

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

JACQUES VÉLU

Le groupe cuspidal des courbes de Fermat

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 20, n° 2 (1978-1979),
exp. n° 28, p. 1-11

http://www.numdam.org/item?id=SDPP_1978-1979__20_2_A5_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1978-1979, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

LE GROUPE CUSPIDAL DES COURBES DE FERMAT

par Jacques VÉLU ⁽¹⁾

[Université de Caen]

I. Introduction.

Soit N un entier impair ≥ 1 . La courbe F_N de genre $((N-1)(N-2))/2$ définie sur $\mathbb{Q}$ par l'équation projective non singulière

$$X^N + Y^N + Z^N = 0$$

possède sur le corps $\mathbb{Q}(\mu_N)$ les $3N$ points suivants :

$$\begin{aligned} (1) \quad A(\alpha) &= (0 : -\zeta^\alpha : 1) \\ B(\beta) &= (1 : 0 : -\zeta^\beta) \\ C(\gamma) &= (-\zeta^\gamma : 1 : 0) \end{aligned}$$

où $\zeta = e^{2\pi i/N}$ et α, β, γ parcourent $\mathbb{Z}/N\mathbb{Z}$. Nous nommerons ces points les "pointes" de F_N ⁽²⁾ et, dans la suite, les lettres α, β et γ désigneront toujours des éléments de $\mathbb{Z}/N\mathbb{Z}$.

Les fonctions

$$(2) \quad x = \frac{Y}{Z}, \quad y = \frac{Z}{X}, \quad z = \frac{X}{Y}$$

ont pour diviseurs

$$\begin{aligned} (3) \quad \operatorname{div} x &= \sum_{\beta} B(\beta) - \sum_{\gamma} C(\gamma) \\ \operatorname{div} y &= \sum_{\gamma} C(\gamma) - \sum_{\alpha} A(\alpha) \\ \operatorname{div} z &= \sum_{\alpha} A(\alpha) - \sum_{\beta} B(\beta). \end{aligned}$$

De plus,

$$\begin{aligned} (4) \quad \operatorname{div}(x + \zeta^\alpha) &= NA(\alpha) - \sum_{\gamma} C(\gamma) \\ \operatorname{div}(y + \zeta^\beta) &= NB(\beta) - \sum_{\alpha} A(\alpha) \\ \operatorname{div}(z + \zeta^\gamma) &= NC(\gamma) - \sum_{\beta} B(\beta). \end{aligned}$$

Soit J la jacobienne de F_N . Appelons groupe cuspidal le sous-groupe C_N de $J(\mathbb{Q}(\mu_N))$ engendré par les diviseurs de degré 0 de F_N dont le support est formé

⁽¹⁾ Texte reçu le 3 janvier 1980.

Jacques VELU, Mathématiques pures, Université de Caen, Esplanade de la Paix, 14032 CAEN CEDEX.

⁽²⁾ Dans [1] la surface de Riemann $F_N(\mathbb{C})$ est décrite comme quotient du demi-plan de Poincaré par un sous-groupe de $SL(2, \mathbb{Z})$ et les pointes de F_N sont les pointes au sens modulaire.

de pointes, c'est-à-dire l'ensemble des expressions

$$(5) \quad R = \sum_{\alpha} \lambda(\alpha) A(\alpha) + \sum_{\beta} \mu(\beta) B(\beta) + \sum_{\gamma} \nu(\gamma) C(\gamma) ,$$

où $\lambda(\alpha)$, $\mu(\beta)$, $\nu(\gamma)$ désignent des entiers tels que

$$\sum_{\alpha} \lambda(\alpha) + \sum_{\beta} \mu(\beta) + \sum_{\gamma} \nu(\gamma) = 0 .$$

Les relations (4) montrent que

$$(6) \quad \begin{aligned} NR &= \operatorname{div} \prod_{\alpha, \beta, \gamma} (x + \zeta^{\alpha})^{\lambda(\alpha)} (y + \zeta^{\beta})^{\mu(\beta)} (z + \zeta^{\gamma})^{\nu(\gamma)} x^{\sum_{\gamma} \nu(\gamma)} y^{-\sum_{\beta} \mu(\beta)} , \\ &= \prod_{\alpha, \beta, \gamma} (Y + \zeta^{\alpha} Z)^{\lambda(\alpha)} (Z + \zeta^{\beta} X)^{\mu(\beta)} (X + \zeta^{\gamma} Y)^{\nu(\gamma)} , \end{aligned}$$

et par conséquent C_N est un groupe abélien fini annulé par N .

Dans [2], ROHRLICH a démontré ⁽³⁾, après des calculs effrayants, le théorème suivant.

THÉOREME 1. - Si $N > 1$, le groupe C_N est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^{3N-7}$.

