François Châtelet

Points rationnels sur certaines surfaces cubiques

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 1 (1958-1959), exp. n° 12, p. 1-9
<http://www.numdam.org/item?id=SD_1958-1959__12_1_A11_0>

26 janvier 1959

POINTS RATIONNELS SUR CERTAINES SURFACES CUBIQUES

par François CHÂTELET

En février 1954, j'ai fait à ce Séminaire un premier exposé sur les points rationnels d'une surface cubique. J'ai alors attiré l'attention sur l'intérêt des surfaces cubiques qui contiennent une droite rationnelle (définie par un système d'équations à coefficients rationnels). On ne connaît pas encore de méthode générale pour étudier les points rationnels de ces surfaces. J'ai pu récemment traiter le cas d'une catégorie de ces surfaces et j'ai exposé brièvement les résultats obtenus au Congrès international d'Edinbourg en août dernier. Je suis heureux d'avoir l'occasion d'en faire un exposé plus complet. Si ces résultats restent limités à des cas trop particuliers, ils font apparaître 2 idées susceptibles d'applications plus étendues :

ils confirment l'intérêt, en analyse diophantienne, des correspondances simplement rationnelles à coefficients rationnels, que j'ai déjà utilisées pour d'autres surfaces cubiques ;

ils établissent pour la première fois un rapport entre la recherche des points rationnels sur une cubique plane (de genre un) et sur une surface cubique (qui admet pourtant des représentations paramétriques birationnelles).

Considérons la surface cubique S :

$$y^2 - az^2 = x(x - a_1)(x - a_2)$$

où a , a_1 , a_2 sont des entiers rationnels. Elle contient une droite rationnelle : la droite à l'infini dans le plan $x = 0$; elle admet en outre 2 points singuliers sur cette droite, par lesquels passent toutes les sections par les plans x constants. Ce sont les points définis par les relations :

$$x + \theta y = 0 \quad \text{ou} \quad x - \theta y = 0 \quad ,$$

avec $\theta^2 = a$.

Nous allons étudier les points rationnels de cette surface par un procédé qui présente des analogies avec l'étude classique de POINCARÉ [2], MORDELL [1] et A. WEIL [3] des points rationnels sur la cubique C :

$$y^2 = x(x - a_1)(x - a_2) \quad .$$

Il reste des différences essentielles entre l'étude des points rationnels de S et de C. La plus importante est due à l'existence de représentations homaloïdales (ou birationnelles) de S à coefficients algébriques. La représentation H, qui sera la plus commode pour la suite de cet exposé, est obtenue en choisissant pour paramètres :

$$\lambda = \frac{y + \theta z}{x - a_1} \quad , \qquad \mu = \frac{y - \theta z}{x - a_2} \quad .$$

On en déduit :

$$x = \lambda \mu$$

et

$$2y = \lambda(x - a_1) + \mu(x - a_2) \quad , \quad 2\theta z = \lambda(x - a_1) - \mu(x - a_2) \quad .$$

Si θ est rationnel, cette représentation permet d'obtenir tous les points rationnels de S en choisissant les valeurs rationnelles des paramètres λ et μ. Nous supposerons donc dans la suite θ irrationnel.

L'étude des points rationnels sur C utilise la représentation de C par les fonctions elliptiques ou son équivalent géométrique ou algébrique, ce qui suppose que C est de genre un, c'est-à-dire $a_1 \neq 0$, $a_2 \neq 0$, $a_1 \neq a_2$; si l'une de ces 3 inégalités n'est pas vérifiée, la recherche des points rationnels sur C, comme sur S, est triviale. Nous supposerons donc C de genre un. La représentation par les fonctions elliptiques permet d'organiser l'ensemble des points rationnels sur C en groupe additif G ; la formule d'addition de 2 points x_1, y_1 et x_2, y_2 peut être définie par les formules :

$$x = \frac{(x_1 y_2 - x_2 y_1)^2}{x_1 x_2 (x_1 - x_2)^2}$$

$$y = \frac{y_2 - y_1}{x_1 - x_2} x + \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2} \quad .$$

Cette addition peut encore être définie géométriquement par les 2 conditions :

la somme de 3 points de C alignés est nulle,

le point à l'infini sur C est l'élément neutre de G .

