Leçon 1 (Lucchesi)

But du cours Expliquer une construction de corps de nombres dont on contrôle la ramification. Au passage, introduire certains liens entre représentation de Galois et automorphes.

Programme

1 (Ch) Enoncé du théorème, rappels de théorie algébrique des nombres

2. (Cl) Introd. aux formes modulaires

3. (Cl) Représentations de Galois associées aux formes modulaires 1

4. (Ch) ——— 2

5. (Cl) Formes automorphes sur les groupes unitaires et rep. Galois.

6. (Ch) Preuve d'un cas particulier du théorème.

---

① Ramification dans les corps de nombres

$\overline{\mathbb{Q}} \subset \mathbb{C}$ désigne le sous-corps des nombres algébriques

- Un corps de nombres est une extension finie du corps des rationnels $\Leftrightarrow$ un sous corps de $\mathbb{C}$ engendré par un nb fini de nb. algébrique. Sa dimension comme $\mathbb{Q}$-ev est notée $[K:\mathbb{Q}]$ si K est le c.dn.

- $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$ sous ens. des entiers algébriques, i.e annulés par un $P \neq 0$ dans $\mathbb{Z}[X]$ unitaire $\Leftrightarrow$ dont le p.min. unitaire est dans $\mathbb{Z}[X]$.

Si K c.dn, $K \subset \mathbb{C}$, on pose $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$ = les entiers de K.
sous-anneau. ($\overline{\mathbb{Z}}$ sous-anneau de $\overline{\mathbb{Q}}$).

- En général, $\mathcal{O}_K$ difficile à calculer.

Ex: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

$K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sans f.carré

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \not\equiv 1 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \ (4) \end{cases}$$

$\Pi_{\frac{1+\sqrt{d}}{2}} = X^2 - X + \frac{d-1}{4}$

$K = (\mathbb{Q}(e^{2i\pi/n}) \quad , \quad \mathcal{O}_K = \mathbb{Z}[e^{2i\pi/n}])$

En général, $K = \mathbb{Q}(x)$ mais $\mathcal{O}_K$ n'est pas très de la forme $\mathbb{Z}[x]$!
$x \in \overline{\mathbb{Z}}$. En revanche $\mathcal{O}_K \simeq \mathbb{Z}^d$, $d = [K:\mathbb{Q}]$

• arithmétique dans $\mathcal{O}_K$ → décomposition de nb premiers associés

ex: $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$ entiers de Gauss - alors c'est un anneau principal

3 cas $2 = -(1+i)^2$ → $p \equiv 3 \ (4)$ alors p premier dans $\mathbb{Z}[i]$
$\mathbb{Z}[i]/(p)$ corps (car p^2 éléments)

$\mathcal{O}_K^\times = \{\pm 1, \pm i\}$ - $p \equiv 1 \ (4)$ $p = \pi\overline{\pi}$ produit de 2 premiers $\neq$
$\pi = a+bi$ $p = a^2+b^2$.

En général, $\mathcal{O}_K$ non principal, mais très de Dedekind : tout idéal $\neq 0$
est produit unique d'idéaux maximaux ⟷ nb premiers.

$\mathfrak{p}$ premier, $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ avec $\forall i \neq j \ \mathfrak{P}_i \neq \mathfrak{P}_j$ les idéaux max. contenant $\mathfrak{p}$.

contrainte $\forall i$ $\mathcal{O}_K/\mathfrak{P}_i$ corps fini $\simeq \mathbb{F}_{p^{f_i}}$ ca. p

$$\sum_{i=1}^{g} e_i f_i = [K:\mathbb{Q}]$$

(ex: $(3) = \mathfrak{P}\overline{\mathfrak{P}}$ $\mathfrak{P} = (3, \sqrt{-5}-1)$ non principal)

On dit que $\mathfrak{p}$ est ramifié dans K si $\exists i$ / $e_i > 1$ dans cette formule

ex: $\mathbb{Q}(i) \rightsquigarrow 2$. , analogue ramif surface de Riemann

Prop: (Dedekind) les premiers ramifiés sont en nb fini,
ce sont les diviseurs du discriminant de K.

Explication. $x \in K$, $m_x : K \to K$ $\mathbb{Q}$-linéaire.
$Tr_K(x) = tr(m_x) \in \mathbb{Q}$., $\in \mathbb{Z}$ si $x \in \mathcal{O}_K$.

$\mathrm{disc}(K) = \det(Tr_K(e_i e_j))$ si $\mathcal{O}_K = \bigoplus_{i=1}^{[K:\mathbb{Q}]} \mathbb{Z} e_i$

discriminant de la forme quadratique $\mathrm{Trace}_K(x^2)$.

(e_i un entier indép. base (e_i))

• si $\mathcal{O}_K = \mathbb{Z}[x]$, en fait $\mathrm{disc}\, K = \mathrm{disc}\, \Pi_x$
$\mathrm{disc}\, K \ \#\mathcal{O}_K/\mathbb{Z}[x] = \mathrm{disc}\, \Pi_x$.

?...

Ex: $\operatorname{disc} \mathbb{Q}(\sqrt{d}) = \begin{cases} d & \text{si } d \equiv 1 \pmod 4 \\ 4d & \text{sinon} \end{cases}$, $\operatorname{disc} \mathbb{Q}(e^{2i\pi/n}) \mid n^{\varphi(n)}$

Le discriminant est un invariant arithmétique important de c.d.n, ex.

thm (Hermite) S ens. fini de premiers et $n \geq 1$ entier, il n'y a qu'un nbre fini de c.d.n non ramifiés hors S et de degré $\leq n$.
(Minkowski) $\operatorname{disc} K \neq \pm 1$ si $K \neq \mathbb{Q}$.

(géométrie des nombres, interprétation disc comme le "volume de $\mathcal{O}_K$")

Théorème du cas (v1) (Ch-Cl JAMS 08)

Soit S un ens. fini de premiers $|S| \geq 2$.
$\forall n \geq 1$, $\exists$ K c.d.n non ramifié hors de S tel que $n \mid [K:\mathbb{Q}]$.

→ existence de c.d.n., difficile (sauf cas abélien) d'où construire.

Remarques - il y a des tables dans la nature d° petit, S petit
on peut pas avoir $n = [K:\mathbb{Q}]$ - en général.
ex: pas de c.d.n d°3 ramifié en 2 et 5 uniquement.
- $|S|=1$ conjecturale ± ok mais encore ouvert. (Mihăilescu)

vers une version plus fine → $\mathbb{Q}_S$

(2) Le corps $\mathbb{Q}_S$. Soit S un ens fini de premiers.

~~Le sous~~ l'ens. des c.d.n de $\bar{\mathbb{Q}}$ qui sont non ram hors S est stable par comp., sous-ext. ⇝ $\mathbb{Q}_S :=$ la composée de tous ces ss cop.

$\mathbb{Q}_S \subset \bar{\mathbb{Q}}$ est une ss ext. Galoisienne.

$G_S := \operatorname{Gal}(\mathbb{Q}_S/\mathbb{Q})$, c'est un quotient de $G_{\mathbb{Q}}$.

reformuler notre pb ⇝ G_S gros. Nombreux pb. ouverts sur G_S
(et $G_{\mathbb{Q}}$, mentionner aalement).

Action de G_S sur l'homologie des variétés alg.

- Soit $X \subset \mathbb{P}^n$ une variété algébrique proj. lisse (pour $X(\mathbb{C})$) définie sur $\mathbb{Q}$.

- Si ℓ premier, Grothendieck a défini une action (continue) $\rho_{X,i,\ell}$ de $G_{\mathbb{Q}}$ sur $H^i(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell$ $\forall i$., $\mathbb{Z}_\ell$-linéaire $\rightsquigarrow$ rep. de $G_{\mathbb{Q}}$.

- On dit que X a bonne réd. en p, premier, si X a des équations sur $\mathbb{Z}[\frac{1}{p}]$, telles que $\overline{X} := X \bmod p$ est lisse. (c'est le cas pour presque tout p ssi $X(\mathbb{C})$ est lisse).

Théorème (Groth.) Soit $S \supset \{\ell$, les premiers de mauvaise réd. de $X\}$.
Alors les $\rho_{X,i,\ell}$ se factorisent par G_S.

- voir l'exposé de N. Rublot pour l'exemple fondamental $X = \text{courbe ell.}$ $i=1$
- dessin $\rightsquigarrow$ courbes modulaires.
- Un pb est d'étudier les $\rho_{X,i,\ell}$, fondamental en géom. arithm.
Pour pouvoir caract. des rep. $G_S \rightsquigarrow$ certains éléments

Retour sur la réd. mod p. en théorie de Galois

Soit K un c.d.n., supposé Galois sur $\mathbb{Q}$.
p premier non ramifié dans K, $p\mathcal{O}_K = P_1 \cdots P_g$.

Théorème $\forall i = 1 \cdots g$, $\exists\, \sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $\sigma(P_i) = P_i$ et σ agit sur $\mathcal{O}_K/P_i$ par $x \mapsto x^p$ (Frobenius)
et les σ_i forment une classe de conj. dans $\mathrm{Gal}(K/\mathbb{Q})$, noté Frob$_p$.

Ex: $K = \mathbb{Q}(e^{2i\pi/m})$ (Cebotarev) $\mathcal{O}_K = \mathbb{Z}[e^{2i\pi/m}]$ donc $K/m^{\text{ème}}$
$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$ Frob$_p = \overline{p} \in (\mathbb{Z}/m\mathbb{Z})^*$
$(\zeta \mapsto \zeta^k) \leftrightarrow k$

Cor: $\forall p \notin S$, il existe dans G_S une ~~unique~~ classe de conj canonique.
notée Frob$_p$ obtenue par recollement des celles du thm. ci-dessus.

Théorème (Cebotarev) La réunion des Frob$_p$ est dense dans G_S.
Plus précisément, si $K/\mathbb{Q}$ est comme plus haut, toute classe de conj de $\mathrm{Gal}(K/\mathbb{Q})$
est un Frob$_p$ pour une infinité de p.

Cor. Si $\rho_1, \rho_2 : G_S \longrightarrow GL_n(\overline{\mathbb{Q}_\ell})$ sont de rep. irred. (ou semi-s.) cont.

et si $\mathrm{tr}(\rho_1(\mathrm{Frob}_p)) = \mathrm{tr}(\rho_2(\mathrm{Frob}_p)) \quad \forall p \notin S.$

alors $\rho_1 \simeq \rho_2$.

Exemple $\sum (-1)^i \mathrm{tr}(\rho_{X,i,\ell}(\mathrm{Frob}_p)) = \#\overline{X}(\mathbb{F}_p) \quad \forall p$ bonne red. $\neq \ell$.

