GROUPES DIÉDRAUX

G.BERHUY

Le but de cet article est de présenter les groupes diédraux. On considère que le lecteur connaît la description des isométries vectorielles du plan.

1. Définition

Définition 1.1. Soit $n \geq 1$. On appelle groupe *groupe diédral d'ordre* $2n$ l'ensemble D_n des isométries (affines) du plan affine qui conserve globalement les sommets d'un n-gone régulier (dans le cas $n = 1$, le n-gone est réduit à un point et si $n = 2$, le n-gone est juste un segment).

C'est clairement un sous-groupe du sous-groupe des bijections affines de $\mathbb{R}^2$.

Remarquons qu'un élément de D_n fixe le centre O du n-gone régulier si $n \geq 2$. En effet, si $n = 2$, on utilise le fait qu'une isométrie préserve les milieux, et si $n \geq 3$, on utilise le fait qu'une isométrie conserve les distances et que le centre du n-gone est le seul point du plan qui soit équidistant à tous les sommets. Ainsi, un élément de D_n se confond avec sa partie vectorielle. De plus, en prenant un repère du plan centré en O et dont l'unité de mesure est la distance de O à un sommet, on peut toujours supposer que les sommets du n-gone sont disposés sur le cercle unité. Notons

$$A_k = (\cos\Big(\frac{2k\pi}{n}\Big), \sin\Big(\frac{2k\pi}{n}\Big)) \in \mathbb{R}^2 \text{ pour tout } k \in \mathbb{Z},$$

ainsi que

$$v_k = \overrightarrow{OA_k} \text{ pour tout } k \in \mathbb{Z}.$$

Si l'on munit $\mathbb{R}^2$ de son produit scalaire canonique, l'analyse précédente montre que si $n \geq 2$, le groupe D_n est le sous-groupe des isométries vectorielles de $\mathbb{R}^2$ qui préservent globalement l'ensemble $\mathscr{S} = \{v_k \mid k \in \mathbb{Z}\}$, c'est-à-dire

$$D_n = \{u \in \mathrm{O}(\mathbb{R}^2) \mid u(\mathscr{S}) = \mathscr{S}\}.$$

C'est aussi trivialement vrai pour $n = 1$. Ainsi, D_n peut se voir comme un sous-groupe de $\mathrm{O}(\mathbb{R}^2)$.

Notons au passage que $v_k = v_\ell$ dès que $k \equiv \ell\ [n]$, et donc que l'on a

$$\mathscr{S} = \{v_0, \ldots, v_{n-1}\}.$$

Commençons par lister quelques éléments du groupe diédral.

Date: 10 novembre 2019.

Lemme 1.2. *Soit $n \geq 1$. Soit r la rotation vectorielle d'angle $\dfrac{2\pi}{n}$, et soit s la symétrie orthogonale d'axe (Ox). Alors, on a $r^k s^\ell \in D_n$ pour tout $k \in [\![0, n-1]\!]$ et tout $\ell \in [\![0, 1]\!]$.*

De plus :

(1) *pour tout $k \in [\![0, n-1]\!]$, r^k est la rotation vectorielle d'angle $\dfrac{2k\pi}{n}$;*

(2) *pour tout $k \in [\![0, n-1]\!]$, $r^k s$ est la symétrie orthogonale dont l'axe passe par O et le milieu du segment $A_{k-1}A_k$ (qui est donc le segment $A_{n-1}A_0$ si $k = 0$).*

En particulier, tous ces éléments sont distincts.

Démonstration. Il est clair que $r \in D_n$. Si l'on veut l'écrire explicitement, il suffit de voir que r est une isométrie de $\mathbb{R}^2$ et que

$$r(v_k) = v_{k+1} \quad \text{pour tout } k \in \mathbb{Z}.$$

Comme l'application

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z} \\ k &\longmapsto k+1 \end{aligned}$$

est bijective, on a le résultat (on peut aussi simplement considérer les indices $k \in [\![0, n-1]\!]$ et se rappeler que $v_n = v_0$). Cela fonctionne même si $n = 1$, puisque dans ce cas, $v_k = v_0$ pour tout $k \in \mathbb{Z}$.