Nous nous proposons d'en donner ici une démonstration moins pénible, et d'apporter quelques compléments, par exemple, l'action de $\operatorname{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ sur C_N .

THÉOREME 2. - En tant que $\operatorname{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ -module, C_N est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mu_3$ si $N = 3$, et à $(\mathbb{Z}/N\mathbb{Z})^2 \times (\mu_N^{\otimes N-2}) \times (\mu_N^{\otimes N-3})^2 \times (\prod_{k=1}^{N-4} \mu_N^{\otimes k})^3$ si N est premier impair différent de 3 .

La démonstration du théorème 1 consiste à calculer $e(R, D)$, le symbole de Weil d'un élément R de C_N et d'un point D d'ordre N de $J(\overline{\mathbb{Q}})$, ce qui permet grâce à la non dégénérescence de ce symbole de déterminer toutes les relations liant les éléments de C_N .

II. L'homologie entière de F_N .

1. Automorphismes de F_N .

Notons π le morphisme de F_N dans F_1 défini par $\pi(X:Y:Z) = (X^N:Y^N:Z^N)$. Posons

$$A = \pi(A(\alpha)) , \quad B = \pi(B(\beta)) , \quad C = \pi(C(\gamma)) .$$

Alors F_N est un revêtement de F_1 , ramifié seulement en A , B et C , de degré N^2 , et F_1 est le quotient de F_N par l'action du groupe d'automorphismes Λ_N de F_N , isomorphe à μ_N^2 , engendré par

$$a : (X : Y : Z) \mapsto (\zeta X : Y : Z)$$

$$b : (X : Y : Z) \mapsto (X : \zeta Y : Z)$$

$$c : (X : Y : Z) \mapsto (X : Y : \zeta Z) .$$

⁽³⁾ ROHRLICH étudie la courbe $X^N + Y^N = Z^N$ sans restriction de parité sur N ; notre méthode s'étend sans difficulté au cas où N est pair.

Tout élément de Λ_N est de la forme $a^\alpha b^\beta c^\gamma$, et $a^\alpha b^\beta c^\gamma = 1$ si, et seulement si, $\alpha = \beta = \gamma$.

L'action de a , b , c sur les pointes est donnée par

(7)

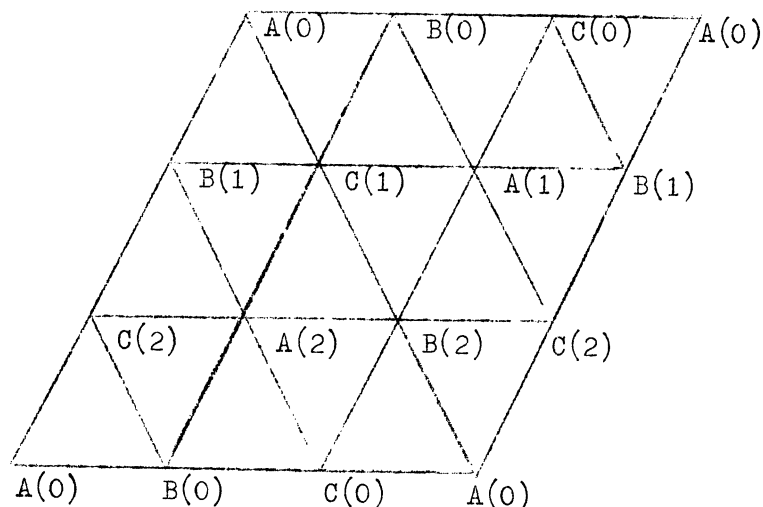
	$A(\alpha)$	$B(\beta)$	$C(\gamma)$
a	$A(\alpha)$	$B(\beta - 1)$	$C(\gamma + 1)$
b	$A(\alpha + 1)$	$B(\beta)$	$C(\gamma - 1)$
c	$A(\alpha - 1)$	$B(\beta + 1)$	$C(\gamma)$

Enfin, le groupe $\mathbb{G}_3$ opère sur F_N par échange des coordonnées X , Y et Z , et nous donnerons toujours les résultats sous une forme symétrique pour cette action.

2. La triangulation cuspidale de F_N .

Le lieu $F_1(\mathbb{R}) \subset F_1(\mathbb{C})$ est un cercle passant par A , B , C qui partage la sphère $F_1(\mathbb{C})$ en deux triangles T^+ et T^- dont il porte les 3 côtés communs $[AB]$, $[BC]$ et $[CA]$. Dans $F_N(\mathbb{C})$, l'ensemble $\pi^{-1}(F_1(\mathbb{R}))$ est la réunion des arêtes d'une triangulation τ que nous appellerons la triangulation cuspidale de F_N . Elle a pour sommets les $3N$ pointes de F_N ; ses arêtes sont les $3N^2$ relèvements $[A(\alpha) B(\beta)]$, $[B(\beta) C(\gamma)]$ et $[C(\gamma) A(\alpha)]$ de $[AB]$, $[BC]$ et $[CA]$; quant à ses $2N^2$ faces ce sont les triangles $[A(\alpha) B(\beta) C(\gamma)]$, avec $\alpha + \beta + \gamma = \pm \frac{1}{2}$ selon que $\pi[A(\alpha) B(\beta) C(\gamma)] = T^+$ ou T^- .

