GÉNÉRATIONS GÉOMÉTRIQUE ET ALGÉBRIQUE DES TRIPLETS PYTHAGORICIENS

André STOLL
Lycée Couffignal Strasbourg

« *L'algèbre et la géométrie sont comme l'aveugle et le paralytique* » Jean Frenkel, un de mes professeurs à l'université de Strasbourg, rappelait régulièrement cette maxime à ses étudiants.

Récemment, en classant les « Ouverts » de ces dernières années, j'y ai repensé en revoyant la couverture du numéro 87 daté de juin 1997. Celle-ci présente *une construction très simple de toutes les fractions pythagoriciennes x/y, c'est-à-dire telles que $x^2+y^2=z^2$ avec x, y, z entiers naturels non nuls, premiers entre eux.* Cette construction est rappelée ci-dessous. La présentation se termine par la remarque suivante : *« le plus remarquable est que chaque triplet pythagoricien est ainsi obtenu, une et une seule fois »*[1] . Cette affirmation est donnée sans démonstration. Le but de cet article est d'en présenter une. Et, bien-sûr, l'algèbre nous rendra un grand service.

1. Génération géométrique des triplets pythagoriciens

La construction : Un cercle est inscrit dans un carré de côté unité dont l'un des sommets est P. Soit A l'un des points de tangence sur un côté du carré ne passant pas par le point P. La droite (AP) coupe le cercle en A'. Le rectangle $A'A_1A_2A_3$ inscrit dans le cercle donne le premier triplet (3, 4, 5) (Les côtés sont dans le rapport 4/3)

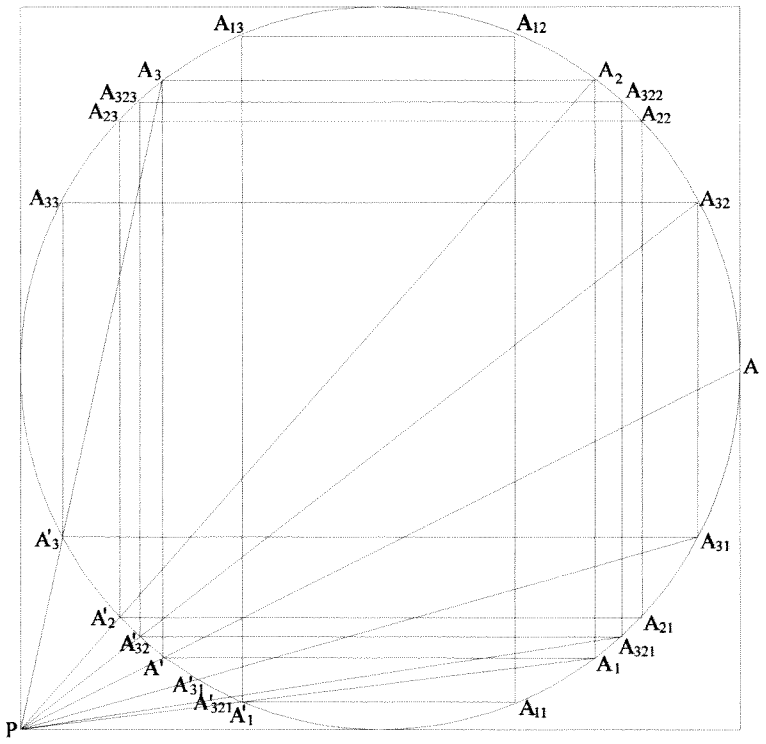


FIGURE 1

En joignant P à A_1, A_2 et A_3, on obtient A_1', A_2', A_3' les points d'intersection avec le cercle correspondant aux triplets (5,12,13), (21,20,29), (15,8,17)

[1] John H. CONWAY, *The book of numbers* p.172 Springer Verlag 1996

respectivement. Joignant à nouveau P aux sommets des rectangles inscrits on obtient d'autres triplets et ainsi de suite.

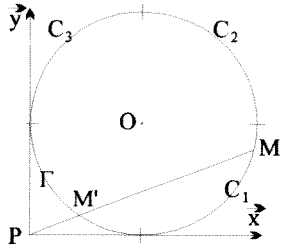
Théorème 1 :

Tout triplet pythagoricien est ainsi obtenu une et une seule fois.

