d)$ traditionnel, ε étant vu comme un homomorphisme de $F_p^*/\{\pm 1\}$ dans Ω_ℓ^*.)

Notons $V_{\ell,a}$ le sous-espace propre en question. On a une action naturelle de Galois sur $V_{\ell,a}$ qui est non ramifiée en dehors de p et de ℓ. Je vais montrer (tout ça est dans Shimura ...) que c'est la repr. de degré 2 que je veux, à cela près que je me suis mal débrouillé ... :

<u>Théorème</u> - <u>Soit</u> q <u>un nombre premier distinct de</u> p <u>et de</u> ℓ. <u>Alors la trace de</u> F_q (opérant sur $V_{\ell,a}$) <u>est</u> a'_q, <u>et son déterminant est</u> $\varepsilon(q)^{-1}q$.

(J'ai noté a'_q l'image de T'_q par le caractère a. Dans les notations standard, on a $a'_q = \overline{a_q}$ (conjugaison complexe) et $\varepsilon(q)^{-1} = \bar{\varepsilon}(q)$; autrement dit, mon $V_{\ell,a}$ correspond à la forme modulaire conjuguée de celle que je voulais. On s'en fout.)

Je vais d'abord prouver la formule relative au déterminant. Je note (x,y) la forme bilinéaire de Weil sur $V_\ell \times V_\ell$; elle est alternée, non dégénérée, invariante par W et les R_d et $(Tx, y) = (x, T'y)$ pour toute correspondance T. On pourrait croire que c'est elle qui fait marcher le fourbi ? Pas du tout. Il faut utiliser

$$B(x,y) = (x, W_z y) \qquad (z \text{ fixé}).$$

On vérifie en effet, par des calculs faciles (que j'ai la flemme de recopier) que B est alternée, non dégénérée sur chaque $V_{\ell,a}$, et que l'on a

$$B(F_q x, F_q y) = \varepsilon(q)^{-1} q \, B(x, y) \qquad (x,y \in V_{\ell,a}).$$

25/5/79

Cela prouve bien que le déterminant de F_q sur $V_{\ell,a}$ est $\varepsilon(q)^{-1}q$.

Reste à calculer la trace. Or, si $\varphi \in GL_2$, et si on définit son "adjoint" φ^* par $\varphi^* = \det(\varphi).\varphi^{-1}$, on a $Tr(\varphi) = \varphi + \varphi^*$, comme on le voit en se ramenant au cas où φ est diagonal $\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$, auquel cas $\varphi^* = \begin{pmatrix}\beta & 0\\ 0 & \alpha\end{pmatrix}$. En appliquant ceci à $F_q = \varphi$, on voit que son adjoint est

$$\varphi^* = \varepsilon(q)^{-1}q\,F_q^{-1} = \varepsilon(q)^{-1}V_q \text{ , d'où}$$

$$Tr(F_q) = F_q + \varepsilon(q)^{-1}V_q = \varepsilon(q)^{-1}T_q = \varepsilon(q)^{-1}a_q = a'_q ,$$

puisque T_q est égal à a_q sur $V_{\ell,a}$, et que $T'_q = R_q^{-1}T_q$.

Bien sûr, une fois qu'on a les représentations ℓ-adiques $V_{\ell,a}$, on n'a pas de mal à attraper des représentations mod ℓ , si l'on en a envie.

Autre remarque : je n'ai pas vraiment utilisé le fait que je me sois placé sur $\Gamma_1(p)$, avec p premier. Ça marche tout aussi bien avec $\Gamma_1(N)$, où N est un entier quelconque.

a.5. Enoncé du résultat qu'on voudrait démontrer

A partir de maintenant, on prend $\ell = p$, surprise ! On se donne comme ci-dessus un caractère p-adique $a : \underline{H} \to \Omega_p$ de l'algèbre de Hecke, et on en déduit une représentation galoisienne de degré 2

$$\rho_{p,a} : Gal(\overline{Q}/Q) \to GL_2(\Omega_p)$$

comme ci-dessus. On s'intéresse à l'action de l'inertie modérée en p sur la réduction (mod p) de cette représentation (on sait que ça a un sens ...). On suppose son caractère ε distinct de 1 .Puisque U, U' appartiennent à $\underline{H}$, on peut parler de leurs images a_p et a'_p dans Ω_p . Ce sont des entiers algébriques, et leur produit $a_p a'_p$ est égal à p. Notons v la valuation p-adique de Ω_p , normalisée par $v(p) = 1$.

Il y a deux cas :

Cas I - $v(a_p) = 0$ et $v(a'_p) = 1$.

Cas II - $v(a_p) > 0$ et $v(a'_p) > 0$.

(Il y a aussi le cas I' où $v(a_p) = 1$ et $v(a'_p) = 0$, mais il se ramène au cas I en conjuguant, i.e. en appliquant W_p. Du point de vue galoisien, c'est une "torsion" à la Tate facile à expliciter.)

