SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

p-torsion des courbes elliptiques

Séminaire N. Bourbaki, 1971, exp. n° 380, p. 281-294

<http://www.numdam.org/item?id=SB_1969-1970__12__281_0>

Séminaire BOURBAKI
22e année, 1969/70, n° 380 Mai-Juin 1970

p-TORSION DES COURBES ELLIPTIQUES

(d'après Y. MANIN)

par Jean-Pierre SERRE

§ 1. Enoncé des principaux résultats.

1.1. Notations.

La lettre K désigne un corps de nombres algébriques, i.e. une extension finie de $\mathbb{Q}$; on note $\bar{K}$ une clôture algébrique de K .

Une courbe elliptique sur K est, par définition, une variété abélienne sur K , de dimension 1 (autrement dit une courbe projective non singulière de genre 1 , munie d'un point rationnel P_o que l'on prend comme origine pour la loi de groupe). Si l'on écrit une telle courbe E sous la forme de Weierstrass

$$y^2 = 4x^3 - g_2x - g_3 , \qquad g_i \in K ,$$

on prend pour P_o le point à l'infini. L'invariant modulaire $j(E)$ de E est défini par

$$j(E) = 1728\, g_2^3/\Delta , \qquad \text{où } \Delta = g_2^3 - 27\, g_3^2 \neq 0 .$$

Une courbe elliptique E' sur K est dite une K-forme de E si $j(E) = j(E')$, i.e. si E et E' deviennent isomorphes par extension du corps de base de K à $\bar{K}$. Si $j(E) \neq 0$, 1728 , les classes d'isomorphisme de K-formes de E correspondent bijectivement aux éléments de K^*/K^{*2} ; si $j(E) = 0$ (resp. 1728), on a un résultat analogue, l'exposant 2 étant remplacé par 6 (resp. par 4). Cela résulte simplement de ce que le groupe des $\bar{K}$-automorphismes de E est isomorphe au groupe μ_n des racines n-ièmes de l'unité, avec $n = 2, 6$ ou 4 suivant les cas.

1.2. Le groupe de torsion d'une courbe elliptique.

Soit E une courbe elliptique sur K, et soit $E(K)$ le groupe des points de E rationnels sur K. D'après le théorème de Mordell-Weil (cf. par exemple [7], chap. V) le groupe $E(K)$ est de type fini. Son groupe de torsion $E_t(K)$ est donc fini (cette finitude peut aussi se démontrer par un argument "local", cf. n° 1.4).

On sait peu de choses sur la structure du groupe $E_t(K)$ à part le fait trivial qu'il est somme directe de deux groupes cycliques. Ainsi, pour $K = \mathbb{Q}$, on a des exemples de courbes E pour lesquelles l'ordre de $E_t(K)$ est $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$ ou 16 et l'on ignore si $E_t(K)$ peut contenir un élément d'ordre premier ≥ 13 (il ne peut pas contenir d'élément d'ordre 11, cf. [1]) ; on a quelques autres résultats partiels, que l'on trouvera résumés dans le rapport de Cassels ([2], p. 264). Ces résultats ont conduit à conjecturer que l'ordre de $E_t(K)$ est borné par un entier dépendant seulement de K (mais pas de E). Dans [10], Manin démontre une forme affaiblie de cette conjecture :

THÉORÈME 1.- Soit p un nombre premier. L'ordre de la p-composante de $E_t(K)$ est borné (par un entier ne dépendant que de K et de p).

Il revient au même de dire qu'il existe un entier $N = N(p,K)$ tel qu'aucune courbe elliptique sur K ne contienne de point rationnel d'ordre p^N.

1.3. Sous-groupes cycliques rationnels sur K.

Soit E une courbe elliptique sur K, et soit C un sous-groupe fini de $E(\bar{K})$. On dit que C est rationnel sur K s'il est stable par l'action du groupe de Galois $\mathrm{Gal}(\bar{K}/K)$; cela équivaut à dire que C est l'ensemble des $\bar{K}$-points d'un sous-schéma en groupes de E. Si tel est le cas, on définit de façon évidente la courbe

elliptique quotient E/C ; la projection $E \to E/C$ est une K-isogénie de noyau C.

