Séminaire Dubreil.
Algèbre et théorie
des nombres

Georges Poitou

Les équations diophantiennes $x^3 + y^3 + dz^3 = 0$, d'après Cassels

Séminaire Dubreil. Algèbre et théorie des nombres, tome 13, n° 2 (1959-1960), exp. n° 24, p. 1-8

<http://www.numdam.org/item?id=SD_1959-1960__13_2_A12_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
13e année, 1959/60, n° 24

30 mai 1960

LES ÉQUATIONS DIOPHANTIENNES $x^3 + y^3 + dz^3 = 0$, D'APRÈS CASSELS

par Georges POITOU

Introduction.

Il n'est pas possible d'exposer ici l'histoire de la théorie des équations diophantiennes qui se ramènent à la recherche des points rationnels sur une courbe de genre 1 , car cette théorie a donné lieu à des publications extrêmement nombreuses et fort diverses. Qu'il me suffise de renvoyer à la monographie classique de SKOLEM [8], à la large bibliographie de CASSELS [2], et à un récent article de F. CHÂTELET [3] notamment pour les prolongements des méthodes connues pour les courbes à l'étude des points rationnels sur les surfaces algébriques.

Du riche mémoire de CASSELS [1], on se bornera ici à dégager les idées principales.

1. - Les points rationnels d'une courbe A de genre 1 forment, l'un d'eux o étant pris pour origine, un groupe G . Ce groupe est de type fini d'après le théorème de Mordell-Weil [5], [9]. Les méthodes connues pour démontrer ce théorème établissent d'abord un résultat relatif à la division par un entier n : le groupe G/nG est lui-même fini ("forme faible" du théorème de Mordell-Weil).

Pour une courbe A donnée explicitement, la détermination d'un système de générateurs de A requiert habituellement la détermination effective d'un groupe G/nG pour un certain entier n . Or, en général, on ne sait que le plonger en un groupe (défini par des conditions locales) fini effectivement calculable. L'objet principal du travail [1] analysé ici est de prouver en détail, sur des cas particuliers, que l'étude simultanée de la division par n et par n^2 permet de cerner de beaucoup plus près le groupe G/nG , jusqu'à conduire dans bien des cas (mais non dans tous) à sa détermination explicite.

2. - L'étude du groupe G/nG s'appuie ([9], [4]) sur sa représentation à l'aide de fonctions rationnelles attachées aux points u de G tels que nu = o . Suivons l'exposé de ROQUETTE [6]. Soit k un corps, mettons de caractéristique 0 (qui pourra être un corps de nombres algébriques ou un complété d'un tel corps)

sur lequel tous les points u de A, tels que $nu = o$, sont rationnels. Soit N le groupe de ces points.

Pour tout point a de A, soit $T_a : z \to z + a$ la translation correspondante, qui opère sur les fonctions φ définies sur A par $(T_a \varphi)(z) = \varphi(z - a)$, et de façon claire sur les diviseurs. Soit X un diviseur sur A, de degré 0, de sorte que, pour tout $a \in A$, $T_a X \sim X$ ($\sim$ désignant l'équivalence linéaire) ; il existe donc une fonction $c_a(X)(z)$ sur A, définie sur le corps k pourvu que a et X le soient, de diviseur $T_a X/X$. Posons alors

$$c_{a,b} = T_b(c_a)\, c_b\, c_{a+b}^{-1} .$$

Le diviseur de cette fonction s'évanouissant, celle-ci est une constante de k^* (ne dépendant plus que de a, b, X et non de z) ; on vérifie sans peine qu'on a l'identité des cocycles

$$T_d(c_{a,b})\, c_{a+b,d} = c_{a,b+d}\, c_{b,d}$$

où T_d peut être omis, puisque les translations n'opèrent plus que trivialement sur les fonctions constantes. De plus, la classe de cohomologie de ce cocycle ne dépend pas de la fonction $c_a(X)$ de diviseur $T_a X/X$, et ne dépend même de X que par la classe de ce diviseur (pour l'équivalence linéaire).