Remarque. - Par relèvement, nous pouvons déduire de τ une triangulation d'un revêtement universel U de $F_N(\mathbb{C})$, et un domaine fondamental dans U représentant $F_N(\mathbb{C})$. Quand $N = 3$, U est isomorphe à $\mathbb{C}$, et nous obtenons



pour domaine fondamental, retrouvant ainsi le réseau des périodes de la courbe elliptique $X^3 + Y^3 + Z^3 = 0$.

3. Les différentielles holomorphes de F_N .

L'espace vectoriel des différentielles holomorphes de F_N admet pour base les $((N-1)(N-2))/2$ différentielles

$$w(\lambda\mu\nu) = X^\lambda Y^\mu Z^\nu \left[\frac{1}{Z^N} \left(\frac{dX}{X} - \frac{dY}{Y} \right) \right] = z^{\lambda-1} x^{N-\nu} dz ,$$

où $\lambda + \mu + \nu = N$ et $\lambda > 0$, $\mu > 0$, $\nu > 0$. On remarquera que $(1/Z^N)(\frac{dX}{X} - \frac{dY}{Y})$ est invariante par permutation circulaire sur X , Y , Z et que

$$(8) \quad \text{div } w(\lambda\mu\nu) = (\lambda-1) \sum_{\alpha} A(\alpha) + (\mu-1) \sum_{\beta} B(\beta) + (\nu-1) \sum_{\gamma} C(\gamma) .$$

L'action de Λ_N sur ces différentielles est donnée par

$$a^\alpha b^\beta c^\gamma w(\lambda\mu\nu) = \zeta^{\lambda\alpha+\mu\beta+\nu\gamma} w(\lambda\mu\nu) .$$

Le groupe $H_1(F_N(\mathbb{C}), \mathbb{Z})$ est un module sous l'action de $\mathbb{Z}[\Lambda_N]$. Si

$$t \longmapsto (z(t), x(t), y(t))$$

est un chemin g dans $F_N(\mathbb{C})$, alors $a^\alpha b^\beta c^\gamma g$ est le chemin

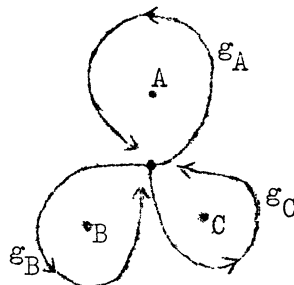
$$t \longmapsto (\zeta^{\alpha-\beta} z(t), \zeta^{\beta-\gamma} x(t), \zeta^{\gamma-\alpha} y(t)) ,$$

et nous avons

$$(10) \quad \int_{a^\alpha b^\beta c^\gamma g} w(\lambda\mu\nu) = \zeta^{\lambda\alpha+\mu\beta+\nu\gamma} \int_g w(\lambda\mu\nu) .$$

4. Le $\mathbb{Z}[\Lambda_N]$ -module $H_1(F_N(\mathbb{C}), \mathbb{Z})$.

Soit $F'_1 = F_1(\mathbb{C}) - \{A, B, C\}$. Alors $F'_N = \pi^{-1}(F'_1)$ est un revêtement non ramifié de F'_1 , et F'_1 est le quotient de F'_N par Λ_N . Fixons un point $u_N \in F'_N$, et posons $u_1 = \pi(u_N)$. Par la projection π , le groupe $G_N = \pi_1(F_N(\mathbb{C}), u_N)$ s'injecte dans $G_1 = \pi_1(F'_1, u_1)$ de sorte que son image H_N s'identifie avec les classes de lacets dont les indices, par rapport à A , B et C , sont divisibles par N . Le quotient G_1/H_N est isomorphe à Λ_N , donc à $(\mathbb{Z}/N\mathbb{Z})^2$. Or G_1 est engendré par g_A , g_B et g_C



qui sont liés par la relation $g_C g_B g_A = 1$; comme c'est un groupe libre à deux générateurs, g_A et g_B par exemple, nous obtenons immédiatement que H_N est le sous-groupe de G_1 engendré par g_A^N , g_B^N , g_C^N et les éléments de la forme $g^{-1}(g_B g_C g_A) g$ avec g dans G_1 .

