Séminaire Delange-Pisot-Poitou. Théorie des nombres

Francine Delmer

Équations diophantiennes et géométrie des courbes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 10, n° 2 (1968-1969), exp. n° 19, p. 1-16

<http://www.numdam.org/item?id=SDPP_1968-1969__10_2_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
10e année, 1968/69, n° 19

2 juin 1969

ÉQUATIONS DIOPHANTIENNES ET GÉOMÉTRIE DES COURBES

par Francine DELMER

Introduction.

Cet exposé relatif aux équations diophantiennes, c'est-à-dire aux solutions d'équations en nombres entiers ou rationnels, d'un type particulier (on étudie les équations : (E) $y^2 = x^3 + ax^2 + bx + c$), est centré sur le théorème de Mordell (1921), et a pour but de présenter les généralisations de ce théorème, ainsi que de poser quelques problèmes qui en découlent.

Le paragraphe 1 introduit la réduction des cubiques non singulières à la forme de Weierstrass (E), et en donne une représentation dans C .

De la même manière que dans le cas complexe, on montre que l'ensemble des solutions rationnelles de (E) peut être muni d'une structure de groupe abélien (sous-groupe du groupe obtenu dans le cas complexe). Ce groupe est de rang fini, c'est le théorème de Mordell, la démonstration constitue le paragraphe 2.

Le paragraphe 3 est consacré aux extensions du théorème de Mordell, dans le cas où on remplace Q par un corps de nombres algébriques (théorème de Weil) ou par un corps de fonctions (théorème de Lang-Néron), ainsi qu'aux conjectures sur le rang du groupe obtenu.

Enfin, on s'attachera dans le paragraphe 4, à l'étude des points entiers (résultats de SIEGEL) et des points exceptionnels (résultats de NAGELL et de Mlle LUTZ).

1. Généralités.

Un problème diophantien est un problème qui peut se ramener à la recherche des systèmes d'entiers x , y , z , ... qui vérifient une ou plusieurs relations à coefficients entiers ou rationnels.

FERMAT utilise dans ses démonstrations, un procédé, dit de descente infinie (d'une solution en nombres entiers d'une équation, on déduit une solution en entiers strictement inférieurs), et un exemple classique en est l'équation $x^4 + y^4 = z^4$. POINCARÉ, vers 1900, revient aux méthodes de FERMAT. Il remarque que l'on n'utilise que des transformations rationnelles à coefficients rationnels, ce qui l'amène à les étudier plus systématiquement, et en particulier il ramène le problème de la recherche des points entiers sur la cubique $z^2 = x(x^2 + 1)$ au problème de Fermat $(x^4 + y^4 = z^2)$.

Le problème de la recherche des solutions rationnelles d'équations de la forme $f(x , y) \in \mathbb{Q}[x , y]$, f du second degré en x et y , est facile à résoudre complètement.

La question la plus simple, que l'on peut ensuite se poser, concerne les points rationnels sur des cubiques dans le plan.

MORDELL montre que l'ensemble des points d'une cubique non singulière peut être muni d'une structure de groupe abélien, et que l'ensemble des points rationnels en est un sous-groupe de rang fini.

Loi de groupe. - Etant donnée une cubique :

$$(\gamma) \qquad ax^3 + bx^2 y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + ky + 1 = 0 \ ,$$

on considère deux points P et Q sur γ , à coordonnées rationnelles (s'il en existe) ; ils déterminent une droite à coefficients rationnels dont la troisième intersection avec γ sera un point rationnel R . La loi de composition qui, à (P , Q) fait correspondre R , n'est pas associative ; on suppose alors que γ possède un autre point rationnel O , on joint O et R , et $OR \cap \gamma$ sera appelé $P + Q$.

En effet, on vérifie que cette loi de composition $(P , Q) \to P + Q$ est une loi de groupe abélien, définie sur tous les points de γ , qui est stable sur l'ensemble des points rationnels.

Elément neutre : O .

Inverse : Soient OS la tangente en O à γ , S son point d'intersection avec γ , $(- P)$ est le troisième point d'intersection de PS avec γ .

Points $(P + P)$: Soient PT la tangente en P à γ , T son point d'intersection avec γ , OT recoupe γ en un point qui est $(P + P)$.

On suppose toujours que les tangentes aux points considérés de γ existent, car on n'étudiera que le cas des cubiques non singulières, le problème de la recherche des points rationnels sur les cubiques singulières se ramenant à celui sur les coniques.

Réduction. - Il est cependant préférable d'avoir une représentation de la cubique la plus simple possible, et l'on a à ce sujet un résultat important :

Toute cubique est $\mathbb{Q}$-birationnellement équivalente à une cubique mise sous la forme de Weierstrass :

(E') $$y^2 = 4x^3 - g_2 x - g_3 \ ,$$

ou encore

(E) $$y^2 = x^3 + ax^2 + bx + c = f(x) \ , \qquad a \ , \ b \ , \ c \in Q \ .$$

On dit que γ et (E') sont Q-birationnellement équivalentes, car on peut passer de l'équation de γ à celle de (E') par des transformations rationnelles à coefficients rationnels et réciproquement.

