Sur l'Analyse indéterminée du troisième degré.— Demonstration de plusieurs théorèmes de M. Sylvester.

PAR EDOUARD LUCAS.

SECTION 1.

L'ARITHMETIQUE DE DIOPHANTE renferme le premier exemple connu d'Analyse indéterminée du troisème degré ; l'immortel auteur y pose, en effet, le problème de trouver deux nombres entiers ou fractionnaires, dont la somme ou la différence de leurs cubes soit égale à la somme ou à la différence des cubes de deux nombres donnés.

FERMAT a indiqué, le premier, un procédé qui permet de déduire, d'une solution initiale, une série indéfinie de solutions nouvelles. Pour résoudre en nombres entiers ou fractionnaires, l'équation

$$x^3 + y^3 = a^3 + b^3 ,$$

dans laquelle a et b sont donnés, il suffit de poser

$$x = a + zu, \quad y = b + u ,$$

et de disposer de z , de manière à faire disparaître, après la substitution, la première puissance de u. On trouve alors une relation de la forme

$$Au^3 + Bu^2 = 0 ,$$

qui permet de déterminer u par une équation du premier degré ; FERMAT calcule ainsi x et y, et fait servir ces valeurs à la recherche de nouvelles solutions, en nombre indéfini.

Nous remplacerons, dans ce qui suit, les inconnues rationnelles, par des inconnues entières. Désignons par (x, y, z) une première solution, en nombres, entiers, de l'équation

$$x^3 + y^3 = Az^3 \tag{1}$$

nous obtiendrons une autre solution, par le procédé indiqué plus haut, au moyen des formules

$$X = x(x^3 + 2y^3), \quad Y = - y(y^3 + 2x^3), \quad Z = z(x^3 - y^3). \tag{2}$$

On trouve ainsi, successivement, pour $A = 9$,

$$\begin{cases} x_1 = 2, & x_2 = 20, & x_3 = 1\,88479, & x_4 = 12\,43617\,73399\,00948\,36481, \\ y_1 = 1, & y_2 = -17, & y_3 = -36520, & y_4 = 4\,87267\,17171\,43523\,36560, \\ z1 = 1, & z_2 = 7\ ; & z_3 = +90391\ ; & z_4 = 6\,09623\,83567\,61372\,97449\ ; \end{cases}$$

Et, pour $A = 28$,

$$\begin{cases} x_1 = 3, & x_2 = 87, & x_3 = 632\,84705, & x_4 = 18\,92071\,22047\,02010\,97176\,90323\,50335, \\ y_1 = 1, & y_2 = -55, & y_3 = 283\,40511, & y_4 = -15\,01104.22682\,05492\,03687\,05698\,29391, \\ z_1 = 1, & z_2 = 26; & z_3 = 214\,46828; & z_4 = 4\,94756\,15518\,27392\,93262\,16777\,58432. \end{cases}$$

On observera que ces solutions croissent très-rapidement, et contiennent à peu près quatre fois plus de chiffres, que la solution précédente.

On peut encore remplacer les formules (2) par les suivantes, qui n'en diffèrent que par la forme. Désignons par (x, y, z) des nombres entiers qui vérifient l' équation

$$x^3 + y^3 = Az^3\ ,$$

nous obtiendrons des nombres entiers (X, Y, Z), tels que l'on ait

$$\frac{X^3 + Y^3}{Z^3} = \frac{x^3 + y^3}{z^3} = A\,,$$

par les formules $\quad \dfrac{X}{x} + \dfrac{Y}{y} + \dfrac{Z}{z} = 0\ , \qquad Xx^2 + Yy^2 = AZz^2\ .$

SECTION 2.