2. La métamorphose : de géométrique, le problème devient algébrique

Dans le plan muni d'un repère orthonormé $\{P, \vec{x}, \vec{y}\}$, on considère le cercle C de centre $O\left(\frac{1}{2}, \frac{1}{2}\right)$ et de rayon $\frac{1}{2}$. On appelle respectivement C_1, C_2, C_3 et Γ les quarts de cercle C correspondant à : $C_1 : \frac{1}{2} \leq x \leq 1$ et $0 \leq y \leq \frac{1}{2}$; $C_2 : \frac{1}{2} \leq x \leq 1$ et $\frac{1}{2} \leq y \leq 1$; $C_3 : 0 \leq x \leq \frac{1}{2}$ et $\frac{1}{2} \leq y \leq 1$; $\Gamma : 0 < x < \frac{1}{2}$ et $0 < y < \frac{1}{2}$.

FIGURE 2



1. On appelle φ l'application de C sur lui-même qui à tout point M associe M' le deuxième point d'intersection de C avec la droite (PM).

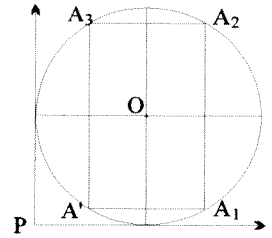
Proposition 1 : Si M a pour coordonnées (a, b) alors les coordonnées de M' sont $\left(\frac{a}{4d}, \frac{b}{4d}\right)$ où $d = a^2 + b^2$.

Démonstration : L'équation du cercle C est : $x^2 + y^2 - x - y + \frac{1}{4} = 0$, celle de la droite (PM) est : $y = \frac{b}{a}x$. Par substitution on est amené à résoudre l'équation du second degré : $(a^2 + b^2)\, x^2 - (a + b)\, ax + \frac{a^2}{4} = 0$.

Or $x = a$ est solution de cette équation. On en déduit l'autre solution puis le résultat ci-dessus.

2. Partant d'un point A' appartenant à Γ, on construit le rectangle $A'A_1A_2A_3$ dont les côtés sont parallèles aux axes de coordonnées et de telle sorte que $A_1 \in C_1$, $A_2 \in C_2$, $A_3 \in C_3$.

FIGURE 3



Il est clair que si A'(a,b) alors $A_1(1-a, b)$, $A_2(1-a,1-b)$, $A_3(a,1-b)$. L'application qui au point A' associe le point A_i (i=1, 2 ou 3) est notée ψ_i.

3. On appelle k l'application

$$k : \Gamma \longrightarrow \mathbb{R},\ A'(a, b) \longmapsto \frac{A'A_1}{A'A_3} = \frac{1-2a}{1-2b}.$$

4. Soit $\mathbf{T}$ l'ensemble des triplets pythagoriciens c'est-à-dire des triplets d'entiers naturels non nuls (n, p, q) tels que $n^2 + p^2 = q^2$ et PGCD(n, p, q) = 1.

Il n'est pas difficile de prouver que n et p sont de parités différentes. On peut alors prendre le nombre n impair ; (n, p, q) $\in \mathbf{T}$ étant donné, on cherche un point $A'(x,y) \in \Gamma$ tel que $k(A') = \frac{n}{p}$. Cette recherche conduit au système suivant :

$x^2 + y^2 - x - y + \frac{1}{4} = 0$, $0 \le x \le \frac{1}{2}$ et $\frac{1-2x}{1-2y} = \frac{n}{p}$. Ce système a exactement une solution : $x = \frac{q-n}{2q}$ et $y = \frac{q-p}{2q}$. Cette application $\mathbf{T} \longrightarrow \Gamma$ est notée f.