En restreignant les indices aux points de la division de o par n, on obtient ainsi une application h qui, à toute classe de diviseurs de degré 0 définie sur k, associe une classe de cohomologie de $H^2(N, k^*)$, application qui est manifestement un homomorphisme de groupes. Le noyau de cet homomorphisme est constitué des classes des diviseurs X tels que $c_{a,b}(X) = \gamma_a \gamma_b \gamma_{a+b}^{-1}$ pour un système de constantes γ_a convenables dans k^*. Si l'on substitue à $c_a(X)(z)$ la fonction $\gamma_a^{-1} c_a(X)(z)$, on obtient un cocycle identique à 1, de sorte qu'avec de nouvelles notations on a l'identité

$$T_b(c_a)\, c_b = c_{a+b}$$

donc $a \to c_a$ définit un cocycle de dimension 1 du groupe N, opérant par les translations sur le groupe multiplicatif K^* du corps K des fonctions sur A définies sur k. D'après la théorie de Galois et le théorème 90 de Hilbert, ce cocycle est dégénéré, et il existe une fonction φ de K^*, telle que $c_a(X)(z) = T_a \varphi(z)/\varphi(z)$; si l'on change alors le diviseur X pour le diviseur linéairement équivalent $X/\mathrm{div}\ \varphi$, on peut obtenir des fonctions c_a constantes ; c'est dire que le nouveau diviseur est invariant par les translations de N.

Réciproquement, les classes de diviseurs contenant un diviseur invariant par les translations de N appartiennent au noyau de h.

Désignons par ν la multiplication par n dans A. Un diviseur X invariant par les translations de N est de la forme $\nu^{-1}(Y)$, où Y est un diviseur équivalent à tous ses translatés ; on sait qu'alors $\nu^{-1}(Y)$ est linéairement équivalent à Y^n, de sorte que toute classe du noyau de h est représentable par un diviseur de la forme Y^n, où Y est un diviseur de degré 0 défini sur k ; et réciproquement.

Utilisons maintenant le fait que toute classe de diviseurs de degré 0 peut être représentée par un diviseur de la forme x/o, où x est un point de A rationnel sur k si la classe l'est, et que $x \to$ (classe de x/o) est un isomorphisme du groupe G des points de A définis sur k, sur le groupe des classes de diviseurs de degré 0 définis sur k ; on en déduit un homomorphisme de G dans $H^2(N, k^*)$, dont le noyau est nG ; donc G/nG s'identifie à un sous-groupe de $H^2(N, k^*)$; ces homomorphismes de G et de G/nG seront encore notés h.

REMARQUE. - Il n'est pas difficile d'établir (en travaillant dans $A \times A$) que le cocycle $c_{a,b}$ dépend rationnellement de x.

3. - Tout ce qui précède peut être recommencé avec un corps k' contenant k, et on obtient une application h' de G' dans $H^2(N, k'^*)$. Si l'on considère un cocycle à valeurs dans k^* comme étant à valeurs dans k'^*, on définit un homomorphisme i de $H^2(N, k^*)$ dans $H^2(N, k'^*)$, et il est clair que, pour les points de G, h' est composé de h et de i ; le cocycle dans k^* associé à $x \in G$ est dégénéré dans k'^* si et seulement si $x \in nG'$; comme ceci peut toujours être obtenu par une extension finie k'/k, le cocycle associé à x est de la forme

$$c_{a,b} = \gamma_a \gamma_b \gamma_{a+b}^{-1}$$

avec des $\gamma_a \in k'^*$; en particulier, ce cocycle est commutatif, on a $c_{a,b} = c_{b,a}$.

4.- Soient maintenant k un corps de nombres algébriques, p l'une de ses valuations (ordinaires ou à l'infini) et k_p le complété correspondant. Désignons par h_p l'application analogue à h relative à k_p et par i_p l'application naturelle de $H^2(N, k^*)$ dans $H^2(N, k_p^*)$ déduite de l'inclusion $k \to k_p$.