LAGRANGE ET CAUCHY ont étendu la méthode que nous venons d'indiquer, à des équations du troisième degré beaucoup plus générales. Soit l'équation

$$Ax^3 + By^3 + Cz^3 + 3Dxyz = 0\ ; \tag{3}$$

On déduit d' une première solution (x, y, z), en nombres entiers, une autre solution (X, Y, Z), par les formules

$$\begin{cases} X = x(By^3 - Cz^3), \\ Y = y(Cz^3 - Ax^3), \\ Z = z(Ax^3 - By^3), \end{cases} \tag{4}$$

Ainsi l'équation

$$x^3 + 2y^3 + 3z^3 = 6xyz,$$

qui a pour solution immédiate

$$x_0 = y_0 = z_0 = 1$$

donne ensuite les solutions

$$\begin{cases} x_1 = 1, & x_2 = 19, & x_3 = 2\,82473, & \ldots \\ y_1 = -2, & y_2 = 4, & y_3 = -86392, & \ldots \\ z_1 = 1\ ; & z_2 = -17\ ; & z_3 = -1\,14427\ ; & \ldots \end{cases}$$

Nous observerons que les formules (4) peuvent être remplacées par celles-ci

$$\frac{X}{x}+\frac{Y}{y}+\frac{Z}{z}=0, \quad AXx^2+BYy^2+CZz^2=0, \tag{5}$$

et conduisent à l'identité

$$Ax^3(Ax^3+2By^3)^3+By^3(By^3+2Ax^3)^3+27A^2B^2x^6y^6 = [A^2x^6+7Abx^3y^3+B^2y^6]^2.$$

Cette identité fournit ainsi une série indéfinie de solutions de l'équation indéterminée

$$Au^3 + Bv^3 + A^2B^2w^3 = t^2.$$

On doit encore à CAUCHY, l'indication suivante.[1] Si (x_0, y_0, z_0) et (x_1, y_1, z_1) désignent deux solutions distinctes de l'équation (3), on obtient une solution nouvelle au moyen des formules

$$\begin{cases} X = By_0y_1(x_0y_1-x_1y_0) + Cz_0z_1(x_0z_1-z_0x_1) + D(x_0^2y_1z_1-x_1^2y_0z_0), \\ Y = Cz_0z_1(y_0z_1-y_1z_0) + Ax_0x_1(y_0x_1-x_0y_1) + D(y_0^2z_1x_1-y_1^2z_0x_0), \\ Z = Ax_0x_1(z_0x_1-z_1x_0) + By_0y_1(z_0y_1-y_0z_1) + D(z_0^2x_1y_1-z_1^2x_0y_0), \end{cases}$$

On peut remplacer ces formules par celles-ci :

$$\begin{vmatrix} X_1, & Y_1, & Z_1, \\ x_0, & y_0, & z_0, \\ x_1, & y_1, & z_1, \end{vmatrix}=0, \quad AX\,x_0\,x_1+BY\,y_0\,y_1+CZ\,z_0\,z_1=0. \tag{6}$$

Ainsi, par exemple, les solutions (x_0, y_0, z_0) et (x_2, y_2, z_2) de l'équation numérique, que nous venons de considérer, donnent

$$X = 143, \quad Y = 113, \quad Z = 71.$$

SECTION 3.

Les résultats précédents sont des cas particuliers de ceux que nous allons indiquer. Soit l'équation du troisième degré

$$f(x, y, z) = 0, \tag{7}$$

d'une courbe en coordonnées rectilignes et homogènes ; désignons par m_1 un point dont les coordonnées (x_1, y_1, z_1) ont rationnelles, et qu' il est facile de rendre entières ; on a ainsi un première solution, en nombre entiers, de l'équation proposée. On obtient de nouvelles solutions, par l'un des trois procédés suivants :

[1] CAUCHY.– *Sur la résolution de quelques équations indéterminées – en nombres entiers.* – Exercices de Mathématiques, 1826, t. 1, pag. 256.

