Séminaire Delange-Pisot-Poitou. Théorie des nombres

ANDREW P. OGG

Automorphismes de courbes modulaires

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 1 (1974-1975), exp. n° 7, p. 1-8

<http://www.numdam.org/item?id=SDPP_1974-1975__16_1_A4_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
16e année, 1974/75, n° 7, 8 p.

9 décembre 1974

AUTOMORPHISMES DE COURBES MODULAIRES

par Andrew P. OGG

Soient N un entier positif, et $\Gamma_0(N)$ le sous-groupe du groupe modulaire $\Gamma = SL(2, \underline{Z})/\pm 1$ défini par les matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec N divisant c. Alors $\Gamma_0(N)$ agit sur le demi-plan supérieur $\mathfrak{H} = \{\tau = x + iy ; y > 0\}$ par $\tau \longmapsto \frac{a\tau+b}{c\tau+d}$.

Soient $Y_0(N) = \Gamma_0(N) \backslash \mathfrak{H}$, et $X_0(N)$ la compactification de $Y_0(N)$ par adjonction des pointes (points paraboliques). Alors $X_0(N)$ est une courbe (projective, non singulière) définie sur $\underline{Q}$; son genre $g = g(N)$ est donné par une formule connue. Par exemple, si N est premier, alors $X_0(N)$ a exactement deux pointes, 0 et ∞, et elles sont rationnelles sur $\underline{Q}$; le genre est 0 si $N = 2$ ou 3, et

$$(1) \qquad g = \frac{N - a}{12} \quad \text{si} \quad \begin{cases} N \equiv a \pmod{12} \\ a = -1, 5, 7, 13. \end{cases}$$

Si u est une involution (automorphisme d'ordre 2) de $X_0(N)$, le genre du quotient $X_0(N)/(u)$ est

$$(2) \qquad g^{(u)} = \frac{g + 1}{2} - \frac{n(u)}{4},$$

d'après la formule de Riemann-Hurwitz, où $n(u)$ est le nombre des points fixes de u. En particulier, $X_0(N)$ a l'involution $w = w_N$ définie par la matrice $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, pour laquelle $n(w)$ est donné par une formule de Fricke :

$$(3) \qquad n(w) = \begin{cases} h(-N) + h(-4N) & (\text{si } N \equiv 3 \pmod 4) \\ h(-4N) & (\text{sinon}), \end{cases}$$

où $h(-m)$ est le nombre des classes des formes quadratiques binaires positives primitives de discriminant $-m$. On pose $X_0^+(N) = X_0(N)/(w)$ et

$$g^+ = g^{(w)} = \text{genre de } X_0^+(N).$$

L'involution w est définie sur $\underline{Q}$, et $X_0^+(N)$ est définie sur $\underline{Q}$.

Si $g \geqslant 2$, alors le groupe $A = \mathrm{Aut}(X_0(N))$ des automorphismes de $X_0(N)$ est fini. Il contient le sous-groupe B des automorphismes "modulaires", i. e. $B = \mathfrak{N}/\Gamma_0(N)$, où $\mathfrak{N}$ est le normalisateur de $\Gamma_0(N)$ dans $\mathrm{Aut}(\mathfrak{H}) = SL(2, \underline{R})/\pm 1$. LEHNER et NEWMAN [2] ont déterminé le groupe B. "En général", i. e. si $4 \nmid N$ et $9 \nmid N$, le groupe B est le groupe W des involutions partielles d'Atkin-Lehner, isomorphe au produit de n groupes d'ordre 2, où n est le nombre des nombres premiers distincts qui divisent N. Les éléments de W sont définis sur $\underline{Q}$. En particulier, $B = \{1, w\}$ si N est premier. Un élément de $A - B$ sera appelé "exceptionnel" ; le seul exemple connu où $A - B$ n'est pas vide est le cas $N=37$.