Le résultat essentiel est que les points rationnels de γ et (E') sont en bijection.

On passe de (E') à (E) en multipliant x et y par des entiers convenables.

La courbe (E) , dans des axes orthonormés, présente une symétrie par rapport à Ox , et suivant la réalité des racines de $f(x)$, elle est en un ou deux morceaux ; d'autre part elle a un point à l'infini dans la direction de Oy qui est un point d'inflexion.

On définit de même que précédemment la loi de groupe sur (E) , en choisissant le point à l'infini de la courbe comme point 0 .

Soient $P_1 = (x_1 , y_1)$ et $P_2 = (x_2 , y_2)$ deux points sur (E) . On pose $P_3 = P_1 P_2 \cap (E)$, $P_3 = (x_3 , y_3)$, alors $P_1 + P_2 = (x_3 , - y_3)$, et l'on a les formules :

$$x_3 = \lambda^2 - a - x_2 - x_1 \ ,$$

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \ , \qquad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2 \ .$$

$$y_3 = \lambda x_3 + \nu \ ,$$

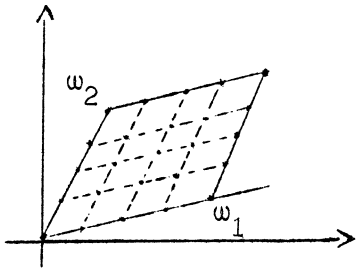
Pour trouver les coordonnées de $(P + P)$, on applique les formules précédentes avec $\lambda = \frac{f'(x)}{2y}$.

On remarque aussi que les points d'ordre 2 , $(2P = 0)$, sont les points d'intersection de la courbe avec l'axe Ox , sans oublier le point à l'infini ; ils forment un sous-groupe d'ordre 4 , isomorphe au groupe de Klein.

Représentation dans le plan complexe. - On considère le groupe $\Gamma_{complex}$, constitué par les points complexes de (E') , avec la loi définie précédemment. La théorie des fonctions elliptiques nous permet de trouver une représentation de $\Gamma_{complex}$ dans le plan complexe.

Si $4x^3 - g_2 x - g_3$ a des racines distinctes, il existe ω_1 , ω_2 , appelés périodes, dans le plan complexe, et une fonction $\mathfrak{P}(z)$, qui admet ω_1 , ω_2 comme périodes, et qui satisfait à l'équation différentielle

$$(\mathfrak{P}')^2 = 4\mathfrak{P}^3 - g_2 \mathfrak{P} - g_3 \ .$$



A tout z , on fait correspondre le point

$$P(z) = (\mathfrak{P}(z) \ , \ \mathfrak{P}'(z))$$

sur (E') . Cette application a des propriétés importantes. Elle est surjective et, à l'addition des nombres complexes, elle fait correspondre l'addition des points sur la courbe.

$$P(z_1 + z_2) = P(z_1) + P(z_2) \ .$$

Le noyau de cet homomorphisme est le réseau $K = \{m_1 \omega_1 + m_2 \omega_2 \mid m_1 , m_2 \in Z\}$. On a donc $\underset{\sim}{C}/K \simeq \Gamma_{complex}$, c'est un tore.

Cette représentation permet de mettre en évidence les éléments de torsion du groupe. Dans le parallélogramme de période, on cherche les points z tels que $mz \in K$; ce sont les éléments de torsion d'ordre m , il leur correspond les points d'ordre m .

Ils forment un groupe d'ordre m^2 , produit direct de deux groupes cycliques d'ordre m .

Remarque. - On va voir les idées de la démonstration de MORDELL, en utilisant l'équation réduite (E) , et en y supposant de plus a , b , c , entiers ; en effet il suffit de multiplier le tout par α^6 , et de changer les coefficients $A = \alpha^2 a$, $B = \alpha^4 b$, $C = \alpha^6 c$, et $Y = \alpha^3 y$, $X = \alpha^2 x$.

2. Théorème de Mordell.

Le groupe Γ_{rat} des points définis sur une cubique non singulière, à coordonnées rationnelles, est de rang fini ([7]).

La notion fondamentale de ce paragraphe est celle de hauteur. Soit $x = \frac{m}{n}$ un nombre rationnel, $(m , n) = 1$; on appelle hauteur de x , et on la note $H(x)$, le sup de $|m|$ et $|n|$.

Remarque. - L'ensemble des nombres rationnels, dont la hauteur est bornée par M fixé, est un ensemble fini.

Soit $P \in \Gamma_{rat}$; on définit alors la hauteur de $P(x , y)$ de la manière suivante: $H(P) = H(x)$ si $P \neq 0$ et $H(0) = 1$.

Les propriétés principales de la hauteur sont les suivantes :

LEMME 1. - Un ensemble de points de hauteur bornée est fini.

En effet, soit M la borne, il y a un nombre fini de coordonnées x telles que $H(x) \leqslant M$ (remarque), et pour chaque x il y a au plus deux y .

LEMME 2.

(i) $\forall\, P_0 \in \Gamma_{rat}$, il existe C_0 tel que $H(P + P_0) \leqslant C_0\, H(P)^2$, $\forall\, P \in \Gamma_{rat}$.