De plus, $s \in D_n$ puisque cette une isométrie de $\mathbb{R}^2$ et que

$$s(v_k) = v_{-k} \quad \text{pour tout } k \in \mathbb{Z}.$$

Comme D_n est un groupe, on a bien $r^k s^\ell \in D_n$ pour tout $k \in [\![0, n-1]\!]$ et tout $\ell [\![0, 1]\!]$.

Les propriétés élémentaires des rotations entraînent clairement le point (1). De plus, pour tout $k \in [\![0, n-1]\!]$,on a

$$\det(r^k s) = \det(r)^k \det(s) = -1,$$

et $r^k s$ est une isométrie indirecte, donc une symétrie orthogonale. De plus, on a

$$r^k s(v_0) = r^k(v_0) = v_k \quad \text{et} \quad r^k s(v_1) = r^k(v_1) = v_{k-1}.$$

En particulier, s fixe $\dfrac{v_{k-1} + v_k}{2}$. Comme l'ensemble des points fixes d'une symétrie est son axe, on en déduit que l'axe de $r^k s$ est la droite passant par O et le milieu du segment $A_{k-1}A_k$. Le fait que ces $2n$ éléments soient tous distincts est clair. □

Remarque 1.3. Si n est impair, on peut voir que l'axe de la symétrie $r^k s$ passe par le sommet A_{n-k}, et cet axe est donc la droite (OA_{n-k}).

En revanche, si n est pair, l'axe de la symétrie $r^k s$ passe par deux sommets si k est pair, et passe par les milieux de deux côtés opposés si k est impair (mais ne passe par aucun sommet).

Proposition 1.4. *Soit $n \geq 1$. Alors, D_n possède $2n$ éléments.*

Plus précisément, tout élément de D_n s'écrit de manière unique sous la forme

$$r^k s^\ell,\ k \in [\![0, n-1]\!], \ell \in [\![0, 1]\!],$$

où r la rotation vectorielle d'angle $\dfrac{2\pi}{n}$, et soit s la symétrie orthogonale d'axe (Ox). En particulier, $D_n = \langle r, s\rangle$. De plus, r est d'ordre n, s est d'ordre 2 et $srs^{-1} = r^{-1}$.

Démonstration. Il est clair que r est d'ordre n et que s est d'ordre 2. L'isométrie srs^{-1} étant de déterminant 1, c'est une rotation. Pour déterminer son angle, il suffit de déterminer l'image de v_0. Or, on a

$$srs^{-1}(v_0) = sr(v_0) = r(v_1) = v_{-1}.$$

Ainsi, srs^{-1} est la rotation d'angle $-\dfrac{2\pi}{n}$, c'est-à-dire r^{-1}.

Démontrons le reste de la proposition.

Commençons par le groupe D_1. Si $u \in D_1$ fixe v_0. Si u est une rotation, c'est donc l'identité. Si u est une symétrie, puisque l'axe de u est l'ensemble de ses vecteurs fixes, u est la symétrie d'axe (Ox), c'est-à-dire. On a donc $D_1 = \{\mathrm{Id}, s\}$, ce qui est bien ce que l'on voulait montrer.

Considérons maintenant le cas du groupe D_2. Dans ce cas, $v_1 = -v_0$. Soit $u \in D_2$. Alors, u fixe v_0 et v_1, ou les échange. Supposons tout d'abord que u soit une rotation. Si u fixe v_0 et v_1, nécessairement $u = \mathrm{Id}$. Si u échange v_0 et v_1, u est la rotation d'angle π (puisque l'angle formé par v_0 et v_1 est plat), c'est-à-dire $u = r$. Si u est une symétrie, et si u fixe v_0 et v_1, alors u fixe (Ox), et on a donc $u = s$. Si u échange v_0 et v_1, puisque $s(v_0) - v_0 = 2v_1$ est orthogonal à l'axe de u, on en déduit que u est la symétrie orthogonale d'axe (Oy). Mais il est facile de voir cette symétrie n'est rien d'autre que rs.

On a donc démontré que $D_2 = \{\mathrm{Id}, r, s, rs\}$ dans ce cas. Notons que ces quatre éléments sont bien distincts.

