CLASSIFICATION DES GROUPES D'ORDRE 8

G.BERHUY

Le but de cet article est de donner une classification complète des groupes d'ordre 8. On en connaît déjà quelques uns :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4.$$

L'objet du premier paragraphe est de présenter un autre groupe d'ordre 8, à savoir le groupe des quaternions.

1. Le groupe des quaternions

Commençons par définir le groupe qui nous intéresse.

Définition 1.1. Soient $A=\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}$ et $B=\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}$. Le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par A et B est appelé le *groupe de quaternions d'ordre* 8. Il est noté Q_8.

On continue par un résultat qui caractérise complètement le groupe Q_8.

Théorème 1.2. *Soit G un groupe engendré par deux éléments $a,b\in G$ satisfaisant les conditions suivantes :*

1. *a est d'ordre 4 ;*
2. *$a^2\in Z(G)$;*
3. *$a^2=b^2$ et $ba=a^{-1}b$.*

Alors, G est un groupe d'ordre 8 non abélien, dont le centre est engendré par a^2, et tout élément de G s'écrit de manière unique sous la forme

$$a^kb^\ell,\ k\in[\![0,3]\!],\ell\in[\![0,1]\!].$$

De plus, Q_8 vérifie les conditions ci-dessus, et tout groupe G vérifiant ces conditions est isomorphe à Q_8.

Démonstration. Gardons les notations de l'énoncé. Notons que b est d'ordre 4. En effet, $b^4=(b^2)^2=(a^2)^2=a^4=1_G$ et $b^2=a^2\neq 1_G$, puisque a est d'ordre 4. Ainsi, $a^{-1}=a^3$ et $b^{-1}=b^3$. Un élément de $G=\langle a,b\rangle$ est donc un produit de puissances positives de a et b. En utilisant la relation $ba=a^3b$, on voit que tout élément de $\langle a,b\rangle$ est de la forme a^rb^s, où $r,s\geq 0$. Écrivons $s=2n+\ell$, avec $\ell\in[\![0,1]\!]$. Alors, on a

$$a^rb^s=a^r(b^2)^nb^\ell=a^r(a^2)^nb^\ell=a^{r+2n}b^\ell.$$

Date: 10 novembre 2019.

En écrivant cette fois $r+2n=4m+k$, avec $k\in[\![0,3]\!]$, on obtient

$$a^rb^s=a^{r+2n}b^\ell=a^kb^\ell,$$

puisque a est d'ordre 4.

Supposons maintenant que $a^kb^\ell=a^rb^s$ avec $k,r\in[\![0,3]\!]$, et $\ell,s\in[\![0,1]\!]$. On a donc $b^{s-\ell}=a^{k-r}$. En particulier, $b^{s-\ell}$ commute avec a. Or, b étant d'ordre 4, on a $b^{s-\ell}=1,b,b^2$ ou b^3. Mais, b ne commute pas avec a, car sinon on aurait $ab=ba=a^3b$, puis $a^2=1_G$, ce qui n'est pas le cas puisque a^2 est d'ordre 2. De plus, b^3 ne commute pas non plus avec a, car sinon $b=b^5=b^2b^3=a^2b^3$ commuterait avec a. Par conséquent $b^{s-\ell}=1_G$ ou b^2, et donc $s-\ell\equiv 0$ ou 2 [4]. En particulier, $s-\ell$ est pair, et comme $-1\leq s-\ell\leq 1$, on obtient $s-\ell=0$, soit $s=\ell$. Par conséquent, $a^{k-r}=1_G$, et donc $k-r\equiv 0$ [4]. Puisque $-3\leq k-r\leq 3$, on en déduit $k=r$.

