Les points exceptionnels sur les cubiques $ax^3+by^3+cz^3=0$

Par T. NAGELL à Uppsala (Suède)

Dédié au 60ième anniversaire de mon ami Ladislaus Rédei

1. Dans un travail qui vient de paraître dans les *Acta Arithmetica*[1]), j'ai établi entre autres le résultat suivant:

Théorème I. *Soit Ω un corps algébrique dans lequel le nombre des classes d'idéaux est égal à 1. Considérons la cubique*

$$ax^3+by^3+cz^3=0, \tag{1}$$

où les coefficients a, b et c sont des nombres, différents de zéro, dans Ω. Deux cubiques de la forme (1) *sont considérées comme identiques quand elles sont linéairement équivalentes dans Ω. Désignons par m le nombre des points exceptionnels dans Ω sur la cubique.*

Supposons d'abord que Ω ne contient pas le nombre $\sqrt{-3}$. Si la relation

$$1+E+E_1=0 \tag{2}$$

est impossible ou si elle est satisfaite par une seule paire d'unités E et E_1 dans Ω, on a $m=0$, sauf dans les cas suivants: Si la cubique a la forme

$$x^3+y^3+cz^3=0, \tag{3}$$

où ni c ni 4c n'est égal à un cube dans Ω, on a $m=1$. Si la cubique a la forme

$$x^3+y^3+2z^3=0, \tag{4}$$

et si le nombre 2 n'est pas égal à un cube dans Ω, on a $m=2$. Enfin, pour la cubique

$$x^3+y^3+z^3=0 \tag{5}$$

[1]) T. NAGELL, Les points exceptionnels rationnels sur certaines cubiques du premier genre, *Acta Arithmetica*, **5** (1959), 333—357. A propos de l'explication des notions nous renvoyons le lecteur à ce travail.

on a $m=6$ *ou* $m=3$, *selon que le nombre* 2 *est égal à un cube dans* Ω *ou non.*

Supposons ensuite que Ω *contient le nombre* $\sqrt{-3}$. *Alors on a* $m=0$ *si la relation* (2) *n'est satisfaite que par la paire d'unités* $\varrho=\frac{1}{2}(-1+\sqrt{-3})$ *et* $\varrho^2=\frac{1}{2}(-1-\sqrt{-3})$ *dans* Ω, *exception faite des cas suivants: Pour la cubique* (3) *on a* $m=3$. *Pour la cubique* (4) *on a* $m=12$. *Pour la cubique* (5) *on a* $m=9$. *Pour la cubique*

$$x^3+\varrho y^3+\varrho^2 z^3=0 \tag{6}$$

on a $m=9$.

Ce théorème est vrai par exemple quand Ω *est un corps quadratique simple ou un corps cubique simple à discriminant négatif.*

2. Dans le présent travail nous allons traiter du cas d'un corps algébrique Ω dans lequel le nombre des classes d'idéaux est plus grand que l'unité. Cependant, pour obtenir un résultat analogue au Théorème I dans ce cas nous sommes forcés à faire certaines suppositions restrictives sur les coefficients a, b et c de la cubique (1).

Nous supposons que les coefficients satisfont aux conditions suivantes:

a, b et c sont des nombres entiers dans Ω, *différents de zéro. Aucun des idéaux principaux* (a), (b), (c) *n'est divisible par le cube d'un idéal premier. Les idéaux* (a), (b) *et* (c) *sont premiers entre eux deux à deux.*

Deux cubiques de la forme (1) sont considérées comme identiques quand elles sont reliées par des transformations linéaires appartenant à Ω.

