Groupe de travail
d'analyse ultramétrique

Jacques Tilouine

Introduction aux travaux de Ihara

Groupe de travail d'analyse ultramétrique, tome 14 (1986-1987), exp. n° 17, p. 1-24
<http://www.numdam.org/item?id=GAU_1986-1987__14__A9_0>

Groupe d'Etude d'Analyse Ultramétrique. (1986/87)
n° 17, 24 pages

6 avril 1987

Exposé n° 17

Introduction aux Travaux de Ihara

Jacques TILOUINE

Dans son article [5], Y. Ihara a amorcé l'étude d'une représentation de $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur la pro-ℓ-partie du groupe fondamental de $\mathbb{P}^1\setminus\{0,1,\infty\}$. En particulier, il a concentré son étude sur le quotient 2-résoluble maximal de ce groupe en montrant que la représentation de $G_{\mathbb{Q}}$ sur ce groupe est décrite par un 1-cocycle :

$$\psi : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell[[\mathbb{Z}^2(1)]]^\times = \mathbb{Z}_\ell[[u,v]]^\times$$

non ramifié hors de ℓ et fournissant une "somme de Jacobi universelle" sur les Frobenius en $p\neq\ell$ (voir théorème 14 ci-dessous). De plus, la série $F_\rho(u,v) = \psi(\rho)$ vérifie la formule de 2-cocycle satisfaite par la fonction bêta classique :

$$F_\rho(u,v)\times F_\rho(u[+]v,w) = F_\rho(u,v[+]w)\times F_\rho(v,w)$$

(l'addition étant définie par $u[+]v = u+v+uv$)

et l'explication est la même que pour la fonction bêta classique : Anderson ([1] - [3]) et Ihara-Kaneko-Yukinari [6] ont montré (seulement si ρ fixe $\mathbb{Q}(\mu_{\ell^\infty})$ pour [6]) qu'il existe une série $\hat{G}_\rho(t) \in \hat{\mathbb{Z}}_\ell^{n.r.}[[t]]$ ("une fonction gamma") telle que : $F_\rho(u,v) = \dfrac{\hat{G}_\rho(u)\hat{G}_\rho(v)}{\hat{G}_\rho(u[+]v)}$.

En outre, Ihara a calculé les coefficients de $\hat{G}_\rho(u)$ à l'aide des dérivées de Coates-Wiles lorsque ρ est dans l'inertie en ℓ de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{\ell^\infty}))$, et Coleman [4] a relié ces coefficients à des caractères de Kummer sur des ℓ-unités cyclotomiques. Il semble de plus que sous la conjecture de Vandiver, l'image modulo ℓ du cocycle ψ soit déterminée par Ichimura et Kaneko.

I. Définition de la représentation totale.

Soit $K = \overline{\mathbb{Q}}(t)$ le corps des fonctions rationnelles de $\mathbb{P}^1_{\overline{\mathbb{Q}}} = \mathbb{P}^1_{\mathbb{Q}} \times \overline{\mathbb{Q}}$. Considérons la pro-$\ell$-extension maximale M non ramifiée hors de $0,1,\infty$, de K. Notons que les places $0,1,\infty$ de K sont rationnelles sur $\mathbb{Q}$. En fait, trois points distincts quelconques de $\mathbb{P}^1(\mathbb{Q})$ conviennent pour la construction qui suit. On choisit $0,1,\infty$ pour simplifier.

On détermine d'abord la structure du groupe Gal(M/K).

Définition 1. On appelle pro-ℓ-groupe libre de rang 2, de base x,y, le groupe $\mathcal{F}$ obtenu comme suit :

Soit $F = \mathbb{Z}x * \mathbb{Z}y$ le groupe libre engendré par x et y, alors :

$$\mathcal{F} = \varprojlim_{N} F/N$$

où N parcourt l'ensemble des sous-groupes distingués de F d'indice fini ℓ-primaire.

On montre que le morphisme canonique d'image dense $F \longrightarrow \mathcal{F}$ est injectif ([7], § 4). On introduit $z \in F \subset \mathcal{F}$ défini par $xyz=1$.

Théorème 2. Il existe des places $\tilde{0}$, $\tilde{1}$, $\tilde{\infty}$ de M au-dessus des places $0,1,\infty$ de K, et un isomorphisme :

$$\iota : \mathcal{F} \xrightarrow{\sim} \mathrm{Gal}(M/K)$$

tels que $\iota(x)$ (resp. $\iota(y), \iota(z)$) engendre topologiquement le groupe d'inertie en $\tilde{\sigma}$ (resp. $\tilde{1}$, $\tilde{\infty}$).

Commentaire : Le choix de ι détermine uniquement les places $\tilde{\sigma}$, $\tilde{1}$, $\tilde{\infty}$. Ceci résulte directement de ce que le normalisateur dans $\mathcal{F}$ du $\mathbb{Z}_\ell$-module engendré par x (resp; y,z) est égal à ce $\mathbb{Z}_\ell$-module.

Démonstration du théorème :

l'extension des scalaires de $\overline{\mathbb{Q}}$ à $\mathbb{C}$ établit une bijection

$$1 = \left\{\begin{array}{l}\text{morphismes finis } Y \xrightarrow{p} \mathbb{P}^1_{\overline{\mathbb{Q}}} \\ Y = \text{courbe propre et lisse} \\ p = \text{revêt. étale hors de } 0,1,\infty\end{array}\right\} \xrightarrow{(i)} 2 = \left\{\begin{array}{l}\text{morphismes finis } Z \xrightarrow{p} \mathbb{P}^1_{\mathbb{C}} \\ Z = \text{courbe propre et lisse/}\mathbb{C} \\ p = \text{revêt. étale hors de } 0,1,\infty\end{array}\right\}$$

qui respecte les groupes de Galois. On peut donc remplacer $\overline{\mathbb{Q}}$ par $\mathbb{C}$ pour définir M.

De plus, si l'on note, pour tout revêtement $p : Z \longrightarrow \mathbb{P}^1/_{\mathbb{C}}$ comme ci-dessus $Z' = Z(\mathbb{C})\backslash p^{-1}(\{0,1;\infty\})$ et $X' = \mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}$, on établit des bijections canoniques :

$$2 \xrightarrow{(ii)} \left\{\begin{array}{l}\text{revêtements holomorphes}\\ \text{finis étales}\\ S \longrightarrow X'\end{array}\right\} \xrightarrow{(iii)} \left\{\begin{array}{l}\text{revêtement}\\ \text{topologiques finis}\\ T \longrightarrow X'\end{array}\right\}$$

$Z \xrightarrow{(ii)} S = Z'_{anal.}$; $S \xrightarrow{(iii)}$ T= espace topologique sous-jacent à S.

La surjectivité de (ii) résulte aisément du fait que le revêtement universel de X' est donné par la fonction λ de Legendre qui se prolonge en un isomorphisme de surfaces de Riemann :

$$\mathcal{H}^*/_{\Gamma(2)} \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$$

où $\Gamma(2) = \{g \in SL_2(\mathbb{Z});\ g \equiv I_2 \bmod. 2\}$.

et $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ muni de la topologie hyperbolique.

On trouve alors Z, antécédent de S, en posant $Z(\mathbb{C}) = \mathcal{H}^*/_{Gal(\xrightarrow{\pi} S)}$, où π est un revêtement tel que $p\circ\pi=\lambda$, puis
anal.
en utilisant le théorème d'algébrisation de Riemann pour passer de $Z_{anal.}$ à Z.

la bijection (iii) est bien connue.

A l'aide de la composée des trois bijections (i) - (iii) on obtient un isomorphisme canonique entre le groupe de Galois de M/K et le pro-ℓ-- complété de $Aut(\lambda) = \Gamma(2)$.

