Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 5 (1959)
Heft: 3: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: POINTS RATIONNELS SUR CERTAINES COURBES ET SURFACES CUBIQUES
Autor: Chatelet, F.
DOI: https://doi.org/10.5169/seals-35486

POINTS RATIONNELS SUR CERTAINES COURBES ET SURFACES CUBIQUES

par F. CHATELET, Besançon

(Reçu le 31 juillet 1959.)

La recherche des points à coordonnées rationnelles (en abrégé points rationnels) sur une variété algébrique est un problème mathématique très ancien; on en trouve des exemples dans les œuvres de Diophante au IIIe siècle de notre ère. Ce problème a fait l'objet de travaux de mathématiciens les plus célèbres, tels Fermat, Euler, Lagrange, Gauss, Hilbert, Poincaré. Pourtant il n'est entièrement résolu que pour des variétés très particulières [1].

1. L'étude des points rationnels sur certaines courbes cubiques a été abordée par de nombreux auteurs depuis Fermat. Mais c'est seulement H. Poincaré [2] qui a proposé une méthode générale qui s'applique à toutes les courbes de genre un. Cette méthode a été perfectionnée par L. J. Mordell et A. Weil [3]; pourtant, comme nous le préciserons ultérieurement, elle ne permet l'étude complète des points rationnels sur ces courbes que dans des cas particuliers.

La méthode de Poincaré, Mordell et Weil nécessite en général l'utilisation des propriétés des idéaux de nombres d'un corps algébrique convenable. Toutefois, l'utilisation de tels idéaux peut être évitée pour une catégorie relativement importante de cubiques, les cubiques de la forme:

$$y^2 = x\,(x^2 + \mathrm{C}x + \mathrm{D})$$

où C et D sont des nombres rationnels donnés, x et y sont les coordonnées rationnelles cherchées. On trouvera un exposé élémentaire et détaillé de ce cas dans un mémoire récent de A. Buquet [4]. Pour simplifier un peu l'exposé, nous considérons seulement dans ce mémoire le cas plus particulier des cubiques de la forme:

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

où a_1 et a_2 sont des nombres rationnels donnés. Sans entrer dans le détail des démonstrations, nous rappelons d'abord les résultats essentiels concernant les points rationnels sur ces courbes.

La représentation d'une cubique de genre un par des fonctions elliptiques permet d'introduire une composition entre les points de cette cubique: le composé, ou somme, de deux points de la cubique est le point dont l'argument elliptique est la somme des arguments des deux points composants. Cette définition peut encore être traduite par une condition géométrique: le composé de trois points alignés est indépendant de la droite qui joint ces points. La composition ainsi définie dépend du choix de la représentation par fonctions elliptiques ou du choix de la somme de trois points alignés. Si cette somme est un point rationnel, l'ensemble des points rationnels sur la cubique forme un groupe additif. En particulier, pour les cubiques C de la forme:

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

on peut choisir pour somme de trois points alignés le point à l'infini sur cette cubique; comme ce point est un point d'inflexion, il est l'élément nul (ou neutre) du groupe G ainsi obtenu.

L'ensemble des doubles de G (obtenus en composant avec eux-mêmes les points de G) forme un sous-groupe 2G de G. On montre que les éléments du groupe 2G sont les points rationnels sur C tels que x, $x - a_1$ et $x - a_2$ sont des carrés parfaits. Un élément du groupe quotient G/2G, c'est-à-dire une classe du groupe G par rapport à son sous-groupe 2G, est un ensemble de points rationnels sur C tels que:

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

où α, α_1, α_2 sont des nombres rationnels arbitraires et où d, d_1, d_2 sont des nombres entiers rationnels fixes vérifiant les deux conditions:

1° le produit $dd_1\,d_2$ est un carré parfait;

2° chacun des entiers d, d_1, d_2 n'a aucun facteur carré.

Ces conditions entraînent que d divise $a_1\,a_2$, d_1 divise a_1 $(a_1 - a_2)$ et d_2 divise a_2 $(a_1 - a_2)$. Il n'existe donc qu'un nombre fini de triplets d, d_1, d_2 vérifiant les conditions précédentes; le groupe quotient G/2G est fini.

Toutefois, les résultats précédents ne suffisent pas pour construire le groupe quotient G/2G. En effet, un triplet d, d_1, d_2 peut correspondre à un système

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

sans solution rationnelle; un tel triplet ne correspond à aucun élément du groupe quotient G/2G. Les conditions imposées au triplet d, d_1, d_2 permettent seulement de construire un groupe contenant le groupe G/2G, sans qu'on sache discerner les éléments de ce groupe qui appartiennent à G/2G.

On montre ensuite que le groupe G admet une base finie qui peut être déduite d'un ensemble de points rationnels sur C représentant les différents éléments de G/2G. Une base de G est un ensemble fini de points rationnels M_1, M_2, ..., M_r sur C tel que tout point rationnel sur C peut être obtenu par une composition convenable des points de base:

$$M = n_1 M_1 + n_2 M_2 + \ldots + n_r M_r ,$$

où n_1, n_2, ..., n_r sont des entiers. Comme la composition peut être définie par des opérations rationnelles sur les coordonnées des points considérés, ce résultat montre que tout point rationnel sur C peut être déduit par des opérations rationnelles sur les points de base.

