Jean-Pierre Serre
E. Bayer (réd.)
C. Goldstein (réd.)

Formes modulaires (mod p)

Cours de Jean-Pierre Serre, tome 8 (1988)
<http://www.numdam.org/item?id=CJPS_1988__8_>

Formes Modulaires (mod p)

J-P. Serre

Cours 1987-88

Notes de E. Bayer et C. Goldstein

Collège de France, 1988

Cours 1987-88

Formes de niveau 1 mod p → p. 59

Notations E_k, $P, Q, R, \ldots$ standard

$A = E_{p-1}$, $B = E_{p+1}$

Définitions de l'invariant de Hasse E_{p-1} → p. 64

Courbes supersingulières (rappels) → p. 66

Formule $\sum \frac{1}{|\mathrm{Aut}\, E|} = \frac{p-1}{24}$, Eichler–Deuring, p. 67

Tous les j s.s. sont dans $\mathbb{F}_p \iff$ genre de $X_0(p)^+ = 0 \iff p$ divise l'ordre du monstre $\iff p = 2,3,5,7,11,13,17,19,23,29,31,41,47,59,71$ → p. 69

Il y a un j s.s. $\in \mathbb{F}_p$ (avec $\pi^2 = -p$) → p. 70

Structure canonique sur $\mathbb{F}_{p^2}$ avec $\pi = -p$ → p. 72

D'où une base canonique de $\omega^{p^2-1}(E)$: si $p \geq 5$, c'est $E_{p+1}^{p-1} = B^{p-1}$ → p. 74

Th. d'isogénie (G. Robert) $\varphi : E \to E'$ isogénie de courbes s.s., alors $\varphi^* B(E') = \deg \varphi \cdot B(E)$ → p. 74

L'invariant $\Gamma \in \omega^{p+1}(E)$: p. 75 … ; on a $\Gamma = -\frac{1}{12} B$ (Oesterlé, p. 87)

La filtration des formes modulaires mod p

$(p \geq 5)$ $\quad 0 \to M_{k-(p-1)} \to M_k \to W_k \to 0$ p. 78

avec $W_k \subset S_k =$ "formes de poids k sur les courbes s.s."

et $W_k = S_k$, $k \geq p+2$ (k pair, bien sûr)

Les S_k sont périodiques de période p^2-1 et même

$$S_{k+p+1} \simeq S_k[1]$$ p. 80

Suite exacte de faisceaux

$$0 \to \mathcal{M}_{k-(p-1)} \to \mathcal{M}_k \to \mathcal{S}_k \to 0 \quad ; \quad S_k = H^0(\mathcal{S}_k).$$

Le quotient S_k / W_k est isomorphe au dual de $W^{cusp}_{p+1-k}[k-1]$ p. 83

Accouplement défini grâce à la formule (p. 83)

$$a_0(f) = -12 \sum_{E\ ss} \frac{1}{w_E} \left(\frac{f}{B}\right)(E) \qquad f \in M_{p+1}$$

$$w_E = \tfrac{1}{2}\,|\mathrm{Aut}\, E|$$

Cet accouplement satisfait à $\langle T_\ell f, g \rangle = \ell^{k-1} \langle f, T_\ell g \rangle$

L'identification se fait par une 3° interprétation : les classes de modules projectifs (à gauche) de rang 1 sur $D_{\mathbb{Z}}$, munis de base mod N p. 108-109

Démonstration au moyen de résultats de Deuring, Tate, Eichler p. 109-113

Formules donnant les opérateurs de Hecke

Lien avec les repr. galoisiennes p. 116

Théorème - Les syst de val. propres des op. de Hecke sur $G_A/G_{\mathbb{Q}}$ (en car. p) sont ceux donnés par les formes modulaires (mod p). p. 118

Critiques p. 119

Représentation de GL_2 en car. p p. 121

$G = GL_2(K)$, K local ; k = c. résiduel ; $q_k = |k|$; p_k = car. k ;

F = corps des valeurs ; p_F = car. F ; X = arbre

(Dans la suite $K = \mathbb{Q}_\ell$, $F = \overline{\mathbb{F}}_p$.)

Rep. universelle pour | action triviale du centre
| vecteur fixé par $GL_2(O_K) = G_0$, f-propre de Hecke pour $a \in F$ donné

C'est le G-module $C_0/(T-a)C_0 = H_a$ où C_0 = 0-chaînes finies de X p. 123
T = op. Hecke

Alors H_a admissible et dim $H_a^{G_0} = 1$. De plus (pour $p_F \neq p_k$)

1) Si $a \neq \pm(q_k+1)$ dans F, H_a est irréd. ($\simeq$ module induit I_λ)

2) Si $a = q_k + 1$, $\neq 0$ ds F, $0 \to H_a^0 \to H_a \to 1 \to 0$ où

$H_a^0 = C_0^0/(T-a)C_0 \simeq St$ irréd.

2') itou si $a = -(q_k+1)$: torsion par $\varepsilon : G \to \pm 1$

3) Si $a = q_k+1 = 0$ dans F, $C_0 \supset C_0^{0,0}$ (0-chaînes de somme 0 sur les sommets pairs et impairs) et $H_0^{00} = C_0^{00}/TC_0$:

$0 \to H_0^{00} \to H_0 \to r_2 \to 0$ p. 124-126

où r_2 = rep. rég. de ± 1 et H_0^{00} irréd.

Interpr. de H_a^0, si $a = q+1$, comme $St = H_c^1(X,F)$ et bouts de l'arbre p. 131

Cours 1987 – 1988

FIN

5/10/87

J-P. Serre, cours 1987

Groupes de Galois et formes modulaires

Historique du sujet :

Formes modulaires

$$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n \qquad q = e^{2\pi i z}, \quad \mathrm{Im}(z) > 0$$

$$= q \prod_{n=1}^{\infty} (1-q^n)^{24}$$

$$\tau(nn') = \tau(n)\tau(n') \quad \text{si} \quad (n,n') = 1$$

$$L_\Delta(s) = \sum \tau(n) n^{-s}$$

$$= \prod_p \frac{1}{1-\tau(p)p^{-s} + p^{11-2s}}$$

$k = 12, \quad 11 = k-1$

$$= \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\alpha_p' p^{-s})}$$

$$(1-\alpha_p T)(1-\alpha_p' T) = 1 - \tau(p) T + p^{11} T^2$$

produit eulérien "de rang 2"

fait penser à $\quad L(s) = \prod \frac{1}{1-\chi(p)p^{-s}}$

prol. analytique
équation fonctionnelle $\Big\}$ Hecke

inv. par $s \longmapsto 12-s$, fact. eul. $(2\pi)^{-s}\Gamma(s)L_\Delta(s)$

(2

Produits eulériens du type géom. alg.

1.) Courbes elliptiques

$E/\mathbb{Q}$, $\widetilde{E}_p$ réd. mod p, $p \nmid \Delta_E$

$\widetilde{E}_p/\mathbb{F}_p$ courbe elliptique

$\widetilde{E}_p$ a un endomorphisme de Frob.

$$\pi_{E,p} : \widetilde{E}_p \longrightarrow \widetilde{E}_p$$
$$(x,y) \longmapsto (x^p, y^p)$$

$$\begin{cases} a_p = Tr(\pi_{E,p}) \in \mathbb{Z} \\ p = N(\pi_{E,p}) \end{cases}$$

$\pi_p, \pi_p' \in \mathbb{C}$, $\begin{cases} a_p = \pi_p + \pi_p' \\ p = \pi_p \pi_p' \end{cases}$

$\pi_p' = \overline{\pi_p}$

$$1 - a_p T + p T^2$$

$$L_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

(aux mauvais termes près, i.e. $p \nmid \Delta_E$)

Problème: Déterminer la variation de a_p avec p.

Eichler (1954)

Pour certaines courbes elliptiques (extraites des Jacobiennes des courbes modulaires)

$L_E = L$ associé à des formes modulaires de poids 2.

aux mauvais facteurs près

Les résultats de Eichler ont été complétés par Shimura et Igusa. (précise les p de mauvaise réduction : $p \nmid$ niveau $\Rightarrow p$ bonne réduction)

(fin des années 1950)

On arrive à un point dont l'histoire est controversée.

~1966 Weil a formulé une conjecture (appelée auj. conj. de Taniyama-Weil, mais la conj. énoncée par T. est (sans doute) fausse en général).

Toute courbe elliptique /$\mathbb{Q}$ est obtenue par le procédé d'Eichler, et le niveau est égal au conducteur de la courbe.

Représentations galoisiennes

$\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\underline{\mathbb{Q}_\ell})$ ou une ext. finie de $\mathbb{Q}_\ell$.

continue

Exemple : Si $E/\mathbb{Q}$

$$E_{\ell^n} = \operatorname{Ker} \ell^n : E(\overline{\mathbb{Q}}) \longrightarrow E(\overline{\mathbb{Q}})$$

$$\simeq (\ell^n, \ell^n) \simeq H_1(E, \mathbb{Z}/\ell^n\mathbb{Z})$$

$$T_\ell(E) = \varprojlim E_{\ell^n} \simeq \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$$

donne représentation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \begin{array}{c} GL_2(\mathbb{Z}_\ell) \\ \cap \\ GL_2(\mathbb{Q}_\ell) \end{array}$$

Soit S l'ensemble des p divisant $\Delta(E)$

Alors

① $\rho_{E,\ell}$ est non ramifiée en dehors de $S \cup \{\ell\}$

② Si $p \neq \ell$, $p \notin S$
$\rho_{E,\ell}(\mathrm{Frob}_p) \in GL_2(\mathbb{Q}_\ell)$
est défini à conjugaison près.

$$\operatorname{Tr} \rho_{E,\ell}(\mathrm{Frob}_p) = a_p$$

$$\det \text{———''———} = p.$$

$$L_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{\det(1 - \rho_{E,\ell}(\mathrm{Frob}_p)\, p^{-s}}$$

Eichler :

$k=2 \longrightarrow$ c. ell $\longrightarrow H_1$

On peut se demander pour k quelconque,
il y a une relation

formes modulaires $\longleftrightarrow$ représentation ~~cohomologie~~
l-adiques fournies
par la cohomologie
de poids $k-1$.

Une forme modulaire de poids k définit une
repr. l-adique de "poids $k-1$" provenant
de la cohomologie d'une variété.

(Deligne 1967).

Quelle est l'image ?

<u>Conjecture</u> (de TW généralisée)

On devrait trouver tout (?)

<u>Conjecture</u> sur un dictionnaire possible

repr. gal. de d°2 de $G_{\mathbb{Q}}$
sur un corps fini : (de car p)

et

formes modulaires mod p.

$\mathbb{F}_p \subset \overline{\mathbb{F}}_p$

$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_p)$ ρ continue

Ker ρ est ouvert

Im ρ est finie

$$\begin{array}{l} K \\ \big| G \hookrightarrow GL_2(\mathbb{F}_q) \\ \mathbb{Q} \end{array}$$

Si S = ens. des ℓ où ρ est ramifiée

et $\ell \notin S$, on a $\rho(\mathrm{Frob}_\ell) \in \mathrm{Im}\,\rho$

définie à conj. près.

ℓ nombre premier

$$\begin{array}{ll} \lambda & K \\ & \big| G \\ \ell & \mathbb{Q} \end{array}$$

λ prol. de la valuation ℓ-adique à K

D_λ = groupe de déc. de $\lambda = \{ s \in G \mid s\lambda = \lambda \}$

I_λ = groupe d'inertie = $\{$ — et opèrent trivialement sur le corps. rés. de λ $\}$

D_λ / I_λ est cyclique avec générateur "Frob" : $x \longmapsto x^\ell$ sur le corps résiduel.

Tout ceci est bien défini à conjugaison près.

ρ ramifié en $\ell \overset{\text{déf}}{\Longleftrightarrow} \rho(I_\lambda) \neq \{1\}$.

$$\begin{cases} \operatorname{Tr} \rho(\mathrm{Frob}_\ell) = a_\ell \\ \det \rho(\mathrm{Frob}_\ell) = \omega(\ell) \end{cases}$$

La connaissance de a_ℓ et $\omega(\ell)$ suffit presque pour reconstituer ρ:

<u>Thm</u> : A semi-simplification près, ρ est déterminée par les a_ℓ, $\omega(\ell)$

semi-simplification : somme des quotients de Jordan-Hölder.

Le thm découle de Čebotarev.

Si $p \neq 2$, les a_ℓ suffisent.

pas vrai en car 2, car si $\rho = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$,

$\operatorname{Tr} \rho = 0$!

<u>Hypothèse</u> sur la conj. complexe.

$$\begin{tikzcd} K \arrow[r, hook] \arrow[d, dash, "G"] & \mathbb{C} \\ \mathbb{Q} & \end{tikzcd}$$

Il existe un unique $c \in G$ t.q. $c(z) = \bar{z}$ pour tout $z \in K$. On a $c^2 = 1$.

La classe de conjugaison de c est bien définie

(c est le Frob. attaché à $\ell\infty$).

$c = \mathrm{Frob}_\infty \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

valeurs propres de $\rho(c)$ sont $\in \{+1, -1\}$

si car $= 2$, on ne distingue pas entre les ?...

Supposons $p \neq 2$.

3 cas : $1, 1, 1$
$1, -1, -1$
$-1, -1, 1$

Conditions sur ρ :

$$(*) \begin{cases} 1.) & \rho \text{ semi-simple} \\ 2.) & \text{Si } p \neq 2, \ \det \rho(c) = -1 \\ & \Longleftrightarrow \ \rho(c) \sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{cases}$$

$$\det \rho : G_{\mathbb{Q}} \longrightarrow \overline{\mathbb{F}}_p^*$$

caractère de $G_{\mathbb{Q}}$

$$\det \rho : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{F}_p^*$$
$$\begin{array}{c} \cup \\ -1 \end{array}$$

2.) $\Longleftrightarrow$ $\det \rho$ est un caractère impair.

Objets à comparer :

- $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_p)$

- Côté modulaire

Formes modulaires mod p de niveau donné

$\Gamma = SL_2(\mathbb{Z})$

$\Gamma_0(N) =$ s/g des $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $c \equiv 0 \bmod N$

$\Gamma_1(N) =$ ——— " ——— $d \equiv 1 \bmod N$

opèrent sur le demi-plan supérieur,

$\mathrm{Im}(z) > 0$.

$f(z)$ avec comportement vis-à-vis de $\Gamma_0(N)$ imposé.

Poids k entier positif

Caractère $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$

(on définit d'abord les formes modulaires sur $\mathbb{C}$, puis on réduit mod p).

$$f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z)$$

pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

$$f|_k \gamma(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

$$f|_k \gamma = \varepsilon(\gamma) f$$

+ holomorphie aux pointes. Formes paraboliques : 0 aux pointes.

Opérateurs de Hecke T_p :

T_p agissent sur ces formes

caractérisées par :

Si : $f = \sum a_n q^n \qquad q = e^{2\pi i z}$

Si $p \nmid N$, $T_p(f) = \sum a_{pn} q^n + p^{k-1} \varepsilon(p) \sum_{n \equiv 0 (p)} a_{(n/p)} q^n$

formule analogue pour $p \mid N$

dans ce cas, on préfère les appeler U_p

$$U_p : \sum a_n q^n \longmapsto \sum a_{pn} q^n$$

Supposons que f soit fonction propre des T_p, avec valeurs propres a_p

Deligne : repr. ℓ-adique ρ_ℓ, non ramifiée en dehors de ℓN, avec
1967

$$\mathrm{Tr}\, \rho(\mathrm{Frob}_p) = a_p, \quad \det = p^{k-1} \varepsilon(p)$$

cette repr. est ds une ext finie de $\mathbb{Q}_\ell$

$a_\ell \in$ corps de nombres $\hookrightarrow \overline{\mathbb{Q}_\ell}$.

le corps des tr. contient les valeurs des det

Par réduction "mod ℓ" à partir des ρ_ℓ de Deligne, on obtient des représentations dont la semi-simplifiée est de type (*) (avec $p = \ell$, [illegible] le trouve toutes comme ça (à préciser !)

Conjecture (à préciser)

Toute représentation galoisienne

$\rho : G_{\mathbb{Q}} \longrightarrow GL_2$ (corps fini)

satisfaisant $(*)$ est obtenue ainsi.

La conjecture précise k et N.

---

k et N sont décrits dans Duke, §§ 1 et 2.

N : conducteur d'Artin de ρ, $N(\rho)$.

$$\begin{array}{ccc} K & \lambda & D_\lambda \supset I_\lambda \\ \mid G \text{ gal.} & & \text{gr. d'inertie} \\ \mathbb{Q} & \ell & \end{array}$$

$s \in D_\lambda$, alors $s \in I_\lambda \iff sx \equiv x \bmod \mathfrak{p}_\lambda$ $\forall\, x$ entier $\in O_K$.

$I_\lambda^n = \{ s \mid sx \equiv x \bmod \mathfrak{p}_\lambda^{1+n} \}$ $\forall\, x \in O_K$

$$D_\lambda \supset I_\lambda = I_\lambda^0 \supset I_\lambda^1 \supset \cdots$$

Si ρ repr. de G, $\rho : G \longrightarrow GL(V)$ (dim $V = 2$ ici)

On attache à ℓ un entier $n_\ell(\rho)$:

$$n_\ell(\rho) = \frac{1}{|I_\lambda^0|} \sum_{n=0}^{\infty} |I_\lambda^n| \operatorname{codim} V^{I_\lambda^n}$$

Thm : $n(\rho) \in \mathbb{Z}$.

$n(\rho) = 0 \iff$ repr. non ramifiée en ℓ.

$N(\rho) = \prod_{\ell \neq p} \ell^{n_\ell(\rho)}$: conducteur d'Artin de ρ

premier à p par construction.
mesure la ramification de ρ en dehors de p

$k(\rho)$: poids, ε : caractère.

$k(\rho)$ mesure la ramification en p de ρ.

(ou plutôt $k(\rho) - 1$ la mesure :
$k(\rho) = 1 \iff \rho$ non ramifiée en p).

Conjecture
Toute repr. ρ vérifiant $(*)$ provient d'une forme parabolique de poids $k(\rho)$, caractère ε, niveau $N(\rho)$.

On se restreint aux ρ irréductibles, car sinon il est difficile de préciser le poids et le niveau.

(e.g. $1 + \chi \leftrightarrow E_2$: n'existe pas !
il faut augmenter le niveau).

Des contre-exemples existent si $p = 2$ ou 3.
Ces contre-ex. disparaissent si on change :
soit la définition des formes de car ε
soit — " — mod p.

Définition directe (ss demander rel. en car 0)
de Katz, 1972.
soit si on refuse en car 2 les repr. induites prov. de $\mathbb{Q}(\sqrt{-1})$, et
en car 3 ——— $\mathbb{Q}(\sqrt{-3})$.

Exemples et applications

Conj. faite la 1ère fois en 1974
Objections de Deligne :

1.) conjecture $\Rightarrow$ tte repr. ρ de type (*) est réduction d'une repr "en car 0"
$G_{\mathbb{Q}} \longrightarrow GL_2$ (ext. finie de $\mathbb{Q}_p$).
Difficile à tester numériquement, comme l'ext. finie n'est pas précisée. (l'image sera infinie en gén.)

2.) Une repr. ρ provenant d'une forme modulaire de niveau $N = \ell^\alpha M$ peut (nombreux ex.

être non ramifiée en un $\ell \in \mathbb{N}$.

La conjecture prédit que ρ provient d'une forme de niveau M.

Ceci est (presque) un théorème de Ribet ($k = 2$, $\varepsilon = 1$, $\alpha = 1$: c'est le cas crucial)

Applications :

Frey : Fermat $\Leftarrow$ conj

(et équations associées)

trivialité des schémas en groupe de type (p,p) sur $\mathrm{Spec}(\mathbb{Z})$ $\Leftarrow$ conj

(il n'y a que les évidents :

$\mathbb{Z}/p\mathbb{Z} \oplus$ —

— $\oplus \mu_p$

$\mu_p \oplus \mu_p$

et un 4^e pour $p = 2$

(Mazur, Eisenstein IHES)).

Thm (Fontaine)

pour $p \leq 17$, tout schéma en groupes de type $(p, \dots, p)$ irréd. est $\mathbb{Z}/p\mathbb{Z}$ ou μ_p

class. existe ~~Vrai~~ aussi ds le cas réd : somme de $\mathbb{Z}/p$, μ_p et ex. de Mazur

Taniyama-Weil $\Leftarrow$ conj

(généralisations)

exemple : X proj. lisse / $\mathbb{Q}$

$H^m(X_{\mathbb{C}}, \mathbb{C})$

hypothèses : m impair

$\dim H^m = 2$

type Hodge est $(m,0)+(0,m)$

(X courbe elliptique, $m=1$)

Représentation ℓ-adique ds $H_m(X, \mathbb{Q}_\ell)$ (étale)

ρ rep. de $d^\circ 2$

conj $\Rightarrow$ ρ provient d'une forme parabolique de poids $m+1$ car 1.

exemples de C. Schoen, $m=3$.

N : pas trop d'ennuis

k : en relation avec la ramification en ℓ

Fontaine, Fontaine-Messing.

Théorème (modulo la conjecture pour $p \neq 2,3$)

Soit L un nombre premier, ni de Fermat (2^n+1) ni de Mersenne (2^n-1)

Soit $\alpha \geq 0$. Il existe ~~$\exists$~~ $P(L)$ calculable t.q. si $p \geq P(L)$, alors

l'équation

$$X^p + Y^p + L^\alpha Z^p = 0$$

n'a pas de solution

Ex : $L = 3, 5, 7, 11, 13, 17, 19, 23, 29,$ non $31, 37,$

~~et~~ $P(L) = 11$ pour $L \leq 29$.

Frey courbe elliptique associée à une solution

$$a^p + b^p + L^\alpha c^p = 0 \qquad a, b, c \text{ premiers entre eux}$$

$$\overset{\shortparallel}{A} + \overset{\shortparallel}{B} + \overset{\shortparallel}{C} = 0$$

$$y^2 = x(x-A)(x+B) \qquad A \equiv -1 \ (4), \quad B \equiv 0 \ (32)$$

A, B, C : permutation de $\{a^p, b^p, L^\alpha c^p\}$

ρ_p définie par les points de p-division de la courbe. $N(\rho) = \text{cond.} = 2L$, $k(\rho) = 2$.

th de Mazur $\Rightarrow$ ρ est irréductible.

Liste des "new forms" de niveau $2L = N$
poids 2

$f^{(1)}, \dots, f^{(i)}$

Alors : Si f est l'une de ces formes, ou bien les coeff. de f ne sont pas tous ds $\mathbb{Q}$, ou bien ils sont tous ds $\mathbb{Q}$ mais $a_p \not\equiv 1+p \pmod{p}$ pour une infinité de p.

A cause du fait que L n'est ni Fermat ni Mersenne.

Sinon, on a une courbe modulaire E_f dont les points d'ordre 2 sont $/\mathbb{Q}$.

$$Y^2 = (X-\alpha)(X-\beta)(X-\gamma) \qquad \alpha, \beta, \gamma \in \mathbb{Q}$$

$A, B, C = 0 \qquad A, B, C$

$L = 2^n + 1 \qquad Y^2 = X(X+1)(X-2^n)$

$L = 2^n - 1 \qquad Y^2 = X(X+1)(X-2^n)$

ρ_p. A montrer : pour p assez grand, ρ_p ne provient pas de la représentation associée à f.

Si coef. de $f \notin \mathbb{Q}$

a_ℓ ℓ premier, $a_\ell \notin \mathbb{Q}$

la trace de $\rho_p(\mathrm{Frob}\,\ell) \in \mathbb{F}_p$

est la réduction mod p d'un entier qui

est soit $\pm(1+\ell)$, soit $\leq 2\sqrt{\ell}$

en valeur absolue.

Soit Ω_ℓ la liste de ces entiers.

$p \nmid N(a_\ell - w)$

On démontre que $w \in \Omega_\ell \Rightarrow 1+\ell \equiv w \pmod 4$

$a_\ell - w \neq 0$ pour tout w.

Réduction mod p

(1) Le principe de Brauer

Soit A un anneau de valuation discrète
π uniformisante de A, $K = \mathrm{Fract}(A)$
$k = A/\pi A$.
V : ev. de dim finie sur K.
Λ : A-algèbre, $K \otimes \Lambda$-module sur V.
Hypothèse : il existe un réseau L de V stable par Λ.
(réseau : A-module libre L t.q. $L \subset V$ et que $K \otimes L \to V$ soit un isom.)

D'où un espace vectoriel $\bar{L} = L/\pi L$ sur lequel opère Λ (i.e. un Λ-module tué par π, i.e. module sur $\bar{\Lambda} = \Lambda/\pi\Lambda$).

<u>Thm</u> : Si L_1 et L_2 sont deux réseaux stables les Λ-modules $\bar{L}_1$, $\bar{L}_2$ ont les mêmes semi-simplifiés ("mêmes" : il existe un isomorphisme).
i.e. $[\bar{L}_1] = [\bar{L}_2]$ dans le groupe de Groth. des $\bar{\Lambda}$-modules (de dim. finie sur k).

<u>Notation:</u> S algèbre $/k$
$G_k(S)$ = groupe de Groth. des S-modules de type fini sur k
= groupe abélien libre de base $[\Sigma]$
Σ : modules simples sur S de dim. finie sur k.

<u>Démonstration:</u>
$\overline{\pi^i L_1} \cong \bar{L}_1$. Supposons $L_1 \subset L_2$ (après mult. par un π^j convenable) : $\pi^m L_2 \subset L_1 \subset L_2$.
Il suffit de traiter le cas $m = 1$.

$$\pi L_2 \subset L_1 \subset L_2 \,, \quad L_2/L_1 = V$$

$$0 \to W \to \bar{L}_1 \to \bar{L}_2 \to V \to 0$$

$$W = \pi L_2 / \pi L_1 \simeq V.$$

$$[W] - [\bar{L}_1] + [\bar{L}_2] - [V] = 0$$

$$[\bar{L}_1] = [\bar{L}_2] .$$

Autre démonstration:

$$0 \to L_1 \to L_2 \to V \to 0$$

$$0 \to \mathrm{Tor}_1^A(V, k) \to \bar{L}_1 \to \bar{L}_2 \to V \to 0$$

$$\mathrm{Tor}_1^A(V,k) \cong \mathrm{Tor}_1^A(k,k) \otimes V, \qquad \mathrm{Tor}_1^A(k,k) = k$$

avantage: s'étend aux modules pas de type fini, si on se restreint au cas $L_2 \supset L_1 \supset \pi' L_2$

A de valuation discrète ?