Finalement, on obtient bien que G est d'ordre 8, et que tout élément de G s'écrit de manière unique sous la forme

$$a^kb^\ell,\ k\in[\![0,3]\!],\ell\in[\![0,1]\!].$$

De plus, un élément de la forme $a^kb, k\in[\![0,3]\!]$, ne commute pas avec a, car sinon $b=a^{-k}(a^kb)$ commuterait avec a. Un tel élément n'est donc pas dans le centre de G. Enfin, a ne commute pas avec b, et a^3 non plus, car sinon $a=a^5=b^2a^3$ commuterait avec b. Ainsi, a et a^3 ne sont pas dans le centre de G. Finalement, puisque 1_G et a^2 sont dans le centre de G, on obtient

$$Z(G)=\{1_G,a^2\}=\langle a^2\rangle.$$

Établissons maintenant la table de multiplication de G. Pour tous $k,r\in[\![0,3]\!]$, et tous $\ell,s\in[\![0,1]\!]$, on a

$$\begin{array}{rcl}(a^kb^\ell)(a^rb^s) & = & a^kb^\ell a^rb^{-\ell})b^{\ell+s}\\ & = & a^k(b^\ell ab^{-\ell})^rb^{\ell+s}\\ & = & a^k(a^{(-1)^\ell})^rb^{\ell+s}\\ & = & a^{k+(-1)^\ell r}b^{\ell+s}\end{array}.$$

Soient $q_{\ell,s}$ et $n_{\ell,s}$ le quotient et le reste de la division euclidienne de $\ell+s$ par 2. On a alors

$$(a^kb^\ell)(a^rb^s)=a^{k+(-1)^\ell r+2q_{\ell,s}}b^{n_{\ell,s}}=a^{m_{k,\ell,r,s}}b^{n_{\ell,s}},$$

où $m_{k,\ell,r,s}$ est le reste de la division euclidienne de $k+(-1)^\ell r+2q_{\ell,s}$ par 4. Par définition, $m_{k,\ell,r,s}\in[\![0,3]\!]$, et $n_{\ell,s}\in[\![0,1]\!]$, et ne dépendent que de k,ℓ,r et s, et pas du groupe G.

Par conséquent, deux groupes vérifiant les conditions du théorème ont « même table de loi de groupes », et sont donc isomorphes. Pour préciser un peu, si G' est un groupe possédant deux éléments $a',b'\in G'$ vérifiant (1), (2) et (3), l'application

$$\begin{array}{rccc}\varphi\colon & G & \longrightarrow & G'\\ & a^kb^\ell & \longmapsto & a'^kb'^\ell\end{array}$$

est un isomorphisme de groupes (où $k\in[\![0,3]\!]$, et $\ell\in[\![0,1]\!]$). En effet, φ est bien un morphisme de groupes, car pour tous $k,r\in[\![0,3]\!]$, et tous

$\ell, s \in [\![0,1]\!]$, on a

$$\begin{array}{rcl} \varphi((a^k b^\ell)(a^r b^s)) & = & \varphi(a^{m_{k,\ell,r,s}} b^{n_{\ell,s}}) \\ & = & a'^{m_{k,\ell,r,s}} b'^{n_{\ell,s}} \\ & = & (a'^k b'^\ell)(a'^r b'^s) \\ & = & \varphi(a^k b^\ell)\varphi(a^r b^s) \end{array} .$$

De plus, φ est surjective, d'après la description des éléments de G', donc bijective car G et G' ont même nombre d'éléments.

Pour obtenir la dernière partie, il suffit donc de constater que Q_8 vérifie les conditions de l'énoncé. Un simple calcul montre que $A^2 = -I_2$, qui est clairement dans le centre de Q_8. En particulier, $A^{-1} = -A$. De plus, $A^4 = (-I_2)^2 = I_2$. Comme $A^2 \neq I_2$, A est bien d'ordre 4. On vérifie également que $B^2 = -I_2$, et que $BA = -AB = A^{-1}B$. Ceci achève la démonstration. □

Remarque 1.3. Comme $A^2 = -I_2$, le théorème précédent montre que Q_8 est d'ordre 8 non abélien, que $Z(Q_8) = \{\pm I_2\}$, et que ses éléments sont

$$\pm I_2,\ \pm A,\ \pm B,\ \pm AB.$$

On remarque que $\pm A, \pm B$ et $\pm AB$ sont tous d'ordre 4, tandis que $-I_2$ est d'ordre 2.

Nous allons maintenant décrire les sous-groupes de Q_8.