L'ensemble des points rationnels de S ne peut être organisé en groupe additif. Néanmoins, on peut introduire une loi de composition de 2 points rationnels M_1 et M_2 de S par les formules :

$$x = \frac{(x_1y_2 - x_2y_1)^2 - a(x_1z_2 - x_2z_1)^2}{x_1x_2(x_1 - x_2)^2}$$

$$y = \frac{y_1 - y_2}{x_1 - x_2} x + \frac{x_1y_2 - x_2y_1}{x_1 - x_2} \quad , \quad z = \frac{z_1 - z_2}{x_1 - x_2} x + \frac{x_1z_2 - x_2z_1}{x_1 - x_2}$$

ou par la condition géométrique : le composé $P = M_1 \star M_2$ est aligné avec M_1 et M_2 . Malheureusement, cette composition n'est pas toujours associative et le composé de 2 points confondus est indéterminé ; ces faits ne permettent pas d'organiser en groupe l'ensemble des points rationnels sur S .

Le principe essentiel de l'étude des points rationnels sur C utilise le groupe $2G$ formé par les "doubles" des éléments de G (c'est-à-dire les points obtenus par addition d'un point rationnel de C avec lui-même : $M * M$) et le groupe-quotient $G/2G$.

Le composé $M \star M$ d'un point rationnel de S avec lui-même est indéterminé ; par contre le composé $M \star \overline{M}$ d'un point M de S à coordonnées dans $R(\Theta)$ et son conjugué $\overline{M}$ (c'est-à-dire du point dont les coordonnées sont les conjuguées $\overline{x}$, $\overline{y}$, $\overline{z}$ de celles de M) est déterminé si M n'est pas rationnel. En outre la représentation homaloïdale H permet d'obtenir tous les points M de S dans $R(\Theta)$ en choisissant les paramètres λ et μ dans ce corps ; elle permet donc aussi d'obtenir les composés $P = M \star \overline{M}$ en fonction des paramètres λ et μ de $R(\Theta)$ ou encore de 4 paramètres rationnels λ_1 , λ_2 , μ_1 , μ_2 en posant :

$$\lambda = \lambda_1 + \Theta \lambda_2 \quad , \mu = \mu_1 + \Theta \mu_2 \ .$$

Le point P est rationnel, puisqu'il est confondu avec son conjugué ; il est d'ailleurs facile de le vérifier sur les formules. L'abcisse X de P est :

$$X = \frac{(x\overline{y} - \overline{x}y)^2 - a(x\overline{z} - \overline{x}z)^2}{x\overline{x}(x - \overline{x})^2}$$

$$= \frac{[(\lambda\mu - a_1)\bar{\lambda} - (\bar{\lambda}\bar{\mu} - a_2)\mu][(\lambda\mu - a_2)\bar{\mu} - (\bar{\lambda}\bar{\mu} - a_1)\lambda]}{(\lambda\mu - \bar{\lambda}\bar{\mu})^2}$$

Les coordonnées Y et Z se déduisent des formules :

$$Y + \theta Z = \frac{[(\bar\lambda\bar\mu - a_2)\mu - (\lambda\mu - a_1)\bar\lambda][(\bar\lambda\bar\mu - a_1)\lambda - (\bar\lambda\bar\mu - a_2)\bar\mu][(\lambda\mu - a_1)\lambda - (\lambda\mu - a_2)\bar\mu]}{(\lambda\mu - \bar\lambda\bar\mu)^3}$$

$$Y - \theta Z = \frac{[(\lambda\mu - a_2)\bar\mu - (\bar\lambda\bar\mu - a_1)\lambda][(\lambda\mu - a_1)\bar\lambda - (\lambda\mu - a_2)\mu][(\bar\lambda\bar\mu - a_1)\bar\lambda - (\bar\lambda\bar\mu - a_2)\mu]}{(\lambda\mu - \bar\lambda\bar\mu)^3}$$

Les formules exprimant X, Y, Z en fonction des 4 paramètres rationnels λ_1, λ_2, μ_1, μ_2 s'en déduisent par simple substitution ; on constate que ce sont des formules rationnelles à coefficients rationnels. Mais il existe une infinité de systèmes de paramètres λ_1, λ_2, μ_1, μ_2 correspondant à un même point P ; les composés $P = M * M$ sont ainsi obtenus par une représentation simplement rationnelle à coefficients rationnels.