Généralisations: A intègre de c.d.f. K

① Soit A un anneau local régulier de dim quelconque, k corps résiduel de A.

Λ une A-algèbre.

Soit M un Λ-module qui est de type fini sur A.

Soit $\chi(M) \in G_k(\Lambda)$ défini par

$$\chi(M) = \sum_i (-1)^i [\mathrm{Tor}_i^A(M, k)]$$

Principe de réduction de Brauer: $\chi(M)$ ne dépend que de la classe de $K \otimes_A M$ dans $G_K(K \otimes \Lambda)$.

Corollaire : Si M est de torsion, $\chi(M)=0$.

(2) Généralisation utile.

$A \to k$ corps

V espace vect. de dim. finie sur K

muni d'une structure de Λ-module.

$L \subset V$ réseau, stable par Λ.

Alors deux L différents donnent le même semi-simplifié $ss(\Sigma)$

$G_k(\Lambda)$:

Extension des scalaires : $k \to k'$ ext. de corps

(1) $G_k(\Lambda) \longrightarrow G_{k'}(\Lambda' = k' \otimes \Lambda)$ est injectif

Lemme : Σ_1, Σ_2 deux modules simples non isom.

(Σ_1') et Σ_2' sont disjoints, i.e pas de facteur simple en commun.

$\lambda \in \Lambda$

$\downarrow$

1 ds Σ_1

0 ds Σ_2

(2) k alg. clos. $\quad G_k(\Lambda) \xrightarrow{Tr} k$-dual de Λ

M module, $\quad M \longmapsto (\lambda \in \Lambda \rightsquigarrow Tr_M \lambda_M)$.

$k \otimes_{\mathbb{Z}} G_k(\Lambda) \longrightarrow$ dual de Λ

est injective.

$\Sigma_1, \dots, \Sigma_m$ simples non isom.

$\chi_1, \dots, \chi_m$ formes trace

Alors les χ_i sont k-lin. ind.

$\sum \lambda_i \chi_i = 0$, $\lambda_i \in k$. $\exists x \in \Lambda$

$$\begin{cases} x_{\Sigma_2} = \cdots = x_{\Sigma_m} = 0 \\ \mathrm{Tr}\,(x_{\Sigma}) = 1 \end{cases}$$

Corollaire : Si k est de car 0,

$G_k(\Lambda) \to$ dual de Λ est injective.

Corollaire :

Si k est alg. clos de car $p>0$,

le noyau de $G_k(\Lambda) \longrightarrow$ dual de Λ

est $p\,G_k(\Lambda)$.

Théorème :

Soit Λ une algèbre sur un un corps k,

et soit $H \subset \Lambda$ tel que H engendre Λ

comme k-espace vectoriel.

Soient M_1 et M_2 deux Λ-modules de

dim finie $/k$.

Supposons que pour tout $x \in H$, pol. car. de $x_{M_1} =$

$=$ pol. car. de x_{M_2}

Alors $[M_1] = [M_2]$ dans $G_k(\Lambda)$.

Démonstration :

On peut supposer k alg. clos.

Si car $k=0$, les traces associées à M_1, M_2

sont les mêmes sur H, donc par linéarité

sur Λ. $\square$

Si car $k = p > 0$, $[M_1] \equiv [M_2] \mod p$

(Σ simple, $n_1(\Sigma)$ nombre de fois où

Σ intervient ds M_1 : $[M_1] = \sum_{\Sigma} n_1(\Sigma)\,\Sigma$

$n_2(\Sigma)$ ... $\quad n_1(\Sigma) \equiv n_2(\Sigma) \mod p$ pour tout Σ.

$$\left.\begin{aligned} n_1(\Sigma) &= n(\Sigma) + p\, N_1(\Sigma) \\ n_2(\Sigma) &= n(\Sigma) + p\, N_2(\Sigma) \end{aligned}\right\}$$

avec $\quad 0 \leq n(\Sigma) \leq p-1.$

$$\Longleftrightarrow \left.\begin{aligned} ss(M_1) &= N \oplus p\, P_1 \\ ss(M_2) &= N \oplus p\, P_2 \end{aligned}\right\}.$$

$x \in H$. $\quad$ Pol. car. $x_{M_1} = (\text{Pol. car } x_N)(\text{Pol}_{P_1})^p$.

$\Longrightarrow$ pour tout $x \in H$,

$$\text{Pol. car. } x_{P_1} = \text{Pol. car } x_{P_2}.$$

On raisonne par récurrence sur $\dim M_1$.

D'où $\quad P_1 \simeq P_2$.

$G_k(\Lambda) \longrightarrow$ Fonctions sur H à valeurs dans $k(T)^*$.

<u>Exemple</u> : 1.) $\Lambda = k[G]$, G monoïde (e.g. un groupe) et on prend $H = G$

2.) Λ alg. de Hecke, $H = \{T_n\}$.

<u>Énoncé</u> (utile) : $\overbrace{\text{Si}}^{\text{en car } p}$ M_1 et M_2 ont même trace, et $\dim M_1 < p$, $\dim M_2 < p$, alors

$$[M_1] = [M_2].$$

Retour à $\begin{matrix} A \to k \\ \cap \\ K \end{matrix}$, L libre, stable

$[L]$ indép. du choix de L.

Si, pour toute sous-algèbre commutative (eng par 1 élé) de Λ

$[M_1] = [M_2]$ ds $G_k(\text{s/alg}) \Rightarrow$ vrai sur Λ

A anneau local noethérien complet

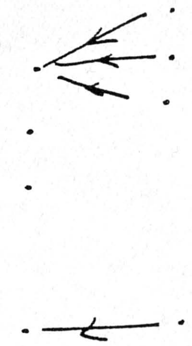
corps résiduel k

M A-module qui est aussi un Λ-module t.f.

(Λ A-algèbre comm.)

On peut supposer $\Lambda \subset \operatorname{End} M$, donc t.f.

Spec Λ



Spec A

pt fermé

$A = \prod \Lambda_i$ les facteurs corr. aux idéaux max. au-dessus de m

m : idéal maximal de A

$M = \prod M_i$

Plus concrètement :

<u>Exemple :</u> A de val. discrète, corps des f. K

corps résiduel k

Λ comm., M libre de type fini

$V = K \otimes_A M$, $\overline{M} = M/\pi M$

<u>Hyp</u> : Pour tout $\lambda \in \Lambda$, les valeurs propres de λ_M sont dans K.

On peut parler de leurs réductions ds k.

Base de M où les matrices de Λ sont triangulaires.

$n = \dim M$, $\quad w_1, \dots, w_n : \Lambda \to A \subset K$

$[K \otimes M]$ ds $G_K(K \otimes \Lambda)$ est dé't. par les w_i

$\overline{w}_1, \dots, \overline{w}_n : \Lambda \to k$

$[\overline{M}]$ est déterminé par les réd. $\overline{w}_i$.

$$M = \bigoplus M_{\overline{w}}$$ où les $M_{\overline{w}}$ correspondent aux divers $\overline{w}$.

Tout module M est somme directe de modules ne donnant lieux qu'à un seul $\overline{w}$.

$h : M \to M$ endomorphisme

Hensel : on décompose.

Corollaire : M libre sur A, de type fini.

Λ commutatif agissant sur M

Soit $m \in \overline{M} = M/\pi M$ vecteur propre $(\neq 0)$ de l'action de Λ sur $\overline{M}$

$\lambda m = \overline{w}(\lambda) m \qquad \overline{w} : \Lambda \to k$

Quitte à faire une ext. finie de K, il existe un vecteur propre x de Λ dans $V = K \otimes M$

$\lambda x = w(\lambda) x \qquad w(\lambda) \to \tilde{w}(\lambda)$

(? : $x \mapsto$ pas néc. m).

Il manque la page 26 dans le document original

Thm (Nakajima, Inv. Math. 75 (1984)).

Soit G un groupe opérant sur une var. alg. projecti[ve] Y sur k (de car p) et sur un faisceau cohérant $\mathcal{F}$ sur Y

$\circlearrowleft \mathcal{F}$ $\qquad\qquad (g^*\mathcal{F})_y = \mathcal{F}_{gy}$

$\circlearrowleft Y$ $\qquad\qquad g : Y \longrightarrow Y$

$$\mathcal{F}_y \simeq (g^*\mathcal{F})_y .$$

action de G sur $H^i(Y, \mathcal{F})$
par transport de structure (action à gauche)
par fonctorialité (action à droite)

On suppose que la ramification de G est modérée : action modérée (on suppose ②).

① les points fixes des élém. $g \in G$, $g \neq 1$ sont isolés, et pour tout $y \in Y(\bar{k})$ le fixateur de y est d'ordre premier à p.

② Si G_p est un p-Sylow de G, G_p opère librement sur Y.

① $\Rightarrow$ ②

Cas simple : on suppose qu'il existe un indice i tel que $H^j(Y, \mathcal{F}) = 0$ pour $j \neq i$.

(i) Alors le kG-module $H^i(Y, \mathcal{F})$ est projectif.

Cas général :

(ii) Alors il existe un complexe $L_\cdot = (L_n)$, $L_n = 0$ en dehors d'un int. de $k[G]$-modules projectifs de type fini, tel que

$$H^i(L) \simeq H^i(Y, \mathcal{F})$$

comme $k[G]$-modules

(ii) $\Rightarrow$ (i) exercice sur les modules projectifs

Un tel complexe $L_\cdot$ est appelé "parfait".

Démonstration du cas simple.

M kG-module de t.f.

M kG-projectif $\Leftrightarrow$ M kG_p projectif

$\Leftrightarrow$ M kG_p-libre

G_p : p-Sylow.

Donc on peut supposer que G est un p-groupe

$$\begin{array}{ll} \mathcal{F} & Y \\ & \downarrow \\ \mathcal{F}_X & X = Y/G \end{array}$$

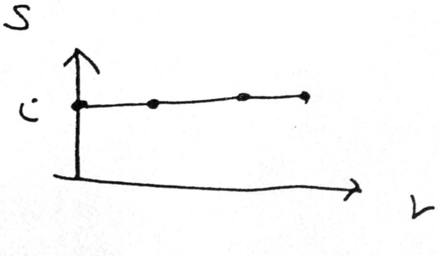
G p-groupe, opère librement

$$H^i(Y, \mathcal{F})$$

Cartan, Leray $\quad H^*(G, H^*(Y, \mathcal{F})) \Rightarrow H^*(X, \mathcal{F}_X)$.

$$H^r(G, H^s(Y, \mathcal{F}))$$

$$H^r(G, H^i(Y, \mathcal{F})) \cong H^{r+i}(X, \mathcal{F}_X).$$



<u>Corollaire</u> $H^r(G, M) = 0$ pour r assez gd

$M = H^i(Y, \mathcal{F})$

Même chose pour tout $G' \subset G$.

par un thm connu (Nakayama-Tate, cf. C.L.)

$\Longrightarrow$ M est k G-libre.

Y variété algébrique $/k$, $\mathrm{car}(k) = p > 0$

G opère sur Y, et sur un faisceau $\mathcal{F}$ sur Y

$X = Y/G$. $\mathcal{F}$ faisceau cohérent

Hyp : G opère de façon "modérée" : fixateurs des points$/k$ de Y sont d'ordre premier à p. (e.g. G opère librement)

Cas simple : $H^j(Y, \mathcal{F}) = 0$ en toute dimension sauf une : i

$H^j = 0$, $j \neq i$

Th (Nakajima) Action de G sur $H^i(Y, \mathcal{F})$ fait de $H^i(Y, \mathcal{F})$ un $k[G]$-module projectif

(Y quasi-projective).

On peut supposer que G est un p-groupe.

Autre cas : (cas général) :

Il existe un complexe $C^i \xrightarrow{\delta} C^{i+1} \to \cdots$ nul si $i < 0$ ou si $i > \dim Y$ formé de $k[G]$-modules projectifs (et C^i de type fini si Y est projective) avec $H^i(C) \simeq H^i(Y, \mathcal{F})$ pour tout i.

$$\begin{array}{c} Y \\ \downarrow \\ X \end{array} \qquad X = Y/G$$

$U_{\alpha, Y}$ recouvrement de Y

$\mathcal{U} = (U_\alpha)$ recouvrement affine de X

Cohomologie se calcule à partir de cochaînes alternées. On peut choisir le rec. de dim $n = \dim Y$.

Le complexe de cochaînes correspondant va de 0 à n. Il est formé de modules projectifs.

Thm sur les complexes
Λ anneau noethérien, C complexe de Λ-modules projectifs borné ($C^i = 0$ si $i \notin$ intervalle), et $H^i(C)$ de type fini sur Λ pour tout i.
Alors il existe $C' \to C$, C' projectif borné de type fini et que $H^i(C') \to H^i(C)$ soit un isom pour tout i.

Réf : Mumford : abelian varieties, p. 46.
Illusie : SGA 6, exp 1.

Corollaire :
Supposons que G soit un p-groupe.
G opère librement sur Y, et $H^j(Y, \mathcal{F}) = 0$ pour $j \neq m, m+1$. Alors $H^m \simeq \Omega^2 H^{m+1}$ (stable^t.)

Ω : espace des lacets
Si M est un $k[G]$-module, L libre,

$$0 \to \Omega M \to L \to M \to 0$$

ΩM est bien déterminé dans la catégorie stable, i.e. $\Omega' M \oplus \text{libre} \simeq \Omega M \oplus \text{libre}$.

Cor : $H^j = 0 \quad j \neq m, m+r$
$\Rightarrow H^m \simeq \Omega^{r+1} H^{m+r}$

Y courbe proj. lisse connexe. $\mathcal{F} = \mathcal{O}$

$H^0 = k$ action triviale
$H^1 = $ dual de $H^0(\omega_Y)$

$H^1 \simeq \Omega^{-2}(1_G)$

Formes différentielles G

$H^0(Y, \omega_Y)$ est $\Omega^2 1_G$

$$0 \to I \to k[G] \to k \to 0$$

$$0 \to J \to L \to I \to 0$$

<u>Thm</u> Supposons Y projective, et G opérant librement. Alors si $H^j(Y, \mathcal{F}) = 0$ pour $j \neq i$, alors $H^i(Y, \mathcal{F})$ est libre sur $k[G]$.

Il suffit de voir que le caractère (au sens Brauer) de la représentation $H^i(Y, \mathcal{F})$ est 0 en dehors de 1.

G^{reg} : éléments d'ordre premier à p

$$G^{reg} \to \text{car } 0$$

Grâce à cette réduction (Brauer ou pol. car.) on peut supposer G cyclique d'ordre premier à p.

1ère méthode : formule de points fixes.

a.) dans le corps de base k

$s \in G$, $s \neq 1$

$$\sum (-1)^j \, \mathrm{Tr}(s : H^j(Y, \mathcal{F}) \to H^j(Y, \mathcal{F}))$$

$= 0$ (somme sur les points fixes de s)

donc $\quad \mathrm{Tr}(s, H^i(Y, \mathcal{F})) = 0.$

b.) variante de la formule des points fixes (si Y lisse).

Variante : travailler avec les traces à la Brauer.

Démonstration directe (= 2ème méthode) :

$$\begin{array}{c} Y \\ \pi \downarrow \; G \\ X \end{array}$$

, G cyclique d'ordre premier à p

k alg. clos

$\chi : G \to k^*$ définit un fibré de rang 1 sur X, noté L_χ.

$$\pi_* \mathcal{O}_Y \simeq \bigoplus_\varphi L_\varphi .$$

$$H^i(Y, \mathcal{F}) = \bigoplus \underbrace{H^i(X, \mathcal{F}_X \otimes L_\chi)}_{\text{action de } G \text{ par } \chi} .$$

$$\sum (-1)^i [H^i(Y, \mathcal{F})] = \text{multiple de la rep. rég.}$$

$$= \chi(X, \mathcal{F}_X) \cdot r_G .$$

$$\|$$

$$L_G(\mathcal{F})$$

$$L_G(\mathcal{F}) = \sum [\varphi] \, \chi_X(\mathcal{F}_X \otimes L_\varphi)$$

A montrer : $\chi(\mathcal{F}_X \otimes L_\varphi) = \chi(\mathcal{F}_X)$.

$L_\varphi^{\otimes n} \cong \mathbb{1} \cong L_1 \cong \mathcal{O}_X$, $n = |G|$.

$K_0(X)$ groupe de Grothendieck des faisceaux cohérents sur X

$K^0(X)$ — " — loc. libres sur X (Tor-dim finie).

$[L_\varphi] \in K^0(X)$ anneau

$[\mathcal{F}_X] \in K_0(X)$ module sur $K^0(X)$.

$\chi : K_0(X) \longrightarrow \mathbb{Z}$

$\chi : \mathbb{Q} \otimes K_0(X) \longrightarrow \mathbb{Q}$

Il suffit de montrer que $[L_\varphi] = 1$ dans $\mathbb{Q} \otimes K^0(X)$.

Lemme 1 : $1 - [L_\varphi]$ est nilpotent dans $K^0(X)$.

Lemme 2 : Si R est une $\mathbb{Q}$-algèbre et $\ell \in R$ tel que $\ell^n = 1$, pour $n \geq 1$, et $1 - \ell$ nilpotent, alors $\ell = 1$.

Preuve du lemme 1 :

$$(1 - [L_\varphi])^{\dim X + 1} = 0$$

(réf : Grothendieck, SGA 6 (?))

X irréductible

Si L avait une section :

$$0 \to \underline{1} \hookrightarrow L_\varphi \to ? \to 0$$

diff. porté par sous-variété de codim 1.

(produit $\dim X + 1$ - fois $= 0$).

On peut aussi utiliser Riemann-Roch : classes de Chern $= 0$.

Formule de Woods Hole. (SGA 5, exp. 3)

$Y \xrightarrow{f} Y$ $\qquad$ $\mathcal{F}$ faisceau coh. / Y

$\varphi : f^*\mathcal{F} \to \mathcal{F}$

$$\begin{tikzcd} H^q(Y, \mathcal{F}) \arrow[r, "f^*"] \arrow[dr] & H^q(Y, f^*\mathcal{F}) \arrow[d, "H^0(\varphi)"] \\ & H^q(Y, \mathcal{F}) \end{tikzcd}$$

k alg. clos

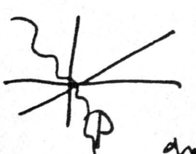
<u>Hyp</u> : (1) Y projective

(2) $\mathcal{F}$ localement libre

(3) points fixes de f isolés, lisses, transversaux.

(pas de v. p. de $df(P) = 1$)

Δ



graphe de f

Alors
$$\sum (-1)^j \operatorname{Tr}(H^j(Y,\mathcal{F}) \to H^j(Y,\mathcal{F}))$$
$$= \sum_{f(P)=P} \frac{\operatorname{Tr} \varphi(P)}{\det(1-df(P))}$$

$f(P)=P$, $\varphi : f^*\mathcal{F} \longrightarrow \mathcal{F}$

Si f, φ provient d'une action d'un groupe fini (d'ordre premier à p).

Egalité au sens Brauer

Donovan : B.S.M.F. (1969)

Cas particulier des courbes :

$\mathcal{F}$ localement libre de dim 1.

$\varphi(P) = z$, racine de 1.

$$t \mapsto \lambda t + \cdots$$

λ racine de 1 , $\lambda^n = 1$

terme local est $\dfrac{z}{1-\lambda}$

$$\frac{1}{1-\lambda} = -\frac{1}{n}(\lambda + 2\lambda^2 + 3\lambda^3 + \cdots + (n-1)\lambda^{n-1})$$

$\lambda^n = 1$, $\lambda \neq 1$.

Ceci permet de relever en car 0.

<u>Thm</u> Le caractère de Brauer de

$$\sum (-1)^i H^i(Y, \mathcal{F}) \quad \text{est}$$

$$\underset{\substack{\neq \\ 1}}{s} \longmapsto \sum_p \frac{z_p}{1-\lambda_p} = \sum -\frac{z_p}{n}\left(\lambda_p + 2\lambda_p^2 + \dots + (n-1)\lambda_p^n\right)$$

(repr. d'Artin : $\lambda + \lambda^2 + \dots + \lambda^{n-1}$).

ici "demi-repr" d'Artin.

Soit A un anneau de valuation discrète et $k = A/\pi A$ son corps résiduel.

Y schéma projectif sur A
plat sur A

$\tilde{Y}$ = réd. de Y mod π

$$\begin{array}{ccc} \tilde{Y} & & Y \\ \text{fibre spéciale} \Big| & & \text{fibre générique} \\ \operatorname{Spec} A & \cdot & \longleftarrow 0 \end{array}$$

$\tilde{\mathcal{F}} = \mathcal{F}/\pi\mathcal{F}$

$$H^q(Y, \mathcal{F})/\pi H^q(Y, \mathcal{F}) \underset{?}{=} H^q(\tilde{Y}, \tilde{\mathcal{F}})$$

Cas simple : $q = 0$ et $H^1(\tilde{Y}, \tilde{\mathcal{F}}) = 0$.

On a alors : $H^0(Y, \mathcal{F})$ est A-libre et sa réduction mod π est bien $H^0(\tilde{Y}, \tilde{\mathcal{F}})$ et $H^1(Y, \mathcal{F}) = 0$.

<u>Démonstration:</u>

$$0 \to \mathcal{F} \xrightarrow{\pi} \mathcal{F} \longrightarrow \tilde{\mathcal{F}} \to 0$$

$$0 \longrightarrow H^0(Y, \mathcal{F}) \xrightarrow{\pi} H^0(Y, \mathcal{F}) \longrightarrow H^0(\tilde{Y}, \tilde{\mathcal{F}}) \to$$

$$\to \underset{\substack{\| \\ X}}{H^1(Y, \mathcal{F})} \xrightarrow{\pi} \underset{\substack{\| \\ X}}{H^1(Y, \mathcal{F})} \to 0$$

$X = \pi X$, X de type fini sur A

$\Rightarrow X = 0$ (Nakayama).

Y courbe lisse, irr., $\mathcal{F}$ fibré de rang 1

$\deg \mathcal{F} > 2 g_Y - 2$. Alors $H^1 = 0$.

(On se servira de ceci pour monter que les formes modulaires mod p proviennent de formes modulaires en car 0 !)

Situation analogue avec G opérant sur tout $(Y, \mathcal{F})$ de façon A-linéaire.

Hyp. $\begin{cases} Y \text{ courbe} \\ H^1(\tilde{Y}, \tilde{\mathcal{F}}) = 0 \\ G \text{ opère de façon modérée sur } \tilde{Y}. \end{cases}$

<u>Conclusion</u>: $H^0(Y, \mathcal{F})$ est un $A[G]$-module projectif de réduction mod π $H^0(Y, \bar{\mathcal{F}})$

On utilise : <u>lemme</u> Si M est un $A[G]$-module libre de type fini sur A, et si $\tilde{M} = M/\pi M$ est $k[G]$-projectif, alors M est $A[G]$-projectif.

Action de $GL_2(\mathbb{Z}/N\mathbb{Z})$: ~~ptes 2,~~ ?

points fixes : pointes, ordre 2, 3.

si $(\ell, 2\cdot 3 \cdot N) = 1$ $\rightarrow$ module projectif.

Une propriété des $A[G]$-modules projectifs.

Soit M un $A[G]$-module projectif de type fini, et $\tilde{M} = M/\pi M$ sa réduction.

Soit H un s/g de G, et $\varepsilon : H \to A^*$ un homomorphisme, d'où $\tilde{\varepsilon} : H \to k^*$

<u>Proposition</u>: Pour tout $x \in \tilde{M}$ tel que $hx = \tilde{\varepsilon}(h)x$ pour tout $h \in H$, il existe un $y \in M$, $\bar{y} = x$, avec $hy = \varepsilon(h)y$ $(h \in H)$

(formes de type k, ε_1 ε_2

lorsque $\varepsilon_1 \equiv \varepsilon_2 \bmod p$).

<u>Démonstration</u> : on peut supposer $G = H$.

Cas particulier : $\varepsilon = 1$

$$0 \to M \xrightarrow{\pi} M \to \tilde{M} \to 0$$

$$0 \to H^0(G, M) \xrightarrow{\pi} H^0(G, M) \to H^0(G, \tilde{M}) \to \underbrace{H^1(G, M)}_{\shortparallel \atop 0}$$

car M est projectif

Cas général :

$[\varepsilon]$ module de rang 1 défini par ε

A avec action tordue par ε

énoncé pour M, ε ; $M \otimes [\varepsilon^{-1}], 1$

Supposons donnés des endomorphismes T_n de M commutant à l'action de G, et commutant entre eux.

Supposons leurs valeurs propres dans A.

Soit $x \neq 0$, $x \in \tilde{M}$, avec $hx = \tilde{\varepsilon}(h) x$
$\forall h \in H$

vecteur propre des T_n :

$$T_n x = \lambda_n x$$ pour tout T_n

$\lambda_n \in k$.

Th|| ~~Alors il existe~~ $y \in M$ (pas néc. avec $\tilde{y} = x$!) $y \notin \pi M$, $hy = \varepsilon(h)y$ pour tout $h \in H$, et $T_n y = \mu_n y$ avec $\mu_n \in A$ et $\tilde{\mu}_n = \lambda_n$ pour tout n.

(On a vu que) M est somme directe de modules M_α correspondant aux systèmes de valeurs propres des T_n ds f

Dans $M_\alpha / \pi M_\alpha$, chaque T_n a une unique valeur propre λ_n.

$M = \bigoplus M_\alpha$ stable par G.

Donc chaque M_α est $A[G]$-projectif

$x \in \tilde{M}_\alpha$, covariant de H pour $\tilde{\varepsilon}$

Soit N_α le sous-module de M_α formé des y avec $hy = \varepsilon(h)y$ $h \in H$.

~~A voir~~ : $N_\alpha \neq 0$.

Il existe $y \in N_\alpha$, $y \neq 0$, vecteur propre commun des T_n. y convient !

Formes modulaires

Deligne - Rapoport   Anvers II   (SLN 349)

Katz   Anvers III   (SLN 350)

On se donne $N \geq 3$, nombre premier $l \nmid N$.

