Groupe de travail
d'analyse ultramétrique

Marie-Claude Sarmant

Points rationnels d'ordre fini des courbes abéliennes (thèse d'Yves Hellegouarch)

Groupe de travail d'analyse ultramétrique, tome 2 (1974-1975), exp. n° 9, p. 1-13

<http://www.numdam.org/item?id=GAU_1974-1975__2__A8_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, P. ROBBA)
2e année, 1974/75, n° 9, 13 p.

27 janvier 1975

POINTS RATIONNELS D'ORDRE FINI DES COURBES ABÉLIENNES
(Thèse d'Yves HELLEGOUARCH)

par Marie-Claude SARMANT

Nous exposerons ici la première partie de la thèse d'Yves HELLEGOUARCH, la deuxième sortant du cadre de ce groupe d'étude.

En partant de l'étude des points rationnels d'ordre fini sur une courbe elliptique, on arrive à trouver une relation entre l'existence possible de tels points et le fait que certaines équations diophantiennes soient résolubles : ce qui amène ultérieurement à des cas particuliers de l'équation de Fermat.

1. Généralités sur les courbes abéliennes.

On appelle courbe abélienne définie sur le corps K la donnée d'une courbe elliptique (courbe algébrique de genre 1 définie sur K) et d'un point de cette courbe, rationnel sur K ([5] et [1]).

Du point de vue de l'étude des points rationnels sur cette courbe, nous pouvons nous ramener à une courbe du type cubique de Weierstrass définie de la manière suivante :

2 courbes abéliennes $\mathcal{A}_1 = (\mathcal{C}_1 , O_1)$ et $\mathcal{A}_2 = (\mathcal{C}_2 , O_2)$ définies sur K sont dites birationnellement équivalentes sur K s'il existe une application birationnelle $\varphi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ telle que $\varphi(O_1) = O_2$.

Une application birationnelle est une application rationnelle (c'est-à-dire où les transformés des coordonnées d'un point sont donnés par des fonctions rationnelles) bijective dont la réciproque est aussi rationnelle : elle transforme un point rationnel de $\mathcal{C}_1$ en un point rationnel de $\mathcal{C}_2$, et réciproquement.

THÉORÈME. - Toute courbe abélienne définie sur un corps K de caractéristique 0 est birationnellement équivalente sur K à une courbe abélienne $(\mathcal{C} , O)$ dite cubique de Weierstrass.

L'équation en coordonnées homogènes de $\mathcal{C}$ est :

$$Y^2 Z = X^3 + AXZ^2 + BZ^3$$

où $A , B \in K$, $4A^3 + 27B^2 \neq 0$, O désigne le "point à l'infini" de coordonnées $(0 , 1 , 0)$.

2 cubiques de Weierstrass dont les équations ont pour coefficients (A , B) et (A_1 , B_1) sont birationnellement équivalentes sur K si, et seulement si, il

existe $\lambda \in K$ tel que

$$\begin{cases} A_1 = \lambda^4 A , \\ B_1 = \lambda^6 B . \end{cases}$$

Nous nous ramènerons donc à étudier les points rationnels sur la courbe $\mathcal{A}$ d'équation :

$$(1) \qquad Y^2 = X^3 + AX + B , \quad 4A^3 + 27B^2 \neq 0 ,$$

où 0 est le point à l'infini $(0 , 1 , 0)$.

Soit $\mathcal{E}_K$ l'ensemble des points de $\mathcal{A}$ rationnels sur K . $\mathcal{E}_K$ peut être muni d'une structure de groupe abélien pour laquelle le point à l'infini de $\mathcal{A}$ est le zéro et pour laquelle 3 points ont pour somme zéro si, et seulement si, ils sont alignés ([1] et [11]).

Nous allons paramétrer $\mathcal{A}$, d'abord dans le cas où $K = \underset{\sim}{C}$, ensuite dans le cas où K est non archimédien.

1er cas : $K = \underset{\sim}{C}$. - L'équation (1) définit une surface de Riemann. Les périodes de l'intégrale abélienne $\omega = \int dx/2y$ attachée à cette courbe forment un réseau $\mathcal{R}$ du plan complexe. On peut uniformiser cette surface à l'aide de la fonction $\wp$ de Weierstrass [12] :

$$\begin{cases} x(u) = \wp(u , \omega , \omega') \\ y(u) = \frac{1}{2} \wp'_u(u , \omega , \omega') , \end{cases}$$

u est un paramètre complexe déterminé modulo $\mathcal{R}$, (ω , ω') est une base de $\mathcal{R}$.

L'application $u \longrightarrow (x(u) , y(u))$ est un isomorphisme de $T = \underset{\sim}{C}/\mathcal{R}$ sur $\mathcal{E}_{\underset{\sim}{C}}$. Pour que trois points de $\mathcal{E}_{\underset{\sim}{C}}$ soient alignés, il faut et il suffit que la somme de leurs paramètres soit nulle modulo $\mathcal{R}$ (théorème d'Abel).

2e cas.

(a) $\mathbf{K} = L$ corps complet valué non archimédien de caractéristique nulle. Soit v la valuation de L .