On suppose jusqu'à la fin que $n \geq 3$. Les vecteurs v_0 et v_1 n'étant pas colinéaires puisque $n \geq 3$, (v_0, v_1) est une base de $\mathbb{R}^2$. Un élément $u \in D_n$ est donc déterminé de manière unique par les images de v_0 et v_1. Puisque u préserve les angles non orientés, il préserve l'angle formé par les deux vecteurs v_0 et v_1. Il existe donc $k \in \mathbb{Z}$ tel que $\{u(v_0), u(v_1)\} = \{v_k, v_{k+1}\}$. Dit autrement, en tant qu'isométrie du plan affine, u envoie une paire de sommets consécutifs sur une paire de sommets consécutifs.

Notons maintenant qu'il y a au plus n choix pour k (puisqu'en fait $\mathscr{S} = \{v_0, \ldots, v_{n-1}\}$), et au plus deux choix possibles pour le couple $(u(v_0), u(v_1))$, à savoir (v_k, v_{k+1}) et (v_{k+1}, v_k). Il y a donc au plus $2n$ choix possibles, donc au plus $2n$ éléments (c'est bien « au plus », puisqu'il n'est a priori pas garanti que tous les choix soient possibles). Le lemme précédent montre alors que D_n possède au moins $2n$ éléments, qui sont exactement ceux de l'énoncé. On a donc bien $|D_n| = 2n$, ainsi que la description annoncée de ses éléments, l'unicité de l'écriture venant du fait que tous ces éléments sont distincts. De

plus, puisque $r, s \in D_n$, on a

$$\langle r, s\rangle \subset D_n = \{r^k s^\ell \mid k \in [\![0, n-1]\!], \ell \in [\![0, 1]\!]\} \subset \langle r, s\rangle,$$

d'où l'égalité $D_n = \langle r, s\rangle$. Ceci achève la démonstration. □

Remarque 1.5. Le groupe D_n est non abélien si $n \geq 3$. En effet, on a

$$srs^{-1}r^{-1} = r^{-2} \neq \mathrm{Id},$$

puisque r est d'ordre $n \geq 3$. Ainsi, r et s ne commutent pas.

En revanche, D_1 est abélien d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. De plus, D_2 est abélien d'ordre 4. Comme tous les éléments de D_2 sont d'ordre 1 ou 2, on a $D_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

2. Quelques caractérisations des groupes diédraux

On va donner ici quelques caractérisations du groupe diédral.

Théorème 2.1. *Soit $n \geq 1$ un entier. Soit G un groupe engendré par deux éléments $\sigma, \tau \in G$ vérifiant les conditions suivantes :*

(1) $o(\sigma) = n,\ o(\tau) = 2$ *et* $\tau\sigma\tau^{-1} = \sigma^{-1}$
(2) $\tau \notin \langle\sigma\rangle$ *si* $n = 2$.

Alors, G est d'ordre $2n$, et tout élément de G s'écrit de manière unique sous la forme

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

De plus, D_n vérifie les conditions précédentes, et tout groupe vérifiant ces conditions est isomorphe à D_n.

Démonstration. Soit G un groupe engendré par deux éléments σ et τ vérifiant (1) et (2). En utilisant la relation $\tau\sigma = \sigma^{-1}\tau$, on voit aisément qu'un élément de $G = \langle\sigma, \tau\rangle$ est de la forme $\sigma^k\tau^\ell$, avec $k, \ell \in \mathbb{Z}$. Comme σ est d'ordre n et τ est d'ordre 2, on voit que l'on peut se restreindre à $k \in [\![0, n-1]\!]$ et $\ell \in [\![0, 1]\!]$. Ainsi, on a

$$G = \langle\sigma, \tau\rangle = \{\sigma^k\tau^\ell \mid k \in [\![0, n-1]\!], \ell \in [\![0, 1]\!]\}.$$