(3) Autre formulation du théorème

S fini. $\mathbb{Q} \longrightarrow \mathbb{Q}_p \longrightarrow \overline{\mathbb{Q}}_p$, puis on choisit $\overline{\mathbb{Q}} \xrightarrow{\iota} \overline{\mathbb{Q}}_p$

on en déduit $i^\iota : G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{Q}}$, dont la classe de conj. est indépendante du choix de ι. En particulier

$$G_{\mathbb{Q}_p} \longrightarrow G_S.$$

Théorème (v2) Si $|S| \geq 2$ et $p \in S$, alors $G_{\mathbb{Q}_p} \longrightarrow G_S$ est injective.

Autrement dit $\mathbb{Q}_S \cdot \mathbb{Q}_p = \overline{\mathbb{Q}}$

Concrètement $\forall F/\mathbb{Q}_p$ finie, $\exists K$ c.de $\subset \mathbb{Q}_S$ tel que $K \cdot \mathbb{Q}_p \supset F$

rmk on peut supposer K galois $\Rightarrow [K\mathbb{Q}_p : \mathbb{Q}_p] \mid [K:\mathbb{Q}]$

Appliquant ceci à $F/\mathbb{Q}_p$ de tout degré (ça existe : non ram)

on obtient la V_1.

(leçon 2, Clozel)

2. Formes modulaires (a crash course)

1. Le demi-plan de Poincaré, groupes arithmétiques

Soit $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Le groupe $G = SL(2, \mathbb{R}) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \det = 1\}$

agit par $g \cdot z = \dfrac{az+b}{cz+d}$. $(z \in \mathcal{H})$.

On s'intéresse aux sous-groupes arithmétiques de G :

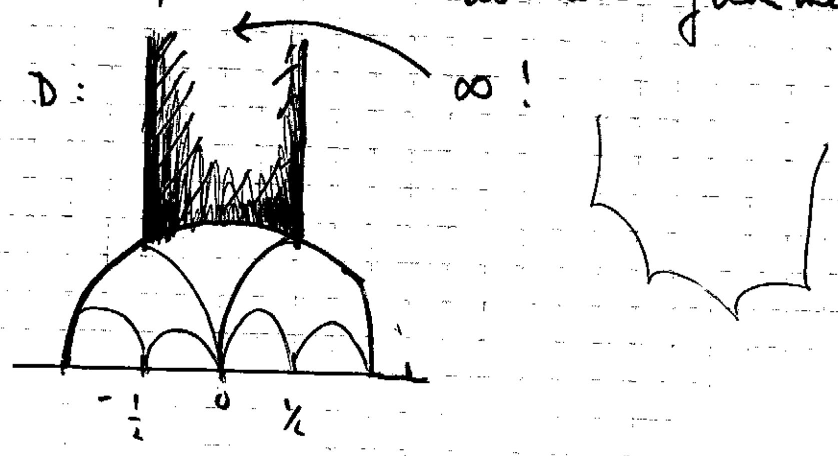
· $\Gamma(1) = SL(2, \mathbb{Z})$

$\Gamma = \Gamma_0(N) = \{\gamma \in \Gamma : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} [N]\}$.

Le groupe Γ agit de façon discrète sur $\mathfrak{H}$.
En particulier $\Gamma \backslash \mathfrak{H}$ = quotient est défini et c'est une surface de Riemann (= courbe algébrique complexe) non compacte.

Ex : $\Gamma = SL(2, \mathbb{Z})$. Un domaine fondamental est

D :



(Π en pointe ?)

Rappelons aussi que la mesure invariante sur $\mathcal{H}$ (pour G) est $\frac{dx\,dy}{y^2}$. On sait que $\mathrm{vol}(D) < +\infty$.

2. Formes modulaires.

Ce sont des fonctions holomorphes sur $\mathcal{H}$, "invariantes" sur Γ selon une loi de transformation convenable. On fixe $k \geq 1$ et on suppose

(1) $f : \mathcal{H} \to \mathbb{C}$ holomorphe

(2) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

(3) f holomorphe à l'infini.

Pour expliquer (3) supposons $\Gamma = SL(2,\mathbb{Z})$.
Alors $f(z+1) = f(z)$: $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \in \Gamma$.
Si $q = e^{2i\pi z}$, on a donc

$$f(z) = \sum_{-\infty}^{+\infty} a_n\,(x)\, e^{2i\pi n(x+iy)}$$

et l'holomorphie de f implique immédiatement (Exercice)

$$f(z) = \sum_{-\infty}^{+\infty} a_n q^n.$$

Une "propriété à l'infini" est $q = e^{2i\pi z}$ (avec $q(\infty) = 0$: considérer $z \in D$, $|z| \to \infty \Rightarrow \mathrm{Im}(z) \to +\infty$). On suppose que f est holomorphe à l'infini, i.e.

$$f(z) = \sum_{0}^{\infty} a_n q^n.$$

[La définition pour tout Γ, en analogue].

On dit que f est une forme parabolique si $a_0 = 0$, $f(z) = \sum_{1}^{\infty} a_n q^n$.

Exemple : les différentielles.

On a $d\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^2} dz$

donc f est une forme modulaire de poids 2

$\Leftrightarrow$ $f(z)\,dz = \omega$ est une différentielle invariante

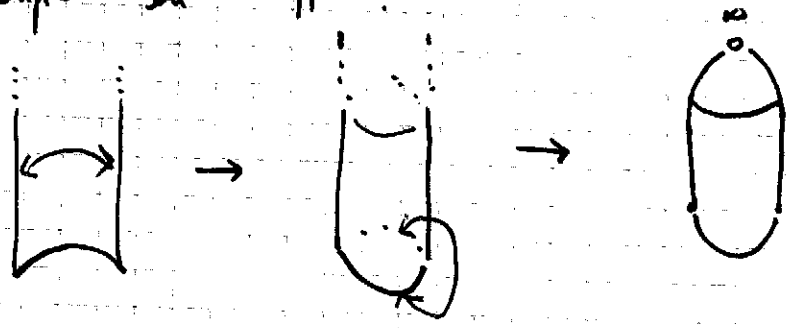
De plus (Exercice) la condition "f cuspidale" est exactement :

$\omega = f(z)dz$ s'étend de façon holomorphe à $\ell'\infty$ ($q=0$).

Notation : $S_k(\Gamma) = \{$formes paraboliques$\}$

$M_k(\Gamma)$.

Remarque : Si $\Gamma = SL(2,\mathbb{Z})$ on sait que $\Gamma\backslash\mathcal{H}$ se compactifie en $\mathbb{P}^1$:



Mais il n'y a pas de différentielle sur $\mathbb{P}^1$, donc

$S_2(\Gamma) = \{0\}$ ($\Gamma = \Gamma(1)$).

3. Un exemple : la fonction Δ

Une façon "évidente" de construire des formes modulaires est comme séries de Poincaré. Soit

$$j(\gamma, z) = cz + d.$$

On vérifie immédiatement la formule "de cocycle":

$$j(\delta\gamma, z) = j(\delta, \gamma z)\, j(\gamma, z).$$

Si on pose

?? $$f(z) = \sum_{\gamma \in \Gamma} j(\gamma, z)^{-k}$$

on vérifie formellement que f vérifie l'équation fonctionnelle de poids k. Il reste à se soucier de la convergence. Prenons $\Gamma = \Gamma(1)$.

- Si $\gamma = \begin{pmatrix} 1 & n \\ * & * \end{pmatrix}$, $j(\gamma, z) = \ldots 1$

La somme ne peut donc pas être convergente. Si $\Gamma_\infty = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \right\}$ on peut plus correctement considérer

$$G_k(z) = \sum_{\Gamma_\infty \backslash \Gamma} \sum_{\Gamma_\infty} j(\gamma, z).$$

(Le quotient est à gauche !). Il est facile de décrire Γ / Γ_∞ : Γ agit sur $\mathbb{Z}^2$ et $\Gamma_\infty = \Gamma_e$, $e = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Le quotient est donc $\mathbb{Z}^2 - \{0\}$.

Un calcul simple donne alors

$$G_k(\zeta) = \sum_{m,n}{}' \frac{1}{(m\zeta+n)^k},$$

où $\sum'$ veut dire qu'on suppose $(m,n) \neq (0,0)$. Notons que $\{m\zeta+n\}$ est un réseau de $\mathbb{C} = \mathbb{R}^2$, et que $(m\zeta+n)^{-k} = O(\|m\zeta+n\|^{-k})$. La série converge donc pour $k \geq 3$. Comme $\Gamma(1)$ contient $(-1,-1)$, elle est nulle pour k impair (mais c'est faux pour les autres groupes de congruence!)

Un calcul un peu moins facile, mais classique, donne

$$G_k(\zeta) = 2\zeta(k) + \frac{2(2i\pi)^k}{(k-1)!} \sum_1^\infty \sigma_{k-1}(n) q^n.$$

On normalise en posant

$$E_k(\zeta) = 1 + \frac{1}{\zeta(k)} \frac{(i\pi)^k}{(k-1)!} \sum_1^\infty \sigma_{k-1}(n) q^n.$$

(k pair ≥ 4). Notons les faits remarquables suivants:

(1) E_k est à coefficients rationnels,

car $\quad \zeta(2m) = \pi^{2m}$ (rationnel)

(2) La croissance des coefficients est connue

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1} \asymp n^{k-1} \quad (\text{mod}^{\times} n^{\pm\varepsilon})$$

En particulier

$$\begin{cases} E_4 = 1 + 240 \sum \sigma_3(n) q^n \\ E_6 = 1 - 504 \sum \sigma_5(n) q^n \end{cases}$$

- Si $f \in M_k$, $g \in M_{k'}$, $fg \in M_{k+k'}$ (ensemblement évident). On peut donc considérer

$$E_4^3 - E_6^2 = (1 + 240q)^3 - (1 - 504q)^2 \pmod{q^2}$$

$$\equiv (3 \cdot 240^2 + 2 \cdot 504)\, q$$

$$= 1728\, q = 2^6 3^3 q \pmod{q^2}$$

On pose

$$\Delta(z) = 2^{-6} 3^{-3} (E_4^3 - E_6^2) = q - 24q^2 + \dots$$

On a démontré l'existence d'une forme parabolique de poids 12. En fait celle-ci a été découverte par Jacobi dans sa théorie des fonctions elliptiques, et il a démontré :

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} := \sum_1^\infty \tau(n) q^n$$

Remarque : l'inverse de $\prod (1 - q^n)$ est

$$\prod_{m \geq 1} (1 - q^m)^{-1} = \sum_0^\infty p(n) q^n$$

fonction de partition ($n = m_1 + \dots + m_r$)

Ramanujan (avec Hardy) a obtenu les

des résultats spectaculaires sur $p(n)$ et il a conjecturé entre autres :

(1) $\quad \tau(mn) = \tau(m)\,\tau(n), \quad (m,n)=1$

(2) $\quad \tau(p) = O(p^{\frac{11}{2}})$, p entier.