Fixons alors $\xi \in X'$. A chaque $\tilde{\xi} \in \lambda^{-1}(\xi)$, on peut associer l'isomorphisme :

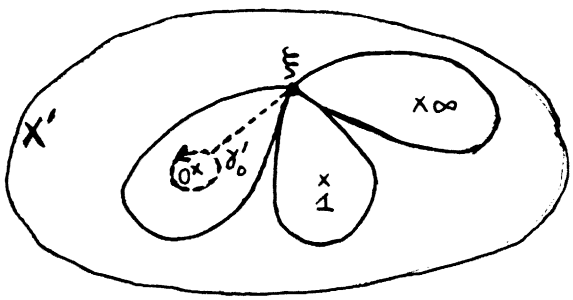
$$\begin{array}{rcl}\Phi_{\tilde{\xi}} : \pi_1(X',\xi) & \xrightarrow{\sim} & Aut(\lambda)\\ [\gamma] & \longrightarrow & g\end{array}$$

où $g \in \Gamma(2)$ est défini par la formule :

$$g.\tilde{\xi} = \tilde{\xi}[\gamma]$$

(si $\tilde{\gamma}$ est un lacet représentant $[\gamma]$; soit $\tilde{\gamma}$ son relèvement sur issu de $\tilde{\xi}$, on note $\tilde{\xi}.[\gamma]$ l'extrémité $\tilde{\gamma}(1)$, indépendante du choix de γ).

Enfin, le théorème de Van Kampen montre que l'inclusion du bouquet des cercles C_0 et C_1 dans X' (voir figure) induit un isomorphisme des groupes fondamentaux :



$$\pi_1(C_0,\xi) * \pi_1(C_1,\xi) \xrightarrow{\sim} \pi_1(X',\xi)$$

On voit enfin qu'il y a un unique choix d'un générateur γ_i du groupe monogène $\pi_1(C_i,\xi)$, $i= 0,1,\infty$, de sorte que $\gamma_0\gamma_1\gamma_\infty=1$.

Si l'on passe alors à la pro-ℓ-complétion ι de $\varphi_{\tilde{\xi}}$, on obtient l'isomorphisme cherché pour $x= \gamma_0$, $y= \gamma_1$, $z= \gamma_\infty$ (en remplaçant γ_i par le lacet homotope γ'_i figuré sur le dessin pour $i=0$, on voit facilement que $\varphi_{\tilde{\xi}}$ induit un isomorphisme de $\pi_1(C_i,\xi)$ avec le stabilisateur dans $\Gamma(2)$ d'une pointe $\tilde{i}$ au-dessus de $i \in \{0,1,\infty\}$, donc ι a bien les propriétés requises dans l'énoncé).

On fixe désormais un tel isomorphisme ι et on note $\mathcal{G}$ le groupe $\mathrm{Gal}(M/K)$.

Remarquons que M est galoisien sur $\mathbb{Q}(t)$ grâce au fait que nos pointes $0,1,\infty$ sont rationnelles sur $\mathbb{Q}$. Or on a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$, donc si on abrège $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ en G_L pour tout sous-corps L de $\overline{\mathbb{Q}}$, on peut définir :

$$\mathrm{Out} : G_{\mathbb{Q}} \longrightarrow \mathrm{Out}(\mathcal{G}) = \frac{\mathrm{Aut}(\mathcal{G})}{\mathrm{Int}(\mathcal{G})},$$

comme suit :

On prend $\rho \in G_{\mathbb{Q}}$, on le prolonge en un automorphisme $\tilde{\rho}$ de M et on considère la conjugaison par $\tilde{\rho}$ comme automorphisme de $\mathcal{G}$. On voit que cette définition fournit un élément de $\mathrm{Out}(\mathcal{G})$ indépendant du prolongement $\tilde{\rho}$ de ρ.

Cette représentation constitue l'objet d'étude de Ihara dans [5]. Nous l'appelons totale car, bien que certaines propriétés générales non triviales la concernant puissent être établies, le problème de la détermination de son image n'est pas abordé directement par Ihara. Il n'est

attaqué que pour des morceaux (sous-quotients de $\mathcal{F}$ issus de sa suite centrale descendante ou dérivée). Quelques propriétés de la représentation totale d'abord :

Théorème 3 (Deligne). Out est non-ramifiée hors de ℓ.

Démonstration : Soit M^{ab}/K la sous-extension abélienne maximale de M/K. On peut écrire

$$M^{ab} = \bigcup_{n=1}^{\infty} K_n$$

où K_n est l'extension abélienne d'exposant ℓ^n non ramifiée hors de $0,1,\infty$ de K. La théorie de Kummer montre facilement que

$$K_n = K(t^{1/\ell^n}, (1-t)^{1/\ell^n}). \tag{1.1}$$

Ainsi K_n est le corps des fonctions de la courbe de Fermat X_n d'équation $X^{\ell^n} + Y^{\ell^n} = Z^{\ell^n}$. En outre, le théorème 2 (ou le théorème de Puiseux donnant la clôture algébrique de $\overline{\mathbb{Q}}((t))$ comme réunion des $\overline{\mathbb{Q}}((t^{1/n}))$; $n= 1,2,\ldots$) montre que le groupe d'inertie de $\tilde{i}$ dans M/K est isomorphe à $\mathbb{Z}_\ell$ (pour $i= 0,1,\infty$). L'égalité (1.1) montre que le groupe d'inertie en i dans M^{ab}/K est aussi isomorphe à $\mathbb{Z}_\ell$ ($i= 0,1,\infty$). On en tire que M/M^{ab} est non ramifiée partout. Soit $K_n^{n.r}$ la pro-ℓ-- extension maximale non ramifiée de K_n. On a $M= \bigcup_{n=1}^{\infty} K_n^{n.r}$, donc :

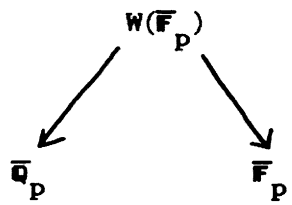
$$\mathrm{Gal}(M/K) = \varprojlim_n \mathrm{Gal}(K_n^{n.r}/K_n).$$

Ces remarques générales, très importantes pour toute la suite, étant posées, considérons un nombre premier $p\neq\ell$, et étudions la restriction de Out à $G_{\mathbb{Q}_p}$. La définition du groupe fondamental algébrique (cf. [10]) permet d'écrire :

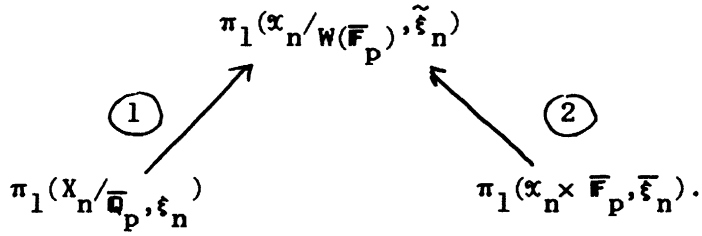
$$\mathrm{Gal}(K_n^{n.r}/K_n) \cong \pi_1^{alg}(X_{n/\overline{\mathbb{Q}}_p}, \xi_n)$$

le point base ξ_n étant $\mathbb{Q}_p$-rationnel, de sorte que l'isomorphisme

soit $G_{\mathbb{Q}}$-équivariant. Soit $\mathfrak{X}_n/\mathbb{Z}_p$ le schéma propre et lisse, d'équation $X^{\ell^n} + Y^{\ell^n} = Z^{\ell^n}$ dans $\mathbb{P}^2/\mathbb{Z}_p$. Les applications naturelles :



fournissent par fonctorialité du π_1 :



où $\tilde{\xi}_n$ prolonge ξ_n par propreté, et $\overline{\xi}_n$ est le point fermé associé à $\tilde{\xi}_n$. Le théorème (6.3.2.1) de [10] montre que 2 et un isomorphisme, et le théorème de Grothendieck ([10] chap. IX et appendice) montre que $(2)^{-1} \circ (1)$ induit un isomorphisme sur les pro-ℓ-parties, compatible avec les actions de $G_{\mathbb{Q}_p}$ et $G_{\mathbb{F}_p}$ pour le morphisme de réduction : $G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{F}_p}$ dont le noyau est le groupe d'inertie en p. Ceci prouve la non-ramification de Out en p.

Un autre résultat général exprime que l'image de la représentation est contenue dans le groupe des tresses défini comme suit.

Le groupe $Tr = Tr(\mathfrak{F}, x, y, z)$ est le quotient par le groupe des automorphismes intérieurs de :

$$\{\sigma \in Aut(\mathfrak{F});\ \exists \alpha \in \mathbb{Z}_\ell;\ \sigma x \sim x^\alpha,\ \sigma y \sim y^\alpha,\ \sigma z \sim z^\alpha\}$$

où $a \sim b$ signifie que les éléments a et b sont conjugués dans $\mathfrak{F}$.