Il est clair que, si la courbe E contient un point rationnel d'ordre p^n, elle contient aussi un sous-groupe cyclique d'ordre p^n rationnel sur K. La réciproque est inexacte en général ; ainsi, si $K = \mathbb{Q}$, on sait (voir ci-dessus) qu'aucune courbe elliptique n'a de point rationnel d'ordre 11, alors qu'il existe trois valeurs de j telles que les courbes correspondantes aient un sous-groupe cyclique d'ordre 11 rationnel sur $\mathbb{Q}$ (l'une de ces valeurs est $j = -2^{15}$ qui correspond aux courbes à multiplication complexe par les entiers de $\mathbb{Q}(\sqrt{-11})$; j'ignore quelles sont les deux autres).

Manin démontre (cf. [10]) :

THÉORÈME 2.- *Soit p un nombre premier. Il existe un entier positif $M = M(p,K)$ et une partie finie J_M de K jouissant de la propriété suivante :*

Si une courbe elliptique E sur K possède un sous-groupe cyclique d'ordre p^M rationnel sur K, son invariant modulaire $j(E)$ appartient à J_M.

La démonstration de ce théorème sera donnée au § 3. Elle repose sur un théorème de finitude des points rationnels de certaines courbes algébriques, voir § 2.

1.4. *Démonstration du théorème 1 à partir du théorème 2.*

Dans les lemmes 1, 2 et 3 ci-après, K_v désigne un corps local de caractéristique zéro, à corps résiduel fini (autrement dit une extension finie d'un corps ℓ-adique $\mathbb{Q}_\ell$).

LEMME 1.- *Soit G un groupe K_v-analytique compact. Les sous-groupes finis de G sont d'ordre borné.*

La théorie de Lie montre que G possède un sous-groupe ouvert U sans torsion.

Comme G est compact, l'indice $(G : U)$ de U dans G est fini. Si C est un sous-groupe fini de G, l'ordre de C divise $(G : U)$, donc est borné.

(Noter que G n'est pas supposé commutatif.)

LEMME 2.- *Soit E une courbe elliptique sur K_v et soit $E(K_v)$ le groupe des points de E rationnels sur K_v. Le sous-groupe de torsion de $E(K_v)$ est fini.*

On applique le lemme 1 au groupe $G = E(K_v)$, qui est un groupe K_v-analytique compact de dimension 1.

LEMME 3.- *Soit $a \in K_v$. Les courbes elliptiques E sur K_v telles que $j(E) = a$ sont en nombre fini, à isomorphisme près. Leurs sous-groupes de torsion sont d'ordre borné.*

La première assertion résulte du fait que K_v^*/K_v^{*n} est fini pour tout $n \geq 1$, donc en particulier pour $n = 2, 4, 6$. La seconde assertion résulte de la première et du lemme 2.

LEMME 4.- *Soit J une partie finie de K. Les ordres des groupes $E_t(K)$ relatifs aux courbes elliptiques E sur K telles que $j(E) \in J$ sont bornés.*

Il suffit de considérer le cas où J est réduit à un élément a. Dans ce cas, le lemme résulte du lemme 3 appliqué à un complété K_v de K (observer que $E_t(K)$ est un sous-groupe du groupe de torsion de $E(K_v)$).

Soient maintenant M et J_M vérifiant les propriétés énoncées dans le théorème 2. En appliquant le lemme 4 à $J = J_M$ on voit que, si E possède un sous-groupe cyclique d'ordre p^M rationnel sur K, l'ordre de $E_t(K)$ est borné. Le théorème 1 résulte immédiatement de là.

§ 2. Finitude du nombre des points rationnels de certaines courbes algébriques.

2.1. Enoncé du résultat.

Soit X une variété projective non singulière sur K, munie d'un point rationnel x_o. On note $X(K)$ l'ensemble des points de X rationnels sur K.

Soit A une variété abélienne sur K. On note $A(K)$ le groupe des points rationnels de A, et $A(X)$ le groupe des morphismes f de X dans A tels que $f(x_o) = 0$. Ces groupes sont de type fini (cf. [7], chap. V).