Le premier résultat a été démontré par Mordell ( ) et Hecke (~193). Le second par Deligne (conjecture de Weil, 1973). Remarquer que pour (2) la construction de Δ donne

$$\tau(n) = O(n^{10+\varepsilon}).$$

Une argument plus fin de Hecke donne "élementairement"

$$\tau(n) = O(n^{6}). \qquad (6 = \tfrac{k}{2}).$$

Pour Γ fixé on peut "compter" les formes paraboliques de poids k. Par exemple pour $SL(2,\mathbb{Z})$ on a pour k pair ≥ 12

$k \equiv$	0	2	4	6	8	10	[12]
$\dim S_k =$	$\frac{k}{12}$	1					

$$\dim S_k = \left[\frac{k}{12}\right] - 1 \qquad k \equiv 2 \quad [6]$$

$$\left[\frac{k}{12}\right] \qquad k \not\equiv 2 \quad [6]$$

Pour tout Γ, $\dim S_k \sim c\,k$, $c>0$. $(c = c_\Gamma !)$

4. Les opérateurs de Hecke.

Je considère tout d'abord $SL(2,\mathbb{Z})$, de sorte qu'une forme modulaire est donnée par

$$f(z) = \sum_0^\infty a_n q^n.$$

Hecke (vers) a découvert une famille remarquable d'opérateurs arithmétiques qui sont sur M_k.

① Définition combinatoire.

Pour $f \in M_k$, p premier, on pose

$$T_k(p) f(z) = p^{k-1} f(pz) + \sum_{b \bmod p} p^{-1} f\left(\frac{z+b}{p}\right).$$

Notez qu'il y a un facteur de normalisation arbitraire. La somme

$$\sum_b f\left(\frac{z+b}{p}\right)$$

implique que $f(z+1) = f(z) \Rightarrow T_k(p) f(z+1) = T_k(p) f(z)$. L'invariance par $SL(2,\mathbb{Z})$ - i.e. par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ car cet élément, avec Γ_∞, engendre Γ - n'est pas évidente! On définit de façon analogue $T_k(n)$.

On vérifie les faits suivants :

(1) $T_k(n)$ et $T_k(m)$ commutent si $(n, m) = 1$

(2) $T_k(n)$ préserve les formes à coeff. entiers (ou rationnels).

② Définition géométrique.

Notons que $T_R(p)$ est "de degré $(p+1)$" ($p+1$ termes). Par ailleurs

$$\begin{array}{ccc} SL(2,\mathbb{Z}) & \twoheadrightarrow & SL(2,\mathbb{F}_p) \quad \text{(exercice!)} \\ \cup & & \\ \Gamma_0(p) & \twoheadrightarrow & \begin{pmatrix} * & * \\ & * \end{pmatrix} \end{array}$$

On a donc $SL(2,\mathbb{Z})/\Gamma_0(p) \cong \mathbb{P}^1(\mathbb{F}_p)$, card. $p+1$. Notons Y_{Γ} la courbe $\Gamma_0(\Gamma) \backslash \mathcal{H}$. On a alors

$$\begin{array}{c} Y_p = \Gamma_0(p) \backslash \mathcal{H} \\ \downarrow \\ Y_1 \end{array}$$

Mais il y a une autre application moins évidente. On a

$$\begin{pmatrix} p & \\ & 1 \end{pmatrix} \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \begin{pmatrix} p^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} a & pb \\ c & d \end{pmatrix} \begin{pmatrix} p^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} a & pa \\ c & d \end{pmatrix}.$$

Si $\tau = \begin{pmatrix} p & \\ & 1 \end{pmatrix}$ on a donc $\tau \Gamma_0(p) \tau^{-1} \subset \Gamma(1)$.

Si $\gamma \in \Gamma_0(p)$ on a donc $\tau \gamma z = (\tau \gamma \tau^{-1}) \tau z$, avec $\tau \gamma \tau^{-1} \in \Gamma(1)$

donc $z \mapsto \tau z$ passe au quotient $\Gamma_0(p) \backslash \mathcal{H} \to Y_1$.

On a donc deux flèches, de degré $(p+1)$:

$$(*) \qquad \begin{array}{ccccc} & & Y_p & & \\ & \swarrow^{\mathrm{can}} & & \searrow^{[\tau]} & \\ Y_1 & & & & Y_1 \end{array}$$

Soit donc, par exemple, $\omega \in S_2$ une différentielle sur Y_1. Alors $\mathrm{can}^*\omega$ est une différentielle sur Y_p et $\tau_* \mathrm{can}^*\omega$ est une ... sur Y_1. Il en est de même si $\omega = f(z)(dz)^{k/2}$ où $f \in S_k$. Ceci donne une expression géométrique des T_p.

Remarque: Si Y_1 est remplacé par Y_N et $(p,N)=1$ on a de même

$$\begin{array}{ccccc} & & Y_{pN} & & \\ & \swarrow^{\mathrm{can}} & & \searrow^{[\tau]} & \\ Y_N & & & & Y_N \end{array}$$

— prendre le produit fibré de $(*)$ avec $\begin{array}{c} Y_N \\ \downarrow \\ Y_1 \end{array}$. En général T_n a une définition ambiguë si $(n,N) = 1$.

Théorème (Hecke)

(1) Les T_n (pour $(n,N)=1$) forment une famille commutative d'opérateurs semi-simples dans $S_k(\Gamma_0(N))$.

(2) $f \in S_k$ est uniquement définie par les valeurs propres des T_n (n,N)

Itecke a démontré (2) pour $SL(2,\mathbb{Z})$ mais, avec une formulation calculable, c'est en fait vrai pour tout N.

(leçon 3, Clozel)

3. Les représentations galoisiennes associées aux formes modulaires.

1. Enoncé du théorème.

On se place dans le cadre de la leçon 2: on a vu que $S_k(N)$ possède une famille commutative d'opérateurs de Hecke $T_k(p) := T_p$. On se restreint aux p tels que $(p, N) = 1$. Les T_p sont autoadjoints, commutent entre eux donc simultanément diagonalisables.

Une forme $f \in S_k(N)$ a une "q-expansion":

$$f(z) = \sum_1^\infty a_n q^n. \tag{1.1}$$

On vérifie que $S_k(N)$ a une base $(f_i)_{i \in I}$ composée de formes à coefficients rationnels, en fait entiers [voir un argument plus loin]. On a vu que l'action de T_p s'exprimait simplement (en théorie) en fonction de (1.1). En particulier

T_p préserve $S_k(N, \mathbb{Q}) \subset S_k(N)$. Il en résulte que

> $S_k(N)$ a une base formée de formes propres f dont les coefficients appartiennent à un corps de nombres $L(f)$.

Si f est forme propre, on vérifie que $a_1 \neq 0$. D'après la formule pour T_p, on a donc

$$\lambda_p = a_p .$$

Exemple: $f = \Delta$ (poids 12): $L = \mathbb{Q}$.

Soit f, $L = L(f)$ on choisit sur une fois pour toutes une place λ de L (= un idéal premier de $\mathcal{O}_L$). On a donc le corps ℓ-adique L_λ. (si $\gamma_S \subset \mathcal{O}_L$ contient $\ell \mathcal{O}_L$, c'est une extension de $\mathbb{Q}_\ell$). Les coefficients de f sont dans $L \subset L_\lambda$.

Théorème 1 - Pour tout λ, il existe une représentation de dimension 2

$$r_\lambda : G_{\mathbb{Q}} \longrightarrow GL(2, L_\lambda)$$

telle que

(i) r_λ est non-ramifiée en dehors de $S = \ell \cup \{p \mid N\}$. Donc $r_\lambda : G_S \to GL(2, L_\lambda)$

(ii) Pour tout $p \notin \ell N$,

$$\operatorname{trace} r_\lambda(\mathrm{Frob}_p) = a_p$$
$$\det r_\lambda(\mathrm{Frob}_p) = p^{k-1}.$$

Ce théorème est dû à Eichler en théorie (variantes antérieures : Kronecker, Weber).

Remarque : On en sait beaucoup plus : Notons que le polynôme caractéristique de Frob_p est

$$X^2 - a_p X + p^{k-1} = 0.$$

On vérifie en fait que les deux racines (α_p, β_p) (qui sont donc quadratiques sur $\mathbb{Q}$, donc algébriques) vérifient

$$|\alpha_p| = |\beta_p| = p^{\frac{k-1}{2}}.$$

C'est la généralisation à $\mathbb{Q}$ de la conjecture de Ramanujan (le cas $k=2$, pour Δ).

• Par ailleurs :

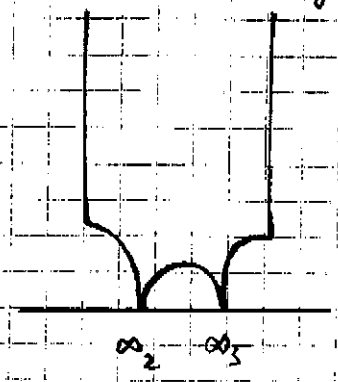
§ La représentation ρ_λ est irréductible.

2. Le cas $k=2$: réduction à la relation de congruence.

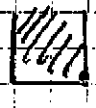
Dans tous les cas, la démonstration repose sur l'action des opérateurs de Hecke sur la cohomologie des courbes modulaires (la cohomologie étale de Grothendieck). On va l'esquisser pour $k=2$.

Soit $Y = Y(N) = \Gamma_0(N) \backslash \mathfrak{h}$. Pour $N=1$, on a vu comment compactifier $Y(1) \to \mathbb{P}^1$. Il y a une compactification naturelle aussi pour $Y(N)$. Géométriquement, on a un domaine

Fondamental de type



Les 3 pointes sont toutes (après une homographie) au voisinage de ∞ du type



---

que l'on complète comme pour $X(1)$ (à un d'un peu)

Soit $X(N) = Y(N) \cup \{\text{pointes}\}$

= courbe compacte lisse

On vérifie (pour ceci il faut essentiellement utiliser que $Y(1)$ classifie les courbes elliptiques ...)

$X(N)$ est naturellement définie sur $\mathbb{Q}$.

Remarque: Maintenant on peut comprendre la notion de la q-expansion ($k=2$): $\omega = f\,dz$ est une forme différentielle, que l'on suppose déf / $\mathbb{Q}$. Il suffit de vérifier que q est un paramètre local sur $\mathbb{Q}$.

Revenons à $X = X(N)_{\mathbb{C}}$ = surface de Riemann.

On a vu que

$S_2(N) = \{$ diff. holomorphes sur $X \}$

$= \Gamma(\Omega^1(X)) = \Omega^1(X)$.

On a la relation de Riemann :

$H^1(X, \mathbb{C}) = H^1_{\text{sing}}(X, \mathbb{Q}) \otimes \mathbb{C} \cong \Omega^1(X) \oplus \overline{\Omega^1(X)}$.