25/5/79

(J'aurais peut-être dû faire remarquer que, si a est un caractère, on peut parler de son transposé a' qui en est un autre; les ε correspondants sont inverses l'un de l'autre; et les espaces $V_{\ell,a}$ et $V_{\ell,a'}$ sont appliqués l'un sur l'autre par W_ℓ. Bref, tous ces fourbis viennent de façon naturelle par couples.)

Regardons le caractère $\varepsilon : (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\} \to \Omega_p^*$. Je peux l'écrire comme une puissance paire ω^h du caractère de Teichmüller ω (représentant multiplicatif). L'entier h est défini mod $(p-1)$. Je prendrai son représentant entre 1 et p (ou plutôt entre 2 et $p-3$, puisque je suppose $\varepsilon \neq 1$). Je poserai $h' = p-1-h$; c'est l'invariant de ε^{-1}. Ceci étant, voilà le résultat principal de la partie a :

Théorème (?) - L'action de l'inertie modérée en p est donnée par :

(i) Dans le cas I : le caractère 1 et le caractère $\chi_1^{1+h'}$ où χ_1 est le caractère fondamental de niveau 1 (donnant l'action sur μ_p).

(ii) Dans le cas II : les caractères $\chi_2^{1+h'}$ et $\chi_2^{p(1+h')}$, où χ_2 et χ_2^p sont les deux caractères fondamentaux de niveau p^2-1 conjugués l'un de l'autre.

(Peut-être devrais-je considérer $V_{p,a'}$ plutôt que $V_{p,a}$ de façon à avoir pour trace a et pour déterminant $\varepsilon\chi_1$. Dans l'énoncé ci-dessus, il faudrait alors remplacer h' par h, ce qui serait plus sympathique.)

Note que, en réalité, je ne m'intéresse pas au cas I. C'est au cas II que j'en ai, pour mon cher " 59 " .

Note aussi que, dans le cas II, les valeurs de $v(a_p)$ et $v(a'_p)$ n'interviennent pas : il suffit qu'elles soient > 0. C'est miraculeux - et c'est fort heureux car en pratique ça ne serait pas drôle à calculer (même pour l'exemple lié à 59).

a.6. Caractéristique p : la courbe d'Igusa

Cette courbe jouera un rôle essentiel dans la fin du §a, ainsi que dans le §b. Autant la définir tout de suite !

On fait exactment comme en caract. 0, i.e. on cherche à paramétrer les triplets (E,C,α) où E est une courbe elliptique, et un isomorphisme de μ_p sur un sous-groupe (i.e. sous-schéma en groupes ...) C de E. Bien sûr, l'existence d'un tel C équivaut à dire que E est ordinaire (de hauteur 1), auquel cas C est unique. Cela t'explique que la paramétrisation des (E,C,α) se fasse par une courbe affine Y, qui est un revêtement de la droite projective P_1 (correspondant à j, si l'on ose dire), avec action des R_d habituels. En fait, Y est un revêtement* de P_1 privé de l'infini et des points supersinguliers. Il est plus commode de compactifier Y en un revêtement (ramifié) X de P_1. Il y a sur X un point à l'infini naturel ∞, correspondant à la courbe de Tate et à son μ_p évident; on peut donc parler de développements en séries de puissances de q, comme dans le cas usuel. Cette courbe X a été étudiée par Igusa, qui a montré qu'elle est aussi ramifiée que possible aux points supersinguliers.

On peut donner une équation d'un modèle birationnel de X (ou Y) qui sera bien commode pour la suite. Considère un triplet (E,C,α) comme ci-dessus. On peut lui associer canoniquement une forme de première espèce ω sur C par la condition que cette forme induise sur μ_p (via α) la forme canonique que je me retiens à peine de noter dt/t. Cette forme est invariante par l'opérateur de Cartier. Et inversement, toute forme invariante s'obtient ainsi. Je peux donc parler des covariants c_4 et c_6 (ou ce qui revient au même Q et R, avec les notations de Ramanujan) de E relativement à ω. Si $A(Q,R)$ désigne le polynôme de poids $p-1$ utilisé par Sw-Dyer (celui qui donne E_{p-1} en fonction de $Q = E_4$ et de $R = E_6$), le fait que ω soit invariante par Cartier se traduit par l'équation

(*) $\qquad A(Q,R) = 1.$

Il est à peu près clair que cette équation définit une courbe affine qui n'est autre que la courbe Y de tout à l'heure à laquelle on a ajouté les pointes (qui correspondent à $R = \zeta^3$,

* Il y a aussi un peu de ramification en $j = 0$, et $j = 1728$; on s'en fo

25/5/79

$Q = \xi^2$, avec $\xi^{(p-1)/2} = 1$; la pointe standard $q = 0$ est le point $(Q,R) = (1,1)$.