5. La construction géométrique du §1, nous indique comment calculer trois nouveaux triplets pythagoriciens à partir d'un triplet pythagoricien. Cette méthode est résumée dans le tableau suivant :

$$\mathbf{T} \xrightarrow{f} \Gamma \xrightarrow{\psi_i} C_i \xrightarrow{\varphi} \Gamma \xrightarrow{k} \mathbb{Q} \longrightarrow \mathbf{T}$$

$$(n,p,q) \longmapsto A' \longmapsto A_i \longmapsto A'_i \longmapsto k(A'_i) = \frac{N}{P} \longmapsto (N, P, Q=\sqrt{N^2+P^2})$$

$$\mathbf{A'}\left(\frac{q-n}{2q}, \frac{q-p}{2q}\right) \quad \mathbf{A_1}\left(\frac{q+n}{2q}, \frac{q-p}{2q}\right) \quad \mathbf{A_2}\left(\frac{q+n}{2q}, \frac{q+p}{2q}\right) \quad \mathbf{A_3}\left(\frac{q-n}{2q}, \frac{q+p}{2q}\right)$$

$$\mathbf{A'_1}\left(\frac{q+n}{2(2n-2p+3q)}, \frac{q-p}{2(2n-2p+3q)}\right) \quad \mathbf{A'_2}\left(\frac{q+n}{2(2n+2p+3q)}, \frac{q+p}{2(2n+2p+3q)}\right) \quad \mathbf{A'_3}\left(\frac{q-n}{2(-2n+2p+3q)}, \frac{q+p}{2(-2n+2p+3q)}\right)$$

$N_1 = n-2p+2q$	$N_2 = n+2p+2q$	$N_3 = -n+2p+2q$
$P_1 = 2n-p+2q$	$P_2 = 2n+p+2q$	$P_3 = -2n+p+2q$
$Q_1 = 2n-2p+3q$	$Q_2 = 2n+2p+3q$	$Q_3 = -2n+2p+3q$

6. L'introduction des matrices permet de simplifier les notations. Posons

$$R_1 = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix} \quad R_2 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix} \quad R_3 = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}.$$

Avec ces notations : $\begin{pmatrix} N_i \\ P_i \\ Q_i \end{pmatrix} = R_i \begin{pmatrix} n \\ p \\ q \end{pmatrix}$

7. Remarque : le lecteur vérifiera que les trois triplets (N_i,P_i,Q_i) ainsi obtenus sont des triplets pythagoriciens et que de plus $N_i > n$ et $P_i > p$.

3. Génération algébrique des triplets pythagoriciens

Théorème 2 :

Tout triplet pythagoricien peut être obtenu à partir du triplet pythagoricien (3,4,5) par application répétée de R_1, R_2 R_3. De plus, cette décomposition est unique.
En d'autres termes : soit $t \in \mathbf{T}$, il existe un et un seul p-uplet $(i_1, i_2, \ldots i_p)$ avec $i_k \in \{1,2,3\}$ tel que $t = R_{i_1} R_{i_2} \ldots R_{i_p} \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$

Démonstration du Théorème 2

Proposition 2 : Soit $t = (a,b,c) \in \mathbf{T}$, $t \neq (3,4,5)$ alors un et un seul des 3 triplets $t_i = R_i^{-1}(t)$ avec $i \in \{1,2,3\}$ est un triplet pythagoricien.

Démonstration :

Les inverses des matrices R_1, R_2, R_3 sont :

$$R_1^{-1} = \begin{pmatrix} 1 & 2 & -2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}, R_2^{-1} = \begin{pmatrix} 1 & 2 & -2 \\ 2 & 1 & -2 \\ -2 & -2 & 3 \end{pmatrix},$$

$$R_3^{-1} = \begin{pmatrix} -1 & -2 & 2 \\ 2 & 1 & -2 \\ -2 & -2 & 3 \end{pmatrix}.$$

En posant $\begin{cases} \alpha = a+2b-2c \\ \beta = -2a-b+2c \\ \gamma = -2a-2b+3c \end{cases}$ on a : $t_1 = (\alpha,\beta,\gamma)$, $t_2 = (\alpha,-\beta,\gamma)$, $t_3 = (-\alpha,-\beta,\gamma)$.Il est clair que $\alpha^2+\beta^2=\gamma^2$ et que PGCD$(\alpha,\beta,\gamma) = 1$.

Supposons $\alpha = 0$, alors $2c = a + 2b$. D'où en élevant au carré et en introduisant $a^2 + b^2 = c^2$: $4c^2 = a^2 + 4b^2 + 4ab = 4a^2 + 4b^2$. Et, après simplification : $4b = 3a$. On en déduit l'existence d'un nombre e tel que : $a=4e$, $b=2e$, $c=5e$.