Dans F'_N les relèvements de g_A^N , g_B^N et g_C^N consistent chacun en un tour

autour d'une pointe et sont donc homologues à zéro dans $F_N(\mathbb{C})$. D'autre part, si g est un lacet de F_1^i dont le relèvement dans F_N^i a pour extrémités u_N et u_N^i , il existe $\lambda \in \Lambda_N$ tel que $\lambda(u_N) = u_N^i$, et pour tout lacet h de F_N^i , le relèvement dans F_N^i du lacet $g^{-1}(\pi h) g$ de F_1^i est homologue à $\lambda(h)$. D'où le théorème suivant.

THÉOREME 3. - Le $\mathbb{Z}[\Lambda_N]$ -module $H_1(F_N(\mathbb{C}), \mathbb{Z})$ est engendré par un relèvement h quelconque dans F_N^i de $\mathcal{E}_B \mathcal{E}_C \mathcal{E}_A$.

Nous allons donner maintenant une amélioration quantitative de ce résultat en calculant $N[A(\alpha) C(\gamma)]$, $N[C(\gamma) B(\beta)]$ et $N[B(\beta) A(\alpha)]$ en fonction de h .

5. Calcul d'intégrales.

Soient α, β, γ dans $\mathbb{Z}/N\mathbb{Z}$ tels que $\alpha + \beta + \gamma = 0$. L'image de $(0, 1)$ dans $F_N(\mathbb{C})$ par l'application

$$t \mapsto (z(t), x(t), y(t)) = (-\zeta^\gamma t, -\zeta^\alpha(1-t^N)^{-1/N}, \zeta^\beta t^{-1}(1-t^N)^{1/N})$$

est l'arête $[A(\alpha) C(\gamma)]$ de la triangulation cuspidale. Par conséquent,

$$\int_{A(\alpha)}^{C(\gamma)} w(\lambda\mu\nu) = (-1)^\mu \zeta^{\lambda\gamma-\nu\alpha} \int_0^1 t^{\lambda-1}(1-t^N)^{(\nu-N)/N} dt,$$

ce qui donne, en posant $t = u^{1/N}$,

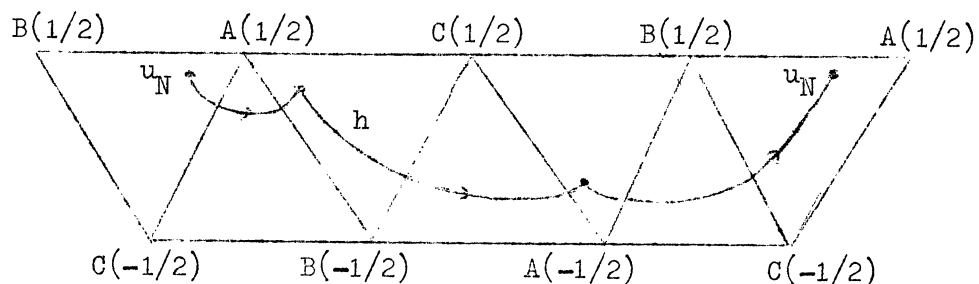
$$\int_{A(\alpha)}^{C(\gamma)} w(\lambda\mu\nu) = (-1)^\mu \frac{\zeta^{\lambda\gamma-\nu\alpha}}{N} \int_0^1 u^{(\lambda/N)-1}(1-u)^{(\nu/N)-1} du.$$

Or, l'intégrale du membre de droite vaut $(\Gamma(\lambda/N) \Gamma(\nu/N)) / \Gamma((\lambda + \nu)/N)$.

La formule des compléments de la fonction Γ et la symétrie des formules sous l'action de $\mathcal{E}_3$ donnent

$$(11) \quad \begin{aligned} \int_{A(\alpha)}^{C(\gamma)} w(\lambda\mu\nu) &= (-1)^\mu \sin \frac{\pi\mu}{N} \zeta^{\lambda\gamma-\nu\alpha} \frac{\Gamma(\lambda/N) \Gamma(\mu/N) \Gamma(\nu/N)}{\pi N} \\ \int_{C(\gamma)}^{B(\beta)} w(\lambda\mu\nu) &= (-1)^\lambda \sin \frac{\pi\lambda}{N} \zeta^{\nu\beta-\mu\gamma} \frac{\Gamma(\lambda/N) \Gamma(\mu/N) \Gamma(\nu/N)}{\pi N} \\ \int_{B(\beta)}^{A(\alpha)} w(\lambda\mu\nu) &= (-1)^\nu \sin \frac{\pi\nu}{N} \zeta^{\mu\alpha-\lambda\beta} \frac{\Gamma(\lambda/N) \Gamma(\mu/N) \Gamma(\nu/N)}{\pi N} \end{aligned}$$

Nous choisissons maintenant un relèvement de h de $\mathcal{E}_B \mathcal{E}_C \mathcal{E}_A$ dans F_N^i en prenant pour u_N un point du triangle $[A(1/2) B(1/2) C(-1/2)]$. Alors h est homologue dans F_N au lacet réunion des arêtes $[A(1/2) C(1/2)]$, $[C(1/2) B(1/2)]$ et $[B(1/2) A(1/2)]$.