1°. Si l'on mène la tangente à la cubique en m_1, cette droite rencontre la courbe en un autre point m dont les coordonnées sont rationnelles ; par conséquent, d' une première solution de l'équation (7) on déduit, en général une autre solution, par les formules

$$f(x, y, z) = 0\ , \qquad x\frac{df}{dx_1} + y\frac{df}{dy_1} + z\frac{df}{dz_1} = 0\ .$$

Cependant, lorsque la tangente est parallèle à l' une des asymptotes de la cubique, ou lorsque la tangente est menée par un point d'inflexion, on n'obtient pas de solutions nouvelles.

2°. Si m_1 et m_2, désignent deux points de la cubique dont les coordonnées (x_1, y_1, z_1) et (x_2, y_2, z_2) sont entières, on obtient, en général, une nouvelle solution de l' équation (7), en prenant l'intersection de la courbe avec la sécante m_1m_2 ; on a donc à résoudre les deux équations

$$f(x_1, y_1, z_1) = 0, \qquad \begin{vmatrix} x, & y, & z, \\ x_1, & y_1, & z_1, \\ x_2, & y_2, & z_2, \end{vmatrix} = 0\ ,$$

en tenant compte des relations

$$f(x_1, y_1, z_1) = 0, \qquad f(x_2, y_2, z_2) = 0$$

3°. Lorsque l'on connait cinq solutions de l'équation (7), on obtient, en général, une sixième solution, en prenant le point d'intersection avec la cubique, de la conique passant par les cinq points qui correspondent aux solutions données. D'ailleurs, on peut supposer plusieurs de ces points réunis en un seul, et en particulier tous les cinq réunis en un seul, à la condition d'établir entre les deux courbes le contact correspondant.

Nous observerons que les méthodes de FERMAT, LAGRANGE, et CAUCHY reviennent aux deux premiers procédés.

SECTION 4.

Nous considérerons, plus particulièrement, dans ce qui suit l' équation (1). EULER et LEGENDRE ont démontré que l'équation

$$x^3 + y^3 = Az^3\ ,$$

est impossible, lorsque A est égal à 1, 2, 3, 4 on 5 ; mais LEGENDRE s'est trompé, pour le cas de $A = 6$, ainsi que nous montrerons plus loin. M. SYLVESTER est venu ajouter une importante contribution à la théorie de cette équation, en donnant un certain nombre de formes générales de A pour lesquelles, l'équation (1) est impossible. Les divers théorèmes indiqués par M. SYLVESTER sont enfermés dans l'énoncé suivant :

Si p et q désignent des nombres premiers des formes respectives $18n+5$ *et* $18n+11$, *il est impossible de décomposer en deux cubes, soit entiers, soit fractionnaires, aucun des nombres A suivants :*

$$p,\ 2p,\ 4p^2\ ; \qquad q^2,\ 2q^2,\ 4q\ .$$

PREMIER CAS. – En effet, soit d'abord à résoudre l' équation indéterminée

$$x^3+y^3=Az^3\ , \tag{1}$$

dans 1aquelle A désigne un nombre premier p de Ia forme $18n+5$, ou le carré q^2 d'un nombre premier de la forme $18n+11$; nous pouvons supposer les entiers x, y, z, premiers entre eux. Mais le cube d' un nombre entier divisé par 9 donne pour reste 0, ou + 1 ou – 1 ; donc, pour que l'équation (1) soit possible, il faut que z^2 soit divisible par 9 ; par suite $z=3z_1$, et z_1 est entier. Cela posé, nous ferons deux hypothèses, selon que z est impair ou pair.