On paramètre certaines courbes elliptiques définies sur L à l'aide des <u>fonctions loxodromiques</u> de période q qui forment un corps $F_L(q)$ (pour $v(q) > 0$) :

$$F_L(q) = \{\text{fonctions } f \text{ méromorphes sur } L^* ; \ f(qx) = f(x) , \ \forall\, x \in L^*\} .$$

$F_L(q)$ est un corps de fonctions elliptiques définies sur L dont l'invariant modulaire j est donné par la formule ([10] et [13]) :

$$j^{-1} = q((\prod_{n=1}^{\infty}(1-q^n)^{24})/[1+240 \sum_{n=1}^{\infty}(n^3 q^n/1-q^n)]^3 = q[1-744q+\ldots] .$$

Pour avoir l'équation d'une courbe elliptique engendrant $F_L(q)$, nous poserons :

$$\begin{cases} \xi(X) = 4 \sum_{n \in \underset{\sim}{Z}} q^n X/(1 - q^n X)^2 + 4 \sum_{n \in \underset{\sim}{Z}} q^n/(1 - q^n)^2 \\ \eta(X) = 4 \sum_{n \in \underset{\sim}{Z}} (q^n X(1 + q^n X)/(1 - q^n X)^3) . \end{cases}$$

ξ et η appartiennent à $F_L(q)$, et on a :

$$(\mathcal{C}_q) \qquad \eta^2 = \xi(\xi^2 - 2S\xi + T)$$

S , $T \in \mathbb{Z}[[q]]$ et S et $T \equiv 1 \mod q$.

L'étude des points rationnels de $\mathcal{C}_q$ au moyen des fonctions loxodromiques repose sur le théorème suivant :

THÉORÈME. - Le groupe des points de $\mathcal{C}_q$ rationnels sur L est isomorphe au groupe-quotient $L^*/(q)$ ([10] et [13]).

Nous appellerons cet isomorphisme Φ_q l'isomorphisme de Jacobi de $F_L(q)$.

L'isomorphisme Φ_q va permettre de définir une valuation sur le groupe $\mathcal{G}_{q,L}$ des points de $\mathcal{C}_q$ rationnels sur L .

Si P est un point de $\mathcal{C}_q$ rationnel sur L , nous avons :

$$P = (\xi(\Phi_q(P)) \ , \ \eta(\Phi_q(P))) \ .$$

Soient $G = \{v(x) \ ; \ v \in L\}$, $H = (v(q))$.

Le diagramme commutatif suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (q) & \longrightarrow & L^* & \longrightarrow & L^*/q & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v} & & & & \\ 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \end{array}$$

permet de définir un homomorphisme unique $L^*/q \longrightarrow G/H \subset \underset{\sim}{R}/\underset{\sim}{Z}$ que l'on notera encore v .

Φ_q est un isomorphisme entre $\mathcal{G}_{q,L}$ et L^*/q , donc Φ_q induit une valuation v sur $\mathcal{G}_{q,L}$ telle que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \mathcal{G}_{q,L} & \xrightarrow{\Phi_q} & L^*/q \\ & \searrow^{v} & \downarrow{\scriptstyle v} \\ & & \underset{\sim}{R}/\underset{\sim}{Z} \end{array}$$

(b) K non archimédien n'est pas complet, L est une complétion non archimédienne de K .

Si $\mathcal{A}$ est birationnellement équivalente à une courbe $\mathcal{C}_q$, nous avons $v[j(\mathcal{A})]<0$: nous dirons qu'une courbe $\mathcal{A}$, telle que $v[j(\mathcal{A})] < 0$, est une cubique de Tate pour v .

Nous nous occuperons essentiellement des cubiques de Tate, puisque ce sont les seules ayant des chances d'être birationnellement équivalentes à des courbes $\mathcal{C}_q$. Nous allons voir dans quels cas on est sûr que $\mathcal{A}$ est birationnellement équivalente à une courbe $\mathcal{C}_q$.

THÉORÈME. - Soit une cubique de Tate $\mathcal{A}$ pour la valuation non archimédienne v de K et soit L le complété de K pour v .

Il existe $q \in L^*$ unique tel que $v(q) > 0$ et tel que :

$$[j(\mathcal{A})]^{-1} = q(\prod_{n=1}^{\infty}(1 - q^n)^{24}/[1 + 240 \sum_{n=1}^{\infty} n^3 q^n/(1 - q^n)]^3) .$$

$\mathcal{A}$ est birationnellement équivalente à $\mathcal{C}_q$ sur une extension L' de L de degré au plus égal à 2 par une application $\psi : \mathcal{A} \longrightarrow \mathcal{C}_q$ et $\Phi_q \circ \psi$ est un isomorphisme $\mathcal{G}_{L'} \longrightarrow L'^*/q$. Il existe une valuation canonique v sur $\mathcal{G}_{L'}$ qui applique homomorphiquement $\mathcal{G}_{L'}$ dans $\mathbb{Q}/\mathbb{Z}$.

Définition. - On appellera branche unitaire de $\mathcal{G}_{L'}$ le noyau $\mathcal{H}_L$, de v .

- Si $\mathcal{G}_L$ admet un point d'ordre premier $p > 3$ n'appartenant pas à $\mathcal{H}_L$, alors $\mathcal{A}$ est birationnellement équivalente à $\mathcal{C}_q$ sur L [3].