On remarquera que la classe de h dans $H_1(F_N(\mathbb{C}), \mathbb{Z})$ est stable par conjugaison complexe.

Si G est un groupe cyclique d'ordre N écrit multiplicativement, et si $g \in G$, nous notons $g^{1/2} = g^{(N+1)/2}$; c'est l'unique élément g' de G tel que $g'^2 = g$. Avec cette notation nous avons

$$(-1)^\lambda \sin \frac{\pi \lambda}{N} = \frac{\zeta^{\lambda/2} - \zeta^{-\lambda/2}}{2i},$$

et des formules analogues pour μ et ν , de sorte que

$$(12) \quad \int_h w(\lambda \mu \nu) = \frac{\Gamma(\lambda/N) \Gamma(\mu/N) \Gamma(\nu/N)}{2\pi i N} (\zeta^{-\lambda/2} - \zeta^{\lambda/2}) (\zeta^{-\mu/2} - \zeta^{\mu/2}) (\zeta^{-\nu/2} - \zeta^{\nu/2})$$

ou encore

$$(13) \quad \int_h w(\lambda \mu \nu) = \frac{4\Gamma(\lambda/N) \Gamma(\mu/N) \Gamma(\nu/N)}{\pi N} \sin \frac{\pi \lambda}{N} \sin \frac{\pi \mu}{N} \sin \frac{\pi \nu}{N}.$$

Il résulte des formules (11) et (12) que

$$(14) \quad \int_{A(\alpha)}^{C(\gamma)} w(\lambda \mu \nu) = \frac{\zeta^{\lambda \gamma - \nu \alpha}}{(\zeta^{\lambda/2} - \zeta^{-\lambda/2})(\zeta^{\nu/2} - \zeta^{-\nu/2})} \int_h w(\lambda \mu \nu).$$

Or $H_1(F_N(\mathbb{C}), \mathbb{Q}) = H_1(F_N(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$ est un $\mathbb{Q}[\Lambda_N]$ -module et dans $\mathbb{Q}[\Lambda_N]$ les éléments $a^{1/2} - a^{-1/2}$, $b^{1/2} - b^{-1/2}$ et $c^{1/2} - c^{-1/2}$ sont inversibles, de sorte que nous pouvons réécrire (14) comme les égalités suivantes dans le $\mathbb{Q}[\Lambda_N]$ - $H_1(F_N(\mathbb{C}), \mathbb{Q})$:

$$(15) \quad \begin{aligned} [A(\alpha) C(\gamma)] &= \frac{a^\gamma c^{-\alpha}}{(a^{1/2} - a^{-1/2})(c^{1/2} - c^{-1/2})} \cdot h \\ [C(\gamma) B(\beta)] &= \frac{c^\beta b^{-\gamma}}{(c^{1/2} - c^{-1/2})(b^{1/2} - b^{-1/2})} \cdot h \\ [B(\beta) A(\alpha)] &= \frac{b^\alpha a^{-\beta}}{(b^{1/2} - b^{-1/2})(a^{1/2} - a^{-1/2})} \cdot h. \end{aligned}$$

Enfin, grâce à l'identité

$$\sum_{k=1}^{N-1} (a^k - 1)(c^k - 1) = N,$$

nous pouvons réécrire (15) sous la forme

$$(16) \quad \begin{aligned} [A(\alpha) C(\gamma)] &= \frac{a^{\gamma+1/2} c^{-\alpha+1/2}}{N} \sum_{k=1}^{N-1} \left(\frac{a^k - 1}{a - 1} \right) \left(\frac{c^k - 1}{c - 1} \right) \cdot h \\ [C(\gamma) B(\beta)] &= \frac{c^{\beta+1/2} b^{-\gamma+1/2}}{N} \sum_{k=1}^{N-1} \left(\frac{c^k - 1}{c - 1} \right) \left(\frac{b^k - 1}{b - 1} \right) \cdot h \\ [B(\beta) A(\alpha)] &= \frac{b^{\alpha+1/2} a^{-\beta+1/2}}{N} \sum_{k=1}^{N-1} \left(\frac{b^k - 1}{b - 1} \right) \left(\frac{a^k - 1}{a - 1} \right) \cdot h. \end{aligned}$$

