Séminaire Dubreil.
Algèbre et théorie
des nombres

F. Châtelet

Points rationnels sur les surfaces cubiques

Séminaire Dubreil. Algèbre et théorie des nombres, tome 7 (1953-1954), exp. n° 8, p. 1-11
<http://www.numdam.org/item?id=SD_1953-1954__7__A8_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire d'ALGÈBRE
Année 1953/1954
-:-:-:-

POINTS RATIONNELS SUR LES SURFACES CUBIQUES

Conférence faite par F. CHÂTELET, le 20 février 1954

-:-:-:-

Cet exposé est consacré à des questions en cours d'étude. Il pose de nombreux problèmes irrésolus. De plus les méthodes employées et les résultats obtenus ont encore besoin d'être améliorées.

Il s'agit des problèmes que l'on peut énoncer sous la forme générale suivante: Etant donné un polynome du $3^{ème}$ degré à 3 variables x , y , z et à coefficients rationnels, $f(x,y,z)$, on demande s'il existe des ensembles de nombres rationnels x , y , z vérifiant la relation

$$f(x,y,z) = 0 .$$

S'il existe de tels ensembles, on demande un procédé permettant de les obtenir tous.

On dit, en abrégé, que l'on recherche les points rationnels sur la surface cubique définie par la relation précédente.

On peut aussi exprimer ce même problème en coordonnées homogènes :

Etant donné un polynome homogène du $3^{ème}$ degré à 4 variables et à coefficients entiers, $F(x,y,z,t)$, on demande s'il existe des ensembles de nombres entiers (positifs ou négatifs) x , y , z , t, non tous nuls, vérifiant la relation :

$$F(x,y,z,t) = 0$$

et le cas échéant, on demande de les obtenir tous.

Certains cas particuliers de ces problèmes ont été résolus dès le siècle dernier. C'est ainsi que l'on reconnait facilement que la relation :

$$x^3 + y^3 = z^3 + t^3$$

admet des solutions entières x , y , z , t non toutes nulles et que l'on sait les obtenir toutes.

Mais les premières études générales datent seulement de 1940. A cette époque, le géomètre italien Benjamino SEGRE s'est réfugié en Angleterre et a travaillé en collaboration avec l'arithméticien anglais L. J. MORDELL. La confrontation entre les méthodes géométriques et arithmétiques a été particulièrement fructueuse.

Elle a permis de regrouper des résultats hétérogènes et d'arriver à une première vue d'ensemble de ces questions.

On trouvera un exposé général, mais succinct, des résultats obtenus dans un article de B. SEGRE : "Arithmetic upon an algebraic surfaces", Bull. of Amer. Math. Soc., t. 51 (1945). On trouvera des démonstrations plus complètes dans un mémoire du même SEGRE : "On the rational solutions of homogeneous cubic equations in four variables", Mathematicae notes, t. 11 (1951). L'un et l'autre de ces mémoires donnent des indications bibliographiques sur les autres publications dans ce domaine.

Un des résultats les plus importants de MORDELL et SEGRE est le suivant : Une surface cubique non singulière contenant un point rationnel en contient une infinité.

Suivant la notation de l'école italienne, on appelle surface singulière une surface algébrique admettant au moins un point singulier.

La recherche des points rationnels sur les surfaces cubiques singulières présente des particularités ou même est essentiellement différente du même problème pour les surfaces non singulières. C'est ainsi que ce problème pour un cône ou un cylindre cubique revient à la recherche des points rationnels sur une section plane de ce cône ou cylindre, problème qui peut admettre un nombre fini et non nul de solutions. Nous n'étudierons dans la suite que les surfaces non singulières, sauf mention expresse du contraire.

Le résultat précédent a été démontré de plusieurs façons différentes, tant par MORDELL que par SEGRE. On trouvera les démonstrations ou les indications bibliographiques sur ces solutions, dans les mémoires cités antérieurement.