- Si $v(K) = \mathbb{Z}$ et si $0 < v(3) < 3$, et si $\mathcal{G}_L$ admet un point d'ordre 2.3^3 , alors $\mathcal{A}$ est birationnellement équivalente à $\mathcal{C}_q$ sur L .

- Si $v(K) = \mathbb{Z}$ et $0 < v(3) < 3$, et si $\mathcal{G}_L$ admet un point d'ordre 3^2 et 3 points d'ordre 2 , $\mathcal{A}$ est birationnellement équivalente à $\mathcal{C}_q$ sur L .

2. Quelques propriétés de $\mathcal{G}_K$ (théorème de Mordell-Weil).

K est maintenant un corps de nombres quelconques. Alors :

- $\mathcal{G}_K$ est un groupe de type fini [7] ;

- Le sous-groupe de torsion de $\mathcal{G}_K$ est fini, et il est somme directe de 2 groupes cycliques ;

- Si K est réel, soit n l'ordre du sous-groupe de torsion de $\mathcal{G}_K$.

Soit ω la plus petite période positive de $\mathcal{A}$, et ω' une période imaginaire de $\mathcal{A}$ telle que (ω , ω') soit une base de $\mathcal{R}$. Alors le sous-groupe de torsion de $\mathcal{G}_K$ admet une base $\mathcal{B}$ appartenant à l'un des types suivants :

$\mathcal{B} = \{u_1\}$ avec $u_1 = \omega/n$,

$\mathcal{B} = \{u_1\}$, $u_1 = \omega/n + \omega'/2$, $n \equiv 0 \pmod 2$,

$\mathcal{B} = \{u_1\}$, $u_1 = 2\omega/n + \omega'/2$, $n \equiv 2 \pmod 4$,

$\mathcal{B} = \{u_1 , u_2\}$, $u_1 = 2\omega/n$, $u_2 = \omega'/2$, $n \equiv 0 \pmod 4$.

3. Isogénies de Gauss et de Landen.

L'application $P \longrightarrow 2P$, qui associe à un point P d'une courbe abélienne $\mathcal{A}$ le double de ce point, se factorise en deux isogénies qui font apparaître une nouvelle courbe abélienne $\mathcal{A}'$ associée à $\mathcal{A}$.

Nous allons décrire cette propriété dans le cas où la courbe $\mathcal{A}$ est définie sur un corps de nombres K , et admet un point d'ordre 2 rationnel sur K .

1er cas : K est plongé dans $\mathbb{C}$. - Soit une courbe abélienne $\mathcal{A}$ d'équation :

$$Y^2 = X(X^2 + CX + D) , \quad C , D \in K , \quad D \neq 0 , \quad C^2 - 4D \neq 0 .$$

Soit (ω , ω') une base du réseau $\mathcal{R}$ des périodes de $\mathcal{A}$ telle que l'argument du point $(0 , 0)$ soit égal à $\omega/2$.

Soit $\mathcal{R}'$ le réseau de $\underset{\sim}{C}$ engendré par ω et $2\omega'$, et soit $\mathcal{A}'$ la courbe abélienne $\underset{\sim}{C}/\mathcal{R}'$.

Il existe une isogénie $f : \mathcal{A} \longrightarrow \mathcal{A}'$ appelée isogénie de Landen, telle que l'on ait pour $t \in \underset{\sim}{C}$:

$$f(t + \mathcal{R}) = 2t + \mathcal{R}' .$$

L'isogénie duale, $f' : \mathcal{A}' \longrightarrow \mathcal{A}$, appelée isogénie de Gauss, est telle que, pour tout $u \in \underset{\sim}{C}$,

$$f'(2u + \mathcal{R}') = u + \mathcal{R}$$

f et f' sont algébriques et définies sur K .

Si le point de $\mathcal{A}$ d'argument $\omega/4$ est rationnel sur K , alors $\mathcal{A}'$ admet 3 points d'ordre 2 rationnels sur K .

Si P est un point d'ordre impair n sur $\mathcal{A}$, $f(P)$ est un point d'ordre impair n sur $\mathcal{A}'$, et réciproquement.

Nous aurons besoin pour l'étude des points d'ordre impair de $\mathcal{A}$, de relations de duplication faisant intervenir systématiquement $\mathcal{A}$ et $\mathcal{A}'$. Pour cela nous allons définir une fonction elliptique U attachée à $\mathcal{A}$ et une fonction elliptique V attachée à $\mathcal{A}'$ par les formules

$$\begin{cases} U(t) = y(t)/x(t) \\ V(t) = \frac{1}{2}\,(y'(t)/x'(t)) \end{cases}$$

$(x(t) , y(t))$ étant le point de paramètre t de la courbe $\mathcal{A}$

$(x'(t) , y'(t))$ étant le point de paramètre t de la courbe $\mathcal{A}'$.

On a les relations :

$$\begin{cases} x(t) = V^2(t) \\ y(t) = V^2(t)\, U(t) \end{cases} \qquad \begin{cases} x'(2t) = U^2(t) \\ y'(2t) = 2U^2(t)\, V(2t) \end{cases}$$

$$\begin{cases} U(2t) + U(t) = (V^2(t)/V(2t)) - V(2t) \\ 2[V(4t) + V(2t)] = (U^2(t)/U(2t)) - U(2t) . \end{cases}$$

<u>2e cas</u> : Soit v une valuation non archimédienne de K , et soit $K \longrightarrow L$ une complétion de K pour v .