1°. *Supposons z impair*. Alors $x-y$ et $x+y$ sont impairs ; on a

$$x^3+y^3=(x+y)(x^2-xy-y^2)=(x+y)\,M\ ,$$

et

$$4M=(x+y)^2+3(x-y)^2\ ;$$

par conséquent, puisque $x+y$ est divisible par 3, M est aussi divisible par 3, mais non par une puissance supérieure ; par conséquent, en désignant par a et b des nombres impairs, premiers entre eux, on doit poser

$$z_1=ab\ , \quad x+y=3^2Aa^3, \quad M=3b^3,$$

et, par suite

$$4b^3=(x-y)^2+3\left(\frac{x+y}{3}\right)^2$$

D'ailleurs, b, diviseur de M, doit être de la forme f^2+3^2g , f et g étant premiers entre eux ; on a ainsi

$$b=f^2+3g^2, \quad b^2=F^2+3G^2, \quad 4b^3=(F-3G)^2+3(F+G)^2\ ;$$

et en identifiant les deux expressions de $4b^3$,

$$F+G=\frac{x+y}{3}=3Aa^3.$$

Mais le développement du cube de $f+g\sqrt{-3}$ donne

$$F=f\,(f^2-9g^2)\ , \qquad G=3g(f^2-g^2)\ ;$$

par suite

$$f\,(f^2-9g^2)+3g\,(f^2-g^2)=3Aa^3\ ;$$

donc f serait divisible par 3, par suite b, et aussi x et y, que nous supposés premiers entre eux. Par conséquent, z ne petit être impair.

2°. *Supposons* z *pair* ; en aurait

$$M=\left(\frac{x+y}{2}\right)^2+3\left(\frac{x-y}{2}\right)^2,$$

et, puique x et y sont impairs, il en est de même de M. On doit donc poser

$$z_1 = 2ab\ , \quad x + y = 3^2.2^3.Aa^3, \quad M = 3b^3\ ,$$

et, par suite

$$\left(\frac{x-y}{2}\right)^2+3\left(\frac{x+y}{6}\right)^2=b^3.$$

soient encore

$$b = f^2 + 3g^2, \quad b^3 = F^2 + 3G^2\ ;$$

on en déduira

$$G=\frac{x+y}{6}, \quad \text{ou} \quad g(f^2 - g^2) = 4Aa^3.$$

D'ailleurs $f^2 + 3g^2$ et $f^2 + 3g^2 - 4g^2 = f^2 - g^2$ sont impairs ; donc g est pair, et en désignant par α, β, γ trois nombres impairs et premiers entre eux dont le produit égale a, on doit poser

$$g = 4A\alpha^3, \quad f + g = \beta^3, \quad f - g = \gamma^3\ ;$$

ou

$$g = 4\alpha^3, \quad f + g = A\beta^3, \quad f - g = \gamma^3\ ;$$

On déduit de ces deux décompositions

$$\beta^3 - \gamma^3 = A\ (2\alpha)^3, \quad \text{ou} \quad \gamma^3 + (2\alpha)^3 = A\beta^3\ ;$$

ces deux équations sont semblables à l'equation (1) ; on ramène donc l'équation proposée, dans laquelle l'une des inc onnues contient le facteur 3^λ, à une autre semblable, dans laquelle l' une des inconnues ne contient plus que le facteur $3^{\lambda-1}$; en continuant de même, on ramènera l'équation pr oposée à une autre de la même forme dans laquelle une des inconnues ne pas divisible par 3. Donc l'équation proposée est impossible lorsque A est égal à un nombre premier $p = 18n + 5$; ou au carré q^2 d'un nombre premier $q = 18n+11$.

SECOND CAS. Considérons maintenant l'équation

$$x^3 + y^3 = 2^nAa^3,$$

dans laquelle A étant impair, le coefficient 2^nA représente l' un des quatre nombres $2p$, $2q^2$, $4p^2$, $4q$. Nous supposerons x, y, z entiers et premiers entre eux ; x et y étant impairs. De plus, nous ferons deux hypothèses suivant que z est ou n'est pas divisible par 3.