Puisqu'il y a un nombre infini de solutions (ou aucune), il ne peut être question de les obtenir effectivement toutes ; mais seulement d'indiquer un procédé commode pour les construire toutes au moyen d'un nombre infini d'opérations rationnelles. On peut espérer employer un procédé qui réussit pour les courbes planes de genre 0 : chercher une représentation birationnelle à coefficients rationnels sur un plan de la surface cubique donnée. C'est-à-dire que l'on cherche à représenter les points de la surface au moyen de 2 paramètres :

$$x = f(u,v) \quad , \quad y = g(u,v) \quad , \quad z = h(u,v)$$

où f , g et h sont des fractions rationnelles, de manière que u et v s'expriment rationnellement en fonction de x , y , z :

$$u = \varphi(x,y,z) \quad , \quad v = \psi(x,y,z) \quad ,$$

les coefficients de toutes les fractions rationnelles f , g , h , φ , ψ étant rationnels. Alors les points rationnels de la surface cubique correspondent aux valeurs rationnelles des paramètres u et v .

Mais un théorème de SEGRE montre que cet espoir est vain dans le cas général :

Pour qu'il existe une représentation birationnelle à coefficients rationnels d'une surface cubique non singulière sur un plan, il est nécessaire que la surface contienne soit une droite rationnelle, soit un doublet rationnel, soit un triplet rationnel, soit un sextuplet rationnel.

On appelle "droite rationnelle" une droite qui peut être définie par un système d'équations à coefficients rationnels.

SEGRE appelle "doublet rationnel" l'ensemble de 2 droites ne se coupant pas (soit à distance finie, soit à l'infini) qui sont soit rationnelles, soit conjuguées l'une de l'autre dans un corps quadratique (c'est-à-dire que chaque droite peut être définie par un système d'équations à coefficients dans un corps quadratique et que l'on peut passer d'un système à l'autre en opérant sur tous les coefficients l'opération du groupe de GALOIS de ce corps).

SEGRE appelle "triplet rationnel" l'ensemble de 3 droites ne se coupant pas 2 à 2 (ni à distance finie, ni à l'infini) qui ont leurs coefficients dans un corps de degré 3 au plus et dont toute conjuguée (dans le corps des coefficients) appartienne à l'ensemble.

Enfin SEGRE appelle "sextuplet rationnel" l'ensemble de 6 droites ne se coupant pas 2 à 2 qui ont leurs coefficients dans un corps de degré 6 au plus et dont toute conjuguée appartienne à l'ensemble.

Le théorème précédent est démontré dans le mémoire cité des Mathematicae Notae.

SEGRE y ajoute les compléments suivants :

Si une surface cubique non singulière contient un doublet rationnel, elle admet une représentation birationnelle à coefficients rationnels sur un plan.

Pour qu'une surface cubique non singulière contenant un sextuplet rationnel admette une représentation birationnelle à coefficients rationnels, il faut et il suffit qu'elle contienne un point rationnel.

L'exemple le plus simple de surface cubique contenant un doublet rationnel est la surface :

$$x^3 + y^3 = z^3 + t^3$$

Elle contient le doublet rationnel formé par les 2 droites :

$$x + jy = z + jt = 0 \qquad \text{et} \qquad x + j^2y = z + j^2t = 0 \quad ,$$

où j est une racine cubique de l'unité. On en trouve facilement une représentation birationnelle à coefficients rationnels, en séparant les parties réelles et imaginaires des relations :

$$x + jy = (u + jv)(z + jt)$$
$$x + j^2y = (u + j^2v)(z + j^2t)$$
$$z + t = (u^2 - uv + v^2)(x + y)$$

Le résultat sur les surfaces cubiques contenant un sextuplet rationnel les apparente aux courbes de genre 0 . En effet un théorème de NOETHER et POINCARÉ démontre le même résultat pour ces courbes.