Le groupe $2G$, formé par les doubles des points rationnels sur C, est distinct de G. A. WEIL a donné un critère pour qu'un élément de G appartienne à $2G$, qui joue un rôle essentiel dans sa méthode : il faut et il suffit que l'abscisse x de ce point et les 2 différences $x - a_1$ et $x - a_2$ soient les carrés de nombres rationnels.

On constate de même que l'abscisse X du composé $P = M * \bar M$ de 2 points conjugués de $R(\theta)$ est la norme d'un nombre de $R(\theta)$. De plus les formules :

$$X - a_1 = \frac{[(\lambda\mu - a_1)\bar\lambda - (\lambda\mu - a_2)\mu][(\bar\lambda\bar\mu - a_2)\bar\mu - (\bar\lambda\bar\mu - a_1)\lambda]}{(\lambda\mu - \bar\lambda\bar\mu)^2}$$

et

$$X - a_2 = \frac{[(\bar\lambda\bar\mu - a_1)\bar\lambda - (\bar\lambda\bar\mu - a_2)\mu][(\lambda\mu - a_2)\bar\mu - (\lambda\mu - a_1)\lambda]}{(\lambda\mu - \bar\lambda\bar\mu)^2}$$

montrent que $X - a_1$ et $X - a_2$ sont aussi les normes de nombres de $R(\theta)$. Inversement, si les coordonnées X, Y, Z d'un point rationnel de S vérifient les conditions :

$$X = \alpha^2 - a\beta^2 \quad , \quad X - a_1 = \alpha_1^2 - a\beta_1^2 \quad , \quad X - a_2 = \alpha_2^2 - a\beta_2^2$$

avec α, β, α_1, β_1, α_2, β_2 rationnels, les relations :

$$\frac{(\lambda\mu - a_1)\bar\lambda - (\bar\lambda\bar\mu - a_2)\mu}{\lambda\mu - \bar\lambda\bar\mu} = \alpha + \theta\beta$$

$$\frac{(\lambda\mu - a_1)\bar\lambda - (\lambda\mu - a_2)\mu}{\lambda\mu - \bar\lambda\bar\mu} = \alpha_1 + \theta\beta_1$$

$$\frac{(\bar\lambda\bar\mu - a_1)\bar\lambda - (\bar\lambda\bar\mu - a_2)\mu}{\lambda\mu - \bar\lambda\bar\mu} = \alpha_2 + \theta\beta_2$$

sont compatibles ; des combinaisons simples permettent d'ailleurs d'en trouver les solutions :

$$\mu = \alpha - \alpha_1 + \theta(\beta - \beta_1) , \quad \bar{\lambda} = \alpha - \alpha_2 + \theta(\beta - \beta_2) .$$

Le composé du point M, dont les paramètres sont les nombres λ, μ ainsi calculés, et de son conjugué $\overline{M}$ a la même abcisse que le point rationnel $P(X , Y , Z)$ considéré ; il peut toutefois avoir 2 autres coordonnées Y' et Z' différentes de Y et Z. Mais si on remplace λ et μ par $\lambda\rho/\bar{\rho}$ et $\mu\bar{\rho}/\rho$, où ρ est un nombre arbitraire de $R(\theta)$, l'abcisse X du composé $M \star M$ reste invariante, tandis que $Y' + \theta Z'$ et $Y' - \theta Z'$ sont remplacés par $(Y' + \theta Z')\rho/\bar{\rho}$ et $(Y - \theta Z')\bar{\rho}/\rho$. Les propriétés classiques des normes dans un corps quadratique montrent qu'on peut choisir ρ de manière que :

$$(Y' + \theta Z')\rho/\bar{\rho} = Y + \theta Z , \quad (Y' - \theta Z')\bar{\rho}/\rho = Y - \theta Z .$$

Ainsi les conditions :

$$X = \alpha^2 - a\beta^2 , \quad X - a_1 = \alpha_1^2 - a\beta_1^2 , \quad X - a_2 = \alpha_2^2 - a\beta_2^2$$

sont nécessaires et suffisantes pour que le point X , Y , Z soit le composé de 2 points conjugués de $R(\theta)$.