Dans les réf. on définit une courbe $X(N)$ sur $\mathbb{Z}[\frac{1}{N}]$ qui classe les courbes elliptiques (généralisées) munies d'une base (α_1, α_2) des points de div. par N

$X(N)$ est projective, lisse (irréd. mais pas abs.

Faisceau ω, f. modulaire de niveau N de poids k = section du faisceau $\omega^{\otimes k}$

Action de $G = GL_2(\mathbb{Z}/N\mathbb{Z})$.

$M_k = H^0(X(N), \omega^{\otimes k})$

$\widetilde{M}_k = M_k / l M_k = H^0(\widetilde{X}(N), \omega^{\otimes k})$

si $k \geq 2$.

<u>Thm</u> :

Si $k \geq 2$ et si $l \neq 2, 3$, alors

$\mathbb{Z}_l \otimes M_k$ est un $\mathbb{Z}_l G$ - module projectif

Suffit de vérifier action de G modérée

<u>Thm</u> $\ell = 3$: même résultat si l'on se restreint aux composantes de $\mathbb{Z}_\ell \otimes M_k$ de "type ~~non~~ diédral provenant de $\mathbb{Q}(\sqrt{-3})$"

composantes : par rapport aux opérateurs de Hecke.

Forme explicite de la condition : il existe $p \nmid N\ell$, $p \equiv -1 \pmod 3$, tel que la valeur propre correspondante de T_p en car ℓ soit $\neq 0$.

Formes modulaires : $f(z)$

avec $f\left(\frac{az+b}{cz+d}\right) = \dots$

On développe $f(z) = \sum a_n q^n$ $q = e^{2\pi i z}$

(ou puissances de $q^{1/N}$).

conditions : e.g. $a_n \in \mathbb{Z}$ ou $\overline{\mathbb{Z}}$ = entiers de $\overline{\mathbb{Q}}$.

réduire mod p (ou $\mathfrak{P}$)

déf. de l'article de Duke

mais ceci conduit à quelques petits contre-exemples aux conj. de Duke.

Comment remédier à cette situation :

1.) interprétation modulaire des formes modulaires $\Longrightarrow$

$\Longrightarrow$ lien entre déf. analytique et une autre $\Longrightarrow$ permet de délimiter les contre-ex.

2.) interprétation "quaternions"

Courbes modulaires $X(N)$

N entier (le plus souvent $N \geq 3$)

Origine des formes modulaires

Jacobi : c. ell., donnée par ses périodes

$y^2 = 4x^3 - g_2 x - g_3$

$g_2 = g_2(\omega_1, \omega_2)$, $g_3 = g_3(\omega_1, \omega_2)$

ω_1, ω_2 périodes . $g_2 = \omega_2^{-4} \cdot$ fct de $\frac{\omega_1}{\omega_2}$

Hurwitz a développé une th. des formes modulaires indép. de l'interprét. elliptique.

On revient au point de vue de Jacobi :

$\mathcal{H}/SL_2(\mathbb{Z}) \longleftrightarrow$ les courbes ell $/\mathbb{C}$

$$\begin{array}{ccc} z & \longrightarrow & \Lambda_z = \mathbb{Z}.1 \oplus \mathbb{Z} z \\ & & \downarrow \\ & & \mathbb{C}/\Lambda_z \end{array}$$

$X(N)$ courbe sur $\mathbb{Z}[\frac{1}{N}]$.

projective, lisse

Pointes : $Y(N)$ courbe affine $/\mathbb{Z}[\frac{1}{N}]$

$= X(N)$ - pointes.

Si $N = 1$, $X(N)$ = droite proj. $\mathbb{P}^1$

Pte = $\{\infty\}$, $Y(1)$ = droite affine paramétré par j

$N \geq 3$:

$Y(N)$ représente les courbes elliptiques E (sur les bases S au-dessus de $\mathbb{Z}[\frac{1}{N}]$), munies d'une base α_1, α_2 des points de division par N

Deligne - Rapoport (LN 350)

$$\begin{array}{c} Y(N) \\ \downarrow \\ \mathrm{Spec}\ \mathbb{Z}[\frac{1}{N}, \zeta_N] \\ \downarrow \\ \mathrm{Spec}(\mathbb{Z}) \end{array}$$

abs. irréd.

ζ_N racine primitive N-ième de 1

$(\alpha_1, \alpha_2) \mapsto e_n(\alpha_1, \alpha_2) \in \mu_N$

(acc. de Weil)

Points de $Y(N)/\mathbb{C}$

Après ext. des sc. à un corps contenant μ_N, $Y(N)$ devient somme disjointe de $\varphi(N)$ courbes.

Points de $Y(N)/\mathbb{C}$ corresp. à $\zeta_N = e^{2\pi i/N}$

$$\Longleftrightarrow \quad \mathcal{H}/\Gamma(N)$$

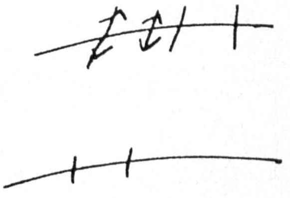
$$\Gamma(N) = \{ s \in SL_2(\mathbb{Z}) \mid s \equiv 1 \pmod N \}$$

2 Dans Husemoller et Koblitz cette corr. est affirmée sans se donner ζ_N.

Faisceau ω sur $Y(N)$: loc. libre de rang 1, défini comme suit :

(47)

$N \geq 3$ $\quad E$ $\quad$ c. ell. universelle



$\downarrow$

$Y(N)$

fibré de rg 1

ω = fibré cotangent à E (le long de 0)

$\omega^{\otimes k}$ puissance $k$ième de ω.

Sections de ce faisceau :

"formes modulaires de poids k avec pôles à l'infini".

$$f(z) = \sum a_n q^n$$

nbre fini de n négatifs.

Ceci ne suffit pas pour la déf. des f. mod.

Compactification $X(N)$ de $Y(N)$:

on généralise c. ell, pour obtenir $j = \infty$.

$E \downarrow S$ courbe sur S, propre, plate (pas néc. lisse)

fibres géom. : ou bien des c. ell ou bien des "polygones" à N côtés

Str. de groupe alg sur E^{reg} (on enlève les sommets)

$\swarrow$ loi de g. sur c. ell $\qquad \to \mathbb{G}_m \times C_N$ cyclique sur fibres exc.

$$E^{reg} \times E^{reg} \longrightarrow E^{reg}$$
$$E^{reg} \times E \to E$$

$X(N)$ représente ce foncteur prolongé

$X(N)$, $N \geq 3$, est propre et lisse sur

$\mathrm{Spec}\left(\mathbb{Z}\left[\frac{1}{N}\right]\right)$.

et le faisceau ω se prolonge :
espace cotangent au groupe E^{reg}.

D'où une notion de forme de poids k ; niv. N
section de $\omega^{\otimes k}$ sur $X(N)$.

Section de $\omega^{\otimes k}$ sur $Y(N)$ se prolonge à
$X(N)$ $\Longleftrightarrow$ pas de terme à exposant <0
dans dével. en série associé.
on ne définit pas cette dével.
en général
courbes de Tate
$$\mathbb{Z}\left[\tfrac{1}{N}\right]\left[\left[q^{1/N}\right]\right]$$
là-dessus : $\mathbb{G}_m / q^{\mathbb{Z}}$

2 pts naturels de N-div
$$(q^{1/N})^N = q \equiv 1$$
sur $\mathbb{Z}\left[\frac{1}{N}, \zeta_N\right]$ $\quad \zeta_N$.

(Voir Katz LN 350)

(autre point de vue :

$N = 1$ on veut $X(1) = \mathbb{P}_1$ par. par j

$X(N)$ au-dessus $= ?$

$$Y(N) \subset X(N)$$ normalisé ?

$$\downarrow$$

$$\text{dte aff.} \subset X(1) = \mathbb{P}_1$$)

Cas $N = 1, 2$:

$G_N = GL(2, \mathbb{Z}/N\mathbb{Z})$ opère de

façon naturelle sur $X(N)$ et $Y(N)$

car opère sur le probl. de modules corr :

$$(E, \alpha_1, \alpha_2) \qquad s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\downarrow$$

$$(E, a\alpha_1 + b\alpha_2, c\alpha_1 + d\alpha_2)$$

on peut définir $X(1) = X(N)/G_N$ $N \geq 3$

$= \mathbb{P}_1$ (indép. du choix de N)

$X(2) = X(2N)/G_N$ $N \geq 3$ $2 \nmid N$.

$= \mathbb{P}_1 - 3$ points.

G_N opère aussi sur ω.

$$\left.\begin{array}{l}\text{forme modulaire}\\ \text{sur } \Gamma_0(N)\\ \text{de pds } k\end{array}\right\} \longleftrightarrow \begin{array}{l}\text{forme modulaire de}\\ \text{poids } k \text{ sur } X(N)\\ \text{invariante par}\\ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.\end{array}$$

$X(N)$, $\omega^{\otimes k}$, G_N opère

A anneau de valuation discrète, car 0

π uniformisante

$k = A/\pi$ de car. $p > 0$, $p \nmid N$

Comparer :

formes mod. de pds k sur $X(N)$ à coeff. ds A

$$= H^0(X(N)_{/A}\,;\,\omega^{\otimes k}) = M_{k,N}(A)$$

avec

$M_{k,N}(F)$ défini de m̂ façon.

On aimerait

$$M_{k,N}(F) = M_{k,N}(A)/\pi M_{k,N}(A)$$

Vraie si $N \geq 3$, $k \geq 2$.

(Katz, LN 350)

car $H^1(X(N)_{/F}, \omega^{\otimes k}) = 0$ si $k \geq 2$

Dualité : dual de $H^0(X(N)_F, \Omega \otimes \omega^{\otimes -k})$

Ω : f. dif., $\Omega = \omega^{\otimes 2}$ (zéro aux pointes)

(isom. de Kodaira-Spencer) $= \omega_0^{\otimes 2}$: faisceau des formes paraboliqu

$(cz+d)^2$

$$\frac{d}{dz}\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^2} \qquad (ad-bc=1)$$

f. diff. d'exp. 1.

$$\Omega \otimes \omega^{-k} \simeq \omega_0^{2-k}$$

$k \geq 3$ $\quad$ $\deg(\omega) > 0$

$k = 2$ $\quad$ pas de fct $\neq 0$ s'annulant aux ptes

Attention : faux si $k=1$

(la dém. ne s'applique pas : et de plus, Mestre a des contre-exemples pour

$k=1$, $N = 1429$

(méthode : rep. gal. image $SL_2(\mathbb{F}_8)$

$GL_2(\mathbb{C})$: s/g finis de PGL_2 : on connaît leur liste, et $SL_2(\mathbb{F}_8)$ n'y est pas)).

Propriétés de projectivité

A ann. de val. discrète, π unif.

$F = A/\pi A$, car $F = p \nmid N$

$N \geq 3$, $G_N = GL_2(\mathbb{Z}/N\mathbb{Z})$

Thm :

① Si $p \neq 2, 3$ et si $k \geq 2$, le $A[G_N]$-module $M_{k,N}(A)$ est projectif.

Vu les théorèmes précédents, il suffit de remarquer que G_N opère de façon modérée sur $X(N)$, i.e. que les fixateurs des points géométriques sont d'ordre premier à p.

$-1 \in G_N$ opère trivialement sur $X(N)$ et par $(-1)^k$ sur le faisceau ω^k.

$(E, \alpha_1, \alpha_2) \simeq (E, -\alpha_1, -\alpha_2)$

$G_N/\{\pm 1\}$ opère sur $X(N)$

Les points à fixateur non trivial proviennent

a.) des courbes à aut. $\neq (\pm 1) \to$ gr. d'ordr 2, 3 (car $\neq 2$, 6 (car 3), 12 (car 2

b.) des pointes.
$\to$ cyclique d'ordre N. $p \nmid N$

$\mathbb{G}_m \times C_N$

$(t, \alpha) \longrightarrow (tz, \alpha)$ $\qquad z^N = 1.$

α gén.

Application aux formes de poids k, car ε
sur $X_0(N) = X(N)/(\text{triang.})$

$p \nmid N$, $k \geq 2$, $p \neq 2, 3$

formes $f = \sum a_n q^n$, à coeff. ds $\overline{\mathbb{Z}}$

de type (k, ε) :

$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to (\overline{\mathbb{Z}})^*$ $\qquad \varepsilon(-1) = (-1)^k$

$$f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

Forment un module M.

On regarde $M/\wp M$, $\quad \wp \mid p$.

A voir : $M/\wp M$ ne dépend que de

$$\tilde{\varepsilon} : (\mathbb{Z}/N\mathbb{Z})^* \to F = \mathcal{O}/\wp .$$

i.e. toute forme modulaire de type $k, \tilde{\varepsilon}$ à coeff. $\in F$ se relève ....
$\ldots ; \varepsilon$, à coeff. $\in \overline{\mathbb{Z}}$

car les covariants de type $\tilde{\varepsilon}$ se relèvent en covariants de type ε.

$\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ appliqué aux car. ε avec

$$\varepsilon \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = \varepsilon(\delta)$$

traduction de la dernière fois + Katz

donne le résultat.

<u>Contre-exemple</u> pour $p = 3$.

$N = 13$, $k = 2$, $\varepsilon : (\mathbb{Z}/13\mathbb{Z})^* \to$ racines de 1.

$\Vert$

cyclique d'ordre 12

$/(\pm 1)$ = cyclique d'ordre 6

6 possibilités pour le caractère ε.

Formes paraboliques de type $(2, \varepsilon)$ sur $\Gamma_0(13)$

$X_1(13)$ genre 2

$\downarrow$ ——— groupe de Gal. cyclique d'ordre 6.

$X_0(13)$ genre 0

espace de ces formes est de dim 1 si ε est d'ordre 6, de dim 0 sinon.

(Mazur–Tate, Invent.)

Δ mod 13 $\equiv$ l'une de ces formes de poids 2.

$p = 3$ $\quad \varepsilon$ d'ordre 6 $\to$ espace de dim 1

$\to$ repr. Gal ds $GL_2(\mathbb{F}_3)$ induite à partir de $\mathbb{Q}(\sqrt{-3})$

ε d'ordre 2 $\longrightarrow 0$

et ont même réduction mod 3.

Même contre-ex. pour $p=2$, ind. de $\mathbb{Q}(\sqrt{-1})$

Thm 2

$p=3$, $N \geq 3$, $p \nmid N$, $k \geq 2$

Les facteurs de $M_{k,N}(A)$ de type "ne provenant pas mod 3 de $\mathbb{Q}(\sqrt{-3})$ par induction" sont des $A[G_N]$-modules projectifs.

Même corollaire pour les formes sur $\Gamma_0(N)$, car ε, à condition n'écarter les facteurs provenant mod 3 de $\mathbb{Q}(\sqrt{-3})$"

"provenant" fait allusion aux repr. gal.

Rep. galoisienne $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$, F alg. clo

"provient de $\mathbb{Q}(\sqrt{-3})$" s'il existe un caractère $\psi : G_{\mathbb{Q}(\sqrt{-3})} \longrightarrow F^*$

tel que $\rho \simeq \operatorname{Ind} \psi$

caractérisée par : Si $s \in G_{\mathbb{Q}}$ et sa restriction à $\mathbb{Q}(\sqrt{-3})$ est non triviale (i.e. $s \notin G_{\mathbb{Q}}(\sqrt{-3})$), alors $\operatorname{Tr} \rho(s) = 0$.

$\Longleftrightarrow$ Si p non ramifié p.r. à ρ
et p inerte dans $\mathbb{Q}(\sqrt{-3})$
(i.e. $p \equiv -1 \pmod 3$), alors
$\mathrm{Tr}(\rho_{\mathrm{Frob}\, p}) = 0$ dans F.

<u>Opérateurs de Hecke T_p</u> $(p \nmid N)$
agissent sur les formes de poids k
de la manière suivante :
f (section de $\omega^{\otimes k}$ sur $X(N)$) en
$f|T_p$, défini comme suit

$$f : (E, \overbrace{\alpha_1, \alpha_2}^{\alpha}) \mapsto \omega^k(E)$$

$$f|T_p (E, \alpha) = \frac{1}{p} \sum_{C} \varphi^*(f(E', \alpha'))$$

$\alpha = (\alpha_1, \alpha_2)$ — C s/g cycl. d'ordre p

$\alpha' =$ image de α. — $E' = E/C$

$\varphi : E \to E'$

(voir article de Katz).

$\downarrow$

$$p^{k-1} \sum_{E' \to E}$$

$X(p, N)$
|
s/g cyclique d'ordre p

$$\begin{tikzcd} & X(p,N) \arrow[dl, "\varphi"'] \arrow[dr, "\psi"] & \\ X(N) & & X(N) \end{tikzcd}$$

fini et plat

$$\frac{1}{p}\,\psi_* \varphi^*(f) = f\,|T_p .$$

$p \in P$: $p \nmid 3N$

$$M_{k,N}(A) = \bigoplus M_{k,N}(A)_a$$

$(a)\left\{\begin{array}{l}\text{syst. de}\\ \text{val. propres}\\ \text{ds } F \text{ de } T_p\end{array}\right.$ $\qquad a = (a_p),\ p \in P$

$a_p \in F = \overline{\mathbb{F}_3}$.

Cas "diédral sur $\mathbb{Q}(\sqrt{-3})$" = tous les a_p ($p \equiv -1\ (3)$, $p \nmid N$) sont 0.

Cas "non diédral ..." = il existe $p \equiv -1\ (3)$ avec $a_p \neq 0$ dans F.

Le th (2) dit que la composante d'indice a est un module projectif dans le cas "non diédral".

Démonstration:

$$\begin{tikzcd}
 & M_{k,p,N} \arrow[dr, "\frac{1}{p}\,\mathrm{Trace}"] & \\
M_{k,N} \arrow[ur] \arrow[rr, "T_p"'] & & M_{k,N}
\end{tikzcd}$$

$$\begin{tikzcd}
(M_{k,N})_a \arrow[r] \arrow[rr, bend right=60, "T_p\ \cong"'] & M_{k,p,N} \arrow[d, "1/p\ \mathrm{Trace}"] & \\
 & M_{k,N} \arrow[r] & (M_{k,N})_a
\end{tikzcd}$$

: module proj. sur $A[G_N]$

A voir : action de G_N sur $X(p, N)$ est modérée en car 3, et $p \equiv -1 \ (3)$.

Ennuis possibles proviennent de la courbe supersingulière de car. 3.

Groupe d'aut. d'ordre 12, $\underbrace{C_3}_{\text{inv.}} \cdot C_4 = \mathrm{Aut}$

C_3 opère librement sur les points super-singuliers de $X(p, N)$.

$C_3 \subset GL_2(\mathbb{F}_p)$, son action sur la droite $\mathbb{P}_1(\mathbb{F}_p)$ est libre.

sinon, droite stable $\to 3 \mid p-1$.

M sur $A[G]$, G groupe fini, A anneau de val. discrète, π, $k = A/m$

M projectif, $\varepsilon : G \to A^*$

$M_\varepsilon = \{ m \in M \mid gm = \varepsilon(g) m$ pour tout $g \in G \}$

$\overline{M} = M/\pi M$, $\bar{\varepsilon} : G \to A^* \to k^*$

$\overline{M}_{\bar{\varepsilon}} \subset \overline{M}$

Assertion: $\overline{M}_{\bar{\varepsilon}}$ "=" $\overline{M_\varepsilon}$

$M_\varepsilon \to M$ induit $\overline{M_\varepsilon} \hookrightarrow \overline{M}$.

$\varepsilon\chi$ ordre une puis. de p ($p = \operatorname{car} k$)

$\overline{\varepsilon\chi} = \bar{\varepsilon}$

Niveau 1

Formes modulaires sur $SL_2(\mathbb{Z})$ à coeff. $\in \mathbb{Z}$ et leur réduction mod p.

Raisonnable si $p \geq 5$

Intéressant si $p = 2, 3$.

Notations:

$$E_k = 1 - \frac{2k}{b_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

k entier pair ≥ 2

$(E_0 = 1)$

$$\sigma_m(n) = \sum_{\substack{d \geq 1 \\ d \mid n}} d^m$$

$\pm b_{2k} = B_k$

$$G_k = -\frac{b_k}{2k} + \sum \sigma_{k-1}(n)\, q^n$$

$$\frac{-b_k}{2k} = \zeta(1-k)/2$$

Séries d'Eisenstein de poids k $(2,4,\dots)$

E_2 n'est pas une forme modulaire (ni sur $SL_2(\mathbb{Z})$, ni sur un s/g d'indice fini).

E_k, k pair ≥ 4, est modulaire.

$(G_k = a_0 + \sum a_n q^n)$

$$\sum a_n n^{-s} = L_k$$

$$= \zeta(s)\,\zeta(s+1-k)$$

Pole simple en $s = k$

(pas en $s = 1$ si $k \geq 4$)

aussi en $s = 1$ si $k = 2$.

$(\zeta(0) = -\frac{1}{2}$

$$E_2(z) - N E_2(Nz) = \sum a_n q^n - N \sum a_n q^{Nn}$$

$\sum a_n'' q^n$ modulaire sur $\Gamma_0(N)$.

$$L_2(1 - N \cdot N^{-s})$$

Hecke: $a_0 = -\left\{ \sum_{n=1}^{\infty} a_n n^{-s} \right\}_{s=0}.$

Terme constant de $G_k = -\zeta(0)\,\zeta(1-k)$

$$= \frac{1}{2}\zeta(1-k).$$

$$a_0 + q + q^4 + q^9 + \cdots = \theta \qquad a_0 = ?$$

$$\sum (n^2)^{-s} = \zeta(2s) \quad \Rightarrow \quad a_0 = \frac{1}{2}.$$

$$\theta = \frac{1}{2}\sum_{-\infty}^{\infty} q^{n^2}.$$

$$Q = E_4 = 1 + 240 \sum \sigma_3(n) q^n$$

$$R = E_6 = 1 - 504 \sum \sigma_5(n) q^n$$

$$P = E_2 = 1 - 24 \sum \sigma_1(n) q^n$$

$$\Delta = \frac{1}{2^6 3^3}(Q^3 - R^2) = q \prod_{n=1}^{\infty} (1-q^n)^{24}$$

Sur $\mathbb{C}$ (ou $\mathbb{Q}$) l'algèbre des formes modulaires est $\mathbb{C}[Q,R]$ (resp. $\mathbb{Q}[Q,R]$).

L'algèbre des formes modulaires à coeff $\in \mathbb{Z}$

$$\bigoplus_{k=0}^{\infty} M_k(\mathbb{Z})$$

est $\mathbb{Z}[Q,R,\Delta] / \left(\Delta = \frac{1}{1728}(Q^3 - R^2)\right)$

$k = 18$ base = ?

$\dim M_{18} = 2$ $\qquad (1, q, q^2, \ldots, q^i)$

$1 + \cdots = Q^3 R$

$q + \cdots = \Delta R$

Pour aujourd'hui,

$$\widetilde{M}_k = \text{red. mod } p \quad \text{(comme série formelle)}$$

de $M_k(\mathbb{Z})$.

Swinnerton-Dyer (~ 1970)

Relation $\quad E_{p-1} \equiv 1 \pmod p$.

comme série formelle en q.

(Exposé précédent

section formelle

ω^{p-1}

coord. locale formelle

$E_{p-1} = 1$ au vg de ∞

(données par courbe de Tate)

$$E_{p-1} = 1 - \frac{2(p-1)}{b_{p-1}} \sum \cdots \equiv 1 \pmod p)$$

$$b_{p-1} = \frac{\cdots}{p} = \frac{\alpha}{p} \qquad \alpha \in \mathbb{Q} \quad \text{unité } p\text{-adique}$$

$E_{p-1} \in M_{p-1}(\mathbb{Z}_p)$. $\qquad$ $\underline{p \geq 5}$

Toute relation entre formes modulaires mod p provient de $E_{p-1} \equiv 1 \pmod p$.

<u>Notation</u>:

$$A = E_{p-1}, \qquad B = E_{p+1} \in M(\mathbb{Z}_p).$$

Multiplication par A

$$\widetilde{M}_k \xrightarrow{A} \widetilde{M}_{k+(p-1)}$$

$$\begin{array}{ccc} \omega^k & & \omega^{k+p-1} \\ f & \longrightarrow & f\, E_{p-1} \end{array}$$

$$B \in M(\mathbb{Z}_p) \cup \widetilde{M}_\alpha = \underbrace{\widetilde{M}_c}_{\text{dim infinie}}$$

α classe c

paire mod $(p-1)$

$$\bigoplus_{c \bmod (p-1)} \widetilde{M}_c \longrightarrow \text{séries formelles}$$

est injective.

Lien entre E_{p-1} et l'invariant de Hasse des courbes elliptiques.

forme modulaire f $\begin{array}{l} \text{car } 0 \\ \text{car } p \end{array}$ de poids k

E c. ell. sur un corps

$$\Longrightarrow f(E) \in \omega^{\otimes k}(E)$$

$\omega(E)$ = dual de l'espace tangent à E en 0

= esp. des formes diff. de 1ère espèce sur E

$$f \longmapsto f(E)$$

$f \mapsto f(E)$

$E_4 \longrightarrow$ "C_4"

$E_6 \longrightarrow$ "$-C_6$"

$\Delta \longrightarrow \Delta$ disc.

$y^2 = 4x^3 - g_2 x - g_3$

$w = \frac{dx}{y}$ $\qquad x = \wp u$, $y = \wp' u$, $w = du$

$g_2 \; w^{\otimes 4}$

$g_3 \; w^{\otimes 6}$

Néron, Tate (formulaire de Tate "mis au goût du jour" par Deligne, LN 476).

$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$

à constante près, $g_2 = c_4$ à signes
$g_3 = c_6$ près.

$E_{p-1} =$ "inv. de Hasse" (Deligne)

E courbe elliptique en car p

$w \neq 0$ diff. de $1^{\text{ère}}$ espèce

$\Rightarrow A(E, w) \in$ corps

$A(E, w)\, w^{\otimes p-1}$.

Lie E a str. nat. de p-alg. de Lie

$X \to X^p$

$t \to t$ $\qquad$ $t \leftrightarrow t^{\otimes p}$

p- linéaire.