Posons

$$V_X = A(X) \otimes_{\mathbf{Z}} \mathbf{R} \quad \text{et} \quad V_K = A(K) \otimes_{\mathbf{Z}} \mathbf{R} .$$

Ce sont des $\mathbf{R}$-espaces vectoriels de dimension finie.

Si $x \in X(K)$, l'application $f \longmapsto f(x)$ se prolonge en une application $\mathbf{R}$-linéaire

$$\varphi_x : V_X \to V_K .$$

THÉORÈME 3 (Demjanenko-Manin).- *Supposons que le groupe de Néron-Severi de X soit de rang 1. Il existe alors un sous-ensemble fini H de $X(K)$ tel que φ_x soit injectif pour tout $x \in X(K) - H$.*

Noter que l'hypothèse faite sur X est satisfaite lorsque le second nombre de Betti de X est égal à 1, et en particulier si X est de dimension 1.

COROLLAIRE.- *Si $rg.A(K) < rg.A(X)$, l'ensemble $X(K)$ est fini.*

En effet on a alors $\dim.V_K < \dim.V_X$ et φ_x ne peut pas être injectif ; d'où $X(K) = H$.

Remarque.- Le cas traité par Demjanenko [4] est celui où X et A sont de dimension 1 . Le cas général est dû à Manin [10]. Pour la suite, il est essentiel de pouvoir prendre A de dimension quelconque.

2.2. Démonstration du théorème 3.

On va commencer par munir les espaces V_X et V_K de structures euclidiennes. Cela se fait au moyen de la théorie des hauteurs de Néron-Tate.

De façon plus précise, choisissons un plongement projectif de X , et soit h la fonction hauteur correspondante (il s'agit ici de hauteurs additives, i.e. de logarithmes de hauteurs au sens usuel, cf. [7], chap. III et IV). La fonction h applique $X(K)$ dans $\mathbf{R}_+$; pour tout $a \in \mathbf{R}_+$ l'ensemble des $x \in X(K)$ tels que $h(x) \leq a$ est fini (autrement dit, h tend vers $+\infty$).

Choisissons d'autre part un faisceau inversible L sur A ; nous supposerons que L est ample (i.e. il existe un entier $n \geq 1$ tel que $L^{\otimes n}$ définisse un plongement projectif de A) et symétrique (isomorphe à son image réciproque par l'automorphisme $a \mapsto -a$ de A). Soit h_A la fonction hauteur normalisée correspondante (au sens de Néron et Tate, cf. [8], [9], [11]) ; c'est une forme quadratique positive sur $A(K)$, à valeurs réelles. Elle se prolonge en une forme quadratique positive non dégénérée sur $V_K = A(K) \otimes \mathbf{R}$, et fait de cet espace un espace euclidien.

Si $f \in A(X)$, l'image réciproque f^*L de L par f est un faisceau inversible sur X . Nous noterons $h_X(f)$ son degré (par rapport au plongement projectif de X choisi plus haut) ; si la classe de ce faisceau est représentée par un diviseur Δ_f , et si l'on note Y une section hyperplane de X , on a

$$h_X(f) = \deg(Y^{d-1}.\Delta_f) \quad , \qquad \text{avec } d = \dim(X) \ .$$

La fonction $h_X : A(X) \to \mathbf{Z}$ ainsi obtenue est une forme quadratique positive non dégénérée ; cela se vérifie, soit par voie algébrique (au moyen du "théorème du carré"), soit, ce qui est encore plus facile, par voie topologique. Ici encore, on prolonge h_X à $V_X = A(X) \otimes \mathbf{R}$ et l'on obtient ainsi sur cet espace une structure d'espace euclidien.

Montrons maintenant que les $\varphi_x : V_X \to V_K$, $x \in X(K)$, sont "presque" des similitudes :

LEMME 5.- *Soient* f *et* g *deux éléments non nuls de* $A(X)$. *Lorsque* $x \in X(K)$ *tend vers l'infini, les nombres réels* $h_A(\varphi_x(f))$ *et* $h_A(\varphi_x(g))$ *tendent vers* $+\infty$, *et l'on a*

$$\lim_{x\to\infty} \cdot \frac{h_A(\varphi_x(f))}{h_A(\varphi_x(g))} = \frac{h_X(f)}{h_X(g)} \cdot$$

(L'expression " x tend vers l'infini " signifie que $h(x)$ tend vers $+\infty$.)