Le groupe Tr possède un caractère naturel appelé la norme :

$$N : Tr \longrightarrow \mathbb{Z}_\ell^\times.$$

On note Tr_1 le noyau de N. On a alors le :

Lemme 4. La représentation Out est à valeurs dans le groupe des tresses Tr_ℓ et la composée $N \circ Out$ coïncide avec le caractère cyclotomique $\chi : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^\times$. En particulier, l'image par Out de $G_{\mathbb{Q}(\mu_{\ell^\infty})}$ est contenue dans Tr_1.

Démonstration : Soit $\rho \in G_{\mathbb{Q}}$, comme i est rationnel sur $\mathbb{Q}$ (i= 0,1,∞), on a $\rho.i=i$ et $\tilde{\rho}\, I_{\tilde{i}}\, \tilde{\rho}^{-1}$ est encore un groupe d'inertie en une place au-dessus de i. On peut donc l'écrire $s_i\, I_{\tilde{i}}\, s_i^{-1}$ pour un s_i dans $\mathcal{F}$. On a donc :

$$\tilde{\rho}\, x\, \tilde{\rho}^{-1} = s_0.x^\alpha.s_0^{-1} \quad \text{pour un } \alpha \in \mathbb{Z}_\ell^\times$$
$$\tilde{\rho}\, y\, \tilde{\rho}^{-1} = s_1.y^\beta.s_1^{-1} \quad \text{pour un } \beta \in \mathbb{Z}_\ell^\times$$
$$\tilde{\rho}\, z\, \tilde{\rho}^{-1} = s_\infty.z^\gamma.s_\infty^{-1} \quad \text{pour un } \gamma \in \mathbb{Z}_\ell^\times$$

or, comme xyz=1, on trouve en passant au plus grand quotient abélien $\mathcal{F}/\mathcal{F}'$ de $\mathcal{F}$:

$$\overline{x}^\alpha.\ \overline{y}^\beta = (\overline{x}\ \overline{y})^\gamma.$$

Or, on a : $\mathcal{F}/\mathcal{F}' = \mathbb{Z}_\ell.\overline{x} \oplus \mathbb{Z}_\ell\ \overline{y}$, donc on obtient $\alpha=\beta=\gamma$.

Notons donc $\alpha = N \circ Out(\rho)$. Pour chaque $n \geq 1$, considérons l'accouplement de Kummer :

$$\langle , \rangle_n : \mathcal{F} \times K^\times / K^{\times \ell^n} \longrightarrow \mu_{\ell^n}.$$

L'égalité (1.1) entraîne que $\langle x,t \rangle_n$ est une racine primitive $(\ell^n)^{\text{ième}}$ de 1.

On a donc : $$\langle x,t \rangle_n^{\tilde{\rho}} = \langle x,t \rangle_n^{\chi(\rho)}$$

mais aussi $$= \langle x^{\tilde{\rho}}, t^{\tilde{\rho}} \rangle_n = \langle s_0 x^\alpha s_0^{-1}, t \rangle_n = \langle x^\alpha, t \rangle_n = \langle x,t \rangle_n^\alpha.$$

Il suffit alors de faire tendre n vers l'infini pour conclure $\alpha=\chi(\rho)$.

L'étude du groupe Tr_1 est effectuée dans [5]. En particulier, l'étude des quotients successifs d'une filtration naturelle de Tr_1 déduite de la suite centrale descendante de $\mathcal{F}$ permet à Ihara de montrer la

Proposition 5. Tr_1 est un pro-ℓ-groupe. D'où le théorème suivant résulte immédiatement.

Théorème 6. La représentation $Out : G_{\mathbb{Q}} \longrightarrow Tr$ se factorise à travers $Gal(\Omega_\ell/\mathbb{Q})$ où Ω_ℓ est la pro-ℓ-extension non ramifiée hors de ℓ maximale de $\mathbb{Q}(\mu_{\ell^\infty})$.

Nous abandonnons désormais l'étude directe de la représentation totale pour nous concentrer sur les sous-quotients suivants de $\mathcal{F}$.

Soit $C^1\mathcal{F}=\mathcal{F}$, $C^{m+1}\mathcal{F}= [\mathcal{F},C^m\mathcal{F}]$ (sous-groupe fermé engendré par les commutateurs $[a,b]$, $a \in \mathcal{F}$, $b \in C^m\mathcal{F}$) la suite centrale descendante de $\mathcal{F}$. Le groupe $\mathcal{F}/C^{m+1}\mathcal{F}$ est le pro-ℓ-groupe m-nilpotent à deux générateurs, universel, et on peut définir le groupe des tresses $Tr^{(m)} \subset Out(\mathcal{F}/C^{m+1}\mathcal{F})$ de façon analogue à celle donnant Tr. Comme tous les groupes $C^m\mathcal{F}$ sont caractéristiques, on a un diagramme évident :

$$\begin{array}{ccc} Out(\mathcal{F}) & \longrightarrow & Out(\mathcal{F}/C^{m+1}\mathcal{F}) \\ \cup & & \cup \\ Tr & \longrightarrow & Tr^{(m)} \end{array}$$

et la norme se factorise en $N : Tr^{(m)} \longrightarrow \mathbb{Z}_\ell^\times$. On obtient alors la représentation $Out_{m-nil.}$:

$$\begin{array}{ccccc} Out_{m-nil.} : & G_{\mathbb{Q}} & \longrightarrow & Tr^{(m)} \\ & \cup & & \cup \\ & G_{\mathbb{Q}(\mu_{\ell^\infty})} & \longrightarrow & Tr_1^{(m)}. \end{array}$$

On peut la définir directement par action de $G_{\mathbb{Q}}$ sur le groupe de Galois de la pro-ℓ-ext. M_m m-nilpotente maximale non ramifiée hors de $0,1,\infty$. Ce programme est actuellement étudié par Anderson, Coleman, Deligne et Ihara. Considérons quelques exemples :

(i) $m=1$: On a $\mathcal{F}/\mathcal{F}' = \mathbb{Z}_\ell\ \bar{x} \oplus \mathbb{Z}_\ell\ \bar{y} = H_1(\mathbb{P}^1\setminus\{0,1,\infty\},\mathbb{Z}_\ell)$.

Le corps M_1 est évidemment égal à M^{ab}, et $Tr^{(1)}$ = matrices d'homothéties dans $GL_2(\mathbb{Z}_\ell)$. La norme N fournit un isomorphisme $Tr^{(1)} \xrightarrow{\sim} \mathbb{Z}_\ell^\times$ qui identifie la représentation $Out_{1\text{-nil}}$ au caractère cyclotomique χ. Nous noterons $\mathfrak{g}/\mathfrak{g}' = \mathbb{Z}_\ell^2(1)$ pour rappeler que $G_{\mathbb{Q}}$ opère sur ce groupe par le caractère cyclotomique.

(ii) m quelconque, étude de la sous-représentation

$$C^m\mathfrak{g}/C^{m+1}\mathfrak{g} \quad \text{de} \quad Out_{m\text{-nil}}.$$

(ceci a du sens car $Int(\mathfrak{g})$ opère trivialement par conjugaison sur $C^m\mathfrak{g}/C^{m+1}\mathfrak{g}$).

On remarque que $C^m\mathfrak{g}/C^{m+1}\mathfrak{g}$ est engendré comme $\mathbb{Z}_\ell$-module par les commutateurs $[x_1,\ldots,[x_{m-1},x_m]\ldots]$, où $x_i \in \{x,y\}$ pour $i = 1,\ldots,m$. De plus, l'action de $\rho \in G_{\mathbb{Q}}$ transforme ce commutateur c en le commutateur c' analogue où l'on remplace x_i par $\tilde{\rho}\, x_i\, \tilde{\rho}^{-1} = s_i\, x_i^{\chi(\rho)} s_i^{-1} = [s_i, x_i^{\chi(\rho)}].x_i^{\chi(\rho)}$. Les formules de calcul de commutateurs montrent que c' est congru mod. $C^{m+1}\mathfrak{g}$ à $c^{\chi^m(\rho)}$. Ainsi, l'action de $G_{\mathbb{Q}}$ sur $C^m\mathfrak{g}/C^{m+1}\mathfrak{g}$ est donnée par χ^m.