$t^{-1} \otimes t^{\otimes p}$

$\left(\omega^{p-1} = \omega^{-1} \otimes \omega^{p} \right)$

Autre façon :

(dual du précédent)

Opération de Cartier

$\omega \longmapsto C\omega$ $\qquad$ p^{-1}- linéaire

$\omega \qquad (C\omega)^{\otimes p} \cdot \omega^{-1} \in \omega^{p-1}(E)$.

Coordonnées locales

p^{-1} - linéaire

$$\begin{cases} C \dfrac{du}{u} = \dfrac{du}{u} \\ C\, dt = 0 \end{cases} \qquad \omega = dt \sum a_n t^n$$

$C\omega$?

$\dfrac{1}{n+1} a_n t^{n+1}$ $\qquad$ sauf si $n \equiv -1 \pmod p$

$$C\omega = \sum_{n = mp-1} a_n^{1/p}\, C(t^{mp}/t\, dt)$$

$$= \sum a_n^{1/p} t^m \frac{dt}{t}$$

$$\sum a_n t^n dt \longmapsto \sum a_n^{1/p} t^m \frac{dt}{t}$$

3ème façon de faire :

effet de V sur esp. tg

$$\begin{tikzcd} A \arrow[r, "F"] \arrow[rr, bend right, "p"'] & A^p \arrow[r, "V"] & A \end{tikzcd}$$

$4^{\text{ème}}$ façon :

Groupe formel, t paramètre

$$F(t,t') = t + t' + \cdots$$

$$[2]t = F(t,t) = 2t + \cdots$$

$$[p](t) = a_p t^p + \cdots$$

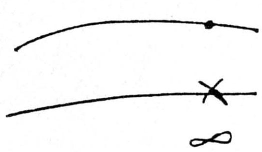
a_p "=" invariant de Hasse

$$\omega = dt + \cdots$$

Méthode de Deligne

Hasse $\in M_{p-1}$ en car p

lequel ?



$$\frac{dx}{x} \qquad C\left(\frac{dx}{x}\right) = \frac{dx}{x} = 1 \cdot \frac{dx}{x}$$

Calcul : $[p](t) = E_{p-1} t^p + \cdots$

<u>Exemple</u> : $p = 5$, $A = E_{p-1} = Q$

$p = 7$, $E_{p-1} = R$

$p = 11$ $E_{p-1} = QR$

. . . .

<u>Rappel</u> sur les courbes supersingulières en car p.

$\overline{\mathbb{F}}_p$ E est super-sing. $\iff$ inv. de Hasse $= 0$

$\iff \omega = df$

$\iff \mathrm{End}\, E$ est un ordre max d'un corps de quat. ram en $\{p, \infty\}$.

$\Leftrightarrow$ $E/\mathbb{F}_q$ $\quad \pi^{\text{puis}} = \text{hom.}$

$$\begin{tikzcd} E \arrow[r, "F"] \arrow[rr, bend right, "p"'] & E^p \arrow[r, "V"] & E \end{tikzcd}$$

ss. $\Leftrightarrow$ appl. tgte à $V = 0$

$$\begin{tikzcd} E \arrow[r, "F"] \arrow[rr, bend right, "p"'] & E^p \arrow[r, "F"] & E^{p^2} \cong E \end{tikzcd}$$

$\Leftrightarrow$ pas de pt d'ordre p

$y^2 = x^3 + ax + b$ $\qquad$ ($a, b = Q, R$ à cte près)

Courbes supersingulières

Formule de masse :

$$\sum_{E \text{ s.s.}} \frac{1}{|\mathrm{Aut}(E)|} = \frac{p-1}{24} \qquad \text{(Eichler-Deuring)}$$

$p = 2$ $\quad$ 1 seule courbe ss $y^2 + y = x^3$

Aut d'ordre 24 $\simeq SL_2(\mathbb{F}_3) = \tilde{A}_4$

$p = 3$ $\quad$ — " — $\quad j = 0 = 1728$ —— 12

$p \geq 5$ $\quad$ $|\mathrm{Aut}| = 2$ $\quad$ sauf si

$p \equiv -1 \pmod 4$ $\quad j = 1728$ $(R = 0)$ $\quad |\mathrm{Aut}| = 4$

$p \equiv -1 \pmod 3$ $\quad j = 0$ $\quad (Q = 0)$, $\quad |\mathrm{Aut}| = 6$

mod 12 :

~~mod~~

$p \equiv 1 \ (12)$ $\quad |Aut| = 2$, nbre de courbes $\frac{p-1}{12}$

$p \equiv 5 \ (12)$ $\quad \frac{1}{6} + \left(\frac{1}{2} + \cdots + \frac{1}{2}\right) = \frac{p-1}{24}$

$p \equiv 7 \ (12)$ $\quad \frac{1}{4} + \left(\frac{1}{2} + \cdots + \frac{1}{2}\right) = -$

$p \equiv 11 \ (12)$ $\quad \frac{1}{4} + \frac{1}{6} + \left(\frac{1}{2} + \cdots + \frac{1}{2}\right) = -$

$p \geq 5$ $\quad (j = Q^3/\Delta)$

Supposons $p \equiv 1 \pmod{12}$

$m = \frac{p-1}{12}$ $\quad j_1, \ldots, j_m$ les j corresp.

$$E_{p-1} \equiv \prod_{i=1}^{m} (Q^3 - j_i \Delta) \pmod{p},$$

$$p-1 = 12 \cdot m$$

$p \equiv 5 \pmod{12}$

$$E_{p-1} = Q \prod_{i=1}^{m} (Q^3 - j_i \Delta)$$

$m = \frac{p-5}{12}$, j_i = invariant des courbes supersing. à aut. ± 1.

$p \equiv 7 \pmod{12}$

$$E_{p-1} \equiv R \prod (Q^3 - j_i \Delta)$$

$p \equiv 11 \pmod{12}$

$$E_{p-1} = QR \prod (Q^3 - j_i \Delta).$$

j_i invariant des courbes supersingulières.

$j_i \in \mathbb{F}_{p^2}$ $\qquad j = j^{p^2}$

$$E \longrightarrow E^{(p^2)} \xrightarrow[\cong]{} E$$

Toute courbe elliptique supersingulière a une structure canonique sur $\mathbb{F}_{p^2}$ t.q. son Frob. soit $-p$.

$E \quad / \overline{\mathbb{F}_p}$.

$j \in \mathbb{F}_{p^2}$: $E/\mathbb{F}_{p^2}$ $\qquad$ Frob $= \pi : E \circlearrowleft$

j supersinguliers se divisent en 2 familles :

ceux dans $\mathbb{F}_p$ $\qquad$ couples de conjugués dans $\mathbb{F}_{p^2} - \mathbb{F}_p$.

1. Il y en a toujours qui sont dans $\mathbb{F}_p$
2. Tous les j ss sont dans $\mathbb{F}_p$

$\iff$ p divise l'ordre du Monstre

($p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$
$31, 41, 47, 59$ et 71).

Tous les j dans $\mathbb{F}_p$ $\iff$ le genre de la courbe $X_0(p)^+$ (qt. de $X_0(p)$ par
$= 0$ $\qquad$ $\mathbb{H}/\Gamma_0(p)$
son involution $z \longrightarrow -\frac{1}{pz}$
$\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$)

$\underset{\text{Ogg}}{\Longleftrightarrow}$ p divise l'ordre du Monstre.

Nombre des $j \in \mathbb{F}_p$: $(p \geq 5)$

Deuring

$$\text{nombre} = \begin{cases} \frac{1}{2} h(-4p) & p \equiv 1 \pmod 4 \\ \frac{1}{2}\left[h(-p) + h(-4p)\right] = \begin{cases} h(-p) & p \equiv 7 \ (8) \\ 2h(-p) & p \equiv 3 \ (8) \end{cases} \end{cases}$$

$h(-4p)$: nbre de classes de $\mathbb{Q}(\sqrt{-p})$

Il existe une courbe elliptique supersing. sur $\mathbb{F}_p$ de Frob. π t.q. $\pi^2 = -p$.

$$D_{p,\infty} \supset \mathbb{Q}(\sqrt{-p}) \ni \pi$$

$\exists$ ordre max qui contient π

Donne courbe $/\mathbb{F}_p$, $\mathrm{End} \ni \pi$

$$\pi^2 = -p \qquad \begin{cases} \pi\bar{\pi} = p \\ \mathrm{Tr}\,\pi = 0 \end{cases}$$

E_0 sur $\mathbb{F}_p$, π $\pi^2 = -p$

$p \equiv 1 \ (4)$

$$\mathbb{Z} + \mathbb{Z}\pi = \mathbb{Z}[\sqrt{-p}]$$

$$\mathrm{End}(E_0) = \mathbb{Z}[\sqrt{-p}] = R$$

P module proj. de rang 1 sur $R = \mathrm{End}\, E_0$

$P \in \mathcal{Cl}(R)$

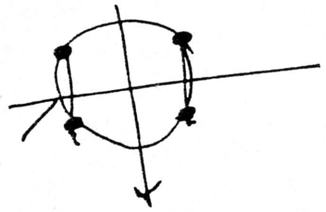
$E_p = P \otimes_R E_0$. $\quad E_p / \mathbb{F}_p$

$Cl(\mathbb{Z}[\sqrt{-p}]) \longrightarrow j$ supersingulier $\in \mathbb{F}_p$.

Fibres ont 2 éléments.

$p \equiv 1\ (4)$

$p = 17 \qquad h(-4.17) = 4$



symétrie

p.r. point qui n'est pas dans la liste.

$p \equiv 1\ (4)$

$p \equiv 3\ (4) \qquad j = 1728 \quad y^2 = x^3 - x$

$R = 0$

$\pi^2 = -p$.

$\mathbb{Z} \oplus \mathbb{Z}\pi \subset \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] = \mathbb{Z}\left[\frac{1+\pi}{2}\right]$

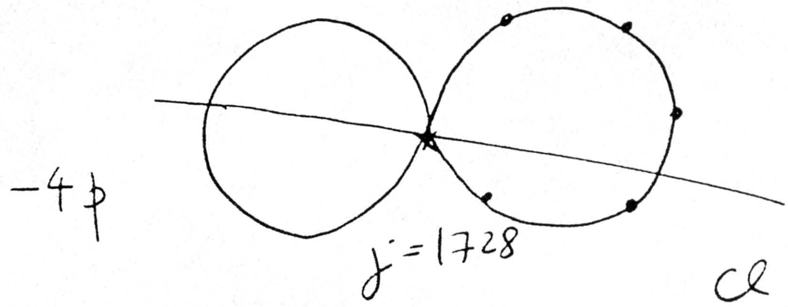
Points de div. par 2 sont rat. $/\mathbb{F}_p$.

$\pi - 1$ est divisible par 2 (dans End).

$y^2 = x^3 + x \qquad$ action par $R_{-4p} = \mathbb{Z}[\sqrt{-p}]$.

$j = 1728$ pour les 2 courbes.

$p \equiv 7 \ (8)$

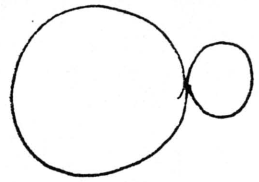


Cl_{-p}

$Cl_{-p} \longrightarrow j$ ss

fibres : $(x, -x)$.

$p \equiv 3 \ (8)$



$$h(-4p) = \begin{cases} h(-p) & \text{si } p \equiv 7 \ (8) \\ 3\, h(-p) & p \text{ inerte.} \end{cases}$$

$(p = 3$: trop d'automorphismes).

E ss a une structure canonique $/\mathbb{F}_{p^2}$

avec Frob $= -p$

Fonctorielle : tout hom. entre c. s.s est $/\mathbb{F}_p$

$\omega^{\otimes(p^2-1)}(E)$ a une base canonique.

$(E$ s.s.$)$ à savoir α^{p^2-1}, où

α est une forme $\neq 0$ rat. sur $\mathbb{F}_{p^2}$

pour la structure canonique.

<u>Th</u> : La base canonique de $\omega^{p^2-1}(E)$ est

$p = 2$ $\quad a_3\, \omega^3$

$p = 3$ $\quad b_4^{\,2}\, \omega^8$.

$p \geq 5$ $\quad (E_{p+1})^{p-1}$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

ss $\iff$ $a_1 = 0$ $\qquad \omega = \dfrac{dx}{a_1 x + a_3} = \dfrac{dx}{a_3}$

$(a_3 \omega^{\otimes 3})$

$E_{p+1} \neq 0$ sur une courbe ss.

E_{p-1}, E_{p+1} "premiers entre eux".

1) Supposons E sur $\mathbb{F}_p$

$\pi^2 = -p$, ω, $E_{p+1} \in \omega^{p+1}(E)$

rat. / $\mathbb{F}_p$

(donc sur $\mathbb{F}_{p^2}$).

$E_{p+1} = \lambda \alpha^{p+1}$ $\quad \lambda \in \mathbb{F}_p^*$.

$E_{p+1}^{p-1} = \alpha^{p^2-1}$.

Transformations de E_{p+1} par isogénie

(G. Robert) prochaine fois.

$$E_2 = P = 1 - 24 \sum_1^\infty \sigma_1(n) q^n$$

$$E_4 = Q = 1 + 240 \sum_1^\infty \sigma_3(n) q^n$$

$$E_6 = R = 1 - 504 \sum_1^\infty \sigma_5(n) q^n$$

$p \geq 5$ $E_{p-1} = A \equiv 1 \pmod p$ comme série en q

$E_{p+1} = B \equiv P \pmod p$

E supersingulière en car p
définie de façon canonique sur $\mathbb{F}_{p^2}$ avec
Frob $= -p$.

ω_E = espace cotangent à E, struct naturelle de $\mathbb{F}_{p^2}$ e.v.

$\omega_E^{\otimes(p^2-1)}$ a une base canonique
α^{p^2-1} où $\alpha \in \omega_E$, $\alpha \neq 0$, α rat. sur $\mathbb{F}_{p^2}$.

Si $p \geq 5$ l'élément canonique est $E_{p+1}^{p-1}(E)$

$E_{p+1}(E)$ forme diff $\in \omega_E^{p+1}$

1^e cas E est définissable sur $\mathbb{F}_p$

$$E_{p+1}(E) = \lambda \alpha^{p+1} \quad \lambda \in \mathbb{F}_p^* \quad \lambda^{p-1} = 1$$

(on utilise $E_{p+1} \neq 0$ essentiellt !).
Car ~~à~~ 1^er à $A \Leftrightarrow$ ne s'annule pas sur supersing
et (B, A) car équa du 2^e ordre en A et B "dérivée".

Théorème (G. Robert) : Si $\varphi : E \to E'$ est une isogénie de courbes supersingulières,

$$\varphi^* B(E') = \deg \varphi \; B(E).$$

On l'admet pour le moment.

Donc si φ est séparable (exp. hgt $\neq 0$),

$$\varphi^* B(E')^{p-1} = B(E)^{p-1}$$

~~Ils co~~ Les invariants coïncident au-sur une courbe (déf sur $\mathbb{F}_p$).

en fait He c. ss est isogène (par une isogénie séparable) à n'importe quelle autre.

Autre construction de $B = E_{p+1}$ (à un facteur près

Remarque: $[-p](t) = \lambda t^{p^2} + \dots$

$$\omega = \alpha t + \dots$$

$$\lambda \omega^{p^2-1} \text{ intrinsèque}$$

sur le groupe formel unif !

On pourrait attraper aussi cela avec module de Dieudonné (avec la structure supplémentaire donnée par la polarisation naturelle de la courbe elliptique).

E c.ell ssp.

ω forme diff de $1^{ère}$ espèce $\neq 0$ $C\omega = 0$.

ie $\exists$ fction rationnelle f sur E $df = \omega$

Ex: $p = 2$ $y^2 + y = x^3$ $\omega = dx$ $f = x$

+ généralt $f \underset{\text{local}}{=} \sum_{i \geq 0} \alpha_i t^{-ip} + \underbrace{g(t)}_{\text{exp} \geq 0}$.

$$f^{\frac{1}{p}} \omega = \left(\sum \alpha_i^{1/p} t^{-i} \right) \omega + \text{série à exp} \geq 0$$

Résidu $f^{1/p} \omega$ ~~$= \alpha_1^{1/p}$~~ $\omega = \alpha_0 dt + \dots$

$= \text{coeff en } t^{-1} dt$.

$$\lambda = \sum_{P \in E} \operatorname{Res}_P (f^{1/p}\omega)$$

Ceci ne dépend pas du choix de f ($f + F^p$ donne $F\omega$ donne m̃ Σ de res).

$\lambda \neq 0$. f peut être choisi avec pôle p-uple en 0 et aucun pôle ailleurs.

$$f = \gamma t^{-p} + \text{hol} \ldots \qquad \omega = dt + \ldots$$

$$\lambda = \gamma^{1/p}$$

A la courbe elliptique, on associe $\frac{1}{\gamma}\omega^{\otimes(p+1)} = \Gamma(E)$

si $\omega' = c\omega$ $\quad f' = cf$

$$\lambda' = c^{1/p}\, c\lambda = c^{\frac{p+1}{p}}\lambda \qquad \gamma' = \lambda'^p = c^{p+1}\gamma$$

$$\Gamma' = \frac{1}{\gamma'}\omega'^{(p+1)} = \frac{1}{c^{p+1}\gamma} c^{p+1}\omega^{p+1} = \frac{1}{\gamma}\omega^{p+1} = \Gamma(E)$$

d'où forme diff. canonique non nulle.

Cet invariant a la propriété des isogénies séparables

$$\varphi^*\Gamma(E) = \deg\varphi\, \Gamma(E).$$

Calcul pour $p = 5$ (ne sait pas faire le cas général).

Γ

$5 \equiv -1 \bmod 3 \Longrightarrow$ E_{p+1} $\quad E \quad y^2 = x^3 + 1$.

$E_{p+1} = E_6 \equiv -1 \bmod 5 \quad$ ("$2^5 3^3 a_6 + \ldots$")

$$\omega = \frac{dx}{2y} \qquad d(xy) = 2\omega \qquad f = \frac{1}{2}xy$$

9 $\quad x = \frac{1}{t^2} + \ldots \qquad y = -\frac{1}{t^3} + \ldots$

$$\omega = dt + \ldots$$

$f^{1/5}\omega \underset{\text{localt}}{=} -\frac{1}{2} t^{-1} dt + \ldots \qquad \lambda = \mathrm{Res} = -\frac{1}{2}$

$\Gamma = -2\omega^5 \qquad B = -\omega^6 \qquad \Gamma = 2B$

Pour $p=7$ et 11 $\qquad \Gamma = 4B$ pour $p=7$

$\Gamma = \cancel{8}2B$ pour $p=11$

Niveau 1 (suite) Action des opér de Hecke T_ℓ $\ell \neq p$ sur M_k = esp des formes modulaires mod p de poids k.

$M_k \xrightarrow{A} M_{k+p-1} \qquad W_k = M_k / M_{k-(p-1)}$

action des T_ℓ sur W_k.

$f \in M_k \longrightarrow \{ \underset{\text{ssup.}}{E} \longmapsto f(E) \in \omega_E^k \}$

$f \in M_{k-(p-1)} \Leftrightarrow f(E) = 0$ pour tte E s.s.

p. ex si $p \equiv 1$ (12) $\quad A = \prod (Q^3 - j_E \Delta)$

$W_k \hookrightarrow S_k \qquad S_k$ = { espace des "formes modulaires de poids k sur les courbes supersing"

$\varphi \in S_k$: $E \longrightarrow \varphi(E) \in \omega_E^k$

$\sigma : E \xrightarrow{\sim} E' \qquad \sigma^* \varphi(E') = \varphi(E)$

Concrètement : $E_1, \ldots, E_h$ supersing (à isom près)

$G_i = \mathrm{Aut}\, E_i$

$\varphi \Leftrightarrow$ pour chaque i d'un élt $\varphi_i \in \omega_{E_i}^k$

invariant par G_i

Exemple $\quad p \equiv 1 \bmod 12 \quad G_i^m = \pm 1$

la propriété $\Longleftrightarrow$ k pair

donc esp de dim h.

$p \equiv 5 \bmod 12 \quad G_i = \pm 1$ sf 1 d'ordre cyclique

k pair $\qquad$ il faudra $6|k$

			dim =
$p \equiv 1 \bmod 12$	$h = \frac{p-1}{12}$	h courbes s.s.	
$p \equiv 5 \bmod 12$	$h = \frac{p-5}{12}$	$h+1$ ss.	$\begin{cases} h & 3\nmid \\ h+1 & 3 \end{cases}$
$p \equiv 7 \bmod 12$	$h = \frac{p-7}{12}$	$h+1$	$\begin{cases} h & 4\nmid \\ h+1 & 4\mid \end{cases}$
$p \equiv 11 \bmod 12$	$h = \frac{p-11}{12}$	$h+2$	$\begin{cases} h & 4\nmid,\ 3\nmid \\ h+1 & 4\mid k \text{ ou } 4\nmid k \\ h+2 & 12\mid k \end{cases}$
$p = 2$		1	$\begin{cases} 0 & \text{si } 3\nmid k \\ 1 & 3\mid k \end{cases}$
$p = 3$		1	$\begin{cases} 0 & \text{si } 4\nmid \\ 1 & \text{si } 4\mid \end{cases}$

$\Gamma = c_p E_{p+1}$ et $c_p \equiv -\frac{1}{12}$? probable. OK Deligne.

$M_k / M_{k-(p-1)} = W_k \subset S_k \qquad p \geq 5$

Théorème $\quad W_k = S_k$ si $k \geq p+1$ k pair.

(Calcul de dimension) : la dim de $M_k \simeq k/12$

$M_{k-(p-1)} \simeq \frac{k-(p-}{12}$

Autre idée (cf + tard) :

$$0 \to \mathcal{M}_{k-(p-1)} \xrightarrow{A} \mathcal{M}_k \to \mathcal{S}_k \to 0$$

~~dim 1 en chaque pt.~~ concentré aux courbes sup. sing.

cohomologie : $H^0(\mathcal{S}_k) = S_k$

$$0 \to M_{k-(p-1)} \to M_k \to S_k \to H^1(\mathcal{M}_{k-(p-1)}) \to \dots$$

dual de $H^0(\Omega^1 \otimes \mathcal{M}_{k-(p-1)}^{\text{dual}})$

(pas correct en niveau 1 !!!

$\Omega^1 = \mathcal{M}_2^{\text{cusp}}$

$\to H^0$ (formes parab de poids $-k+p+1$)

$= 0$ si $k \geq p+1$.

(1) $S_k \simeq S_{k+p^2-1}$ (action des T_ℓ compris).

action des T_ℓ sur S_k : $\varphi \in S_k \mapsto \varphi | T_\ell (E)$

$= \frac{1}{\ell} \sum_C \pi_C^* (\varphi(E/C))$

ss gpes cycliques d'ordre ℓ contenus ds E

$\pi_C : E \to E/C$

si $k = 0$ $\quad \varphi = 1 \quad 1 | T_\ell = 1 + \ell^{-1}$

$(\neq 1 + \ell^{k-1})$.

② $S_{k+p+1} \cong S_k[1]$ (action des T_ℓ - -)

ie M module sur les T_ℓ

$M[h] = M$ muni de $\ell^h T_\ell$.

dû à G. Robert

Tate pour semi simp des S_k.

$\varphi \in S_k \longmapsto \varphi . B$

$T_\ell(\varphi B) \overset{?}{=} \ell T_\ell(\varphi) B$ Notation arbitraire $\varphi | T_\ell = T_\ell \varphi$

Sur E

$T_\ell(\varphi B)$ donne $\frac{1}{\ell} \sum_C \pi_c^*(\varphi(E/C) B(E/C))$

$\ell T_\ell(\varphi) B$ — $\sum_C B(E) \pi_c^*(\varphi(E/C))$

Or $\pi^* B(E/C) = \ell B(E)$.

Démonstration de cette formule :

1ère étape Il y a un b dans S_{p+1}, $b \neq 0$

avec $\pi^* b(E') = (\deg \pi) b(E)$ pour π sép.

(Rque : si non sép, vrai aussi mais 0 de chaque côté

2ème étape $M_{p+1} = W_{p+1} = S_{p+1}$

A cause de $M_{p+1} \simeq S_{p+1}$, il y a une fction $f \in M_{p+1}$ correspdt.

3e étape $T_\ell b = (\ell+1) b$ pour $\forall \ell$ 1er à p.

donc $T_\ell f = (\ell+1) f$ ds M_{p+1}

4e étape caractérise la série d'Eisenstein E_{p+1}

$1^{\text{ère}}$ étape : par exemple Γ^1 !

$0 \neq b(E)$ pour une courbe supersing

$\pi \quad E' \to E$

On définit $\quad b(E') =: \dfrac{1}{\deg \pi} \pi^* b(E)$

Lemme Si $u \in \operatorname{End} E$ $\quad E$ supersing

l'action de u sur ω_E^{p+1} $(\alpha \mapsto u^*\alpha)$ est

$\alpha \longrightarrow \deg u \; \alpha$

(On sait que $\operatorname{End} E = D \quad u \in D \xrightarrow[\theta]{\text{sur}} \mathbb{F}_{p^2}$

u agit sur ω^1 par multipl. par $\theta(u) \in \mathbb{F}_{p^2}$.

$\theta(u)^{p+1} = \theta(u)\,\theta(u)^p = \theta(u\bar{u})$.

4^e étape : $\quad E_{p+1} = B$ est caract (à hom près)

par $T_\ell \quad (f) = (\ell+1) f \quad (\ell \neq p)$.

$f = \sum a_n q^n \longmapsto \tilde{f} = \sum_1^\infty n a_n q^n$ détruit les n divisibles par p

$T_p = U$ annule $\tilde{f}$ et $\tilde{B}$ $\quad f' = \tilde{f} - \lambda \tilde{B}$

tq coeff de q soit 0

$\to$ ts les coeff sont 0.

$\tilde{f} - \lambda \tilde{B} = 0 . \longrightarrow f - \lambda B = g^p$

$g = \sum b_n q^n$.

$g = U g^p$ est de poids $p+1$

en poids $p(p+1)$ $\quad g^p = A^{p+1} (f - \lambda B)$

$A \mid g^p$, donc g (or rien en poids 2)

$\longrightarrow g = 0$.

$$T_\ell(fB) = \ell\, T_\ell(f).B + \text{ forme de poids } k-(p-1) \bmod p.$$

Rappel sur $\sim$: on baptise cet opérateur θ

$$\theta f \cdot \frac{dq}{q} = df$$

Théorème Si f est modulaire de poids k

$\theta f - \frac{k}{12} Pf$ est modulaire de poids $k+2$

Par ex parce que $\frac{\Delta^k}{f^{12}}$ mod de poids 0 donc sa diff (log) est de poids 2.