(théorie de Hodge : $H^1 = H^{1,0} \oplus H^{0,1}$).

Donc :

$H^1(X, \mathbb{C}) = S_2(N) \oplus \overline{S_2(N)}$

formes antiholomorphes de poids 2.

NB : C'est au vu de cette décomposition qui va fractionner les représentations de dimension 2.

Considérons donc $X = X(N)/\mathbb{Q}$. Shimura a expliqué qu'il y avait une notion de bonne réduction pour les variétés algébriques. On montre :

$X(N)$ a bonne réduction pour tout $p \nmid N$.

Autrement dit :

(1) $X(N)$ est naturellement définie sur $\mathbb{Z}[\frac{1}{N}]$

(2) $\mathbb{Z}[\frac{1}{N}] \to \mathbb{F}_p$ $(p \nmid N)$, d'où une courbe X_p définie sur $\mathbb{F}_p$. C'est une courbe lisse (complète, géométriquement irréductible).

D'après Grothendieck, on sait dans cet exercice pour tout ℓ la cohomologie étale

$$H^1_{et}(X \times \bar{\mathbb{Q}}, \mathbb{Q}_\ell) = H_\ell \quad \begin{pmatrix} \mathbb{Q}_\ell\text{-e.v.} \\ \text{de dim. finie} \end{pmatrix}$$

Faits :

① Les opérateurs de Hecke $(p \nmid N)$ opèrent par des correspondances définies sur $\mathbb{Q}$

② $G_{\mathbb{Q}}$ opère sur H_ℓ. Il commute alors avec les opérateurs de Hecke.

③ On a

$$H^1_{\text{Betti}}(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_\ell = H^1_{et}(X \times \bar{\mathbb{Q}}, \mathbb{Q}_\ell)$$

(isomorphisme canonique), bien sûr compatible aux T_p.

On va maintenant faire l'hypothèse fondamentale

Hypothèse - La famille de valeurs propres (a_p) intervient avec multiplicité 1 dans $S_2(N)$.

...

Alors (a_p) décrit un espace de dimension 2 dans $H^1(X(\mathbb{C}), \bar{\mathbb{Q}})$ ↖ en L, L assez grand.

[Démonstration : f donne $\bar{f}$, avec v.p. $(\bar{a_p})$. Mais S_2 def $/\mathbb{Q} \Rightarrow$ il existe aussi f^c (action sur les coefficients), $f^c \in S_2$! Alors $\bar{f}^c$ donne (a_p)].

Pour L_λ corresp. à ρ_ℓ, on voit donc que (a_p) décrit un sous-espace V de dimension 2 dans $H^1_{et}(X \times \bar{\mathbb{Q}}, L_\lambda)$, sur lequel agit $G_{\mathbb{Q}}$.

De plus la formule inductive implique que $G_{\mathbb{Q}}$ agit par G_S, $S = \ell \cup \{q \mid N\}$. Le Théorème 1 sera donc démontré si on prouve:

Le polynôme caractéristique de Frob_p dans V est $X^2 - a_p X + p = 0$.

("relation de congruence")

3. "Démonstration" de la relation de congruence

On considère maintenant la courbe $X / \mathbb{F}_p$. On dispose toujours sur X de la correspondance géométrique T_p. On a aussi l'endomorphisme de Frobenius: $X \in \mathbb{P}^N$ est définie par des équations à coeff. dans $\mathbb{F}_p$ et

$$\varphi_p \quad (x_i) \mapsto (x_i^p)$$

préserve donc X.

Par ailleurs on a un théorème de comparaison:

$$H^1_{et}(X \times \bar{\mathbb{Q}}, L_\lambda) = H^1_{et}(X \times \bar{\mathbb{F}}_p, L_\lambda)$$

compatible avec Frob_p ↑ et φ_p ↑

(Cas élémentaire). Pour que le théorème de gauche ait de bonnes propriétés il faut faire certaines suppositions

$\ell \neq p$

. Par ailleurs T_p agit toujours sur $H^*(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$ en L_2.

. Enfin on a un troisième opérateur, le transposé de Frobenius. On peut penser à φ_p comme à une correspondance, i.e.

$$\varphi_p = (x, x^p) \subset X \times X$$

(d'où $C \to X$) et le transposé est obtenu en échangeant les deux flèches : $C \to X$ (par x^p), $C \to X$ (par x). Notons que le degré de la flèche de gauche est p.

. Propriétés fondamentales

(1) $\quad \varphi_p {}^t\varphi_p = [p] \quad (\text{sur } H^*)$

Démonstration : Comme deux cycles finis, $C \to X$, $C' \to X$, consiste à prendre le produit fibré $C \to X \to X \leftarrow C'$ "au milieu". Ici on a $X \to X^p \leftarrow X$.

Le produit fibré est $(x, y : x^p = y^p)$. L'équation locale (carte affine) est $(x-y)^p = 0$, donc on obtient

p fait la dichotomie $\Delta = (2, x)$. La dichotomie agit transitivement, et $p\Delta$ fixe $[p]$.

② (Kronecker, Weber, Eichler-Shimura):

On a $T_p = \varphi_p + {}^t\varphi_p$.

(égalité de correspondances sur X — il y a une notion naturelle de somme de correspondances).

En termes classiques, ceci s'appelle "la relation modulaire p de l'équation modulaire". Pour $X(1)$ on la trouve dans l'Algèbre de Weber; pour X on l'a déduite par produit fini...

[TRANSPARENT].

Corollaire: Après extension des scalaires à $\mathbb{L}_\lambda$, on a sur V:

$$\begin{cases} \varphi_p + {}^t\varphi_p = a_p \\ \varphi_p \, {}^t\varphi_p = p \end{cases}$$

d'où $\varphi_p^2 - a_p \varphi_p + p = 0$, QED.

La démonstration modulaire de ② fait, de nouveau, appel à la description de $X = X(n)$ comme module de courbe elliptique.

LEHRBUCH

DER

ALGEBRA

VON

HEINRICH WEBER

PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT STRASSBURG

DRITTER BAND

CHELSEA PUBLISHING COMPANY
NEW YORK, N. Y.

Hierdurch ist die Lösung der Invariantengleichung $F_n = 0$ auf die successive Lösung solcher Fälle zurückgeführt, in denen n eine Primzahl ist.

6. Während bei der Ableitung der Transformationsgleichungen aus den Teilungsgleichungen von Haus aus feststeht, daß die numerischen Koeffizienten in diesen Gleichungen rationale Zahlen sind, so lehrt uns die zweite Ableitung zunächst nichts über die Zahlenkoeffizienten. Wir können aber nachträglich beweisen, daß diese Koeffizienten nicht nur rationale, sondern auch ganze Zahlen sind und gelangen zugleich zu einem wichtigen Satz über die Teilbarkeit dieser Koeffizienten.

Wenn wir beweisen können, daß, wenn p eine Primzahl ist, die Koeffizienten in $F_p(x, y)$ ganze Zahlen sind, so folgt das Gleiche aus 4. und 5. für jedes zusammengesetzte n.

Nach (4) ist $j(\omega)$ in eine Reihe von der Form entwickelbar

$$j(\omega) = q^{-2} \sum_{0,\infty}^{h} a_h q^{2h}, \tag{25}$$

deren Koeffizienten a_h ganze Zahlen sind, und zwar $a_0 = 1$.

Bilden wir hiervon, wenn p eine Primzahl ist, die $p$te Potenz, und beachten den für jede ganze Zahl gültigen Fermatschen Satz:

$$a^p \equiv a \pmod{p},$$

so folgt

$$j(\omega)^p = q^{-2p} \sum_{0,\infty}^{h} a_h q^{2hp} + p\, q^{-2(p-1)} \sum_{0,\infty}^{h} b_h q^{2h}, \tag{26}$$

worin b_h ebenfalls ganze Zahlen sind. Andererseits ist, wenn man in (25) ω durch $p\omega$ ersetzt:

$$j(p\omega) = q^{-2p} \sum_{0,\infty}^{h} a_h q^{2hp} \tag{27}$$

und daraus, wenn man

$$j(\omega) = u, \quad j(p\omega) = v$$

setzt:

$$u^p - v = p\, q^{-2(p-1)} \sum_{0,\infty}^{h} b_h q^{2h},$$

wofür wir auch schreiben können:

$$(u^p - v)(u - v^p) = p\, q^{-2(p^2+p-1)} \sum_{0,\infty}^{h} c_h q^{2h}, \tag{28}$$

wenn c_h ein drittes System ganzer Zahlen bedeutet.

Nun kommen in $F_p(x, y)$ die in bezug auf x, y höchsten Glieder $x^{p+1} + y^{p+1}$ vor, und wir setzen demnach

$$F_p(x, y) = (x^p - y)(x - y^p) - \sum_{0,p}^{h,k} c_{h,k} x^h y^k, \tag{29}$$

worin $c_{h,k}$ die zu bestimmenden Koeffizienten sind, die nach 3. der Bedingung

$$c_{h,k} = c_{k,h}$$

genügen. Um sie zu bestimmen, setzen wir in (29)

$$x = u, \quad y = v,$$

wodurch F_p verschwindet, und erhalten

$$(30) \qquad (u^p - v)(u - v^p) = \sum_{0,0}^{h,k} c_{h,k} u^h v^k.$$

Hieraus folgt zunächst, daß

$$c_{p,p} = 0$$

sein muß, da nach (28) bei der Entwickelung (der linken Seite) nach Potenzen von q die Potenz $q^{-2(p^2+p)}$ nicht vorkommen kann, und wir können (29) jetzt in die Form setzen:

$$(31) \qquad (u^p - v)(u - v^p) = \sum_{0,p}^{h} \sum_{0,h-1}^{k} c_{h,k}(u^h v^k + u^k v^h) + \sum_{0,p-1}^{h} c_{h,h} u^h v^h.$$

Hierin sind die aus (25) und (27) sich ergebenden Entwickelungen von

$$u^h v^k + u^k v^h, \quad u^h v^h$$

nach Potenzen von q einzusetzen, deren Anfangsglieder

$$q^{-2(hp+k)}, \quad q^{-2h(p+1)}$$

die Koeffizienten 1 haben.

Auf der rechten Seite von (31) kommen nicht zwei Glieder vor, deren Entwickelung mit derselben Potenz von q beginnt, denn aus

$$hp + k = h'p + k'$$

folgt $k \equiv k' \pmod{p}$ und mithin, da k und $k' < p$ sind, $k = k'$, $h = h'$.