(iii) On peut se proposer d'étudier après la sous-représentation $C^2\mathfrak{g}/C^3\mathfrak{g}$ (action de $G_{\mathbb{Q}}$ par χ^2) la représentation $\mathfrak{g}'/\mathfrak{g}''$ (où $\mathfrak{g}'' = [\mathfrak{g}',\mathfrak{g}'] \subset C^3\mathfrak{g}$) qui contient la précédente comme quotient. Il s'avère (voir prop. 12 ci-dessous) que cette étude révèle une structure très riche de la représentation $\mathfrak{g}'/\mathfrak{g}''$ et c'est elle que Ihara mène à bien dans la seconde moitié de son article [5]. Nous allons maintenant exposer ses résultats.

II. Etude de la représentation $\mathfrak{g}'/\mathfrak{g}''$ de $G_{\mathbb{Q}}$.

Considérons la suite exacte de pro-ℓ-groupes :

$$1 \longrightarrow \mathfrak{g}'/\mathfrak{g}'' \longrightarrow \mathfrak{g}/\mathfrak{g}'' \longrightarrow \mathfrak{g}/\mathfrak{g}' \longrightarrow 1.$$

Le quotient opère sur le noyau abélien et donc l'algèbre complétée de groupe $\mathbb{Z}_\ell[[\mathfrak{g}/\mathfrak{g}']]$ opère sur $\mathfrak{g}'/\mathfrak{g}''$. Comme $\mathfrak{g}/\mathfrak{g}' = \mathbb{Z}_\ell\overline{x} \oplus \mathbb{Z}_\ell\overline{y}$, on a un isomorphisme :

$$\Lambda = \mathbb{Z}_\ell[[u,v]] \xrightarrow{\sim} \mathbb{Z}_\ell[[\mathfrak{g}/\mathfrak{g}']]$$

envoyant $1+u$ sur $\overline{x}$ et $1+v$ sur $\overline{y}$. L'action de $G_{\mathbb{Q}}$ sur Λ linéarisant l'action sur $\mathfrak{g}/\mathfrak{g}' = \mathbb{Z}_\ell^2(1)$ est donnée par :

$$\rho.u = (1+u)^{\chi(\rho)}-1, \quad \rho.v = (1+v)^{\chi(\rho)}-1.$$

De plus, l'action de $G_{\mathbb{Q}}$ sur $\mathfrak{g}'/\mathfrak{g}''$ est Λ-semi-linéaire :

$$\rho.(\alpha.\mathfrak{p}) = \rho(\alpha).\rho(\mathfrak{p})$$

pour tout $\rho \in G_{\mathbb{Q}}$, $\alpha \in \Lambda$, $\mathfrak{p} \in \mathfrak{g}'/\mathfrak{g}''$.

Ihara démontre que $\mathfrak{g}'/\mathfrak{g}''$ est libre de rang 1 sur Λ, ce qui entraîne l'existence d'un 1-cocycle $G_{\mathbb{Q}} \longrightarrow \Lambda^\times$ donnant l'action de $G_{\mathbb{Q}}$ sur $\mathfrak{g}'/\mathfrak{g}''$. L'idée est la suivante :

Etape 1 : La théorie des revêtements abéliens ramène l'étude de $\mathfrak{g}'/\mathfrak{g}''$ à celle des jacobiennes des courbes de Fermat X_n (i.e. de l'homologie étale ℓ-adique des X_n) : Soit en effet J_n la jacobienne de la courbe de Fermat X_n d'équation $X^{\ell^n} + Y^{\ell^n} = Z^{\ell^n}$. Soit $T_\ell J_n$ son module de Tate. Les revêtements $X_{n+1} \longrightarrow X_n$, définis sur $\mathbb{Q}$, donnés par $(X,Y,Z) \longrightarrow (X^\ell, Y^\ell, Z^\ell)$ fournissent par fonctorialité covariante un système projectif

$$T_\ell J_{n+1} \longrightarrow T_\ell J_n$$

dont nous notons $\mathfrak{H}$ la limite projective. C'est un $G_{\mathbb{Q}}$ et un Λ-module (par fonctorialité covariante) et l'action de $G_{\mathbb{Q}}$ est encore Λ-semi-linéaire :

$$\rho.(\alpha.t) = \rho(\alpha).\rho(t)$$

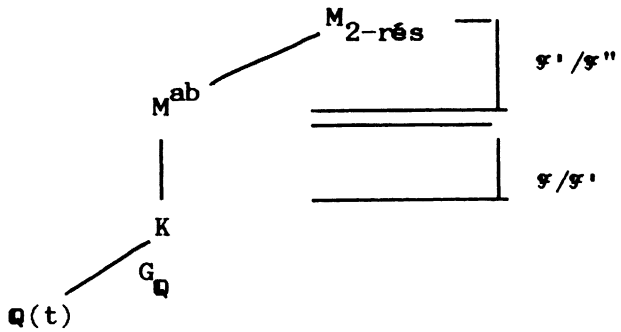
pour tout $\rho \in G_{\mathbb{Q}}$, $\alpha \in \mathcal{A}$, $t \in \mathcal{S}$.

Proposition 7. Il y a un isomorphisme canonique :

$$\mathcal{S} \cong \mathcal{G}'/\mathcal{G}''$$

de $\mathcal{A}$ et $G_{\mathbb{Q}}$-modules.

Démonstration : Soit $M_{2\text{-rés.}}$ la pro-ℓ-extension maximale 2-résoluble non ramifiée hors de $0,1,\infty$ de K. On a le diagramme de corps :



En utilisant encore le théorème de Puiseux (cf. théorème 3 ci-dessus), on voit que $M_{2\text{-rés}}/M^{ab}$ est non ramifiée. Soit $K_n^{n.r.ab}$ la pro-ℓ-extension abélienne maximale non-ramifiée de K_n. On obtient :

$$\mathcal{G}'/\mathcal{G}'' = \mathrm{Gal}(M_{2\text{-rés}}/M^{ab}) = \varprojlim \mathrm{Gal}(K_n^{n.r.ab.}/K_n).$$

Il suffit d'obtenir des isomorphismes

$$T_\ell\, J_n \xrightarrow{\sim} \mathrm{Gal}(K_n^{n.r.ab.}/K_n)$$

compatibles avec les différentes actions et aux applications de transition. Or, pour tout entier $N \geq 1$, en notant $K_n^{(N)}$ l'extension abélienne d'exposant N maximale non ramifiée maximale, et $\mathcal{A}_n^{(N)}$ le sous-groupe de $K_n^\times/K_n^{\times N}$ lui correspondant par la théorie de Kummer :

$$\mathcal{A}_n^{(N)} = \{f \in K_n^\times ;\ \forall\, P \in X_n(\overline{\mathbb{Q}});\ \mathrm{ord}_P(f) \equiv 0 \bmod N\}/K_n^N$$

on a un isomorphisme canonique :

$$\mathcal{A}_n^{(N)} \xrightarrow{\sim} \mathrm{Pic}^0(X_n)[N]$$

$$f \bmod K_n^N \longrightarrow \frac{1}{N}.\mathrm{div}(f).$$

On passe alors aux duaux de Cartier en utilisant l'accouplement de Kummer et celui de Weil pour obtenir :

$$\mathrm{Gal}(K_n^{(N)}/K_n) \xrightarrow{\sim} J_n[N].$$

Toutes les compatibilités requises sont évidentes, on passe donc à la limite pour $N|\ell^\infty$ et $n \longrightarrow \infty$.

Etape 2 : On utilise des calculs de Rohrlich [11] pour montrer que $\mathcal{S}$ est libre de rang 1 sur $\mathcal{A}$.

