Ramifications Mathématiques

(Cette chronique a pour but de présenter des sujets variés de l'arbre des mathématiques, sous forme d'exemples simples et de questions intégrées au texte, de façon à mettre en évidence des résultats mathématiques fondamentaux).

CARACTERISATION DE CERTAINES ALGEBRES

par Robert V. Anderson
Université du Québec à Mtl

Le texte qui suit est dû à R.V. Anderson, professeur à l'U.Q.A.M.. Il contient des caractérisations élégantes de certaines algèbres. Merci à M. Anderson pour avoir bien voulu en faire l'objet de cette chronique qui, habituellement, revient exclusivement à Gilbert Labelle.

0. *INTRODUCTION:*

Historiquement, la structure des réels $\mathbb{R}$ a été la source de beaucoup de progrès en mathématiques. En fouillant ses sous-structures on considéra certains anneaux ou sous-corps tels les entiers algébriques réels, les rationnels, les nombres algébriques réels, les nombres du type $\alpha + \beta\sqrt{2}$ (où α, $\beta \in \mathbb{Q}$) etc.

On fut naturellement amené à des sur-structures de $\mathbb{R}$ par l'étude des polynômes à coefficients réels qui n'avaient pas toutes leurs racines réelles. Le corps $\mathbb{C}$ des nombres complexes fit alors son apparition comme sur-corps (ou extension) du corps $\mathbb{R}$. Comme, vectoriellement, $\mathbb{R}^2 \approx \mathbb{C}$ on réalisa que de nouvelles notions méritaient une attention spéciale: celle d'espace vectoriel et celle d'algèbre (i.e. espace vectoriel muni d'une multiplication compatible de vecteurs entre eux pour obtenir encore des vecteurs). Les quaternions (algèbre spéciale sur $\mathbb{R}^4$) se situaient dans les premiers exemples et fournissaient même une structure de corps (non commutatif) englobant $\mathbb{R}$ aussi bien que $\mathbb{C}$ et permettait de faire de la géométrie à 4 dimensions. Ce travail caractérise et classifie des algèbres semblables.

1. *DEFINITIONS:*

Dans cet article, on appelle anneau tout ensemble R muni de deux opérations " + " et " . " telles que R est un groupe abélien pour l'opération " + " et où pour l'opération " . " on a:

1) Fermeture: $x, y \in R \Longrightarrow x \cdot y \in R$

2) Distributivité:
$\forall x, y, z \in R$: $x.(y+z) = xy + xz$, $(x+y)z = x.z + y.z$

3) Il existe un élément neutre unique 1 tel que:
pour tout $x \in \mathbb{R}$, $x.1 = 1.x = x$.

Remarquer que l'associativité n'est pas requise dans notre contexte! On appelle anneau de division tout anneau dont chaque élément $x \neq 0$ possède un inverse multiplicatif unique x^{-1} tel que $xx^{-1} = x^{-1}x = 1$. Il est à noter qu'un anneau de division peut contenir des éléments $x \neq 0$ et $y \neq 0$ tels que $xy = 0$.

Un antiautomorphisme involutif T d'un anneau R est un antiendomorphisme bijectif de R tel que $T^2 = I$, l'identité. Donc, pour tout $x, y \in R$, on a:

1) $T(x+y) = T(x) + T(y)$

2) $T(x \cdot y) = T(y)T(x)$

3) $T\left[T(x)\right] = T^2(x) = I(x) = x$

En général, on notera $T(z) = \bar{z}$

On appelle Q-anneau un anneau R de division tel que:

I) R admet un antiautomorphisme involutif T, différent de l'identité, tel que l'ensemble X des éléments invariants sous T est isomorphe à $\mathbb{R}$.

II) $X \subseteq C_R \cap A_R$ où C_R est le centre de R et
$A_R = \left\{ z \in R \;\middle|\; \forall\, y_1, y_2 \in R : z(y_1y_2) = (zy_1)y_2 \right\}$

III) $\forall\, z \in R : z\bar{z} = 0 \longrightarrow z = 0$

Un Q*-anneau est un Q-anneau avec la propriété suivante pour la multiplication.
(*) Si $x, y \in R$ alors $x(xy) = x^2y$ et $(yx)x = yx^2$.