Quant aux R_d , ils opèrent ainsi : si ω est la forme différentielle attachée à (E,C,α), celle correspondant à

$$R_d.(E,C,\alpha) = (E,C,d\alpha)$$

est $d^{-1}\omega$ (sauf erreur ...); on en conclut que les covariants (Q,R) attachés à $(E,C,d\alpha)$ sont d^4Q et d^6R. Autrement dit, R_d opère sur la courbe Y (ou X) par

$$(Q,R) \longmapsto (d^4Q, d^6R) \qquad \text{(avec } d \in F_p^*\text{)}.$$

Cela met bien en évidence le revêtement d'ordre $(p-1)/2$ donné par cette action. Note aussi que l'équation (*) est bien invariante par les R_d du fait que A est de poids $p-1$ en Q,R.

Exemple. Si $p = 13$, on a $E_{12} = (441Q^3 + 250Q^2)/691$ qui est congru mod 13 à $6Q^3 + 8R^2$. La courbe d'Igusa est donc la cubique d'équation

$$6Q^3 + 8R^2 = 1.$$

C'est une courbe de genre 1, avec un groupe d'automorphismes d'ordre 6, comme il se doit (puisque $6 = (p-1)/2$).

Plus généralement, Igusa a donné une formule pour le genre g_X de la courbe X. Je m'en servirai plus tard. C'est :

$$2g_X - 2 = (p-1)(p-11)/24 - k_p,$$

où k_p est le nombre des j supersinguliers en caract.p, à savoir $(p-1)/12$, $(p+7)/12$, $(p+5)/12$ ou $(p+13)/12$ suivant que p est congru à 1, 5, 7 ou 11 (mod 12). Par exemple, lorsque p est congru à 11 (mod 12), ce qui est le cas pour $p = 59$, on trouve $g_X = (p-3)(p-11)/48$.

On a sur X des correspondances analogues aux T_ℓ ($\ell \neq p$), qui se définissent de la même façon. L'analogue de U est un peu moins évident. Si on réfléchit un peu, on voit que ça ne peut être que la correspondance " V " : celle qui associe à un point x p fois le point $x^{1/p}$; autrement dit, on a $VF = p$. Quant à l'analogue de U' , ça ne peut être que F, mais n'anticipons pas ...

a.7. Le modèle de Deligne-Rapoport

J'en arrive - moment redoutable - à des choses que je ne comprends qu'à moitié (une très petite moitié ...), mais dont Delig m'assure qu'elles sont dans Deligne-Rapoport (entre les pages 234 à 257). Je veux bien le croire ...

25/5/79

Soit $\underline{O} = \underset{\sim}{Z}_p[z]$ l'anneau obtenu en adjoignant à Z_p une racine primitive p-ième de l'unité z. J'identifie le groupe de Galois du corps cyclotomique à $\Gamma = (Z/pZ)^*$ à la manière habituelle ($z \mapsto z^d$). Je note $\underline{O}^+$ le sous-anneau de $\underline{O}$ fixé par le sous-groupe $\{\pm 1\}$ de Γ ; son indice de ramification est (p-1)/2.

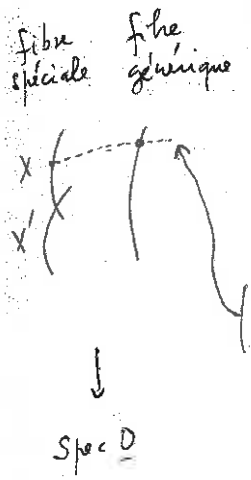
Deligne-Rapoport construisent un schéma $\underline{X}_1(p)$ sur $\underline{O}$ (et même sur $\underline{O}^+$, mais pour le moment je préfère me placer sur $\underline{O}$) jouissant d'un certain nombre de propriétés :

i) Ses fibres sont des courbes ; sa fibre générique est $X_1(p)$; sa fibre spéciale (au-dessus du corps F_p) est une courbe réduite, formée de deux courbes lisses X et X' se coupant transversalement; la courbe X est la courbe d'Igusa de a.6.

ii) $\underline{X}_1(p)$ est un schéma régulier, et projectif sur $\underline{O}$.

iii) Les correspondances R_d, T_ℓ et U se prolongent à $\underline{X}_1(p)$ et appliquent chacune des courbes X et X' dans elle-même. Par contre les W_z échangent X et X' (de sorte que X' est isomorphe à X).

D-R définissent $\underline{X}_1(p)$ par un problème de module astucieux (utilisant la structure à la Oort-Tate des schémas en groupes d'ordre p : ça devrait te plaire). Intuitivement, je vois ça comme ça : considère un triplet (E,C,α) sur le corps des fractions de $\underline{O}$ (ou sur une extension), et suppose que E ait bonne réduction. Alors C se prolonge en un schéma en groupes. Il se peut que ce schéma soit μ_p. Dans ce cas (favorable), on a une section de $\underline{X}_1(p)$ qui aboutit en un point ordinaire de la courbe d'Igusa X, à savoir la réduction (mod $\underline{p}$) de (E,C,α). Il se peut aussi que le schéma C soit isomorphe à Z/pZ, i.e. soit étale. En appliquant une symétrie W_z à (E,C,α) on se ramène au 1er cas; cela signifie que la section de $\underline{X}_1(p)$ considérée aboutit en un point ordinaire de X'. Les cas écartés correspondent aux réductions en les pointes, ou aux réductions supersingulières.



