Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Daniel Christy

Courbes elliptiques dans les corps de nombres

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 2 (1972-1973), exp. n° G14, p. G1-G4

<http://www.numdam.org/item?id=SDPP_1972-1973__14_2_A20_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théories des nombres)
14e année, 1972/73, n° G14, 4 p.

12 mars 1973

COURBES ELLIPTIQUES DANS LES CORPS DE NOMBRES

par Daniel CHRISTY

Introduction.

Soient K un corps de nombres, et $(\mathcal{C})$ une courbe de genre 1 définie sur K. Si $(\mathcal{C})$ admet un point rationnel sur K, POINCARÉ et NAGELL ont montré que $(\mathcal{C})$ est birationnellement équivalente à une cubique d'équation

$$y^2 = x^3 + Mx + N ,$$

où $M , N \in K$ et $4M^3 - 27N^2 \neq 0$.

L'ensemble des points de $(\mathcal{C})$, rationnels sur K, peut être muni d'une structure de groupe abélien $\mathcal{C}(K)$.

Le "gros" théorème sur $\mathcal{C}(K)$ est le théorème de Mordell-Weil :

$\mathcal{C}(K)$ est un groupe de type fini .

Pour une démonstration de ce théorème, voir le livre de LANG [9] et l'exposé de Francine DELMER [4]. On en déduit que $\mathcal{C}(K)$ est somme directe d'un groupe fini T (dit groupe de torsion de la courbe) et d'un groupe libre $\underset{\sim}{Z}^r$, r est appelé rang de la courbe.

1. La loi de groupe de $\mathcal{C}(K)$.

Dans ce paragraphe, nous rappelons rapidement comment est définie la loi de groupe de $\mathcal{C}(K)$:

La courbe $(\mathcal{C})$ admet la paramétrisation

$$x = \wp(u) , \quad y = \frac{1}{2} \wp'(u) ,$$

où $\wp$ est la fonction de Weierstrass correspondant au réseau Γ de $\underset{\sim}{\mathcal{C}}$, déterminée par les invariants y_2 et y_3 qui se calculent en fonction de M et N.

Si P_1 et P_2 sont des points de $(\mathcal{C})$ correspondant aux arguments u_1 et u_2 (mod Γ), alors $P_1 + P_2$ (resp. $2P_1$) est le point d'argument $u_1 + u_2$ (resp. $2u_1$) (mod Γ). L'élément neutre de $\mathcal{C}(K)$ est le point à l'infini de la courbe $\mathcal{C}$.

Géométriquement, le point $P_1 + P_2$ (resp. $2P_1$) est le symétrique par rapport à l'axe $x'x$ du troisième point d'intersection de la droite $P_1 P_2$ (resp. de la tangente en P_1 à $(\mathcal{C})$ avec la courbe $(\mathcal{C})$).

On a $P_1 + P_2 + P_3 = 0$ si, et seulement si, les trois points P_1 , P_2 , P_3 sont alignés.

2. Quelques résultats sur le groupe de torsion.

Pour connaître $\mathcal{C}(K)$, il faut donc déterminer T et r . Les principaux résultats sur T sont les suivants :

(a) Points d'ordre 2 . - Ce sont les points P tels que $P + P = 0$, autrement dit tels que la tangente en P soit verticale. On obtient ainsi les points d'intersection de $(\mathcal{C})$ avec l'axe $x'x$.

Si $X^3 + MX + N = 0$ n'a pas de racine dans K , $\mathcal{C}(K)$ ne contient pas de points d'ordre 2 . Si $X^3 + MX + N = 0$ a une (resp. 3) racines dans K , $\mathcal{C}(K)$ contient alors un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (resp. $\mathfrak{K}_0$ groupe de Klein).

Remarque. - Dans la littérature, on appelle point trivial sur la courbe $(\mathcal{C})$ tout point défini sur K d'ordre 2 .

(b) Points d'ordre n . - Un résultat étonnant et récent, dû à DEM'JANENKO [5] (1971) montre qu'il existe une constante ν telle qu'aucune courbe de genre 1 , définie sur $\mathbb{Q}$, n'admette de points rationnels d'ordre $> \nu$. La valeur de ν n'est pas connue. Il existe des cubiques possédant des points rationnels d'ordre 10 , 12 :

$$n = 10 , \qquad 9y^2 = 8x^3 + 25x^2 - 64x .$$

$$n = 12 , \qquad y^2 = x^3 - 122x^2 + 9^3.7^2\, x .$$

Le cas $n = 13$ n'est pas encore élucidé. Sur cette question, consulter OGG [11], Tena AYUSO [1].

Un résultat plus ancien (voir HELLEGOUARCH [6]-[8]) est le théorème suivant :

T est soit cyclique, soit produit d'un groupe cyclique et d'un cycle d'ordre 2 .

Dans sa thèse, HELLEGOUARCH s'est intéressé aux points rationnels d'ordre $2p^h$, où p est un entier premier impair en connexion avec l'équation de Maillet

$$x^{p^h} + y^{p^h} = cz^{p^h} . \qquad ([6]\text{-}[8]).$$

3. Extensions du corps.

Nous nous plaçons maintenant dans les hypothèses suivantes : Soient K un corps de nombres, et $\mathcal{C}(K)$ le groupe des points de la cubique $(\mathcal{C})$ rationnels sur K . Supposons que $\mathcal{C}(K) \subset \mathfrak{K}$ (autrement dit, $(\mathcal{C})$ n'admet sur K que des points triviaux). Un problème se pose alors : Comment se comporte $\mathcal{C}(L)$, où L est une extension de degré fini de K , galoisienne, de groupe de Galois $\mathcal{G}(L/K)$. On ne connaît pas la réponse à ce problème actuellement.