Enfin, comme PGCD$(a,b,c) = 1$, on a : $a=4$, $b=3$, $c=5$. Ce cas ayant été exclus, on a nécessairement $\alpha > 0$ ou $\alpha < 0$. De la même manière, on a nécessairement $\beta > 0$ ou $\beta < 0$. Enfin, lorsque $\alpha < 0$ alors on a aussi $\beta < 0$ car $\beta = \alpha - 3(a+b) + 4c$. En effet $\alpha > 0 \Leftrightarrow a+2b<2c \Leftrightarrow \frac{4}{3}b<a$ et de même $\beta < 0 \Leftrightarrow \frac{3}{4}b<a$, d'où le résultat.

Finalement, si $\alpha > 0$ et $\beta > 0$ alors seul $t_1 \in \mathbf{T}$, si $\alpha > 0$ et $\beta < 0$ alors seul $t_2 \in \mathbf{T}$ et si $\alpha < 0$ alors $\beta < 0$ et seul $t_3 \in \mathbf{T}$.

Proposition 3 : Soit (a_1,b_1,c_1) ce triplet, alors $a>a_1$

Démonstration : En effet, si $\alpha > 0$ alors :

$a_1 = \alpha = a + 2(b - c) < a$ car $c > b$ et si $\alpha < 0$ alors $a_1 = -\alpha = -a -2b +2c = a +2(c - a - b) < a$.

En réitérant le processus, on construit une suite d'éléments de $\mathbf{T}$: (a, b, c), (a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3), …

La méthode de descente infinie

Cette méthode, inventé par Pierre de Fermat (1601-1665) peut s'énoncer de la manière suivante : il n'existe qu'un nombre fini d'entiers plus petits qu'un entier donné. On peut également l'énoncer de la manière suivante :

Soit (a_n) une suite décroissante d'entiers naturels, alors il existe $m \in \mathbb{N}$, tel que pour tout $n \geq m$, $a_n = a_m$.

Pierre de Fermat a utilisé cette méthode pour prouver le théorème : « *L'aire d'un triangle rectangle en nombres ne peut être un carré* » ce que l'on traduirait actuellement en disant que le système d'équations :

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2c \end{cases}$$

n'a pas de solution dans $\mathbb{N}^3$ autre que la solution évidente $a = b = c = 0$.

Pour démontrer ce théorème, P. Fermat suppose qu'un tel triangle (a,b,c) existe. Il construit alors un triangle (a',b',c') ayant les mêmes propriétés et tel que : $a'<a$, $b'<b$, $c'<c$. Il obtient ainsi une suite strictement décroissante de nombres entiers naturels.

Ce qui est impossible.

Je renvoie le lecteur intéressé par cette démonstration au livre de Catherine Goldstein, **Un théorème de Fermat et ses lecteurs** *aux éditions Presses Universitaires de Vincennes.*

Proposition 4 : Cette suite est finie.

En d'autres termes, il existe un entier naturel m tel que $(a_m, b_m, c_m) = (3, 4, 5)$.

Démonstration : il suffit d'appliquer la méthode dite de descente infinie de Fermat (voir encadré).

EXEMPLE : La démonstration ci-dessus nous fournit une méthode pour calculer le p-uplet $(i_1, i_2, \ldots i_p)$.

$t_1 = (2\,225, 3\,648, 4\,273)$ $\quad t_2 = R_1^{-1}(t_1) = (975, 448, 1\,073)$

$t_3 = R_3^{-1}(t_2) = (275, 252, 373)$ $\quad t_4 = R_2^{-1}(t_3) = (33, 56, 65)$

$t_5 = R_1^{-1}(t_4) = (15, 8, 17)$ $\quad t_6 = R_3^{-1}(t_5) = (3, 4, 5)$

et par conséquent : $(2\,225, 3\,648, 4\,273) = R_1 R_3 R_2 R_1 R_3 (\mathbf{3}, \mathbf{4}, \mathbf{5})$

Relation entre les théorèmes 1 et 2

Ces deux théorèmes sont clairement équivalents. (Il suffit de se souvenir que le produit de la matrice R_i par un triplet pythagoricien correspond à la construction $\psi_i \circ \varphi$).