On pourrait dire qu'un Q-anneau est une "algèbre" sur le corps $\mathbb{R}$ des nombres réels.

Dorénavant, le symbole R désignera un Q*-anneau.

Comme T est différent de l'identité, il existe un élément $z \in R$ tel que $\bar{z} \neq z$. Si $w = z - \bar{z}$, alors $\bar{w} = -w$. Notons par Y l'ensemble de tous les éléments w de R tels que $\bar{w} = -w$. Chaque $w \in Y$ est appelé élément pur de R. Il est clair que $X \cap Y = \{0\}$. Si $z \in R$ alors $z = x + v$ où $x = \frac{1}{2}(z+\bar{z}) \in X$ et $v = \frac{1}{2}(z-\bar{z}) \in Y$. De plus, si $z_1 = x_1 + v_1$ et $z_2 = x_2 + v_2$ avec $x_1, x_2 \in X$, $v_1, v_2 \in Y$, alors $z_1 = z_2 \Longrightarrow x_1 = x_2$ et $v_1 = v_2$. Donc il n'y a rien qui nous empêche d'écrire $R = X \oplus Y$.
(La somme directe de X et Y).

2. *La norme N(z) d'un Q*-anneau*:

La norme N(z) de R est l'application $N : R \longrightarrow X$ définie par $N(z) = z\bar{z}$.

Lemme 2.1 La norme N(z) possède les propriétés suivantes:

(1) $N(z) = N(\bar{z})$ et (2) $N(z) \geq 0$.

Démonstration:

(1) Soit $z = x + v$, un élément de R. Alors $\bar{z} = 2x - z$. Donc $z\bar{z} = z[2x - z] = 2xz - z^2 = (2x - z)z = \bar{z}z$.

(2) D'abord, si $x \in X$, alors $N(x) = x^2 \geq 0$. Si $0 \neq v \in Y$ alors $v^2 = -N(v) = -v\bar{v}$. Donc $v^2 \in X$. Supposons que $v \neq 0$ et que $v^2 = N > 0$. Alors $v^2 - N = (v + \sqrt{N})(v - \sqrt{N}) = -(v + \sqrt{N})(\overline{v + \sqrt{N}}) = 0$ qui implique (voir 3), $v = \pm\sqrt{N}$. Ceci est une contradiction puisque $v \notin X$. Donc $v^2 = -N$ où $N > 0$. Si $z = x + v$ on aura $N(z) = N(x) + N(v)$. Enfin $N(z) = 0 \Longrightarrow N(x) = N(v) = 0$, d'où $x = v = 0$. Observons que si $z \neq 0$ alors $z^{-1} = \frac{\bar{z}}{N(z)}$.

Lemme 2.2 $\forall z, w \in R,\ \bar{z}(zw) = z(\bar{z}w) = (wz)\bar{z} = (w\bar{z})z = N(z)w.$

Démonstration:

Il existe $x \in X$ et $v \in Y$ tels que $z = x + v$. Alors $\bar{z}(zw) = (2x - z)(zw)$ $= 2x(zw) - z^2w = (2xz - z^2)w = \left[(2x - z)z\right] w = (\bar{z}z)w = N(z)w$. Les autres égalités sont établies de façon semblable.

Lemme 2.3 $\forall z, w \in R,\ N(zw) = N(z)N(w)$.

Démonstration:

Posons $\lambda = zw$. Alors $\bar{z}N(zw) = \bar{z}N(\lambda) = \bar{z}(\lambda\bar{\lambda}) = (\bar{z}\lambda)\bar{\lambda} = \left[\bar{z}(zw)\right]\bar{\lambda}$ $= N(z)\left[w\bar{\lambda}\right] = N(z)\left[w(\bar{w}\bar{z})\right] = N(z)N(w)\bar{z}$, d'où

(2.1) $\bar{z}\left[N(zw) - N(z)N(w)\right] = 0.$

Or, du Lemme 2.2 il s'ensuit que, dans un Q*-anneau, $A\,B = 0$ entraîne $A = 0$ ou $B = 0$ ou bien $A = B = 0$. Donc, si $z \neq 0$ alors $\bar{z} \neq 0$ et notre lemme se prouve à partir de (2.1). Si $z = 0$, alors $zw = 0$ d'où $N(zw) = 0 = 0.N(w) = N(z)N(w)$.