Avant de discuter cet exemple, rappelons qu'une courbe X, de genre ≥ 2, est hyperelliptique si elle possède une fonction $f : X \longrightarrow \mathbb{P}^1$ de degré 2, i. e. si elle possède une involution hyperelliptique v telle que $X/(v)$ est de genre 0. Dans ce cas, v est unique (par exemple parce qu'elle induit -1 sur la jacobienne de X, ou sur l'espace des différentielles holomorphes sur X) ; donc v est dans le centre de $\mathrm{Aut}(X)$, et définie sur tout corps de définition de X. Dans la suite, la lettre v est toujours réservée aux involutions hyperelliptiques, et la lettre w à $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Enfin, toute courbe de genre 2 est hyperelliptique.

Pour $N = 37$, on a $g = 2$ et $g^+ = 1$, et donc $X_0(37)$ est hyperelliptique avec $v \neq w$ (i. e. v est exceptionnelle). L'involution v applique les deux pointes de $X_0(37)$ sur deux points rationnels de $Y_0(37)$, en fait les seuls éléments rationnels de $Y_0(37)$ (cf. [5]). Le problème des automorphismes exceptionnels se trouve ainsi lié au problème des points rationnels de $Y_0(N)$ (cf. [7]).

THÉORÈME 1 [6]. - $X_0(N)$ est hyperelliptique pour exactement dix-neuf valeurs de N. Le seul cas où v est exceptionnelle est $N = 37$. Les autres dix-huit valeurs sont $N = 22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71$.

Le vrai problème (évidemment plus difficile que celui résolu par le théorème 1) est de déterminer le groupe $A = \mathrm{Aut}(X_0(N))$ pour tout N (avec $g \geq 2$) ; pour l'instant, on ne connaît la réponse que dans le cas où N est premier.

THÉORÈME 2. - Si N est premier, $N \geq 23$ (i. e. $g \geq 2$), et $N \neq 37$, alors $A = \{1, w\}$. Pour $N = 37$, $A = \{1, w, v, vw\}$ est le groupe de Klein.

Le paragraphe 1 de cet article esquisse la démonstration du théorème 1 (sans détails, [6] étant maintenant disponible). Le paragraphe 2 donne la démonstration du théorème 2, complète si on admet des résultats inédits de K. RIBET et B. MAZUR ; des conversations avec A. BRUMER et J. VÉLU, en automne 1974, m'ont beaucoup aidé. Enfin, le paragraphe 3 discute le lien avec les courbes elliptiques supersingulières.

1. Le problème hyperelliptique (cf. [6]).

On aura besoin de l'interprétation modulaire (i. e. en termes de courbes elliptiques variables) de $X_0(N)$, qui est la suivante : On associe à $\tau \in \mathfrak{H}$ la paire (E, C), où $E = \mathbb{C}/L$ est la courbe elliptique correspondant au réseau $L = \mathbb{Z}\tau \oplus \mathbb{Z}$, et C est le sous-groupe cyclique de E, d'ordre N, engendré par l'image de $1/N$. Les paires (E, C) et (E', C'), associées à $\tau, \tau' \in \mathfrak{H}$, sont isomorphes (i. e. il existe un isomorphisme $f : E \xrightarrow{\sim} E'$ avec $f(C) = C'$) si, et seulement si, τ et τ' sont $\Gamma_0(N)$-équivalents. Il y a donc une bijection entre $Y_0(N)$ et les classes d'isomorphisme des paires (E, C), où E est une courbe elliptique, et C un sous-groupe cyclique d'ordre N. L'involution w associe à

la (classe de la) paire (E , C) la paire (E' , C') , où $E' = E/C$ et $C' = E_N/C$, $E_N = \{P \in E : N.P = 0\}$.

Si on préfère parler d'isogénies au lieu de sous-groupes cycliques, on a une isogénie $\lambda : E \longrightarrow E'$ de courbes elliptiques, dont le noyau C est cyclique d'ordre N , et $w(\lambda) = \hat{\lambda}$ est l'isogénie $E' \longrightarrow E$ avec $\hat{\lambda} \circ \lambda = N : E \longrightarrow E$ et $\lambda \circ \hat{\lambda} = N : E' \longrightarrow E'$.