Pour que $\mathcal{A}$ soit une cubique de Tate pour v , il faut et il suffit que $\mathcal{A}'$ soit une cubique de Tate pour v .

$\mathcal{A}'$ étant définie par l'équation :

$$Y^2 = X'(X^2 - 2CX' + G) , \text{ où } G = C^2 - 4D .$$

Si $\mathcal{C}$ est une cubique de Tate pour v, alors $\mathcal{C}$ (resp. $\mathcal{C}'$) est birationnellement équivalente à $\mathcal{C}_q$ (resp. $\mathcal{C}_{q'}$) sur une clôture algébrique de L, et :

si $v(D) > v(G)$, on a $q = q'^2$,

si $v(D) \leqslant v(G)$, on a $q' = q^2$.

4. Théorèmes de Nagell [1].

Lorsque $K = \mathbb{Q}$, ces théorèmes permettent la détermination effective des points d'ordre fini d'une courbe abélienne donnée.

THÉORÈME I. - Soient un corps de nombres algébriques K et une valuation non archimédienne v de K, p la caractéristique du corps résiduel de v, et K_v une complétion de K pour v.

On suppose que la courbe :

$$Y^2 = X^3 + AX + B$$

est rationnelle sur K_v et que $v(A) \geqslant 0$ et $v(B) \geqslant 0$. Soit un point (x_1, y_1) de cette courbe, rationnel sur K_v et d'ordre $n > 1$.

1° si $p = 2$ ou si $n \neq p^r$ (r entier > 0), alors $v(x_1) \geqslant 0$,

2° si $p \neq 2$ et $n = p^r$, alors :

$$v(x_1) \geqslant -2\eta v(p), \quad v(y_1) \geqslant -3\eta v(p)$$

avec

$$\eta = \begin{cases} (3^{2r} - 3^{2r-2})^{-1} & \text{si } p = 3 \\ (p^r - p^{r-1})^{-1} & \text{si } p \neq 3. \end{cases}$$

THÉORÈME II. - $y_1 = 0$ si $n = 2$ et sinon :

$$v(y_1^2) \leqslant \begin{cases} v(4A^3 + 27B^2) + 2\eta v(p) & \text{si } n = p^r \text{ ou } 2p^r \text{ avec } p \neq 2 \\ v(4A^3 + 27B^2) & \text{dans les autres cas.} \end{cases}$$

Si $A, B \in \mathbb{Z}$ et si $\mathcal{C}$ admet un point (x_1, y_1) d'ordre > 2 rationnel sur $\mathbb{Q}$, x_1 et y_1 sont des entiers et y_1^2 divise $4A^3 + 27B^2$.

5. Groupes de Lutz [8].

Nous allons maintenant examiner certains sous-groupes de $\mathcal{E}_K$ fournissant un système fondamental de voisinages de l'origine.

K sera maintenant le complété d'un corps de nombres algébriques pour une valuation non-archimédienne v. Nous supposerons que $u(K) = \mathbb{Z}$, et nous poserons :

$$\mathfrak{A} = \{a \in K ; \ v(a) \geqslant 0\}$$

$$\mathfrak{p} = \{a \in K ; \ v(a) > 0\}$$

$$k = \mathfrak{A}/\mathfrak{p}.$$

1° Donnons-nous une courbe abélienne $\mathcal{A}$, d'équation

$$Y^2 = X^3 + AX + B \qquad A , B \in \mathfrak{A} , \quad 4A^3 + 27B^2 \neq 0 .$$

L'espace projectif $\underset{\sim}{P}_2(K)$, induit sur le groupe $\mathcal{G}_K$, une structure de groupe topologique et un point $(x , y) \in \mathcal{G}$ est d'autant plus voisin du zéro de $\mathcal{G}$ (c'est-à-dire du point à l'infini de $\mathcal{A}$) que $v(x)$ et $v(y)$ sont plus proches de $- \infty$.

Si $(x , y) \in \mathcal{G}$ et si $v(x) < 0$ il existe un entier $n(P) > 0$ tel que :

$$v(x^3) = v(y^2) = - 6n(P)$$

où P désigne le point (x , y) .

m étant un entier > 0 , nous désignons par $\mathcal{G}_m$ l'ensemble des points $P \in \mathcal{G}$ tels que $n(P) \geq m$.

Propriétés de $\mathcal{G}_m$.

$\mathcal{G}_m$ est un sous-groupe de $\mathcal{G}$

$(\mathcal{G}_m : \mathcal{G}_{m+1}) = \text{card } k$.

- si $v(4A^3 + 27B^2) = 0$.