Proposition 1.4. *Les sous-groupes de Q_8 sont*

$$\{I_2\},\ \langle -I_2\rangle,\ \langle A\rangle,\ \langle B\rangle,\ \langle AB\rangle,\ Q_8,$$

qui sont respectivement d'ordre $1, 2, 4, 4, 4,$ *et* 8.

En particulier, tous les sous-groupes stricts de Q_8 sont abéliens.

De plus, tous les sous-groupes de Q_8 sont distingués dans Q_8, bien que Q_8 ne soit pas abélien.

Démonstration. Notons que si $M = A, B$ ou AB, alors $\langle M\rangle = \langle -M\rangle$. En effet, $-M = (-I_2)M = M^3$, et comme M est d'ordre 4, qui est premier à 3, M^3 et M engendrent le même sous-groupe cyclique (on peut aussi procéder par calcul direct). Les sous-groupes de Q_8 engendrés par 0 ou 1 élément sont donc exactement

$$I_2,\ \langle -I_2\rangle,\ \langle A\rangle,\ \langle B\rangle,\ \langle AB\rangle.$$

Considérons maintenant un sous-groupe engendré par deux éléments M_1 et M_2 distincts, et différents de I_2. Vu les égalités $A^2 = B^2 = (AB)^2 = -I_2$, on a $\langle -I_2\rangle \subset \langle M\rangle$ si $M = \pm A, \pm B, \pm AB$ et vu l'égalité $\langle M\rangle = \langle -M\rangle$, il suffit de considérer les cas $(M_1, M_2) = (A, B), (A, AB)$ ou (B, AB). Dans les trois cas, le sous-groupe obtenu est $\langle A, B\rangle = Q_8$, puisque

$$\langle A, AB\rangle = \langle A, A^{-1}(AB)\rangle = \langle A, B\rangle,$$

et

$$\langle B, AB\rangle = \langle B, (AB)B^{-1}\rangle = \langle A, B\rangle.$$

Clairement, $\{I_2\}$ et Q_8 sont distingués dans Q_8. De plus, $Z(Q_8) = \langle -I_2\rangle$ est distingué dans Q_8. Notons maintenant que les trois sous-groupes restants

sont d'ordre 4, donc d'indice 2, donc distingués. On peut aussi procéder de manière calculatoire. Par exemple, on a

$$AAA^{-1} = A \in \langle A \rangle \text{ et } BAB^{-1} = -A = A^3 \in \langle A \rangle,$$

ce qui suffit à montrer que $\langle A \rangle$ est distingué dans Q_8, puisque A et B engendrent Q_8. □

Ce résultat permet de démontrer que Q_8 n'est pas isomorphe à un produit semi-direct.

Proposition 1.5. *Le groupe Q_8 n'est pas isomorphe à un produit semi-direct de deux groupes d'ordre < 8.*

Démonstration. Supposons que l'on ait un isomorphisme $\varphi : H \times_\rho K \xrightarrow{\sim} Q_8$, où H et K sont d'ordre < 8.

Soient $H' = \varphi(H \times \{1_K\})$ et $K' = \varphi(\{1_H\} \times K)$. On sait que $H \times \{1_K\}$ est distingué dans $H \times_\rho K$. Comme φ est un isomorphisme , H' est distingué dans Q_8. De plus, pour tout $h \in H$ et tout $k \in K$, on a

$$(h, 1_K)(1_H, k) = (h\rho_k(1_H), k) = (h1_K, k) = (h, k),$$

et par conséquent $\varphi((h,k)) = \varphi((h,1_K))\varphi((1_H,k))$. Comme φ est bijective, il s'ensuit que tout élément de Q_8 s'écrit comme le produit d'un élément de H' et d'un élément de K' Ainsi, $Q_8 = H'K' = \langle H', K' \rangle$, puisque H' est distingué dans Q_8. Enfin, $H \times \{1_K\}$ et $\{1_H\} \times K$ s'intersectent trivialement, et comme φ est bijective, on en déduit aisément que H' et K' s'intersectent trivialement. Bref, $Q_8 = H' \rtimes K'$.