Si ℓ est un nombre premier qui ne divise pas N , alors la courbe $X_0(N)$ a une bonne réduction modulo ℓ , encore notée $X_0(N)$, d'après un théorème d'Igusa. La courbe réduite $X_0(N)$ est donc une courbe non singulière sur $\underset{\sim}{F}_\ell$, du même genre g ; elle a le "même" ensemble de "pointes" $X_0(N) - Y_0(N)$ qu'en caractéristique 0 , et les éléments de $Y_0(N)$ correspondent aux classes de paires (E , C) , de courbes elliptiques E et sous-groupes cycliques C , en caractéristique ℓ .

Supposons maintenant $X_0(N)$ hyperelliptique, avec N impair ; alors la courbe réduite modulo 2 est encore hyperelliptique en caractéristique 2 . La courbe étant un revêtement double de $\underset{\sim}{P}^1$, le nombre de points rationnels dans un corps fini $\underset{\sim}{F}_{2^n}$ est $\leqslant 2(1 + 2^n)$; en particulier

$$|X_0(N)(\underset{\sim}{F}_4)| \leqslant 10 . \tag{4}$$

Considérons la courbe elliptique $E : y^2 + y = X^3$. Elle est la seule courbe elliptique supersingulière (i. e. $E_2 = 0$) en caractéristique 2 , et le groupe de ses automorphismes est d'ordre 24 . Sur $\underset{\sim}{F}_4$, le Frobenius $\varphi(x,y) = (x^4,y^4)$ est $\varphi = -2$, un entier, donc tous les sous-groupes finis C de E sont $\underset{\sim}{F}_4$-rationnels (i. e. stables sous l'action de $\mathrm{Gal}(\overline{\underset{\sim}{F}}_4/\underset{\sim}{F}_4)$, i. e. stables par φ). Le nombre des sous-groupes cycliques C de E , d'ordre N , est

$$\psi(N) = (\Gamma : \Gamma_0(N)) = N \prod_{p|N}(1 + 1/p) . \tag{5}$$

On a donc au moins $\psi(N)/12$ points de $X_0(N)(\underset{\sim}{F}_4)$ correspondants, parce qu'une paire (E , C) rationnelle sur un corps K représente un élément de $Y_0(N)(K)$ (cf. [1], [7]), et parce que $|\mathrm{Aut}(E)| = 24$, et l'automorphisme -1 de E fixe toute paire (E , C) . On a aussi les deux "pointes" 0 et ∞ , rationnelles sur $\underset{\sim}{F}_2$; en utilisant (4), on trouve $2 + \psi(N)/12 \leqslant 10$, i. e. $\psi(N) \leqslant 96$. Il y a des bornes analogues si $X_0(N)$ est hyperelliptique, et $p \nmid N$, pour $p = 3,5,7,\ldots$, donc avec l'aide de diverses astuces [6], on a le théorème 1.

Ce qui est agréable avec cette méthode, c'est qu'elle donne des majorations des valeurs de N pour lesquelles $X_0(N)$ est hyperelliptique, sans se soucier de savoir si v est exceptionnelle ou non.

2. Le groupe des automorphismes (N premier).

Soit $J = J_0(N)$ la jacobienne de $X = X_0(N)$; J est une variété abélienne sur $\underset{\sim}{Q}$ de dimension g . Soient $\mathrm{End}(J)$ l'anneau des endomorphismes de J , et $\mathrm{End}_{\underset{\sim}{Q}}(J)$ le sous-anneau des endomorphismes définis sur $\underset{\sim}{Q}$. Alors $\mathrm{End}_{\underset{\sim}{Q}}(J)$ contient l'algè-

bre de Hecke $\mathcal{H}$, engendrée par les opérateurs de Hecke.