En fait, l'analogie peut être poursuivie très loin. Si on choisit un sextuplet sur une surface cubique non singulière, il existe des cubiques gauches rencontrant les six droites du sextuplet et ces cubiques forment un "réseau homaloïdal". C'est-à-dire qu'il existe des représentations birationnelles de la surface cubique sur un plan dans lesquelles ces cubiques sont représentées par toutes les droites du plan. Si le sextuplet est rationnel, une telle représentation n'a pas nécessairement ses coefficients rationnels ; mais toute conjuguée de cette représentation peut s'en déduire en la multipliant par une transformation homographique du plan. (On appelle encore conjuguées de la représentation les représentations qui s'en déduisent en effectuant sur tous les coefficients de la représentation une même opération du groupe de GALOIS du corps qui contient tous ces coefficients). La recherche de celles des représentations birationnelles précédentes qui ont leurs coefficients rationnels (et aussi celle des points rationnels sur la surface) peut ainsi être ramenée à des problèmes concernant les transformations homographiques du plan ou les matrices qui représentent ces transformations en coordonnées homogènes. La théorie des algèbres normales et simples permet de résoudre ces problèmes, comme je l'ai montré dans ma thèse (Ann. Scient. Ecole Norm. Sup., t.61, 1944).

Un exemple simple de ces surfaces est celle qui a pour équation :

$$(1) \qquad N(x + \theta y + \theta^2 z) = A \quad ,$$

où A est un nombre rationnel et θ un nombre <u>cyclique</u> cubique et où le symbole N désigne la norme des nombres du corps engendré par θ . En fait, cette surface est singulière ; elle contient 3 points singuliers situés à l'infini sur les 3 axes de coordonnées. Les 27 droites de la surface se réduisent aux 3 droites du plan de l'infini situées dans les plans de coordonnées (dont chacune doit être comptée

plusieurs fois).

Mais toutes les surfaces :

$$N(\alpha_1 x + \alpha_2 x + \alpha_3 z + \alpha_4) = A\, N(\beta_1 x + \beta_2 y + \beta_3 z + \beta_4)$$

où α_1 , α_2 , α_3 , α_4 , β_1 , β_2 , β_3 , β_4 sont des nombres du corps engendré par θ , peuvent être déduites de la surface (1) par des transformations birationnelles à coefficients rationnels. Donc la recherche des points rationnels sur toutes ces surfaces sont des problèmes équivalents. On peut choisir α_1 , α_2 , α_3 , α_4 , β_1 , β_2 , β_3 , β_4 de manière que la surface correspondante ne soit pas singulière ; elle contient alors un sextuplet rationnel.

Un théorème de Hilbert montre que la surface (1) admet une représentation birationnelle à coefficients rationnels si elle contient un point rationnel. Un théorème de HASSE permet de reconnaître si cette surface contient des points rationnels. Ces 2 résultats appartiennent à la théorie du corps des classes, équivalente à celle des algèbres normales et simples sur un corps de nombres algébriques. (On pourra consulter l'ouvrage de DEURING : "Algebren" paru dans la collection Ergebnisse der Mathematik en 1935).

On ne sait pas encore si une surface cubique non singulière contenant soit une droite rationnelle, soit un triplet rationnel peut admettre une représentation birationnelle à coefficients rationnels sur un plan. Il semble qu'elle ne puisse en admettre que dans des cas exceptionnels. On est ainsi amené à chercher un autre procédé pour obtenir tous les points rationnels de la surface. Or le théorème de MORDELL et SEGRE cité au début peut être précisé de la façon suivante :

Une surface cubique non singulière qui contient un point rationnel admet une représentation simplement rationnelle à coefficients rationnels sur un plan ou sur un espace linéaire.

On peut espérer obtenir les points rationnels de la surface en utilisant une ou plusieurs représentations simplement rationnelles. Si on utilise une représentation simplement rationnelle de la surface, on obtient une infinité de points rationnels sur la surface correspondant aux valeurs rationnelles des paramètres. Mais on n'obtient pas nécessairement tous les points rationnels de la surface ; car un point rationnel admet plusieurs systèmes de paramètres qui sont en général algébriques. Il faut donc trouver un ensemble de plusieurs représentations rationnelles qui permettent d'obtenir tous les points rationnels.