1°. *Supposons* z *non divisible par* 3. On arrive facilement à l'équation

$$f\,(f^2 - 9g^2) = 2^{n-1}Aa^3\ ;$$

mais $f^2 - 9g^2$ est impair, en même temps que $b = f^2 + 3g^2$ et l'on a

$$f = 2^{n-1}A\alpha^3, \quad f + 3g = \beta^3, \quad f - 3g = \gamma^3\ ;$$

ou bien

$$f = 2^{n-1}\alpha^3, \quad f + 3g = \beta^3, \quad f - 3g = \gamma^3 \;;$$

Ces deux décomposition conduisent aux deux équations

$$\beta^3 + \gamma^3 = 2^n A\alpha^3, \quad \text{ou} \quad A\beta^3 + \gamma^3 = 2^n\alpha^3 \;;$$

celles-ci sont impossibles suivant le module q, puisque, pour la première, les indéterminées α, β et γ ne sont pas divisible par 3.

2°. *Supposons z divisible par* 3. En posant $z = 3ab$, on arrive, comme plus haut à l'équation

$$g\,(f^2 - g^2) = 2^{n-1}Aa^3 \,,$$

et, puisque $f^2 - g^2$ est impair, à l' une des décompositions

$$g = 2^{n-1}A\alpha^3, \quad f + g = \beta^3, \quad f - g = \gamma^3 \;;$$

ou bien

$$g = 2^{n-1}\alpha^3, \quad f + g = A\beta^3, \quad f - g = \gamma^3 \,.$$

La seconde décomposition conduit à une équations déjà reconnue impossible ; la première conduit à l' équation

$$\beta^3 - \gamma^3 = 2^n A\alpha^3 \,.$$

Celle-ci est de même forme que la proposée ; mais l' indéterminée du second membre contiendra un facteur 3 en moins. On conclura, comme précédemment, que l' équation proposée est impossible à résoudre en nombres entiers.

SECTION 5.

Les six valeurs générales de A données par M. SYLVESTER sont, jusqu'à présent, les seules valeurs connues qui rendent insoluble l'équation donnée en ajoutant toutefois les valeurs

$$A = 1, 2, 3, 4, 18, 36,$$

données par FERMAT, EULER et LEGENDRE. On a encore le théorème suivant :

Pour que l'équation

$$X^3 + Y^3 = AZ^3,$$

soit vérifiée par des valeurs entières de $X, Y, Z, A,$ *il faut et suffit que* A *appartienne à la forme*

$$xy(x + y)$$

préalablement débarassée des facteurs cubiques qu' elle peut contenir.

En effet, on a l' identité

$$[x^3 - y^3 + 6x^2y + 3xy^2]^3 + [y^3 - x^3 + 6y^2x + 3yx^2]^3$$
$$= xy(x + y).3^3[x^2 + xy + y^2]^3 \,,$$

et l'on résout l'équation proposée, par les valeurs

$$\left\{\begin{aligned} X &= x^3 - y^3 + 6x^2y + 3xy^2, \\ Y &= y^3 - x^3 + 6y^2x + 3yx^2, \\ Z &= 3(x^2 + xy + y^2), \\ A &= xy(x + y). \end{aligned}\right.$$

Réciproquement, si l'équation est vérifiée pour les valeurs x_0, y_0, z_0 des variables, et si l'on pose

$$x = x_0^3, \quad y = y_0^3,$$

on a

$$xy(x + y) = A(x_0 y_0 z_0)^3.$$

C'est ce qu'il fallait démontrer. Il résulte encore de l'identité précédente que toute solution de l'équation proposée conduit à une série indéfinie d'autres solutions, en posant A constant. Il faut excepter le cas de $x = \pm y$.

EXEMPLE : Pour $x = 1$, $y = 2$, on a la solution

$$17^3 + 37^3 = 6.21^3\,;$$

de laquelle on déduit une série indéfinie d'autres solutions. Ainsi l'équation

$$x^3 + y^3 = 6z^3,$$

est résoluble en nombres entiers, et d'une infinité de manières, bien que LEGENDRE ait affirmé le contraire.

PARIS, *Mai, 1879.*