3. *Structure de R dans le cas commutatif:*

Soit R un Q*-anneau. Il existe au moins un élément $v \in R$ tel que $\bar{v} = -v$ avec $v \neq 0$. Posons $I = \frac{v}{\sqrt{N(v)}}$. Il est clair $I^2 = -1$. Considérons le sous-anneau Ω_2 de R défini comme suit:

(3.1) $\Omega_2 = \left\{ z \in R \,\middle|\, z = x_0 + x_1 I\ ,\ x_0\ ,\ x_1 \in X \right\}.$

Or, soit R commutatif et $z = x + v$, un élément de R. Alors $\overline{vI} = \bar{I}\bar{v} = Iv = vI$, impliquant que $vI = -y$ où $y \in X$ d'où $z = x + yI \in \Omega_2$.

Théorème 3.1 Un Q*-anneau est commutatif si et seulement si il est isomorphe au corps $\mathbb{C}$ des nombres complexes.

Pour le reste de cet article, on suppose que R est strictement non-commutatif.

4. *Structure de R lorsque R est associatif et non-commutatif:*

Si R est strictement non-commutatif, il doit exister un élément J tel que $J \in R$ mais $J \notin \Omega_2$. On peut supposer que J est pur et que $J^2 = -1$. Soit Ω_3 l'ensemble défini par

$$(4.1) \qquad \Omega_3 = \left\{ z \in R \mid z = x_0 + x_1 I + x_2 J,\ x_0, x_1, x_2 \in X \right\}.$$

L'ensemble Ω_3 n'est pas clos par rapport à la multiplication de R. Ceci peut être démontré par l'absurde comme suit. Si Ω_3 est clos, alors $IJ \in \Omega_3$.

Alors $IJ = y_0 + y_1 I + y_2 J$ où $y_0, y_1, y_2 \in X$. Donc $I(IJ) = I^2 J = -J = y_0 I - y_1 + y_2 IJ$ d'où $(-y_1 + y_0 y_2) + (y_0 + y_1 y_2)I + (1 + y_2^2)J = 0$. Comme $1 + y_2^2 \neq 0$, ceci est une contradiction car $J \notin \Omega_2$.

Posons $K = IJ$ et $\Omega_4' = \left\{ z \in R \mid z = x_0 + x_1 I + x_2 J + x_3 K \text{ où } x_0, x_1, x_2, x_3 \in X \right\}$. Introduisons le changement de base défini par

$$i = I\ ,\ j = \frac{cI + J}{\sqrt{N(cI + J)}}\ ,\ k = i\,j \quad \text{où} \quad c = \tfrac{1}{2}(IJ + JI).$$

Si $\Omega_4 = \left\{ z \in R \mid z = y_0 + y_1 i + y_2 j + y_3 k \right\}$ où $y_0, y_1, y_2, y_3 \in X$, il est évident que $\Omega_4 = \Omega_4'$. De plus, on voit facilement que

$$i^2 = j^2 = k^2 = -1\ ,\ ij = k\ ,\ ji = -k\ ,\ jk = i\ ,\ kj = -i\ ,\ ki = j\ ,\ ik = -j$$

Un élément $x = x_0 + x_1 i + x_2 j + x_3 k$ de Ω_4 peut être écrit sous la forme $x = z + wj$ où z et w sont deux nombres complexes et j n'est pas un nombre complexe, mais $j^2 = -1$. De plus, $\bar{x} = \bar{z} + \overline{wj} = \bar{z} + \bar{j}\bar{w} = \bar{z} - j\bar{w} = \bar{z} - wj$. La norme N(x) est exprimée par

$$N(x) = x\bar{x} = (z + wj)(\bar{z} - wj) = z\bar{z} + w\bar{w} \geq 0\ .$$

Si $x_1 = z_1 + w_1 j$ et $x_2 = z_2 + w_2 j$, alors

$x_1 x_2 = (z_1 z_2 - \overline{w}_2 w_1) + (z_1 w_2 + w_1 \overline{z}_2) j$

Observons que la correspondance

$$S : z + wj \longrightarrow \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}$$

est un isomorphisme de Ω_4 dans l'anneau des matrices deux par deux où les éléments sont des nombres complexes. Il s'ensuit que la multiplication définie dans Ω_4 est associative puisque celle sur ces matrices l'est.