Ordnet man daher die Reihen, welche die beiden Seiten von (31) darstellen, nach aufsteigenden Potenzen von q, und setzt dann die Koeffizienten gleich hoher Potenzen einander gleich, so erhält man eine Reihe linearer Gleichungen für die Unbekannten $c_{h,k}$, von denen jede folgende nur eine neue Unbekannte enthält, und diese mit dem Koeffizienten 1. Die aus der linken Seite sich ergebenden bekannten Glieder dieser Gleichungen sind nach (28) lauter durch p teilbare ganze Zahlen, und es ergeben sich also für die $c_{h,k}$ ebenfalls ganzzahlige, durch p teilbare Zahlwerte. Demnach haben wir

$$(32) \qquad F_p(x, y) = (x^p - y)(x - y^p) - p \sum_{0,0}^{h,k} a_{h,k} x^h y^k,$$

. Ramanujan ($k=2$).

La relation ci-dessus montre que les valeurs propres (α, β) de Fr_p vérifient l'équation.

Mais d'après Weil on sait que ce sont des nombres algébriques tels que $|\alpha| = |\beta| = p^{1/2}$.

On a donc $a_p = \alpha + \beta$, $|\alpha| = |\beta| = p^{1/2}$, d'où la conjecture de Ramanujan.

2. Correction, et un mystère.

① J'ai fait l'hypothèse de multiplicité 1, qui n'est pas toujours vérifiée. Par exemple: $N|M$, $X_N \xrightarrow{\pi} X_M$, $V \to \pi^* V$ ($\hat{m}$ valeurs propres de T_p, $p \nmid N$) et $\pi^* V$ est de dimension $\geq$ quelque. En négligeant quelques cycles "de niveau divisant N", l'argument de multiplicité 1 reste correct.

② On connaît maintenant $R_\lambda(\mathrm{Frob}_p)$ — on plutôt sa trace. Par Čebotarev on connaît donc R_λ sur tout $G_{\mathbb{Q}_p}$ (G_S) et donc aussi $R_\lambda|_{G_p}$ pour $p \mid N$. (Dirac, $p \neq \ell$). Quelle est cette représentation? La réponse générale repose sur une idée très profonde de Langlands (Fréchet exposé)!

(Leçon 1) (Clément)

Formes automorphes adéliques et cohomologie des courbes modulaires

Rappel Clozel a introduit $\rho_{f,\lambda} : G_{\mathbb{Q},S} \longrightarrow GL_2(\bar{\mathbb{Q}}_\ell)$, $S = \{\ell, \text{ premiers de niveau de } f\}$

caractérisé par $\mathrm{tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p(f) \quad \forall p \notin S$. f propre

il y a aussi une relation, nettement plus fine, entre f et $\rho_{f,\lambda} \mid G_{\mathbb{Q}_p}$ si $p \neq \ell \in S$. La théorie des op. de Hecke est trop complexe dans ce cas et on a besoin de formuler les choses en terme de rep.

(1) Adélisation

- Soit $\mathcal{P}$ l'ensemble des places de $\mathbb{Q} = \{\infty, 2, 3, \dots, p \text{ premier}, \dots\}$.
  $v \in \mathcal{P} \rightsquigarrow \mathbb{Q}_v$ = la complétion associée $= \begin{cases} \mathbb{R} = \mathbb{Q}_\infty \\ \mathbb{Q}_p \text{ si } v = p \text{ premier.} \end{cases}$
- adèles $\mathbb{A} \subset \prod_{v \in \mathcal{P}} \mathbb{Q}_v$ sous-anneau des $(x_v) \mid x_v \in \mathbb{Z}_v$ pp.t. v.
  il contient $\mathbb{Q}$ par $x \longmapsto (x_v = x)_v$ $(\forall_v)$ diagonalement
  anneau top, base v. de $0 = \{\prod_v \Omega_v, \ \Omega_v \text{ ouvert de } 0 \text{ ds } \mathbb{Q}_v, \ \Omega_v = \mathbb{Z}_v \text{ pp.t.v}\}$
  $\rightsquigarrow$ localement compact.
- de plus $\mathbb{Q}$ discret dans $\mathbb{A}$: $\mathbb{Q} \cap \left(]-\frac{1}{2}, \frac{1}{2}[\times \prod_v \mathbb{Z}_v\right) = \{0\}$.
  $\rightsquigarrow$ analogue de $\mathbb{Z}$ dans $\mathbb{R}$. (ex: $\mathbb{A}/\mathbb{Q}$ compact) $\prod_{v \notin P_f} \mathbb{Z}_v$

$\|$ c'est le cadre naturel pour de nombreux énoncés en arithmétique.
(Chevalley, Weil, Nasse...)

$GL_2(\mathbb{A}) \subset \prod GL_2(\mathbb{Q}_v)$ ss groupe des $(g_v) \mid g_v \in GL_2(\mathbb{Z}_p)$ pp.t. v
même idem, top. naturelle $\rightsquigarrow$ localement compact
et $GL_2(\mathbb{Q}) \subset GL_2(\mathbb{A})$ diag discret "réseau"

Lemme
(i) $GL_2(\mathbb{Q}_p) = GL_2(\mathbb{Z}[\frac{1}{p}])\ GL_2(\mathbb{Z}_p)$
(ii) $GL_2(\mathbb{A}) = GL_2(\mathbb{Q})\ (GL_2(\mathbb{R})^+ \times GL_2(\hat{\mathbb{Z}}))$
(iii) (approx faible) si $K \subset GL_2(\hat{\mathbb{Z}})$ ss groupe ouvert $\mid \det(K) = \hat{\mathbb{Z}}^\times$
alors $GL_2(\mathbb{A}) = GL_2(\mathbb{Q})\ (GL_2(\mathbb{R})^+ \times K)$

Preuve (i) B = matrice Δ sup de Gl_2

$Gl_2(\mathbb{Q}_p) = B(\mathbb{Q}_p)\, Gl_2(\mathbb{Z}_p)$, $B(\mathbb{Z}[\frac{1}{p}])\, B(\mathbb{Z}_p) = B(\mathbb{Q}_p)$ (facile)

$(\mathbb{P}^1(\mathbb{Q}_p) = \mathbb{P}^1(\mathbb{Z}_p))$

(ii) immédiat par le (i)

(iii) découle de (ii) et de ce que $SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$ $\forall N \geq 1$. □

(2) On va étudier $Gl_2(\mathbb{Q}) \backslash Gl_2(\mathbb{A}) /$ (courbes modulaires vs quotients adéliques)

Soit $K \subset Gl_2(\mathbb{A}_f) = \prod_p{}' Gl_2(\mathbb{Q}_p)$ un sous-groupe compact ouvert

le groupe $\Gamma_K := K \cap Gl_2(\mathbb{Q})^+$ est un ss g. discret de $Gl_2(\mathbb{R})$

commensurable à $SL_2(\mathbb{Z})$ "ss g. congruence"

ex: $K = K_0(N) = \{ (g_p) \in Gl_2(\hat{\mathbb{Z}}) \mid \forall p \mid N \quad g_p \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \}$.

alors $\Gamma_K = \Gamma_0(N)$

Cette notion un peu plus générale que la notion usuelle permet la construction utile suivante.

K comme plus haut, $Y_K := Gl_2(\mathbb{Q}) \backslash Gl_2(\mathbb{A}) / (SO_2(\mathbb{R}) \cdot \mathbb{R}_+^\times \times K) \underset{\det K = \hat{\mathbb{Z}}^\times}{=} Gl_2(\mathbb{R})^+ \backslash Gl_2(\mathbb{A}_f) / K \simeq \Gamma_K \backslash \mathcal{H}$

$$\boxed{Y_K = \Gamma_K \backslash \mathcal{H}}$$

↓ autre écriture de la courbe mod Y_K.

On la compactifie de manière usuelle $X_K = \mathcal{H}^* / \Gamma_K \amalg \mathbb{P}^1(\mathbb{Q})$

on s'intéresse à $H^1(X_K, \mathbb{Q})$ (ou $H_1(X_K, \mathbb{Q})$) quand K varie.

si $K \subset K'$, $X_K \twoheadrightarrow X_{K'}$ revêt. $H^1(X_{K'}, \mathbb{Q}) \hookrightarrow H^1(X_K, \mathbb{Q})$

on pose $$\boxed{H^1(\tilde{X}, \mathbb{Q}) := \varinjlim_K H^1(X_K, \mathbb{Q})}$$

Rq: c'est aussi la limite des $H^1(\Gamma(m) \backslash \mathcal{H}^*, \mathbb{Q})$! mais on attrape gratuitement une action de $Gl_2(\mathbb{A}_f)$ par translation à droite

$g \in Gl_2(\mathbb{A}_f)$, $Rg: X_K \to Y_{g^{-1}Kg}$. (isom.)

on obtient donc une rep. de $GL_2(\mathbb{A}_f)$ sur $H^1(\tilde{X}, \mathbb{Q})$!

Def: une rep V de $G = GL_2(\mathbb{A}_f)$ ou $G(\mathbb{Q}_p)$ (gp. localement prof.) est dite

- lisse si $V = \bigcup_{K \subset G} V^K$ (ssgp. compact ouvert)
- admissible si V^K de dim. finie $\forall$ K ssgp. compact. ouvert.

Prop: $H^1(\tilde{X}, \mathbb{Q})$ est lisse admissible. $H^1(\tilde{X}, \mathbb{Q})^K = H^1(X_K, \mathbb{Q})$.

Ce que l'on a fait avec H^1_{betti} peut être fait avec le $H^0(X_K, \Omega^1)$ "$S_2(\Gamma_K)$"

$H^0(\tilde{X}, \Omega^1)$ est simplement l'espace de formes mod. de poids 2 qui sont paraboliques. $\subset GL_2(\mathbb{A}_f)$. On peut la voir comme suit: si $f \in S_2(\Gamma_K)$ $\rightsquigarrow$ $\tilde{f} : GL_2(\mathbb{R})^+ \longrightarrow \mathbb{C}$ $\tilde{f}(g) = f(g(i))j(g,i)$ (Γ_K)

puis $\rightsquigarrow$ $\widetilde{\tilde{f}} : GL_2(\mathbb{A}) \longrightarrow \mathbb{C}$ par $\widetilde{\tilde{f}}(\gamma g \kappa) = \tilde{f}(g)$ ($\det K = \hat{\mathbb{Z}}^\times$, $GL_2(\mathbb{Q})$) — approx faible

Prop: $H^0(\tilde{X}, \Omega^1) = \bigoplus_{f \text{ poids 2 niveau } /\sim} \Pi(f)$ avec mult. 1. (Π irred.)

- $H^1(\tilde{X}) = H^0(\tilde{X}, \Omega^1) \oplus \overline{H^0(\tilde{X}, \Omega^1)}$
- $H^1(\tilde{X}, \mathbb{Q}) \otimes \bar{\mathbb{Q}}_\ell = \bigoplus_f \Pi(f) \otimes \rho_{\Pi, \lambda}$ ($\bar{\mathbb{Q}} \xrightarrow{\lambda} \bar{\mathbb{Q}}_\ell$)

action de $G_{\mathbb{Q}}$ par f ; la rep. ass. à f.

car tout est déf / $\mathbb{Q}$

reformulation de ce qu'a expliqué Clozel.