(ii) Il existe $C > 0$ tel que $H(P)^4 \leqslant CH(2P)$, $\forall\, P \in \Gamma_{rat}$.

D'autre part, on considère 2Γ , sous-groupe de Γ , formé des points de la forme $P + P$, $P \in \Gamma$, et on démontre le résultat suivant, encore appelé théorème de Mordell faible.

THÉORÈME. - L'indice de 2Γ dans Γ est fini.

On peut montrer ce théorème simplement dans le cas où Γ possède un point d'ordre 2 rationnel ; c'est un point dont l'abscisse est une racine de $f(x) = 0$, et c'est donc un entier, car $f(x)$ a pour coefficient directeur 1 .

Soit $E(x_0 , 0)$ ce point, on fait une translation d'axes qui amène l'origine en E , la nouvelle équation de la cubique est encore à coefficients entiers et s'écrit

$$y^2 = x^3 + ax^2 + bx = f(x) \quad .$$

Le discriminant de $f(x)$ est $D = b^2(a^2 - 4b)$; comme il n'est jamais nul, on a $b \neq 0$ et $a^2 - 4b \neq 0$.

Dans la translation, le groupe Γ est inchangé ; on se place pour cette démonstration toujours dans les nouveaux axes.

On étudie l'application $\Gamma \longrightarrow 2\Gamma$. La fonction rationnelle, qui donne l'abscisse de $2P$ en fonction de celle de P , est de degré 4 ; on va décomposer l'application, qui à P fait correspondre $2P$, en deux applications de degré 2 .

L'idée de cette décomposition vient de la représentation complexe de la courbe.

On considère la représentation complexe des points complexes de la courbe par les points d'un parallélogramme de côtés ω_1 , ω_2 , pour des périodes convenablement choisies. E est donc représenté par $\frac{\omega_1}{2}$. On considère alors le parallélogramme

$\overline{\omega_1}$, $\overline{\omega_2}$, avec $\overline{\omega_1} = \frac{1}{2}\omega_1$, et $\overline{\omega_2} = \omega_2$. Il lui correspond une courbe $\overline{\Gamma}$, et une application naturelle φ de Γ dans $\overline{\Gamma}$.

Si on recommence cette opération pour ω_2 , on obtient un nouveau parallélogramme $\overline{\overline{\omega_1}}$, $\overline{\overline{\omega_2}}$, et une nouvelle courbe $\overline{\overline{\Gamma}}$, les fonctions elliptiques de périodes ω_1 , ω_2 , et $\overline{\overline{\omega_1}}$, $\overline{\overline{\omega_2}}$, sont essentiellement les mêmes, et $\overline{\overline{\Gamma}} \simeq \Gamma$.

φ est un homomorphisme de noyau $\{0 , E\}$, et si on appelle ψ la seconde application, $(\psi : \overline{\Gamma} \to \overline{\overline{\Gamma}})$, l'application composée $\psi\varphi$ est un homomorphisme de Γ dans $\overline{\overline{\Gamma}}$, et on a $\psi\varphi\Gamma = 2\Gamma$.

Ces résultats sont des propriétés connues des courbes elliptiques que l'on peut d'autre part retrouver par des calculs élémentaires ; avec les équations suivantes:

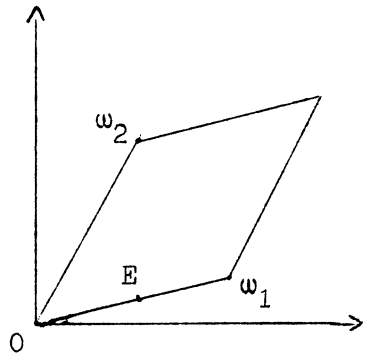
$$\overline{\Gamma} : \quad y^2 = x^3 + \bar{a}x^2 + \bar{b}x , \qquad \bar{a} = -2a , \quad \bar{b} = a^2 - 4b ,$$

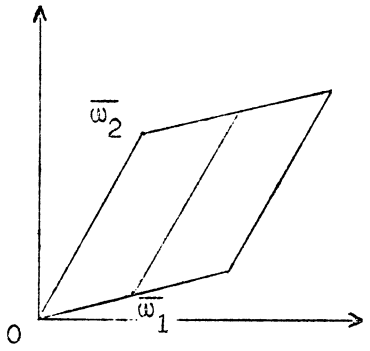
$$\overline{\overline{\Gamma}} : \quad y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x , \qquad \bar{\bar{a}} = 4a , \quad \bar{\bar{b}} = 16b .$$

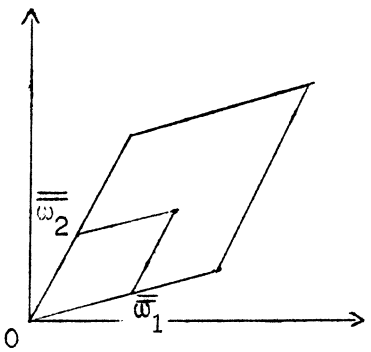
Si on pose $Y = 8y$ et $X = 4x$, on obtient l'équation de Γ en Y et X à partir de celle de $\overline{\overline{\Gamma}}$. Le groupe des points rationnels de $\overline{\overline{\Gamma}}$ est isomorphe au groupe des points rationnels de Γ .