On appelle quaternion un élément de Ω_4. Cette algèbre non-commutative est due à W.R. Hamilton. L'idée de Hamilton était d'utiliser les quaternions comme on utilise aujourd'hui les vecteurs. L'avantage principal est que la division est possible avec les quaternions tandis qu'elle ne l'est pas pour les vecteurs. Le désavantage principal, c'est que cette algèbre ne se généralise pas à plusieurs dimensions comme dans le cas des vecteurs ordinaires.

Théorème 4.1 Un Q*-anneau, strictement non-commutatif, est associatif si et seulement s'il est isomorphe à l'algèbre des quaternions.

Tout ce qui reste à faire pour la démonstration de ce théorème est de prouver que $R = \Omega_4$ lorsque R est associatif. Supposons que $P \in R$ mais $P \notin \Omega_4$. On peut supposer que $P \in Y$ et que $P^2 = -1$. Or, il existe trois éléments C_1, C_2, C_3 de X tels que:

$$iP + Pi = C_1 \ , \quad jP + Pj = C_2 \ , \quad kP + Pk = C_3 \ .$$

Alors $Pk = P(ij) = (Pi)j = (c_1 - iP)j = c_1 j - i(Pj) = c_1 j - i(c_2 - jP) = c_1 j - c_2 i + kP = c_1 j - c_2 i + c_3 - Pk$, d'où $2Pk = c_1 j - c_2 i + c_3$, qui entraîne que $2P = c_1 i + c_2 j + c_3 k$. Ceci contredit le fait que $P \notin \Omega_4$.

5. *La détermination de R lorsqu'il est strictement non-commutatif et non-associatif:*

Si R n'est pas associatif, il doit exister un élément $E \in R$ tel que $E \notin \Omega_4$. On peut supposer que $E \in Y$ et que $E^2 = -1$. De plus, on peut prendre pour acquis que $iE = I$, $jE = J$ et $kE = K$ sont des éléments purs, car si ceci n'était pas le cas, on aurait

$iE + Ei = c_1$, $jE + Ej = c_2$, $kE + Ek = c_3$, $c_1, c_2, c_3 \in X$.

Etant donné cela, on pourrait remplacer E par $E^* = E'/\sqrt{N(E')}$ où

$E' = E + \frac{1}{2}c_1 i + \frac{1}{2}c_2 j + \frac{1}{2}c_3 k$.

Plus loin, on démontrera que les éléments 1, i, j, k, E, I, J, K sont linéairement indépendants, ce qui prouvera qu'il n'existe pas de Q*-anneaux pour les dimensions 5, 6 et 7.

Considérons l'ensemble $\Omega = \Omega_8$ défini par

$$\Omega = \left\{ z \mid z = q + QE \ , \ q, Q \in \Omega_4 \right\}.$$

A cause de l'axiome (*) d'un Q*-anneau, on trouve que $(q + QE)^2 E = (q + QE)\left[(q + QE)E \right]$, d'où la condition suivante

$$(5.1) \quad -qQ + (QE)(qE) = \left[q(QE) + (QE)q \right] E = \lambda E$$

Si q est un élément pur, alors $\lambda \in X$. Donc $(QE)(qE) = qQ + \lambda E$. Par le Lemme 2.3 on voit que

$$N\left[(QE)(qE) \right] - N(Qq) = N(qQ) - \left[(qQ)E + E(Qq) \right] \lambda + \lambda^2$$

Mais $(qQ)E$ est un élément pur. Donc le coefficient de λ est zéro. Comme $N(Qq) = N(qQ)$, il s'ensuit que $\lambda = 0$.

Donc, si q est pur $(QE)(qE) = qQ$ et si Q et R sont des quaternions quelconques avec $R = R_1 + R_2$, $R_1 \in X$, $R_2 \in Y$, alors $(QE)(RE) = (QE)\left[R_1 E + R_2 E \right] = R_1(QE)E + (QE)(R_2 E) = -R_1 Q + R_2 Q = -\bar{R}Q$.