Fait: tout Π irred. admissible de $GL_2(\mathbb{A}_f)$ est de la forme $\otimes' \Pi_p$, Π_p irred. adm. de $GL_2(\mathbb{Q}_p)$ univ. déf.

$\rightsquigarrow \Pi_p(f)$. $\forall p$ premier.

Le théorème suivant est une précision importante de celui d'Eichler et Shimura. aux "p | niveau".

Théorème si f propre de poids 2 et niveau N, $S = \{\ell, p | N\}$.

alors $\rho_{\pi_f} | G_{\mathbb{Q}_p} \simeq \mathcal{LL}(\pi_p(f))$ $\forall p \neq \ell$ (Deligne, Leyfelds, Carayol)

Rq poids k

(3) Correspondance de Langlands locale (très très très vite)

- fixons $\mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$ pour simplifier, p premier $\neq \ell$. c'est une bijection naturelle entre $n \geq 1$ entier

$$\left\{\begin{array}{l}\text{rep. complexe}\\ \text{lisses adm. irréd.}\\ \text{de } GL_n(\mathbb{Q}_p)/\simeq\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{l}\text{rep. continues } W_{\mathbb{Q}_p} \to GL_n(\bar{\mathbb{Q}}_\ell)\\ \text{"Frobenius ss"}\\ \text{(mais pas nec. irréd.)}\end{array}\right\}/\simeq$$

(dues à Harris Taylor (Langlands réel), $n=2$ Lafforgue, $n=3$ Henniart...)
(en première approche $W_{\mathbb{Q}_p} = G_{\mathbb{Q}_p}$...)

- $\bar{\mathbb{Q}}_p$ / $\mathbb{Q}_p^{nr}$ / $\mathbb{Q}_p$ — def := groupe d'inertie I (ou $I_{\mathbb{Q}_p}$)

$\mathbb{Q}_p^{nr}$ = "composé des ext. non ram.") galois de groupe $\simeq \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}} = \langle \mathrm{Frob} \rangle$

$\mathbb{Q}_p^{nr}$ explicite : c'est $\mathbb{Q}_p(\xi,\ \xi^m = 1,\ (m,p)=1)$.

I est aussi extension d'un groupe pro-cyclique ($\pi\mathbb{Z}_\ell$) par un pro-p-groupe ab. ans cyclique. $\ell \neq p$

($G_{\mathbb{Q}_p}$ pro résoluble)

def: $W_{\mathbb{Q}_p} \subset G_{\mathbb{Q}_p}$ est l'image inverse de $\mathbb{Z} \subset \hat{\mathbb{Z}}$, on décrète que $I_{\mathbb{Q}_p}$ est ouvert dans $W_{\mathbb{Q}_p}$.

- cas $n=1$ découle des cors de classes locale $\mathbb{Q}_p^{ab} = \mathbb{Q}_p^{cyclotomique}$

$W_{\mathbb{Q}_p}^{ab} \simeq \mathbb{Q}_p^*$: l'isomorphisme du c.d.c. local.

- en général, la corresp. est compatible à diverses opérations de deux côtés induction $\leftrightarrow$ somme directe.

de point le plus dur est le sous cas {supercuspidales} $\leftrightarrow$ {irréductibles}

- les supercusp. se caractérisent par le fait d'avoir des coeff. matriciels qui sont à support compact modulo le centre.

(Leçon 5, Vignéras)

Formes automorphes sur les groupes unitaires. Représentations galoisiennes.

1. Groupes unitaires arithmétiques.

Soit $E = \mathbb{Q}(i)$. Rappelons que $\mathcal{O}_E = \mathbb{Z}[i]$; le discriminant est -4. En particulier seul 2 est ramifié. Par ailleurs :

p impair $\Rightarrow$ $\begin{cases} p \text{ décomposé} & (p \equiv 1 \ [4]) \\ p \text{ inerte} & (p \equiv 3 \ [4]). \end{cases}$

On fixe n, et on considère une forme hermitienne (relativement à $E/\mathbb{Q}$) sur E^n :

$$h(z_1, \dots z_n) = \sum_1^{n-1} z_i \bar{z}_i - z_n \bar{z}_n.$$

Pour p inerte, h définit donc une forme hermitienne h_p sur E_p^n ($E_p = E \otimes \mathbb{Q}_p$ est un corps !), relativement à $E_p/\mathbb{Q}_p$.

Hypothèse – Pour tout p impair, inerte, h_p est maximalement isotrope. ($h(z,z) = 0$ pour z dans un sous-espace de dimension $[\frac{n}{2}]$.)

"A l'infini" (i.e. pour $\mathbb{R} \subset E \otimes \mathbb{R} = \mathbb{C}$) h définit une forme hermitienne ordinaire h_∞. On

a de plus :

| La signature de h_∞ est $\begin{pmatrix} \cdot & \\ (n-1,1) & \end{pmatrix}$

L'hypothèse pour p fini est équivalente à

$\delta = \mathrm{disc}(h) = (-1)^{\left[\frac{n}{2}\right]} \in \mathbb{Q}_p^\times$ est, à une norme près, celui de la forme hyperbolique : $\delta = (-1)^{\left[\frac{n}{2}\right]} \beta\bar{\beta}$ $(\beta \in E_p)$ $\forall p \equiv 3 \ [4]$

Mais p étant non ramifié, (-1) (et à fortiori 1) est une norme.

On considère le groupe G (attention ce n'est plus $G_{\mathbb{Q}}$!) défini sur $\mathbb{Q}$:

$$(*) \qquad G(\mathbb{Q}) = \{ g \in GL(n,E),\ h(gZ, gZ) \equiv h(Z,Z) \}$$

$(Z \in E^n)$. Donc $G(\mathbb{Q}) \subset GL(n,E)$. Alors

G est un groupe algébrique défini sur $\mathbb{Q}$, ie.

(1) G est un schéma sur $\mathbb{Q}$: $G(R)$ est défini par $(*)$ pour toute $\mathbb{Q}$-algèbre R ; remplacer E par $E \otimes R$

(2) En fait, G est une variété algébrique (affine) sur $\mathbb{Q}$.

. <u>Sous-groupes de congruence</u>.

On a $G(\mathbb{Q}) \subset GL(n,E) = (a_{ij})$. Soit

$\Gamma_E \subset GL(n, \mathcal{O}_E)$ un sous-groupe défini par

. Un idéal $\mathfrak{a} \subset \mathcal{O}_E$

. Des congruences $a_{ij} \equiv \alpha_{ij} \ [\mathfrak{a}]$

Alors $G(\mathbb{Q}) \cap \Gamma_E$ est par définition un sous-groupe de congruence de $G(\mathbb{Q})$.

. Groupes locaux.

. $G(\mathbb{R}) = U(1, n-1)$

. $G(\mathbb{Q}_p) \subset G'(E \otimes \mathbb{Q}_p) = GL_n(\mathbb{Q}_p)^2$
$\quad E \otimes \mathbb{Q}_p = \mathbb{Q}_p \times \mathbb{Q}_p$

si p se décompose dans A des deux puis la "conjugaison" est $(g_1, g_2) \mapsto ({}^t g_2^{-1}, {}^t g_1^{-1})$. En particulier $G(\mathbb{Q}_p) \cong GL_n(\mathbb{Q}_p)$

. Si $p \equiv 3$ [4] (ou $p=2$) G est un vrai groupe unitaire sur $\mathbb{Q}_p$. < 3.1 : ss-groupes compacts.

2. Action de $G(\mathbb{R})$ sur la boule unité. Formes modulaires ($\equiv$ automorphes).

Soit $g \in G(\mathbb{R})$, $g = \begin{pmatrix} A & b \\ c & d \end{pmatrix}$. On note maintenant z un élément de la boule unité B de $\mathbb{C}^{n-1}$:

$$z = \begin{pmatrix} z_1 \\ \vdots \\ z_{n-1} \end{pmatrix}, \quad \sum |z_i|^2 < 1.$$

Alors la formule

$$g.z = \left(\frac{Az + b}{c.z + d} \right)$$

définit une action de $G(\mathbb{R})$ sur B^{n-1}.

Exercice (1) Ecrire les relations vérifiées par A, b, c, d [NB : la matrice de h est $J = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$]. – Vérifier que B^{n-1} est conservé.

Remarques : sous-groupes compacts maximaux :

. Si $p \equiv 1$, $GL(n, \mathbb{Q}_p) \supset GL(n, \mathbb{Z}_p)$

. Si $p \equiv 3$, $G(\mathbb{Q}_p)$ a un "bon" sous-groupe compact maximal K_p. (Par exemple, $K_p / \mathbb{Z}_p$ est $\bar{K}_p$ = groupe sur $\mathbb{F}_p$ est $U(n, \mathbb{F}_p)$...)

[Car: G agit sur $\mathbb{C}^n$, donc sur $\mathbb{P}^n\mathbb{C}$.
Mais B^{n+1} est donné par $\sum_1^{n+1} |z_i|^2 < 1$
$\Leftrightarrow \quad R(Z,Z) < 0, \quad Z = (z_1, \dots z_{n-1}, 1)$]

. L'espace des formes différentielles holomorphes Ω^1 sur B est l'espace des sections d'un fibré de dimension n, base locale $dz_1, \dots dz_n$. En particulier les fonctions holomorphes sont à des "facteurs". En regarde on plus considère $\underline{\omega} = \Lambda^n \Omega^1 =$ espace des n-formes holomorphes: c'est un fibré en droites. Par ailleurs

$$j(g,z) = cz + d \in \mathbb{C}^\times$$

est un facteur d'automorphie: il vérifie la formule de cocycle du § 2.3:

$$j(gh, z) = j(g, hz)\, j(h, z).$$

Alors $dz_1 \wedge \dots \wedge dz_{n-1} \circ g = j(g,z)^{-(n+1)} \underset{(\det g)}{\lambda}\, dz_1 \wedge \dots dz_{n-1}$

($g \in \mathcal{C}(\mathbb{R})$, action naturelle sur les formes différentielles).

Définition — Une forme modulaire scalaire de poids k sur $\mathcal{B}$, pour un groupe de congruences $\Gamma \subset G(\mathbb{Q}) \subset G(\mathbb{R})$, est une fonction $f : \mathcal{B} \to \mathbb{C}$ vérifiant

$$f(\gamma z) = (\det \gamma)^{-k} j(\gamma, z)^{k} f(z)$$

$(z \in \mathcal{B},\ \gamma \in \Gamma)$

C'est donc une section de $\otimes^k \omega$ sur la variété quotient $\Gamma \backslash \mathcal{B}$. Notons que Γ agit "proprement discontinûment sans point fixe", donc le quotient est bien défini.