Puisqu'on ne sait pas encore construire le groupe G/2G, on ne sait pas obtenir une base des points rationnels sur une cubique C. Toutefois certains auteurs ont pu obtenir de telles bases pour des cubiques particulières (pour des valeurs numériques convenablement choisies des coefficients, ou même pour des coefficients vérifiant des conditions arithmétiques convenables) [5].

2. L'étude des points rationnels sur certaines surfaces cubiques a été abordée par divers auteurs. Les résultats les plus étendus sont dus à B. Segre [6], mais sont encore très incomplets. Je vais traiter ici le cas d'une classe nouvelle de surfaces cubiques dont l'étude présente de grandes analogies avec celle des courbes cubiques.

B. Segre a proposé d'utiliser une notion de composition entre les points rationnels d'une surface cubique définie par la même condition gréométrique que pour les courbes cubiques: la somme de trois points alignés est constante, par exemple nulle. Malheu-

reusement, cette notion de composition ne permet pas d'introduire une structure de groupe dans l'ensemble des points rationnels pour deux raisons:

1° le composé d'un point rationnel avec lui-même n'est pas déterminé de façon unique: ce composé est l'un quelconque des points rationnels situé sur l'intersection de la surface et du plan tangent au point considéré;

2° la composition ainsi définie n'est pas associative; la somme de trois points dépend de la façon d'obtenir cette somme.

Pour ces raisons, cette notion de composition n'a conduit qu'à des résultats secondaires.

Mais, si on étudie la méthode de Poincaré-Mordell-Weil, on peut remarquer qu'elle n'utilise pas toutes les propriétés qui résultent de la structure de groupe introduite dans l'ensemble des points rationnels sur une cubique. Les propriétés qui semblent les plus importantes dans cette démonstration sont l'existence d'un sous-groupe 2G défini par une condition simple et la possibilité de répartir les éléments de G en classes par rapport à ce sous-groupe. Or il est possible d'obtenir des propriétés analogues dans d'autres structures que celle de groupe.

D'autre part, toute surface cubique à coefficients rationnels admet des représentations birationnelles à coefficients algébriques. En particulier, la surface S:

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

où a, a_1 et a_2 sont trois nombres rationnels donnés admet la représentation à cofficients quadratiques:

$$x = \lambda\mu$$

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

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

où λ et μ sont deux paramètres et où θ est le nombre quadratique défini par:

$$\theta^2 = a\ .$$

Cette représentation permet d'obtenir tous les points de S à coordonnées dans le corps R (θ) engendré par θ; il suffit de considérer toutes les valeurs de λ et μ dans R (θ).

Si θ est rationnel, c'est-à-dire si a est carré parfait, le résultat précédent permet d'obtenir tous les points rationnels sur S.

Supposons donc θ irrationnel et désignons par $\overline{\theta} = -\theta$ son conjugué. Plus généralement, désignons par $\overline{\alpha}$ le conjugué d'un nombre α de $R(\theta)$ et par $\overline{M}$ le point dont les coordonnées $\overline{x}$, $\overline{y}$, $\overline{z}$ sont les conjuguées de celles d'un point M de $R(\theta)$ (c'est-à-dire d'un point M dont les coordonnées x, y, z sont des nombres du corps $R(\theta)$).

Considérons le composé de deux points conjugués M et $\overline{M}$ de $R(\theta)$ sur S, c'est-à-dire le troisième point d'intersection de S et de la droite qui joint M et $\overline{M}$. Cette droite peut être définie par des équations à coefficients rationnels, puisque les fonctions symétriques des coordonnées de M et $\overline{M}$ sont des nombres rationnels. L'intersection de cette droite avec S est formée par les deux points conjugués M et $\overline{M}$ et un troisième point P dont les coordonnées sont des fonctions symétriques à coefficients rationnels de celles de M et $\overline{M}$, donc sont rationnelles. Il est d'ailleurs facile d'écrire les expressions des coordonnées X, Y, Z de P en fonction des coordonnées x, y, z de M:

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

$$Y = \frac{y - \overline{y}}{x - \overline{x}}\,X + \frac{x\overline{y} - \overline{x}y}{x - \overline{x}}, \qquad Z = \frac{z - \overline{z}}{x - \overline{x}}\,X + \frac{x\overline{z} - \overline{x}z}{x - \overline{x}}$$

On peut aussi exprimer X, Y, Z en fonction des paramètres λ, μ de M, par exemple:

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

Les coordonnées Y et Z peuvent être déduites des formules:

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

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

Ces formules montrent que X, Y, Z sont rationnels et que de plus X est le produit de deux nombres conjugués de $R(\theta)$,

c'est-à-dire de la forme $\alpha^2 - a\beta^2$ avec α et β rationnels. Comme les trois expressions x, $x - a_1$ et $x - a_2$ jouent des rôles symétriques dans l'équation de S, il y a lieu d'étudier également la forme de $X - a_1$ et de $X - a_2$:

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

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

On constate encore que $X - a_1$ et $X - a_2$ sont des produits de nombres conjugués de R (θ).