L'algèbre $\mathcal{H} \otimes \underset{\sim}{Q}$ est commutative, et de dimension g sur $\underset{\sim}{Q}$; on a

$$\mathcal{H} \otimes \underset{\sim}{Q} \simeq K_1 \times \ldots \times K_n , \tag{6}$$

où K_i est un corps totalement réel. La décomposition (6) de $\mathcal{H} \otimes \underset{\sim}{Q}$ correspond à une décomposition de J, à isogénie près :

$$J \sim J^{(1)} \times \ldots \times J^{(n)} , \tag{7}$$

où $J^{(i)}$ est une variété abélienne, définie sur $\underset{\sim}{Q}$, et $\underset{\sim}{Q}$-simple, avec

$$\dim J^{(i)} = [K_i : \underset{\sim}{Q}] \quad \text{et} \quad \mathrm{End}_{\underset{\sim}{Q}}(J^{(i)}) \otimes \underset{\sim}{Q} = K_i .$$

K. RIBET a démontré que tout endomorphisme de J est défini sur $\underset{\sim}{Q}$, et est donc dans $\mathcal{H} \otimes \underset{\sim}{Q}$, par la "congruence d'Eichler-Shimura" :

$$\mathrm{End}(J) \otimes \underset{\sim}{Q} = \mathcal{H} \otimes \underset{\sim}{Q} . \tag{8}$$

[Plus généralement, RIBET montre qu'un endomorphisme d'une variété abélienne, "semi-stable" sur K, est défini sur une extension non ramifiée K' de K ; pour $K = \underset{\sim}{Q}$, on a nécessairement $K' = \underset{\sim}{Q}$. La démonstration, très simple, n'occupe qu'une page [8]. Ici "semi-stable" veut dire que la réduction, modulo une place quelconque, ne contient pas de groupes additifs ; dans notre cas, J a bonne réduction modulo ℓ pour $\ell \nmid N$ (IGUSA) et réduction multiplicative modulo N (DELIGNE).] En particulier, les facteurs $J^{(i)}$ de J sont absolument simples, et absolument non-isogènes.

Supposons maintenant $N \geq 23$, i. e. $g \geq 2$ (N étant toujours premier). Le groupe $A = \mathrm{Aut}(X)$ est fini, et continu dans $\mathrm{Aut}(J)$; les corps K_i étant réels, il s'ensuit de (6) et (8) que

$$A \subset (\pm 1) \times (\pm 1) \times \ldots \times (\pm 1) \quad (\text{n fois}). \tag{9}$$

En particulier, A est commutatif, et tout $u \in A$ est défini sur $\underset{\sim}{Q}$ et d'ordre ≤ 2.

Pour $N = 37$, $g = 2$, et J est isogène au produit de deux courbes elliptiques, d'où $A \subset (\pm 1) \times (\pm 1)$. Nous connaissons déjà quatre éléments de A, d'où la partie du théorème 2 qui concerne 37. Supposons $N \neq 37$ dorénavant.

LEMME. - Si $u \in A$ fixe la pointe ∞, alors $u = 1$.

Démonstration. - Les valeurs propres de u sur l'espace Ω des différentielles holomorphes sur X sont toutes ± 1. Si elles sont toutes -1, alors u est une involution hyperelliptique, donc $u = w$ d'après le théorème 1 ($N \neq 37$) en contradiction avec l'hypothèse $u(\infty) = \infty$ (parce que $\omega(\infty) = 0$). Supposons que u a les valeurs propres $+1$ et -1. Alors on peut choisir deux différentielles ω_1, $\omega_2 \in \Omega$ avec

$$\omega_1 \circ u = \omega_1 , \quad \omega_2 \circ u = -\omega_2 , \tag{10}$$

qui soient fonctions propres de $\mathcal{H}$. Le développement à la pointe ∞ de ω_i est donc de la forme

$$\omega_i = (\sum_{m=1}^{\infty} a_m q^m).\frac{dq}{q} \qquad (q = \exp(2\pi i\tau))$$

où $\sum_{m=i}^{\infty} a_m m^{-s}$ a un produit eulérien et en particulier $a_1 \neq 0$, disons $a_1 = 1$. Alors $\omega = \omega_1 + \omega_2$ ne s'annule pas en ∞ , mais $\omega \circ u = \omega_1 - \omega_2$ s'annule en ∞ , en contradiction avec $u(\infty) = \infty$. Les valeurs propres de u sont donc toutes $+ 1$, i. e. $u = 1$.