Cette façon rudimentaire de procéder me permet en tout cas de voir que les R_d, T_ℓ et U induisent sur la courbe d'Igusa X les opérateurs qu'on pense (pour U, on trouve l'opérateur V).

Continuons la liste des brillantes propriétés de $\underline{X}_1(p)$:

iv) Les points d'intersection de X et X' sont les points supersinguliers. Ils sont fixés par les R_d et permutés entre eux (si j'ose dire) par les T_ℓ (la façon dont ils sont permutés est donnée par les matrices de Brandt relativement au corps de quaternions ramifié en $\{p,\infty\}$ - on pourrait déduire de là le th.d'Eichler reliant les formes de poids 2 sur $\Gamma_0(p)$ aux séries Θ à 4 variables; comme ce théorème a été vastement généralisé par Jacquet-Langlands, je préfère ne pas insister). L'opérateur W_z agit sur les points supersinguliers comme Frobenius : il fixe les points qui sont rationnels sur F_p, et permute ceux qui sont rationnels sur F_{p^2} sans l'être sur F_p.

Le schéma $X_1(p)$ est lisse sur $\underline{Q}$ en dehors des points d'intersection de X et X'. En ces points là, il n'est pas lisse, mais il est régulier, et D-R donnent une équation locale (qqe chose comme $xy = \pi$, où π est une uniformisante de $\underline{Q}$ - à moins que ce ne soit de $\underline{Q}^+$, je ne sais pas).

v) Le schéma $X_1(p)$ est "canonique" : le groupe d'inertie opère (semi-linéairement) dessus. D'où une action (F_p-linéaire, cette fois) sur sa fibre spéciale $X \cup X'$. Cette action est la suivante : l'identité sur X, et l'action par les R_d^{-1} sur X' (je vois ça sur la description intuitive de la p.10). En particulier, le sous-groupe $\{\pm 1\}$ de Γ opère trivialement sur la fibre spéciale.

On est maintenant armé pour passer aux jacobiennes. La variété $J_1(p)$ admet une réduction semi-stable sur $\underline{Q}$ (et même sur $\underline{Q}^+$), qui admet pour composante connexe de la fibre spéciale la jacobienne généralisée de la courbe réductible $X \cup X'$. Cette composante connexe se présente donc comme une extension

$$\longrightarrow \mathbb{X} \to G_m^{k_p - 1} \to J_1 \to J \times J' \to 0 \ ,$$

où J (resp. J') est la jacobienne de X (resp. X'), et k_p est le nombre des points supersinguliers.

En fait, cette suite exacte correspond à la suite exacte (sur la fibre générique) :

$$0 \to J_0(p) \to J_1(p) \to A \to 0 \ ,$$

provenant de la projection de $X_1(p)$ sur $X_0(p)$. C'est comme ça

25/5/79

que j'aurais dû définir A au début : comme un quotient, et non pas comme un sous-truc. J'avais oublié que les jacobiennes sont fonctorielles dans les deux directions : comme variété d'Albanese et comme variété de Picard ! Ici, je prends le point de vue Picard. _7

Il résulte de ceci que A (qui est la variété abélienne qui m'intéresse le plus) a bonne réduction sur O, avec pour fibre spéciale le produit direct $J \times J'$. Et l'action du groupe d'inerti Γ sur cette réduction est l'identité sur J, et l'action par les R_d^{-1} sur J'.

Quant à l'effet de U sur la fibre spéciale $J \times J'$ de A, j'ai déjà dit que c'était V (Verschiebung) sur le morceau J. Il en résulte (en utilisant les identités entre R_d, W_z et U) que c'est le Frobenius F sur J'.

Ouf ! Je crois que l'on a maintenant tous les renseignements nécessaires pour que les fourbis de ta lettre (complétés au cas (q,q)) s'appliquent; ces fourbis doivent démontrer le th. de la page 7. Ceci achève la partie a.

(Il y a pas mal de points sur lesquels je ne me sens pas à l'aise : a) la technique D-R ; b) les conventions de covariance ou contravariance; c) les ennuis du genre " j = 0 ou 1728 " provenant de ce que $X_o(p)$ n'est pas un vrai schéma de modules. Il faut donc que tu prennes toutes les affirmations ci-dessus avec pas mal de grains de sel ... ou avec des pincettes, suivant l'image que tu préfères.)

b) Passage des formes paraboliques sur $SL_2(Z)$ aux formes de poids 2 sur $\Gamma_1(p)$

b.1. Formes de 1ère espèce sur la courbe d'Igusa

Soit k un entier pair, tel que $2 \leqslant k \leqslant p-1$. Soit S_k le F_p-espace vectoriel des formes paraboliques de poids k, à coef. dans F_p, sur $SL_2(Z)$. Un élément de S_k peut s'écrire de façon unique sous la forme

$$f = F(Q,R)$$

où F est un polynôme isobare de de poids k en Q,R (Q étant de poids 4 et R de poids 6, bien sûr), avec $F(1,1) = 0$ puisque je désire que f soit parabolique. Une telle forme a un

développement en série de puissances de q :

$$f = \sum_{n \geqslant 1} a_n q^n \qquad , \quad a_n \in F_p .$$

Posons

$$\omega_f = f \frac{dq}{q} = \sum a_n q^n dq/q .$$

Théorème (?) - (i) <u>Pour tout</u> $f \in S_k$, <u>il existe une forme différentielle de 1ère espèce sur la courbe d'Igusa</u> X <u>dont le développement à la pointe à l'infini est</u> ω_f .