Nous poserons $N=\ell^n$. Soit $p : X_n \longrightarrow \mathbb{P}^1$ le revêtement standard $(X,Y,Z) \longrightarrow (X^N,Y^N,Z^N)$. Soient $X' = \mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}$, $X'_n = X_n(\mathbb{C})\backslash p^{-1}(\{0,1,\infty\})$. On fixe un point base ξ de X' et $\xi_n \in X'_n$ au-dessus de ξ. Ceci permet d'écrire la suite exacte canonique :

$$1 \longrightarrow \pi_1(X'_n,\xi_n) \xrightarrow{P*} \pi_1(X',\xi) \xrightarrow{\Psi_{\xi_n}} \mathrm{Aut}(p) \longrightarrow 1$$

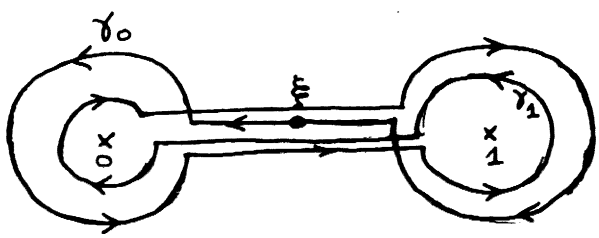
où $\Psi_{\xi_n}([\gamma])$ est l'unique automorphisme g de p tel que $g.\xi_n = \xi_n[\gamma]$.

Comme $\mathrm{Aut}(p) \cong \mu_N \times \mu_N$ est abélien, on voit que le commutateur $[\gamma_0,\gamma_1] \in \pi_1(X',\xi)$ est dans l'image de p_* (avec les notations de la démonstration du théorème 2).

Soit $\mathcal{P}'_n$ son unique antécédent par l'injection p_*. On définit le contour de Pochhammer $\mathcal{P}_n$ comme l'image de $\mathcal{P}'_n$ par la composée :

$$\pi_1(X'_n,\xi_n) \longrightarrow H_1(X'_n,\mathbb{Z}) \longrightarrow H_1(X_n,\mathbb{Z}).$$

Le lacet de X' qu'il relève peut être représenté par la figure :



Proposition 8. Le groupe $H_1(X_n,\mathbb{Z})$ est un $\mathbb{Z}[\mathrm{Aut}(p)]$-module monogène engendré par $\mathcal{P}_n$. Son annulateur est l'idéal engendré par :

$$\sum_{i=0}^{\ell^n-1} \bar{x}^i, \quad \sum_{i=0}^{\ell^n-1} \bar{y}^i, \quad \sum_{i=0}^{\ell^n-2} \bar{x}^i \left(\sum_{j=0}^{i} \bar{y}^j\right)$$

où $\bar{x}$, $\bar{y}$ sont les images de x et y dans la restriction :

$$\mathcal{G} \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(K_n/K) = \mathrm{Aut}(p).$$

Démonstration : cf. [8] chap. V ou [11].

On considère alors la suite exacte canonique :

$$0 \longrightarrow ((1+u)^{\ell^n}-1,(1+v)^{\ell^n}-1) \longrightarrow \mathcal{A} \longrightarrow \mathbb{Z}_\ell[\mathrm{Gal}(K_n/K)] \longrightarrow 0$$

donnée par $u \longrightarrow \bar{x}-1$, $v \longrightarrow \bar{y}-1$.

Soit $\mathcal{I}_n$ l'idéal de $\mathcal{A}$ image réciproque de l'annulateur de $\mathcal{P}_n$.

Lemme 9. $\bigcap_{n=1}^{\infty} \mathcal{I}_n = \{0\}$.

Démonstration : On montre en fait que :

$$\mathcal{I}_n = \{F\in\mathcal{A};\ F(\zeta-1,\zeta'-1)=0 \text{ pour } \zeta,\zeta'\in \mu_{\ell^n}\setminus\{1\} \text{ et } \zeta\zeta'\neq 1\}.$$

On déduit facilement le lemme de cela grâce au théorème préparatoire de Weierstrass.

On constate alors que par le revêtement $X_{n+1} \longrightarrow X_n$, le contour $\mathcal{P}_{n+1}$ s'envoie sur $\mathcal{P}_n$.

En outre, la description de J_n comme tore complexe

$$\Omega^*/H_1(X_n,\mathbb{Z}) \xrightarrow{\sim} J_n$$

montre qu'on a un isomorphisme de $\mathbb{Z}_\ell[\mathrm{Gal}(K_n/K)]$-modules :

$$H_1(X_n,\mathbb{Z}_\ell) \xrightarrow{\sim} T_\ell J_n$$

Si l'on passe à la limite projective, on obtient

Théorème 10. $\mathfrak{s}$ est un Λ-module libre de rang 1. Une base en est fournie par le système projectif $\mathcal{P}=(\mathcal{P}_n)_{n\geq 1}$ des contours de Pochhammer. Dans l'isomorphisme de la prop. 7, $\mathcal{P}$ correspond à $[x,y]$ mod. $\mathfrak{s}''$.

On en déduit le :

Théorème 11. Il existe un 1-cocycle

$$\Psi : G_{\mathbb{Q}} \longrightarrow \Lambda^{\times}$$

$$\rho \longrightarrow F_{\rho}$$

tel que pour tout $\rho\in G_{\mathbb{Q}}$: $\rho.\mathcal{P}=F_{\rho}.\mathcal{P}$
ou, ce qui est équivalent : $\rho.[x,y]=F_{\rho}.[x,y]$.

Nous noterons $F_{\rho}=F_{\rho}(u,v)$ ou bien, en identifiant Λ avec $\mathbb{Z}_{\ell}[[u,v,x]]/_{(1+u)(1+v)(1+w)-1)}$ de sorte que $1+u \longrightarrow \overline{x}$, $1+v \longrightarrow \overline{y}$, $1+w \longrightarrow \overline{z}$); nous écrirons :

$$F_{\rho}=F_{\rho}(u,v,w).$$

La base $\{[x,y]\}$ donne un isomorphisme $I : \mathfrak{s}'/\mathfrak{s}'' \xrightarrow{\sim} \Lambda$ et on a :

Proposition 12. Dans l'isomorphisme I, le sous-Λ-module $C^3\mathfrak{s}/\mathfrak{s}''$ de $\mathfrak{s}'/\mathfrak{s}''$ s'identifie à l'idéal $u\Lambda+v\Lambda$ de Λ et $\mathfrak{s}'/C^3\mathfrak{s} \cong \mathbb{Z}_{\ell}(2)$ comme $G_{\mathbb{Q}}$-module. Il en résulte donc que la restriction Ψ_1 de Ψ à $G_{\mathbb{Q}(\mu_{\ell^\infty})}$ est à valeurs dans le pro-ℓ-groupe

$$\{F\in\Lambda^{\times};\ F(0,0)=1\}.$$

Commentaires : 1) Pour la sous-représentation $\mathfrak{s}'/\mathfrak{s}''$, on obtient donc l'analogue du théorème 6 sans utiliser l'étude de la filtration du groupe des tresses.

2) Un calcul un peu plus fin permet de montrer que l'image de Ψ_1 est, en fait contenue dans $\{F\in\Lambda^{\times};\ F\equiv 1 \text{ mod. } uvw\}=1+uvw\Lambda$.

Démonstration : On a $C^3\mathfrak{s}=[\mathfrak{s},\mathfrak{s}']$. Ce groupe est donc engendré mod $\mathfrak{s}''$ par $[x,\mathfrak{s}']$ et $[y,\mathfrak{s}']$ or si $s\in\mathfrak{s}'$, $[x,s]=u.s$, $[y,s]=v.s$. En prenant $s=[x,y]$, on obtient donc $C^3\mathfrak{s}/\mathfrak{s}'' \xrightarrow[\sim]{I} u\Lambda+v\Lambda$. On a déjà vu (exemple 2,

chap. I) que l'action de $G_{\mathbb{Q}}$ sur $\mathcal{F}'/C^3\mathcal{F}$ est donnée par χ^2 et nous savons maintenant que ce $\mathbb{Z}_\ell$-module est isomorphe à $\mathcal{A}/u\mathcal{A}+v\mathcal{A} = \mathbb{Z}_\ell$. Enfin, si nous réduisons modulo $C^3\mathcal{F}$ la congruence :

$$\rho.[x,y] \equiv F_\rho(u,v).[x,y] \text{ mod. } \mathcal{F}''$$

nous obtenons :

$$\chi^2(\rho).[x,y] \equiv F_\rho(0,0).[x,y] \text{ mod. } C^3\mathcal{F}.$$

Si $\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})}$ nous avons donc $F_\rho(0,0)=1$.