Soient H , H_p les images respectives de h et de h_p . Il est clair que $i_p(H) \subset H_p$, donc H est contenu dans le sous-groupe $\bar{H}$ de $H^2(N , k^*)$ constitué des classes α telles que $i_p(\alpha) \in H_p$ pour toute valuation p . C'est ce sous-groupe $\bar{H}$ dont on démontre qu'il est fini, ce qui entraîne la même propriété pour H . Mais de nombreux exemples montrent que $\bar{H}$ est souvent trop grand et le but de CASSELS est de définir et de calculer un groupe $\bar{\bar{H}}$ intermédiaire, souvent bien plus voisin de H . Cf. les tables de SELMER [7].

Pour cela, soient N' le groupe des $u \in A$ tels que $n^2 u = o$, et k' un corps contenant k et sur lequel ces points sont rationnels ; désignons par $\tilde{H}^2(N' , k'^*)$ le sous-groupe de $H^2(N' , k'^*)$ engendré par des cocycles dont la restriction à N est à valeurs dans k^* , par h' l'application analogue à h de G dans $\tilde{H}^2(N' , k'^*)$, et par H' l'image de G dans cette application. Par restriction des cocycles à N , on obtient un homomorphisme ρ de $\tilde{H}^2(N' , k'^*)$ dans $H^2(N , k^*)$, tel que $\rho H' = H$; en effet, H est isomorphe à G/nG , H' à $G/n^2 G$, et, par ces isomorphismes, ρ correspond à l'application naturelle de $G/n^2 G$ sur G/nG .

Désignons encore par k'_p l'algèbre $k' \otimes_k k_p$, par i'_p l'application de $\tilde{H}^2(N' , k'^*)$ dans $\tilde{H}^2(N' , k'^*_p)$ déduite de l'inclusion $k' \to k' \otimes k_p$, et par ρ_p l'application de $\tilde{H}^2(N' , k'^*_p)$ dans $H^2(N , k^*_p)$ obtenue par restriction du cocycle à N , et observons que $i_p \circ \rho = \rho_p \circ i'_p$, de sorte que, si $\bar{H}'$ est le sous-groupe de $\tilde{H}^2(N' , k'^*)$ composé des β tels que $i'_p(\beta) \in H'_p$ pour tout p , et $\bar{\bar{H}}$ le sous-groupe $\rho(\bar{H}')$ de $H^2(N , k^*)$, alors $\bar{\bar{H}}$ est contenu dans $\bar{H}$: car $\alpha \in \bar{\bar{H}}$ implique $\alpha = \rho(\beta)$ avec $\beta \in \bar{H}'$, donc $i'_p(\beta) \in H'_p$ pour tout p , et par suite $i_p(\alpha) = i_p(\rho(\beta)) = \rho_p(i'_p(\beta)) \in \rho_p(H'_p) = H_p$ pour tout p , donc $\alpha \in \bar{H}$.

De plus, il est clair que $H \subset \bar{\bar{H}}$, donc $\bar{\bar{H}}$ est bien un groupe intermédiaire entre H et $\bar{H}$. L'un des principaux résultats (conjecturé par SELMER) est que la différence des rangs de $\bar{H}$ et de $\bar{\bar{H}}$ est paire ; CASSELS le démontre comme conséquence de l'existence d'une forme bilinéaire antisymétrique $U(x , y)$ sur $\bar{H}$, ayant pour valeurs des racines de l'unité, et telle que $\bar{\bar{H}}$ est caractérisé comme l'ensemble des $x \in \bar{H}$ tels que $U(x , y) = 1$ pour tout $y \in \bar{H}$. La différence des rangs de $\bar{H}$ et de $\bar{\bar{H}}$ est donc le rang de U , c'est un nombre pair puisque U est antisymétrique.