(ii) <u>L'application</u> $f \longmapsto \omega_f$ <u>est un isomorphisme de</u> $\bigoplus_{k=2}^{p-1} S_k$ <u>sur l'espace vectoriel des formes de 1ère espèce sur</u> X.

<u>Démonstration</u>. Il faut d'abord vérifier que $\omega_f = f\,dq/q$ est une différentielle rationnelle sur X, i.e. peut s'exprimer au moyen de Q, R et de leurs différentielles. Or, on a (cf. par exemple mon exposé Bourbaki de 1972, p.416-06) :

$$dQ = \Theta Q.dq/q = \tfrac{1}{3}(BQ - R)dq/q \qquad \text{avec} \quad B = E_{p+1}$$

$$dR = \Theta R.dq/q = \tfrac{1}{2}(BR - Q^2)dq/q$$

d'où, en éliminant B,

$3RdQ - 2QdR = (Q^3 - R^2)dq/q$, ce qui permet de récrire ω_f sous la forme visiblement rationnelle :

$$\omega_f = F(Q,R)(3RdQ - 2QdR)/(Q^3 - R^2).$$

Il faut voir ensuite que cette expression définit une différentiell<u>de 1ère espèce</u> sur la courbe X (modèle lisse et projectif de la courbe affine $A(Q,R) = 1$). Il est clair que ω_f est holomorphe aux points ordinaires, ainsi qu'aux pointes. Il faut voir ce qui se passe aux points supersinguliers. Or, en un tel point, on vérifie par un calcul local que $F(Q,R)$ a un pôle d'ordre au plus $k/2$, alors que dq/q a un zéro d'ordre $(p-1)/2$. Vu l'inégalité $k \leqslant p-1$, on est sauvé. (Ici encore, il faut faire un peu attention aux points où $Q = 0$ ou $R = 0$. Je laisse tomber ce genre d'ennuis.)

Pour prouver (ii) , je ne me fatigue pas : l'application $f \mapsto \omega_f$ est injective (car les valeurs de k que l'on prend sont deux à deux non congruentes mod $(p-1)$), et un petit calcul montre que les deux espaces considérés ont même dimension. Cqfd.

<u>Exemple</u>. Si $p = 13$, la seule valeur de k pour laquelle $S_k \neq 0$

25/5/79

est $k = 12$, et S_{12} a pour base $Q^3 - R^2$. On en conclut que la courbe d'Igusa est de genre 1 (ce qu'on savait, cf. p.9), et qu'elle a pour différentielle de première espèce la différentielle $\omega = (Q^3 - R^2)dq/q = 3RdQ - 2RdR$ (qui se trouve d'ailleurs être égale à $2dQ/R$ compte tenu de la relation $6Q^3 + 8R^2 = 1$).

Remarque - Je suis un peu étonné de n'avoir jamais vu ce résultat si simple dans la littérature. Peut-être est-il dissimulé dans les nombreuses pages que Katz a écrites sur le sujet ?

Fonctorialité - On a vu (p.9) que Q et R sont de poids 4 et 6 du point de vue de l'action (à droite) des R_d :

$$Q|R_d = d^4Q \quad \text{et} \quad R|R_d = d^6R \qquad (d \in (\mathbb{Z}/p\mathbb{Z})^*).$$

La formule donnant ω_f montre alors que ω_f est de poids $h = k-2$ i.e.

$$\omega_f|R_d = d^h\omega_f = \omega(d)^h\omega_f ,$$

avec les notations de la page 7; autrement dit, ω_f est une forme modulaire de type $(2,\omega^h)$ sur la courbe d'Igusa.

Note aussi que $f \longmapsto \omega_f$ commute aux opérateurs de Hecke T_ℓ, avec $(\ell,p) = 1$; cela se voit sur le développement en série de puissances, combiné avec le fait que

$$\ell^{k-1} \equiv \ell\,\omega^h(\ell) \pmod{p}.$$

Quant à l'opérateur T_p, il se transforme évidemment en l'opérateur U induit par la "Verschiebung" V (il y a là un hasard malheureux ; les "modulaires" appellent V un autre opérateur; tâche de t'y retrouver !).

b.2. Formes de 1ère espèce sur $X_1(p)$ et sur X

Je reviens en caract.0; plus précisément, je me place sur l'anneau $\underline{Q}$. Je m'intéresse aux formes différentielles de 1ère espèce sur $X_1(p)$, autrement dit aux formes modulaires de poids 2 Si T est une correspondance sur $X_1(p)$, je fais opérer T à droite (i.e. par fonctorialité) sur les formes différentielles ; j'écris $\omega|T$, comme ci-dessus.