Soit $N(X)$ le groupe de Néron-Severi de X . Par hypothèse, $N(X) \otimes \mathbf{Q}$ est de dimension 1 sur $\mathbf{Q}$; il admet donc pour base la classe $[Y]$ de la section hyperplane Y de X . L'image de f^*L (resp. g^*L) dans $N(X) \otimes \mathbf{Q}$ est égale à $a[Y]$ (resp. à $b[Y]$), avec $a, b \in \mathbf{Q}$. Utilisant le fait que f et g sont $\neq 0$, on voit facilement que a et b sont > 0 . On a

$$h_X(f)/h_X(g) = a/b \cdot$$

D'autre part, les propriétés fonctorielles des hauteurs (cf. [8], [9], [11]) montrent que, lorsque $h(x) \to +\infty$, on a

$$\lim_{x\to\infty} \cdot h_A(f(x))/h(x) = a \qquad \text{et} \qquad \lim_{x\to\infty} \cdot h_A(g(x))/h(x) = b \cdot$$

D'où

$$\lim_{x\to\infty} \cdot \frac{h_A(f(x))}{h_A(g(x))} = \frac{a}{b} = \frac{h_X(f)}{h_X(g)} ,$$

ce qui démontre le lemme.

Pour achever la démonstration du théorème 3 il ne reste plus qu'à établir le lemme suivant :

LEMME 6.- Soient V et W deux espaces euclidiens. Si v appartient à V ou W, on note H(v) le carré de la norme de v . Soit Λ un réseau de V , et soit $\varphi_1,\dots,\varphi_n,\dots$ une suite d'applications linéaires de V dans W . On fait l'hypothèse suivante :

(*) Pour tout couple d'éléments non nuls f , g de Λ , $H(\varphi_i(f))$ et $H(\varphi_i(g))$ sont non nuls pour i assez grand, et leur rapport tend vers $H(f)/H(g)$ quand i tend vers l'infini.

Alors φ_i est injectif pour i assez grand.

(Autrement dit, une "presque-similitude" est une injection.)

Soit g un élément non nul de Λ . Quitte à multiplier chaque φ_i par une homothétie, on peut supposer que $H(\varphi_i(g)) = H(g)$ pour i assez grand. L'hypothèse (*) signifie alors que, pour tout $f \in \Lambda$, $H(\varphi_i(f))$ tend vers $H(f)$. En appliquant ceci à la somme de deux éléments f_1 , f_2 de Λ , on voit que le produit scalaire de $\varphi_i(f_1)$ et $\varphi_i(f_2)$ tend vers le produit scalaire de f_1 et f_2 . Si (e_σ) est une base de Λ , le déterminant des produits scalaires des $\varphi_i(e_\sigma)$ entre eux (déterminant "de Gram") tend vers le déterminant correspondant pour les (e_σ) , donc est $\neq 0$ pour i assez grand, et φ_i est bien injective.

§ 3. Démonstration du théorème 2.

3.1. La courbe Y_m .

Soit m un entier ≥ 1 . Nous aurons besoin d'une certaine courbe algébrique Y_m , définie sur $\mathbb{Q}$, dont les points (mis à part un nombre fini d'entre eux) correspondent aux isogénies à noyau cyclique de degré m . On peut donner diverses définitions (*) de cette courbe :

a) (méthode analytique, cf. [5] par exemple). Soit $\Gamma_0(m)$ le sous-groupe de $\mathbf{SL}_2(\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \pmod{m}$, et soit $H = \{\tau \mid \mathrm{Im}(\tau) > 0\}$ le demi-plan de Poincaré. Le quotient $H/\Gamma_0(m)$ est une courbe algébrique affine $Y_{m/\mathbb{C}}^{aff}$ sur $\mathbb{C}$. La courbe $Y_{m/\mathbb{C}}$ est définie comme la compactification de $Y_{m/\mathbb{C}}^{aff}$; les points ajoutés correspondent aux "pointes" de $\Gamma_0(m)$, i.e. aux classes de conjugaison des sous-groupes unipotents maximaux de $\Gamma_0(m)$. Le corps des fonctions rationnelles de $Y_{m/\mathbb{C}}$ est engendré par j et j_m , où $j = j(\tau)$ est la fonction modulaire usuelle, et où $j_m(\tau) = j(m\tau)$.