Il est encore intéressant de connaître les transformations qui permettent de déduire d'un couple de points conjugués M, $\overline{M}$ de S un autre couple M', $\overline{M}'$ tel que :

$$M \star \overline{M} = M' \star \overline{M}' .$$

Les propriétés précédentes montrent que ces transformations forment un groupe qui est le produit direct de 2 groupes isomorphes au groupe multiplicatif des nombres de norme unité de $R(\theta)$ (qui sont encore les nombres de $R(\theta)$ de la forme $\rho/\bar{\rho}$). Mais on peut aussi donner une interprétation géométrique de ce groupe qui explique la condition nécessaire et suffisante précédente.

Il est toutefois plus simple de considérer le groupe des transformations qui remplacent un couple M, $\overline{M}$ de points conjugués de S par un couple M', $\overline{M}'$ tel que $M \star \overline{M}$ et $M' \star \overline{M}'$ aient même abcisse X. Le groupe précédent s'en déduit comme groupe quotient. Désignons par D_0 la droite à l'infini sur S, par I et J les points singuliers de S sur D_0. La section de S par un plan contenant D_0 (ou plan X constant) est une conique (non rationnelle si X est irrationnel) qui admet une infinité de transformations birationnelles à coefficients rationnels en elle-même. Pour définir le transformé d'un point M

de cette conique dans une telle transformation, on peut définir le transformé de la droite MI qui joint M à l'un des points singuliers I de la droite de l'infini, puisque cette conique passe par I ; on peut encore définir le transformé du plan passant par MI et par un point fixe du plan de l'infini non situé sur D_0. La transformation T ainsi définie par l'intermédiaire de ce plan peut alors être étendue à tous les points de S. Elle transforme tout couple de points conjugués M, $\overline{M}$ de S en un autre couple de points conjugués M', $\overline{M}'$. L'ensemble de ces transformations T dépend d'un seul paramètre rationnel ; l'ensemble des droites $M'\overline{M}'$ qui joignent les transformés de 2 points fixes conjugués M, $\overline{M}$ dans ces différentes transformations engendre une quadrique Q. Cette quadrique Q coupe S suivant 3 coniques dont les plans passent par D_0 : le lieu de M', le lieu de $\overline{M}'$ et le lieu du composé $P' = M' * \overline{M}'$. Ces transformations font donc partie du groupe cherché ; analytiquement, ce sont les transformations qui remplacent $y + \theta z$ et $y - \theta z$ par $(y + \theta z)\rho/\bar{\rho}$ et $(y - \theta z)\bar{\rho}/\rho$, où ρ est un nombre arbitraire de $R(\theta)$.