Opérateur ∂ défini par $12\,\theta f = kPf + \partial f$.

$$\partial : M_k \to M_{k+2}$$

Formules :

$$\theta P = \frac{1}{12}(P^2 - Q)$$

$$\theta Q = \frac{1}{3}(PQ - R)$$

$$\theta R = \frac{1}{2}(PR - Q^2)$$

L'opérateur stabilise l'alg engendrée par P, Q, R

$p \geq 5$ θ, ∂ existent mod p.

$$P \equiv B \bmod p$$

Formes mod p de niveau $N = 1$.
$p \geq 5$

$S_0, S_1, \dots, S_{p+1} \simeq S_0[1]$
En général $N_k \subset S_k$, et $\neq$.
par ex : $k = 0$ $W_0 =$ cte.
S_0 repère les courbes supersing.
Théorème : Le quotient S_k / W_k est isomorphe (comme module sur les T_ℓ) au dual de $W^{cusp}_{p+1-k}[k-1]$
$0 \leq k \leq p+1$

Rque : $M_k = W_k$ sf si $k = p-1$ $W_{p-1} = M_{p-1} / M_0$
" ctes.
On fait agir les opérateurs de Hecke par transposition sur le dual.
Autrement dit : $S_k \underset{\text{(gpe de Grothendieck)}}{\simeq} W_k + W^{cusp}_{p+1-k}[k-1]$ (Tate non publié en 73).

S_{p+1} $(= W_{p+1})$

$\mathbb{F}_p$: coefficients $S_{p+1} (= W_{p+1}) \longrightarrow \mathbb{F}_p$

$$f \in S_{p+1} = W_{p+1} = M_{p+1} \longmapsto a_0(f) \in \mathbb{F}_p.$$
$$f = \sum_0^\infty a_n(f) q^n.$$

(Cela marche parce qu'il n'y a pas de formes modulaires en poids 2 !!!).
Autre forme naturelle $S_{p+1} \simeq S_0[1] \to$ somme des valeurs.
Thme si $f \in M_{p+1}$, $a_0(f) = -12 \sum_E \frac{1}{w_E} \left(\frac{f}{B}\right)(E)$

$w_E = \frac{1}{2} |\mathrm{Aut}\, E|$. (à isom près).
c. superr

$f \in S_k,\ g \in S_{p+1-k} \longmapsto \langle f, g\rangle = \lambda(fg)$ $\quad fg \in S_{p+1}$

Thme ① Ce produit scalaire est non dégénéré

② Si $f \in W_k$, $g \in W^{cusp}_{p+1-k}$, alors $\langle f, g\rangle = 0$.

③ L'orthogonal de W_k dans $S_{p+1-k} = W^{cusp}_{p+1-k}$

$\hookrightarrow S_k / W_k$ dual de W^{cusp}_{p+1-k} : reste l'action de Hecke : on a « Formule de transposition » ;

④ $\langle T_\ell f, g\rangle = \ell^{k-1} \langle f, T_\ell g\rangle$.

Base explicite de $M_{p+1} = W_{p+1} = S_{p+1}$.

Pour chaque E supersingulière, il y a une unique $\varphi_E \in S_{p+1}$ telle que $\frac{\varphi_E}{B}(E) = 1$ et $\frac{\varphi_E}{B}(E') = 0$ si E' non iso à E.

φ_E est caractérisée par la formule suivante

Thme $\quad \varphi_E \dfrac{dq}{q} = \dfrac{12}{w_E} \dfrac{dj}{j - j_E}$

j_E = invariant de la courbe E.

$A = \prod_{\substack{E \text{ supers} \\ \text{avec } w_E = 1}} (Q^3 - j_E \Delta)\, Q^\alpha R^\beta \qquad \alpha, \beta \in \{0, 1\}$.

$A = \prod H_E \qquad H_E = Q^3 - j\Delta$ si E ss $w_E = 1$

$H_E = Q$ si $p \equiv -1 \bmod 3$, $j(E) = 0$, $w_E = 3$

$H_E = R \qquad p \equiv -1\ (4)$, $j(E) = 1728$, $w_E = 2$

Théorème $\varphi_E = \partial H_E \cdot \prod_{E' \neq E} H_{E'}$ poids $p-1$

$= \dfrac{\partial H_E}{H_E}$. comme série en q

Démonstration

$A = \prod H_E \quad B = \partial A = \sum \varphi_E$

$\dfrac{\varphi_E}{B}(E') = 0$ évidemment car $H_{E'} = 0$ sur E' par constr. $\quad \dfrac{\varphi_E}{B}(E) = \sum_{E'} \dfrac{\varphi_{E'}}{B}(E) = 1$

$H_E = Q^3 - j_E \Delta \qquad \partial H_E = 3Q^2 \partial Q - j_E \partial\Delta$

$\partial\Delta = 0$. (pas de ~~poids~~ formes modulaires paraboliques de poids 14).

$\partial Q = -4R$

$12\, \theta f = k P f + \partial f$

$\hphantom{12\,\theta f} = 0 \qquad k.1.a_0(f) + a_0(\partial f) \qquad a_0(\partial Q) = -4$

terme cte:

$\partial Q = -4R \quad -12Q^2R = \partial H_E$

$\varphi_E = -12 \dfrac{Q^2R}{Q^3 - j_E\Delta} \qquad \varphi = \dfrac{dq}{q} = -12 \dfrac{Q^2R/\Delta}{j - j_E} \dfrac{dq}{q}$

$dj = -\dfrac{Q^2R}{\Delta} \dfrac{dq}{q}$

Reste la formule d'unicité des formes naturelles :
Il suffit de la vérifier sur les φ_E, où elle devient

$a_0(\varphi_E) = -\dfrac{12}{w_E} \qquad j = \dfrac{1}{q} + \cdots$

$dj = -\dfrac{1}{q^2}dq + \cdots$

Variante $f \mapsto w_f = f \dfrac{dq}{q}$ = forme différentielle ration. (par rapport à j) avec des pôles simples au plus aux pts régul.

La formule dev. une formule de résidus.

②

$S_k \times S_{p+1-k} \longrightarrow \mathbb{F}_p$ défini par $\lambda(fg)$, est non dégénéré.

à 1 cte près, c'est $\sum \frac{1}{w_E} \frac{fg}{\Delta}(E)$

forme quadratique

Vérification des dimensions de $S_k / W_k = \dim W^{\text{cusp}}_{p+1-k}$ pour $0 < k \leq p+1$.

Formule d'adjonction :

$S_k \times S_{-k} \quad f, g \longrightarrow c \sum \frac{1}{w_E} fg(E)$

$f \in S_k \quad g \in S_{-k} \quad \langle T_\ell f, g \rangle = \ell^k \langle f, T_\ell g \rangle$

gauche : $= c \sum_E \frac{1}{w_E} g(E) \sum_{\substack{C \subset E \\ C \text{ ordre } \ell}} \frac{1}{\ell} \pi_C^* f(E/C)$.

$\pi_C : E \to E/C$

triplets : $\pi : E \to E'$ $\quad E, E'$ s.sing

π isogénie de degré ℓ

à isomorph. près

$$\begin{array}{ccc} E & \xrightarrow{\pi} & E' \\ {\scriptstyle 12}\downarrow & & \downarrow{\scriptstyle n} \\ E_0 & \xrightarrow[\pi_1]{} & E_1 \end{array}$$

$\alpha = (E, E', \pi)$

$w_\alpha = \frac{1}{2} |\mathrm{Aut}\, \alpha|$.

$(f, g) \mapsto a(f, g) = c \sum_{\substack{\alpha = (E, E', \pi) \\ \text{à iso}}} \frac{1}{\ell w_\alpha} \pi^* f(E') g(E)$

$t\alpha = \ell \quad E' \to E$

$p \equiv 1, 5, 7, 11 \mod 12$

$k = 0, 2, 4, 6, 8, 10 \mod 12$ $\rightarrow$ 24 cas !!!

$$\dim M_k + \dim M_{p+1-k} = 1 + \dim S_k$$
$$0 \leq k \leq p+1.$$

Par ex $p \equiv 11 \mod 12$
$k \equiv 8\ (12)$

$$\dim M_k = 1 + \frac{k-8}{12}$$

$$\dim M_{p+1-k} = 1 + \frac{p+1-k-4}{12}$$

$\frac{p-11}{12}$ c. hypersing avec $w = 1$

1 avec $w_E = 3$ mais pas stable

1 " 2

$$\dim S_k = 1 + \frac{p-11}{12}$$

Remarque : il peut être utile de considérer des N-rigidifications avec $p \nmid Gl_2(\mathbb{Z}/N\mathbb{Z})$.

Retour sur $f(E) = -\frac{1}{12} G_{p+1}(E)$ $p \geq 5$

(intérêt parce que formule d'isog claire).

$\mathbb{Z}_{(p)}$ E/S S schéma sur $\mathbb{Z}_{(p)}$

ω forme diff intégral. t

$$\omega = (1 + a_1 t + a_2 t^2 + \dots)\, dt$$

On choisit t : $\omega = (1 + a_{p-1} t^{p-1} + O(t^{2p-2}))\, dt$

$$t' \simeq t + \lambda t^p + O(t^{2p-1})$$

Par Riemann-Roch, $f \in O(pO)$

(pôle d'ordre p à l'origine)

$$f = t^{-p} + b_{-1} t^{-1} + b_1 t + \dots$$

unique

$t \to t'$ $t'^{-p} = t^{-p} + \ast\, t^{-1} + \ast\, t^{p-2}$

$\Rightarrow b_1$ indépendant de t

si $\omega \to \mu\omega$, ce qui est intrinsèque est $b_1\omega^{p+1}$

$E \xrightarrow{\Gamma} b_1\omega^{p+1}$ forme bien déf.

en car p et pour courbes supersing, on retrouve Γ.

$d\frac{\wp}{1} = (b_{-1}t^{-2} + b_1 t + \dots)\,dt$

$\Rightarrow \quad b_{-1} = 0 \quad d\frac{\wp}{1} = b_1\omega$ avec $b_1 \neq 0$

Thme : sur $\mathbb{Z}_{(p)}$, on a $\Gamma = \frac{1}{(p-1)!}\frac{b_{p+1}}{p+1} E_{p+1}$

en car p $\quad (p-1)! \equiv -1 \bmod p$

$\frac{b_{p+1}}{p+1} \equiv \frac{a_2}{2} \bmod p$

$\quad\quad a_2 = \frac{1}{12}$

Démonst : on se place sur $\mathbb{C}$ $\qquad \mathbb{C}/\underbrace{\mathbb{Z}+\mathbb{Z}\tau}_{L}$

$\omega = dz$

$t = z$

$\wp(z) = \frac{1}{z^2} + \sum_{k \text{ pair} \geq 2} (k+1)\, G_{k+2}(L) z^k$

$f = -\frac{\wp^{(k-2)}}{(p-1)!} = \frac{1}{z^p} + \dots$

$= \frac{1}{z^p} - pG_{p+1}(L)z + \dots$

$\Gamma(E) = -pG_{p+1}(L)\,dz^{p+1}$

$2\zeta(p+1)E_{p+1}(\tau) = G_{p+1}(L) \qquad E_{p+1}(E) = E_{p+1}(\tau)(2\pi i\,dz)$

$\zeta(p+1) = -(2\pi i)^{p+1}\frac{b_{p+1}}{2(p+1)!}$

$\Rightarrow$ le résultat.

$\rho : G_{\mathbb{Q}} \to Gl_2(\overline{\mathbb{F}}_p)$. syst de valeurs propres.

Tordre $\rho \mapsto \rho \otimes \chi$

Si $p = 5, 7$ séries d'Eisenstein $\quad a_\ell = 1 + \ell^{k-1}$

$$\rho = 1 \oplus \chi^{k-1}$$

Conjecture $(p = 5, 7) \Leftrightarrow$ il n'y a pas de rep irréductible $G_{\mathbb{Q}} \to Gl_2(\overline{\mathbb{F}}_p)$, niveau 1, non ram en dehors de p et de dét impair.

Pour $p = 2$ ou 3, l'analogue est vrai.

Tate : Si ordre de l'image $G < 60$, le groupe est résoluble et on "descend".

On peut regarder la ramif.

K non ram en dehors de p $\quad$ si mod ram, $d_K^{1/\deg K} \leq p$

$\mathbb{Q}$ $\quad$ avec $\deg K$, contrad avec les bornes de Minkowski

Sinon $d_K^{1/\deg K} \leq p^{2+\frac{1}{p}}$ $\quad$ $p = 2$ Odlyzko.

Exercice : Montrer qu'il n'y a pas de repres. absol irréduct. $G_{\mathbb{Q}} \to Gl_2(\mathbb{F}_5)$ non ram. en dehors de 5.

Un des problèmes est qu'on ne contrôle pas le corps d'arrivée.

f modulaire mod p ($p \geq 5$) "se ramènent aux poids $k \leq p+1$".
On va utiliser thme de Fontaine donnant la structure de l'inertie :

$f \in W_k \neq 0$ fction propre des T_ℓ, $\ell \neq p$ et $U = T_p$. ($k \leq p+1$)
$\rho_f : G_{\mathbb{Q}} \to Gl_2(\overline{\mathbb{F}_p})$ représentation associée
ρ_f peut être déduite de la rep de $G_{\mathbb{Q}}$ sur les pts de p division de $J_1(p) = \mathrm{Jac}(X_1(p))$.

Cas $k = p+1$ $\quad W_{p+1} = M_{p+1} \simeq$ formes de poids 2 mod p sur $\Gamma_0(p)$.
$M_{p+1}^{\mathrm{cusp}} =$ formes de 1ère espèce mod p sur $X_0(p)$
(cf Anvers III).

ρ_f : f poids $p+1$ sont données par les points de division par p de $\mathrm{Jac}(X_0(p))$.

Ramification en p de ρ_f (f poids $p+1$), supposons ρ_f irr

$$\rho_f \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \qquad \chi : \text{car cycl } G_{\mathbb{Q}} \to \mathbb{F}_p^*$$

ρ_f sauvagement ramifiée
et même très ramifiée. (Corps fixé par Ker contient $\mathbb{Q}_p(\sqrt[p]{\pi}, \sqrt[p]{u})$, $v_p(u) = 1$)

B. Mazur : Eisenstein ideals IHES

Décomp $\to \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ $\qquad \mathrm{Frob}_p \mapsto \begin{pmatrix} * & * \\ 0 & \lambda \end{pmatrix}$

$\lambda =$ val propre de U.
$(= \pm 1)$

conjecture dit qu'inversement une représentation de $G_\mathbb{Q}$ dans $GL_2(\overline{\mathbb{F}}_p)$ doit provenir d'une forme modulaire de poids $p+1$.

Exercice Si $G_{\mathbb{Q}_p} \xrightarrow{\rho_f} GL_2(\overline{\mathbb{F}}_p)$ du type $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ très ramifié sur l'inertie,

montrer que $\mathrm{Frob}_p \mapsto \begin{pmatrix} \alpha & \alpha \\ 0 & \pm 1 \end{pmatrix}$. $\det \rho_\chi = \cancel{\chi}$.

$k < p+1$ Il faut regarder les formes sur $\Gamma_1(p)$ cf Katz Mazur.

Si on les regarde p-adiquement ou mod p, il n'est pas raisonnable de ne s'occuper que de la pointe ∞. On regarde $\begin{cases} a_n \ p\text{-entier} \\ f|W = \sum b_n q^n \quad b_n \ p\text{-entier} \end{cases}$

$\Gamma_1(p) \subset \Gamma_0(p)$ quotient cyclique d'ordre $p-1$ où -1 agit trivialement.

$f|R_d = d^k f \to \overline{f} = M_{k+2}$

Traduire ρ_f en termes de la jacobienne de $X_1(p)$
Wiles Invent
Mazur Wiles

Fontaine $\to$ structure locale de ρ_f

$f : M_k$ f propre de Hecke $\quad$ parabolique $\quad 2 \leq k \leq p+1$.
T_ℓ

$* \ f|U = 0$. $\quad$ Res de ρ_f au gpe d'inertie en p est donnée par $\begin{pmatrix} \psi^{k-1} & 0 \\ \cdot\ \sigma & \overline{\psi}^{k-1} \end{pmatrix}$.

où ψ est : Inertie $\to \mathbb{F}_{p^2}^*$ (car fondamental de hauteur 2)

Inertie modérée $\rightleftarrows \varprojlim \mu_n$

Inertie ——— $= \mu_{p^2-1} = \mathbb{F}_{p^2}^*$

Ambiguïté de $\mathbb{F}_{p^2}^*$: K corps local à corps rés algr clos

$\mathrm{Gal}(\bar{K}|K) =$ inertie $\quad \mathrm{Gal}(K^{nr}/K) =$ inertie modérée

$$\downarrow$$

$$\mathbb{F}_{p^2}^*(k)$$

$$\parallel$$

$$\mathbb{F}_q^*(k)$$

$*$ $\quad f|U = \lambda f \quad \lambda \neq 0$

Alors $\rho_f \cong \begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix}$ sur le groupe d'inertie

Eventuellement modérément ramifié ou sauvagement

Le rep de Frob est λ ("en bas à dte").

Toute représentation locale de $G_{\mathbb{Q}_p}$

$$\rho : \mathrm{Gal}_{\mathbb{Q}_p} \to GL_2(\mathbb{F}_p) \ \chi^{k-1} \quad k \text{ pair}$$

$$\det = \chi^{k-1} \quad k \text{ pair}$$

On vérifie qu'une tordue $\chi^* \otimes \rho$ est de l'un des types $(*), (*)$.

(Conjecture par Tate ~ 1974

Dem par Fontaine ~ 1979).

Les formes compagnes

$f \quad k \quad \overset{?}{\cdot} \quad f' \quad p+1-k$

Soit f de poids k $\quad 2 \leq k \leq p+1$

f propre de U, T_ℓ.

$f|U = \lambda f \quad \lambda \neq 0$.

$\rho_f \cong \begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix}$ sur inertie.

~~Lcas~~ Supposons que $\rho_f \mid \text{Inertie} \cong \begin{pmatrix} \chi^{k-1} & 0 \\ 0 & 1 \end{pmatrix}$

(ie ordre de l'image de inertie premier à p)

$\chi^{p-k} \otimes \rho_f \simeq \begin{pmatrix} 1 & 0 \\ 0 & \chi^{p-k} \end{pmatrix} \simeq \begin{pmatrix} \chi^{p-1} & 0 \\ 0 & 1 \end{pmatrix}$

Conjecture : Il existe f' de poids $p+1-k$ fction propre de T_ℓ, avec $\rho_{f'} \simeq \chi^{p-k} \otimes \rho_f$.

"forme compagne".

$f | T_\ell = a_\ell f \qquad f' | T_\ell = \ell^{p-1} a_\ell \; f'$

$\theta f' = \theta^{p+1-k} f \qquad \theta f = \theta^k f'$. $\qquad$ de poids $p+1-k$

$U f = \lambda f \qquad U f' = \lambda^{-1} f'$

Si elle existe, réciproquement l'action de l'inertie est modérée.

Exemple :

$k = 12 \qquad p \geq 12 \qquad f = \Delta$.

$\Delta | T_p \bmod p \equiv \tau(p) \Delta$

$\tau(p) \not\equiv 0 \bmod p \qquad 11 < p < 2411$

ρ_Δ irréductible $\simeq \begin{pmatrix} \chi^{11} & * \\ 0 & 1 \end{pmatrix}$ sur inertie.

Dans quel cas $*$ disparait ?

$p = 17$ ou 19

pas de compagne car $p+1-k = 6$ ou 8

donc la représent devrait être sauvagt ramifiée

ce qui est vrai avec les bornes d'Odlyzko.

$$\begin{array}{l} E \\ | \\ \mathbb{Q} \end{array} \Big) \; GL_2(\mathbb{F}_{17}) \quad \sqrt[p]{\text{disc}} \quad \begin{array}{l} d^p > 10^5 \\ \leq 17 \end{array} \quad \Big| \text{ impossible}$$

$p = 23$ $\quad \rho_\Delta : G_{\mathbb{Q}} \to S_3 \subset GL_2$

$$S_3 \left(\begin{array}{c} E \\ |_3 \\ \mathbb{Q}(\sqrt{-23}) \\ |^2 \\ \mathbb{Q} \end{array} \right. \qquad \text{modérée en } p = 23 \quad \begin{pmatrix} \chi^{11} & 0 \\ 0 & 1 \end{pmatrix}$$

Conjecture: compagne ~~de~~ poids 12

Exercice modulaire

f, f' $\qquad \theta f = \theta^{*} f'$.

$f | U = \lambda f$

$f' | U = \mu f$ $\qquad \lambda\mu \neq 0 \quad$ A montrer $\lambda\mu = 1$.

Serre montre ± 1 : $\quad F = ff'$ en poids $p+1$

$F | U = \lambda\mu F$ calcul.

vap en poids $p+1$ est ± 1.

Reste à montrer modulairement que le produit est invariant par U.

Problème analogue sur les c. ellipt.

E réd ordinaire $\qquad E \equiv$ relevt canonique mod p ??

$$0 \to W_k \to S_k \to W^{\text{unop}\,\vee}_{p+1-k}[k-1] \to 0$$

f, f'

La même ρ est obtenue 2 fois par S_k

Par ex $k=12$ $p=23$ $\chi \otimes \rho_\Delta$ se voit 2 fois dans les formes de poids 26.

d'où une "multiplicité".

Cas supersingulier : c'est cette fois un théorème

Soit f de poids $k \leq p+1$

$f|U=0$ $f|T_\ell = a_\ell f$.

Alors il existe une compagne de poids $p+3-k$ avec $f'|U=0$ $f|T_\ell = a'_\ell f$ telle que $\rho_f \simeq \chi^{p+1-k} \otimes \rho_{f'}$.

Cas $p=2$

Q, R, Δ

$$\Delta \equiv q + q^9 + q^{25} + \cdots \equiv \sum_{q \text{ impair}} q^{n^2} \bmod 2$$

$\Delta | T_2$

$\Delta | T_\ell \equiv 0 \mod 2$

$\Downarrow$

$\tau(p) \equiv 0 \pmod 2$ pour $\forall p$ premier.

$$\Delta = q \prod (1-q^n)^{24} \equiv q \prod (1-q^{8n})^3 \bmod 2$$

$$\prod (1-x^n)^3 = 1 - 3x + 5x^3 - 7x^6 + \cdots$$

formes modulaires mod 2 = polynômes en Δ.

$T_\ell \Delta^i = a_0 \Delta^i + \cdots \bmod 2$

...... $a_0(x) = 0$.

$T_\ell\, \Delta^i$ est (mod 2) un polynôme en Δ de degré <

mod 8 $\quad \Delta^i \mid T_\ell \quad \ell$ 1er $\neq 2$

$$\Delta^i \mid T_\ell \equiv (1+\ell)\,\Delta + \text{polyn de } d^o < i \quad \text{mod } 8.$$

Démonstration

du résultat mod 2

$$T_\ell\, \Delta^i = a_0 \Delta^i + a_1 \Delta^{i-1} \ell^3 + \dots \quad \text{mod } 2$$

poids $12i$.

On teste sur E, courbe sing. $\quad y^2+y=x^3$

$\alpha_1\, R(E) \equiv 0$

$$T_\ell\, \Delta^i(E) = \frac{1}{\ell} \sum_{C \subset E} \pi_C^{*}\, \Delta^i(E/C)$$

ss gpe cyclique d'ordre ℓ

$E/C \simeq E \quad$ On le fixe

$$= \underbrace{\frac{1}{\ell}}_{1 \text{ mod } 2} \sum_{\pi : E \to E} \pi^{*} \Delta^i(E)$$

de degré ℓ

$\operatorname{End} E \xrightarrow{\varepsilon} \mathbb{F}_4$

$$\pi^{*} \Delta^i(E) = \varepsilon(\pi)^{12i}\, \Delta^i(E)$$
$$= \Delta^i(E)$$

$$T_\ell\, \Delta^i(E) = (\ell+1)\, \Delta^i(E) \equiv 0 \text{ mod } 2.$$

$\mathbb{F}_4 \quad \tau(p) \equiv p+1 \text{ mod } 3$

Autre méthode : la formule des traces

Ceci revient à démontrer que la trace de T_ℓ sur les formes paraboliques $\equiv \ell(1+\ell) \bmod 8$ de poids 12 :

formule d'Eichler-Selberg

$$\underset{\text{poids } k \geq 4}{\operatorname{Tr} T_p} = -1 - \sum \dots (k)$$

$$\sum \alpha_j \left(\pi^{k-2} + \pi^{k-3}\bar{\pi} + \dots + \bar{\pi}_j^{k-2}\right)$$

$$\pi_j \bar{\pi}_j = p.$$

$$\operatorname{Tr}_k T_\ell = -1 - \sum_{\substack{E \text{ c. ellip}/\mathbb{F}_\ell \\ \text{à } \mathbb{F}_\ell \text{ isomorph. près}}} \frac{1}{w_E} \operatorname{Tr}\left[\operatorname{Sym}^{k-2}(\operatorname{Frob}_E)\right]$$

$$w_C = \frac{1}{2} |\operatorname{Aut}_{\mathbb{F}_\ell} E|$$

si $\operatorname{Frob}_E \sim \pi, \bar{\pi}$ $\quad \operatorname{Tr} = \dfrac{\pi^{k-1} - \bar{\pi}^{k-1}}{\pi - \bar{\pi}} \sim \pi^{k-2} + \dots + \bar{\pi}^{k-2}$

Théorème Soit $F_p(X,Y)$ "le" polynôme tel que $F_p(j,j') \Leftrightarrow \exists$ une isogénie de degré p entre les courbes correspondants.

Alors $\quad F_p(X,Y) \equiv (X-Y)^{p+1} + \dots \bmod 8$

(Ceci est pratiquement équivalent à l'énoncé précédent).

1^e^ problème (résolu par Hatada)
complété par Haberland & Paper.