Soient deux points P_1 et $P_2 \in \mathcal{G} - \mathcal{G}_1$; posons $P_i = (x_i , y_i)$. Une condition nécessaire et suffisante pour que P_1 et P_2 soient congrus modulo $\mathcal{G}_1$ est que :

$$\begin{cases} x_1 \equiv x_2 \\ y_1 \equiv y_2 \end{cases} \quad (\text{modulo } \mathfrak{p})$$

et l'application $(x , y) \longrightarrow (\overline{x} , \overline{y})$, où $\overline{x}$ et $\overline{y}$ sont les images de x et y dans k , induit un isomorphisme entre $\mathcal{G}/\mathcal{G}_1$ et le groupe des points rationnels sur k de la courbe réduite modulo $\mathfrak{p}$.

- si $v(4A^3 + 27B^2) = \delta > 0$, et si $v(2) = e$, une condition suffisante pour que P_1 et P_2 soient congrus modulo $\mathcal{G}_1$ est que :

$$\begin{cases} x_1 \equiv x_2 \text{ modulo } \mathfrak{p}^{[(\delta + 2)/2] + e} \\ y_1 \equiv y_2 \text{ modulo } \mathfrak{p}^{\delta+3} \end{cases} ,$$

Remarque. - D'après les théorèmes de Nagell , si $\mathcal{G}_m$ possède un point d'ordre fini > 1 , alors $m \leq \eta v(p)$.

Comme $\eta \leq \frac{1}{4}$ on en déduit que si $m > \frac{v(p)}{4}$, $\mathcal{G}_m$ ne peut admettre de point d'ordre fini > 1 .

2° Nous allons prendre maintenant un autre système fondamental de voisinages de l'origine de $\mathcal{G}$.

Nous nous donnerons la courbe abélienne $\mathcal{A}$ sous la forme :

$$Y^2 = X(X^2 + CX + D) \qquad C , D \in \mathfrak{A} .$$

Si $(x , y) \in \mathfrak{S}$ et si $v(x) < 0$, il existe un entier $n^*(P) > 0$ tel que $v(x^3) = v(y^2) = -6n^*(P)$.

m étant un entier > 0 nous désignons par $\mathfrak{S}^*_m$ l'ensemble des points $P \in \mathfrak{S}$ tels que $n^*(P) \geq m$.

Propriétés de $\mathfrak{S}^*_m$.

$\mathfrak{S}^*_m$ est un sous-groupe de $\mathfrak{S}$

$(\mathfrak{S}^*_m : \mathfrak{S}^*_{m+1}) = \text{card } k$.

On suppose $v(DG) = 0$, où $G = C^2 - 4D$.

Soient deux points $P_1 , P_2 \in \mathfrak{S} - \mathfrak{S}_1$, nous poserons

$$P_i = (x_i , y_i) .$$

Alors une condition nécessaire et suffisante pour que P_1 et P_2 soient congrus modulo $\mathfrak{S}^*_1$ est que :

$$\begin{cases} x_1 \equiv x_2 \\ y_1 \equiv y_2 \end{cases} \text{ modulo } (\mathfrak{p})$$

et l'application $(x , y) \longrightarrow (\overline{x} , \overline{y})$ induit un isomorphisme entre $\mathfrak{S}/\mathfrak{S}^*_1$ et le groupe g^* des points rationnels sur k de la courbe réduite modulo $\mathfrak{p}$.

6. Limitation de l'ordre des groupes quotients lorsque $j(\mathcal{A}) \in \mathfrak{A}$ [4].

Soit la courbe $\mathcal{A}$ d'équation :

$$Y^2 = X^3 + AX + B .$$

Nous pouvons effectuer une transformation birationnelle sur $\mathcal{A}$, pour que :

$$\alpha = \inf\{3v(A) , 2v(B)\} < 12 .$$

Nous dirons alors que cette équation est primitive.

THÉORÈME. - Pour les courbes $\mathcal{A}$ telles que $j(\mathcal{A}) \in \mathfrak{A}$ et pour les formes primitives de l'équation de $\mathcal{A}$, l'indice de $\mathfrak{S}_m$ dans $\mathfrak{S}$ est borné par une constante $O(m , q)$ indépendante de A et de B .

COROLLAIRE. - Si $v(6) = 0$, si $j(\mathcal{A}) \in \mathfrak{A}$ et si $\mathcal{A}$ admet une équation primitive pour laquelle

$$v(4A^3 + 27B^2) > 0$$

l'ordre du sous-groupe de torsion de $\mathfrak{S}$ divise $4q^{u(v)}$ ou $3q^{u(v)}$ où

$$u(v) = [v(p)/4] + 1 .$$

DÉFINITION. - π étant un nombre premier quelconque, nous désignerons par $I_\pi(m , K)$ la borne supérieure des index des composantes π-primaires des groupes $\mathfrak{S}/\mathfrak{S}_m$ pour les formes primitives de l'équation des courbes abéliennes $\mathcal{A}$ telles

que $j(\mathcal{A}) \in \mathfrak{A}$.

Cas particulier. - Nous nous donnons $\mathcal{A}$ par l'équation :

$$Y^2 = X(X^2 + CX + D) ,$$

et nous supposerons $\beta = \inf\{2v(C) , v(D)\} < 4$.

Nous dirons alors que cette équation est primitive.

PROPOSITION. - Si cette équation est primitive, si $v(D^2 C) > 0$ et si $j(\mathcal{A}) \in \mathfrak{A}$, l'ensemble $\mathcal{S}_0^*$ des points de $\mathcal{S}$ tels que $v(x) \leqslant 0$ est un sous-groupe de $\mathcal{S}$.