Q. E. D.

Le sous-groupe Z_n de $J(\underset{\sim}{Q})$, engendré par la classe du diviseur $(0) - (\infty)$, de degré 0 , est cyclique d'ordre

(11) $$n = \text{ numérateur de } \frac{N-1}{12} .$$

Tout récemment MAZUR ([3], [4]) a démontré qu'en fait Z_n est le groupe de tous les points rationnels sur J , d'ordre fini :

(12) $$Z_n = J(\underset{\sim}{Q})^{tors} \qquad (\text{"conjecture d'Ogg"}).$$

Démontrons maintenant le théorème 2. Si $u \in A$, alors u agit sur le groupe Z_n (cf. (12)) ; on a donc

(13) $$(u0) - (u\infty) \sim m((0) - (\infty)) ,$$

où $m \in \underset{\sim}{Z}/n\underset{\sim}{Z}$.

Si $m = 1$, alors $(u0) + (\infty) \sim (0) + (u\infty)$. Si $u\infty = \infty$ alors $u = 1$, d'après le lemme. Si $u\infty \neq \infty$, alors X est hyperelliptique (parce que $u\infty \neq u0$ aussi) avec $v = w$ (théorème 1, $N \neq 37$ encore), donc $u\infty = w0 = \infty$. Donc $u = 1$ si $m = 1$; de même, $u = w$ si $m = -1$.

Un théorème de MAZUR [3] dit qu'il n'y a que cinq possibilités pour m , c'est-à-dire $m = \pm 1$, 0 , $\pm 1/3$; dans notre cas, il est clair que $m \neq 0$. De plus, $m = \pm 1/3$ n'est possible que si $N \equiv -1 \pmod 3$ et $N = 53$, 113 , 137 , donc $n \geq 13$. Mais $u^2 = 1$ implique $m^2 = 1$ dans $\underset{\sim}{Z}/n\underset{\sim}{Z}$, i. e. $1 \equiv 9 \pmod n$, évidemment impossible pour $n \geq 13$. Donc $m = \pm 1$, $u = 1$, w , et on a le théorème 2.

3. Réduction modulo p de $X_0(p)$.

Si E est une courbe elliptique en caractéristique $p > 0$, l'application $p : E \longrightarrow E$ est inséparable de degré p^2 . Il y a donc deux cas :

1° p est totalement inséparable, i. e. $E_p = 0$. Dans ce cas, on dit que E est supersingulière ; son invariant $j = j(E)$ est nécessairement dans $\underset{\sim}{F}_{p^2}$.

2° Le degré de séparabilité de p est p , i. e. E_p est d'ordre p .

En tous cas, E admet l'isogénie de Frobenius $\varphi : E \longrightarrow E^{(p)}$, qui est inséparable de degré p (Si E est définie par une équation $F(x , y) = \sum a_{ij} x^i y^j = 0$,

alors $E^{(p)}$ est définie par $\sum a_{ij}^p x^i y^j = 0$, et $\varphi(x , y) = (x^p , y^p)$).

A un isomorphisme près, φ est l'unique isogénie sur E qui est inséparable de degré p . On note par $\hat{\varphi} = w(\varphi)$ sa transposée $\hat{\varphi} : E^{(p)} \longrightarrow E$ (Donc $\hat{\varphi} \circ \varphi$ est l'endomorphisme p de E). Si E n'est pas supersingulière, alors $\hat{\varphi}$ est l'unique (à un isomorphisme près) isogénie sur $E^{(p)}$ qui est séparable de degré p (Son noyau est $E_p^{(p)}$).