On définit l'application φ qui sera un homomorphisme de groupe, qui à Γ_{rat} fait correspondre $\overline{\Gamma}_{rat}$, par les formules :

$$\bar{x} = x + a + \frac{b}{x} = \frac{y^2}{x^2} , \qquad \bar{y} = y\,\frac{x^2 - b}{x^2} , \qquad \varphi(0) = \bar{0} , \qquad \varphi(E) = \bar{0} .$$







On vérifie que φ est un homomorphisme de groupe, qui à un point rationnel de Γ fait correspondre un point rationnel de $\overline{\Gamma}$.

On appelle im φ , la restriction de φ à Γ_{rat} , et on cherche à quelle condition un point de $\overline{\Gamma}_{rat}$ provient d'un point de Γ_{rat} par φ .

Des calculs simples donnent le résultat suivant :

Si $\bar{x} \neq 0$, $(\bar{x} , \bar{y}) \in \text{im } \varphi \iff \bar{x}$ est carré d'un rationnel ;
Si $\bar{x} = 0$, c'est le cas de $\bar{0}$ et $\bar{E}$, il est clair que $\bar{0} \in \text{im } \varphi$ et

$$(\bar{E} \in \text{im } \varphi) \iff (\bar{b} = a^2 - 4b \text{ est un carré parfait}) .$$

On s'intéresse désormais à Γ_{rat} et $\bar{\Gamma}_{rat}$, que l'on note plus simplement $\Gamma , \bar{\Gamma}$. On a donc deux applications $\varphi : \Gamma \to \bar{\Gamma}$ et $\psi : \bar{\Gamma} \to \Gamma$, telles que

$$\psi\varphi P = \pm 2P , \qquad \forall P \in \Gamma ,$$

et on va montrer que

$$[\bar{\Gamma} : \varphi\Gamma] \leqslant 2^{s+1} ,$$

où s est le nombre de facteurs premiers distincts de $\bar{b}$,

$$[\Gamma : \psi\bar{\Gamma}] \leqslant 2^{r+1} ,$$

où r est le nombre de facteurs premiers distincts de b .

Il suffit de montrer la seconde inégalité ; on appelle α l'application de Γ dans $\underset{\sim}{Q}^*/\underset{\sim}{Q}^{*2}$ définie par

$$\alpha(0) \equiv 1 \quad [\underset{\sim}{Q}^{*2}] ,$$

$$\alpha(E) \equiv b \quad [\underset{\sim}{Q}^{*2}] ,$$

$$\alpha(x , y) \equiv x \quad [\underset{\sim}{Q}^{*2}] , \qquad x \neq 0 .$$

$\psi\bar{\Gamma} = \{(x , y) \in \Gamma , \ x \neq 0 , \ x \text{ carré d'un rationnel}\} \cup \{0\} \cup \{E \text{ si } b \text{ est carré}\}$.

On vérifie que α est un homomorphisme, et il est clair que

$$\ker \alpha = \text{im } \psi = \psi\bar{\Gamma} .$$

Il suffit de regarder quels sont les rationnels que l'on peut obtenir comme abscisse de points de Γ .

On montre que l'on peut écrire $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $(m , e) = (n , e) = 1$. En portant ces valeurs dans l'équation de la courbe :

$$n^2 = m^3 + am^2 e^2 + bme^4 = m(m^2 + ame^2 + be^4) .$$

Si m et $m^2 + ame^2 + be^4$ sont premiers entre eux, chacun d'eux est égal plus ou moins un carré, on a donc

$$x = \frac{m}{e^2} = \pm 1 \quad [\underset{\sim}{Q}^{*2}] .$$

Dans le cas général, si $d = (m , m^2 + ame^2 + be^4)$, $d|be^4$, mais $(m , e) = 1$ entraîne $d|b$, donc si $m = \prod p^{a_p}$ est la décomposition de m en facteurs premiers, a_p est pair si p ne divise pas b , on a donc

$$m = \text{carré} \times (\pm\, p_1^{\varepsilon_1} , \dots , p_r^{\varepsilon_r}) ,$$

$$\varepsilon_i = 0 \quad \text{ou} \quad 1 , \qquad \text{et} \quad p_1 \dots p_r \quad \text{diviseurs de} \quad b .$$

Donc le nombre total de possibilités modulo des carrés est 2^{r+1} .