Montrons que tous ces éléments sont distincts. Soient $k, r \in [\![0, n-1]\!]$ et $\ell, s \in [\![0, 1]\!]$ tels que

$$\sigma^k\tau^\ell = \sigma^r\tau^s.$$

On a donc $\sigma^{k-r} = \tau^{s-\ell}$. Supposons que $s - \ell$ soit impair. Alors, τ étant d'ordre 2, on obtient $\tau = \sigma^{k-r} \in \langle\sigma\rangle$. En particulier, τ et σ commutent. On a alors

$$\sigma^{-1} = \tau\sigma\tau^{-1} = \sigma,$$

d'où $\sigma^2 = 1_G$. Comme σ est d'ordre n, cela force à avoir $n = 1$ ou $n = 2$. Le cas $n = 2$ est exclu par hypothèse, et le cas $n = 1$ ne peut se produire, car sinon on aurait $\sigma = 1_G$, et donc $\tau = 1_G$, qui n'est pas d'ordre 2. Bref, $s - \ell$ est pair. Comme $-1 \leq s - \ell \leq 1$, on a alors $s - \ell = 0$, soit $s = \ell$. Mais alors, $\sigma^{k-r} = 1_G$. Comme σ est d'ordre n, on obtient $k - r \equiv 0\ [n]$. Puisque $-(n-1) \leq k - r \leq n - 1$, on en déduit que $k - r = 0$, soit $k = r$.

Ainsi, on obtient bien que G est d'ordre $2n$, et que tout élément de G s'écrit de manière unique sous la forme

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

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

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

où $u_{k,\ell,r,s}$ est le reste de la division euclidienne de $k + (-1)^\ell r$ par n, et $v_{\ell,s}$ est le reste de la division euclidienne de $\ell + s$ par 2. Par définition, $u_{k,\ell,r,s} \in [\![0, n-1]\!]$, et $v_{\ell,s} \in [\![0, 1]\!]$, 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 $\sigma', \tau' \in G'$ vérifiant (1) et (2), l'application

$$\begin{array}{rccc}\varphi\colon & G & \longrightarrow & G'\\ & \sigma^k\tau^\ell & \longmapsto & \sigma'^k\tau'^\ell\end{array}$$

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

$$\begin{aligned}\varphi((\sigma^k\tau^\ell)(\sigma^r\tau^s)) &= \varphi(\sigma^{u_{k,\ell,r,s}}\tau^{v_{\ell,s}})\\ &= \sigma'^{u_{k,\ell,r,s}}\tau'^{v_{\ell,s}}\\ &= (\sigma'^k\tau'^\ell)(\sigma'^r\tau'^s)\\ &= \varphi(\sigma^k\tau^\ell)\varphi(\sigma^r\tau^s).\end{aligned}$$

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 D_n vérifie les conditions du théorème. Or, on sait déjà que les éléments $r, s \in D_n$ engendrent D_n, et qu'ils vérifient (1). De plus, on a $s \notin \langle r\rangle$, puisque s est une symétrie orthogonale, alors que les éléments de $\langle 1\rangle$ sont des rotations (ceci est même valable pour tout $n \geq 1$). Ceci achève la démonstration. □

Corollaire 2.2. *Soit $n \geq 1$ un entier. Les propriétés suivantes sont équivalentes :*

(1) *G est isomorphe à D_n ;*
(2) *G est d'ordre $2n$, et il existe deux éléments $\sigma, \tau \in G$ vérifiant les conditions suivantes :*
   (a) *$o(\sigma) = n,\ o(\tau) = 2$ et $\tau\sigma\tau^{-1} = \sigma^{-1}$*
   (b) *$\tau \notin \langle\sigma\rangle$ si $n = 2$.*

Démonstration. Supposons tout d'abord que G soit isomorphe à D_n. Comme les propriétés (1) et (2) sont conservées par isomorphisme, il suffit de considérer le cas $G = D_n$. Or, on sait que D_n est d'ordre $2n$ et vérifie les conditions

demandées d'après la proposition précédente. Réciproquement, soit G un groupe d'ordre $2n$ vérifiant les conditions de l'énoncé. Toujours d'après la proposition précédente, on a $\langle\sigma,\tau\rangle \simeq D_n$. En particulier, $\langle\sigma,\tau\rangle$ possède $2n$ éléments. Comme $\langle\sigma,\tau\rangle \subset G$. On obtient alors $G = \langle\sigma,\tau\rangle \simeq D_n$. □

On continue en identifiant D_n à un produit semi-direct.

