Quelques avatars

du groupe alterné sur 5 lettres

Le groupe alterné $\mathcal{A}_5$ est bien connu ainsi que sa représentation usuelle comme le sous-groupe des rotations de $O^+(3,\mathbf{R})$ qui laissent stable un icosaèdre ou un dodécaèdre. Mon objectif ici est d'en donner une description comme sous-groupe de $PSU(2,\mathbf{C})$, sans passer par l'isomorphisme de $O^+(3)$ et de $PSU(2)$. Le ressort de la preuve est une description par générateurs et relations qui remonte à Hamilton.

0.1 Le théorème de Hamilton

0.1.1 Énoncé et schéma de preuve

On suppose que le lecteur sait ce qu'est le groupe libre $F_{a,b}$ à deux générateurs. Le résultat de Hamilton *(Letter to John T. Graves on the Icosian, 17 octobre 1856, Œuvres, Tome III, page 612)* est le suivant (même s'il n'est pas formulé ainsi dans Hamilton) :

0.1.1 Théorème. *Soit N le sous-groupe distingué de $F_{a,b}$ engendré par les éléments a^2, b^3 et $(ab)^5$. Alors, le quotient $G = F_{a,b}/N$ est isomorphe à $\mathcal{A}_5$.*

Démonstration. Notons déjà qu'on obtient un homomorphisme $\Phi : G \to \mathcal{A}_5$ en associant à a la permutation $\alpha = (12)(45)$ et à b la permutation $\beta = (134)$. En effet, α est bien d'ordre 2 et β d'ordre 3 et le produit $\alpha\beta = (13542)$ d'ordre 5. Cet homomorphisme est surjectif car l'image contient des éléments d'ordres $2, 3, 5$, de sorte qu'elle est de cardinal multiple de 30 et il n'y a pas dans $\mathcal{A}_5$ (simplicité oblige) de sous-groupe non trivial aussi gros. Il reste à montrer que Φ est injectif. Pour cela on va montrer que G est fini de cardinal < 120. Comme son cardinal est aussi multiple de 60, G ne pourra être que $\mathcal{A}_5$.

0.1.2 Les calculs

La majoration du cardinal de G n'est pas triviale et demande quelques calculs.

0.1.2 Lemme. *On peut écrire tous les éléments non triviaux de G sous l'une des formes suivantes :*

$$a^{i_1}b^{j_1}\cdots a^{i_k}b^{j_k}\cdots a^{i_n}b^{j_n},$$

$$a^{i_1}b^{j_1}\cdots a^{i_k}b^{j_k}\cdots a^{i_n},$$

$$b^{j_1}\cdots a^{i_k}b^{j_k}\cdots a^{i_n}b^{j_n},$$

$$b^{j_1}\cdots a^{i_k}b^{j_k}\cdots a^{i_n},$$

avec $n \geq 1$, (et même > 1 pour le dernier) $i_k = 1$ et $j_k = 1$ ou 2 pour tout k. La longueur d'une telle écriture est le nombre de termes en a et en b ou b^2 (respectivement ici, $2n$, $2n-1$, $2n-1$, $2n-2$). Une écriture sera dite minimale si sa longueur l'est.

Démonstration. C'est clair avec les seules relations $a^2 = b^3 = 1$.

0.1.3 Notations. On pose $x = ab$, $y = ab^2$, $z = ba = y^{-1}$ et $t = b^2a = x^{-1}$.

0.1.4 Lemme. *On a les formules suivantes :*
1) $x^5 = y^5 = z^5 = t^5 = 1$,
2) $x^3 = t^2$, $y^3 = z^2$, $z^3 = y^2$, $t^3 = x^2$,
3) $x^2y = t^2b$, $y^2x = z^2b^2$, $zt^2 = b^2x^2$, $tz^2 = by^2$,
4) $xyx^2 = t^2zt$, $yxy^2 = z^2tz$ *et ces éléments sont d'ordre 2,*
5) $(xy)^5 = (yx)^5 = (zt)^5 = (tz)^5 = 1$.

Démonstration. 1) On a $x^5 = 1$ par hypothèse, d'où $t^5 = 1$. Comme on a $y = ata = ata^{-1}$ on en déduit $y^5 = 1$, puis $z^5 = 1$.

2) On a $x^5 = 1$, donc $x^3 = x^{-2} = t^2$ et de même pour les autres.

3) Comme on a $y = xb$, on a $x^2y = x^3b = t^2b$ par 1). De même pour les autres.

4) Comme on a $t^2zt = (xyx^2)^{-1}$ il suffit de montrer que xyx^2 est d'ordre 2. Pour cela on part de la relation $bt = xb^2 = a$ et on tient compte de $t = x^{-1} = x^4$. Cela donne $bx^4 = xb^2$, puis $bx^4b = x$. Avec $xb = y$ on a $bx^3y = x$ et en multipliant à gauche par x, $yx^3y = x^2$, relation équivalente à $xyx^2xyx^2 = x^5 = 1$. De même pour l'autre.

5) On note que $ababa$ est d'ordre 5 comme conjugué de ab^2 : $ababa = (ab)(ab^2)(b^2a)$, puis que $babab$ est d'ordre 5 comme inverse du précédent. Mais on a $xy = b^2(babab)b$, d'où le résultat.