La démonstration du théorème est alors claire :

$$\Gamma/\psi\overline{\Gamma} = \Gamma/\mathrm{Ker}\ \alpha \simeq \alpha\Gamma ,$$

$$[\Gamma : \psi\overline{\Gamma}] \leqslant 2^{r+1} , \qquad [\overline{\Gamma} : \varphi\Gamma] \leqslant 2^{s+1} ,$$

$$[\Gamma : 2\Gamma] = [\Gamma : \psi\varphi\Gamma] \leqslant 2^{r+s+2} .$$

Les deux lemmes et le théorème, joints à une technique de descente, impliquent le résultat suivant :

<u>Soit</u> Q_i <u>un système de représentants des classes de</u> Γ <u>modulo</u> 2Γ , <u>alors il existe un entier</u> m <u>et un nombre</u> M <u>tels que</u>, $\forall\ P \in \Gamma$,

$$P = a_1 Q_{i_1} + a_2 Q_{i_2} + \dots + a_m Q_{i_m} + a_{m+1} Q , \qquad \underline{\text{avec}} \quad H(Q) \leqslant M .$$

Ceci entraîne que $\{Q_i\} \cup \{Q \mid H(Q) \leqslant M\}$ est un système de générateurs de Γ , on a vu d'autre part que c'est un ensemble fini, c'est le théorème de Mordell.

On montre simplement l'existence de m et M . En effet, si $\{Q_i\}_{i \in (1,n)}$ est le système considéré, $\forall\ P \in \Gamma$, $\exists\ i_1$ dépendant de P tel que $P - Q_{i_1} = 2P_1$, de même $\exists\ i_2$ tel que

$$P_1 - Q_{i_2} = 2P_2$$

$$\vdots$$

$$P_{m-1} - Q_{i_m} = 2P_m ,$$

avec $(Q_{i_1} , \dots , Q_{i_m}) \in \{Q_i\}_{i \in (1,n)}$ et $(P_1 , \dots , P_m) \in \Gamma$, alors

$$P = Q_{i_1} + 2Q_{i_2} + \dots + 2^{m-1} Q_{i_m} + 2^m P_m .$$

L'idée de la démonstration est que, pour un certain m , P_m a une hauteur bornée.

Le lemme 1, appliqué à $(- Q_i)$, donne :

$$\exists\ C_i \text{ tel que } H(P - Q_i) \leqslant C_i\, H(P)^2 , \qquad \forall\ P \in \Gamma\ .$$

Il n'y a qu'un nombre fini de i , on appelle donc C' le plus grand des C_i ,

$$H(P - Q_i) \leqslant C'H(P)^2 , \qquad \forall\ P \in \Gamma , \quad i \in (1 , n)\ .$$

Le lemme 2 donne l'inégalité suivante :

$$H(P_m)^4 \leqslant CH(2P_m) = CH(P_{m-1} - Q_{i_m}) \leqslant CC'H(P_{m-1})^2 ,$$

ou encore

$$H(P_m)^4 \leqslant \frac{16CC'}{H(P_{m-1})^2} \left(\frac{H(P_{m-1})}{2}\right)^4 ,$$

$$H(P_m) \leqslant 4\sqrt{\frac{16CC'}{H(P_{m-1})^2}}\ \frac{H(P_{m-1})}{2}\ .$$

Si $H(P_{m-1})^2 > 16CC'$, alors $H(P_m) < \frac{1}{2} H(P_{m-1})$; ceci est impossible, car si la suite de points P_1 , P_2 , ... vérifiait cette relation indéfiniment, on arriverait à une hauteur inférieure à 1 . On en déduit que

$$H(P_{m-1})^2 \leqslant 16CC'\ .$$

Il en résulte que les Q tels que $H(Q) < 4\sqrt{CC'}$ et les $\{Q_i\}_{i \in (1,n)}$ constituent un système de générateurs fini de Γ .

3. Généralisations.

En 1928, WEIL a montré que l'on pouvait généraliser le théorème de Mordell au cas des corps de nombres et des variétés abéliennes de dimension 1 , et plus généralement de dimension n ([12]).

Le schéma de la démonstration est le même que celui indiqué dans le paragraphe précédent.

On introduit la notion de hauteur de la façon suivante :

Etant donné K , corps de nombres algébriques, on définit $H(a)$ par

$$H(a) = \prod_v \sup(|a|_v , 1) \quad ,$$

où $|\ |_v$ désigne l'ensemble des valuations de K , y compris les valuations archimédiennes, vérifiant la formule du produit.

On remarque que, dans le cas $K = Q$, la définition coïncide avec celle donnée précédemment :

$$H(\tfrac{m}{n}) = \prod_v \sup(|\tfrac{m}{n}|_v , 1) , \qquad m , n \in Z , \quad (m , n) = 1 .$$

$|\ |_v$ sont les valuations p-adiques, et $|\ |$ la valuation archimédienne. Soit $n = \prod_i p_i^{a_i}$ la décomposition de n en facteurs premiers :

Si $|m| > |n|$, $|\frac{m}{n}| = \frac{|m|}{|n|}$ et $H(\frac{m}{n}) = |m|$;

Si $|n| > |m|$, $\sup(|\frac{m}{n}| , 1) = 1$ et $H(\frac{m}{n}) = |n|$.

C'est bien la définition du paragraphe 2.

On a alors les deux lemmes suivants :

LEMME 1. - M <u>étant donné, il n'y a qu'un nombre fini de</u> a <u>tels que</u> $H(a) \leqslant M$.