5. - Tout ceci est exposé sur l'exemple des courbes de la forme

(*) $$x^3 + y^3 + dz^3 = 0$$

avec $k = Q(\rho)$ où ρ est une racine cubique de l'unité, et $k' = k(d^{1/3})$. Le point o est $(1 , -1 , 0)$. On peut donner ici aux groupes de cohomologie une forme simple, grâce à deux lemmes faciles :

LEMME 1. - Si $N' = N \times N_1$ et si un cocycle commutatif sur N' est dégénéré sur N et sur N_1 , il l'est sur N' .

Ce lemme où on suppose seulement N' commutatif, montre qu'on a une injection

$$H^2(N' , k'^*) \to H^2(N , k'^*) \times H^2(N_1 , k'^*)$$

et en particulier

$$H^2(N' , k'^*) \to H^2(N , k^*) \times H^2(N_1 , k'^*) \quad .$$

LEMME 2. - Pour un groupe cyclique M d'ordre m opérant trivialement sur B , on a $H^2(M , B) \simeq B/B^m$, l'isomorphisme consistant à associer au cocycle $c_{a,b}$ la classe modulo B^m du produit $\prod_{a \in M} c_{g,a}$ où g est un générateur de M .

Ces deux lemmes permettent de caractériser les classes de cohomologie de N' par deux nombres, si les groupes N et N_1 sont cycliques. Or, c'est le cas pour les courbes $(*)$ si l'on remplace la multiplication par n des paragraphes 1 à 4 par la multiplication complexe par le nombre $\tau = \rho - \rho^2$, tel que $\tau^2 = -3$. Pour vérifier qu'on a bien une telle multiplication complexe, il suffit de vérifier que la multiplication par ρ

$$(x , y , z) \to (x , y , \rho z)$$

est bien un automorphisme de la structure de groupe de A , ce qui est immédiat si l'on écrit les formules d'addition.

Les points de N sont alors, outre $\underset{\sim}{o} = (1 , -1 , 0)$

$$\underset{\sim}{d} = (\rho , -1 , 0) \qquad -\underset{\sim}{d} = (1 , -\rho , 0)$$

et les autres points de N' sont, en posant $\delta = d^{1/3}$,

$$\underset{\sim}{d'} = (0 , \delta , -1) \qquad -\underset{\sim}{d'} = (\delta , 0 , -1)$$

$$\underset{\sim}{d'} + \underset{\sim}{d} = (0 , \delta\rho , -1) \qquad -\underset{\sim}{d'} - \underset{\sim}{d} = (\delta\rho , 0 , -1)$$

$$\underset{\sim}{d'} - \underset{\sim}{d} = (0 , \delta\rho^2 , -1) \qquad -\underset{\sim}{d'} + \underset{\sim}{d} = (\delta\rho^2 , 0 , -1)$$

et l'on peut prendre $N' = N \times N_1$, avec $N_1 = \{\underset{\sim}{o} , \underset{\sim}{d'} , -\underset{\sim}{d'}\}$; N' est ainsi le produit de deux groupes cycliques d'ordre 3 .

On est donc amené à considérer les deux fonctions de $\underset{\sim}{x}$ suivantes

$$m(\underset{\sim}{x}) = c_{d,d}(\underset{\sim}{x})\ c_{d,-d}(\underset{\sim}{x}) \qquad m'(\underset{\sim}{x}) = c_{d',d'}(\underset{\sim}{x})\ c_{d',-d'}(\underset{\sim}{x})$$

qu'on peut encore écrire en remplaçant $c_{a,b}$ par sa définition

$$m(\underset{\sim}{x}) = c_{d}^{3}(\underset{\sim}{x})(\underset{\sim}{z})\ T_{d}\ f(\underset{\sim}{x})(\underset{\sim}{z})/f(\underset{\sim}{x})(\underset{\sim}{z}) \qquad \text{et de même pour } m'(\underset{\sim}{x})$$

en posant

$$f(\underset{\sim}{x})(\underset{\sim}{z}) = c_{d}(\underset{\sim}{x})(\underset{\sim}{z})\ c_{-d}(\underset{\sim}{x})(\underset{\sim}{z}) \qquad \text{et de même pour } m'(x).$$

Grâce à ces fonctions, on peut représenter la classe de cohomologie $h(\underset{\sim}{x})$ par les nombres $m(\underset{\sim}{x})$ et $m'(\underset{\sim}{x})$ modulo k^{*3} et k'^{*3} respectivement.