Remarque. — Pour un groupe de congruence "assez petit" on a $\det \gamma = 1$. On peut donc essentiellement négliger ce terme. Le plus souvent on va en fait s'intéresser aux poids $k = 1$: sections de ω.

. Formes paraboliques.

Comme $GL(2)$ notre groupe est un compact (au sens arithmétique : il est discret).

La forme h a un pôle sur $\mathcal{B}$: $W = (e_{n-1}, e_n) : z\bar{z} - w\bar{w}$ qui a une base formée de deux vecteurs (e, f) avec $(e,e) = 0$, $(e,f) = 1$, $(f,f) = 0$.

Dans la base $(e, e_1, \dots e_{n-2}, f)$ la matrice de h est

$$\begin{pmatrix} & & 1 \\ & \boxed{1_{n-2}} & \\ 1 & & \end{pmatrix}$$

et on peut considérer le groupe des transvections unitaires

$$N = \begin{pmatrix} 1 & u & \lambda \\ & \boxed{1} & v \\ & & 1 \end{pmatrix} \qquad (u \in E^n,\ u + {}^t\bar{v} = 0,\ \lambda + \bar{\lambda} + v\,{}^t\bar{v} = 0)$$

Noter que ceci a un sens sur $\mathbb{Q}$ ou $\mathbb{R}$. Comme le groupe est rationnellement défini, $N \cap \Gamma \backslash N(\mathbb{R})$ est compact et on peut considérer les formes f telles que

$$(!!) \qquad \int_{N \cap \Gamma \backslash N(\mathbb{R})} f(n z)\, dn = 0 \qquad (z \in B)$$

comme dans le cas de $GL_2(\mathbb{Z})$ (ceci n'a pas de sens avec les définitions précédentes car $j(\gamma, z) \neq 1$ pour $\gamma \in N \cap \Gamma$. Il faut choisir une <u>autre</u> réalisation de B où N "fixe l'∞" comme dans le cas de GL_2).

On définit ainsi les formes paraboliques.

<u>Notation</u>: $S_k(\Gamma)$ ou $S_k(\Gamma \backslash B^{n-1})$

3. Cohomologie des quotients arithmétiques.

Adélisation.

On procède comme pour $GL(2)$. On a

$$K_\infty \subset G(\mathbb{R}), \quad K_\infty = U(n-1) \times U(1)$$

et $$B^{n-1} = G(\mathbb{R})/K_\infty.$$

Le groupe $G(\mathbb{A}) = G(\mathbb{R}) \times G(\mathbb{A}_f)$ est bien défini et on considère

$$G(\mathbb{Q}) \backslash G(\mathbb{A}) / K_\infty := \tilde{X} = G(\mathbb{Q}) \backslash [G(\mathbb{A}_f) \times B]$$

La situation est analogue à celle de $GL(2)$ mais un peu plus compliquée car on n'a plus l'approximation forte. Soit $K \subset G(\mathbb{A}_f)$, sous-groupe compact.

$$K = \prod_p K_p \subset G(\mathbb{Q}_p)$$

(K_p maximal pour presque tout p de sorte que K est ouvert) Alors

- $X_K = \coprod_i \Gamma_i \backslash B^{n-1}$ (Γ_i congruence).
- $\tilde{X} \twoheadrightarrow X_K$, et $\tilde{X}$ est la "limite".

On peut considérer

$$H^{n-1}_!(X_K, \mathbb{C})$$

(image de la cohomologie à supports compacts dans la cohomologie)

d'où

$$\varinjlim H_!^{n-1}(X_K, \mathbb{C}) := H_!^{n-1}(\tilde{X}, \mathbb{C}).$$

Comme pour $GL(2)$, on obtient maintenant une représentation lisse et admissible de $G(\mathbb{A}_f)$.

Supposons $k=1$. Alors

$$S_{1,1}(K) = \bigoplus_i S_{i,1}(\Gamma_i)$$

s'injecte dans $H_!^{n-1}(X_K)$. [une n-forme holomorphe donne une classe de cohomologie.]

En fait $H_!^{n-1}$ a une décomposition de Hodge, et (comme pour GL_2) on a

$$S_1(K) \subset H_!^{0,n-1}$$

(généralisation du théorème d'Eichler-Shimura).

4. Cohomologie ... ible et représentations galoisiennes.

Tout d'abord, on vérifie que toutes nos variétés S_K sont en fait des variétés algébriques (quasi-projectives) définies sur $E = \mathbb{Q}(i)$. ("théorie des modèles canoniques"). Les morphismes $S_{K'} \to S_K$ ($K' \subset K$) ainsi que l'action de $G(\mathbb{A}_f)$ sont aussi définis sur E. Par conséquent

$H_!^{n-1}(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ est muni de deux actions, qui commutent, de $\mathrm{Gal}\,E$ et de $G(\mathbb{A}_f)$.

Notons qu'on a toujours le isomorphisme de comparaison, au niveau fini :

$$H_!^{n-1}\left(X_K(\mathbb{C}), \mathbb{Q}\right) \otimes \mathbb{Q}_\ell$$

$$\| \quad (\text{étale})$$

$$H_!^{n-1}\left(X_{K,\bar{\mathbb{Q}}}, \mathbb{Q}_\ell\right)$$

et $H_!^{n-1}\left(X_K(\mathbb{C}), \mathbb{Q}\right) \otimes \mathbb{C}$ = cohomologie analytique rigidifiée.

Si on passe à la limite, il résulte de la théorie analytique des formes automorphes que

$$H_!^{n-1}\left(\tilde{X}, \mathbb{C}\right) = \bigoplus_{\pi_\infty} \pi \quad (\text{somme directe})$$

où $\{\pi\}$ = représentations irréductibles (complexes) de $G(\mathbb{A}_f)$. On en déduit — au moins en éliminant les scalaires — que

$$(*) \qquad H_!^{n-1}\left(\tilde{X}_{\bar{\mathbb{Q}}}, \bar{\mathbb{Q}}_\ell\right) = \bigoplus_{\pi} \pi$$

essentiellement sur la même π (si on veut, identifier $\mathbb{C}$ à $\bar{\mathbb{Q}}_\ell$ ...)

Si ρ (irréductible) est fixée, Gal_E opère alors sur $\bigoplus_{\pi_\infty \simeq \rho} \pi$ (NB : le problème de "multiplicité 1" déjà rencontré pour GL_2 intervient ici aussi).

La théorie de Langlands-Kottwitz permet de déterminer l'action de Gal_E sur l'espace, de dimension m_ρ, $\mathrm{Hom}\left(\rho, \bigoplus \pi\right) = \mathrm{Hom}\left(\rho, H_!^{n-1}\right)$

Voici le résultat précis qui nous servira.

Soit $\pi = \otimes \pi_v$ une représentation apparaissant dans le schéma (*). Soit $p \equiv 1 \ [\ell]$ de sorte que

. p se décompose en v, v'

. On choisit v, de sorte que $G(\mathbb{Q}_p)$ est identifié à $GL(n, \mathbb{Q}_p)$. Notons aussi que $G_v \subset G_E$ est identifié à $Gal(\overline{\mathbb{Q}}_p / \mathbb{Q}_p)$

. Supposons que π_p est une représentation supercuspidale de $G(\mathbb{Q}_p)$.

. Par ailleurs, soit $S \supset \{p, \infty\}$ un ensemble fini de premiers, et supposons que pour $q \notin S$, π_q a un vecteur fixe par "le" bon sous-groupe compact K_q.

Théorème. - (1) Il existe une extension finie L_λ de $\mathbb{Q}_\ell$, et une représentation R_λ de dimension n de Gal_E, unique mais déterminée par π, telle que l'action de Gal_E sur $Hom(\pi, H^{n-1}_!(\tilde{X}_{\overline{\mathbb{Q}}}, L_\lambda))$ soit, après semi-simplification, isomorphe à $\oplus^m R_\lambda$.

(2) De plus, $R_\lambda|_{G_v}$ est associée par la correspondance de Langlands à π_p.

(3) Enfin, R_λ est non ramifiée en toute place v divisant $p \notin \{\ell\} \cup S$.

Remarques:

(1) En particulier, R_λ est irréductible.

(2) Il y a deux types de multiplicités de π qui apparaissent. D'abord $n = \dim R_\lambda$, comme dans le cas de $GL(2)$. Ceci correspond aux types de Hodge possibles:

$$(0, n-1), (1, n-2), \ldots (n-1, 0).$$

↑ formes holomorphes

Ensuite une multiplicité "parasite" m, qui est sans doute égale à 1.

(3) J'ai énoncé le théorème sous une forme (vraie) qui résulte des travaux de:

Harris, Taylor,
Clozel, Harris, Labesse.
S.-W. Shin
Chenevier, Harris.

Mais la forme donnée ici ne se trouve pas dans la littérature. Pour la version (démontrée dans la littérature) utilisée par Chenevier, voir son papier.

5. Addendum : systèmes de coefficients.

J'ai énoncé le résultat concernant les formes "de poids 1" mais ceci ne suffira pas pour l'exposé final. Rappelons (§ 2) qu'on a plus généralement des formes de poids k.

Pour les formes de poids k, il faut considérer la représentation algébrique irréductible de $Gl_2(n)$ (ou $U(n,1)$) de plus haut poids

$$(k-1, \ldots k-1, (k-1)(1-k)).$$

soit V. Alors $\Gamma \backslash B^{n-1} \times V$ définit un système local $\mathcal{V}_k$ sur $\Gamma \backslash B^{n-1}$. ($\mathcal{V}_1$ est trivial!).

On obtient une famille compatible de systèmes locaux sur les X_K. Tout ce qui précède reste vrai, mais il faut considérer la cohomologie de ces systèmes locaux.

(leçon 6) (Abenener)

On se propose de démontrer le cas particulier suivant du théorème énoncé au cours 1.

Théorème (Ch, compositio '07)
Soit S un ens. fini de premiers $\supset \{2, p\}$ avec $p \equiv 1 \ (4)$.
Alors "l'"application naturelle $G_{\mathbb{Q}_p} \longrightarrow G_S$ est injective.

Autrement dit, $\mathbb{Q}_p \cdot \mathbb{Q}_S = \overline{\mathbb{Q}}_p$, soit encore
(*) $\forall$ $F/\mathbb{Q}_p$ finie, il existe un c.d.m $K \subset \mathbb{Q}_S$ et $\mathfrak{P} \mid p$ tel que $K_{\mathfrak{P}} \supset F$.

Remarque (*) appliquée à $F/\mathbb{Q}_p$ non ram dm, montre que $[K^{sal} : \mathbb{Q}]$ est divisible par n. "Il existe bcp de cdm de $\mathbb{Q}_S$"

Le reste de l'exp. est consacré à la preuve du thm. On commence par une première réduction. On dira que $F/\mathbb{Q}_p$ est bonne si elle galois finie et si son groupe de Galois admet une rep $\rho : Gal(F/\mathbb{Q}_p) \longrightarrow GL_n(\mathbb{C})$ irréd. et injective.