Si de plus $v(2) = 0$ on a :

$(\mathcal{S} : \mathcal{S}_0^*) = 1$, 2 ou 4 et $2\mathcal{S} \subset \mathcal{S}_0^*$.

COROLLAIRE. - Si $\mathcal{A}$ n'est pas une cubique de Tate sur $\mathbb{Q}_3$, $\mathcal{S}$ n'admet pas de point rationnel d'ordre impair > 3 .

PROPOSITION. - Si cette équation est primitive, et si $\mathcal{S}$ n'est pas une cubique de Tate sur $\mathbb{Q}_2$, $\mathcal{S}$ n'a pas de point rationnel d'ordre impair > 1 .

7. Etude locale des points d'ordre impair.

Nous allons préciser pour les points d'ordre impair, l'étude locale des théorèmes de NAGELL en distinguant le cas où $\mathcal{A}$ est une cubique de Tate de celui où elle n'en est pas une.

Soit K un corps valué complété d'un corps de nombres algébriques pour une valuation non archimédienne v , et soit une courbe abélienne $\mathcal{A}$ d'équation :

$$Y^2 = X^3 + AX + B , \qquad A , B \in \mathfrak{A} .$$

Soient $\overline{K}$ une clôture algébrique de K , et $\mathcal{S}_{\overline{K}}$ le groupe des points de $\mathcal{A}$ rationnels sur $\overline{K}$.

Soient α , β , γ les racines de $X^3 + AX + B$. On pose :

$a^2 = \beta - \gamma$, $b^2 = \gamma - \alpha$, $c^2 = \alpha - \beta$,

$\lambda = 4(\frac{c}{b} - \frac{b}{c})$, $\lambda' = 4(\frac{a}{c} - \frac{c}{a})$, $\lambda'' = 4(\frac{b}{a} - \frac{a}{b})$.

$\mathcal{A}$ est birationnellement équivalente sur $\overline{K}$ aux cubiques d'équations :

$Y^2 = X(X - b^2)(X + c^2)$

$Y^2 = X'(X' - c^2)(X' + a^2)$ $\qquad (X' = X + c^2)$

$Y^2 = X''(X'' - a^2)(X'' + b^2)$ $\qquad (X'' = X - b^2)$

et l'invariant modulaire de $\mathcal{A}$ est :

$$j(\mathcal{A}) = \frac{(\lambda^2 + 48)^3}{\lambda^2 + 64} = \frac{(\lambda'^2 + 48)^3}{\lambda'^2 + 64} = \frac{(\lambda''^2 + 48)^3}{\lambda''^2 + 64} .$$

Remarque. - $j(\mathcal{C}) \in \mathfrak{U}$ équivaut à $v(\lambda^2 + 64) \in [0 , 12v(2)]$. En particulier, si λ , λ' et λ'' ne sont pas tous dans l'anneau des entiers de $\overline{K}$, $\mathcal{C}$ est une cubique de Tate.

Nous poserons, en désignant par i une racine carrée de -1 :

$$z = -\frac{iX}{bc} , \quad z' = -\frac{i}{ca} X' , \quad z'' = -\frac{i}{ab} X'' .$$

Soit un nombre entier impair $n > 1$.

Une condition nécessaire et suffisante pour que x soit l'abscisse d'un point $P \neq 0$ de $\mathcal{C}_{\overline{K}}$ tel que $nP = 0$ est que z soit racine d'un polynôme en x :

$$D_n(\lambda , z) = 1 + \ldots + a_h(\lambda)\, Z^h + \ldots + (-1)^{(n-1)/2}\, {}_nZ^{(n^2-1)/2}$$

où les $a_h(\lambda)$ appartiennent à $\underset{\sim}{Z}[\lambda]$.

Les éléments irréductibles de l'anneau de polynômes $\underset{\sim}{Z}[\lambda]$, qui divisent le discriminant de $D_n(\lambda , \underset{\sim}{Z})$, divisent $n(\lambda^2 + 64)$.

Si $j(\mathcal{C}) \in \mathfrak{U}$, si $P \neq 0$ est un point de $\mathcal{C}_{\overline{K}}$ tel que $nP = 0$, et si x , x' , x'' sont les trois abscisses de P

$$x \sim bc \; ; \quad x' \sim ca , \quad x'' \sim ab$$

(c'est-à-dire $v(x) = v(bc)$, etc.), et $y \sim abc$, où y désigne l'ordonnée de P .

Si $j(\mathcal{C})$ est quelconque, on a :

si $v(n) = 0$, x , x' , x'' sont des entiers de $\overline{K}$,

si $v(n) > 0$ et $n = p^h$ avec p premier impair, alors :

$$\inf\{v(x) , v(x') , v(x'')\} \geq -2p^h/\varphi(p^h) .$$

Nous supposerons maintenant que $\mathcal{C}$ est une cubique de Tate, birationnellement équivalente à la cubique :

$$(\mathcal{C}_q) \qquad y^2 = \xi(\xi^2 - 2S\xi + T) .$$

Notation. - Pour $x \in \underset{\sim}{R}$ et $n \in \underset{\sim}{N}^*$, nous désignerons par $\|x\|_n$ la distance de x à $n\underset{\sim}{Z}$.