III. Le symbole de Weil

1. Rappel.

Soient C une courbe projective non singulière définie sur $\mathbb{C}$, N un entier

≥ 1 , D un diviseur de C , et f une fonction sur C telle que

$$\operatorname{div} f = ND.$$

En adjoignant au corps des fonctions de C , g telle que $g^N = f$, on obtient le corps des fonctions d'un revêtement non ramifié C' de C possédant un groupe d'automorphismes G isomorphe à μ_N , et C est le quotient de C' par l'action de G . Si $\sigma : [0, 1] \rightarrow C(\mathbb{C})$ est un lacet tel que $\sigma(0) = \sigma(1) = u$ n'appartient pas au support de D , et si σ' est un relèvement de σ à $C'(\mathbb{C})$ tel que $\sigma'(0) = u'$, et $\sigma'(1) = u'_2$, alors u'_2 et u'_1 ont pour image u dans C et

$$\left[\frac{g(u'_2)}{g(u'_1)} \right]^N = \frac{f(u)}{f(u)} = 1.$$

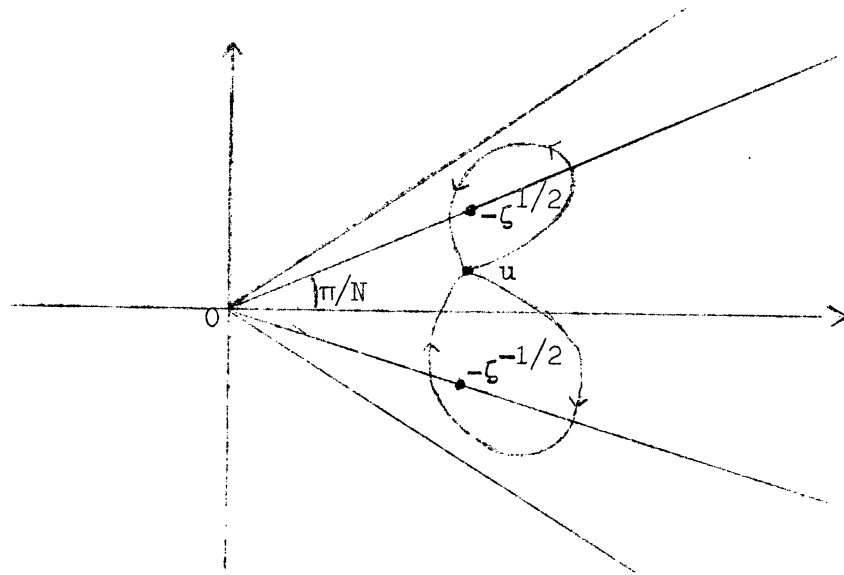
L'application qui associe $(g(u'_2)/g(u'_1))$ à σ' ne dépend que de la classe de σ dans $\Omega = H_1(C(\mathbb{C}), \mathbb{Z})$ qui n'est autre que le réseau des périodes de la jacobienne J de C . On construit ainsi un homomorphisme de $\Omega/N\Omega$ dans μ_N , qui ne dépend en fait que de l'image de D dans J . D'où un accouplement entre le groupe J_N des points d'ordre N de J et $\Omega/N\Omega$ qui est isomorphe à $\frac{1}{N}\Omega/\Omega$ et à J_N ; c'est le symbole de Weil. Enfin, si a est un automorphisme de C , l'accouplement $e(D, a\sigma)$ peut être calculé par la méthode précédente soit à l'aide du lacet $a\sigma$ et de la fonction f , soit à l'aide du lacet σ et de la fonction $f \circ a$ dont le diviseur est $a^{-1}D$, ce qui donne

$$(17) \quad e(D, a\sigma) = e(a^{-1}D, \sigma).$$

2. Le calcul des symboles de Weil.

Nous allons appliquer ce qui vient d'être écrit aux diviseurs D de F_N ayant pour support des pointes de F_N . Il résulte du théorème 3 et de (17) qu'il suffit de calculer $e(R, h)$ pour un élément quelconque R de C_N afin de connaître complètement l'accouplement entre C_N et $H_1(F_N(\mathbb{C}), \mathbb{Z})$.

Il est facile de suivre les valeurs prises par la fonction x quand on parcourt le lacet h .