Montrer que si λ_p est une valeur propre de T_p ($p \neq 2$) pour une forme modulaire parabolique de poids k (de niveau 1).

alors $\lambda_p \equiv 0 \mod 2$

($\Leftarrow$) $\frac{\lambda_p}{2}$ est un entier algébrique)

$\lambda^N + a_1\lambda^{N-1} + \dots + a_N = 0 \Rightarrow 2 | a_i$

Pb $\leftrightarrow$ $2^i | a_i$.

Utilise l'isomorphisme d'Eichler-Shimura:

$V = H^1(\Gamma, \mathrm{Sym}^{k-2})$ $\qquad V_{\mathbb{Z}}$ réseau naturel

$T_p/2$ laisse stable le réseau (+ ou −)

Rque: Le réseau des formes à coeff entiers n'est justement pas stable !

2^e^ problème

Formules donnant explicitement $T_p \Delta^i$ mod 2.

$T_p \Delta = 0$ $\qquad$ mod 2

$T_p \Delta^2 = 0$

$$T_p \Delta^3 = \begin{cases} 0 & \text{si } p \not\equiv 3 \mod 8 \\ \Delta & \text{si } p \equiv 3 \mod 8 \end{cases}$$

$T_p \Delta^5$ aussi (on utilise la décomp binaire de 3 ou 5 qui n'a que 2 chiffres)

Les coefficients de $\Delta^i | T_p$ dépendent Frobeniennement de p (ie il existe une extension $E/\mathbb{Q}$, finie, non ram en 2 tel que les coeff de $\Delta^i | T_p$ ne dep que du Frob p dans $\mathrm{Gal}(E_i/\mathbb{Q})$).

Serre

7/12/87

99

Lien entre formes mod p et quaternions

N niveau ≥ 3 quelconque

$X(N)$ en car. première à N

$\varphi(N)$ composantes connexes $\underline{\omega}$

$$M_k = H^0(X(N), \underline{\omega}^{\otimes k})$$

Deligne - Rappoport, p. 275 - 282

$$\varphi(N) = N \prod_{p \mid N} \left(1 - \frac{1}{p}\right)$$

$$s_N = |SL_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)$$

$$m_N = |GL_2(\mathbb{Z}/N\mathbb{Z})| = \varphi(N)\, s_N =$$

$$= N^4 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p}\right)$$

p_N = nombre de pointes de $X(N) = \dfrac{m_N}{2N}$

$GL_2(\mathbb{Z}/N\mathbb{Z}) = G_N$ $\quad \pm\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

d_N = degré de $\underline{\omega}$ sur une composante

$$= \frac{s_N}{24}$$

g_N = genre de chaque composante =

$$= 1 + s_N \left(\frac{1}{24} - \frac{1}{4N}\right)$$

dim M_k sur chaque composante, $k \geq 2$

dim $H^0(\text{comp.}\ \underline{w}^{\otimes k})$

$$= (k-1)\frac{s_N}{24} + \frac{s_N}{4N}$$

$$\dim M_k = (k-1)\frac{m_N}{24} + \frac{m_N}{4N}.$$

$w^{\otimes 2} = \Omega^1$ (pôles simples aux pointes)

Kodaira - Spencer

$$f \longmapsto \underset{\substack{\uparrow \\ (2\pi i)\ ?}}{\ } f(z)\, dz \ .$$

Katz, LN 350

Isomorphisme de Kodaira - Spencer

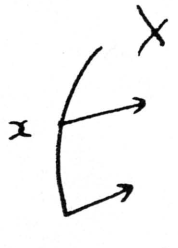
X lisse, projective $/k$

déformation sur $k[\varepsilon]$

$$\begin{array}{ccc} X_\varepsilon & & \text{plat} \\ | & & X_\varepsilon/\varepsilon=0 = X \\ k[\varepsilon] & & \end{array}$$

$X_\varepsilon \iff$ espace fibré principal homogène sous T_X = fibré tg à X

(isom. unique près)



$$0 \to T_X \to T_{X_\varepsilon} \to 1 \to 0$$

dual: $0 \to \mathcal{O}_X \to \mathcal{V} \to \Omega^1 \to 0$

fonction sur $X_{\mathcal{E}} = (f, v)$ f section de $\mathcal{O}$
v " " $\mathcal{V}$

$df = \alpha(v)$.

loc. libre

$$0 \to \mathcal{A} \to \mathcal{E} \to \mathcal{B} \to 0$$

$$\mathrm{Ext}(\mathcal{B}, \mathcal{A}) \simeq H^1(X, \mathcal{H}om(\mathcal{B}, \mathcal{A}))$$

$$0 \to \mathcal{H}om(\mathcal{B}, \mathcal{A}) \to \mathcal{H}om(\mathcal{E}, \mathcal{A}) \to \underset{\substack{\psi \\ 1}}{\mathcal{H}om(\mathcal{A}, \mathcal{A})} -$$

$\partial 1 \in H^1(X, -)$ donne isom.

autre choix d'isom :

$$0 \to \mathcal{H}om(\mathcal{B}, \mathcal{A}) \to \mathcal{H}om(\mathcal{B}, \mathcal{E}) \to \underset{\substack{\psi \\ 1}}{\mathcal{H}om(\mathcal{B}, \mathcal{B})}$$

$\partial 1 \in H^1(X, -)$

ces isom. sont opposés l'un de l'autre.

D'où problème de signe.

On obtient

$$\text{Tgt à la base} \xrightarrow{KS} H^1(X, T_X)$$

$X = E$ courbe elliptique

alors T_E est trivial

$$H^1(E, T_E) = H^1(E, \mathcal{O}) \otimes t_E \simeq t_E^{\otimes 2}$$

$$\underset{t_E}{\wr\wr}$$

$\mathrm{tgt}_{\text{para}} \to tg_E^{\otimes 2}$

$\Omega^1 \to \omega^2$.

car p $\quad N \geq 3, \quad p \nmid N$

$$0 \to \mathcal{M}_{k-(p-1)} \xrightarrow{A} \mathcal{M}_k \to \mathcal{S}_k \to 0$$

$$\mathcal{M}_{k-(p-1)} = \underline{\omega}^{\otimes k-(p-1)}, \qquad \mathcal{M}_k = \underline{\omega}^{\otimes k}$$

faisceaux sur $X(N)$

A forme de poids $p-1$ donné par l'invariant de Hasse.

$A \in H^0(\mathcal{M}_{p-1}) = M_{p-1}$

$$\left.\begin{array}{ll} p=2 & \text{"}a_1\text{"} \\ p=3 & \text{"}b_2\text{"} \\ p\geq 5 & E_{p-1} \end{array}\right\} = A$$

zéros de A : simples et correspondent aux points supersinguliers

$(E, \alpha_1, \alpha_2) \longmapsto \omega^k(E)$

α_1, α_2 base des points d'ordre N.

$$0 \to M_{k-(p-1)}(N) \xrightarrow{A} M_k \to S_k(N) \to$$

$$S_k(N) = H^0(X_s(N))$$

$$\to H^1(\mathcal{M}_{k-(p-1)}) \to H^1(\mathcal{M}_k) \to 0.$$

$$W_k(N) = M_k(N)/M_{k-(p-1)}(N)$$

$$0 \to W_k(N) \longrightarrow S_k(N) \to \text{dual de } W^{cusp}_{p+1-k}(N) \to$$

W^{cusp} = image dans W des formes modulaires

$$H^0(\ , \ \omega^{2}(cusp) \otimes \mathcal{M}_{p-1-k}) = H^0(\ , \mathcal{M}^{cusp}_{p+1-k})$$

dual de Coker $M_2^{cusp} \xrightarrow{A} M^{cusp}_{p+1-k}$

$$M^{cusp}_{2-k} = M^{cusp}_{p-1-k} \cap M_{2-k}$$

$$\mathcal{A} \xrightarrow{A} \mathcal{B} \qquad A \in H^0(\mathcal{H}om(\mathcal{A}, \mathcal{B}))$$

$$H^0(\mathcal{A}) \to H^0(\mathcal{B})$$

$$H^1(\mathcal{A}) \to H^1(\mathcal{B})$$

$$H^0(\Omega^1 \otimes \check{\mathcal{A}}) \longleftarrow H^0(\Omega^1 \otimes \check{\mathcal{B}})$$

$$\mathcal{H}om(\check{\mathcal{B}}, \check{\mathcal{A}}) = \mathcal{H}om(\mathcal{A}, \mathcal{B}).$$

$S_k(N)$ = espace des "formes modulaires de poids k sur les (E, α), E s.s., $\alpha = (\alpha_1, \alpha_2)$, base de $E(N)$"

$(E, \alpha) \longmapsto$ élé' de $\omega^{\otimes k}(E, \alpha)$

comp. aux isom.

(E, ω, α) E, ω forme diff. inv. sur E s.s $\neq 0$, rat. sur $\mathbb{F}_{p^2}$

α base de $E(N)$

$f \in S_k(N)$

$$(E, \omega, \alpha) \longmapsto f(E, \omega, \alpha) \in \mathbb{F}$$

$$f(E, \lambda\omega, \alpha) = \lambda^{-k} f(E, \omega, \alpha) \quad , \lambda \in \mathbb{F}_{p^2}^*$$

$\mathbb{F}$ corps de base (car. p), $\mathbb{F} \supset \mathbb{F}_{p^2}$

$f\,\omega^{\otimes k}$

E structure sur $\mathbb{F}_{p^2}$, Frob. $= -p$

S_k ne dépend que de $k \bmod (p^2-1)$

$$S_k(N) \xrightarrow{\sim} S_{k+p^2-1}(N)$$

isom. canonique

$$S_k[1] \simeq S_{k+p+1}$$

forme canonique Γ de poids $p+1$

$$\Gamma \quad \begin{array}{ll} a_3 & p = 2 \\ -b_4 & p = 3 \\ -\dfrac{E_{p+1}}{12} & p \geq 5 . \end{array}$$

$$S(N) = \bigoplus_{k \bmod (p^2-1)} S_k(N)$$

$$S = \varinjlim_{(N,p)=1} S(N)$$

$$S_k(N) \to S_k(NM)$$

Quaternions

D alg. de quat. sur $\mathbb{Q}$ ramifiée en $\{p, \infty\}$ et pas ailleurs.

$D_{\mathbb{Z}}$ = ordre maximal de D.

$D_{\mathbb{Z}} \otimes \mathbb{Z}_p$ = l'ordre maximal d'un corps de quaternions $/\mathbb{Q}_p$

$$D_{\mathbb{Z}} \otimes \mathbb{Z}_\ell \simeq M_2(\mathbb{Z}_\ell)$$

G = groupe mult. de D, groupe alg. $/\mathbb{Q}$

Λ $\mathbb{Q}$-alg. comm.,

$G(\Lambda) = (D \otimes_{\mathbb{Q}} \Lambda)^\times$

$\mathbb{A}$: adèles de $\mathbb{Q}$

$\mathbb{A}_f$: adèles finies

$G(\mathbb{A}) = G_{\mathbb{A}}$: pts de G ds $\mathbb{A}$

$$= \prod_v G(\mathbb{Q}_v) = G(\mathbb{A}_f) \times G(\mathbb{R})$$

(produit restreint)

$$G(\mathbb{A}_f) = \prod_\ell G(\mathbb{Q}_\ell)$$

$$G(\mathbb{A}) \supset G(\mathbb{Q}) \quad \text{s/g discret}$$

$$U \backslash G(\mathbb{A}) / G(\mathbb{Q})$$

U ouvert s/g.

$$G(\mathbb{A})/G(\mathbb{Q})G(\mathbb{R}) \quad \text{compact}$$

$$G(\mathbb{A}_f) = G(\mathbb{Q}_p) \times \prod_{\ell \neq p} G(\mathbb{Q}_\ell)$$

$$GL_2(\mathbb{Z}_\ell)$$

$$D_p = D \otimes_{\mathbb{Q}} \mathbb{Q}_p \qquad \text{valuation}$$

$\mathcal{O}_p$ ~~$\mathcal{O}_p$~~ = entiers de D_p

π unif. $\quad \mathcal{O}_p / \pi \mathcal{O}_p \cong \mathbb{F}_{p^2}$

$$D_p^\times \supset \mathcal{O}_p^\times \supset \cdots \supset \mathcal{O}_p^{\times, m}$$

$$\mathcal{O}_p^{\times, m} = \{ u \mid u \in \mathcal{O}_p^\times, \ u \equiv 1 \mod \pi^m \}$$

$$1 \longrightarrow \mathcal{O}_p^{\times, 1} \longrightarrow \mathcal{O}_p^\times \longrightarrow \mathbb{F}_{p^2}^\times \longrightarrow 1.$$

<u>Th</u> : "Il y a ~~des~~ isomorphismes" entre $S = \lim S(N)$ et l'espace des fonctions localement constantes sur $G_{\mathbb{A}}/G_{\mathbb{Q}}$ invariantes à gauche par $\mathcal{O}_p^{\times, 1}$

Enoncé avec N précisé : $N = \prod_{\ell \in L} \ell^{n_\ell}$

même énoncé avec f invariant par

$$\mathcal{O}_p^{\times,1} \times \prod_{\ell \notin L} GL_2(\mathbb{Z}_\ell) \times \prod_{\ell \in L} \{s/g \text{ de } GL_2(\mathbb{Z}$$

formé des élé' $\equiv 1$ (ℓ

ouvert dans G_{A_f}

$S(N)$ = fcts localement constantes sur $G_A / G_\mathbb{Q}$ invariantes par $\uparrow$.

(Deligne, LN 349 pas de

On choisit

une courbe ss E_0 sur $\mathbb{F}_{p^2}$ avec Frob $= -p$

on choisit une forme diff. $\omega \neq 0$, rat.

$\mathbb{F}_{p^2} = \mathbb{F}_{p^2}(\mathbb{F})$.

pour tout N premier à p, α^N base des points de div. par N (de façon compatible)

$D = \operatorname{End} E_0 \otimes \mathbb{Q}$, $D_\mathbb{Z} = \operatorname{End} E_0$

$\operatorname{End} E_0 \longrightarrow \mathbb{F}$ (action par esp. tg)

$\mathcal{O}_p = \operatorname{End} E_0 \otimes \mathbb{Z}_p$

$D_p /$

E_0 = courbe de référence

Bijection (canonique) entre

classes d'isom. (E, ω, α) $\Longleftrightarrow$ $U(N) \backslash G_A / G_\mathbb{Q}$

α base mod N

$$U(N) = O_p^{\times,1} \times \prod_{\ell \nmid N} D^{\times}_{\mathbb{Z}_\ell} \times \prod_{\ell \mid N} D^{\times, n_\ell}_{\mathbb{Z}_\ell} \times G_{\mathbb{R}}$$

Classes ~~d'idéaux~~ de modules à gauche proj. de rang 1 sur $D_{\mathbb{Z}}$ munis de bases mod$(\mathfrak{p}N)$

$\mathfrak{p} = (\pi)$: idéal max$^{\ell}$ au dessus de p de $D_{\mathbb{Z}}$

$= \mathrm{Ker}\ D_{\mathbb{Z}} \to \mathbb{F}_{p^2}$

$D_{\mathbb{Z}} / \mathfrak{p} D_{\mathbb{Z}} \simeq \mathbb{F}_{p^2}$

$I / \mathfrak{p} I = \mathbb{F}_{p^2}$ - ev. de dim 1.

I/NI = module libre de rang 1 sur $\mathrm{End}_{\mathbb{Z}}/N \simeq M_2(\mathbb{Z}/N\mathbb{Z})$

$\updownarrow$

$U(N) \backslash G_{\mathbb{A}} / G_{\mathbb{Q}}$

C/L $\quad L' \supset_{\ell} L \quad E \xrightarrow[\ell]{\pi} E'$ $\quad \varepsilon \neq 1$

fixé $\quad$ Koblitz

$(E, \omega, \alpha) \longmapsto (I, i_p, i_N)$ $\quad i_p$ base mod p

i_N base mod N.

$D_{\mathbb{Z}} = \mathrm{End}\, E_0$

$I = \mathrm{Hom}_{\mathbb{F}}(E, E_0)$.

$i_p \in I/\pi I = \mathrm{Hom}(tg\, E, tg\, E_0) \cong \mathbb{F}$ par choix des bases

$i_p^*(\omega_0) = \omega$. $\quad I/NI \simeq \mathrm{Hom}(E_N, E_{0N})$ $\quad i_N(\alpha) = \alpha_0$

Formes modulaires (mod p)

Fonctions sur $D_{\mathbb{A}}^{\times}/D_{\mathbb{Q}}^{\times}$ à valeurs mod p

D alg. de quat. $/\mathbb{Q}$, ramifiée en (∞, p)

choix E_0, s.s. sur $\mathbb{F}_{p^2} \subset \overline{\mathbb{F}}$, Frob. $-p$

base de l'espace tgt w_0

bases de $E_0[N]$ compatibles entre elles $(p \nmid N)$

Dieud(E_0) module libre de rang 2 sur $W(\mathbb{F}_{p^2})$,

V, F semi-linéaires, $V = -F$, $FV = p$.

$\Lambda = \{W(\mathbb{F}_{p^2}), F\} \simeq F\lambda = \lambda^{\sigma} F$, $F^2 = -p$

module de D. du groupe formel

$$T_p E_0 / F T_p E_0 \simeq \text{tgt } E_0 .$$

(E, w, α) $\quad w$ base de l'espace tgt

E s.s., α base de $E[N]$

$d(E, w, \alpha) \Longleftrightarrow U(N)\backslash D_{\mathbb{A}}^{\times}/D_{\mathbb{Q}}^{\times}$

classes de modules projectifs à gauche de rang 1, muni de base mod $\wp N$

$D_{\mathbb{Z}} = \operatorname{End} E_0$; $D = \mathbb{Q} \otimes D_{\mathbb{Z}}$

$\wp$ idéal maximal de $D_{\mathbb{Z}}$, $D_{\mathbb{Z}}/\wp \simeq \mathbb{F}_{p^2}$

$(E, w, \alpha) \longmapsto I = \operatorname{Hom}(E, E_0)$

$i_{\wp}, i_N$ bases mod $\wp, N$

$i_{\wp}^{*} w_0 = w$, $i_N \alpha = \alpha_0$

idèle $g_v \longmapsto$ l'unique idéal de $D_{\mathbb{Q}}$ dont les localisés sont les $(D_{\mathbb{Z}})_v\, g_v$

Théorème :

Ces flèches définissent des bijections

$$V(N) = \prod_p O_p^{\times,1} \times \prod_{\ell \neq p} (\text{groupe de congr. mod } N) \times G_{\mathbb{R}\,\infty}$$

Flèche courbes s.s. $\longrightarrow$ modules proj. de rg 1

(1) $I = \mathrm{Hom}(E, E_0)$: $I \neq 0$ (et est un module proj. de rg 1

(2) On peut reconstruire E à partir de I

$I \neq 0 \iff$ 2 courbes s.s. sont isogènes

I module proj. de rg 1 $\longmapsto E^I = \mathrm{Hom}_{D_{\mathbb{Z}}}(I, E_0)$

$\mathcal{C}$ catégorie abélienne

$C \in \mathrm{ob}\,\mathcal{C}$, $R \to \mathrm{End}(C)$

M R-module de pr. finie

"$\mathrm{Hom}_R(M, C)$" $\in \mathrm{ob}\,\mathcal{C}$ $= C^M$

$M = R \implies C^R = C$

$M = R^n$ $\quad C^{R^n} = C \times \cdots \times C$ $\quad n$ fois

$$R^m \to R^n \longrightarrow M \to 0$$

$$C^m \leftarrow C^n \leftarrow C^M \leftarrow 0$$

$$\mathrm{Hom}(C', C^M) = \mathrm{Hom}_R(M, \mathrm{Hom}(C', C))$$

E_0, module proj $\longrightarrow$ courbes s. s.

calculé par Eichler $\sim \frac{p-1}{12}$ — nbre de j $\sim \frac{p-1}{12}$

Deuring : Hamb. Abh. 1941

Thm de Tate :

A, B / c fini :

$T_\ell A \xrightarrow[\text{hom}]{} T_\ell B$ — commute à l'action du groupe de Galois

$$\mathrm{Hom}_{Gal}(T_\ell A, T_\ell B) \cong \mathbb{Z}_\ell \otimes \mathrm{Hom}(A, B).$$

$\ell \neq$ car

E, E_0 non isogènes ?

$A = E \times E_0$ — s/esp. tot. isotr. Λ_ℓ

$\ell, \ell \quad \ell, \ell$ — A/Λ_ℓ a pol. de d^o 1.

"

Jacobienne d'une courbe de genre 2

E, E_0 il existe une isogénie

$$E \xrightarrow{\varphi} E_0$$

d^o ? Si ℓ nbre premier donné, $\ell \neq p$ il existe une isogénie $E \to E_0$ de degré une puissance de ℓ.

$D_{\mathbb{Z}}[\frac{1}{\ell}]$ a nombre de classes 1.

Eichler - Kneser :

k corps de nombres, G abs. simple, simpl. convexe $/k$. v place, G_v pas compact

$$G_A \supset G_k \cdot G_{k_v} \quad , \text{ dense}$$

$$A'_v = \prod_{w \neq v} k_w$$

(autre façon de trouver le degré :

E, E_0 $\quad \theta_{E,E_0} = \sum_{\varphi : E \to E_0} q^{\deg \varphi}$

à 4 variables

$p = 2$ $\quad E = E_0$

$D_{\mathbb{Z}}$ = quat. entiers : $a + bi + cj + dk$

$a, b, c, d \in \mathbb{Z}$

ou $\quad \in \frac{1}{2} + \mathbb{Z}$

$$\theta_{E,E} = \sum_{a,b,c,d} q^{a^2+b^2+c^2+d^2}$$

forme modulaire de poids 2 sur $\Gamma_0(p)$)

$$\theta_{E,E_0} = 1 + \cdots$$

Problème sur les θ_{E,E_0} :

mod p : θ_{E,E_0} est une forme mod de niveau 1, de poids $k = p+1$.

$$\vartheta_{E,E_0}(E') \in \omega^{p+1}(E')$$

$$\vartheta_{E,E_0}(E')/B(E') \in \mathbb{F}_{p^2}.$$

calcul de $\uparrow$?

(B : dérivée de l'invariant de Hasse)

$I \neq 0$:

$E \qquad E_0^I = \mathrm{Hom}_{D_{\mathbb{Z}}}(I, E_0)$

Thm

$$E \xrightarrow{\sim} \mathrm{Hom}_{D_{\mathbb{Z}}}(\mathrm{Hom}(E, E_0), E_0)$$

$$I/NI \xrightarrow{\sim} \mathrm{Hom}(E[N], E_0[N])$$

sur le thm de Tate.

$$I/pI \cong \mathrm{Hom}_{\mathbb{F}_{p^2}}(tg\, E, tg\, E_0).$$

il faut montrer : il existe $\varphi \in I = \mathrm{Hom}(E, E_0)$ qui est séparable.

On choisit $\varphi : E \to E_0$ donné, s'il est inséparable, degré d'insép m

Si $m \geq 2$, φ se factorise par $\mathrm{Frob}/\mathbb{F}_{p^2}$.

$$\begin{tikzcd} E \arrow[r, "\mathrm{Frob}"', "\underset{p}{\shortparallel}"] \arrow[rr, bend right, "\varphi"'] & E \arrow[r] & E_0 \end{tikzcd}$$

$\mathrm{End}\, E_0 = D_{\mathbb{Z}} \qquad \pi$ avec $v(\pi) = 1$

Formes modulaires — fonctions sur $G_{\mathbb{A}}/G_{\mathbb{Q}}$

$G = D^*$

$S_k[N]$ poids k sur les c.s.s. α — $f(E, \omega, \alpha)$;

$||$ — $f(E, \lambda\omega, \alpha) = \lambda^{-k} f(E, \omega, \alpha)$

$M_k[N] / M_{k-(p-1)}[N]$ — $\lambda \in \mathbb{F}_{p^2}^*$

$k \geq p+1$

$f \rightsquigarrow F$ sur $G_{\mathbb{A}}/G_{\mathbb{Q}}$ invariante par $G_{\mathbb{R}}$; le groupe des unités $\equiv 1 \bmod$

inv. par $O_p^{\times, 1}$ = inv. par $U(N)$

$$O_p^\times / O_p^{\times, 1} \cong \mathbb{F}_{p^2}^*$$

Si $\lambda \in O_p^\times$, λ identifié à un élé de $G_{\mathbb{A}}$

$$F(\lambda_? \cdot x) = \tilde{\lambda}^{-k} F(x).$$

$$f \Longleftrightarrow F$$

Bijection $f \Longleftrightarrow F$ est compatible avec les opérateurs de Hecke T_ℓ, $\ell \nmid pN$ à condition d'utiliser, du côté $G_{\mathbb{A}}$, les op.

$\frac{1}{\ell} T_\ell^{\text{nat}}$

$f \in S_k[N]$, $f' = f | T_\ell$ $\Longleftrightarrow F$, $\Longleftrightarrow F'$, alors $F' = \frac{1}{\ell} F | T_\ell$

Rappel : T_ℓ^{nat} ds le langage de $G_{\mathbb{A}}$:

$GL_2(\mathbb{Q}_\ell)$ module V à droite

$v \in V$ invariant par $GL_2(\mathbb{Z}_\ell)$

on définit $v | T_\ell^{nat} = \sum v \cdot g$

$g \in GL_2(\mathbb{Q}_\ell)$

g coeff. $\in \mathbb{Z}_\ell$

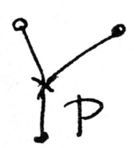
$\det g = \ell$

g mod $GL_2(\mathbb{Z}_\ell)$

$D_\ell^\times = GL_2(\mathbb{Q}_\ell)$

$\mathcal{O}_\ell^\times = GL_2(\mathbb{Z}_\ell)$.

si centre opérait trivialement :



somme sur les voisins

anneau de Hecke attaché à (G, H)

Hecke (G, H) = alg. des doubles classes

$= \mathrm{End}_G(\mathbb{Z}[G/H])$.

$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$.

$E \xrightarrow[\ell]{} E'$ isogénie de d° ℓ.

$I \underset{\ell}{\supset} I'$

$g \in G_{\mathbb{A}}$, F $G_{\mathbb{A}} / G_{\mathbb{Q}}$

$F \cdot g(x) = F(gx)$.