3. Soit $P=P(x, y, z)$ un point rationnel dans Ω sur la cubique (1), c'est-à-dire que les coordonnées x, y, z sont proportionnelles à trois nombres dans Ω. Désignons par

$$(x, y, z)=\mathfrak{j} \tag{7}$$

le plus grand commun diviseur des idéaux (x), (y) et (z). Alors on a

$$\left(\frac{x}{\mathfrak{j}}, \frac{y}{\mathfrak{j}}\right)=\left(\frac{x}{\mathfrak{j}}, \frac{z}{\mathfrak{j}}\right)=\left(\frac{y}{\mathfrak{j}}, \frac{z}{\mathfrak{j}}\right)=1. \tag{8}$$

En effet, soit $\mathfrak{p}$ un idéal premier qui divise l'un et l'autre des deux idéaux $\left(\frac{x}{\mathfrak{j}}\right)$ et $\left(\frac{y}{\mathfrak{j}}\right)$. Alors il suit de l'équation (1) que

$$c\cdot\left(\frac{z}{\mathfrak{j}}\right)^3\equiv 0 \pmod{\mathfrak{p}^3}.$$

Or, d'après l'hypothése faite sur les coefficients, c n'est pas divisible par le cube $\mathfrak{p}^3$. Donc on aura

$$\left(\frac{z}{\mathfrak{j}}\right)\equiv 0 \pmod{\mathfrak{p}}.$$

Il en résulterait que l'idéal $\left(\frac{x}{\mathfrak{j}}, \frac{y}{\mathfrak{j}}, \frac{z}{\mathfrak{j}}\right)$ serait divisible par $\mathfrak{p}$. Or, cela serait en contradiction avec (7). Donc, les relations (8) sont vraies.

Si $N(\mathfrak{A})$ signifie la norme de l'idéal $\mathfrak{A}$ dans Ω, nous appelons le nombre

$$N\left(\frac{xyz}{\mathfrak{j}^3}\right) \tag{9}$$

l'index du point $P(x, y, z)$. L'index est un nombre entier positif dans $\mathbf{K}(1)$, sauf quand P est un point d'inflexion; l'index d'un point d'inflexion est évidemment $=0$.

4. Désignons par $P_1 = P_1(\xi, \eta, \zeta)$ le point tangentiel du point $P=P(x, y, z)$. Les coordonées ξ, η et ζ de P_1 sont alors données par les formules

$$\begin{cases} \xi = x(by^3 - cz^3), \\ \eta = y(cz^3 - ax^3), \\ \zeta = z(ax^3 - by^3). \end{cases} \tag{10}$$

Il résulte de là que ξ, η et ζ sont tous les trois divisibles par $\mathfrak{j}^4$. Soit $\mathfrak{A}$ un idéal tel qu'on ait

$$\left(\left(\frac{\xi}{\mathfrak{j}^4}\right), \left(\frac{\eta}{\mathfrak{j}^4}\right), \left(\frac{\zeta}{\mathfrak{j}^4}\right)\right) = \mathfrak{A}. \tag{11}$$

Soit $\mathfrak{p}$ un idéal premier qui divise $\mathfrak{A}$. Supposons que $\left(\frac{x}{\mathfrak{j}}\right)$ soit divisible par $\mathfrak{p}$. On déduit alors de la seconde équation dans (10)

$$\left(\frac{y}{\mathfrak{j}}\right)\left(\frac{cz^3 - ax^3}{\mathfrak{j}^3}\right) = \left(\frac{y}{\mathfrak{j}}\right)\left(\frac{-2ax^3 - by^3}{\mathfrak{j}^3}\right) \equiv 0 \pmod{\mathfrak{p}},$$

donc

$$b\left(\frac{y}{\mathfrak{j}}\right) \equiv 0 \pmod{\mathfrak{p}}, \tag{12}$$

et on déduit de la troisième équation dans (10)

$$\left(\frac{z}{\mathfrak{j}}\right)\left(\frac{ax^3 - by^3}{\mathfrak{j}^3}\right) = \left(\frac{z}{\mathfrak{j}}\right)\left(\frac{2ax^3 + cz^3}{\mathfrak{j}^3}\right) \equiv 0 \pmod{\mathfrak{p}},$$

donc

$$c\left(\frac{z}{\mathfrak{j}}\right) \equiv 0 \pmod{\mathfrak{p}}. \tag{13}$$

Or, les congruences (12) et (13) ne peuvent pas être satisfaites en même temps. Cela se voit aisément à l'aide des relations (8) et de $(b, c) = 1$.