Réciproquement, considérons un point P de coordonnées X, Y, Z telles que X, $X - a_1$, $X - a_2$ soient les normes de nombres de R (θ), c'est-à-dire telles qu'il existe des nombres rationnels α, β, α_1, β_1, α_2, β_2 vérifiant les relations:

$$X = \alpha^2 - a\,\beta^2\ ,$$
$$X - a_1 = \alpha^2{}_1 - a\,\beta^2{}_1\ ,$$
$$X - a_2 = \alpha^2{}_2 - a\,\beta^2{}_2\ .$$

S'il existe des nombres λ, μ du corps R (θ) vérifiant les relations:

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

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

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

le composé du point M de S de paramètres λ, μ et de son conjugué a même abscisse que P. Or on constate que ce système de relations est équivalent au système de deux relations:

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

ou encore au système:

$$\lambda = \alpha - \alpha_2 - \theta\,(\beta - \beta_2)\ , \qquad \mu = \alpha - \alpha_1 + \theta\,(\beta - \beta_1)\ .$$

Les coordonnées Y_1, Z_1 du composé de M et de $\bar{M}$ peuvent être différentes des coordonnées Y et Z de P. Mais, si on remplace le point M par le point M′ de paramètres:

$$\lambda' = \frac{\lambda\,\rho}{\rho}\ , \qquad \mu' = \frac{\mu\,\bar{\rho}}{\rho}$$

où ρ est un nombre arbitraire de R (θ), le composé de M′ et de $\overline{M}'$ a même abscisse X que le composé de M et de $\overline{M}$; par contre, ses coordonnées Y'_1 et Z'_1 vérifient:

$$Y_1' + \theta Z_1' = (Y_1 + \theta Z_1)\,\frac{\bar{\rho}}{\rho}$$

$$Y_1' - \theta Z_1' = (Y_1 - \theta Z_1)\,\frac{\bar{\rho}}{\rho}$$

Or il est possible de choisir ρ de manière que:

$$Y + \theta Z = (Y_1 + \theta Z_1)\,\frac{\rho}{\bar{\rho}}\ , \qquad Y - \theta\, Z = (Y_1 - \theta Z_1)\,\frac{\rho}{\rho}$$

puisque:

$$Y^2 - aZ^2 = X\,(X - a_1)\,(X - a_2) = Y_1^2 - aZ_1^2$$

Pour un tel choix de ρ, le point P est le composé de M′ et de $\overline{M}'$. Il y a lieu de remarquer que les nombres rationnels α, β, α_1, β_1, α_2, β_2 ne sont pas déterminés de façon unique par X, Y, Z; il existe une infinité de couples M, $\overline{M}$ dont le composé est le point P donné.

Nous avons ainsi obtenu le résultat:

Pour qu'un point rationnel P *sur* S, *de coordonnées* X, Y, Z, *soit le composé de deux points conjugués du corps* R (θ), *il faut et il suffit qu'il existe des nombres rationnels* α, β, α_1, β_1, α_2, β_2 *telles que:*

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

Ce résultat est analogue au résultat de Poincaré-Mordell-Weil:

Pour qu'un point rationnel P *sur* C *de coordonnées* X, Y *soit le double d'un point rationnel de* C, *il faut et il suffit qu'il existe des nombres rationnels* α, α_1, α_2 *tels que:*

$$X = \alpha^2\ , \qquad X - a_1 = \alpha_1^2\ , \qquad X - a_2 = \alpha_2^2$$

3. Avant de poursuivre l'étude des points rationnels sur S, précisons encore certains aspects du théorème précédent.

Considérons d'abord un point P sur la cubique C:

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

et cherchons les points M tels que:

$$P = 2M\ .$$

Les propriétés classiques des fonctions elliptiques montrent qu'il existe quatre points qui vérifient cette relation et que la différence de deux quelconques d'entre eux a pour argument elliptique la moitié d'une période. Cette différence est donc l'un des quatre points:

$$\begin{aligned} x_1 &= 0 \ , & y_1 &= 0 \ , \\ x_2 &= a_1 \ , & y_2 &= 0 \ , \\ x_3 &= a_2 \ , & y_3 &= 0 \ , \\ x_4 &= \infty \ , & y_4 &= \infty \ . \end{aligned}$$

Au sens de l'addition des points sur C, ces quatre points forment un produit direct de deux groupes cycliques d'ordre 2. La théorie de Galois montre alors que les coordonnées de M peuvent être déduites de celles de P par des opérations rationnelles et l'extraction de deux racines carrées. Le théorème précédent de Poincaré-Mordell-Weil précise seulement qu'on peut choisir pour ces deux racines carrées celles de $X - a_1$ et de $X - a_2$. (Si $X - a_1$ et $X - a_2$ sont carrés parfaits, il en est de même de X d'après l'équation de C).