Lemme 2.3. *Soit $n \geq 1$. Alors, on a $D_n = \langle r\rangle \rtimes \langle s\rangle$. De plus, on a*

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \times_\rho \mathbb{Z}/2\mathbb{Z},$$

où $\rho_{\widetilde{1}} \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est donné par

$$\rho_{\widetilde{1}}(\overline{m}) = -\overline{m} \quad \textit{pour tout } \overline{m} \in \mathbb{Z}/n\mathbb{Z}.$$

Démonstration. Le sous-groupe $\langle r\rangle$ est distingué dans D_n, puisqu'il est d'ordre n, donc d'indice 2. On peut également le démontrer directement en remarquant que

$$rrr^{-1} = r \in \langle r\rangle \quad \text{et} \quad srs^{-1} = r^{-1} \in \langle r\rangle,$$

ce qui suffit à démontrer que $\langle r\rangle$ est distingué dans D_n, puisque r et s engendrent D_n.

D'autre part, on a $|D_n| = 2n = |\langle r\rangle||\langle s\rangle|$, puisque r est d'ordre n et s est d'ordre 2. Enfin, s n'appartient pas à $\langle r\rangle$ puisque ce dernier sous-groupe ne contient que des rotations. Par conséquent, $\langle r\rangle$ et $\langle s\rangle$ s'intersectent trivialement, d'où la première partie du lemme. Pour la seconde, posons $\sigma = (\overline{1},\widetilde{0})$ et $\tau = (\overline{0},\widetilde{1})$. Alors, on voit aisément que $\sigma^k = (\overline{k},\widetilde{0})$ et que $\tau^\ell = (\overline{0},\widetilde{\ell})$ pour tous $k,\ell \geq 0$. On en déduit alors que σ est d'ordre n et τ est d'ordre 2. De plus, on a

$$\tau\sigma = (\overline{1},\widetilde{0})(\overline{0},\widetilde{1}) = (\overline{1},\widetilde{1}),$$

et par conséquent

$$\tau\sigma\tau^{-1}\sigma = (\tau\sigma)^2 = (\overline{1},\widetilde{1})(\overline{1},\widetilde{1}) = (\overline{1-1},\widetilde{1+1}) = (\overline{0},\widetilde{0}),$$

d'où $\tau\sigma\tau^{-1} = \sigma^{-1}$. Enfin, on a clairement $\tau \notin \langle\sigma\rangle$ (comparer les secondes coordonnées). On applique alors le théorème 2.1 pour conclure. □

On finit par une description des groupes engendrés par deux éléments d'ordre 2.

Théorème 2.4. *Soit G un groupe engendré par deux éléments $a,b \in G$ d'ordre 2. Alors, $G \simeq D_n$, où $n = o(ab)$.*

Démonstration. Posons $\sigma = ab$ et $\tau = b$. Enfin, notons $n = o(ab)$. On a donc $o(\sigma) = n$ et $o(\tau) = 2$. De plus,

$$G = \langle a,b\rangle = \langle ab,b\rangle = \langle\sigma,\tau\rangle,$$

ainsi que

$$\tau\sigma\tau^{-1} = b(ab)b^{-1} = ba = b^{-1}a^{-1} = (ab)^{-1} = \sigma^{-1}.$$

Enfin, si $n = 2$, on a $\tau \notin \langle\sigma\rangle$. En effet, dans le cas contraire, on aurait $\tau = 1_G$, ce qui est impossible puisque τ est d'ordre 2, ou $\tau = \sigma$, ce qui n'est pas possible non plus puisque dans ce cas on aurait $a = 1_G$, qui n'est pas d'ordre 2. Le théorème 2.1 montre alors que G est isomorphe à D_n. □

Les résultats précédents permettent de donner plusieurs avatars de D_n. Par exemple, on peut vérifier que les groupes suivants sont isomorphes à D_n :