D'autre part, chaque point rationnel est ainsi obtenu plusieurs fois, puisqu'il correspond, dans chaque représentation, à plusieurs systèmes de paramètres. On peut penser qu'il y a intérêt à choisir des représentations réduisant ce nombre de systèmes de paramètres et, tout d'abord, des représentations simplement rationnelles

sur un plan, dans laquelle chaque point de la surface n'est représenté que par un nombre fini de systèmes de paramètres. Mais les essais dans cette vois se heurtent à de grandes difficultés. C'est au contraire l'utilisation de représentations sur des hyperespaces de dimension assez élevée (dans lesquelles chaque point de la surface est représentée par une infinité de systèmes de paramètres) qui m'a permis d'étudier un nouveau cas comme je vais l'exposer maintenant.

Il s'agit de surfaces cubiques contenant un triplet rationnel. Il y a exactement 6 droites d'une surface cubique non singulière qui ne rencontrent pas les droites d'un triplet T_0 de la surface. Ces 6 droites se répartissent en 2 triplets T_1 et T_2 qui forment avec le triplet T_0 2 sextuplets. Si le triplet T_0 est rationnel, les sextuplets ainsi formés ne sont pas en général rationnels, mais dans un corps du $6^{ème}$ degré. Choisissons l'un d'eux, celui formé par T_0 et T_1 par exemple ; on peut choisir une représentation birationnelle de la surface sur un plan de manière que les droites de T_1 correspondent aux trois sommets du triangle de référence (l'origine et les points à l'infini sur les 2 axes en coordonnées cartésiennes). On sait que les droites de T_2 correspondent alors aux côtés du même triangle de référence. Cette représentation n'a pas ses coefficients rationnels ; les représentations conjuguées s'en déduisent par multiplication par des transformations simples du plan : homographies qui conservent le triangle de référence et transformations quadratiques qui permutent les sommets et les côtés du triangle de référence. Les transformations homographiques précédentes peuvent être définies en coordonnées homogènes λ , μ , ν par des relations de la forme :

$$\frac{\lambda'}{c_1\mu} = \frac{\mu'}{c_2\nu} = \frac{\nu'}{c_3\lambda}$$

les transformations quadratiques précédentes peuvent être définies par des relations de la forme :

$$\frac{\lambda'}{c_1\lambda\nu} = \frac{\mu'}{c_2\mu\nu} = \frac{\nu'}{c_3\lambda\mu}$$

où c_1 , c_2 , c_3 sont des constantes.

Introduisons alors les paramètres surabondants λ_1 , λ_2 , μ_1 , μ_2 , ν_1 , ν_2 par les relations :

$$\lambda = \lambda_1\lambda_2\nu_2 \quad , \quad \mu = \mu_1\mu_2\nu_2 \quad ,$$

$$\nu = \nu_1\lambda_2\mu_2 \quad .$$

Les transformations précédentes peuvent être représentées par des transformations homographiques sur ces nouveaux paramètres. Pour la première transformation, on peut choisir une homographie de la forme :

$$\frac{\lambda'_1}{c_1 \mu_1} = \frac{\mu'_1}{c_2 \nu_1} = \frac{\nu'_1}{c_3 \lambda_1} = \frac{\lambda'_2}{c_4 \nu_2} = \frac{\mu'_2}{c_5 \lambda_2} = \frac{\nu'_2}{c_6 \mu_2}$$

et pour la seconde, on peut choisir une homographie de la forme :

$$\frac{\lambda'_1}{c_1 \lambda_2} = \frac{\mu'_1}{c_2 \mu_2} = \frac{\nu'_1}{c_3 \nu_2} = \frac{\lambda'_2}{c_4 \lambda_1} = \frac{\mu'_2}{c_5 \mu_1} = \frac{\nu'_2}{c_6 \nu_1}$$

où c_1 , c_2 , c_3 , c_4 , c_5 , c_6 sont encore des constantes.