Elles décrivent successivement deux boucles autour de $-\zeta^{1/2}$ et $-\zeta^{-1/2}$, la première dans le sens positif, la seconde dans le sens négatif. Par conséquent, l'indice de 0 est nul par rapport au lacet décrit par y , mais, par rapport au lacet décrit par $x + \zeta^\alpha$, il est égal à $+1$ si $\alpha = 1/2$, à -1 si $\alpha = -1/2$, et est nul dans les autres cas. Posons

$$\varepsilon(\alpha) = \begin{cases} \zeta & \text{si } \alpha = 1/2 \\ \zeta^{-1} & \text{si } \alpha = -1/2 \\ 1 & \text{sinon.} \end{cases}$$

Alors entre l'extrémité et l'origine de h la fonction $\sqrt[N]{x + \zeta^\alpha}$ est multipliée par $\varepsilon(\alpha)$ tandis que $\sqrt[N]{x}$ est invariante. On montre de même que $\sqrt[N]{y + \zeta^\beta}$ est multipliée par $\varepsilon(\beta)$, que $\sqrt[N]{z + \zeta^\gamma}$ est multipliée par $\varepsilon(\gamma)$, et que $\sqrt[N]{y}$ et $\sqrt[N]{z}$ sont invariantes.

Nous sommes en mesure d'énoncer la proposition suivante.

PROPOSITION. - Soit R l'élément de C_N défini par (5). Alors

$$e(R, a^\ell b^m c^n h) = \zeta^P$$

avec

$$(18) \quad P = \lambda(1/2+m-n) - \lambda(-1/2+m-n) + \mu(1/2+n-\ell) - \mu(-1/2+n-\ell) \\ + \nu(1/2+\ell-m) - \nu(-1/2+\ell-m).$$

En effet, $e(R, a^\ell b^m c^n h) = e(a^{-\ell} b^{-m} c^{-n} R, h)$ d'après (17) et

$$a^{-\ell} b^{-m} c^{-n} R = \sum_{\alpha} \lambda(\alpha+m-n) A(\alpha) + \sum_{\beta} \mu(\beta+n-\ell) B(\beta) + \sum_{\gamma} \nu(\gamma+\ell-m) C(\gamma).$$

La formule (6) permet d'écrire une fonction dont le diviseur est $a^{-\ell} b^{-m} c^{-n} R$. Elle est le produit, avec des puissances convenables de x , y , z , $x + \zeta^\alpha$, $y + \zeta^\beta$, $z + \zeta^\gamma$, et l'étude qui vient d'être faite montre qu'entre l'extrémité et l'origine de h elle est multipliée par

$$\prod_{\alpha, \beta, \gamma} \varepsilon(\alpha)^{\lambda(\alpha+m-n)} \varepsilon(\beta)^{\mu(\beta+n-\ell)} \varepsilon(\gamma)^{\nu(\gamma+\ell-m)}$$

ce qui, compte tenu de la définition de ε , donne le résultat énoncé dans la proposition.

3. Les relations dans C_N .

Pour que R défini par (5) soit nul, il faut et il suffit que $e(R, a^\ell b^m c^n h) = 1$ pour tous ℓ , m et n car le symbole de Weil est non dégénéré. Par conséquent, il faut et il suffit que P , défini par (18), soit nul modulo N .

PROPOSITION. - Soient λ , μ , ν trois fonctions de $\mathbb{Z}/N\mathbb{Z}$ dans lui-même

telles que

$$(19) \quad \begin{aligned} \lambda(1/2+m-n) - \lambda(-1/2+m-n) + \mu(1/2+n-l) - \mu(-1/2+n-l) \\ + \nu(1/2+l-m) - \nu(-1/2+l-m) = 0 . \end{aligned}$$

identiquement. Alors il existe u, v, w, u', v', w' et M dans $\mathbb{Z}/N\mathbb{Z}$ tels que

$$(20) \quad \begin{aligned} \lambda(t) &= u + u' t + Mt^2 \\ \mu(t) &= v + v' t + Mt^2 \\ \nu(t) &= w + w' t + Mt^2 \end{aligned}$$

et ces nombres sont liés par la seule relation

$$(21) \quad u' + v' + w' = 0 .$$

Preuve. - On a

$$\nu(t) - \nu(t-1) = \mu(-t) - \mu(1-t) + \lambda(-1/2) - \lambda(1/2)$$

en faisant $m = n = 0$ et $l = t - 1/2$ dans (19), et par récurrence sur t

$$(22) \quad \nu(t) = \nu(0) - \mu(0) + \mu(-t) + t[\lambda(-1/2) - \lambda(1/2)] .$$

De même, en faisant $l = m = 0$ et $n = 1/2 - t$ dans (19), on obtient successivement

$$\lambda(t) - \lambda(t-1) = \mu(-t) - \mu(1-t) + \nu(-1/2) - \nu(1/2)$$

et par récurrence sur t

$$(23) \quad \lambda(t) = \lambda(0) - \mu(0) + \mu(-t) + t[\nu(-1/2) - \nu(1/2)] .$$

Enfin, en faisant $l = m = n = 0$ dans (19), il vient

$$(24) \quad \lambda(-1/2) - \lambda(1/2) + \mu(-1/2) - \mu(1/2) + \nu(1/2) - \nu(-1/2) = 0 .$$