0.1.5 Lemme. *Les éléments de G ont une écriture minimale de l'une des formes suivantes :*
1) $A(x,y) = 1, x, y,\ x^2, y^2, xy,\ xy^2, yx^2, xyx, yxy,\ xyx^2, yxy^2,\ xyxy, yxyx,$

$xyxy^2, yxyx^2, xyxyx$, $yxyxy$, $xyxyx^2$ *et* $yxyxy^2$,
2) $A(x,y)a$,
3) $B(t,z) = 1, z, t, z^2, t^2, zt, z^2t, t^2z, ztz, tzt, z^2tz, t^2zt, ztzt, tztz, z^2tzt, t^2ztz$, $tztzt, ztztz$, z^2tzt *et* t^2ztz,
4) $B(t,z)b$ *ou* $B(t,z)b^2$.

Démonstration. Soit $g \in G$ écrit avec une écriture minimale. Le lemme 0.1.2 montre que les éléments qui commencent par a (resp. b ou b^2) s'écrivent comme produits de x et y en alternance avec éventuellement avec un a à droite (resp. produits de z et t avec éventuellement b ou b^2 à droite). Traitons le cas des formes en x, y, l'autre est analogue. Il suffit d'établir le résultat pour les formes qui n'ont pas de a à droite. Le lemme 0.1.4.2 montre qu'il n'y a pas de termes x^3 ni y^3 (sinon l'écriture ne serait pas minimale puisqu'on peut remplacer x^3 par t^2 qui est plus court). Le point 3 du même lemme, montre que les éventuels termes en x^2 ou y^2 sont nécessairement à droite de l'écriture. Sinon, s'il y a par exemple un terme en $x^2y = ababab^2$ (longueur 6), on le remplace par $t^2b = b^2ab^2ab$ (longueur 5).

Par ailleurs, comme on a $(xy)^5 = 1$, tout produit de six termes xy ou plus se ramène à un produit de moins de 5 : par exemple $xyxyxy = (xyxy)^{-1} = ztzt$. Il reste donc à énumérer les produits d'au plus 5 termes ce qui est fait dans le lemme.

0.1.6 Corollaire. *On a* $|G| \leq 100$.

Démonstration. En effet, il y a 20 formes du type $A(x,y)$ et autant du type $B(t,z)$ et il faut doubler ce nombre pour tenir compte des éléments $A(x,y)a$ et le tripler pour tenir compte des éléments $B(t,z)b$ et $B(t,z)b^2$.

0.1.7 *Remarque.* Bien entendu, il y a des relations entre ces différentes formes. Par exemple, cf. 0.1.4, on a $xyx^2 = t^2zt$.

Cela achève de prouver le théorème de Hamilton.

0.2 Le sous-groupe du groupe unitaire

0.2.1 Théorème. *Soit* ζ *une racine primitive cinquième de l'unité. On considère le sous-groupe* G *de* $GL(2,\mathbf{C})$ *engendré par*

$$-\mathrm{Id}, \quad \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^4 \end{pmatrix}, \quad \frac{1}{\sqrt{5}} \begin{pmatrix} \zeta - \zeta^4 & -\zeta^2 + \zeta^3 \\ -\zeta^2 + \zeta^3 & -\zeta + \zeta^4 \end{pmatrix}.$$

Alors, $H/\{\pm\mathrm{Id}\}$ *est isomorphe à* $\mathcal{A}_5$.

Démonstration. Appelons ρ et τ les deux matrices ci-dessus et notons $\overline{\rho}$ et $\overline{\tau}$ leurs images dans H. On vérifie qu'on a $\rho^5 = \mathrm{Id}$ et $\tau^2 = -\mathrm{Id}$ (donc $\overline{\tau}^2 = 1$ dans H) et

$$\sigma = \rho^2\tau = \frac{1}{\sqrt{5}}\begin{pmatrix} \zeta^{-2} - \zeta & -\zeta^{-1} + 1 \\ -1 + \zeta & -\zeta^{-1} + \zeta^2 \end{pmatrix}.$$

Cette dernière matrice est de déterminant 1 et de trace -1. Elle vérifie donc $\sigma^2 + \sigma + \mathrm{Id} = 0$, donc $\sigma^3 = \mathrm{Id}$.

On pose alors $\alpha = \overline{\tau}$ et $\beta = \overline{\tau\rho}^{-2} = \overline{\sigma}^{-1}$. On a $\alpha^2 = 1$, $\beta^3 = 1$, $(\alpha\beta)^5 = (\overline{\rho}^{-2})^5 = 1$. On considère l'homomorphisme $\Psi : F_{a,b} \to H$ qui à a, b associe α, β. Il est surjectif (car on a $(\alpha\beta)^2 = \overline{\rho}$) et son noyau contient N. Il en résulte que le groupe H est un quotient de $G = F_{a,b}/N \simeq \mathcal{A}_5$. Mais $\mathcal{A}_5$ est simple, et comme H n'est pas réduit à 1, il est isomorphe à $\mathcal{A}_5$.

0.2.2 *Remarque.* Bien entendu, H est contenu dans $PSU(2, \mathbf{C})$.