La recherche de certaines représentations rationnelles à coefficients rationnels de la surface sur l'hyperespace λ_1 , λ_2 , μ_1 , μ_2 , ν_1 , ν_2 peut ainsi se ramener à des opérations sur les transformations homographiques de cet espace (ou sur les matrices qui les représentent). On peut utiliser de nouveau dans cette recherche les résultats de la théorie des algèbres normales et simples. Les conclusions sont moins simples que dans le cas précédent. En effet, il existe toute une classe de transformations homographiques de cet hyperespace (et non plus une seule transformation) dont le produit par une représentation de la surface sur l'hyperespace donne une même représentation. Il faut tenir compte de ce fait lorsqu'on cherche les conditions pour que 2 représentations soient identiques. Ce qui introduit, au lieu d'égalités strictes entre matrices, certaines congruences au produit près par les matrices d'uh groupe fixe.

Néanmoins, ces difficultés ne sont pas insurmontables. La méthode permet effectivement d'obtenir des représentations à coefficients rationnels, s'il en existe, et l'ensemble de tous les points rationnels.

L'exemple le plus simple de ces surfaces est celle qui est définie par la relation :

$$N(x + \theta y + \theta^2 z) = A \quad ,$$

où θ est un nombre cubique <u>non cyclique</u>. Cette surface est encore une surface cubique singulière ; mais, comme dans un exemple précédent, on peut la transformer, par une transformation birationnelle à coefficients rationnels, en une surface cubique non singulière contenant un triplet rationnel.

Si on pose :

$$x + \theta y + \theta^2 z = \frac{\lambda}{\mu}$$

$$x + \theta' y + \theta'^2 z = \frac{\mu}{\nu}$$

$$x + \theta'' y + \theta''^2 z = A \frac{\nu}{\lambda}$$

on obtient une représentation birationnelle sur le plan de coordonnées homogènes λ , μ , ν dont les coefficients sont dans le corps engendré par θ , et ses conjugués θ' , θ'' . Les conjuguées de cette représentation s'en déduisent en la multipliant par des transformations des types précedemment indiqués. On peut

donc utiliser les méthodes précédentes.

Je vais exposer une méthode légèrement différente qui utilise directement la théorie des idéaux de nombres algébriques.

Cherchons d'abord tous les points rationnels sur la surface :

$$N(x + \theta y + \theta^2 z) = 1$$

qui contient évidemment de tels points. Une généralisation facile d'un théorème de Hilbert montre d'abord que le nombre :

$$\alpha = x + \theta y + \theta^2 z \qquad (x\ ,\ y\ ,\ z \text{ rationnels})$$

doit être de la forme :

$$\alpha = \frac{\lambda}{\sigma(\lambda)}$$

où λ est un nombre du corps $R(\theta, \theta', \theta'')$ engendré par θ et ses 2 conjugués θ' et θ'' et où σ désigne l'élément du groupe de GALOIS de ce corps qui permutte circulairement θ, θ' et θ''. Si le nombre α est de cette forme, il vérifie la relation :

$$\alpha\, \sigma(\alpha)\, \sigma^2(\alpha) = 1 \ .$$

Il suffit donc de trouver la condition pour qu'il soit contenu dans le corps $R(\theta)$ engendré par θ seulement.