Sur le schéma $\underline{X}_1(p)$, il y a un faisceau naturel $\underline{\Omega}$ qui prolonge le faisceau des formes différentielles sur la fibre générique. C'est le faisceau "dualisant relatif" (j'espère que je ne dis pas de bêtise !). Je noterai Ω l'ensemble de ses sections. C'est un $\underline{Q}$-réseau dans l'espace vectoriel des formes de 1ère espèce sur $X_1(p)$ à coefficients dans le corps des fractions $Q_p(z)$ de $\underline{Q}$. Si π est une uniformisante de $\underline{Q}$, le quotient $\Omega/\pi\Omega$ s'identifie aux "formes de 1ère espèce" sur la courbe (singulière)

ω : caractère de Teichmüller !

$X \cup X'$. Comme les deux morceaux sont lisses, et que l'intersection $\Sigma = X \cap X'$ est transversale (si j'ose dire), une telle forme de 1ère espèce n'est autre qu'un <u>couple</u> (ω, ω'), où ω et ω' sont des formes diffelles sur X et X' ayant les propriétés suivantes :

a) ω et ω' sont holomorphes en dehors du lieu supersingulier Σ ;

a') en tout point de Σ, ω et ω' ont au plus un pôle simple et leurs résidus en ce point sont opposés.

(Dans "Gr.Alg.et C.de Cl." , j'appelle ça les différentielles <u>régulières</u>, au sens de Rosenlicht, voir par exemple p.76.)

Bien sûr cet isomorphisme entre $\Omega/\pi\Omega$ et l'ensemble des couples (ω,ω') de ce type commute à tout ce qu'on veut, et en particulier aux opérateurs R_d . Je ne m'intéresse ici qu'aux formes ayant un caractère $\varepsilon = \omega^h$ non trivial (i.e. $2 \leq h \leq p-3$). (Elles correspondent aux formes invariantes sur la variété abélienne A utilisée plus haut.) Notons Ω_A l'espace de ces formes. On a alors :

Théorème - <u>L'application ci-dessus induit un isomorphisme entre $\Omega_A/\pi\Omega_A$ et $\Omega \times \Omega'$ où Ω (resp. Ω') est l'espace des formes de 1ère espèce sur la courbe d'Igusa</u> X (resp. sur X').

Cela résulte de ce qui précède compte tenu des faits suivants :

i) une forme de 1ère espèce sur X , $\neq 0$, ne peut pas être invariante par les R_d (car elle proviendrait d'une forme sur la droite projective, qui est de genre 0 - ça résulte aussi du th. de la p.13);

ii) une forme ω sur X telle que $\omega \mid R_d = \varepsilon(d)\,\omega$ avec $\varepsilon \neq 1$ ne peut pas avoir de pôle simple sur Σ (ça provient de ce que les R_d fixent les points de Σ).

(Variante : utiliser le fait que A a bonne réduction sur $\underline{0}$, et que sa réduction est $J \times J'$.)

[Ce qui se passe pour la partie fixe par les R_d est bien connu, et ne m'intéresse pas ici.]

25/5/79

Description "explicite" du réseau Ω

On considère une forme différentielle $\omega = \sum a_n q^n \frac{dq}{q}$ sur $X_1(p)$, à coefficient dans $Q_p(z)$. On cherche à quelle condition elle appartient au réseau Ω. Soit $\sum b_n q^n \frac{dq}{q}$ le développement de $\omega | W_z$ où z est une racine primitive p-ème de 1.

Proposition - Pour que ω appartienne à Ω, il faut et il suffit que les coefficients a_n et b_n de ω et $\omega | W_z$ appartiennent à l'anneau Q.

Il est clair que c'est nécessaire. Pour voir que c'est suffisant, on remarque que l'ensemble des points du schéma $X_1(p)$ où ω "n'est pas une section" (i.e. "a un pôle") du faisceau inversible Ω est un diviseur. Or l'hypothèse faite sur ω entraîne que les points ∞ et $W_z\infty$ de X et de X' n'appartiennent pas à ce diviseur. Comme le diviseur en question est concentré sur la fibre spéciale, il ne peut être que $\emptyset$.

Remarque. Pour les formes sur $X_0(p)$, i.e. invariantes par les R_d, le fait que ω soit à coefficients dans Q entraîne la même propriété pour $\omega | W_z$ (cf. mon exposé à Anvers, p.228, th.11). Il n'en est pas de même pour les formes de Ω_A.

b.3. Où l'on met ensemble b.1 et b.2

Revenons aux notations de b.1, et posons $S = \bigoplus_{k=2}^{p-1} S_k$ (formes paraboliques mod p sur $SL_2(Z)$, de poids $\leq p-1$).