D'autre part S contient, en plus de D_0, six droites situées 2 à 2 dans les plans $x = 0$, $x = a_1$, $x = a_2$. Désignons par D_1 la droite située dans le plan $x = 0$ et passant par I et par D_2 la droite située dans le même plan et passant par J. Ces 2 droites ne sont pas rationnelles, mais conjuguées dans le corps $R(\theta)$. Un plan passant par D_1 coupe S suivant une conique γ qui admet une infinité de transformations birationnelles à coefficients rationnels en elle-même. Pour définir une telle transformation, on peut remarquer que γ coupe la droite D_4 située dans le plan $x = a_1$ et passant par J ; on peut définir le transformé d'un point M de γ en définissant le transformé du plan déterminé par M et D_4. On obtient ainsi une transformation T de chacune des sections de S par les plans passant par D_1, donc une transformation de S en elle-même. La transformation conjuguée $\overline{T}$ de T (pour laquelle la droite D_4 est remplacée par la droite D_3 du plan $x = a_1$ et passant par I) définit une transformation de chacune des sections de S par les plans passant par D_2 ; ces sections sont les coniques $\bar{\gamma}$ conjugués des coniques γ. Les couples T, $\overline{T}$ dépendent d'un seul paramètre rationnel ; la droite qui joint les transformées M' et $\overline{M}'$ d'un couple fixe de points conjugués M, $\overline{M}$ par ses différentes transformations engendre une quadrique Q. Cette quadrique Q coupe S suivant 3 coniques : le lieu γ de M', le lieu $\bar{\gamma}$ de $\overline{M}'$ et une conique dont le plan passe par D_0 qui est le lieu du composé $P' = M' * \overline{M}'$. Ces transformations T font donc encore partie du groupe cherché ; analytiquement, ce sont les transformations de S qui remplacent

$(y + \theta z)/(x - a_1)$ et $(y - \theta z)/x$ par $(y + \theta z)\rho/(x - a_1)\bar{\rho}$ et $(y - \theta z)/x$.

On obtient des transformations analogues en changeant le rôle des 3 plans $x = 0$, $x = a_1$, $x = a_2$. L'ensemble des transformations obtenues et de leurs produits est le groupe cherché.

A. WEIL a montré qu'une classe du groupe G par rapport au groupe $2G$ est formée par l'ensemble des points rationnels de G dont les coordonnées x , y , z vérifient :

$$x = d\,\alpha^2 , \quad x - a_1 = d_1\,\alpha_1^2 , \quad x - a_2 = d_2\,\alpha_2^2 ,$$

où d , d_1 , d_2 sont 3 entiers rationnels fixes et où α, α_1 , α_2 sont 3 nombres rationnels arbitraires. Il en a déduit que le groupe quotient $G/2G$ est fini en montrant en outre que les triplets d , d_1 , d_2 ne peuvent prendre qu'un nombre fini de valeurs : d doit diviser $a_1 a_2$, d_1 doit diviser $a_1(a_1 - a_2)$ et d_2 doit diviser $a_2(a_1 - a_2)$. Ces résultats se transposent facilement aux points rationnels de S .

La formule :

$$x = \frac{(x_1 y_2 - x_2 y_1)^2 - a(x_1 z_2 - x_2 z_1)^2}{x_1 x_2 (x_1 - x_2)^2}$$

montre que, si x_2 est la norme d'un nombre de $R(\theta)$, l'abcisse x du composé de x_1 , y_1 , z_1 et x_2 , y_2 , z_2 se déduit de celle de x_1 par multiplication par la norme d'un nombre de $R(\theta)$. Les formules :

$$x - a_1 = \frac{[(x_1 - a_1)y_2 - (x_2 - a_1)y_1]^2 - a[(x_1 - a_1)z_2 - (x_2 - a_1)z_1]^2}{(x_1 - a_1)(x_2 - a_1)(x_1 - x_2)^2}$$

$$x - a_2 = \frac{[(x_1 - a_2)y_2 - (x_2 - a_2)y_1]^2 - a[(x_1 - a_2)z_2 - (x_2 - a_2)z_1]^2}{(x_1 - a_2)(x_2 - a_2)(x_1 - x_2)^2}$$

montrent que si $(x_2 - a_1)$ et $(x_2 - a_2)$ sont les normes de nombres de $R(\theta)$, les différences $(x - a_1)$ et $(x - a_2)$ se déduisent de $(x_1 - a_1)$ et de $(x_1 - a_2)$ par multiplications par des normes de nombres de $R(\theta)$.

Réciproquement, si les quotients x_1/x_2 , $(x_1 - a_1)/(x_2 - a_1)$, $(x_1 - a_2)/(x_2 - a_2)$ sont les normes de nombres de $R(\theta)$, le composé x , y , z des points x_1 , y_1 , z_1 et x_2 , y_2 , z_2 vérifie les conditions :

$$x = \alpha^2 - a\,\beta^2 \quad , \quad x - a_1 = \alpha_1^2 - a\,\beta_1^2 \quad , \quad x - a_2 = \alpha_2^2 - a\,\beta_2^2$$

avec α, β, α_1, β_1, α_2, β_2 rationnels, donc est le composé de 2 points conjugués de S dans $R(\Theta)$.