b) Le procédé précédent ne définit que des courbes algébriques sur $\mathbb{C}$. Toutefois, on constate qu'il existe un polynôme $T_m(U,V)$, absolument irréductible, et à coefficients entiers, tel que $T_m(j, j_m) = 0$. On peut alors définir Y_m comme la courbe projective non singulière sur $\mathbb{Q}$ de corps des fonctions $\mathbb{Q}(j, j_m)$ (autrement dit comme la normalisée de la courbe projective définie par $T_m = 0$) ; de même Y_m^{aff}

(*) L'équivalence de ces diverses définitions est "bien connue", mais n'est exposée nulle part de façon détaillée ; c'est bien dommage, vu le rôle essentiel que jouent les courbes Y_m dans diverses questions (notamment la classification des courbes elliptiques sur $\mathbb{Q}$).

est définie comme la normalisée de la courbe affine d'équation $T_m = 0$.

Cette méthode peut d'ailleurs être rendue entièrement algébrique, cf. Igusa [6] ; on constate alors qu'elle s'applique en toute caractéristique première à m .

c) On peut enfin définir Y_m^{aff} comme quotient d'une variété modulaire convenable (cf. Deligne [3]) : on choisit un entier $N \geq 3$ qui soit multiple de m et l'on note X_N la variété modulaire qui classifie les courbes elliptiques munies d'une base du $\mathbf{Z}/N\mathbf{Z}$-module des points de division par N ("rigidification d'échelon N ") ; le groupe $G_N = GL_2(\mathbf{Z}/N\mathbf{Z})$ opère sur X_N . Soit $H_{N,m}$ le sous-groupe de G_N formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \pmod{m}$. Le quotient $X_N/H_{N,m}$ est la courbe Y_m^{aff} cherchée.

L'intérêt de Y_m provient de la propriété suivante : à tout couple (E,C) , où E est une courbe elliptique sur $\bar{K}$ et C un sous-groupe cyclique d'ordre m de $E(\bar{K})$, il correspond un point $j(E,C) \in Y_m^{aff}(\bar{K})$. Inversement, tout point de $Y_m^{aff}(\bar{K})$ est de la forme $j(E,C)$, et cela de façon unique à isomorphisme près. De plus, la fonction $(E,C) \longmapsto j(E,C)$ commute à l'action de $Gal(\bar{K}/K)$: on a $j(s(E), s(C)) = s(j(E,C))$ pour tout $s \in Gal(\bar{K}/K)$. En particulier, si E et C sont rationnels sur K , il en est de même de $j(E,C)$; inversement, tout point de $Y_m^{aff}(K)$ correspondant à une valeur de $j(E)$ distincte de 0 et de 1728 est de la forme $j(E,C)$, avec (E,C) rationnel sur K .

[Ces diverses propriétés se vérifient de la façon la plus commode sur la définition c). On peut aussi utiliser b), mais il faut alors faire attention aux points singuliers de la courbe plane $T_m = 0$.]

On peut donc reformuler le théorème 2 de la façon suivante :

THÉORÈME 2'.- Soit p un nombre premier. Il existe un entier positif $M = M(p,K)$ tel que la courbe Y_m, avec $m = p^M$, n'ait qu'un nombre fini de points rationnels sur K.