LEMME 2. - <u>Pour</u> $m > 1$ <u>et</u> $P \in \Gamma$, <u>il existe</u> $\alpha > 0$ <u>et</u> β <u>tels que</u>

$$H(mP' - P) > \frac{1}{\beta} [H(P')]^{(1+\alpha)} , \qquad \forall\ P' \in \Gamma .$$

On démontre d'autre part le théorème faible de Mordell. Pour $m \geqslant 2$, $[\Gamma : m\Gamma]$ est fini. Le principe de la démonstration est alors identiquement le même.

Une autre généralisation a été donnée par LANG et NÉRON (1959) du théorème de Mordell, dans le cas des corps de fonctions. On introduit le groupe des diviseurs sur une variété abélienne de dimension 1 , définie sur un corps parfait K . On montre qu'il admet un système fini de générateurs. On a encore la possibilité de réduction, par équivalences birationnelles. Si K est de caractéristique différente de 2 ou 3 , et si C est une variété abélienne définie sur K , possédant un point O défini sur K , elle est birationnellement équivalente à la cubique plane $Y^2 = X^3 + AX + B$. On utilise, pour démontrer ce résultat, le théorème de Riemann-Roch ([5]).

Dans beaucoup de cas étudiés, le rang de C , pour $K = Q$, est petit : 0 , 1 , 2 ; on a conjecturé que, pour un corps de base donné, le rang serait borné. Pourtant, il parait assez probable que le contraire soit vrai, car si les équations sont

données avec de grands coefficients, le rang sera plus grand. NÉRON a d'ailleurs montré l'existence de variétés abéliennes de dimension 1 sur Q dont le rang est au moins 10 ([9]).

4. Points exceptionnels.

On appelle points exceptionnels, les points qui correspondent aux éléments de torsion du groupe. On a vu que les points exceptionnels d'ordre m forment un sous-groupe de $\Gamma_{complex}$ d'ordre m^2, isomorphe au produit de groupes cycliques d'ordre m.

On va démontrer le résultat dû à NAGELL, sur les points exceptionnels rationnels (1935), sur la courbe (E) ([8]).

THÉORÈME. - Les points rationnels d'ordre fini sont à coordonnées entières, et si y est l'ordonnée, on a, ou bien $y = 0$ (c'est le cas des points d'ordre 2), ou bien y divise D, où D est le discriminant de $f(x) = x^3 + ax^2 + bx + c$.

Ce résultat est très intéressant, car on peut en déduire deux choses :

- L'ensemble des points rationnels exceptionnels est fini ;
- On peut, au bout d'un nombre fini d'étapes, les obtenir tous.

En effet, y divise D qui est un nombre entier connu ; on décompose D en produit de facteurs premiers, on a donc tous ses diviseurs. D'autre part, $f(x)$ a pour coefficient directeur 1, donc tout nombre entier qui divise D et qui vérifie $y^2 = f(x)$ doit diviser le terme constant de $f(x)$. On a donc un nombre fini d'essais à faire, pour obtenir les points entiers d'ordre fini.

Démonstration.

On suppose tout d'abord que l'on a montré la première partie du théorème.

Dans $Z[x]$, comme $f(x)$ a un coefficient directeur égal à 1, le discriminant est dans l'idéal de $Z[x]$ engendré par $f(x)$ et $f'(x)$, on a donc

$$D = r(x)\, f(x) + s(x)\, f'(x) \quad ,$$

où $r(x)$ et $s(x)$ sont des polynômes à coefficients entiers.

Soit $P = (x , y)$ un point d'ordre fini.

Si $y = 0$, il est d'ordre 2, et c'est une condition nécessaire et suffisante.
Si $y \neq 0$, $2P$ est aussi d'ordre fini, et $2P \neq 0$.

On a $2P = (X , Y)$, avec X et Y donnés par

$$2x + X = \lambda^2 - a , \qquad \lambda = \frac{f'(x)}{2y} .$$

x , X , a , sont des entiers, donc λ est entier, et comme $2y$ et $f'(x)$ sont entiers, on obtient $2y | f'(x)$, soit $y | f'(x)$, mais $y^2 = f(x)$, donc y divise $f(x)$ et $f'(x)$, y divise donc D .

On va montrer maintenant que tout point exceptionnel rationnel est à coordonnées entières.

L'idée vient de la remarque suivante : si aucun nombre premier ne divise un nombre entier, cet entier est égal à 1 ; il en résulte que si $\frac{m}{n} \in Q$ avec $(m , n) = 1$, il est entier si aucun nombre entier ne divise le dénominateur n .

- On montre tout d'abord que si x est entier, y l'est, et réciproquement.

Tout rationnel non nul peut s'écrire $r = \frac{m}{n} p^{\nu}$, $m > 0$,

$$(m , n) = (m , p) = (n , p) = 1 \ ;$$

on appelle <u>ordre de</u> r , l'entier ν .

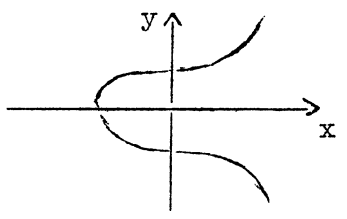
Soit $P = (x , y)$ un point rationnel de Γ , où p divise le dénominateur de x .