D'autre part, l'abcisse x de tout point rationnel de S vérifie des relations de la forme :

$$x = d(\alpha^2 - a\,\beta^2) \quad , \quad x - a_1 = d_1(\alpha_1^2 - a\,\beta_1^2) \quad , \quad x - a_2 = d_2(\alpha_2^2 - a\,\beta_2^2)$$

où α, β, α_1, β_1, α_2, β_2 sont des nombres rationnels arbitraires, où d est un entier rationnel qui divise $a_1 a_2$, d_1 un entier qui divise $a_1(a_1 - a_2)$ et d_2 un entier qui divise $a_2(a_2 - a_1)$.

Ce qui montre que tout point rationnel de S correspond à un point rationnel de l'une des variétés en nombre fini S_{d,d_1,d_2} :

$$\alpha^2 - a\,\beta^2 = \alpha_1^2 - a\,\beta_1^2 + a_1 = \alpha_2^2 - a\,\beta_2^2 + a_2 \quad .$$

Si d, d_1, d_2 vérifie les conditions précédentes, il est néanmoins possible que S_{d,d_1,d_2} ne contienne aucun point rationnel. Mais si cette variété contient un premier point rationnel N_1, considérons le point P_1 de S correspondant et construisons le point P obtenu par 2 compositions successives :

$$P = P_1 \star (M \star \overline{M})$$

où M est un point arbitraire de S à coordonnées dans $R(\Theta)$. Les propriétés précédentes montrent que P correspond à un point N de la même variété S_{d,d_1,d_2}, que P_1 et que tout point rationnel de cette variété correspond à un point P de cette forme. Or on peut obtenir les coordonnées de $M \star \overline{M}$, donc aussi celles de P et de N, par des expressions simplement rationnelles à coefficients rationnels de 4 paramètres rationnels λ_1, λ_2, μ_1, μ_2.

Ces résultats permettent d'obtenir tous les points rationnels de S pourvu qu'on sache reconnaître les variétés de la forme :

$$\alpha^2 - a\,\beta^2 = \alpha_1^2 - a\,\beta_1^2 + a_1 = \alpha_2^2 - a\,\beta_2^2 + a_2$$

qui contiennent des points rationnels. La recherche des points rationnels sur S se ramène à celle des points rationnels sur un nombre fini de telles variétés. Les points rationnels d'une de ces variétés s'obtiennent au moyen d'une représentation simplement rationnelle à coefficients rationnels.

Remarquons que les démonstrations précédentes n'exigent pas l'utilisation de la méthode de descente infinie, comme l'exigent les démonstrations complètes concernant les points rationnels sur une cubique C.

Pour simplifier l'exposé, j'ai envisagé seulement les surfaces cubiques S de la forme :

$$y^2 - az^2 = P(x)$$

où $P(x)$ est un polynôme du troisième degré décomposable en facteurs rationnels. Mais il est possible de traiter également le cas où $P(x)$ est un polynôme du troisième degré indécomposable dans le corps des nombres rationnels. Il suffit de transposer directement les méthodes utilisées par A. WEIL pour les points rationnels de cubiques :

$$y^2 = P(x)$$

avec $P(x)$ polynôme du troisième degré indécomposable dans le corps des nombres rationnels.

Par contre, il semble malaisé de généraliser les méthodes précédentes à toutes les surfaces cubiques contenant une droite rationnelle.

BIBLIOGRAPHIE

[1] 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.

[2] POINCARÉ (Henri). - Sur les propriétés arithmétiques des courbes algébriques, J. Math. pures et appl., Série 5, t. 7, 1901, p. 161-233.

[3] WEIL (André). - Sur un théorème de Mordell, Bull. Sc. math., Série 2, t. 54, 1930, p. 179-192.