Décomposons α en produit de puissances (positives ou négatives) d'idéaux premiers dans le corps $R(\theta)$. Si $\mathfrak{p}$ est un de ces idéaux premiers, il peut soit rester premier dans le corps $R(\theta, \theta', \theta'')$ soit se décomposer dans ce corps en un produit de 2 idéaux premiers $\mathfrak{p}_1$, $\mathfrak{p}_2$ (distincts ou confondus). Dans le premier cas, $\mathfrak{p}$ figure dans la décomposition dans $R(\theta, \theta', \theta'')$ soit de λ, soit de $\sigma(\lambda)$. Ce qui exige que soit $\sigma(\mathfrak{p})$ figure avec le même exposant dans la décomposition de $\sigma(\lambda)$, soit que $\sigma^2(\mathfrak{p})$ figure dans celle de λ. Mais puisque $\mathfrak{p}$ est un idéal de $R(\theta)$, $\sigma(\mathfrak{p})$ ou $\sigma^2(\mathfrak{p})$ ne peut être contenu dans ce corps que si $\mathfrak{p}$ est rationnel ; et dans ce dernier cas, $\mathfrak{p}$ disparait de la décomposition de α. Le nombre α du corps $R(\theta)$, qui contient l'idéal $\sigma(\mathfrak{p})$ ou $\sigma^2(\mathfrak{p})$ non contenu dans $R(\theta)$, doit contenir aussi le conjugué de cet idéal avec le même exposant ; ce conjugué est soit $\sigma^2(\mathfrak{p})$, soit $\sigma(\mathfrak{p})$. Mais cela exige à nouveau que $\mathfrak{p}$ soit encore contenu, avec l'exposant opposé, dans la décomposition de α. Finalement, on voit que α contient une puissance (positive ou négative) du produit :

(1) $$\frac{\mathfrak{p}^2}{\sigma(\mathfrak{p})\, \sigma^2(\mathfrak{p})}$$

Si $\mathcal{y}$ est décomposé, dans le corps $R(\theta, \theta', \theta'')$, en un produit de 2 idéaux $\mathcal{y}_1 \mathcal{y}_2$ (distincts ou confondus), $\mathcal{y}_2$ est le conjugué de $\mathcal{y}_1$, soit $\tau(\mathcal{y}_1)$ où τ désigne l'élément du groupe de GALOIS qui conserve θ et qui permute θ' et θ''. Le nombre α doit encore contenir soit $\sigma(\mathcal{y}_1)$, soit $\sigma^2(\ _1)$ avec l'exposant opposé. Si cet idéal $\sigma(\mathcal{y}_1)$ ou $\sigma^2(\mathcal{y}_1)$ est contenu dans le corps $R(\theta)$, on retrouve le cas déjà étudié. Si cet idéal $\sigma(\mathcal{y}_1)$ ou $\sigma^2(\mathcal{y}_1)$ n'est pas contenu dans $R(\theta)$, l'idéal conjugué $\tau[\sigma(\mathcal{y}_1)]$ ou $\tau[\sigma^2(\mathcal{y}_1)]$ doit aussi être contenu dans la décomposition de α, avec le même exposant. Or :

$$\tau[\sigma(\mathcal{y}_1)] = \sigma^2[\tau(\mathcal{y}_1)] \qquad \text{et} \qquad \tau[\sigma^2(\mathcal{y}_1)] = \sigma[\tau(\mathcal{y}_1)]$$

Donc le produit :

(2) $$\frac{\mathcal{y}_1 \tau(\mathcal{y}_1)}{\sigma(\mathcal{y}_1)\tau[\sigma(\mathcal{y}_1)]}$$

qui est contenu dans $R(\theta)$ est de la forme

$$\frac{\mathcal{a}}{\sigma(\mathcal{a})}$$

où $\mathcal{a}$ est un idéal (non premier) du corps $R(\theta, \theta', \theta'')$. De même le produit

(3) $$\frac{\mathcal{y}_1 \tau(\mathcal{y}_1)}{\sigma^2(\mathcal{y}_1)\tau[\sigma^2(\mathcal{y}_1)]}$$

qui est contenu dans $R(\theta)$ est de la même forme.

Finalement, α est un produit de facteurs d'une des formes (1), (2) ou (3) ; mais on voit facilement que ces 3 formes peuvent toutes se ramener à la forme (2) en choisissant convenablement l'idéal $\mathcal{y}_1$ qui y figure.

Si α est un produit de facteurs de la forme (2), on voit que c'est un idéal de $R(\theta)$ et que cet idéal vérifie la relation :

$$\alpha\, \sigma(\alpha)\, \sigma^2(\alpha) = 1$$

Mais, il faut encore que cet idéal soit principal.