On en conclut qu'aucun des idéaux $\left(\frac{x}{\mathfrak{j}}\right)$, $\left(\frac{y}{\mathfrak{j}}\right)$ et $\left(\frac{z}{\mathfrak{j}}\right)$ n'est divisible par $\mathfrak{p}$. Donc, tous ces idéaux sont premiers à $\mathfrak{A}$. Il résulte alors de (10) que

$$by^3 - cz^3 \equiv cz^3 - ax^3 \equiv ax^3 - by^3 \equiv 0 \pmod{\mathfrak{A}\mathfrak{p}^3}. \tag{14}$$

On en déduit aisément

$$3a\left(\frac{x}{\mathfrak{j}}\right)^3 \equiv 3b\left(\frac{y}{\mathfrak{j}}\right)^3 \equiv 3c\left(\frac{z}{\mathfrak{j}}\right)^3 \equiv 0 \pmod{\mathfrak{A}}.$$

Vu que $(a, b) = (a, c) = b, c) = \left(\frac{x}{\mathfrak{j}}, \mathfrak{A}\right) = \left(\frac{y}{\mathfrak{j}}, \mathfrak{A}\right) = \left(\frac{z}{\mathfrak{j}}, \mathfrak{A}\right) = 1$, on en conclut que

$$3 \equiv 0 \pmod{\mathfrak{A}}. \tag{15}$$

5. Supposons maintenant que ni P ni P_1 n'est un point d'inflexion. Alors tous les nombres

$$x, y, z, \xi, \eta, \zeta, by^3 - cz^3, cz^3 - ax^3, ax^3 - by^3$$

sont différents de zéro.

Supposons que P est un point exceptionnel dans Ω. Vu que le nombre des points exceptionnels dans Ω est limité, les indices de ces points a un certain maximum M. Supposons que

$$\text{Index } P = N\left(\frac{xyz}{\mathfrak{j}^3}\right) = M.$$

Alors on a

$$\text{Index } P_1 = N\left(\frac{\xi\eta\zeta}{\mathfrak{j}^{12}\mathfrak{A}^3}\right) \leqq M.$$

D'autre part il résulte de (10) et (14) que

$$N\left(\frac{\xi\eta\zeta}{\mathfrak{j}^{12}\mathfrak{A}^3}\right) \geqq N\left(\frac{xyz}{\mathfrak{j}^3}\right).$$

Nous aurons donc

$$\text{Index } P_1 = \text{Index } P = M,$$

et par conséquent:

$$(by^3 - cz^3) = (cz^3 - ax^3) = (ax^3 - by^3) = \mathfrak{A}\mathfrak{j}^3. \tag{16}$$

Ces relations entraînent

$$cz^3 - ax^3 = E(by^3 - cz^3),$$
$$ax^3 - by^3 = E_1(by^3 - cz^3),$$

où E et E_1 sont des unités dans Ω, qui satisfont à l'équation

$$1+E+E_1=0. \tag{17}$$

6. De ce qui précède nous aurons le résultat suivant:

Théorème II. *Soit Ω un corps algébrique qui ne contient pas le nombre $\sqrt{-3}$. Soit donnée la cubique*

$$ax^3+by^3+cz^3=0,$$

où les coefficients a, b et c sont des nombres entiers dans Ω qui satisfont aux conditions suivantes: Les idéaux principaux (a), (b) et (c) sont premiers entre eux deux à deux, et aucun d'eux n'est divisible par le cube d'un idéal premier.