On a vu au n° b.1 que l'on peut identifier S à l'espace Ω des formes de 1ère espèce sur X. Comme $\Omega_A/\pi\Omega_A = \Omega \oplus \Omega'$, cela conduit à écrire :

$$(*) \qquad \Omega_A/\pi\Omega_A \simeq S \oplus S' ,$$

en convenant que $S' = \Omega' = S | W_z$.

C'est cet isomorphisme qui fait le pont entre formes modulaires sur $SL_2(Z)$ et formes de poids 2 sur $\Gamma_1(p)$. Ses propriétés fonctorielles sont agréables : définissons H_Z comme la Z-algèbre d'endomorphismes de A engendré par les T_ℓ, les R_d, U et U' (cf.§a). Alors Ω_A est de façon naturelle un H_Z-module à droite, et l'on a :

Théorème - (i) S et S' sont des sous-H_Z-modules de $\Omega_A/\pi\Omega_A$.
(ii) Sur S, les opérateurs T_ℓ, R_d, U et U' sont les suivants :
T_ℓ est l'opérateur de Hecke usuel ;
R_d est tel que $f|R_d = d^{k-2}f$ si $f \in S_k$;
U est l'opérateur T_p (ou U, cela revient au même puisqu'on est en caract. p) ;
U' est l'opérateur 0.

Tout ceci est essentiellement clair. La seule chose un peu surprenante est la dernière assertion : l'opérateur U' est 0 sur S (ou ce qui revient au même sur Ω). Mais on a vu que U' donne sur $J \times J'$ l'opérateur égal à F (Frobenius) sur J et V (Verschiebung) sur J'. Son action sur les formes différentielles de J est donc 0.

Note aussi qu'il n'y a pas lieu d'énoncer un (ii') relatif à S' : le fait que $S' = S|W_z$, et les identités du § a.2 suffisent.

Le but de ce § est maintenant atteint : on sait passer d'un système de valeurs propres du côté S à un système du côté Ω_A. Plus précisément, suppose que tu partes d'un système de valeurs propres (a_ℓ, a_p) des T_ℓ et de T_p (dans une extension de F_p) donné par une forme parabolique appartenant à S_k $(2 \leq k \leq p-1)$. Le th. précédent te dit que ce système "se trouve" quelque part dans $\Omega_A/\pi\Omega_A$, pour le caractère $\varepsilon = \omega^h$ (où $h = k-2$), avec les mêmes valeurs propres, et avec $a'_p = 0$. Avec les notations de a.5, on a donc un système de type I si $a_p \neq 0$ et un système de type II si $a_p = 0$; on n'attrape jamais un système de type I' (ce sont les vecteurs propres de S' qui les donnent), ce qui est bien agréable. En combinant ça avec le th.de la p.7, on obtient le résultat que tu avais deviné :
THÉORÈME FINAL - L'action de l'inertie modérée dans une représentation p-adique provenant d'une forme parabolique de poids $k \leq p-1$ sur $SL_2(Z)$ est donnée par les caractères suivants :
(i) le caractère 1 et le caractère χ_1^{k-1} si $v_p(a_p) = 0$
(ii) les caractères χ_1^{k-1} et $\chi_2^{p(k-1)}$ si $v_p(a_p) > 0$.

OUF !

25/5/79

Remarque - Dans le cas (i), il ne doit pas être trop difficile de prouver que l'on peut choisir la repr. galoisienne mod p correspondant à la forme f de telle sorte que χ_1^{k-1} soit donné par une droite, et le caractère 1 par le quotient par cette droite, la valeur propre de Frobenius sur ce quotient étant a_p. On ne peut pas s'attendre en général à ce qu'il y ait complète réductibilité de l'inertie. Voici ce que je peux dire à ce sujet (je suppose la repr. globale irréductible, pour simplifier) :

suppose qu'il existe une forme parabolique f' de poids k' tel que $k + k' = p+1$ telle que $\Theta^N f' = \Theta^{N+1-k} f$ pour $N \geqslant k$ (ce qui revient à dire que les valeurs propres a'_ℓ des T_ℓ pour $\ell \neq p$ sont $\ell\, a'_\ell = \ell^{1-k} a_\ell$, ou encore que la repr. mod p attachée à f' est isomorphe à celle de f tordue par χ_1^{1-k}. Alors la repr. de l'inertie dans ces deux repr. est semi-simple ; c'est clair si on admet ce que j'ai dit plus haut, car les deux caractères jouent des rôles symétriques dans les deux représentations, donc chacun d'eux peut être aussi bien en sous-truc qu'en quotient, si j'ose dire.

Pour de petites valeurs de k et surtout de p, on peut tester l'existence ou la non-existence de la forme "compagnon" f'. (Elle existe rarement en pratique. Le cas de $k = (p+1)/2$, où $k = k'$, est fort intéressant; on en reparlera peut-être, car il serait possible de faire faire (par H.Cohen ?) des calculs sur machine.)