On voit qu'il existe une application $(\ )_n$ telle que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \underset{\sim}{R} & \longrightarrow & \underset{\sim}{R}/n\underset{\sim}{Z} \\ & \searrow^{\|\ \|_n} & \downarrow (\ )_n \\ & & [0 , (n/2)] \end{array}$$

Définition. - Soit une cubique de Tate $\mathcal{C}$.

$\mathfrak{p}$ étant l'idéal maximal de $\mathfrak{U}$, et P un point de $\mathcal{C}$, rationnel sur $\overline{K}$, on appellera caractéristique $\mathfrak{p}$-adique de P , et on notera $\chi_{\mathfrak{p}}(P)$ le nombre :

$$(\Phi_q(P))_1 = \|v(P)\|_1 .$$

8. Propriétés de $\chi_p(P)$.

$\chi_p(jP) = (j\chi_p(P))_1$.

si $nP = 0$, $\chi_p(P) \in \frac{1}{n}\underset{\sim}{Z}$.

Soit un point P d'ordre p^h dans $\mathfrak{S}_{\overline{K}}$. Si s est un entier tel que $0 \leqslant s \leqslant h$, on a :

$$\chi_p(p^s P) = \frac{(p^h \chi_p(P))}{p^{h-s}}\, p^{h-s}$$

soit un point P d'ordre $p^h > 2$ dans le groupe $\mathfrak{S}_{\overline{K}}$ des points rationnels sur $\overline{K}$ d'une cubique de Tate équivalente à $\mathfrak{C}_q$.

Si y et y_i désignent les coordonnées des points P et iP , et si $iP \neq 0$, on a :

$$v(y_i) - v(y) = (\chi_p(iP) - \chi_p(P))v(q)$$

lorsque $v(p) = 0$, ou lorsque iP n'appartient pas à la branche unitaire de $\mathfrak{S}_{\overline{K}}$, ou lorsque i n'est pas divisible par p .

COROLLAIRE. - Soit un nombre premier $p > 3$, et soit un point P d'ordre $p^h > 1$ dans le groupe $\mathfrak{S}_{\overline{K}}$.

Une condition nécessaire et suffisante pour que P n'appartiennent pas à la branche unitaire de $\mathfrak{S}_{\overline{K}}$ (i. e. $v(P) \neq 0$) est que $v(y_i)$ ne soit pas indépendants de i quand i parcourt $\underset{\sim}{Z}^*_{p^h}$.

COROLLAIRE. - On suppose $v(K) = \underset{\sim}{Z}$. Soit un nombre premier $p > 3$ et soit un point P d'ordre $p^h > 1$ dans le groupe $\mathfrak{S}_K$.

Si on note y_i l'ordonnée du point $Q_i = ip^s P$, avec $i \in \underset{\sim}{Z}^*_{p^{h-s}}$, (groupe des unités de l'anneau $\underset{\sim}{Z}/p^{h-s}\underset{\sim}{Z}$), on a

$$v(y_i) - v(y_1) \in p^s \underset{\sim}{Z} .$$

Notons y'_i l'ordonnée du point $R_i = ip^{h-1} P$, avec $i \in \underset{\sim}{Z}^*_p$, et désignons par $[x]'$ le plus petit entier supérieur ou égal au réel x .

Alors si R_1 n'appartient pas à la branche unitaire de $\mathfrak{S}_K$ les nombres q et $j(\mathfrak{a})$ sont des puissances d'ordre p^K d'éléments de K^* , et les quotients y'_i/y_1 sont des puissances d'ordre

$$p^{\inf\{h\ ,\ [p^{h-1}/v(p)]'\}} - 1$$

d'éléments de K^* .

9. Relation avec les sommes de puissances.

THÉORÈME. - Soit une courbe abélienne $\mathfrak{A}$ définie sur $\underset{\sim}{Q}$ par l'équation :

$$Y^2 = X^3 + AX + B\ ,\quad 4A^3 + 27B^2 \neq 0 .$$

On suppose que $\mathcal{E}_{\underset{\sim}{Q}}$ admet un point P d'ordre p^h avec p premier > 3 et que :

$$p^h > \sup\{I_p(1 , 2) , I_p(1 , 3)\} .$$

Posons $p'^h = (p^h - 1)/2$. Il existe p'_h entiers positifs $\alpha_1 \dots \alpha_{p'_h}$ premiers entre eux deux à deux et un nombre $\gamma \in \underset{\sim}{Q}^*$ tels que si $i \in \underset{\sim}{Z}_{p^h}$ n'est pas nul, et si y_i désigne l'ordonnée du point iP , on ait :

$$y_i \sim \gamma\, \alpha_1^{(i)_{p^h}} \dots \alpha_\nu^{(i\nu)_{p^h}} \dots \alpha_{p'_h}^{(ip'_h)_{p^h}} .$$

D'autre part, si le nombre premier π divise α_ν , on a :

$$\pi \equiv 1 \quad (\text{modulo } p^{v_p(\nu)})$$

et lorsque $h > 1$ le produit $\alpha_1 \dots \alpha_\nu \dots \alpha_{p'_h}$ est divisible par le produit de nombres premiers $\leqslant p$.