La réduction modulo p de $X_0(p)$ est la réunion de deux droites projectives Z et Z' , se coupant transversalement. Les points de Z sont représentés par des Frobenius $\varphi : E \longrightarrow E^{(p)}$ et les points de Z' par les transposées

$$\hat{\varphi} : E^{(p)} \longrightarrow E .$$

Les intersections de Z et Z' sont les points supersinguliers, où $\hat{\varphi}$ est inséparable. L'involution w échange Z et Z' , et opère sur $Z \cap Z'$ comme le Frobenius. [Voir DELIGNE-RAPOPORT [1] pour les détails. En caractéristique 0 , il est classique que $0 = F(j \circ w , j)$, où $j \circ w(\tau) = j(-1/p\tau) = j(p\tau)$, et $F(X , Y) \in \underset{\sim}{Z}[X , Y]$ est irréductible, et $X_0(p)$ est la normalisée de $F = 0$. On a $F(X , Y) \equiv (X - Y^p)(X^p - Y) \pmod p$, la "congruence de Kronecker-Weber", d'où le fait que les intersections sont transversales ; c'est la démonstration de DELIGNE du fait que le polynôme de Hasse (qui a comme racines les valeurs supersingulières de j) a des racines distinctes.] Notons que $Z + Z'$ n'est pas en général le modèle de Néron, mais suffit pour nos besoins.

Rappelons que le genre arithmétique $p_a(C)$ d'une courbe réductible C satisfait aux règles suivantes :

1° $p_a(C + D) = -1 + p_a(C) + p_a(D) + C.D$, où $C.D$ est le nombre des intersections de C et D (multiplicités comptées).

2° $p_a(C)$ est invariant par spécialisation et par éclatement.

3° Si C est irréductible, et si g est le genre de sa normalisée, alors $p_a(C) \geq g$, avec $p_a(C) = g$ si, et seulement si, C est non-singulière. En particulier, $p_a(C) = 0$ si, et seulement si, $C = \underset{\sim}{P}^1$.

Dans notre cas, $Z + Z'$ est une spécialisation (réduction modulo p) de $X_0(p)$, de genre g en caractéristique 0 . Le 1° donne :

$$1 + g = 1 + p_a(Z + Z') = p_a(Z) + p_a(Z') + Z.Z' ,$$

i. e.

(14) $\quad 1 + g = Z.Z' =$ nombre des valeurs supersingulières de j .

Ecrivons $1 + g = r + 2s$, où r valeurs supersingulières $a_1 , \ldots , a_r$ de j sont dans $\underset{\sim}{F}_p$, et $2s$ valeurs supersingulières $b_1 , b_1^p , \ldots , b_s , b_s^p$ de j dans $\underset{\sim}{F}_{p^2} - \underset{\sim}{F}_p$. L'automorphisme w de $Z + Z'$ échange Z et Z' , fixe $a_1 , \ldots , a_r$, et échange b_i et b_i^p ; le quotient $(Z + Z')/(w)$ est donc une droite C avec s points doubles ordinaires, et donc avec genre arithmétique s ,

comme on le vérifie en éclatant ces points doubles, grâce aux 1° et 2°. Encore par le principe de spécialisation, ce genre arithmétique est g^+ , le genre de $X_0^+(p)$ en caractéristique 0 . D'où :

(15) $2g^+$ = nombre des valeurs supersingulières de j dans $\underset{\sim}{F}_{p^2} - \underset{\sim}{F}_p$.

J'ignore les origines exactes de (15) ; la formule était mentionnée dans le cours de SERRE de 1972/73 au Collège de France, dans le cadre de la théorie des formes modulaires modulo p . En tous cas, on a comme corollaire de (15) et du théorème 1, le résultat suivant.