Remarque.- Soit $g(m)$ le genre de Y_m. Il est facile de calculer $g(m)$ en fonction de m et de vérifier que $g(m)$ tend vers l'infini avec m (cf. [5], p. 356-357). En particulier, on a $g(m) \geq 2$ pour $m = 2^6, 3^4, 5^3, 7^3, 11^2, 13^2, 17^2, 19^2$ ainsi que pour tout nombre premier ≥ 23 ; vu la conjecture de Mordell, les courbes Y_m correspondantes ne devraient avoir qu'un nombre fini de points rationnels sur K ; on devrait donc pouvoir prendre $M = 6, 4, 3, 2$ ou 1 suivant que $p = 2$, $p = 3$, $p = 5, 7$, $p = 11, 13, 17, 19$ ou $p \geq 23$.

3.2. Démonstration du théorème 2'.

On applique à la courbe Y_{p^M} le critère fourni par le corollaire au théorème 3. Il s'agit donc de trouver une variété abélienne A telle que le rang du groupe $A(Y_{p^M})$ soit strictement plus grand que celui de $A(K)$.

Pour cela, Manin commence par choisir un exposant m tel que le genre de Y_{p^m} soit ≥ 1. Par exemple (cf. [5], loc. cit.), pour $p = 2$, on prend $m = 5$; pour $p = 3$, $m = 3$; pour $p = 5, 7, 13$, $m = 2$; pour $p = 11$ et $p \geq 17$, on prend $m = 1$. Soit A la jacobienne de Y_{p^m}. On va voir que A convient.

Soit M un entier $\geq m$, et soit a un entier compris entre 0 et $M - m$. L'application $\tau \mapsto p^a\tau$ définit par passage au quotient une application $f_a : Y_{p^M}/C \to Y_{p^m}/C$. On constate sans difficulté que f_a est une application rationnelle, et qu'elle est définie sur $\mathbb{Q}$. Son interprétation en termes de couples (E,C) est la suivante : f_a transforme (E,C) en (E_a, C_a), avec :

$$E_a = E/p^{M-a}C \quad , \quad C_a = p^{M-m-a}C/p^{M-a}C \ .$$

On obtient ainsi $M - m + 1$ morphismes

$$f_o \ , \ f_1 \ , \ldots , \ f_{M-m} \ : \ Y_{p^M} \ \to \ Y_{p^m} \ .$$

Soit P_M (resp. P_m) la "pointe" de Y_{p^M} (resp. de Y_{p^m}) correspondant à $\tau = i\infty$; c'est un point rationnel sur $\mathbb{Q}$, et chaque f_a transforme P_M en P_m.

Plongeons Y_{p^m} dans sa jacobienne A en prenant comme origine le point P_m. Les f_a s'identifient alors à des morphismes de Y_{p^M} dans A appliquant le point origine P_M en 0. Ce sont donc des éléments du groupe noté $A(Y_{p^M})$ au n° 2.1. De plus :

LEMME 7.- Les éléments $f_o \ , \ldots , \ f_{M-m}$ de $A(Y_{p^M})$ sont linéairement indépendants sur $\mathbb{Z}$.

Soit Ω une forme différentielle invariante non nulle sur A, et soit ω sa restriction à Y_{p^m}. La forme ω est une forme de première espèce sur Y_{p^m}, non identiquement nulle. On peut l'écrire

$$\omega = \sum_{n=0}^{\infty} c_n \, q^n \, dq \quad , \qquad q = e^{2\pi i \tau} \ ,$$

les c_n étant des constantes telles que la série $(c_n q^n)$ converge pour $|q| < 1$.

Soient d'autre part $b_o \ , \ldots , \ b_{M-m}$ des entiers non tous nuls, et soit $f = b_o f_o + \ldots + b_{M-m} f_{M-m}$. Il nous faut montrer que f est un élément non nul de $A(Y_{p^M})$. Or l'image réciproque $f^*(\Omega)$ de Ω par f est égale à $\sum_a b_a f_a^*(\Omega)$, et $f_a^*(\Omega)$ n'est autre que l'image réciproque de ω par f_a (considéré comme morphisme de Y_{p^M} dans Y_{p^m}). Tout revient donc à montrer que la forme différentielle $f^*(\Omega) = \sum_a b_a f_a^*(\omega)$ est $\neq 0$. Vu la définition des f_a, cette forme s'écrit

$$f^*(\Omega) = \sum_{a=0}^{M-m} \sum_{n \geq 0} b_a\, c_n\, q^{n\, p^a}\, d(q^{p^a}) = \sum_{a,n} b_a\, p^a\, c_n\, q^{(n\, p^a + p^a - 1)}\, dq\ .$$