COROLLAIRE. - Posons $Q = p^{h-\nu} P$. Soit z_i l'ordonnée du point iQ , avec $i \in \underset{\sim}{Z}_{p^\nu}$ non nul ; on a :

$$z_i \sim \gamma A_1^{(i)_{p^\nu}} \dots A_{p'_\nu}^{(ip'_\nu)_{p^\nu}} ,$$

où

$$A_\mu = \prod_{(j)_{p^\nu} = \mu} \alpha_j^{p^{h-\nu}} \quad \text{pour} \quad \mu = 1 \dots p'_\nu ,$$

et où la constante γ est la même que ci-dessus.

THÉORÈME. - Il existe un polynôme universel homogène

$$F(T_1 , T_2 , T_3 , T_4) \in \underset{\sim}{Z}[T_1 , T_2 , T_3 , T_4]$$

tel que l'existence d'un point rationnel P d'ordre p^h sur une courbe abélienne $\mathcal{A}$, définie sur $\underset{\sim}{Q}$, entraîne l'existence d'au moins p'_ν solutions rationnelles distinctes de l'équation :

$$F(\alpha_1^{p^{h-\nu}} , \alpha_2^{p^{h-\nu}} , \alpha_3^{p^{h-\nu}} , \alpha_4^{p^{h-\nu}}) = 0$$

lorsque $p > 3$, $p^h > \sup\{I_p(1 , 2) , I_p(1 , 3)\}$ et $0 < \nu \leqslant h$.

Indication de la démonstration. - On écrit d'abord une relation d'alignement entre multiples du point $p^{h-\nu}$, P ne faisant intervenir que les ordonnées de ces points :

$$F[y(u) , y(2u) , y(4u) , y(8u)] = 0 .$$

Puis on applique le corollaire précédent.

COROLLAIRE. - Soit une courbe abélienne $\mathcal{A}$, définie sur $\underset{\sim}{Q}$, et admettant un point rationnel P d'ordre p^h , avec p premier > 13 et $h > 1$.

Il existe un entier universel calculable N tel que si $p > 93$ et $0 < \nu \leq h$:

$$\sum_{i=0}^{N} \alpha_i^{p^{h-\nu}} = 0$$

admette au moins p'_ν solutions distinctes $(\alpha_0 \ldots \alpha_N)$ dans $\underline{Z}$.

BIBLIOGRAPHIE

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

[2] HASSE (H.). - Zur Theorie der abstraken elliptischen Funktionenkörper, I, J. für reine und angew. Math., t. 175, 1936, p. 55-62.

[3] HELLEGOUARCH (Y.). - Une propriété arithmétique des points exceptionnels rationnels d'ordre pair d'une cubique de genre 1 , C. R. Acad. Sc. Paris, t. 260, 1965, p. 5989-5992.

[4] HELLEGOUARCH (Y.). - Applications d'une propriété arithmétique des points exceptionnels d'ordre pair d'une cubique de genre 1 , C. R. Acad. Sc. Paris, t. 260, 1965, p. 6256-6258.

[5] LANG (S.). - Introduction to algebraic geometry. - New York, London, Interscience Publishers, 1958 (Interscience Tracts in pure and applied Mathematics, 5).

[6] LANG (S.). - Abelian varieties. - New York, London, Interscience Publishers, 1959 (Interscience Tracts in pure and applied Mathematics, 7).

[7] LANG (S.). - Diophantine geometry. - New York, London, Interscience Publishers, 1962 (Interscience Tracts in pure and applied Mathematics, 11).

[8] LUTZ (E.). - Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques, J. für reine und angew. Math., t. 177, 1937, p. 238-247.

[9] NORTHCOTT (D. G.). - An introduction to homological algebra. - Cambridge at the University Press, 1960.

[10] ROQUETTE (P.). - Analytic theory of elliptic functions over local fields. - Göttingen, Vandenhoech and Ruprecht, 1970 (Hamburger mathematische Einzelschriften, Neue Folge, 1).

[11] SEIDENBERG (A.). - Elements of the theory of algebraic curves. - Reading, Menlo Park, London, Addison-Wesley publishing Company, 1968 (Addison-Wesley Series in Mathematics).

[12] SIEGEL (C.). - Topics in complex function theory. Vol. I : Elliptic functions and uniformization theory. - New York, London, Sydney, Wiley Interscience, 1969 (Interscience Tracts in pure and applied Mathematics, 25).

[13] VALIRON (G.). - Cours d'analyse mathématique : Théorie des fonctions. - Paris, Masson, 1942.

[14] WEBER (H.). - Lehrbuch der Algebra. Vol. 3, 3rd edition [Reprint of the 2nd 1908) edition]. - New York, Chelsea publishing Company, s. d.

[15] WHITTAKER (E. T.) et WATSON (G. N.). - A course of modern analysis. 4th edition. - Cambridge, University Press, 1927.

et, bien sûr :

HELLEGOUARCH (Y.). - Courbes elliptiques et équation de Fermat, Thèse Sc. math. Univ. Besançon, 1972.

(Texte reçu le 3 février 1975)

Marie-Claude SARMANT
36 rue des Plantes
75014 PARIS