(1) le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ engendré par les matrices
$$R = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
(2) le sous-groupe des bijections de $\mathbb{C}$ dans lui-même engendré par les fonctions
$$z \longmapsto e^{\frac{2i\pi}{n}} z \quad \text{et} \quad z \longmapsto \overline{z}$$
(3) le sous-groupe de $\mathfrak{S}_n$ engendré par
$$\sigma = (1\ 2 \cdots\ n) \text{ et } \tau = (1\ n-1)(2\ n-2)\cdots(m\ m+1)$$
si $n = 2m+1$, et par
$$\sigma = (1\ 2 \cdots\ n) \text{ et } \tau = (1\ n-1)(2\ n-2)\cdots(m-1\ m)$$
si $n = 2m$.

3. Sous-groupes, sous-groupes distingués

On s'intéresse ici aux sous-groupes de D_n. En guise d'échauffement, on commence par déterminer son centre.

Lemme 3.1. *Soit $n \geq 1$ un entier. Alors, on a*
$$Z(D_n) = \begin{cases} D_n & \text{si } n = 1, 2 \\ \{\mathrm{Id}\} & \text{si } n \geq 3 \text{ et } n \text{ est impair} \\ \{\mathrm{Id}, r^{\frac{n}{2}}\} & \text{si } n \geq 3 \text{ et } n \text{ est pair} \end{cases}$$

Démonstration. Puisque D_1 et D_2 sont abéliens d'après la remarque 1.5, on a $Z(D_1) = D_1$ et $Z(D_2) = D_2$. Supposons maintenant que $n \geq 3$. Pour tout $k \in [\![0, n-1]\!]$, on a
$$r(r^k s)r^{-1} = r^{k+1} s r^{-1} = r^{k+1}(s r^{-1} s^{-1})s.$$
Comme $srs^{-1} = r^{-1}$, on a $sr^{-1}s^{-1} = r$, et ainsi $r(r^k s)r^{-1} = r^{k+2}s$. Par conséquent,
$$r(r^k s)r^{-1}(r^k s)^{-1} = r^{k+2} s s^{-1} r^{-k} = r^2 \neq \mathrm{Id},$$
puisque $n \geq 3$. Ainsi, $r^k s$ et r ne commutent pas. Par conséquent un élément de $Z(D_n)$ est nécessairement de la forme r^k, avec $k \in [\![0, n-1]\!]$.

Soit $k \in [\![0, n-1]\!]$. Si $r^k \in Z(D_n)$, r^k et s commutent, et donc $sr^k s^{-1} r^{-k} = \mathrm{Id}$. Or, on a
$$sr^k s^{-1} r^{-k} = (srs^{-1})^k r^{-k} = r^{-2k}.$$
On obtient donc $r^{-2k} = \mathrm{Id}$, soit encore $r^{2k} = \mathrm{Id}$. Puisque r est d'ordre n et que $2k \in [\![0, 2n-2]\!]$, on en déduit que $2k = 0$ ou n. Puisque k est un entier, le second cas ne peut se produire que si n est pair. On a donc $Z(D_n) \subset \{\mathrm{Id}\}$ si n est impair, et $Z(D_n) \subset \{\mathrm{Id}, r^{\frac{n}{2}}\}$ si n est pair. Les autres inclusions étant évidentes puisque $r^{\frac{n}{2}} = -\mathrm{Id}$, ceci démontre le résultat voulu. □

Nous allons maintenant décrire les sous-groupes de D_n. On a le théorème suivant.

Théorème 3.2. *Soit $n \geq 1$ un entier. Pour tous diviseurs positifs d et d' de n, et pour tout $k \in [\![0, \frac{n}{d'} - 1]\!]$, on pose*

$$H_d = \langle r^{\frac{n}{d}} \rangle \quad et \quad H_{d',k} = \langle r^{\frac{n}{d'}}, r^k s \rangle.$$

Alors, tout sous-groupe de D_n est égal à un sous-groupe H_d pour un unique diviseur positif d de n ou à un sous-groupe $H_{d',k}$, pour un unique diviseur positif d' de n et un unique entier $k \in [\![0, \frac{n}{d'} - 1]\!]$.

De plus, H_d est cyclique d'ordre d, et $H_{d',k}$ est isomorphe à $D_{d'}$.