REMARQUE. - Pour chaque $\underset{\sim}{x}$ donné, les fonctions c et par suite m, m' peuvent être choisies de façon à indiquer la classe de cohomologie $h(\underset{\sim}{x})$, mais un choix unique ne peut convenir à tous les $\underset{\sim}{x}$ simultanément : il faut utiliser plusieurs de ces fonctions pour recouvrir G, et lorsque deux d'entre elles sont définies et non nulles au même point, elles donnent des résultats concordants. Négligeons dans la suite cette difficulté de détail.

En fait, dans le cas des courbes (*), CASSELS peut définir directement ces fonctions m et m' (qui sont d'un type déjà considéré par A. WEIL, avec un diviseur de la forme a^3/b^3, pour $a, b \in \mathbf{N}$ ou $\mathbf{N}'$) par des formules élémentaires

$$m(\underset{\sim}{x}) = \frac{\rho^2 x + \rho y}{\rho x + \rho^2 y} \qquad m'(\underset{\sim}{x}) = \frac{\tau(y + z\delta)}{x + y} \quad .$$

Ces deux fonctions ne sont pas indépendantes ; en fait, si l'on pose

$$\ell(\underset{\sim}{x}) = c_{d',-d'}\ c_{d+d',d'-d} \qquad \text{ou} \quad \frac{-\tau x}{x + y}$$

$$\alpha(x) = c_{d,d}\ c_{d,d+d'}^{-1} \qquad \text{ou} \quad \frac{\rho x + \rho^2 y + \rho\delta z}{\rho^2 x + \rho y + \rho^2 \delta z}$$

on a $N_{k'/k}(\alpha) \equiv m^{-1}\ \ell\alpha^{D-D^2} \equiv m'$, où D désigne le générateur du groupe de Galois de k'/k, défini par $\delta^D = \rho\delta$, les congruences s'entendant modulo k^{*3} et k'^{*3} respectivement. Ceci peut être vérifié sous l'une ou l'autre des deux formes.

6. - En fait, la propriété qu'ont les valeurs de la fonction m (c'est-à-dire les éléments de H) d'être des normes dans k'/k s'étend au groupe $\overline{H}$; soit en effet, $\mu \in k$, tel que pour tout p, il existe sur A un point $\underset{\sim}{x}_p$ défini

sur k_p tel que $\mu \equiv m(\underset{\sim}{x}_p) \mod k_p^{*3}$; il existe donc d'après le paragraphe 3, un point $\underset{\sim}{y}_p$ tel que $\tau \underset{\sim}{y}_p = \underset{\sim}{x}_p$, défini sur $k_p(\mu^{1/3})$; des calculs simples montrent qu'alors d est une norme de $k_p(\mu^{1/3})$ et par suite de la réciprocité du symbole de restes normiques, μ est une norme de $k_p(d^{1/3})$; d'après le théorème de Hasse sur les extensions cycliques, μ est donc une norme de $k(d^{1/3}) = k'$.