Désignons par m le nombre des points exceptionnels dans Ω sur la cubique. Si la relation (17) *n'est satisfaite par aucune paire d'unités E et E_1 dans Ω, on a $m=0$, sauf dans les cas suivants: Si la cubique a la forme*

$$x^3+y^3+cz^3=0, \tag{18}$$

où ni c ni 4c n'est égal au cube d'un nombre dans Ω, on a $m=1$. Si la cubique a la forme

$$x^3+y^3+2z^3=0, \tag{19}$$

on a $m=2$.[1]) *Si la cubique a la forme*

$$x^3+y^3+z^3=0, \tag{20}$$

on a $m=3$.

Les cubiques d'exception (18), (19) et (20) représentent, tout comme au Théorème I, les cas dans lesquels un seul ou plusieurs points d'inflexion appartiennent à Ω.

Théorème II est vrai quand Ω est un corps quadratique ou un corps cubique à discriminant négatif. En effet, dans mon travail précité, j'ai montré que la relation (17) n'est pas satisfaite dans ces corps, exception faite d'un nombre fini de corps simples.

7. Les Théorèmes I et II sont encore vrais quand Ω est un corps biquadratique jouissant des propriétés suivantes: Tous les quatre corps conjugués sont imaginaires. Ω est différent des corps engendrés par les cinquièmes, huitièmes et douzièmes racines primitives de l'unité. Ω admet un sous-corps quadratique réel différent de $\mathbf{K}(\sqrt{5})$. Ω ne contient pas le nombre $\sqrt{-3}$.

[1]) Le nombre 2, étant par hypothèse indivisible par le cube d'un idéal premier, ne peut être le cube d'un nombre dans Ω.

En effet, dans ce cas il y a une seule unité fondamentale η dans Ω, telle que toutes les unités du corps soient données sous la forme $\varrho\eta^M$, où ϱ est une racine de l'unité appartenant à Ω, et où M est un nombre entier rationnel. On peut supposer que $|\eta| > 1$, et si η est réel que $\eta > 1$. A cause des restrictions faites sur Ω il ne reste pour ϱ que les possibilités ± 1 et $\pm i$. Ω ne peut contenir qu'un seul sous-corps quadratique réel. Désignons par ε l'unité fondamentale de ce sous-corps; nous pouvons choisir $\varepsilon > 1$. Pour une certaine valeur entière de N on a donc

$$\varepsilon = \varrho\eta^N. \tag{21}$$

Vu que $\varepsilon > 1$ et $|\eta| > 1$ on a $N \geqq 1$.

Supposons d'abord que Ω ne contient pas le nombre i. Alors on a dans (21) $\varrho = \pm 1$. D'après le théorème de CAPELLI, le nombre $(\pm\varepsilon)^{\frac{1}{N}}$ est du $2N$-ième degré. Ainsi, quand η est du quatrième degré, on aura

$$\varepsilon = -\eta^2, \tag{22}$$

et quand η est du second degré, on aura

$$\varepsilon = \eta. \tag{23}$$

Dans le dernier cas toutes les unités sont du second degré, et la relation (17) est impossible dans Ω, ainsi que nous l'avons montré dans notre travail précité. Dans le cas (22) la relation (17) est encore impossible quand E et E_1 sont réels et conséquemment du second degré. Si l'unité E est imaginaire, elle est évidemment racine d'une équation de la forme

$$x^4 - ax^2 + 1 = 0,$$

où a est un nombre entier rationnel. Alors E_1 est racine de l'équation

$$(y+1)^4 - a(y+1)^2 + 1 = 0.$$

Comme E_1 et ses conjuguées sont imaginaires, on a nécessairement $a = 1$. Or, les racines de l'équation $x^4 - x^2 + 1 = 0$ sont les douzièmes racines primitives de l'unité.