Puisque H et K sont d'ordre < 8, il en est de même de H' et K'. Ainsi, H' et K' sont des sous-groupes stricts de Q_8. D'après la proposition précédente, H' et K' sont abéliens, et distingués dans Q_8. On a donc $Q_8 = H' \odot K' \simeq H' \times K'$. Mais comme H' et K' sont abéliens, on obtient que Q_8 est abélien, d'où une contradiction. □

2. Classification des groupes d'ordre 8

Nous allons pouvoir donner une liste des groupes d'ordre 8 à isomorphisme près.

Théorème 2.1. *Il y a cinq groupes d'ordre 8 à isomorphisme près (trois abéliens, et deux non abéliens) :*

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4 \ \text{ et } \ Q_8.$$

De plus, Q_8 est l'unique groupe non abélien d'ordre 8 dont tous les sous-groupes sont distingués. C'est aussi l'unique groupe non abélien d'ordre 8 possédant un unique élément d'ordre 2.

Démonstration. Soit G un groupe d'ordre 8, et soit m le maximum des ordres des éléments de G. D'après le théorème de Lagrange, on a $m = 1, 2, 4$ ou 8. Le cas $m = 1$ est impossible, puisque sinon G serait trivial. Nous allons maintenant traiter les cas restants séparément.

Si $m = 8$, G possède un élément d'ordre 8, et est donc cyclique. On a donc $G \simeq \mathbb{Z}/8\mathbb{Z}$.

Si $m = 2$, tous les éléments sont d'ordre 1 ou 2, et donc $x^2 = 1_G$ pour tout $x \in G$. Mais alors, G est abélien. En effet, pour tous $x, y \in G$, on a

$$yx = y^{-1}x^{-1} = (xy)^{-1} = xy.$$

Passons en notation additive pour plus de clarté. On a donc $2{\cdot}x = 0$ pour tout $x \in G$. On vérifie facilement que la loi externe

$$\begin{aligned} \mathbb{F}_2 \times G &\longrightarrow G \\ (\overline{m}, x) &\longmapsto \overline{m} * x = m{\cdot}x \end{aligned}$$

est bien définie, et muni le groupe abélien $(G, +)$ d'une structure de $\mathbb{F}_2$-espace vectoriel, nécessairement de dimension finie, puisque G est fini. Mais alors, si $n = \dim_{\mathbb{F}_2}(G)$, on a un isomorphisme d'espaces vectoriels $G \simeq \mathbb{F}_2^n$, qui est en particulier un isomorphisme de groupes abéliens. Comme G est d'ordre 8, on obtient $n = 3$, soit $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

Il reste le cas $m = 4$, qui est le plus délicat. Soit $a \in G$ un élément d'ordre 4. Le sous-groupe $H = \langle a \rangle$ est d'ordre 4, donc d'indice 2. Il est donc distingué dans G. De plus, pour tout $b \in G \setminus H$, on a $G/H = \{\overline{1}_G, \overline{b}\}$, puisque G/H est d'ordre 2 et que $\overline{b} \neq \overline{1}_G$.

Si $x \in G$, on a donc $\overline{x} = \overline{b}^{\ell} = \overline{b^\ell}$, avec $\ell \in [\![0, 1]\!]$, et par conséquent, il existe $y \in H$ tel que $x = b^\ell h$. Il existe donc $k \in \mathbb{Z}$ tel que $h = a^k$, et ainsi $x = b^\ell a^k$. Par conséquent, $G = \langle a, b \rangle$.

Supposons tout d'abord qu'il existe $b \in G \setminus H$ d'ordre 2. Posons $K = \langle b \rangle$. On a donc

$$G = \langle a, b \rangle = \langle H, K \rangle,$$

et de plus $|G| = 8 = 4{\cdot}2 = |H||K|$. Enfin, $H \cap K = \{1_G\}$. En effet, dans le cas contraire, on aurait $b \in H$. Bref, puisque H est distingué dans G, on a $G = H \rtimes K$.