Or, on sait que le nombre de classes d'idéaux de $R(\theta, \theta', \theta'')$ est fini. Donc, les produits α de facteurs de la forme (2), sont encore de la forme :

$$\frac{\mathcal{a}_i \tau(\mathcal{a}_i)}{\sigma(\mathcal{a}_i)\tau[\sigma(\mathcal{a}_i)]} \cdot \frac{\mu\tau(\mu)}{\sigma(\mu)\tau[\sigma(\mu)]}$$

où $\mathcal{a}_i$ est un idéal de $R(\theta, \theta', \theta'')$ qui ne peut prendre qu'un nombre fini de valeurs (un représentant de chacune des classes d'idéaux du corps) et où μ est un nombre arbitraire du corps $R(\theta, \theta', \theta'')$.

Désignons par (μ_j) les idéaux de la forme :

$$\frac{\alpha_i \zeta(\alpha_i)}{\sigma(\alpha_i)\zeta[\sigma(\alpha_i)]}$$

qui sont principaux. Le nombre α est nécessairement de la forme :

$$\mu_j \quad \frac{\mu \zeta(\mu)}{\sigma(\mu)\zeta[\sigma(\mu)]}$$

Enfin si le nombre α est de la forme précédente, il est bien dans $R(\theta)$ et l'idéal principal engendré par α vérifie :

$$(\alpha)\sigma(\alpha)\sigma^2(\alpha) = 1$$

Le nombre α vérifie donc seulement la relation :

$$N(\alpha) = \pm 1 \quad .$$

Mais il est facile de distinguer les valeurs de μ_j qui conduisent à des nombres α dont la norme est exactement $+1$.

Cherchons maintenant s'il existe des points rationnels sur une surface :

$$N(x + \theta y + \theta^2 z) = A$$

où A est un nombre rationnel arbitraire. Il faut d'abord que A soit la norme d'un idéal de $R(\theta)$; ce qu'on peut vérifier facilement en décomposant A en produit de puissances d'idéaux premiers du corps $R(\theta, \theta', \theta'')$. Si dans ce produit figure un idéal premier $\mathfrak{p}$ non contenu dans $R(\theta)$, il doit aussi y figurer avec le même exposant l'idéal $\zeta(\mathfrak{p})$. Si un idéal rationnel figure dans cette décomposition, il doit y figurer avec un exposant multiple de 3 . Enfin si un idéal de $R(\theta)$, décomposé ou non dans $R(\theta, \theta', \theta'')$, figure dans cette décomposition, il doit aussi y figurer les idéaux $\sigma(\mathfrak{p})$ et $\sigma^2(\mathfrak{p})$. Ces conditions suffisent pour que A soit la norme d'un idéal α_1 de $R(\theta)$.

Mais il faut encore trouver la condition pour qu'il existe un idéal principal dont la norme soit A . Or tous les idéaux dont la norme est A sont de la forme :

$$\alpha_1 \quad \frac{\alpha \zeta(\alpha)}{\sigma(\alpha)\zeta[\sigma(\alpha)]}$$

Il faut donc vérifier si un des idéaux :

$$\alpha_1 \quad \frac{\alpha_i \zeta(\alpha_i)}{\sigma(\alpha_i)\zeta[\sigma(\alpha_i)]}$$

où α_i décrit encore l'ensemble d'un représentant de chaque classe d'idéaux de $R(\theta, \theta', \theta'')$, est principal. Toutefois, si un tel idéal (α) existe, on en

conclut seulement que sa norme est $\pm A$. Il faut encore vérifier si la norme du produit de α par une unité est exactement égale à $+A$.

En conclusion, la recherche des points rationnels sur les surfaces cubiques peut se faire si la surface contient, soit un doublet rationnel, soit un sextuplet rationnel, soit un triplet rationnel. Mais il reste encore à traiter les cas où la surface contient une droite rationnelle et le cas général où la surface ne contient aucun des éléments rationnels précédents.