Supposons ensuite que Ω contient le nombre i. Si dans (21) $\varrho = \pm 1$, on aura comme tout-à-l'heure les possibilités (22) et (23). Or, si $\eta = \sqrt{-\varepsilon}$ le corps ne peut pas contenir le nombre i vu que le produit $-i\sqrt{-\varepsilon} = \sqrt{\varepsilon}$ est un nombre réel du quatrième degré. On a donc $\eta = \varepsilon$. Nous savons déjà que la relation (17) est impossible quand E et E_1 sont du second degré. Soit maintenant E du quatrième degré. Alors le nombre iE est une unité réelle du second degré et racine d'une équation

$$x^2 - ax \pm 1 = 0,$$

où a est un nombre entier rationnel. Alors E est racine de l'équation

$$z^2 + aiz \mp 1 = 0$$

et de l'équation

$$(z^2 \mp 1)^2 + a^2 z^2 = 0.$$

Donc l'unité E_1 est racine de l'équation

$$(y+1)^4 + (y+1)^2(a^2 \mp 2) + 1 = 0.$$

Comme E_1 et ses conjuguées sont imaginaires, on a nécessairement

$$2 + a^2 \mp 2 = 1,$$

d'où il s'ensuit que $a = \pm 1$. Les équations corréspondantes

$$x^2 \mp x \pm 1 = 0$$

sont inadmissibles, vu que Ω ne contient pas les nombres $\sqrt{5}$ et $\sqrt{-3}$.

Supposons finalement que, dans (21), $\varrho = \pm i$. D'après le théorème de CAPELLI, le nombre $(\pm i\varepsilon)^{\frac{1}{N}}$ est ou du $4N$-ième degré ou du $2N$-ième degré. Donc on doit avoir ou $N=2$ ou $N=1$, c'est-à-dire ou $\eta^2 = \pm i\varepsilon$ ou $\eta = \pm i\varepsilon$. Si E et E_1 sont du second degré, on procédera comme tout-à-l'heure. Si E et E_1 sont du quatrième degré, le raisonnement sera le même que dans le cas $\eta = \varepsilon$.

Nous finissons par quelques exemples numériques.

Exemple 1. Soit Ω le corps biquadratique engendré par le nombre $\eta = \sqrt{-2-\sqrt{3}}$, racine de l'équation

$$x^4 + 4x^2 + 1 = 0.$$

Ω est un corps de Galois et contient les trois sous-corps quadratiques $\mathbf{K}(\sqrt{3})$, $\mathbf{K}(\sqrt{-2})$ et $\mathbf{K}(\sqrt{-6})$. L'unité fondamentale dans $\mathbf{K}(\sqrt{3})$ est $\varepsilon = 2+\sqrt{3}$, et η est l'unité fondamentale dans Ω.

Exemple 2. Soit Ω le corps biquadratique engendré par le nombre $\alpha = \sqrt{-3-\sqrt{7}}$, racine de l'équation

$$x^4 + 6x^2 + 2 = 0.$$

Le seul sous-corps quadratique de Ω est $\mathbf{K}(\sqrt{7})$. L'unité fondamentale dans le sous-corps est $\varepsilon = 8+3\sqrt{7}$. Le nombre $\beta = \sqrt{-8-3\sqrt{7}}$ n'appartient pas à Ω. En effet, le quotient $\frac{\alpha}{\beta}$ est égal à $\sqrt{3-\sqrt{7}}$, nombre réel du quatrième degré. Ainsi le nombre $\varepsilon = 8+3\sqrt{7}$ est l'unité fondamentale dans Ω.

Parmi les corps biquadratiques en question il y en a aussi des corps simples, c'est-à-dire des corps dans lesquels le nombre des classes d'idéaux est égal à 1. En effet, les corps de Dirichlet $\mathbf{K}(\sqrt{D}, \sqrt{-D})$ sont simples pour $D = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$. Dans nos raisonnements plus haut nous avons exclus les cas $D = 2$, 3 et 5. Dans les autres cas Théorème I est vrai.

(Reçu le 13 janvier 1960)