Ainsi, tout élément de G s'écrit de manière unique sous la forme

$$a^k b^\ell, \ k \in [\![0, 3]\!], \ell \in [\![0, 1]\!].$$

Puisque H est distingué dans G, on a $bab^{-1} \in H$. Comme a est d'ordre 4, bab^{-1} est d'ordre 4, et donc $bab^{-1} = a$ ou a^{-1}. Dans le premier cas, a et b commutent, et les éléments de H et K commutent donc. On a alors

$$G = H \odot K \simeq H \times K \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Supposons maintenant que $bab^{-1} = a^{-1}$. Dans ce cas, G est isomorphe à D_4. En effet, pour tout $k \in [\![0, 3]\!]$, et tout $\ell \in [\![0, 1]\!]$, on a

$$\begin{aligned} (a^k b^\ell)(a^r b^s) &= a^k (b^\ell a b^{-\ell})^r b^{\ell+s} \\ &= a^k (a^{(-1)^\ell})^r b^{\ell+s} \\ &= a^{u_{k,\ell,r,s}} b^{v_{\ell,s}}, \end{aligned}$$

où $u_{k,\ell,r,s}$ est le reste de la division euclidienne de $k + (-1)^\ell r$ par 4, et $v_{\ell,s}$ est le reste de la division euclidienne de $\ell + s$ par 2.

Or, D_4 possède la même table de loi de groupe : si σ est la rotation d'angle $\frac{\pi}{4}$ et τ est la symétrie orthogonale d'axe (Ox), σest d'ordre 4, τ est d'ordre 2, $\tau\sigma\tau^{-1} = \sigma^{-1}$, et tout élément de D_4 s'écrit de manière unique sous la forme

$$\sigma^k\tau^\ell,\ k \in [\![0,3]\!], \ell \in [\![0,1]\!].$$

Les mêmes calculs que précédemment montrent alors que pour tout $k \in [\![0,3]\!]$, et tout $\ell \in [\![0,1]\!]$, on a

$$(\sigma^k\tau^\ell)(\sigma^r\tau^s) = \sigma^{u_{k,\ell,r,s}}\tau^{v_{\ell,s}}.$$

On conclut alors comme dans la démonstration du théorème 1.2.

Il reste à traiter le cas où $G \setminus H$ ne contient pas d'élément d'ordre 2. Un élément $b \in G \setminus H$ est alors d'ordre 4 (puisque G ne contient pas d'élément d'ordre 8, vu que $m = 4$). Comme G/H est d'ordre 2, on a $\overline{b}^2 = \overline{1}_G$, et donc $b^2 \in H = \langle a\rangle$. Comme $\langle a\rangle$ est cyclique, il contient un unique élément d'ordre 2, à savoir a^2. On a ainsi $a^2 = b^2$. Comme précédemment, bab^{-1} est un élément de H d'ordre 4, donc égal à 1_G ou a^{-1}.

Si $bab^{-1} = a$, a et b commutent. Mais alors, $ab \in G \setminus H$ (car $a \in H$ et $b \in G \setminus H$), mais $(ab)^2 = a^2b^2 = a^4 = 1_G$. Par conséquent, $G \setminus H$ contient un élément d'ordre 2, ce qui contredit l'hypothèse. Par conséquent, $bab^{-1} = a^{-1}$, soit $ba = a^{-1}b$. Observons maintenant que $a^2 \in Z(G)$, puisque a^2 commute à a et b (car $a^2 = b^2$), et a et b engendrent G. Par le théorème 1.2, G est isomorphe à Q_8.

On a donc obtenu les cinq groupes de l'énoncé. Il reste à constater que tous ces groupes sont deux à deux non isomorphes. Les groupes D_4 et Q_8 sont non abéliens, donc non isomorphes aux trois premiers. Ils sont de plus non isomorphes, car D_4 contient un sous-groupe non distingué, à savoir le sous-groupe engendré par la symétrie d'axe (Ox), tandis que tous les sous-groupes de Q_8 sont distingués (cf. proposition 1.4). On peut aussi constater que Q_8 possède un seul élément d'ordre 2, tandis que D_4 en contient quatre (les quatre symétries).

Enfin, les trois groupes abéliens sont deux à deux non isomorphes, puisque l'analyse précédente montre que l'ordre maximal m d'un élément d'un de ces groupes est $8, 4$ et 2 respectivement. Ceci achève la démonstration. □