Or, si q est un quaternion pur, alors $(QE)N(q) = (qQ)(\overline{qE}) = -(qQ)(qE)$.

Posons $\alpha = qQ$, $\beta = q$. Alors $\alpha(\beta E) = \beta^2\left[(\beta^{-1}\alpha)E \right]$. Comme $\beta^2 \in X$, on voit que

$$\alpha(\beta E) = \left[\beta^2(\beta^{-1}\alpha) \right] E = \left[\left\{ \beta(\beta\beta^{-1}) \right\} \alpha \right] E = (\beta\alpha)E.$$

Il s'ensuit que si r et R sont des quaternions quelconques alors

$$r(RE) = (Rr)E.$$

De façon semblable, on prouve que

$$r(ER) = (\bar{R}r)E.$$

La combinaison de tous ces calculs démontre que si q + QE et r + RE sont deux éléments de Ω alors

$$(5.2) \qquad (q + QE)(r + RE) = (qr - \bar{R}Q) + (Rq + Q\bar{r})E.$$

On peut démontrer directement que ce produit satisfait l'axiome (*). Cette vérification doit être faite parce que la condition utilisée pour la dérivation de (5.2) est nécessaire mais non suffisante pour (*).

Notons que si $z = q + QE$, alors $N(z) = q\bar{q} + Q\bar{Q} \geq 0$ et est égale à zéro si et seulement si $z = 0$.

La table de multiplication pour les éléments 1, i, j, k, E, I, J, K est la suivante:

	1	i	j	k	E	I	J	K
1	1	i	j	k	E	I	J	K
i	i	-1	k	-j	I	-E	-K	J
j	j	-k	-1	i	J	K	-E	-I
k	k	-j	-i	-1	K	-J	I	-E
E	E	-I	-J	-K	-1	i	j	k
I	I	E	-K	J	-i	-1	-k	j
J	J	K	E	-I	-j	k	-1	-i
K	K	-J	I	E	-k	-j	i	-1

Or, supposons que ces éléments soient dépendants. Alors il existerait huit éléments $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in X$ tels que

$$x_0 + x_1 i + x_2 j + x_3 k + x_4 E + x_5 I + x_6 J + x_7 K = 0.$$

Mais $x_0 = 0$, puisque $R = X \oplus Y$. Alors

$$-x_1 + x_2 k - x_3 j + x_4 I - x_5 E - x_6 K + x_7 J = 0,$$

ce qui entraînerait $x_1 = 0$ etc. On aurait alors une contradiction. Il s'ensuit que Ω est le plus petit Q*-anneau qui ne soit pas associatif. Cette algèbre, c'est-à-dire celle de Ω , est due à Cayley et Dickson.

Théorème 5.1 Un Q*-anneau est strictement non-commutatif et non-associatif si et seulement s'il est isomorphe à l'algèbre des octonions définie par la multiplication (5.2).

Pour compléter la preuve de ce théorème, il faut démontrer que, sous ces conditions, $R = \Omega$. On le prouve par l'absurde.

Soit P un élément de R tel que $P \notin \Omega$. On peut supposer que $P \in Y$ et $P^2 = -1$. Posons

$$\Omega^* = \{ z \mid z = A + BP \ , \ A, B \in \Omega \}.$$

Si on utilise les arguments de cette section, on est amené à une structure à 16 dimensions pour laquelle la multiplication est définie par

$$(A + BP)(C + DP) = (AC - \bar{D}B) + (DA + B\bar{C})P.$$

Cependant, on trouve que cette multiplication n'est pas du type requis par (*). Ceci est clairement démontré si on considère le produit:

$$(E + JP)(-I + KP) = (-EI + KJ) + (KE + JI)P = 0$$

Ceci s'explique par le fait que la condition (5.1) utilisée pour déduire la multiplication (5.2) est une condition nécessaire mais non suffisante pour que l'axiome (*) soit satisfait.

REFERENCES

1. Dickson, L.E. "Algebras and their arithmetics". Dover Publications Inc., New-York, N.Y., 1960.

2. De Cicco, J. "Some theorems concerning commutative rings which admit involutional automorphisms". Atti della Accademia delle Scienze di Torino. Vol. 92, pp. 1-18, 1957.