Correspondance avec les repr. gal.

f pds k, niveau N, valeur pr. T_ℓ, $\ell \nmid pN$

$$f \mid T_\ell = a_\ell f$$

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{F}^*$$

f a ε pour caractère central

$$f(E, \omega, n\alpha) = \varepsilon(n)\, f(E, \omega, \alpha) \qquad (n, N) = 1.$$

A f correspond une repr. semi-simple

$$\rho_f : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}) \quad , \quad D_\ell^* \simeq GL_2(\mathbb{Q}_\ell)$$

non ramifiée en dehors de pN

$$\mathrm{Tr}\, \rho_f\, (\mathrm{Frob}_\ell) = a_\ell \qquad \ell \nmid pN$$

$$\det \rho_f\, (\mathrm{Frob}_\ell) = \ell^{k-1} \varepsilon(\ell)$$

Pas de bonne référence. Pour niveau 1 :
Deligne, sém. Bourbaki
(Séminaire IHES : non publié)
Carayol, Ann ENS. langage repr.
pour les formes paraboliques.
Pour les séries d'Eisenstein, se vérifie directement.
Pour les repr. mod p : passer sur $\Gamma_0(p)$, en pds 2

$\Gamma_1(N)$ $\quad f(E, \omega, \alpha_1, \alpha_2)$

par une petite opération pas compliquée, cela entraîne l'existence pour $\Gamma_0(p)$.
Hida Invent. 63/64.

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{F}^*$$

$$\varepsilon_{Gal} : G_{\mathbb{Q}} \longrightarrow \mathbb{F}^*$$

$$\varepsilon_{Gal}(\mathrm{Frob}_\ell) = \varepsilon(\ell) \quad \text{si } \ell \nmid N$$

$$\varepsilon_{\mathbb{A}} : \mathbb{A}^*/\mathbb{Q}^* \longrightarrow \mathbb{F}^*$$ par corps de classes.

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \hookrightarrow \mathbb{F}^*$$

$$\det(\rho_f) = \chi_{Gal}^{k-1}\, \varepsilon_{Gal}$$

$$\varepsilon_{\mathbb{A}}(1, \dots, 1, \ell, 1, \dots, 1) = \varepsilon(\ell)$$

ℓ mod p.

F sur $G_{\mathbb{A}}/G_{\mathbb{Q}}$, constante mod $U(N)$

de poids k

fct propre des T_ℓ, $\ell \nmid pN$

$$T_\ell = \frac{1}{\ell}\, T_\ell^{nat}$$

valeur propre $a_\ell = \frac{1}{\ell}\, a_\ell^{nat}$

F car. central $\chi_{\mathbb{A}}^k\, \varepsilon_{\mathbb{A}} = \psi_{\mathbb{A}}$

$$F(gx) = \psi_{\mathbb{A}}(g)\, F(x) \quad \forall g \in \text{centre } D_{\mathbb{A}}^\times = \mathbb{A}$$

$\rho_F = \rho_f$, $\mathrm{Tr}\, \rho_F(\mathrm{Frob}_\ell) = a_\ell$, $\ell \nmid pN$

Deligne: "corr de Hecke" (ou de Tate).

$$(\det \rho_F)_{\mathbb{A}} = \psi_{\mathbb{A}} \cdot \chi_{\mathbb{A}}^{-1}.$$

$$\rho_F^{nat} = \chi \otimes \rho_F$$

$$\det = \Psi_A \cdot \chi_A$$

<u>Tous</u> les systèmes de valeurs propres des op. de Hecke sur $G_A/G_{\mathbb{Q}}$ (pour les fct. loc. ctes) proviennent de ceux obtenus à partir des formes modulaires mod p.

F loc. cte sur $G_A/G_{\mathbb{Q}}$.

fixée par s/g ouvert

$U = O_p^{\times, m} \times \{$groupe de congruence mod $N\}$.

Inversément, les fct invariantes par U (loc. c sur $G_A/G_{\mathbb{Q}}$ forment un ev. de dim finie avec action du centre et des T_ℓ.

$m \geq 1$ se ramène à $m = 1$.

V espace des f inv. par $O_p^{\times, m}$ et groupes de congruence mod N.

$V' =$ s/esp. propre de V corr. à un système de valeurs propres des op. de Hecke et un car. du centre.

Alors, si $V' \neq 0$, V' contient $F \neq 0$, inv. par $O_p^{\times, 1}$.

$O_p^{\times, 1} / O_p^{\times, m}$ est un p-groupe.

(donc fixe un vecteur).

Commentaires et critiques :

1.) Autre façon de faire (à vérifier)

fcts loc. ctes (en car 0) sur $G_{\mathbb{A}}/G_{\mathbb{Q}}$.

$/\mathbb{C}$

dictionnaire de Jacquet-Langlands :

formes modulaires de poids 2 sur $\Gamma_0(p^\infty; N)$

(ne donne pas de construction).

comparer les 2 points de vue :

problème sur $\theta_{E,E'}$ évoqué précédemment

2.) Critique :

Traduction quaternionienne des

$$S_k[N] = \text{fct sur } G_{\mathbb{A}}/G_{\mathbb{Q}}$$

$\cup$ sous-espace

$W_k[N]$ $\qquad 1 \leq k < p+1$

construire en termes de quaternions

$W_k[N]$.

3.) Autre critique :

Sur $\Gamma_0(N)$, il y a un opérateur T_p

$(p = p\,!)$

$$\sum a_n q^n \longmapsto \sum a_{np} q^n + p^{k-1} \varepsilon(p) \sum a_{n/p} q^n$$

$k \geq 2$ $\qquad T_p = U_p \qquad \sum a_n q^n \mapsto \sum a_n q^n$

$k = 1$: non

Gross : $M_1 \hookrightarrow M_p$ – U_p agit pas compatible

T_p agit

Sur $S_p \supset M_p / M_1$, rien de raisonnable n'opère.

Sur $W_k \subset S_k$ $\quad 2 \le k \le p-1$

on a opérateurs U, mais pas de définition quaternionienne.

$U(M_k) \subset M_{k-(p-1)}$

En janvier: $\quad G_A / G_{\mathbb{Q}}$

Fonct loc. ctes $(G_A / G_{\mathbb{Q}})$ contient très peu de sous-modules simples (seulement de dim 1).

$GL_2(\mathbb{Q}_\ell)$ en car $p \neq \ell$

(Marie-France Vignéras).

Serre, 18 jan. 88

$G = GL_2(K)$ $\qquad$ K corps local à corps résiduel k fini

π uniformisante

v valuation

$q_k = |k|$, $p_k = \operatorname{car} k$

Corps "des valeurs" F, $\operatorname{car} F = p_F$

provisoirement, pas d'hypothèse sur p_K.

Dans la suite, $K = \mathbb{Q}_\ell$, $F = \overline{\mathbb{F}}_p$.

Repr. de G dans un ev. sur F

V ev. sur F sur lequel opère G à gauche.

Hyp : ① action de G continue pour top. discr. de G i.e. le fixateur ds G de tout $v \in V$ est ouvert

② Admissibilité : Pour tout s/g ouvert U de G, le sous-espace V^U des invariants de U dans V est de dim. finie.

A cause de ①, $V = \bigcup_U V^U$.

② $H^0(U, V)$ de dim finie (U ouvert compact)

si $p_k = p_F$, il n'est pas clair que

$\dim H^i(U, V) < \infty$

On veut étudier des modules de la "série principale".

$G = GL_2(K)$, O_K = anneau des entiers de K

$G_0 = GL_2(O_K)$ compact maximal standard

Couple : V repr. de G, $v \in V$ invariant par G_0.

$v \in V^{G_0}$ action des opérateurs de Hecke et de centre $G = \{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \}$.

<u>Hypothèse sur V :</u>

1.) Le centre de G opère trivialement sur V (repr. de PGL_2).

2.) $Tv = av$, $a \in F$

Rappel sur les opérateurs de Hecke :

$$Tv = \sum_{i=0}^{i=q_k} g_i v ,$$

où $g_i \in GL_2(K) = G$, $g_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$

coef. $\in O_K$. $\det g_i = \pi$,

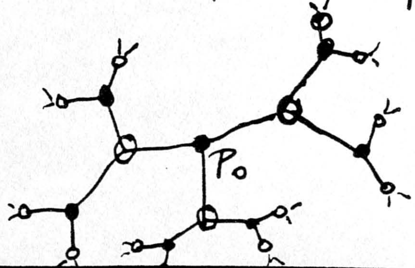
représentants mod. G_0 à droite.

Arbre de G :

Sommets : classes d'équivalence (homothétie près de réseaux

Arêtes : proviennent de $L \supset L'$, $\ell_{O_K}(L/L') = 1$

$[L : L'] = q_k$



$\{ g_i P_0 \}$ = les sommets voisins.

Module universel relatif à a : H_a

$H_a = C_0$: 0-chaînes à coeff $\in F$ finies sur l'arbre X $/ (T-a) C_0$

T : opérateur (de Hecke) sur C_0 : applique un sommet sur la somme des voisins

$H_a := C_0 / (T-a) C_0$, G-module.

admissible si $p_k \neq p_F$, ou si $a \neq 0, 1, -1$.

P_0 est invariant par G_0.

PGL_2 opère sur l'arbre

$T(P_0) = a P_0$

H_a est universel : v, V sat. ① et ②

il existe un unique homomorphisme

$$H_a \to V$$
$$P_0 \mapsto v$$

$$H_a \otimes V^{G_0} \longrightarrow V$$

Situation générale :

G groupe, H s/g de G, V G-module

$R(G, H)$: commutant de la repr. de G dans $F[G/H]$

$R(G, H)$ alg. de Hecke de G rel. à H.

On a un G-hom. canonique

$$F[G/H] \otimes_{R(G,H)} V^H \longrightarrow V$$

$\left(C_0 \otimes V^H \longrightarrow V \right.$: on aboutit à ce qui est au-dessus$)$

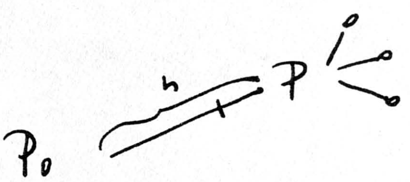
(A. Borel, Inv. 1976).

$$0 \longrightarrow C_0 \xrightarrow{T-a} C_0 \longrightarrow H_a \longrightarrow 0 \qquad \text{exacte}$$

c 0-chaine, $c \in C_0$ $\quad c \neq 0$

distance à P_0: $\quad d(P_0, c) = \sup\{d(P_0, P)\}$
$\qquad\qquad \overset{\shortparallel}{d(c)} \qquad\qquad P$ à coef $\neq 0$

<u>Lemme:</u> $\quad d((T-a)c) = d(c) + 1$.



$$H_a = C_0/(T-a)C_0, \quad a \in F$$

Supposons $p_K \neq p_F$.

Alors : H_a est admissible, et

$$\dim H_a^{G_0} = 1.$$

1.) Si $a \neq \pm(q_k + 1)$ dans F,
alors H_a est irréductible,
et isomorphe à un certain module induit I_λ (à définir).

2.) Si $a = q+1$ et $q+1 \neq 0$ ds F, alors

C_0^0 = 0-chaînes à somme des coef. 0

$C_0 \supset C_0^0 \supset (T-\alpha)C_0$ si $\alpha = q+1$ ds F

$(\deg (T-\alpha)P = 0$? $)$

alors $H_\alpha \supset H_\alpha^0$ hyperplan :

$$H_\alpha^0 = C_0^0/(T-\alpha)C_0$$

$$0 \longrightarrow H_\alpha^0 \longrightarrow H_\alpha \longrightarrow \underline{1} \longrightarrow 0$$

H_α^0 irréductible $\cong St$

suite exacte non scindée

2') Si $\alpha = -(q+1)$, $q+1 \neq 0$ ds F

$H_\alpha = \varepsilon \otimes H_{q+1}$ où ε rep. de d° 1

$\varepsilon\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$ si $v(ad-bc) \equiv 0\ (2)$

-1 sinon.

$H^0_{-(q+1)}$ est l'image des chaînes de somme alternée 0.

Cas 3.) : $\alpha = 0 = q+1$ ds F $(q = q_k)$

$(p_F \mid q+1)$

$C_0 \supset C_0^{0,0}$ = 0-chaînes à somme des coeff. 0 à la fois sur les bleus et les rouges.

$C_0^{00} \supset T\,C_0$ (car $q+1=0$)

$$H_\alpha^{00} := C_0^{00}/T\,C_0$$

ste exacte : $(\alpha = 0,\ p_F \mid q+1)$

$$0 \to H_\alpha^{00} \to H_\alpha \to r_2 \to 0$$

$G \xrightarrow{\varepsilon}$ groupe d'ordre 2

$r_2 \simeq \underline{1} \oplus \varepsilon$ si $p_F \neq 2$

$0 \to \underline{1} \to r_2 \to \underline{1} \to 0$ si $p_F = 2$

$H_\alpha^{0,0}$ est irréductible, tout sous G-module de H_α, $\neq 0$, le contient.

Dans le cas $\alpha = 0 = q+1$ ds F, $p_F \neq 2$, H_α possède 2 quotients irréductibles distincts, à savoir $\underline{1}$, $\underline{\varepsilon}$.

Dans tout autre cas, H_α possède un seul quotient irréductible (de dim 1 si et seulement si $\alpha = \pm(q+1)$).

$PGL_2 \subset \mathrm{Aut}\,X$ $\overline{\text{agit}}$, tous les modules ont une action de $\mathrm{Aut}\,X$ (c'est parce qu'ils sont dans la série principale).

Si $p_K = 0$ et $p_k = p_F$, alors

$H^0(U,V)$ de dim. finie $\Rightarrow H^1(U,V)$ aussi.

$G_0 = GL_2(O_K)/\text{centre} \subset G = PGL_2$

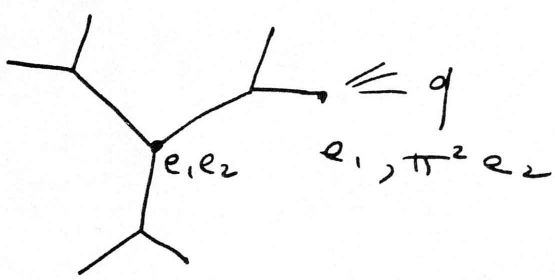
G_n = s/g de congruence

$= \{ s \in G_0 \mid s \equiv 1 \mod \pi^n \}$, $n \geq 1$

G_n fixe les sommets de l'arbre de dist. $\leq n$ de P_0.

$G_n \subset PGL_2$ est le fixateur de ces sommets.

G_n bouge les autres sommets



G_2 opère sur les q arrêtes par translation.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv 1 \pmod{\pi^2}$

e_1

$\downarrow$

$a e_1 + c\pi^{-2} e_2$

$$\begin{pmatrix} a & \pi^2 b \\ \pi^{-2} c & d \end{pmatrix}$$

mod π $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$

$C(n)$: ev. des chaînes c à distance au plus n de P_0.

$$(d(c) \leq n \text{ ou } c = 0)$$

$$C(0) \subset C(1) \subset \cdots$$

$$C(n-1) \xrightarrow{T-a} C(n)$$

$$H(a) = \bigcup_n C(n)/(T-a)C(n-1)$$

Proposition: Si $p_F \neq p_k$:

Les invariants de G_n dans H_a sont réduits à $C(n)/(T-a)C(n-1)$

Corollaire :

Les éléments de H_a fixés par G_0 sont les multiples de P_0.

Démonstration:

Pour $n \geq 1$. G_n est un pro-p_k-groupe, $p_F \neq p_k$. Les ~~...~~ éléments de H_a invariants par G_n sont les images des éléments de C_0.

G_1 fixe C_1.

G_n permute transitivement les sommets de X qui sont à distance fixée $m \geq n$ de P_0.

X_m : sommets de X à distance m de P_0

$(m \geq 1)$ $X_m \to X_{m-1}$ projection canonique vers P_0.

G_n permute transitivement les sommets $\in X_m$ qui ont même image ds X_n.

A démontrer : tout invariant de G_n ds $C(m)$, $m \geq n$, est congru mod$(T-\alpha)C_0$ à un inv. de G_n ds $C(n)$.

Ces invariants sont engendrés par les invariants élémentaires suivants : Si $Q \in X_n$, Soient P_α les éléments de X_m qui se projettent sur Q

$$C_Q^m = \Sigma P.$$

$$(T-\alpha)\, C_Q^{m-1} = C_Q^m + q\, C_Q^{m-2} - \alpha\, C_Q^{m-1}.$$

$n=0$: $V^{G_0} \subset V^{G_1}$

inv. de G_0/G_1 opérant sur V^{G_1}.

$V^{G_1} = 1 + r$ ds C_0, r = repr. de PGL_2 sur la droite projective

$$0 \to 1 \xrightarrow{T-\alpha} 1+r \to V^{G_1} \to 0$$

Si $\alpha \neq 0$, $V^{G_1} \simeq r$

Si $\alpha = 0$, $V^{G_1} \simeq 1 \oplus r/1$

<u>Lemme</u> : r contient une seule fois 1 et $r/1$ ne la contient pas.

<u>Lemme</u> : Soit G un groupe de permutations transitif sur un ens. $\Omega \neq \emptyset$.
Soit r la repr. de G ~~ds~~ dans les fct sur Ω (à val $\in F$)

(a) r contient 1 une seule fois

(b) Si G est 2 fois transitif,

$r/1$ ne contient pas 1 que si $p = 2$

et si $|\Omega| = 2$

f sur Ω, $gf - f$ constante pour tout g

$\Longrightarrow$ f est cte.

$|\Omega| \geq 3$ $\quad \cdot y \quad \cdot z \quad \dot{x}$ $\quad \exists\, g : x, y \mapsto x, z$

$\Longrightarrow f(y) = f(z)$.

Ω : droite proj. sur k

$|\Omega| = q_k + 1 \geq 3$

$PGL_2(k)$ est 2 (et même 3)-transitif.

$\dim H_a^{G_n} = (q+1)q^{n-1}$

$n \geq 1$

H_a, $a = q+1$,

$$0 \to H_a^0 \to H_a \xrightarrow[\text{des coef}]{\text{somme}} 1 \to 0$$

<u>Thm</u> $H_a^0 \simeq St$: repr. de Steinberg de G

St = Fonctions localement constantes sur $\mathbb{P}_1$ / ctes

$= H^1_c(X, F)$

Bouts de l'arbre

appartement : géodésique infinie ds les 2 sens

• Deux demi-géodésiques sont équivalents s'ils sont égaux sauf sur un compact.

Bout : classes d'équivalence

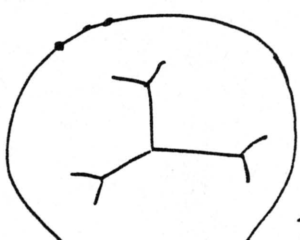
$X = \bigcup K_n \qquad K_n \subset K_{n+1}$ compacts

Espace des bouts $= \varprojlim$ (comp. connexes de $X - K_n$)

$$\text{Bouts } X = \varprojlim X_m$$

$$= \mathbb{P}_1(K).$$

$$X \subset \overline{X} = X \cup bX$$



$$0 \to \overbrace{H^0_c(X)}^{\substack{0 \\ \|}} \to \overbrace{H^0(\overline{X})}^{1} \to H^0(bX) \to$$

$$\to H^1_c(X) \to \underbrace{H^1(\overline{X})}_{\substack{\| \\ 0}}$$

$$H^1_c(X) \cong (\text{Fcts loc. ctes sur } \mathbb{P}^1) / (\text{fct ctes})$$

$$\cong \underline{St}.$$

Façon de faire plus terre à terre :

Fonction loc. cte sur bX

$= \begin{cases} \text{fct sur les sommets de } X \text{ définie} \\ \text{presque partout, et} \\ \text{presque constante :} \end{cases}$ $*$

C_0^∞ = ev. des chaînes de dim 0 à support qque

C_1^∞ : 1-chaînes

$* = \operatorname{Ker} : \left(C_0^\infty / C_0 \xrightarrow{\delta} C_1^\infty / C_1 \right)$

= fcts sur l'espace des bouts bX

$$0 \to C \to C^\infty \to C^\infty / C \to 0$$

$$0 \to \overbrace{H^0(C)}^{0} \to \overbrace{H^0(C^\infty)}^{1} \to \underbrace{H^0(C^\infty/C)}_{\text{fcts sur les bouts loc. ctes}} \to$$

$$\to \underbrace{H^1(C)}_{H^1_c(X)} \to 0$$

$H^0_{q-1} \cong St$ $\qquad C_1 \underset{\cong}{\xrightarrow{\partial}} C_0^0$

arbre contractile.

$C_0^0 / ((T - (q+1)) C_0)$

$\wr\wr$ S

Coker : $C_0 \longrightarrow C_1$

$x \longmapsto \cancel{\delta}(T - (q+1))x$

$H^1(X) = \operatorname{Coker}(C_0 \xrightarrow{\delta} C_1)$.

$$\delta = \partial^{-1} \circ (T - (q+1))$$

$$\partial \delta = T - (q+1) \qquad \text{sur } C_0$$

$$\delta P = \sum_{\text{ext.}(y) = P} y \quad ; \qquad \partial(\delta P) = (q+1)P - TP .$$

Th (Marie-France Vignéras).

1.) Si $p_F = p_k$, St est irréductible.

2.) Si $p_F \neq p_k$ et si $q+1 \neq 0$ dans F,

St est irréductible

3.) Si $p_F \neq p_k$ et $q+1 = 0$ ds F

alors $0 \to St^0 \to St \to \varepsilon \to 0$

K corps local $\quad k$ corps résiduel

$\mathcal{O}_K \quad \pi \quad \mathcal{O}_K / \pi\mathcal{O}_K = k \qquad q = q_k = |k|$

F corps ; $p_F = \mathrm{car}\, F$

$G = Gl_2(K) \qquad G_0 = Gl_2(\mathcal{O}_K)$.

X = arbre de Gl_2 $\qquad C_0(X)$ = esp. vect sur F des 0-chaînes de X

= esp. de base somm. X.

PGl_2 opère sur $C_0(X)$

T = somme des voisins

$a \in F$ représentations $\quad H_a = C_0(X)/(T-a)\,C_0(X)$

$a = q+1. \qquad 0 \to H_a^0 \to H_a \to 1 \to 0.$

$\wr\!\wr$

St module de Steinberg

$\|$

$H_c^1(X)$

$\simeq$ fonctions localt ctes sur $\mathbb{P}_1(K)/1$.

$\mathbb{P}_1(K)$ = espace des bouts de X

Étude de l'irréductibilité

$aX+b \qquad f \mapsto f - f(\infty)$

∞.

$\mathcal{F}$: fonctions continues à support compact sur K.

$g \in B = \left\{\begin{pmatrix} a & b \\ 0 & 1\end{pmatrix}\right\}, \quad g.f(x) = f(g^{-1}x)$,

Théorème : a) $p_k = p_F$

$\mathcal{F}$ est irréductible comme B-module

b) $p_k \neq p_F$

Les seuls ss B-modules de $\mathcal{F}$ sont $0, \mathcal{F}_0, \mathcal{F}$

(1) où $\mathcal{F}_0 = \{ f \mid \int f(x)\,|dx| = 0 \}$.

Digression sur l'intégration sur les K-variétés analytiques à valeurs dans F. (135)

V K-variété de dim n : ω forme différ analyt de deg n partout non nulle

on peut lui associer une mesure $|\omega|$ sur V.

si sur K : mesure de Haar normalisée par $\mu(\mathcal{O}_K)=1$.

unique mesure $|\omega|$ tq $|\omega| = |f|\, dz_1 \ldots dz_n$

si $\omega = f\, dz_1 \wedge \ldots \wedge dz_n$

si U est un ouvert compact de V

$$\int_U |\omega| \in \mathbb{Z}\left[\frac{1}{p_k}\right].$$

En particulier on peut intégrer les fctions localt constantes à valeurs dans F (ou ds un groupe où p_k est inversible).

On a un fibré de mesures

Ω^n $\quad x \in K^*$ $\quad |x| = q_k^{-v(x)} \in F^*$

$GL_n(K) \longrightarrow F^*$ $\qquad |x|_F$

$g \longmapsto |\det g|_F$

sur $\mathbb{Z}/(p_k-1)\mathbb{Z}$, toutes les formes dif donnent la m mesure : il y a une mesure canonique

si V compact, son volume est un invariant.

Remarque : il est plus difficile d'intégrer des fonctions qui s'annulent

$$\int_{\mathcal{O}_K} |x|_F^m \, |dx|_F \;?$$

on définit $U_n = \{ x \mid v(f(x)) = n \}$

$\int_{U_n} |\omega| = a_n$ et on somme (comme pr intégrale de Lebesgue)

d'où $\sum a_n q^{-n}$ fction rationnelle de T (Igusa)

Démonstration du théorème (M. F Vignéras) (136)

① $f \in \mathcal{F}$ $f \neq 0$

les transformées par B de f engendrent $\mathcal{F}$

$f \in$ fonction caractéristique de $\mathcal{O}_K = \begin{cases} 1 & \text{si } |x| \leq 1 \\ 0 & \text{si } |x| > 1 \end{cases}$

$\pi^n \mathcal{O}_K$ ~~//////~~

Par homothétie, on peut supposer f à support $\subset \mathcal{O}_K$

f est constant mod $\pi^n \mathcal{O}_K$

V_f = combinaison linéaire des translatées de f par $\mathcal{O}_K / \pi^n \mathcal{O}_K$. ($p_k$-groupe).

$V_f \neq 0$. V_f contient un $\varphi \neq 0$ invariant par translation par $\mathcal{O}_K$ (lemme standard sur p-groupes).

$\varphi = c$ fonction car de $\mathcal{O}_K$, $c \neq 0$.

② $p_k \neq p_F$ A montrer $f \neq 0$ $f \in \mathcal{F}$

$\int f(x)\,|dx| \neq 0$, les transf de f engendrent $\mathcal{F}$.

si $\int$ ———— $= 0$, ———— $\mathcal{F}_0$.

Soit f, OPS f à support dans $\mathcal{O}_K$, constant mod $\pi^n \mathcal{O}_K$, $n \geq 1$.

V_f = espace engendré par les translatés de f par $\mathcal{O}_K / \pi^n \mathcal{O}_K$

Hyp: F algt clos (les caract seront vraiment à valeurs dans le bon corps!)