Cette série F_ρ est considérée comme un analogue ℓ-adique de la fonction bêta d'Euler à cause de la série de propriétés dont elle jouit tant quant aux valeurs spéciales qu'elle prend que pour ce qui est des coefficients de $F_\rho(u,v)$.

III. Etude des propriétés de $F_\rho(u,v)$.

Commençons par les propriétés d'interpolation. On rappelle la décomposition de J_n (jacobienne de X_n) en variétés abéliennes de type C.M. :

Nous abrégeons ℓ^n en N.

Nous connaissons une base des différentielles régulières sur X_n, d'équation affine $x^N+y^N=1$:

$$\omega_{\alpha,\beta,\gamma} = x^{\alpha-1}\, y^{\beta-1}\, \frac{dx}{y^{N-1}}$$

pour $\alpha,\beta,\gamma \geq 1$ et $\alpha+\beta+\gamma=N$ (il y a $g(X_n)=\frac{(N-1)(N-2)}{2}$ tels triplets).

L'application des périodes relative à cette base est également connue :

$$H_1(X_n,\mathbb{Z}) \longrightarrow L_n \subset \mathbb{C}^{(N-1)(N-2)}$$

$$(1+u)^j.(1+v)^k.\mathcal{P}_n = x^j.y^k.\mathcal{P}_n \longrightarrow (\ldots,\zeta_n^{\alpha j+\beta k} \times \int_{\mathcal{P}_n} \omega_{\alpha,\beta,\gamma},\ldots)_{\substack{\alpha,\beta,\gamma\geq 1 \\ \alpha+\beta+\gamma=N}}$$

et

$$\int_{\mathcal{P}_n} \omega_{\alpha,\beta,\gamma} = (1-\zeta_n^{\alpha})(1-\zeta_n^{\beta}).\ \frac{1}{N}\ .B(\tfrac{\alpha}{N},\tfrac{\beta}{N})$$

où $B(u,v)=\int_0^1 x^{u-1}(1-x)^{v-1}dx$ est la fonction B d'Euler, et où ζ_n est la racine primitive $(\ell^n)^{\text{ième}}$ de l'unité définie par l'accouplement de Kummer :

$$\langle,\rangle_n : \mathcal{F} \times K^{\times}/K^{\times \ell^n} \longrightarrow \mu_{\ell^n} \subset \mathbb{C}^{\times}$$

par : $\zeta_n = \langle x,t\rangle_n = \langle y,1-t\rangle_n$.

On voit donc que l'action de $\mathcal{A}$ sur L_n est donnée par :

$$(3.1)\qquad \begin{cases} (1+u).(\Omega_{\alpha,\beta,\gamma}) = (\zeta_n^{\alpha}.\Omega_{\alpha,\beta,\gamma}) \\ (1+v).(\Omega_{\alpha,\beta,\gamma}) = (\zeta_n^{\beta}.\Omega_{\alpha,\beta,\gamma}). \end{cases}$$

Ceci permet de décomposer $J_n/_{\mathbb{Q}(\zeta_n)}$, à isogénie près, en produit de variétés abéliennes de type C.M. :

$$J_n \sim \prod_{m=1}^{n} \prod_{(a,b,c)\in\mathcal{L}_m} A_m^{a,b,c}$$

où $\mathcal{L}_m = \{(a,b,c)\in(\mathbb{Z}/\ell^m\mathbb{Z}\setminus\{0\})^3;\ \ell\nmid(a,b,c) \text{ et } a+b+c=0\}$.

et où la variété $A_m^{a,b,c}$, définie sur $\mathbb{Q}(\zeta_m)$ et à C.M. par $\mathbb{Q}(\zeta_m)$ est définie comme suit. On définit $X_{m/\mathbb{Q}(\zeta_m)}^{a,b,c}$ comme le quotient de la courbe X_m par le sous-groupe de $\mathrm{Gal}(K_m/K)$, noyau du caractère $\chi^{a,b,c}$: $\overline{x} \longrightarrow \zeta_m^a$, $\overline{y} \longrightarrow \zeta_m^b$, $\overline{z} \longrightarrow \zeta_m^c$. Le groupe de Galois du revêtement $X_m^{a,b,c} \longrightarrow \mathbb{P}^1$ est isomorphe à μ_{ℓ^m} (par le caractère $\chi^{a,b,c}$). L'algèbre $\mathbb{Z}[X]/(X^{\ell^m}-1)$ opère donc sur $\mathrm{Jac}(X_m^{a,b,c})$ par fonctorialité covariante. Donc $\mathbb{Z}[\zeta_m]$ opère sur $A_m^{a,b,c} = \dfrac{\mathrm{Jac}(X_m^{a,b,c})}{\mathrm{Ker}(\theta_m^{\ell^{m-1}}-\mathrm{Id})}$. On a un morphisme naturel $J_n \longrightarrow A_m^{a,b,c}$, composé de $J_n \longrightarrow J_m$ et de $\alpha : J_m \longrightarrow A_m^{a,b,c}$. L'espace cotangent de $A_m^{a,b,c}$ s'identifie par α^* au sous-espace de $H^0(X_m,\Omega)$ engendré par les $\omega_{\alpha,\beta,\gamma}$ pour (α,β,γ) dans :

$$\{(\langle ka\rangle_m, \langle kb\rangle_m, \langle kc\rangle_m);\ k\in(\mathbb{Z}/\ell^m\mathbb{Z})^{\times} \text{ et } \langle ka\rangle_m+\langle kb\rangle_m+\langle kc\rangle_m = \ell^m\}$$

où $\langle s\rangle_m$ consiste à prendre le reste $\in[0,\ell^m[$ de l'entier s dans la division par ℓ^m. Le cardinal de l'ensemble ci-dessus étant bien égal à $\frac{1}{2}[\mathbb{Q}(\zeta_m):\mathbb{Q}]$, on voit que $A_m^{a,b,c}$ est CM. Les formules (3.1) montrent alors que Λ opère sur $T_\ell A_m^{a,b,c}$ par la spécialisation :

(3.2) $$(u,v,w) \longrightarrow (\zeta_m^a-1, \zeta_m^b-1, \zeta_m^c-1).$$

Si l'on définit donc $\mathcal{P}_m^{a,b,c} \in T_\ell A_m^{a,b,c}$ comme l'image de $\mathcal{P}_n$ par l'application naturelle déduite de $J_n \longrightarrow A_m^{a,b,c}$, on obtient le :

Théorème 13. Pour tout F de Λ,

$$F.\mathcal{P}_m^{a,b,c} = F(\zeta_m^a-1, \zeta_m^b-1, \zeta_m^c-1).\mathcal{P}_m^{a,b,c}$$

le point . du second membre représente l'action de

$$\mathbb{Z}_\ell[\zeta_m] \quad \text{sur} \quad T_\ell A_m^{a,b,c}.$$

Les variétés $A_m^{a,b,c}$ apparaissent comme des auxiliaires utiles, grâce au théorème ci-dessus pour le calcul des spécialisations (3.2) de F_ρ :

Soit $p \neq \ell$ et $\mathfrak{p}_n$ une place de $\mathbb{Q}(\zeta_n)$ au-dessus de p. Soit $\rho = \mathrm{Frob}_{\mathfrak{p}_n}$. Le symbole $\mathcal{P}(\rho)$ est bien défini soit grâce au théorème 2, soit par le critère de Néron-Ogg-Shafarevitch appliqué à la variété abélienne J_n qui a bonne réduction en $\mathfrak{p}_n$.