Conjecture.- La repr. de l'inertie en caract. p est semi-simple si et seulement si f possède une forme compagnon f' au sens ci-dessus. (Ça me paraît raisonnable, mais je n'ai pas beaucoup d'exemples à me mettre sous la dent ...)

b.4. Une autre définition de la projection $\Omega_A/\pi\Omega_A \to S$

La méthode que j'ai suivie plus haut est "géométrique" : j'ai utilisé de façon essentielle le modèle de Deligne-Rapoport et la courbe d'Igusa. Il est rassurant d'avoir un argument analytique (si j'ose dire) qui redonne essentiellement l'isomorphisme

$$(*) \qquad \Omega_A/\pi\Omega_A \simeq S \oplus S' \ .$$

Voici cet argument (qui généralise celui de mon exposé d'Anvers, pour les formes de poids 2 sur $\Gamma_0(p)$, cf. p.228, th.11) :

On <u>définit</u> Ω_A par les propriétés de la prop. de la p.16 : c'est l'ensemble des formes de 1ère espèce ω sur $X_1(p)$, ayant un caractère $\varepsilon = \omega^h$, avec $2 \leq h \leq p-3$, qui sont telles que les coeff.de ω et de $\omega|W_z$ sont dans O.

Il s'agit de prouver :

Théorème - <u>Si</u> $\omega = \sum a_n q^n (dq/q)$ <u>appartient à</u> Ω_A, <u>la réduction</u> (mod π) <u>de la série</u> $\sum a_n q^n$ <u>appartient à l'espace</u> S_k (où $k = h+2$) <u>des formes paraboliques de poids</u> k <u>sur</u> $SL_2(Z)$.

(Cela donne la projection $\Omega_A/\pi\Omega_A \to S$; en combinant avec W_z on en déduit $\Omega_A/\pi\Omega_A \to S \times S$, qui est visiblement injectif, donc surjectif pour des raisons de dimensions.)

<u>Démonstration</u>.

Considère la série d'Eisenstein

$$G_h(\omega^{-h}) = \tfrac{1}{2}L(1-h, \omega^{-h}) + \sum_{n=1}^{\infty} \sum_{d|n} d^{h-1}\omega^{-h}(d)\, q^n \ .$$

La valuation p-adique de son terme constant est -1 (analogue de Clausen - von Staudt). En la multipliant par l'inverse de ce terme (i.e. par une constante de valuation +1), on trouve une série $E_h(\omega^{-h})$, dont le développement à la pointe ∞ est 1 (mod p).

D'autre part, un calcul un peu embêtant (qui devrait se trouver dans la littérature) montre que

$$G_h|W_z = c\, G_h' \ ,$$

où G_h' est " l'autre" série d'Eisenstein de poids h et de caractère ω^h (i.e. $\sum_n \left(\sum_{d|n} d^{h-1}\omega^h(n/d)\right) q^n$), et où c est une constante (où figure une somme de Gauss) avec

$$v_p(c) = \frac{h}{2} - 1 + \varepsilon \quad , \text{ avec } \varepsilon > 0$$

($\varepsilon > 0$ provient de la valuation de la somme de Gauss).

En passant à $E_h(\omega^{-h})$, il en résulte que son transformé par W_z est divisible par $p^{h/2 + \varepsilon}$, si j'ose dire .

Considère alors la forme $F = F_h(\omega^{-h}).(\sum a_n q^n)$. C'est une forme de poids $k = h+2$ sur $\Gamma_0(p)$, de caractère $\varepsilon = 1$. Soit $Tr(F) = f$ la forme de poids k sur $SL_2(Z)$ qui est la trace de F (cf. Anvers, p.223). Je dis que f répond aux conditions, i.e. que son développement en caract. p est $\sum a_n q^n$. En effet, d'après le lemme 7 d'Anvers, on a

$$Tr(F) = F + p^{1-k/2}(F \mid W_z) \mid U .$$

Mais je me suis arrangé pour que $F \mid W_z$ soit divisible par $p^{h/2+\varepsilon}$. Comme $k/2 = 1 + h/2$, cela montre que le second terme de $Tr(F)$ donne 0 en caract. p. Comme $F \equiv f \pmod p$, cela démontre le théorème.

(J'ai la flemme de rédiger le calcul " un peu embêtant " de c, tu me comprendras !)

Si l'on adoptait ce point de vue terre à terre, on aurait besoin de nettement moins de choses sur la courbe d'Igusa. En fait, la meilleure solution serait de mettre les deux méthodes dans le papier.

Voilà, c'est tout, du moins pour le moment. Il faudrait pourtant :

i) rédiger l'application à 59 : ça va tout seul grâce à la borne d'Odlyzko;

ii) étendre tout le fourbi aux formes modulaires avec un niveau N (premier à p). Je crois que, dans ce cas, on ne coupera pas à monter jusqu'à $\underline{O}$ lui-même (et pas seulement à $\underline{O}^+$); il faudrait que tu voies ce que tu peux faire.

Salut et fraternité. Amitiés à tes femmes

J-P. Serre

Adresse jusqu'à Bourbaki : Math.Inst. , 10 Wegelerstr., D 5300, BONN, Allemagne.