Lemme La composée des bonnes extensions est $\overline{\mathbb{Q}}_p$ tout entier.
(cela serait vrai $\forall$ k corps et k^{ab})

preuve si $F/\mathbb{Q}_p$ est galoisienne finie quelconque et si G est $Gal(F/\mathbb{Q}_p)$ considérons $\rho_1 \cdots \rho_n : G \to GL_{d_i}(\mathbb{C})$ ses rep. irréductibles (à isom près).
Par déf. $F_i = F^{\ker \rho_i}$ est bonne. De plus $F = F_1 \cdots F_n$.
car $\bigcap \ker \rho_i = Gal(F/F_1 \cdots F_n) = \{1\}$ ou $\bigoplus d_i \rho_i = \mathbb{C}(G)$ est fidèle !

Ca: il suffit de montrer (*) pour les $F/\mathbb{Q}_p$ bonnes.

Fixons $F/\mathbb{Q}_p$ une telle ext et $\rho : \mathrm{Gal}(F(\mathbb{Q}_p) \hookrightarrow \mathrm{Gln}(\mathbb{C})$ inj. ined.

$W_{\mathbb{Q}_p}$

donc il lui correspond une représentation lisse inéd. de $\mathrm{Gln}(\mathbb{Q}_p)$ qui est supercuspidale par Langlands local, notons la π_0.

On va "globaliser" π_0.

Soit G le groupe unitaire à n variables (relativement à $\mathbb{Q}(i)/\mathbb{Q}$) défini par Clozel.

Prop: Il existe une rep. automorphe cuspidale holomorphe de G, Π, telle que
(i) $\Pi_\ell^{G(\mathbb{Z}_\ell)} \neq 0$ si $\ell \neq 2, p$
(ii) $\Pi_p \simeq \pi_0$

c'est un résultat d'existence de rep. aut. avec conditions prescrites partout (sauf en 2 ici) qui n'est pas sans rappeler le pb initial. On verra plus tard que c'est un énoncé analytique!

Expliquons d'abord que la prop. $\Rightarrow$ théorème.

Considérons $\rho_{\Pi,2} : G_{\mathbb{Q}(i)} \to \mathrm{Gln}(\mathbb{Q}_2)$ une rep. 2-adique associée à Π comme dans l'exp. de Clozel.

par (i) et (ii) plus haut + la compat. à LL expliquée par Clozel

(i) $\rho_{\Pi,2}$ se factorise par $G_{\mathbb{Q}(i),\{2,\infty,\bar{\mathfrak{p}}\}}$ ($\leq$ le 2 premier de $\mathbb{Q}(i)$ au dessus de p)

(ii) $\rho_{\Pi,2} \mid G_{\mathbb{Q}_p} = LL(\pi_p) = \rho$!

On a gagné!

ex: si on regarde $E = \overline{\mathbb{Q}(i)}^{\ker(\rho_{\Pi,2})} \subset \mathbb{Q}(i)_{\{2,\mathfrak{p},\bar{\mathfrak{p}}\}} \subset \mathbb{Q}_S$

et $\mathbb{Q}_p \cdot E = \overline{\mathbb{Q}}_p^{\ker \rho} \subset \overline{\mathbb{Q}}_p$

$\parallel$

F car ρ est injective.

donc tout corps de nombres assez gros dans E satisfait $(\star)$.

(dire autrement peut-être).

temps restant : preuve prop. . Séries de Poincaré.

Construction de formes automorphe (1) : cas réel

B = boule unité hermitienne $\subset \mathbb{C}^{n-1}$

$\Gamma \subset PU(n-1,1)$ un ss groupe discret

" ~~$\frac{dgz_1}{dz}$~~ Clozel a introduit le Jacobien complexe

$g \in PU(n-1,1)$ $\quad g^* dz_1 \wedge \dots \wedge dz_{n-1} = \underbrace{j(g,z)}_{J(g,z)} \det g \, dz_1 \wedge \dots \wedge dz_{n-1}$ $\quad -n \to n$

Soit $h : B \to \mathbb{C}$ une fonction holomorphe bornée. (ex. polynôme)

$m \geq 1$ entier

Prop : (Cartan) (i) $Ph(z) = \sum_{\gamma \in \Gamma} h(\gamma z)\, J(\gamma, z)^m$ converge normalement sur tout compact si $m \geq 2$ vers une forme automorphe pour Γ.

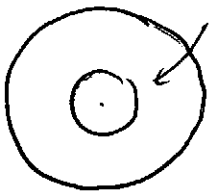
(ii) ~~Pour m et h bien choisis, $Ph \neq 0$.~~

Pour m et h bien choisis, $Ph \neq 0$.

Preuve (i) cond. cocycle $J \Rightarrow$ Ph automorphe si ça converge.

convergence, ops. $h=1$ et $m=2$. : $\sum |J(\gamma,z)|^2$ cv. normalement

ν = volume euclidien ($\mathbb{C}^{n-1}$)



$$\sum_{\gamma \in \Gamma} \nu(\gamma(B(0,r))) < \infty.$$

la raison vient de ce que ~~$\leq$~~ $\leq N \, \nu(B(0,1))$

où $N = \#\{\gamma \in \Gamma,\ \gamma B(0,1) \cap B(0,r) \neq \emptyset\}$.

si $x \in B(0, \frac{r}{2})$ $\quad \nu(\gamma B(0,\frac{r}{2})) = \int_{B(0,\frac{r}{2})} |J(\gamma, z)|^2 \mu$ (par inv.)

$\geq \nu(B(0,\frac{r}{2}))\, |J(\gamma,x)|^2$

$\Rightarrow$ cv. normale sur $B(0,\frac{r}{2})$. ∎

(ii) on cherche $Ph(0) \neq 0$ ie $\sum_{\gamma \in \Gamma} h(\gamma 0)\, J(\gamma,0)^m \neq 0$.

, $\{\gamma \in \Gamma,\ |J(\gamma,0)| \geq 1\}$, c'est fini. $= \{\gamma_1 \dots \gamma_N\}$, $\gamma_1 = 1$

, h s'annule en γ_i si $i \neq 1$, $h(1) = 1$. ($J(1,0) = 1$)

, $m \to \infty$ $\quad Ph(0) \to$ ~~$\sum$~~ $h(1) = 1 \neq 0$. ∎

Construction de formes automorphes 2 (adélique semi-simple) → preuve prop. thm

$K = \prod_{\ell \neq \infty} K_\ell$ où $K_\ell \subset G(\mathbb{Q}_\ell)$ ss gp compact ouvert $\begin{cases} K_\ell \text{ assez petit} \\ K_\ell = G(\mathbb{Z}_\ell) \text{ p.t.} \end{cases}$

$\Gamma = G(\mathbb{Q}) \cap K \subset G(\mathbb{R}) \times G(\mathbb{Q}_p)$ discret, sans torsion si K_ℓ assez petit (cond. connue)

modulo traduction, on cherche à construire une fonction $\Psi : \Gamma \backslash G(\mathbb{R}) \times G(\mathbb{Q}_p) \to \mathbb{C}$

telle que $\begin{cases} (i)\ \Psi \text{ engendre une rep} \cong \pi_0 \text{ sous l'action de } G(\mathbb{Q}_p) \text{ par translation à droite} \\ (ii)\ \Psi(g,1) \text{ est de la forme } \widetilde{\varphi}(g(0))\, J(g,0)^m \end{cases}$ où $m \geq 1$, $\widetilde{\varphi} : B \to \mathbb{C}$ automorphe poids $m \neq 0$

(hol. suffit ici) si $\widetilde{\varphi}$ hol, elle est aut. poids m pour $\Gamma' = \Gamma \cap K_p$ K_p assez petit

c'est une variante de la const. précédente

on pose $\varphi : G_\infty \times G_p \to \mathbb{C} \quad = \varphi_\infty \times \varphi_p$

où $\begin{cases} \varphi_\infty(g) = h(g(0))\, J(g,0)^m & \text{avec } h : B \to \mathbb{C} \text{ hol. à déterminer} \\ \varphi_p(g) = \text{coeff. matriciel lisse de la rep. } \pi_0 \text{ à supp-compact} \end{cases}$ $\varphi_p(1) \neq 0$.

mod centre. Pour simplifier on fera comme si à supp-compact.

puis $P\varphi(g) = \sum_{\gamma \in \Gamma} \varphi(\gamma g)$

En utilisant que φ_p supp-compact, on voit par les cas précédents que ça converge norm. sur tout compact de $G_\infty \times G_p$.

Vérifions que l'on peut choisir h, m de sorte que $P\varphi(1) \neq 0$.

On introduit $\Omega \subset G(\mathbb{Q}_p)$ compact ouvert contenant $\operatorname{Supp} \varphi_p$.

alors $\exists\, K_p \subset G(\mathbb{Z}_p)$ ss gp compact ouvert tel que φ_p est bi K_p-invariante et Ω aussi.

$$\Gamma \cap \Omega = \coprod_{i=1}^{n} \gamma_i \Gamma' \quad \text{où} \quad \Gamma' = \Gamma \cap K_p \subset G(\mathbb{R})$$

on a alors $P\varphi(1) = \sum \varphi(\gamma_i \gamma) = \sum_i \varphi_p(\gamma_i) \sum_\gamma \varphi_\infty(\gamma_i \gamma)$

nb fini de γ / $|J(\gamma_i \gamma, 0)| \geq 1$ pour au moins un i.

les $\gamma_i \gamma(0)$ sont tous $\neq$ car Γ sans torsion

on choisit alors h nulle sur les $\gamma_i \gamma(0)$ mauvais sauf en 1 et $m \to \infty$ ■.

Remarques

(i) Comme ρ_p n'est pas tout à fait au sens complet, la preuve, et en fait l'énoncé, n'est pas tout à fait exacte. Il le seraient si $\det \rho = 1$ auquel cas on travaillerait avec PG plutôt que G. En général, il faut rajouter de la torsion par des caractères non ramifiés, ce que l'on négligera ici.

(ii) Cette méthode se généralise (travaillent) à d'autres S, en remplaçant $\mathbb{Q}$ par un corps q. imaginaire quelconque. Par ex. cela montre que si $l \neq p$ et $l \equiv 1 \pmod 4$, et $\left(\frac{p}{l}\right) = 1$, le théorème vrai si $\{l, p\}$ remplace $\{2, p\}$.

Pour enlever ces hyp. parasites sur l et p, c'est plus difficile : cf article avec Clozel. On travaille directement sur $GL_n(A_Q)$ et constructions de rep. aut. (autoduals) avec des conditions premières, avec la formule des traces.