Ihara calcule la spécialisation (3.2) de $\mathcal{P}(\rho) = F_\rho(u,v,w)$ comme la somme de Jacobi $J_{\ell^n}^{a,b,c}(\mathfrak{p}_n)$ définie comme suit :

Soit $\chi_{\mathfrak{p}_n}$ le caractère :

$$\mathbb{F}_q^\times = (\mathbb{Z}[\zeta_n]/\mathfrak{p}_n)^\times \longrightarrow \mu_{\ell^n} \subset \mathbb{Q}(\mu_{\ell^n})$$

défini par : $\chi_{\mathfrak{p}_n}(x) \equiv x^{\frac{q-1}{\ell^n}} \mod \mathfrak{p}_n$. On pose :

$$J_{\ell^n}^{a,b,c}(\mathfrak{p}_n) = -\sum_{x,y \in \mathbb{F}_q^\times} \chi_{\mathfrak{p}_n}^a(x)\, \chi_{\mathfrak{p}_n}^b(y).$$

La formule d'interpolation s'écrit alors :

Théorème 14. Avec les notations précédentes : pour tout $m \geq 1$ et tout $(a,b,c) \in \mathcal{L}_m$:

$$F_\rho(\zeta_m^a - 1, \zeta_m^b - 1, \zeta_m^c - 1) = J_{\ell^m}^{a,b,c}(\rho_m).$$

Commentaires : 1) Ces égalités caractérisent la représentation ρ_1 grâce au théorème de Cebotarev et au théorème préparatoire de Weierstrass.

2) La démonstration de ce théorème repose sur une idée de A. Weil développée dans [12].

Corollaire du théorème 14 (voir [6]).

Pour tout $\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})}$ on a les symétries :

(1) $F_\rho(u,v,w)$ est invariante par S_3.

(2) $F_\rho * F_\rho$ est invariante par S_4.

où, pour chaque $F(u,v) \in \mathcal{A}$, on note $F*F$ l'élément de $\mathcal{A}*\mathcal{A} = \mathbb{Z}_\ell[[u,v,u',v']]/((1+u)(1+v)(1+u')(1+v')-1)$ défini par $F*F(u,v,u',v') = F(u,v)F(u',v')$.

Remarque : 2) équivaut à la formule de 2-cocycle donnée dans l'introduction.

La démonstration de ce corollaire utilise le théorème 14 et le théorème préparatoire de Weierstrass pour se ramener aux propriétés de symétrie analogues des sommes de Jacobi, qui sont faciles à vérifier.

Démonstration du théorème 14 :

Grâce au théorème 13, on est ramené à montrer que Frob_{ρ_m} opère sur $T = T_\ell A_m^{a,b,c}$ par la somme de Jacobi de l'énoncé, disons π'. Or, Frob_{ρ_m} opère par le relèvement π dans $\mathbb{Z}[\zeta_m]$ de l'endomorphisme de Frobenius de la variété $A_m^{a,b,c}$ réduite modulo ρ_m, que nous notons $\tilde{A}$. Pour montrer $\pi = \pi'$ dans $\mathbb{Q}(\zeta_m)$, il suffit bien sûr de montrer que pour tout entier $k \geq 0$,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m^{-k}.\pi) = \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m^{-k}\pi'). \tag{3.3}$$

Soit θ_m l'automorphisme de la courbe $X_m^{a,b,c}$ correspondant à ζ_m dans l'isomorphisme :

$$\chi^{a,b,c} : \mathrm{Gal}(X_m^{a,b,c}/\mathbb{P}^1) \xrightarrow{\sim} \mu_{\ell^m}.$$

Il résulte de la définition de $A_m^{a,b,c}$ que le membre de gauche de (3.3) est égal à la trace de l'endomorphisme $f_{\tilde{A}}$ de $H_1(\tilde{A}) = H_1^{ét}(\tilde{A}\times\bar{\mathbb{F}}_q, \mathbb{Q}_\ell)$ déduit de $f_m = \theta_m^{-k}\circ(\mathrm{Frobenius}/\mathbb{F}_q)$. Or il y a une isogénie naturelle

$$\mathrm{Jac}(X_m^{a,b,c}) \longrightarrow A_m^{a,b,c} \times \mathrm{Jac}(X_{m-1}^{a,b,c}). \tag{3.4}$$

Toutes les variétés concernées ont bonne réduction en p_m. Posons $X(m) = \tilde{X}_m^{a,b,c}$. On tire de (3.4) une décomposition naturelle :

$$\begin{cases} H_1(X(m)) = H_1(\tilde{A}) \oplus H_1(X(m-1)). \\ \\ f_m = f_{\tilde{A}} \oplus f_{m-1}. \end{cases} \tag{3.5}$$

On applique alors le théorème du point fixe de Lefschetz ([9] théorème V.2.5) à f_j; $j = m-1, m$:

$$\#\{x\in X(j)(\bar{\mathbb{F}}_q); f_j x = x\} = 1 - \mathrm{Tr}(f_j; H_1(X(j))) + \mathrm{Tr}(f_j; H_2(X(j))) \tag{3.6$_j$}$$

mais $\mathrm{Tr}(f_j, H_2(X(j))) = \text{degré}(f_j) = \text{degré}(\mathrm{Frob.}/\mathbb{F}_q)$ et $\mathrm{Tr}(f_m; H_1(X(m))) = \mathrm{Tr}\, f_{\tilde{A}} + \mathrm{Tr}(f_{m-1}; H_1(X(m-1)))$. On obtient donc en soustrayant (3.6$_{m-1}$) à (3.6$_m$) :

$$-\mathrm{Tr}\, f_{\tilde{A}} = \#\{x\in X(m)(\bar{\mathbb{F}}_q); f_m x = x\} - \#\{x\in X(m-1)(\bar{\mathbb{F}}_q); f_{m-1} x = x\}.$$

Mais $f_m x = x$ équivaut à (3.7) $\theta_m^k\, x = x^q$. Cette relation implique en particulier que l'image t de x par le revêtement $\mathbb{F}_q$-rationnel $r_j : X(j) \longrightarrow \mathbb{P}^1$ satisfait $t^q = t$ i.e. $t\in\mathbb{P}^1(\mathbb{F}_q)$. Réciproquement, pour

$t \in \mathbb{P}^1(\mathbb{F}_q)$ non ramifié dans r_j (i.e. $\neq 0,1,\infty$), l'existence d'un $x \in r_j^{-1}(t)$ satisfaisant (3.7) équivaut à $(\frac{X(j)/\mathbb{P}^1}{t}) = \theta_j^k$ (symbole d'Artin relatif à l'extension abélienne $\mathbb{F}_q(X(m))/\mathbb{F}_q(\mathbb{P}^1)$).

Nous supposons pour simplifier que $\ell \nmid abc$; de sorte que r_j est totalement ramifié en $0,1,\infty$ (si $\ell \mid a$ par exemple, $\ell \nmid bc$ et la modification est très facile). On trouve alors :

$$
\begin{aligned}
-\mathrm{Tr}\, f_{\tilde{A}} &= \ell^m . \#\{t \in \mathbb{P}^1(\mathbb{F}_q)\setminus\{0,1,\infty\}; (\tfrac{X(m)/\mathbb{P}^1}{t}) = \theta_m^k\} \\
&\quad -\ell^{m-1}\#\{t \in \mathbb{P}^1(\mathbb{F}_q)\setminus\{0,1,\infty\}; (\tfrac{X(m-1)/\mathbb{P}^1}{t}) = \theta_{m-1}^k\} \\
&= -(\ell^m - \ell^{m-1}) \times \#\{t \in \mathbb{P}^1(\mathbb{F}_q)\setminus\{0,1,\infty\}; (\tfrac{X(m)/\mathbb{P}^1}{t}) = \theta_m^k\} \\
&\quad +\ell^{m-1}\#\{t \in \mathbb{P}^1(\mathbb{F}_q)\setminus\{0,1,\infty\}, (\tfrac{X(m)/\mathbb{P}^1}{t}).\theta_m^{-k}
\end{aligned}
\tag{3.8}
$$

est d'ordre exactement ℓ}.

Nous remarquons alors que le corps des fonctions de $X_m^{a,b,c}$ (resp. $X(m)$) est engendré sur K (resp. $\mathbb{F}_q(t)$) par une racine $(\ell^m)^{\text{ième}}$, s, de $t^{\langle a\rangle}(t-1)^{\langle b\rangle}$ (où $\langle\ \rangle$ désigne le reste dans la division par ℓ^m) et que le caractère $\chi^{a,b,c} : \mathrm{Gal}(X_m^{a,b,c}/\mathbb{P}^1) \xrightarrow{\sim} \mu_{\ell^m}$ n'est autre que le caractère Kummerien $\sigma \longrightarrow \langle \sigma, s\rangle = \sqrt[\ell^m]{s}^{\,\sigma-1}$.