On reporte (22), (23) et (24) dans (19) afin d'obtenir

$$\begin{aligned} \mu(-1/2 - m + n) + \mu(-1/2 - l + m) + \mu(1/2 + n - l) + \mu(1/2) \\ = \mu(1/2 - m + n) + \mu(1/2 - l + m) + \mu(-1/2 + n - l) + \mu(-1/2) . \end{aligned}$$

Ensuite, on écrit cette égalité, d'abord avec $m - l = 1/2$ et $n - m = t - 1/2$, puis avec $m - l = 1/2$ et $n - m = t$, et on ajoute membre à membre pour trouver

$$\mu(t+1) - 2\mu(t) + \mu(t-1) = 2[\mu(1) - \mu(0) + \mu(-1/2) - \mu(1/2)] .$$

Cette équation fonctionnelle montre que les différences secondes de la fonction μ sont constantes. Par conséquent, il existe v, v' et M tels que

$$\mu(t) = v + v' t + Mt^2 .$$

En conduisant le calcul de façon semblable pour les fonctions λ et ν on montre qu'elles aussi sont des polynômes du second degré en t . Enfin, en repor-

tant ce résultat dans (19) on voit que le coefficient de t^2 est le même pour λ , μ et ν et que (21) doit être vérifié. On peut d'ailleurs calculer les coefficients des trinômes définissant λ , μ , ν en fonction de leurs valeurs en 0 et $\pm 1/2$ ce que donne

$$\lambda(t) = \lambda(0) + t[\lambda(1/2) - \lambda(-1/2)] + 2t^2[\lambda(1/2) - 2\lambda(0) + \lambda(-1/2)]$$

$$\mu(t) = \mu(0) + t[\mu(1/2) - \mu(-1/2)] + 2t^2[\mu(1/2) - 2\mu(0) + \mu(-1/2)]$$

$$\nu(t) = \nu(0) + t[\nu(1/2) - \nu(-1/2)] + 2t^2[\nu(1/2) - 2\nu(0) + \nu(-1/2)]$$

et (21) n'est autre que (24).

A présent nous pouvons terminer la démonstration du théorème 1. D'après la proposition précédente, les solutions (λ, μ, ν) de (19) sont combinaisons linéaires modulo N des 7 solutions particulières.

$\lambda(t)$	$\mu(t)$	$\nu(t)$
1	0	0
0	1	0
0	0	1
t	$-t$	0
0	t	$-t$
$-t$	0	t
t^2	t^2	t^2

ce qui montre que les éléments de C_N sont liés par les relations suivantes, où P désigne une pointe quelconque,

$$\begin{aligned} \sum_{\alpha} [A(\alpha) - P] &= 0, & \sum_{\beta} [B(\beta) - P] &= 0, & \sum_{\gamma} [C(\gamma) - P] &= 0 \\ \sum_k k[A(k) - B(k)] &= 0, & \sum_k k[B(k) - C(k)] &= 0, & \sum_k k[C(k) - A(k)] &= 0 \\ \sum_k k^2[A(k) + B(k) + C(k) - 3P] &= 0 \end{aligned}$$

et que toute relation liant les pointes dans C_N est combinaison de celles-ci et de (4).

Pour démontrer le théorème 2, supposons N premier > 3 , le cas $N = 3$ se traitant directement du fait que F_3 est une courbe elliptique.

Les diviseurs $B(0) - A(0)$ et $C(0) - A(0)$ engendrent un groupe isomorphe à $(\mathbb{Z}/N\mathbb{Z})^2$ car il n'existe pas dans C_N , quand $N > 3$, de relation de la forme $\lambda A(0) + \mu B(0) + \nu C(0) = 0$ avec $\lambda + \mu + \nu = 0$. Ensuite,

$$\sum_{k=1}^{N-1} k^r [A(k) - A(0)], \quad \sum_{k=1}^{N-1} k^r [B(k) - A(0)],$$

et

$$\sum_{k=1}^{N-1} k^r [C(k) - A(0)]$$

engendrent dans C_N des groupes isomorphes à $\mu^{\otimes N-r-1}$ et la connaissance des relations liant les éléments de C_N permet de déterminer quels sont parmi ces éléments ceux qui forment une base de C_N , donnant ainsi le théorème 2.

BIBLIOGRAPHIE

- [1] FRICKE (R.). - Ueber die Substitutionsgruppen welche zu den aus dem Legendre'schen Integralmodul $k^2(w)$ gezogenen Wurzeln gehören, Math. Annalen, t. 28, 1887, p. 99-118.
 - [2] ROHRLICH (D. E.). - Points at infinity on the Fermat curves, Invent. Math., Berlin, t. 39, 1977, p. 95-127.
-