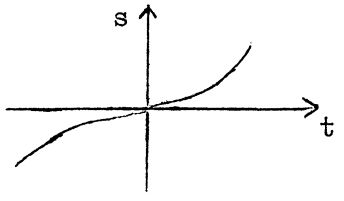
$$x = \frac{m}{np^k} , \qquad y = \frac{d}{ep^{\ell}} , \qquad k > 0 , \quad p \nmid m , n , d , e .$$

Alors on en déduit $2\ell = 3k$. En particulier, $\ell > 0$, et p divise le dénominateur de y . Pour un entier positif q , on a donc $\ell = 3q$, $k = 2q$. Réciproquement, si p divise le dénominateur de y , il divise celui de x , avec les mêmes puissances.

On appelle $\Gamma(p^r)$ l'ensemble des points rationnels de Γ tels que p^{2r} divise le dénominateur de x , et p^{3r} divise le dénominateur de y . Les $\Gamma(p^r)$ sont des sous-groupes de Γ_{rat} , qui dans la topologie p-adique forment des voisinages de 0 , qui correspond au 0 du groupe.

On veut montrer que les points exceptionnels ne peuvent être dans $\Gamma(p)$, et comme $\Gamma_{rat} \supset \Gamma(p) \supset \Gamma(p^2) \supset \ldots \supset \Gamma(p^r) \ldots$, ils seront bien entiers. On change alors de coordonnées, pour ramener le point à l'infini à distance finie, en posant $t = \frac{x}{y}$, $s = \frac{1}{y}$. La courbe se transforme de la manière suivante :





,

et on a une bijection, qui à une droite fait correspondre une droite.

On appelle R le localisé en p de Q, $\mathbb{Z}_{(p)}$, c'est un sous-anneau de Q tel que

$$x \in R \iff \mathrm{ord}(x) \geqslant 0 \ .$$

On a alors

$$(x , y) \in \Gamma(p^r) \iff t \in p^r R \ , \quad s \in p^{3r} R \ .$$

On appelle $t(P)$ la coordonnée de P, $t = \frac{x}{y}$. Si on considère l'application $f : P \to t(P)$, on a

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \quad [p^{3r} R] \ ;$$

f est un homomorphisme de $\Gamma(p^r)$ dans $p^r R / p^{3r} R$, dont le noyau est $\Gamma(p^{3r})$.

- On peut alors montrer le théorème de Nagell, c'est-à-dire que si P est un point rationnel exceptionnel, $P \notin \Gamma(p)$.

Supposons que $P \in \Gamma(p)$. Soit $r > 0$ tel que $P \in \Gamma(p^r)$, $P \notin \Gamma(p^{r+1})$.

Si $p \nmid m$, $t(P_1 + P_2) \equiv t(P_1) + t(P_2) \quad [p^{3r} R]$, alors par récurrence

$$t(mP) = mt(P) \quad [p^{3r} R] \ ,$$

mais $mP = 0$ et $(m , p) = 1$, donc $t(P) \equiv 0 \quad [p^{3r} R]$, c'est en contradiction avec $t(P) \not\equiv 0 \quad [p^{(r+1)} R]$.

Si $p \mid m$, $m = pn$. Soit $P' = nP$. P' est d'ordre p, et si $P \in \Gamma(p)$, $P' \in \Gamma(p)$. Soit encore $r > 0$ tel que $P' \in \Gamma(p^r)$ et $P' \notin \Gamma(p^{r+1})$, on a le même résultat.

$0 = t(pP') \equiv pt(P') \quad [p^{3r} R]$, $t(P') \equiv 0 \quad [p^{3r-1} R]$, mais comme $3r - 1 \geqslant r + 1$, c'est en contradiction avec $P' \notin \Gamma(p^{r+1})$.

On a donc montré par l'absurde que $P \notin \Gamma(p)$, c'est-à-dire que les points exceptionnels de Γ à coordonnées rationnelles sont en fait à coordonnées entières, et ceci achève la démonstration.

Mlle E. LUTZ, en 1937, a montré que dans le cas des corps p-adiques, le groupe Γ n'a qu'un nombre fini de points exceptionnels ([6]). Ceci est généralisé au cas des variétés abéliennes de dimension quelconque par MATTUCK, en 1955.

D'après les travaux de Mlle LUTZ, CASSELS montre que les coordonnées x, y d'un point exceptionnel sur (E) dans K, corps de nombres algébriques, ne sont plus nécessairement des entiers de K, et donne des propriétés de ces coordonnées, mais cela est moins intéressant, car il faut faire un nombre infini d'essais ([2]).

CHÂTELET utilisant aussi les méthodes de Mlle LUTZ, pense à chercher l'ordre des points exceptionnels, et montre que l'on peut limiter les ordres de tous les points exceptionnels de (E) dans K , ceci ne demande qu'un nombre fini d'essais ([3]).

Un certain nombre de problèmes se posent encore.