Démonstration. Soit H un sous-groupe de D_n. On note $r_1, \ldots, r_p, s_1, \ldots, s_q$ les éléments de H, avec $p, q \geq 0$, où $r_1, \ldots, r_p$ sont des rotations et $s_1, \ldots, s_q$ sont des symétries orthogonales. On a en particulier

$$H = \langle r_1, \ldots, \ldots, r_p, s_1, \ldots, s_q \rangle.$$

Notons que $\langle s_1, s_2 \rangle = \langle s_1, s_1 s_2 \rangle$, et que $s_1 s_2$ est une rotation, puisque son déterminant est égal à 1. On en déduit aisément que l'on peut toujours supposer que $q = 0$ ou 1. Enfin, remarquons que, d'après la description des éléments de D_n, chaque rotation r_i est une puissance de r. Ainsi, $\langle r_1, \ldots, r_p \rangle$ est un sous-groupe du groupe cyclique $\langle r \rangle$, qui est d'ordre n. Il est donc de la forme $\langle r^{\frac{n}{d}} \rangle$, où d est un diviseur positif de n.

Vu la description des éléments de D_n, on a finalement $H = \langle r^{\frac{n}{d}} \rangle$ ou $H = \langle r^{\frac{n}{d'}}, r^k s \rangle$, avec $k \in [\![0, n-1]\!]$. Notons que dans le second cas, on peut toujours supposer que $k \in [\![0, \frac{n}{d'} - 1]\!]$. En effet, si $k = a\dfrac{n}{d'} + \ell$, avec $\ell \in [\![0, \frac{n}{d'} - 1]\!]$, on a

$$\langle r^{\frac{n}{d'}}, r^k s \rangle = \langle r^{\frac{n}{d'}}, (r^{\frac{n}{d'}})^a r^\ell s \rangle = \langle r^{\frac{n}{d'}}, (r^{\frac{n}{d'}})^{-a} (r^{\frac{n}{d'}})^a r^\ell s \rangle = \langle r^{\frac{n}{d}}, r^\ell s \rangle.$$

Bref, on a donc $H = H_d$ ou $H = H_{d',k}$.

Le groupe H_d est clairement cyclique d'ordre d. Montrons que $H_{d',k} \simeq D_{d'}$. Pour cela, posons $\sigma = r^{\frac{n}{d'}}$ et $\tau = r^k s$. Alors, σ est d'ordre d' et τ est d'ordre 2. De plus, on a

$$\tau \sigma \tau^{-1} = r^k (s r^{\frac{n}{d'}} s^{-1}) r^{-k} = r^k r^{-\frac{n}{d'}} r^{-k} = r^{-\frac{n}{k'}} = \sigma^{-1}.$$

Enfin, supposons que $d' = 2$. Alors, $\tau \notin \langle \sigma \rangle$ car τ est une symétrie orthogonale et les éléments de $\langle \sigma \rangle$ sont des rotations. Le théorème 2.1 montre alors que $H_{d',k} \simeq D_{d'}$.

En ce qui concerne la première partie, il reste donc à démontrer que les sous-groupes décrits sont deux à deux distincts. Remarquons que l'on ne peut avoir une égalité du type $H_d = H_{d',k}$, puisque H_d ne contient que des rotations, tandis que $H_{d',k}$ contient la symétrie $r^k s$. De plus, H_d étant clairement cyclique d'ordre d, les groupes H_d sont donc deux à deux distincts lorsque d parcourt l'ensemble des diviseurs positifs de n. Supposons maintenant que $H_{d'_1,k_1} = H_{d'_2,k_2}$, avec des notations évidentes. Puisque $H_{d'_i,k_i}$ est isomorphe D_{d_i}, il possède $2d'_i$ éléments. Ainsi, on a $d'_1 = d'_2$. Notons d' cette valeur commune. Sans perte de généralité, on peut supposer que $k_1 \leq k_2$.