Considérons maintenant un point rationnel P sur la surface S:

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

et cherchons les points M de $R(\theta)$ sur S tels que le composé de M et de son conjugué $\overline{M}$ soit le point P considéré. Ces points, s'ils existent, sont en nombre infini et se déduisent les uns des autres par des correspondances sur S formant un groupe que nous allons préciser.

En fait, il est plus commode de construire le groupe des correspondances sur S qui conservent l'abscisse du composé de M et de son conjugué $\overline{M}$; le groupe cherché des correspondances qui conservent les trois coordonnées de ce composé s'en déduit comme groupe-quotient.

La surface S coupe le plan à l'infini suivant une droite unique D_0 (la droite à l'infini du plan yOz). Sur cette droite D_0 existent deux points conjugués I et $\overline{I}$ multiples pour la surface; ce sont les intersections de cette droite et des deux plans conjugués:

$$\begin{aligned} P \quad & y + \theta z = 0 \\ \overline{P} \quad & y - \theta z = 0 \ . \end{aligned}$$

En chacun de ces points, la surface admet un plan tangent multiple, respectivement le plan P en I et le plan $\overline{P}$ en $\overline{I}$. La section de S par un plan passant par D_0 (plan pour lequel x est constant) est une conique qui passe par I et $\overline{I}$ et est tangente en ces points aux plans P et $\overline{P}$ respectivement.

Considérons un point M de R (θ) sur S et construisons la conique γ intersection de S et du plan passant par M et D_0. La conique $\overline{\gamma}$ conjuguée de γ (définie par les équations obtenues en remplaçant les coefficients d'un système d'équations de γ par leurs conjugués) est l'intersection de S et du plan défini par D_0 et le conjugué $\overline{M}$ de M. Puisque les coniques γ et $\overline{\gamma}$ ont en commun les points $\overline{I}$ et I, il existe une quadrique Q et une seule qui contient γ, $\overline{\gamma}$ et la droite $M\overline{M}$. Cette quadrique Q peut être définie par une équation à coefficients rationnels. Elle coupe S suivant les coniques γ, $\overline{\gamma}$ et suivant une troisième conique Γ dont le plan est rationnel.

Montrons que le plan de Γ passe par D_0. En effet, les intersections de Q et S par un plan Π passant par D_0 sont deux coniques qui contiennent I et $\overline{I}$ et sont tangentes en ces points aux intersections de Π avec les plans P et $\overline{P}$. Ou bien ces deux coniques n'ont aucun point d'intersection autre que I et $\overline{I}$, ou bien ces deux coniques sont confondues. Choisissons le plan Π déterminé par D_0 et un point P de Γ distinct de I et $\overline{I}$; les deux coniques intersections de Π avec S et Q ont en commun les points I, $\overline{I}$ et P, donc sont confondues. Cette conique unique fait partie de l'intersection de S et Q et est distincte de γ et de $\overline{\gamma}$; c'est donc la conique Γ. Ce qui montre que le plan de cette conique Γ passe par D_0. On sait qu'une quadrique Q qui contient une génératrice rationnelle contient une infinité de génératrices rationnelles [7]. Une telle génératrice coupe les coniques γ et $\overline{\gamma}$ en deux points conjugués M′ et $\overline{M}'$ et coupe Γ en un point rationnel P′ qui est le composé de M′ et de $\overline{M}'$. Or il existe une infinité de correspondances birationnelles à coefficients rationnels sur Q qui transforment chaque génératrice rationnelle en une génératrice rationnelle et qui conservent en outre les intersections de Q par les plans qui contiennent D_0. Une telle correspondance transforme un point M de γ en un point M′ de γ; en outre, les composés des points conjugués M, $\overline{M}$ et M′, $\overline{M}'$ sont

sur la conique Γ dont le plan passe par D_0, donc ont même abscisse. Ainsi cette correspondance conserve l'abscisse du composé de deux points conjugués. Toutefois elle n'est définie que pour les points de la conique γ.

Mais considérons les homographies H de l'espace qui conservent les plans passant par D_0, et qui laissent invariants les points I et $\bar{I}$ et les plans P et $\bar{P}$. Une telle homographie transforme toute conique qui est située dans un plan contenant D_0, qui passe par I et $\bar{I}$ et qui est tangente respectivement en ces points aux plans P et $\bar{P}$ en une conique qui vérifie les mêmes conditions. Si une homographie H conserve en outre une des coniques précédentes, elle les conserve toutes. Une homographie H vérifiant cette dernière condition conserve la surface cubique S car elle peut être engendrée par des coniques vérifiant les conditions précédentes. Une quadrique Q déterminée comme précédemment par un point arbitraire M de R (θ) sur S peut aussi être engendrée par de telles coniques. Donc elle est transformée en elle-même par l'homographie H et chacune de ses génératrices est transformée en une génératrice puisque H transforme toute droite en une droite. Si H est définie par des relations à coefficients rationnels, elle transforme toute génératrice rationnelle de Q en une génératrice rationnelle. Ainsi une homographie H qui vérifie toutes les conditions précédentes détermine sur chaque quadrique Q une correspondance du type précédent; H conserve donc le composé de chaque point de R (θ) sur S et de son conjugué. Une telle homographie H doit vérifier les quatre conditions:

1° H conserve chaque plan passant par D_0, donc l'abscisse x;

2° H conserve les plans P et $\bar{P}$, donc multiplie par un coefficient constant de proportionnalité $y + \theta z$ et $y - \theta z$;

3° H conserve les coniques passant par I et $\bar{I}$ et tangentes aux plans P et $\bar{P}$, donc conserve le produit $(y + \theta z)(y - \theta z)$;

4° l'homographie $\overline{H}$ conjuguée de H est confondue avec H.

Ces homographies H peuvent donc être définies par les systèmes de relations de la forme:

$$\frac{\rho\,(y' + \theta z')}{\bar{\rho}\,(y + \theta z)} = \frac{\bar{\rho}\,(y' - \theta z')}{\rho\,(y - \theta z)} = \frac{x'}{x} = 1$$

On constate que ces homographies forment un groupe isomorphe au groupe multiplicatif des nombres de R (θ) de la forme $\frac{\overline{\rho}}{\rho}$, c'est-à-dire des nombres de R (θ) de norme unité.

D'autre part, la surface S contient aussi les six droites intersections des plans P et $\overline{P}$ par les trois plans $x = 0$, $x = a_1$ et $x = a_2$. Désignons par D_1 la droite située dans le plan $x = 0$ et le plan P; par D_2 la droite située dans le plan $x = 0$ et le plan $\overline{P}$. Ces deux droites ont leurs coefficients dans R (θ) et sont conjuguées l'une de l'autre. Considérons un point M de R (θ) sur S et la conique γ intersection de S et du plan déterminé par D_1 et M. Cette conique passe par I et y est tangente au plan de l'infini; elle coupe D_1 en I et en un autre point variable avec γ. La conique $\overline{\gamma}$ conjuguée de γ est l'intersection de S et du plan déterminé par D_2 et $\overline{M}$. L'intersection des plans des coniques γ et $\overline{\gamma}$ coupe S au point commun à D_1 et D_2 et en deux autres points qui sont situés sur γ et $\overline{\gamma}$. Il existe donc une quadrique Q qui contient les coniques γ, $\overline{\gamma}$ et la droite $M\overline{M}$. Cette quadrique coupe S suivant les coniques γ et $\overline{\gamma}$ et suivant une troisième conique Γ dont le plan est rationnel.

Montrons que le plan de la conique Γ passe par D_0. En effet, les intersections de Q et de S par un plan Π passant par D_0 sont deux coniques qui passent par les quatre points d'intersection du plan Π et des deux coniques γ et $\overline{\gamma}$; un tel plan Π coupe γ en I et en un point variable et coupe $\overline{\gamma}$ en $\overline{I}$ et en un point variable. Ou bien ces deux intersections n'ont pas de point commun autre que les quatre points précédents; ou bien elles sont confondues. Choisissons le plan Π déterminé par D_0 et un point P de Γ situé ni sur $\overline{\gamma}$ ni sur γ; les deux coniques intersections de Q et S par ce plan ont en commun les quatre points situés sur γ ou sur $\overline{\gamma}$ et le point P, donc sont confondues. Cette conique unique fait partie de l'intersection de Q et de S et est distincte de γ et de $\overline{\gamma}$; c'est donc la conique Γ. Ce qui montre que le plan de la conique Γ passe par D_0.

La quadrique Q qui contient la génératrice rationnelle $M\overline{M}$ contient une infinité de génératrices rationnelles. Une telle génératrice coupe les coniques γ et $\overline{\gamma}$ en deux points conjugués M′ et $\overline{M}'$ et coupe Γ en un point rationnel P′ qui est le composé

de M′ et de $\overline{M}'$; ce composé P′ a même abscisse que le composé P de M et de $\overline{M}$, puisque P et P′ sont tous deux sur la conique Γ dont le plan passe par D_0. Il existe des correspondances birationnelles à coefficients rationnels entre les génératrices rationnelles de Q. Mais il n'est pas possible de définir une telle correspondance par une transformation entre les points de Q qui conserve à la fois les plans passant par D_1 et les plans passant par D_2. Toutefois, considérons une correspondance birationnelle à coefficients rationnels T entre les droites d'un des systèmes de génératrices de Q. La correspondance T engendre une correspondance birationnelle t à coefficients dans R (θ) entre les points de la conique γ: le transformé par t d'un point M de γ est obtenu en prenant l'intersection de γ et de la transformée par T de la génératrice du système considéré qui passe par M. La correspondance T engendre de la même façon une correspondance entre les points de $\overline{\gamma}$; cette correspondance est d'ailleurs la conjuguée $\bar{t}$ de t. Donc $\bar{t}$ transforme le conjugué $\overline{M}$ d'un point M de γ en le conjugué $\overline{M}'$ du transformé M′ de M par t; par suite, T conserve l'abscisse du composé d'un point de R (θ) sur γ et de son conjugué.