Soit a (resp. n) le plus petit entier tel que b_a (resp. c_n) soit $\neq 0$. La formule ci-dessus montre que le développement en série de $f^*(\Omega)$ contient le terme non nul $b_a\, p^a\, c_n\, q^{(n\, p^a + p^a - 1)}\, dq$, et que tous les autres termes ont un exposant de q strictement plus grand que $n\, p^a + p^a - 1$. On a donc bien $f^*(\Omega) \neq 0$ et le lemme 7 est démontré.

Nous pouvons maintenant achever la démonstration du théorème 2'. En effet, soit r le rang du groupe $A(K)$ et prenons $M \geq m + r$. D'après le lemme 7, le rang de $A(Y_{p^M})$ est $\geq r + 1$. Le corollaire au théorème 3 montre alors que $Y_{p^M}(K)$ est fini, C.Q.F.D.

Remarques.- 1) La démonstration du lemme 7 donnée ci-dessus est due à Atkin-Lehner. Celle de Manin [10] est moins simple et donne un résultat un peu moins fort ; toutefois elle a l'avantage de s'appliquer à d'autres groupes que le groupe modulaire.

2) On peut préciser le théorème 2' et prouver que, pour n assez grand, les seuls points rationnels sur K de $Y^{aff}_{p^n}$ sont ceux correspondant à des courbes elliptiques ayant de la multiplication complexe par un corps quadratique imaginaire F contenu dans K, et tel que p se décompose complètement dans F.

Cela se démontre en combinant le th. 2' avec les résultats connus sur les groupes de Galois des points d'ordre fini des courbes elliptiques (voir notamment [12], p. IV-9 et IV-10).

[Noter que, pour un corps K donné, il n'y a qu'un nombre fini de valeurs de j appartenant à K qui correspondent à des courbes à multiplication complexe.]

BIBLIOGRAPHIE

[1] G. BILLING and K. MAHLER - On exceptional points on cubic curves, J. London Math. Soc., 15 (1940), p. 32-43.

[2] J. W. S. CASSELS - Diophantine equations with special reference to elliptic curves, J. London Math. Soc., 41 (1966), p. 193-291.

[3] P. DELIGNE - Formes modulaires et représentations ℓ-adiques, Sém. Bourbaki, 21e année, 1968/69, exposé n° 355, New York, Benjamin.

[4] V. A. DEMJANENKO - Points rationnels sur une classe de courbes algébriques [en russe], Izv. Akad. N. C.C.C.P., 30 (1966), p. 1373-1396. [Trad. anglaise : Amer. Math. Transl., 66 (1968), p. 246-272.]

[5] R. FRICKE - Die elliptischen Funktionen und ihre Anwendungen, II, Teubner, Leipzig-Berlin, 1922.

[6] J. IGUSA - Fibre systems of Jacobian varieties, III, Amer. J. of Math., 81 (1959), p. 453-476.

[7] S. LANG - Diophantine Geometry, Interscience, New York, 1962.

[8] S. LANG - Les formes bilinéaires de Néron et Tate, Sém. Bourbaki, 16e année, 1963/64, exposé n° 274, New York, Benjamin.

[9] Y. MANIN - Hauteurs de Tate des points des variétés abéliennes ; variantes et applications [en russe], Izv. Akad. N. C.C.C.P., 28 (1964), p. 1363-1390. [Trad. anglaise : Amer. Math. Soc. Transl., 59 (1966), p. 82-110.]

[10] Y. MANIN - Borne uniforme de la p-torsion des courbes elliptiques [en russe], Izv. Akad. N. C.C.C.P., 33 (1969), p. 459-465. [Trad. anglaise à paraître dans "Mathematics of the U.S.S.R.-Izvestja".]

[11] A. NÉRON - Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math., 82 (1965), p. 249-331.

[12] J.-P. SERRE - Abelian ℓ-adic representations and elliptic curves, New York, Benjamin, 1968.