Puisque $r^{k_1}s \in H_{d',k_1} = H_{d',k_2}$, d'après le théorème 2.1, il existe un unique $k \in [\![0, d'-1]\!]$ et un unique $\ell \in [\![0,1]\!]$ tels que

$$r^{k_1}s = (r^{\frac{n}{d'}})^k (r^{k_2}s)^\ell,$$

soit

$$r^{k_1}s = r^{\frac{nk}{d'}+k_2\ell}s^\ell.$$

En comparant les déterminants, par exemple, on obtient $\ell = 1$, puis par simplification

$$r^{\frac{nk}{d'}+k_2-k_1} = \mathrm{Id},$$

d'où $\frac{n}{d'}k + k_2 - k_1 \equiv 0\ [n]$, puisque r est d'ordre n. En particulier, on obtient $k_2 - k_1 \equiv 0\ [\frac{n}{d'}]$. Mais, on a

$$0 \leq k_2 - k_1 \leq k_2 < \frac{n'}{d},$$

d'où $k_2 - k_1 = 0$, soit $k_1 = k_2$. Ceci achève la démonstration. □

On peut maintenant décrire les sous-groupes distingués de D_n

Corollaire 3.3. *Soit $n \geq 1$. Alors, les sous-groupes distingués de D_n sont :*

1. *les sous-groupes H_d, $d \mid n$ et D_n si $n \geq 1$ est impair*
2. *les sous-groupes H_d, $d \mid n$, $H_{\frac{n}{2},0}$, $H_{\frac{n}{2},1}$ et D_n si $n \geq 2$ est pair.*

Démonstration. Commençons par montrer que H_d est un sous-groupe distingué de D_n pour tout $d \mid n$. Or, on a

$$rr^{\frac{n}{d}}r^{-1} = r^{\frac{n}{d}} \in H_d,$$

ainsi que

$$sr^{\frac{n}{d}}s^{-1} = r^{-\frac{n}{d}} \in H_d,$$

ce qui suffit à démontrer que H_d est distingué dans D_n. Cherchons maintenant les sous-groupes distingués de la forme $H_{d',k}$. On doit avoir

$$r(r^k s)r^{-1} = r^{k+2}s \in H_{d',k}.$$

Mais alors, $(r^{k+2}s)(r^k s) = r^2 \in H_{d',k}$.

Comme les rotations de $H_{d',k}$ sont les éléments de $\langle r^{\frac{n}{d'}}\rangle$, on a $r^2 \in \langle r^{\frac{n}{d'}}\rangle$, puis $o(r^2) \mid d'$. Si n est impair, r^2 est d'ordre n, et on a $\langle r^2\rangle = \langle r\rangle$. Ainsi, $n \mid d' \mid n$, d'où $d' = n$. Mais alors, nécessairement $k = 0$ et $H_{d',k} = \langle r, s\rangle = D_n$. Si n est pair, r^2 est d'ordre $\dfrac{n}{2}$. On obtient alors $\dfrac{n}{2} \mid d' \mid n$.

Si $d' = n$, on obtient encore le groupe D_n. Si $d' = \frac{n}{2}$, on a $k = 0$ ou 1, et on obtient les groupes $H_{\frac{n}{2},0}$ et $H_{\frac{n}{2},1}$. Vérifions que ces deux sous-groupes sont bien distingués dans D_n. Soit $k = 0$ ou 1. On a

$$r(r^{\frac{n}{2}})r^{-1} = r^{\frac{n}{2}} \in H_{\frac{n}{2},k} \quad \text{et } s(r^{\frac{n}{2}})s^{-1} = r^{-\frac{n}{2}} \in H_{\frac{n}{2},k}$$

ainsi que

$$r(r^k s)r^{-1} = r^{k+2}s = r^2(r^k s) \in H_{\frac{n}{2},k} = \langle r^2, r^k s\rangle$$

et

$$s(r^k s)s^{-1} = r^{-k}s = (r^2)^{-k}(r^k s) \in H_{\frac{n}{2},k},$$

ce qui suffit à démontrer le résultat souhaité. Ceci achève la démonstration. □

Remarque 3.4. Le lecteur vérifiera que si $n = 1$ ou 2, on obtient que tous les sous-groupe de D_n sont distingués, ce qui est normal, puisque D_n est abélien dans ces deux cas.