Pour déterminer une correspondance birationnelle entre les génératrices d'un système de la quadrique Q, il suffit de connaître la correspondance qu'elle engendre sur l'intersection de Q par un plan fixe. En effet, il ne passe qu'une génératrice du système considéré par chaque point de cette intersection. Choisissons l'intersection de Q par le plan $x = 0$; c'est une conique qui passe par I et $\overline{I}$. Elle peut donc être définie par une équation de la forme:

$$(y + \theta z + \lambda)(y - \theta z + \bar{\lambda}) = d$$

où λ et $\bar{\lambda}$ sont deux nombres conjugués de R (θ) et où d est un nombre rationnel. Les coefficients λ, $\bar{\lambda}$, d peuvent être exprimés en fonction des coordonnées du point M. Parmi les correspondances à coefficients rationnels sur cette conique, celles qui conservent les points I et $\overline{I}$ peuvent être définies dans tout le plan et pour toutes les coniques qui passent par ces deux points. Les formules de ces transformations sont

$$y' + \theta z' + \lambda = \frac{\bar{\rho}}{\rho}(y + \theta z + \lambda) \quad ,$$

$$y' - \theta z' - \bar{\lambda} = \frac{\rho}{\bar{\rho}} (y - \theta z + \bar{\lambda}).$$

Elles forment donc un groupe isomorphe au groupe multiplicatif des nombres de R (θ) de norme unité.

Les correspondances ainsi obtenues ne sont pas toutes les correspondances qui conservent l'abscisse du composé d'un point de R (θ) sur S et de son conjugué. En effet, nous n'avons pas utilisé toutes les correspondances birationnelles à coefficients rationnels entre les points d'une quadrique Q. Mais, si nous considérons les deux droites D_3 et D_4 situées dans le plan $x = a_1$, nous pouvons construire un nouveau groupe isomorphe au groupe multiplicatif des nombres de R (θ) de norme unité. De même, en utilisant les deux droites D_5 et D_6 situées dans le plan $x = a_2$, nous pouvons construire un troisième groupe isomorphe aux deux précédents. On peut montrer que le produit direct de ces trois groupes isomorphes entre eux est le groupe de toutes les correspondances qui conservent l'abscisse du composé de deux points conjugués arbitraires de R (θ) sur S.

Le groupe des transformations qui conservent le composé de deux points conjugués de R (θ) peut être obtenu comme groupe quotient: il est donc isomorphe au produit direct de deux groupes isomorphes au groupe multiplicatif des nombres de R (θ) de norme unité.

La théorie de Galois permet donc de montrer qu'un point rationnel P sur S est le composé de deux points conjugués de R (θ) sur S si et seulement si deux fonctions convenables des coordonnées de P sont normes de nombres de R (θ). Le résultat final du paragraphe précédent précise seulement qu'on peut choisir ces deux fonctions égales respectivement à $X - a_1$ et $X - a_2$.

4. Nous avons distingué, dans l'ensemble des points rationnels sur S, le sous-ensemble (P) formé par les points P dont l'abcisse X vérifie les relations:

$$X = \alpha^2 - a\beta^2 , \qquad X - a_1 = \alpha_1^2 - a\beta_1^2 , \qquad X - a_2 = \alpha^2{}_2 - a\beta_2^2$$

avec α, β, α_1, β_1, α_2, β_2 nombres rationnels.

Il s'agit maintenant d'étudier les points rationnels sur S qui ne font pas partie du sous-ensemble (P), c'est-à-dire les

points M d'abscisse x, tel que l'un au moins des trois nombres x, $x - a_1$, $x - a_2$ n'est pas norme d'un nombre de R (θ).

Or la formule qui donne l'abscisse x du composé des points M′ et M″:

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

montre que cette abscisse x est le produit des abscisses x' et x'' de M′ et M″ et de la norme d'un nombre de R (θ). Les formules analogues:

$$x - a_1 = \frac{[(x' - a_1) y'' - (x'' - a_1) y']^2 - a [(x' - a_1) z'' - (x'' - a_1) z']^2}{(x' - a_1) (x'' - a_1) (x' - x'')^2}$$

$$x - a_2 = \frac{[(x' - a_2) y'' - (x'' - a_2) y']^2 - a [(x' - a_2) z'' - (x'' - a_2) z']^2}{(x' - a_2) (x'' - a_2) (x' - x'')^2}$$

montrent aussi que $x - a_1$ est le produit de $x' - a_1$, de $x'' - a_1$ et de la norme d'un nombre de R (θ), et que $x - a_2$ est le produit de $x' - a_2$, de $x'' - a_2$ et de la norme d'un nombre de R (θ).