Par conséquent, (3.8) peut s'écrire :

$$
-\sum_{t \in \mathbb{P}^1\mathbb{F}_q\setminus\{0,1,\infty\}} \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\chi^{a,b,c}((\tfrac{X(m)/\mathbb{P}^1}{t})\ \theta_m^{-k}))
$$

ou encore :

$$
= \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(-\sum_{\substack{t \in \mathbb{F}_q \\ t \neq 0,1}} \zeta_m^{-k} \times \chi_{p_m}(t^a \times (t-1)^b)) = \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m^{-k}\pi').
$$

Nous avons détaillé cette démonstration (pour $\ell \nmid abc$) car elle nous semble le point central de l'article [5]. Cependant un autre aspect de l'étude de $F_\rho(u,v)$ concerne les coefficients de cette série. L'idée sous-jacente est qu'une fonction bêta se doit de s'écrire $\frac{\Gamma(u)\Gamma(v)}{\Gamma(u+v)}$ en un

certain sens. Le premier théorème dans cette direction a été obtenu par G. Anderson en 1985 puis par Ihara-Kaneko-Yukinari [6] de manière plus élémentaire mais avec moins de généralité. Les théorèmes de I-K-Y. s'énoncent :

Théorème 15. Soit $U= \log(1+u)$, $V= \log(1+v)$ $W= \log(1+w)$ dans $\mathbb{Q}_\ell \bullet \mathcal{A}$. Pour tout $\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})}$ on a :

$$\log F_\rho(u,v,w)= \sum_{\substack{m\geq 3 \\ m \text{ impair}}} \frac{\beta_m(\rho)}{m!} (U^m+V^m+W^m)$$

où $\beta_m(\rho) \in \mathbb{Z}_\ell$ et définit un élément de

$$\mathrm{Hom}_{G_\infty}(\mathcal{G}_1, \mathbb{Z}_\ell(m)).$$

$G_\infty = \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$

Ω_ℓ = pro-ℓ-extension non ramifiée hors de ℓ maximale de $\mathbb{Q}(\mu_{\ell^\infty})$.

$\mathcal{G}_1 = \mathrm{Gal}(\Omega_\ell/\mathbb{Q}(\mu_{\ell^\infty}))$.

Théorème 16. Pour tout $\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})}$, il existe une série $\hat{G}_\rho(t) \in \hat{\mathbb{Z}}_\ell^{n.r.}[[t]]$ telle que :

$$F_\rho(u,v)= \frac{\hat{G}_\rho(u)\hat{G}_\rho(v)}{G_\rho(u[+]v)} \quad \text{où l'on pose} \quad u[+]v= u+v+uv.$$

Enfin, le théorème 10 de [5] relie les β_m et les homomorphismes de Coates-Wiles de manière très intéressante :

Soit $\Omega_\ell^{n.r}$ la pro-ℓ-extension non ramifiée maximale de $\mathbb{Q}(\mu_{\ell^\infty})$. Soit $\mathcal{G}_2 = \mathrm{Gal}(\Omega_\ell/\Omega_\ell^{n.v.})$. Soit U_n le groupe des unités locales principales de $\mathbb{Q}(\mu_{\ell^n})$, et $\mathcal{U} = \varprojlim U_n$, la limite étant prise relativement aux applications de normes locales. La théorie du corps de classes global fournit un isomorphisme canonique :

(3.9) $$\text{Artin} : \mathcal{U} \xrightarrow{\sim} \mathcal{G}_2^{ab}.$$

De plus, si l'on fixe une base (ζ_n) de $\mathbb{Z}_\ell(1)$, Coleman a démontré que pour tout élément $\epsilon = (\epsilon_n)$ de $\mathcal{U}$, il existe une unique série $f_\epsilon(t) \in \mathbb{Z}_\ell[[t]]^\times$ telle que $f_\epsilon(\zeta_n - 1) = \epsilon_n$. Soit $T = \log(1+t)$ et $D = (1+t)\frac{d}{dt} = \frac{d}{dT}$. Comme nous avons pris des unités principales, on a $f_\epsilon(o) \equiv 1 \bmod \ell$, donc $\log f_\epsilon(t) \in \mathbb{Z}_\ell[[t]]$ existe et nous pouvons écrire :

$$\log f_\epsilon(t)/f_\epsilon(o) = \sum_{m=1}^{\infty} \frac{\mathcal{P}_m(\epsilon)}{m!} T^m.$$

où

$$\mathcal{P}_m(\epsilon) = D^m \log f_\epsilon(t)\big|_{t=0}.$$

On voit facilement que $\mathcal{P}_m \in \mathrm{Hom}_{G_\infty}(\mathcal{U}, \mathbb{Z}_\ell(m))$. Si l'on compose m avec l'isomorphisme d'Artin (3.9), on obtient deux homomorphismes β_m, $\mathcal{P}_m$ dans $\mathrm{Hom}_{G_\infty}(\mathcal{U}, \mathbb{Z}_\ell(m))$. Un théorème d'Iwasawa montre que ce $\mathbb{Z}_\ell$-module est de rang 1 si m est impair et $m \neq 1$. La question du facteur de proportionalité est résolue par Ihara dans le

Théorème 17. Soit $L_\ell(s, \omega^{1-m})$ la fonction L ℓ-adique de Kubota-Leopoldt associée au caractère ω^{1-m}. Alors pour tout $m \geq 3$ impair, on a :

$$\beta_m = -L_\ell(m, \omega^{1-m}) . \mathcal{P}_m.$$

Un mot des démonstrations :
le théorème 15 ne fait intervenir que des calculs très élémentaires basés sur le corollaire du théorème 14 concernant les symétries de F_ρ ainsi que la congruence $F_\rho \equiv 1 \bmod. uvw$ pour $\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})}$.

Le théorème 16 utilise un résultat de Coleman [4] identifiant les β_m à des caractères Kummeriens de $\mathcal{C}_1$ pour lesquels l'énoncé analogue est démontré en utilisant un critère de Dwork pour l'intégralité des coefficients de séries dans $\hat{\mathbb{Q}}_\ell^{n.r.}[[t]]$ (voir [6]).

Le théorème 17 utilise à nouveau la multiplication complexe des $A_m^{a,b,c}$ et un lemme de Jannssen sur les idéaux $\mathcal{C}_n$ du lemme 9.

BIBLIOGRAPHIE

[1] G. Anderson.- The hyperadelic Gamma function : A Precis, Adv. Studies in Pure Math. Vol. 12, 1987.

[2] G. Anderson.- Torsion points on Fermat jacobians, Roots of Circular units and relative singular homology. Duke Journal (dédié à Manin), à paraître.

[3] G. Anderson.- The arithmetic life of the simplex. Exposé au Galois Workshop, M.S.R.I., Berkeley, Mars 1987.

[4] R. Coleman.- Anderson-Ihara Theory : Gauss Sums and Circular Units. Exposé au Iwasawa Workshop, M.S.R.I., Berkeley, Janvier 1987.

[5] Y. Ihara.- Profinite braid groups, Galois representations and complex multiplications. Ann. of Math. 123 (1987), 43-106.

[6] Y. Ihara, M. Kaneko, A. Yukinari.- On some properties of the universal power series for Jacobi sums. A paraître dans Adv. Studies in Pure Math. vol. 12, 1987.

[7] H. Koch.- Galoissche Theorie der p-Erweiterungen. V.E.B. Deutscher Verlag der Wissenschaften, Berlin (DDR), 1970.

[8] S. Lang.- Introduction to Algebraic and Abelian Functions, Grad. Texts in Math. 89, Springer-Verlga, 1982.

[9] J. Milne.- Etale Cohomology. P.U.P., 1980.

[10] J.-P. Murre.- Lectures on an Introduction to Grothendieck's Theory of the Fundamental Group. Tata Institute of Fundamental Research, Bombay, 1967.

[11] D. Rohrlich.- The periods of the Fermat Curve, Appendix to B. Gross, Inv. Math. 45 (1978), 193-221.

[12] A. Weil.- Number of solutions of equations in finite fields, [1949 b] in Collected Papers, volume I, Springer-Verlag, 1980.

Université Paris 11
Mathématiques, UA 753
Bâtiment 425
91405 ORSAY