Si $\mathcal{G}(L/K)$ est cyclique, engendré par σ , de degré n , si $P \in \mathcal{C}(L)$,

$$\sigma P , \ldots , \sigma^{n-1} P$$

sont dans $\mathcal{C}(L)$. Soit $\mathfrak{N}$ l'application $\mathcal{C}(L) \longrightarrow \mathcal{C}(K)$, définie par

$$\mathfrak{N}(P) = P + \sigma P + \ldots + \sigma^{n-1} P .$$

Si $P \in \mathcal{C}(L)$, $\mathfrak{N}(P) \in \mathcal{C}(K)$. Donc, par l'hypothèse faite sur $\mathcal{C}(K)$, $\mathfrak{N}(P) \in \mathcal{K}$, et par conséquent

$$\mathfrak{N}(2P) = 0 .$$

THÉORÈME. - Si $\mathcal{C}(K) \subset \mathcal{K}$, alors, $\forall\, P \in \mathcal{C}(L)$, où L est une extension galoisienne finie cyclique de degré n , on a

$$\mathfrak{N}(2P) = 0 .$$

Ce théorème donne des résultats intéressants dans le cas des corps quadratiques.

Si $K \longrightarrow L$ est une extension quadratique, si $\mathcal{C}$ admet un point d'ordre 2 dans K , et si $\mathcal{C}(K) \subset \mathcal{K}$, alors $\mathcal{C}(L)$ n'est pas réduit à $\mathcal{K}$ si, et seulement si, $\mathcal{C}_1(K)$ n'est pas réduit à $\mathcal{K}$, où $\mathcal{C}_1$ est la cubique.

$(\mathcal{C}_1)$ $$^2 = x(d^2 x^2 - 6\rho dx - 3\rho^2 - 4M)$$

où $d \in K$ et $L = K(\sqrt{d})$, et où ρ est racine dans K de $X^3 + MX + N = 0$.

En particulier, si $\mathcal{C}_2$ est la courbe $y^2 = x(x^2 + 1)$,

$$\mathcal{C}_2(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \subset \mathcal{K} .$$

Alors $\mathcal{C}_2(\mathbb{Q}(\sqrt{d})) \subset \mathcal{K} \Longleftrightarrow d$ n'est pas tel que $dr^2 = 2pq(p^2 - q^2)$, où p , $q \in \mathbb{Z}$, $(p , q) = 1$, $p \not\equiv q \mod 2$, $r \in \mathbb{Z}$.

De même, si $\mathcal{C}_3$ est la courbe $y^2 = x(x^2 - 1)$,

$$\mathcal{C}_2(\mathbb{Q}) \simeq \mathcal{K} .$$

Alors $\mathcal{C}_2(\mathbb{Q}(\sqrt{d})) \subset \mathcal{K} \Longleftrightarrow d$ n'est pas tel que l'une des deux conditions suivantes est réalisée.

(1) $dr^2 = p^4 - q^4$, où p , $q \in \mathbb{Z}$, $(p , q) = 1$, $p \not\equiv q \mod 2$ ou

$$p \equiv q \equiv 1 \mod 2 .$$

(2) $dr^2 = \pm (p^2 - q^2)(2p^2 - q^2)$, où p , $q \in \mathbb{Z}$, $(p , q) = 1$, $q \equiv 1 \mod 2$ ou $q \equiv 0 \mod 2$ $p \not\equiv q \mod 2$.

Par une méthode analogue [2], on peut montrer que l'équation de Fermat de degré 4, $x^4 + y^4 = z^4$ est régulière (c'est-à-dire n'admet que les points triviaux) dans tous les corps quadratiques sauf $\mathbb{Q}(\sqrt{-7})$, où l'on a

$$\left(\frac{1 + \sqrt{-7}}{2}\right)^4 + \left(\frac{1 - \sqrt{-7}}{2}\right)^4 = 1 .$$

BIBLIOGRAPHIE

[1] AYUSO (Tena). - Sur l'existence d'un point rationnel d'ordre n sur une courbe elliptique, Séminaire d'Arithmétique, Grenoble 1971/72, p. 20-27.

[2] CHRISTY (Daniel). - L'équation $x^4 + y^4 = z^4$ dans le corps des nombres, C. R. Acad. sc. Paris, t. 274, 1972, Série A, p. 1193-1196.

[3] CHRISTY (Daniel). - Courbes de genre 1 dans les corps quadratiques, C. R. Acad. Sc. Paris (à paraître).

[4] DELMER (Francine). - Equations diophantiennes et géométrie des courbes, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 10e année, 1968/69, n° 19, 15 p.

[5] DEM'JANENKO (V. A.). - Sur la torsion des courbes elliptiques [en russe], Izv. Akad. Nauk SSSR, serija Mat., t. 35, 1971, p. 280-307.

[6] HELLEGOUARCH (Yves). - 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.

[7] HELLEGOUARCH (Yves). - 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.

[8] HELLEGOUARCH (Yves). - Courbes elliptiques et équation de Fermat, Thèse Sc. math. Besançon 1972.

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

[10] LIND (C. E.). - Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom geschlecht Eins, Dissertation, Uppsala 1940.

[11] OGG (A. P.). - Rational points of finite order on elliptic curves, Inventiones math., t. 12, 1971, p. 105-111.

(Texte reçu le 15 mai 1973)

Daniel CHRISTY
45 allée des Troënes
14760 BRETTEVILLE SUR ODON