Répartissons l'ensemble des points rationnels sur S en sous-ensembles de telle manière que, si deux points M′ et M″ appartiennent à un même sous-ensemble, les quotients:

$$\frac{x'}{x''} \quad , \quad \frac{x' - a_1}{x'' - a_1} \quad , \quad \frac{x' - a_2}{x'' - a_2} \quad ,$$

sont normes de nombres de R (θ). Pour construire un tel sous-ensemble, nous pouvons choisir un triplet de nombres rationnels d, d_1, d_2 et considérer tous les points de S qui vérifient les relations:

$$x = d (\gamma^2 - a\delta^2) \ , \quad x - a_1 = d_1 (\gamma_1^2 - a\delta_1^2) \ , \quad x - a_2 = d_2 (\gamma^2{}_2 - a\delta^2{}_2)$$

où γ, δ, γ_1, δ_1, γ_2, δ_2 sont des nombres rationnels arbitraires. Un triplet d, d_1, d_2 détermine ainsi un sous-ensemble, mais inversement un sous-ensemble ne définit chacun des trois nombres d, d_1, d_2 qu'au produit près par une norme d'un nombre de R (θ).

Les résultats précédents montrent que la composition des points de S introduit entre ces sous-ensembles une loi de composition: le composé des deux sous-ensembles déterminés par les deux triplets d', d'_1, d'_2 et d'', d''_1, d''_2 peut être défini par le triplet $d' d''$, $d'_1 d''_1$, $d'_2 d''_2$. Ces sous-ensembles forment alors un groupe pour cette loi de composition. En particulier, le sous-ensemble

distingué (P) est l'unité de ce groupe; nous pouvons obtenir tous les points d'un autre sous-ensemble en composant un de ses points avec tous les points du sous-ensemble distingué (P). On dit que chacun de ces sous-ensembles est une « classe » de points rationnels par rapport au sous-ensemble (P).

Mais un triplet d'entiers rationnels d, d_1, d_2 ne peut déterminer une classe de points rationnels que s'il satisfait à une condition que nous allons expliciter. Le produit $dd_1\,d_2$ de ces trois nombres doit être norme d'un nombre de R (θ); en effet les coordonnées x, y, z d'un point de la classe vérifie l'équation de S, donc:

$$\begin{aligned} y^2 - az^2 &= x\,(x - a_1)\,(x - a_2) \\ &= dd_1\,d_2\,(\gamma^2 - a\delta^2)\,(\gamma_1{}^2 - a\delta_1{}^2)\,(\gamma_2{}^2 - a\delta_2{}^2) \end{aligned}$$

D'autre part, nous avons dit qu'une classe ne détermine chacun des entiers d, d_1, d_2 qu'au produit près par la norme d'un nombre de R (θ); nous allons utiliser ce facteur arbitraire pour simplifier d, d_1, d_2 autant que possible. Or la théorie des entiers d'un corps quadratique [8] montre qu'on peut distinguer deux espèces d'entiers rationnels premiers:

1° ceux qui sont normes d'idéaux premiers de R (θ);

2° ceux qui engendrent des idéaux premiers du corps R (θ).

Tout nombre premier p de la première espèce peut être mis sous la forme du produit d'un entier rationnel choisi parmi un ensemble fini (l'ensemble des normes de représentants des classes d'idéaux du corps R (θ) par la norme d'un nombre de R (θ). Si un tel entier divise l'un des entiers d, d_1, d_2, nous pouvons donc le remplacer par un entier choisi dans l'ensemble fini précédent. Tout nombre premier p de la seconde espèce qui divise la norme d'un nombre de R (θ) figure dans la décomposition en facteurs premiers rationnels de ce nombre avec un exposant pair. Si un tel entier premier p divise le produit $dd_1\,d_2$, il doit soit figurer dans la décomposition de chacun des entiers d, d_1, d_2 avec un exposant pair, soit diviser deux au moins de ces nombres. Mais si p figure dans la décomposition de d, d_1 ou d_2 avec un exposant pair, nous pouvons le remplacer dans ce coefficient par l'unité. Si un tel entier p divise d et d_1, les relations:

$$x = d\,(\gamma^2 - a\,\delta^2) = d_1\,(\gamma_1{}^2 - a\,\delta_1{}^2) + a_1$$

montrent qu'il divise aussi a_1; s'il divise d et d_2, il divise aussi a_2; s'il divise d_1 et d_2, il divise aussi $a_1 - a_2$.

Ainsi, si un triplet d, d_1, d_2 détermine une classe de points rationnels sur S, il peut être remplacé par un triplet dont chaque terme est un produit d'entiers rationnels choisis dans un ensemble fini: ensemble des normes de représentants des classes d'idéaux de R (θ) et des diviseurs premiers de a_1, de a_2 et de $a_1 - a_2$. Les triplets d, d_1, d_2 peuvent donc être choisis dans un ensemble fini. Ce qui démontre le résultat:

Les classes de points rationnels sur S *par rapport au sous-ensemble distingué* (P) *sont en nombre fini.*

Ce résultat est analogue au théorème de Poincaré-Mordell-Weil:

Les classes du groupe G *des points rationnels sur* C *par rapport au sous-groupe* 2G *sont en nombre fini.*

5. Les formules:

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

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

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

permettent d'obtenir les points du sous-ensemble (P) en fonction de deux paramètres λ et μ à valeurs dans R (θ). Or nous pouvons exprimer deux tels paramètres au moyen de quatre paramètres rationnels:

$$\lambda = \lambda_1 + \theta\lambda_2\,, \qquad \mu = \mu_1 + \theta\mu_2\,.$$

Les formules ainsi obtenues expriment rationnellement les coordonnées X, Y, Z d'un point P en fonction de λ_1, λ_2, μ_1, μ_2, les coefficients de ces formules étant rationnels.