Par exemple, la construction du point du cercle C qui correspond au triplet $t_1 = (2\,225, 3\,648, 4\,273)$ est la suivante :

$$A \xmapsto{\varphi} A' \xmapsto{\psi_3} A_3 \xmapsto{\varphi} A'_3 \xmapsto{\psi_1} A_{31} \xmapsto{\varphi} A_{31} \xmapsto{\psi_2} A_{312} \xmapsto{\varphi} A_{312} \xmapsto{\psi_3} A_{3123} \xmapsto{\varphi} A'_{3123} \xmapsto{\psi_1} A_{31231}$$

4. Équations $x^2 + y^2 + z^2 = t^2$ et $x^2 + y^2 = z^2 + t^2$

1. Quelques solutions de ces deux équations.

Soit t un nombre entier quelconque ; le quadruplet (x, y ,z, t) = (t, 0, 0, t) est solution de l'équation $x^2 + y^2 = z^2 + t^2$; soit M une matrice produit dans un ordre quelconque des matrices R_1, R_2, R_3 , alors les produits $M\begin{pmatrix}t\\0\\0\end{pmatrix}$ et $M\begin{pmatrix}0\\t\\0\end{pmatrix}$ nous donnent deux autres solutions de cette équation et le produit $M\begin{pmatrix}0\\0\\t\end{pmatrix}$ nous donne une solution de l'équation $x^2 + y^2 + t^2 = z^2$.

EXEMPLE : $M = R_1 R_2^2 R_3 = \begin{pmatrix}-89 & 92 & 128\\ -188 & 191 & 268\\ -208 & 212 & 297\end{pmatrix}$;

$x = -89$, $y = -188$, $z = -208$, $t = 1$et $x = 92$, $y = 191$, $z = 212$, $t = 1$ vérifient $x^2 + y^2 = z^2 + t^2$;

$x = 128$, $y = 268$, $z = 297$, $t = 1$ vérifie $x^2 + y^2 + t^2 = z^2$.

2. Ensemble des solutions de $x^2 + y^2 = z^2 + t^2$

Soit $t \in \mathbb{N}^*$ fixé .

Posons $S(t) = \left\{(a;b;c) \in \mathbb{N}^3 \,\middle|\, a^2 + b^2 = c^2 + t^2\right\}$. Il est aisé de montrer que si $X \in S(t)$ alors $R_iX \in S(t)$ pour $i \in \{1,2,3\}$.

Inversement, à quelle condition $R_i^{-1}X$ appartient-il à S(t) ?

Avec les notations du § 0, posons $X = \begin{pmatrix}a\\b\\c\end{pmatrix}$ et $\gamma = -2a - 2b + 3c$.

$(\gamma - c)(c+a+b) = 2(c-(a+b))(c+(a+b)) = -2(2ab + a^2 + b^2 - c^2) = -2(2ab + t^2) < 0$

Comme $a + b + c > 0$, on a nécessairement $\gamma < c$.

Si $\gamma \geq 0$ alors, de la même manière qu'au § 0, l'un des trois vecteurs $R_i^{-1}X$ appartient à S(t) et on recommence la même procédure. Posons à présent :

$E(t) = \{X \in S(t) \mid \gamma < 0\}$; nous pouvons énoncer le

Théorème 3

Quel que soit $X \in S(t)$, X est de la forme MU où $U \in E(t)$ et M est produit dans un ordre quelconque des matrices R_i.

Le problème qui se pose alors est de trouver l'ensemble E(t) c'est-à-dire l'ensemble des solutions du système $\begin{cases} a^2 + b^2 = c^2 + t^2 & (1) \\ 3c < 2a + 2b & (2) \end{cases}$

En élevant l'inéquation (2) au carré et en multipliant (1) par 9, on obtient tout calcul fait : $5a^2 + 5b^2 - 8ab < 9t^2$; a et b jouent des rôles symétriques. Il suffit donc de chercher les solutions vérifiant $a \leq b$.