COROLLAIRE. - Toutes les valeurs supersingulières de j sont dans $\underset{\sim}{F}_p$ si, et seulement si, $g^+ = 0$, i. e. $g \leqslant 1$ où $X_0(p)$ est hyperelliptique avec $v = w$, i. e. $p \leqslant 31$ ou $p = 41 , 47 , 59 , 71$.

Autrement dit, toutes les racines du polynôme de Hasse sont dans $\underset{\sim}{F}_p$, si, et seulement si, p est une de ces quinze valeurs. Notons que d'après les formules (2) et (14), la formule (15) peut être exprimée aussi sous la forme

(16) $n(w)/2$ = nombre des valeurs supersingulières de j dans $\underset{\sim}{F}_p$,

où $n(w)$ est donné par (3).

Remarque 1. - Dans sa leçon d'ouverture au Collège de France, le 14 janvier 1975, J. TITS mentionna le groupe de Fischer, "le monstre", qui, s'il existe, est un groupe simple "sporadique" d'ordre

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71 ,$$

i. e. divisible exactement par les quinze nombres premiers de la liste du corollaire. Une bouteille de Jack Daniels est offerte à celui qui expliquera cette coïncidence.

Remarque 2. - Une des diverses astuces utilisées dans la démonstration du théorème 1 est un résultat de Schoeneberg [9], qui montre que, dans le mauvais cas, où $X_0(N)$ est hyperelliptique avec $v \neq w$, on a $n(w) \leqslant 4$ (cf. (3)). Il est amusant que, dans le cas $N = p$, on puisse donner une démonstration très éloignée de la démonstration originale de Schoeneberg (exercice sur les points de Weierstrass). En effet, dans ce cas, on a $(Z + Z')/(v) = \underset{\sim}{P}^1$, i. e. v échange Z et Z' , et fixe tous les points d'intersection $a_1 , \ldots , a_r , b_1 , b_1^p , \ldots , b_s , b_s^p$. Alors l'involution $u = v.w$ fixe Z et Z' et $a_1 , \ldots , a_r$. Un automorphisme non trivial de $\underset{\sim}{P}^1$ ayant $\leqslant 2$ points fixes, on a $r \leqslant 2$, i. e. $n(w) \leqslant 4$, d'après (16).

BIBLIOGRAPHIE

[1] DELIGNE (P.) et RAPOPORT (M.). - Les schémas de modules de courbes elliptiques, "Modular functions of one variable, II", p. 143-316. - Berlin, Heidelberg, New York, Springer-Verlag, 1973 (Lecture Notes in Mathematics, 349).

[2] LEHNER (J.) and NEWMAN (M.). - Weierstrass points of $\Gamma_0(N)$, Annals of Math., t. 79, 1964, p. 360-368.

[3] MAZUR (B). - Modular curves and the Eisenstein ideal (en préparation).

[4] MAZUR (B.). - Lettre à Andrew Ogg (datée du 25 novembre 1974).

[5] MAZUR (B.) and SWINNERTON-DYER (P.). - Arithmetic of Weil curves, Invent. Math., Berlin, t. 25, 1974, p. 1-61.

[6] OGG (A.). - Hyperelliptic modular curves, Bull. Soc. math. France, t. 102, 1974, p. 449-462.

[7] OGG (A.). - Diophantine equations and modular forms, Bull. Amer. math. Soc., t. 81, 1975, p. 14-27.

[8] RIBET (K.). - Lettre à Andrew Ogg (datée du 29 novembre 1974, reçue le 27 décembre 1974).

[9] SCHOENEBERG (B.). - Über die Weierstrasspunkte in den Körpern der elliptischen Modulfunktionen, Abh. Math. Semin. Hamburg, t. 17, 1951, p. 104-111.

(Texte reçu le 30 janvier 1975)

Andrew P. OGG
Department of Mathematics
University of California
BERKELEY, Calif. 94720
(Etats-Unis)