Toutefois, les paramètres λ_1, λ_2, μ_1, μ_2 ne peuvent être exprimés rationnellement en fonction des coordonnées X, Y, Z et il existe même une infinité de tels paramètres pour un même point P. Ainsi les points du sous-ensemble distingué (P) s'obtiennent de façon simplement rationnelle en fonction de quatre paramètres rationnels.

Nous avons dit que les points d'une classe par rapport au sous-ensemble (P) s'obtiennent en composant un point fixe de cette classe avec tous les points du sous-ensemble (P). Puisque les points du sous-ensemble (P) ont été obtenus en fonctions rationnelles à coefficients rationnels de quatre paramètres rationnels et que les formules de composition de deux points de S sont rationnelles, nous pouvons aussi obtenir tous les points d'une même classe en fonctions rationnelles de quatre paramètres rationnels. Comme le nombre des classes est fini, nous obtenons le résultat:

Tous les points rationnels sur S *peuvent être obtenus au moyen d'un nombre fini de formules simplement rationnelles en fonction de paramètres rationnels.*

Ce résultat diffère sensiblement du théorème de Poincaré-Mordell-Weil:

Les points rationnels sur la cubique C *peuvent être obtenus par des opérations rationnelles sur les points d'une base finie.*

6. Le résultat du paragraphe précédent ne résoud pas entièrement le problème des points rationnels sur une surface cubique S. En effet, pour obtenir effectivement une représentation simplement rationnelle d'une classe de ces points, nous avons besoin de connaître un point de cette classe. Or nous avons déterminé les différentes classes par des triplets d'entiers rationnels d, d_1, d_2; nous avons obtenu des conditions nécessaires pour qu'un tel triplet puisse représenter une classe, mais nous ne connaissons aucune condition suffisante pour qu'il en soit ainsi. *A fortiori*, nous ne savons pas obtenir un point rationnel d'une classe déterminée par un tel triplet.

Le problème des points rationnels sur une surface cubique S pose encore une question ouverte analogue d'ailleurs à la ques-

tion de Poincaré-Mordell-Weil: déterminer les triplets d, d_1, d_2 qui correspondent effectivement aux classes du groupe G par rapport au sous-groupe 2G.

Enfin, signalons que les résultats précédents peuvent être généralisés aux surfaces cubiques de la forme:

$$y^2 - az^2 = \mathrm{P}(x)$$

où $\mathrm{P}(x)$ est un polynome du troisième degré à coefficients rationnels. Cette généralisation utilise les propriétés des idéaux dans le corps cubique défini par une solution de l'équation:

$$\mathrm{P}(x) = 0 .$$

BIBLIOGRAPHIE

1. On trouvera une bibliographie détaillée sur ces problèmes dans l'ouvrage de Th. Skolem: *Diophantische Gleichungen* (Ergebnisse der mathematik und ihrer Grenzgebiete, Springer, 1938). Les travaux plus récents concernent surtout les courbes et surfaces cubiques.
2. Poincaré, H., Sur les propriétés arithmétiques des courbes algébriques. *J. Math. pures et appl.*, série 5, t. 7, 1901, pp. 161-233.
3. Mordell, L. J., On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge phil. soc.*, t. 21, 1922, pp. 179-192.
   Weil, A., Sur un théorème de Mordell. *Bull. Soc. math.*, série 2, t. 54, 1930, pp. 179-192.
4. Buquet, A., Démonstration élémentaire du théorème de Mordell-Weil pour l'équation diophantienne en nombres rationnels
   $$x(x^2 + \mathrm{C}x + \mathrm{D}) = \mathrm{Z}^2$$
   Mathesis, 1956, pp. 379-190.
5. On trouvera une bibliographie sur ces travaux dans la thèse de G. Billing: Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins. *Nova acta regiae societatis scientiarum Upsaliensis*, série 4, tome 11, 1938.
6. On pourra consulter l'ouvrage de B. Segre: *Arithmetical questions on algebraic varieties*. Londres, 1951.
7. Voir F. Châtelet: Relations entre l'arithmétique et la géométrie sur une quadrique. *Bull. Soc. math.*, 76 (1948), pp. 108-113.
8. On trouvera la théorie des entiers d'un corps quadratique dans le mémoire de D. Hilbert: Theorie der algebraischen Zahlkörper (*Jahresbericht der Deut. Math. Ver.*, 1897 ou traduction française publiée par Hermann) ou dans un mémoire de M. Albert Châtelet qui doit paraître prochainement dans l'*Enseignement mathématique*.