Une façon de généraliser la notion de point d'ordre fini est la suivante : Connaissant un point rationnel M sur (E) , on cherche s'il existe un autre point rationnel N dont M soit un multiple, $M = nN$; plus généralement, étant donné un sous-groupe G de Γ_{rat} sur (E) , on cherche s'il existe une extension G_1 de G , $G_1 \subset \Gamma_{rat}$, telle que G_1/G soit fini. Mlle LUTZ a donné des résultats, mais ne résoud pas complètement les problèmes ; la méthode de descente infinie de Mordell donne des solutions, sauf pour le cas des points exceptionnels.

Une conjecture importante est faite sur l'ensemble des points d'ordre fini. Soit $\mathfrak{T}$ l'ensemble des points d'ordre fini, pour une variété abélienne donnée dans K , on a vu que c'est un ensemble fini, on considère toutes les variétés sur K .

Conjecture. - Pour K donné (en particulier $K = Q$), l'ordre de $\mathfrak{T}$ est borné. Ce résultat est faux pour les corps locaux.

Pour les variétés de dimension 1 sur Q , on a un certain nombre de résultats. $\mathfrak{T}$ est cyclique, ou produit d'un groupe cyclique et d'un cycle d'ordre 2 [NAGELL (1946, 1952, 1953), BERGMAN (1954), SELMER (1954), HELLEGOUARCH (1965)].

D'autre part, en 1917, dans le cas de $K = Q$, HURWITZ a montré que, pour des $a , b , c , d \in Z$ sans carrés avec $c > b > a$, la courbe $aX^3 + bY^3 + cZ^3 + dXYZ$ ne peut avoir des points d'ordre fini, et que Γ est infini si, et seulement si, il y a un point rationnel.

On peut citer aussi, le problème de l'existence des points rationnels, car en effet, on suppose toujours l'existence au départ d'un point rationnel.

Etant donnée une courbe elliptique (E) définie sur K , corps global, qui a partout localement un point sur K , comment dire s'il existe un point global.

REICHARDT (1942) est le premier qui ait donné un résultat à ce sujet. Il existe un point O sur (E) défini sur K' , extension de K , normale de groupe de Galois $\mathfrak{G}$. Sur K' , (E) a la structure d'une variété abélienne avec O comme zéro, et on peut déterminer le groupe $\Gamma_{K'}$ des points définis sur K' . Le groupe de Galois $\mathfrak{G}$ agit sur $\Gamma_{K'}$, et comme $\Gamma_{K'}$ est de rang fini, on détermine s'il contient un point fixe par $\mathfrak{G}$, c'est-à-dire un point défini sur K . REICHARDT a montré qu'il existe des points rationnels sur $x^4 - 17 = 2y^2$ de cette manière, avec $K = Q$, $K' = Q(\sqrt{2})$ ([10]).

Il y a encore un résultat intéressant de finitude, donné par SIEGEL [11]. Si (E) est une courbe définie sur un anneau qui est un Z-module de type fini, si cette courbe est de genre supérieur ou égal à (1) , (E) n'a qu'un nombre fini de points dans cet anneau.

Il utilise le théorème de Mordell et les méthodes d'approximation diophantienne (théorème de Thue-Siegel) pour montrer que les courbes de genre supérieur ou égal à 1 n'ont qu'un nombre fini de points entiers.

En ce qui concerne le théorème le plus important, qui a été largement généralisé, le théorème de Mordell-Weil, il faut remarquer la méthode, qui dans le cas de Q est assez élémentaire, et se généralise très bien.

Les deux points sont la notion de hauteur, et le théorème faible de Mordell, et la méthode est celle de descente infinie.

L'étude des points exceptionnels est différente et utilise des propriétés des corps p-adiques.

BIBLIOGRAPHIE

[1] CASSELS (J. W. S.). - Arithmetic on curves of genus 1 , J. für reine und angew. Math., t. 202, 1959, p. 52-99.

[2] CASSELS (J. W. S.). - A note on the division values of $\mathfrak{P}(u)$, Proc. Cambridge phil. Soc., t. 45, 1949, p. 167-172.

[3] CHÂTELET (François). - Utilisation des congruences en analyse indéterminée, Ann. Univ. Lyon, 3e série, Section A : Sc. math. et Astron., t. 10, 1947, p. 5-22.

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

[5] LANG (Serge) and NÉRON (A.). - Rational points of abelian varieties over function fields, Amer. J. of Math., t. 81, 1959, p. 95-118.

[6] LUTZ (Elisabeth). - 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.

[7] MORDELL (L. J.). - On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cambridge phil. Soc., t. 21, 1922, p. 179-192.

[8] NAGELL (Trygve). - Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, Vid. Akad. Skrifter, Oslo, 1935, vol. 1, n° 1, 25 p.

[9] NÉRON (André). - Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps, Bull. Soc. math. France, t. 80, 1952, p. 101-166.

[10] REICHARDT (Hans). - Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen, J. für reine und angew. Math., t. 184, 1942, p. 12-18.

[11] SIEGEL (Carl Ludwig). - Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. Berlin, Phys.-Math. Kl., 1929, n° 1, 70 p.

[12] WEIL (André). - L'arithmétique sur les courbes algébriques, Acta Math., Uppsala, t. 52, 1928, p. 281-315.

(Texte reçu le 9 juin 1969)

Mlle Francine DELMER
16 rue Aristide Briand
76 - PAVILLY