$\mathcal{O}_K / \pi^n \mathcal{O}_K$ gpe abélien fini

donc $V_f \subset$ rep. régulière de $\mathcal{O}_K / \pi^n \mathcal{O}_K$.

V_f admet une base formée de certains caractères $\psi : \mathcal{O}_K / \pi^n \mathcal{O}_K \to F^*$

⑨

$\Rightarrow 1 \in V_f \underset{(a)}{\Longrightarrow}$

On peut supposer que $f = \psi$, car $\neq 1$ de $\mathcal{O}_K$

π^m = conducteur de ψ

m = plus petit exposant ≥ 1 tel que $\psi = 1$ sur $\pi^m \mathcal{O}_K$.

$x \mapsto ax$

$\mathcal{F}_f$ = B esp eng par f

$\mathcal{F}_f$ contient $\psi(ax)$ $a \in \mathcal{O}_K^\times$.

$$\sum_{a \in \mathcal{O}_K^* / (1+\pi^m \mathcal{O}_K)} \psi(ax) := \varphi(x) \in \mathcal{F}_f$$

$\psi(ax)$ $a \in \mathcal{O}_K / \pi^m \mathcal{O}_K$

Tous les caractères additifs de $\mathcal{O}_K / \pi^m \mathcal{O}_K$

$\psi(ax)$, a divisible par π

$\Updownarrow$

caractères triviaux sur $\pi^{m-1} \mathcal{O}_K / \pi^m \mathcal{O}_K$

$$\varphi(x) = \sum_{\text{ts les } a} \psi(ax) - \sum_{a \text{ div par } \pi}$$

$$= \begin{cases} q^m \text{ sur } \pi^m \mathcal{O}_K \\ 0 \text{ ailleurs} \end{cases} - \begin{cases} q^{m-1} \text{ sur } \pi^{m-1} \mathcal{O}_K \\ 0 \text{ ailleurs} \end{cases}$$

($\sum_{\text{ts les } a}$ = reguliere)

$\mathcal{F}_f$ contient $\varphi - q\varphi'$ où φ = fct'on car de $\mathcal{O}_K$

φ' = —— $\pi \mathcal{O}_K$

$\mathcal{F}_f + D$ $\quad D =$ droite de $\mathcal{F}$ engendrée par φ (138)

D stable par B modulo $\mathcal{F}_f$

D stable mod $\mathcal{F}_f$ par

a) le groupe $ax+b$ $a \in \mathcal{O}_K^*$ $b \in \mathcal{O}_K$

b) le groupe $x \mapsto \pi x$

qui engendre B

donc $\mathcal{F}_f + D = \mathcal{F}$ $\quad \mathcal{F}_f \subset \mathcal{F}_0$ hyperplan

donc $\mathcal{F}_f = \mathcal{F}_0$

Remarque : autre dém en transf par Fourier et en utilisant car additif.

Irréductibilité de St

a) Si $p_F = p_K$ St est irréduct.

b) Si $p_F \neq p_K$ et $q_k+1 \neq 0$ dans F, St irréductible

c) Si $q_k+1 = 0$ dans F, St a un ss-module irréductible de codim 1.

Si $q = \pm 1$ dans F $\mathbb{P}_1(K)$ a une mesure μ canonique sur la boule unité $|dx|_F$ (en fait coïncident si $|x| > 1$ $\quad \left|d\left(\frac{1}{x}\right)\right|_F$ sf en 0 et 1 car $|x|_F^2 = q_F^{-2v(x)} = 1$

Si $q = 1$ dans F μ est invariant par PGL_2

$= -1$ ———— ε - inv

$\varepsilon : PGL_2 \to (\pm 1)$

$s \mapsto (-1)^{v(\det s)}$.

(3)

$\int_{\mathbb{P}_1(K)} \mu = 1 + \frac{1}{q}$ si $q = -1$ $\int_{\mathbb{P}_1(K)} \mu = 0$

$\mathcal{F}$ = fonct / constes $\xrightarrow{\int}$

$\Omega \xrightarrow{\ ||\ }$

$\mathcal{O}(-2)$ carré $\mathcal{O}(-1)$

⚠ Ω^1 isomorphe à $\mathcal{O}(-2)$ mais non canoniquement (façon de σ_2 !)

Fin de la démonstration :

$\mathcal{F}$ = fonct/$\underline{1}$

F ~~$\simeq$~~ choix de l'∞

$\mathcal{F}$ à fctions supp compact.

$\mathcal{F} \supset \mathcal{F}_0$ irréductible

Tout sous-module de $\mathcal{F} \neq 0$, $\mathcal{F}$ est $\mathcal{F}_0$.

Reste à savoir si $\mathcal{F}_0$ stable : si $q = -1$, on vient de voir que oui

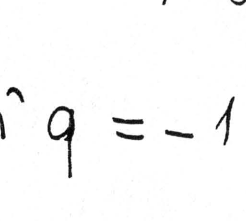
si $q \neq -1$, $\mathcal{F}_0$ n'est pas stable par G

$\mathcal{F}_0$: fonctions sur $\mathbb{P}_1$ $\int_K (f(x) - f(\infty)) |dx| = 0$.

$|x| \le q^{-N}$ disque autour de 0 ; φ_N fonction caractérist

Modulo ctes, $\alpha \varphi_N + \theta$, θ à support dans une couronne

φ.



$\int = \alpha q^{-N} + \int \theta(x) |dx|$.

$f(\frac{1}{x}) - \alpha = \alpha(\varphi_N(\frac{1}{x}) - 1) + \theta(\frac{1}{x})$

$\int = -\alpha q^{N-1} + \int \theta(\frac{1}{x}) \frac{dx}{|x|^2}$

2 formes linéaires $\Longrightarrow$ si hyperplan stable elles st proportionnelle donc égale

donc $q^N = q^{N-1}$ $\quad$ ($\alpha = 0$, θ concentrée sur le unités) $\quad \forall N \geq 1$

$$\int \theta\left(\frac{1}{x}\right) \frac{dx}{|x|^2} = \int \theta(x)\,|dx| \qquad |x|^2 = |d_F|$$

$q = \pm 1 \to q = -1$

Repr. H_a $\quad a \neq \pm(q+1)$

[Pb : si $p_k = p_F$ $\quad a = 0$ $\quad H_a$ est-il irréductible ?]

On va montrer que H_a est associée à une représentation induite.

$\lambda^2 - a\lambda + q = 0$ $\quad \lambda, \mu \in F$ $\quad \begin{cases} \lambda + \mu = a \\ \lambda\mu = q \end{cases}$

Th : $H_a \simeq I_\lambda$ (représentation induite définie par λ)

1ère définition de I_λ $\quad G = Gl_2$ $\quad B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ Borel

caractère de B $\quad \chi_\lambda \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \lambda^{v(d) - v(a)}$

représentation induite : fctions $f : G \to F$, localt ctes

$$f(sx) = \chi_\lambda(s) f(x) \qquad s \in B$$

G opérant par $(g \cdot f)(x) = f(xg)$

$\lambda = 1 \Rightarrow I_1 = \{$espace des fonctions sur $G/B\}$

2e définition : χ_λ définit G-fibré sur G/B en F droites
(variante) et on prend ses sections

$$\begin{array}{ccc} & G & \\ B & \downarrow & \xrightarrow{\chi_\lambda} F \\ & G/B & \end{array} \qquad \begin{array}{c} E \\ \downarrow \\ G/B \end{array}$$

(4)

2ème définition

fonctions localement constantes sur $K^2 - \{0\}$

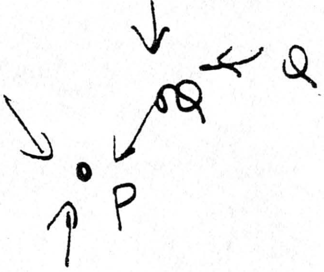
$I_\lambda = \{ f \mid$ localt ctes sur $K^2 - \{0\}$

$$f(cx) = \lambda^{2v(c)} f(x) \quad c \in K^* \}$$

action de G $\quad gf(x) = \lambda^{v(\det g)} f(g^{-1}x)$

$I_\lambda \xrightarrow{\theta} F$ $\quad$ B-av. χ_λ $\quad \theta(bx) = \chi_\lambda(b)\theta(x)$

3e définition sur l'arbre



On oriente toutes les arêtes vers P $\quad Q \neq P$ $\quad \sigma_P Q$ défini par $\sigma_P Q$ dans la géodésique $[P, Q]$

$$d(P, \sigma Q) = d(P, Q) - 1$$

$$\sigma_P(P) = P$$

$\sigma_P = \sigma_{P'}$ en dehors d'un nbre fini de points (ceux de la géodésique P, P')

Donc σ est un germe d'application au voisinage de ∂X.

$I_\lambda = \{ f$ définies p.p sur som(X), telles que
$f(\sigma x) = \lambda f(x)$ presque partout $\}$

Autre façon de voir les choses: $X_n(P)$ = les pts à distance n de P; F_n = fonctions sur $X_n(P)$

$F_n \to F_{n+1}$ flèche : $\times \lambda^{-1}$

$\varinjlim F_n = I_\lambda$

espace principal homogène sur $\mathbb{Z}$
base P_1

$\mathbb{Z} \xrightarrow{\lambda} F^*$ ie ~~of~~ action évidente de PG_1 (qui ne l'était pas du point de vue "induite").

$a = \lambda + q/\lambda$ $\alpha : H_a \longrightarrow I_\lambda$
$\beta : I_\lambda \longrightarrow H_a$

Def de α Il me faut $f \in I_\lambda$ invariant par G_0 et $Tf = af$

$$f(Q) = \lambda^{-d(P,Q)}$$

$Tf = af$ $p \cdot p$ Q à dist n de P

$$Tf_P(Q) = \sum_{P' \text{ voisin de } P} f_{P'}(Q). = \lambda^{-(n-1)} + q\lambda^{-(n+1)}$$
$$= a\lambda^{-n}.$$

Définition de β $H_a \leftarrow I_\lambda$

$f \in I_\lambda$ $(T-a)f = c$

f est une 0-chaîne ∞

$(T-a)f$ est à support fini

$(T-a)f \in C_0$

f est déf. à l'addition près d'un élément de C_0.

$\alpha \circ \beta = \lambda - \lambda^{-1}$

$\beta \circ \alpha = \lambda - \lambda^{-1}$

$a \neq \pm(q+1) \Rightarrow \lambda \neq \pm \underline{1}$.

d'où les isomorphismes (commutent à l'action de G, car H est intrinsèque)

si $a \neq \pm(q+1)$ $\quad I_\lambda \simeq I_\mu$

~~($\lambda = q$)~~

Or $I_\lambda \simeq I_\mu^*$ (dual)

Rque : Steinb est selfdual.

Théorème : $a = \lambda + q/\lambda \neq \pm(q+1)$

si $(\lambda, \mu) \neq \{1, q\}$ et $\{-1, -q\}$

I_λ, H_a sont irréductibles

Dém : 1 ou 2 dém

$\mathbb{P}_1(K)$: on regarde sections du fibré qui s'annulent à l'∞ $\quad I_\lambda^\infty$

on les transf en fonctions sur dte affine

Plus concrètement $\quad f$ sur $K^2 - \{0\}$

$f(e_2 + te_1)$ $\quad e_1 = (1,0)$

$e_2 = (0,1)$

I_λ^∞ = fctions cont à supp compact sur K

On constate que le grpe $x \mapsto ax+b$

$$gf(x) = \lambda^{\pm v(a)} f(g^{-1}x)$$

$I_\lambda^\infty \simeq \mathcal{F} \otimes$ (représent de d° 1)

Si I_λ non irréductible, il y aurait un quotient de dim 1 de I_λ (comme G-module)

Il n'y a pas de formes linéaires $\theta : H_a \to F$ G-covariante (pour un car $G \to F^*$) $\underline{1}, \underline{\varepsilon}$

Si $\exists$ $\theta(P) \neq 0$, parer 1.

$\theta(\mathbb{P}) = f(a) \ldots$ impossible

Remarques

* $0 \to H_a^0 \to H_a \to 1 \to 0$

$a = q+1$

n'est pas triviale.

$\mathrm{End}\, H_a = F$ (propriété universelle de H_a)

H_a n'est donc pas décomposable, ni irréductible

(Irréd $\Rightarrow$ End $= 1 \Rightarrow$ indécomp)

* Dans le groupe de Grothendieck des représ admissibles

$$[H_a] = [I_\lambda] = [I_\mu]$$

(même si $a = \pm(q+1)$).

I_λ peut être décomposable

Principe de la dém :

$[H_a] = [I_\lambda]$ génériq^t

$\Rightarrow [\ \ ] = [\ \ ]$ toujours

$\mathcal{F}$

$|$ du existence de 2 réseaux L_1, L_2

F

$\pi^N L_2 \subset L_1 \subset L_2$

lemme de Brower donne ind réd ds le gpe de Grothend.

Serre 1/2/88

rep. PGL_2 vect fixé par $GL_2(\mathcal{O}_K)$.

$a \in F$ rep. H_a universelle $T_v = av$

Si $\omega : K^* \to F^*$ On considère une représ. $\rho : G \to GL(V)$ avec car central $\rho = \omega$

$$\rho\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} = \omega(\lambda)$$

ω trivial sur les unités $U_K = \mathcal{O}_K^*$ (= car non ramifié)

Choisissons ε $\varepsilon^2 = \omega$. ω caract def par $\omega(\pi)$ et

F algt clos On tord par ε^{-1} : on a une rep de PGL_2

Donc grâce à cette manip on peut définir une rep universelle $H_{a,\omega}$ par torsion

$$H_{a,\omega} = \varepsilon \otimes H \qquad b\,\varepsilon(\pi) = a.$$

Rappel : cas exceptionnel $a = \pm(q+1)$ (où H_a n'est pas irréductible) : ici $H_{a,\omega}$ non irréductible

$$P(T) = T^2 - aT + q\,\omega(\pi) = (T-\lambda)(T-\mu)$$

Le rapport des racines était q ou q^{-1}

On garde cette condition ici aussi !

Lemmes variés

(1) Lemme de Schur.

1ère forme G localement profini

V représentation irréductible admissible de G sur F algt clos. Alors $\mathrm{End}_G V = F$

U ouvert $V^U \neq 0$ $\dim V^U < \infty$ Si $\varphi \in \mathrm{End}_G V$ $\varphi : V^U \to V^U$

$\exists\, \lambda \in F$ $\varphi - \lambda$ non inversible $\Rightarrow$ $\varphi = \lambda$

(1) 2e forme Soit Λ une F-algèbre. Soit V

un Λ-module irréduct, F algt clos ; on suppose $\operatorname{card} F > \dim_F V$. Alors $\operatorname{End} V = F$

(souvent utilisé avec $F = \mathbb{C}$ $\dim V \leq \aleph_0$)

- Si $\operatorname{End} V \supsetneq F$, il contient $F(T)$ donc $\frac{1}{T-\alpha}$ card F - élts indépendants.

Corollaire : Si V est absolument irréductible, $\operatorname{End} V = F$.

Lemme 2 Soit Λ une F-algèbre, S un Λ-module irréductible, $\operatorname{End} S = F$. Si W est un F-esp vect $W \otimes_F S$ est un Λ-module semi-simple isotypique de type S

$W \mapsto W \otimes_F S$ est une équivalence de catégories (Bourbaki A VIII, §4 n°4, corol à la prop 4)

En particulier, tout sous Λ-modules de $W \otimes_F S$ est de la forme $W' \otimes_F S$ pour $W' \subset W$

(Morale de la théorie des rep : écrire comp isotyp sous forme d'un produit $\otimes$, car alors tt ce qui commute à S se lit pour W')

Lemme 3 Soit $\rho : Gl_2(K) = G \longrightarrow GL(V)$ une représentation admissible de G, de car central $\omega : K^* \to F^*$ (F algt clos $p_F \neq p_K$). non ramifié. Soit $a \in F$

Soit $W \subset V$, W est fixé par le compact maximal $Gl_2(\mathcal{O}_K) = G_0$ et $T v = av$ pour $\forall v \in W$.

Prop universelle définit

$W \otimes H_{a,\omega} \longrightarrow V$

Cet homomorphisme est injectif si aucun élément $\neq 0$ de W n'est fixé par $Sl_2(K)$ (cond évidt nécessaire!)

Démonstr : Soit $N = \mathrm{Ker} : W \otimes H_{a,\omega} \longrightarrow V$. C'est un sous-$G$-module. Soit $H^s_{a,\omega}$ l'unique ss/module simple de $H_{a,\omega}$ ($= H_{a,\omega}$ si $a/\mu \neq \{q, q^{-1}\}$) et $H_{a,\omega} / H^s_{a,\omega}$ est de dim 1 ou 2.

Soit $N' = N \cap (W \otimes H^s_{a,\omega})$: est de la forme $W' \otimes H^s_{a,\omega}$ pour un certain $W' \subset W$ par le lemme 2.

Soit $w \in W'$ $w \neq 0$, l'image de $w \otimes H_{a,\omega}$ dans V se factoriserait par $w \otimes (H_{a,\omega} / H^s_{a,\omega})$: or, l'action de Sl_2 là-dessus est triviale, donc $w = 0$!!

Alors $N = 0$: en effet $N \hookrightarrow W \otimes (H_{a,\omega} / H^s_{a,\omega})$
l'action de G là-dessus par $G \longrightarrow \{\pm 1\}$
$s \longmapsto (-1)^{v(\det s)}$

En particulier G_0 fixe ceci, donc N. Mais les pts fixes de G_0 dans $H_{a,\omega}$ sont les multiples de $e_{a,\omega}$ (vect canonique de $H_{a,\omega}$).
Autrement dit l'action de $Sl_2(K)$ sur $H_{a,\omega}/H^s_{a,\omega}$ donc sur N est triviale. Or $Sl_2(K)$ ne laisse fixe que 0 dans $H_{a,\omega}$ donc aussi ds $W \otimes (\ )$

Retour aux quaternions.

p $F = \overline{\mathbb{F}_p}$ D corps de quaternions sur $\mathbb{Q}$ ramifié en $\{p, \infty\}$ et pas ailleurs

G = gpe multipl de D (comme gpe alg / $\mathbb{Q}$)

G_A = gpe des adèles de G

$\mathcal{F}$ = espace des fonctions localt ctes sur $G_A / G_{\mathbb{Q}}$

Rep de G_A :

$f \in \mathcal{F}$ $g \in G_A$

rep à droite $f \mapsto \{x \mapsto f(gx)\}$

On regarde cela comme un module à gauche par $(gf)(x) = f(g^{-1}x)$

Si $\omega : A^* / \mathbb{Q}^* \to F^*$ est un caractère (continu)

$f_\omega(x) = \omega(\mathrm{Nrd}(x))$ $G \xrightarrow{\mathrm{Nrd}} G_m$

Les multiples de f_ω ~~forment~~ $G_A \xrightarrow{\mathrm{Nrd}} A^*$

un s/G_A-module S_ω de dim 1 (ols $\omega \neq$ des $S_\omega \neq$)

Théorème : les seuls ss-mod simples de $\mathcal{F}$ st le S_ω.

1ère propriété de $\mathcal{F}$ (comme G_A-module)

Lemme : SG = gpe dérivé de G

Si $f \in \mathcal{F}$ est fixé par un $SG(\mathbb{Q}_\ell)$ avec $\ell \neq p$, alors f est fixé par SG_A tt entier.

= gpe des élts de norme réduite 1

$SG(\mathbb{Q}_\ell) \simeq SL_2(\mathbb{Q}_\ell)$ $\ell \neq p, \infty$

$G(\mathbb{Q}_\ell) \simeq GL_2(\mathbb{Q}_\ell)$.

Th me d'approximation (Eichler–Kneser) Le sous-groupe $SG(\mathbb{Q}_\ell)$. $SG_{\mathbb{Q}}$ est dense dans $SG_{\mathbb{A}}$
i.e $SG_{\mathbb{Q}}$ est dense dans $SG_{\mathbb{A}'}$ si $\mathbb{A}'$ = adèles avec ℓ-compos. enlevée

$f \in \mathcal{F}$ est invariante à droite par $SG_{\mathbb{Q}}$

$SG_{\mathbb{Q}_\ell}$

donc

par $SG_{\mathbb{A}}$.

Donc

Corollaire: f provient d'une fonction sur $\mathbb{A}^*/\mathbb{Q}^*$

Construction de sl modules : Soit $V \neq 0$ une représentation admissible de $G_{\mathbb{A}}$ ayant un caractère central $\omega : \mathbb{A}^*/\mathbb{Q}^* \to F^*$.

Hypothese: Aucun $v \neq 0$ dans V n'est fixé par un $SG(\mathbb{Q}_\ell)$ $\ell \neq p\infty$ (ie $V^{SG(\mathbb{Q}_\ell)} = 0$ pour tout $\ell \neq p, \infty$)

Alors V contient un G-module du type
$$W \otimes \bigotimes_{\ell \notin S} H_{a_\ell, \omega_\ell}.$$
où W est un mod admissible $\neq 0$ sur $G_S = \prod_{\ell \in S} G(\mathbb{Q}_\ell)$
pour S assez grand

Corollaire: Supposons qu'au moins un des H_{a_ℓ, ω_ℓ} soit du type exceptionnel. Alors V n'est pas simple.

Explication sur ce qui précède:
$$\varinjlim_{\substack{T \subset S \\ \text{fini}}} \bigotimes_{\ell \in T} H_{a_\ell, \omega_\ell}$$

③

e_ℓ vecteur canonique $\in H_{a_\ell, \omega_\ell}$

$x_{\ell_1} \otimes x_{\ell_2} \otimes \cdots$ avec presque tt = vect canonique

Soit $v \in V$ $v \neq 0$. Il existe S assez grand pour que v soit fixe par $U \times \prod_{\ell \notin S} G_{0,\ell}$

où U est ouvert dans G_S et $G_{0,\ell}$ = compact maximal stand.

Soit $V' \subset V$ les vect fixés par $U \times \prod_{\ell \notin S} G_{0,\ell}$

Les opérateurs de Hecke rel. aux $\ell \notin S$ opèrent sur V'.

On a donc $v \in V$ qui a les propriétés ci-dessus et vap a_ℓ pour T_ℓ.

Soit W le ss espace de V formé des $f \in V$ qui sont fixés par les $G_{0,\ell}$ $(\ell \notin S)$, $T_\ell f = a_\ell f$ pour tout $\ell \notin S$. Alors W est un G_S-module

On a une flèche $W \otimes \bigotimes H_{a_\ell, \omega_\ell} \to V$

$W \otimes H_{a_\ell, \omega_\ell} \to V$; définie par action de G_ℓ.

La flèche est injective par un des lemme du début.

$W_S \otimes H_{a_\ell, \omega_\ell} \hookrightarrow V$

Puis :

$\underbrace{W_S \otimes H_{a_\ell, \omega_\ell}}_{\subset W_{S \cup \{\ell\}}} \otimes H_{a_{\ell'}, \omega_{\ell'}} \to V$ injectif encore

etc... cqfd.

Lemme sur les representations galoisiennes :

$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F)$ une representation semi-simple

de déterminant impair ($\det \rho(c) = -1$, c = conj cplexe)

① Les l non ramifiés de ρ, $l \neq p$, pour lesquels $\rho(\mathrm{Frob}_l)$ est exceptionnel pour l ont une densité > 0.

② Cette densité est 1 ssi $\rho \simeq \alpha \oplus \chi\alpha$, α car de degré 1

Terminologie : $g \in GL_2(F)$ est exceptionnel pour l si le rapport de ses val propres est l ou l^{-1}.

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{(\rho,\chi)} \underset{\text{finie}}{\mathrm{Im}\,\rho} \times \mathbb{F}_p^*$

ens des élts (g, x) tq le rapport des val propres de $g = x$ ou x^{-1}.

Les l de ① ont une densité > 0 si l'ens des (g, χ) except dans $\mathrm{Im}(\rho, \chi)$ est $\neq \emptyset$: c'est vrai car contient c et 1

② résulte d'un lemme : soit $\rho : G \to GL_2(F)$, F algt clos, G quelconque, ρ semi-simple et soit $\chi : G \to GL_1(F) = F^\times$

Supposons que pour tout $g \in G$, le rapport des valeurs propres de $\rho(g)$ soit $\chi(g)$ ou $\chi(g)^{-1}$.

Alors $\rho \sim \alpha \oplus \chi\alpha$, α caract de deg 1.

Démons : (rep adjointe de $\rho)^{ss} \simeq 1 \oplus \chi \oplus \chi^{-1}$

$\Rightarrow \rho$ réduct $\sim \beta \oplus \gamma$

$\beta/\gamma = \chi$ ou χ^{-1}

④ Or si un gpe est $\cup$ de 2 ss gpes, c'est l'un des deux !

Proposition Soit $v \in \mathcal{F}$ $v \neq 0$ car central ω
v fixé par $G_{0,\ell}$ $\ell \notin S$ $T_\ell v = a_\ell v$, $a_\ell \in \mathbb{F}$
Alors les ℓ tels que H_{a_ℓ, ω_ℓ} soit exceptionnel (et m: type 2) ont une densité strictement positive

On se ramène à des val propres des opérateurs de Hecke usuelles (f modul. mod p)
d'où représent galoisiennes ρ
le rapport a_ℓ / μ_ℓ = rapport des val p de $\rho(\mathrm{Frob}_\ell)$

Th 1 : Les seuls s/mod simples de $\mathcal{F}$ sont les S_ω de dim 1.

Dém : Soit V un ss-module simple de $\mathcal{F}$; il a un caractère central ω.

① SG_A fixe V ; donc V de dim 1 et du type S_ω.

② Les pts fixes $= 0$ donc aussi $V^{SL(\mathbb{Q}_\ell)} = 0$ pour $\forall \ell \neq p$, ℓ (prop 1).
Par thme de struct $V \supset W \otimes X\, H_{a_\ell, \omega_\ell}$, une astre de H_{a_ℓ,ω_ℓ} ne st pas simples, d'où impossible

Remarque : si $p \neq 2$ cas except de type 2 $\begin{cases} a_\ell = 0 \\ \ell \equiv -1 \bmod p \end{cases}$
H_{a_ℓ, ω_ℓ} a 2 quotients simples de dimension 1 distincts
$W \otimes X \ldots$ fait donc intervenir une astre contenue de mod simples de dim 1.