Enfin pour b fixé, l'étude de la fonction définie pour $a \in [b, +\infty[$:
$a \longmapsto \Psi_b(a) = 5a^2 - 8ab + 5b^2 - 9t^2$, montre que l'on peut se limiter au cas où $0 \leq b \leq \frac{\sqrt{3}}{2} t$, $0 \leq a \leq \frac{\sqrt{3}}{2} t$.

EXEMPLES

$\boxed{t = 1}$, $E(1) = \{(1,0,0),(0,1,0),(1,1,1)\}$

$\boxed{t = 7}$ $\frac{3}{\sqrt{2}} t \approx 14{,}8$: il suffit de chercher a, b, c vérifiant $c^2 = a^2 + b^2 - 7^2$,

$0 \leq a \leq 14$, $0 \leq b \leq 14$. Un tableur nous rendra quelques services (première ligne : a ; première colonne : b ; puis dans chaque case le nombre $a^2 + b^2 - 7^2$)

b\a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	-49	-48	-45	-40	-33	-24	-13	**0**	15	32	51	72	95	120	147
1		-47	-44	-39	-32	-23	-12	**1**	**16**	33	52	73	96	**121**	148
2			-41	-36	-29	-20	-9	**4**	19	**36**	55	76	99	124	151
3				-31	-24	-15	-4	**9**	24	41	60	**81**	104	129	156
4					-17	-8	3	**16**	31	48	67	88	111	136	163
5						**1**	12	**25**	40	57	76	97	120	145	172
6							23	**36**	51	68	87	108	131	156	183
7								**49**	**64**	**81**	**100**	**121**	**144**	**169**	**196**
8									79	96	115	136	159	184	211
9										113	132	153	176	201	228
10											151	172	195	220	247
11												193	216	241	268
12													239	264	291
13														**289**	316
14															343

Le triplet a =13, b =1, c =11 ne convient pas car $3c \geq 2a + 2b$

$E(7) = \{(5,5,1)(8,1,4)(1,8,4)(9,2,6)(2,9,6)(11,3,9)(3,11,9)(13,13,17)(7,b,b)(b,7,b) \mid 0 \leq b \leq 14\}$

Le

Théorème 3 peut être généralisé à $\mathbb{Z}^3$ de la manière suivante :

Théorème 4

Quel que soit $X = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{Z}^3$ tel que $a^2 + b^2 = c^2 + t^2$, X est de la forme MU ou JMU où $U \in E(t)$, $J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ et M est produit dans un ordre quelconque des matrices R_i ou $(R_i)^{-1}$.

En effet, le produit de X par l'une des trois matrices $I_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $I_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, ou J nous ramène aux hypothèses du

Théorème 3.

Or $I_1 = R_2^{-1}R_3 = R_3^{-1}R_2$ et $I_2 = R_1^{-1}R_2 = R_2^{-1}R_1$. D'où le résultat.

Exemple : $X = \begin{pmatrix} -17 \\ -6 \\ 18 \end{pmatrix}$, $X = I_1\, I_2 \begin{pmatrix} 17 \\ 6 \\ 18 \end{pmatrix} = I_1\, I_2 R_3^2 R_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = R_3^{-1}R_1R_3^2R_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

5. Le groupe orthogonal

On l'aura compris : si tout ceci « marche bien » c'est tout simplement parce que les matrices R_1, R_2, R_3 sont des matrices orthogonales pour la forme quadratique

$$Q(x,y,z) = x^2 + y^2 - z^2 \quad (*)$$

Pour ceux qui l'auraient oublié, je rappelle qu'une matrice M est dite orthogonale (sous-entendu pour la forme quadratique Q) lorsque :

$$\forall X \in \mathbb{R}^3 \quad Q(MX) = Q(X) \quad (**)$$

En introduisant la matrice $J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ et en posant $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ la relation (*) se traduit par l'égalité $Q(X) = {}^tXJX$ et (**) par ${}^tMJM = J$.

L'ensemble des matrices orthogonales forme un groupe noté O(Q).

Si $M \in O(Q)$ et $N \in O(Q)$ alors :

— $MN \in O(Q)$ car ${}^t(MN)J(MN) = {}^tN({}^tMJN)\,N = {}^tNJN = J$;

— M est inversible car $dét(J) = dét(MJM) = dét^2(M)\, dét(J)$ donc $dét(M) = \pm 1$;

— $M^{-1} \in O(Q)$ car $t(M^{-1})JM^{-1} = (MJ^tM)^{-1} = J$.