Nous pouvons maintenant donner une définition de la forme bilinéaire U de CASSELS. Soient μ_1 , μ_2 deux éléments de $\overline{H}$, et $\beta \in k'$ tel que $\mu_2 = N_{k'/k}(\beta)$; soit aussi $\underset{\sim}{x}_p$ un point de A défini sur k_p tel que $\mu_1 \equiv m(\underset{\sim}{x}_p) \mod k_p^{*3}$. Posons alors

$$U(\mu_1 , \mu_2) = \prod_P \left(\frac{m'(\underset{\sim}{x}_p)\ \beta_2}{P}\right)$$

où le produit est étendu à toutes les valuations P de k' , et où $\left(\frac{a\ b}{P}\right)$ désigne le symbole de restes normiques de Hilbert. On vérifie successivement

i. que ce produit a un sens, en montrant qu'il est fini ;

ii. qu'il est indépendant des choix des $\underset{\sim}{x}_p$;

iii. qu'il est indépendant du choix de β_2 .

Donc, on a bien défini une fonction sur $\overline{H} \times \overline{H}$, qui est évidemment bilinéaire. On établit ensuite, par quelques calculs, qu'elle est antisymétrique. Il reste à voir que la classe de μ_1 appartient à $\overline{\overline{H}}$ si et soulement si $U(\mu_1 , \mu_2) = 1$ pour tout $\mu_2 \in \overline{H}$; dans un sens, la démonstration est assez difficile et résulte de calculs d'indices analogues à ceux de la théorie du corps des classes sous la forme classique de CHEVALLEY ; dans l'autre sens, elle est presque immédiate : si la classe de $\mu_1 \in \overline{\overline{H}}$, c'est qu'il existe $\mu_1' \in k'$ et pour tout p un $\underset{\sim}{x}_p$ tel que $m(\underset{\sim}{x}_p) = \mu_1$, $m'(\underset{\sim}{x}_p) = \mu_1'$; on peut alors choisir ces $\underset{\sim}{x}_p$ pour définir $U(\mu_1 , \mu_2)$, et alors

$$U(\mu_1 , \mu_2) = \prod_P \left(\frac{\mu_1'\ \beta_2}{P}\right)$$

est égal à 1 d'après la formule du produit de Hilbert.

L'auteur termine son mémoire en montrant sur un exemple ($d = 5610 = 2.3.5.11.17$) l'utilité du remplacement de $\overline{H}$ par $\overline{\overline{H}}$. Il montre que $\overline{H}$ est alors le produit des cinq cycles d'ordre 3 engendrés par 2 , 3 , 5 , 11 , 17 modulo les cubes, et que le rang de U est 4 , ce qui ramène $\overline{\overline{H}}$ à l'ordre 3 et suffit à montrer que l'équation (*) n'a pas d'autres solutions sur $Q(\rho)$ que les points

$\underset{\sim}{o} \pm \underset{\sim}{d}$, donc pas d'autre solution rationnelle que la solution triviale $(1 , -1 , 0)$ et les solutions proportionnelles.

BIBLIOGRAPHIE

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

[2] CASSELS (J. W. S.). - The rational solutions of the diophantine equation $Y^2 = X^3 - D$, Acta Math., t. 82, 1950, p. 243-273.

[3] CHÂTELET (François). - Points rationnels sur certaines courbes et surfaces cubiques, Ens. math., 2e série, t. 5, 1959, p. 153-170.

[4] HASSE (Helmut). - Der n-Teilungskörper eines abstrakten elliptischen Funktionenkörpers als Klassenkörper, nebst Anwendung auf den Mordell-Weilschen Endlichkeitssatz, Math. Z., t. 48, 1942/43, p. 48-66.

[5] MORDELL (L. J.). - On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cambridge phil. Trans., t. 21, 1922, p. 179-182.

[6] ROQUETTE (Peter). - Über das Hassesche Klassenkörper-Zerlegungsgesetz und seine Verallgemeinerung für beliebige abelsche Funktionenkörper, J. für reine und angew. Math., t. 197, 1957, p. 49-67.

[7] SELMER (Ernst S.). - The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math., t. 85, 1951, p. 203-362 et t. 92, 1954, p. 191-197.

[8] SKOLEM (T.). - Diophantische Gleichungen. - Berlin, J. Springer, 1938 (Ergebnisse der Mathematik, Band 5, 4).

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