Considérons à présent le sous-ensemble E des matrices orthogonales à coefficients entiers. E est un sous-groupe de O(Q) car si $M \in E$ et $N \in E$ alors $MN \in E$ (évident parce que $\mathbb{Z}$ est un anneau) et $M^{-1} \in E$ car $dét(M) = \pm 1$.

Théorème 5

E est engendré par les trois matrices R_1, R_2, R_3, leurs inverses et la matrice J.

Tout d'abord, il est clair que ces sept matrices appartiennent à E.

Inversement, soit $P \in E$; il s'agit de montrer que P est produit de ces matrices.

Introduisons la forme polaire de Q, c'est-à-dire l'application $\varphi : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$, $(X, Y) \longmapsto \varphi(X, Y) = {}^tXJY$ {en particulier $Q(X) = \varphi(X, X)$}.

En appelant, e_1, e_2, e_3 les trois vecteurs colonnes qui forment P, on a :

$$Q(e_1) = Q(e_2) = 1 \ , \ Q(e_3) = -1 \quad \text{et lorsque } i \neq j \ , \ \varphi(e_i, e_j) = 0 \quad (¤)$$

Comme $Q(e_1) = 1$, il existe une matrice M produit dans un ordre quelconque des matrices R_i ou $(R_i)^{-1}$ telle que : $e_1 = Me$ ou $e_1 = JMe$ avec $e \in E(1)$ (voir § 4 et **Théorème 4**).

Posons pour i=1,2,3 $f_i = M^{-1}(e_i) = \begin{pmatrix} a_i \\ b_i \\ c_i \end{pmatrix}$. $M \in E$, les relations (¤) sont conservées : $Q(f_1) = Q(f_2) = 1$, $Q(f_3) = -1$ et lorsque $i \neq j$, $\varphi(f_i, f_j) = 0$

Lorsque $e = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ alors $a_2 + b_2 - c_2 = 0$ et $a_2^2 + b_2^2 - c_2^2 = 1$. D'où $2\,a_2b_2 = -1$. Cette équation n'a pas de solution dans l'ensemble des entiers. Ce cas n'est pas possible. On a donc $e = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ puis $\varphi(f_1, f_2) = 0 \Rightarrow a_2 = 0$ et $Q(f_2) = 1 \Rightarrow b_2 - c_2 = 1$ et par conséquent $f_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ ou $f_2 = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$. De la même manière, $f_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ ou $f_3 = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$.

Finalement : $P=(e_1, e_2, e_3) = M(f_1, f_2, f_3) = MS$ où S est produit des matrices I_1, I_2 et J. Or $I_1 = R_2^{-1}R_3 = R_3^{-1}R_2$ et $I_2 = R_1^{-1}R_2 = R_2^{-1}R_1$ et la démonstration est terminée.

Exemple : $P = \begin{pmatrix} -17 & -6 & 18 \\ -6 & -1 & 6 \\ 18 & 6 & -19 \end{pmatrix}$

$e_1 = I_1\, I_2 \begin{pmatrix} 17 \\ 6 \\ 18 \end{pmatrix} = I_1\, I_2 R_3^2 R_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = R_3^{-1}R_1R_3^2R_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ et $P = R_3^{-1}R_1R_3^2R_2J$.

Questionnement

Ce paragraphe pourrait faire l'objet de problèmes de la rubrique « À vos stylos »

1. Comment construire géométriquement les solutions des équations du § 4 – à la manière de la construction qui est à l'origine de cette article – ?
2. Trouver des générateurs du sous groupe E du groupe de Lorentz formé des matrices à coefficients entiers. (Rappel : le groupe de Lorentz est le groupe orthogonal de la forme quadratique $Q(x,y,z,t) = x^2 + y^2 + z^2 - t^2$)
3. Même question pour le sous groupe E du groupe orthogonal de la forme quadratique $Q(x,y,z,t) = x^2 + y^2 - z^2 - t^2$ formé des matrices à coefficients entiers.