Sous-groupes du groupe diédral

Cette feuille présente un corrigé de l'exercice 4 de la feuille de TD du lundi 4 novembre 2019 consacrée au groupe diédral.

Exercice 4. (*Sous-groupes*) Établissez la liste des sous-groupes de $\mathbb{D}_n$. Indiquez lesquels sont distingués. (*On pourra classer les sous-groupes H selon la nature de $H^+ := H \cap \langle r \rangle$.*)

Corrigé. On note $G = \mathbb{D}_n$ le groupe diédral à $2n$ éléments (que, attention !, certains auteurs notent parfois $\mathbb{D}_{2n}$). Soit H un sous-groupe de G. On note $H^+ := H \cap \langle r \rangle$ l'ensemble des déplacements de H, et H^- l'ensemble des antidéplacements de H, de sorte que $H = H^+ \cup H^-$. Alors H^+ est un sous-groupe de $G^+ = \langle r \rangle$ qui est cyclique d'ordre n. Il existe donc un diviseur d de n tel que

$$H^+ = \langle r^d \rangle \simeq \mathbb{Z}/m\mathbb{Z} \qquad \text{où } n = md.$$

On notera $\rho = r^d$. Dans toute la suite, nous conserverons ces notations.

▶ Si H ne contient aucun antidéplacement, on a $H = H^+$ et nous venons de faire la liste de tous ces sous-groupes.

▶ Si H contient au moins un antidéplacement σ, nous allons justifier le fait que l'application de multiplication à gauche par σ induit une bijection $L_\sigma : H^+ \xrightarrow{\sim} H^-$, $x \mapsto \sigma x$. En effet, pour tout $x \in H^+$ le produit σx est dans H et est un antidéplacement, donc $\sigma x \in H^-$. Par ailleurs L_σ est injective car il s'agit de la multiplication à gauche par un élément, qui est inversible dans le groupe ambiant G. Enfin L_σ est surjective car tout $y \in H^-$ peut s'écrire $y = \sigma(\sigma^{-1}y)$ avec $x := \sigma^{-1}y \in H^+$. On pourrait résumer (ou court-circuiter) les deux derniers arguments en disant que $L_{\sigma^{-1}} : H^- \longrightarrow H^+$ est une bijection inverse pour L_σ. Si l'on note $\rho = r^d$ et $k \in \{0, \dots, n-1\}$ tel que $\sigma = sr^k$, on obtient exhaustivement :

$$H = H^+ \cup H^- = \{1, \rho, \dots, \rho^{m-1}, \sigma, \sigma\rho, \dots, \sigma\rho^{m-1}\} = \{1, r^d, \dots, r^{(m-1)d}, sr^k, sr^{k+d}, \dots, sr^{k+(m-1)d}\}.$$

Réciproquement, vérifions que pour tout choix de couple (d, k) avec $d|n$ et $k \in \{0, \dots, n-1\}$, l'ensemble

$$H_{d,k} := \{1, r^d, \dots, r^{(m-1)d}, sr^k, sr^{k+d}, \dots, sr^{k+(m-1)d}\}$$

est bien un sous-groupe. Pour cela, on observe qu'on a les relations $\rho^m = (r^d)^m = 1$, $\sigma^2 = 1$ et $(\rho\sigma)^2 = 1$, cette dernière relation venant du fait que $\rho\sigma$ est un antidéplacement et tous les antidéplacements de G sont de carré égal à l'identité. On est en présence des relations bien connues (au moins depuis qu'on a fait l'exercice 1 de la feuille ☺) dans le groupe diédral, qui montrent que l'ensemble $H_{d,k}$ ci-dessus est bien un sous-groupe, d'ailleurs isomorphe à $\mathbb{D}_m$.

Les raisonnements précédents montrent que tout sous-groupe de G est isomorphe

- soit à $\mathbb{Z}/m\mathbb{Z} \simeq \langle r^d \rangle \subset G^+$, s'il ne contient pas de déplacement,
- soit à $H_{d,k}$ s'il contient un déplacement.

▶ Il reste à vérifier que notre liste de sous-groupes ne comporte pas de redondance. Les sous-groupes cycliques $H = \langle r^d \rangle$ sont bien tous distincts. Passons au groupe $H = H_{d,k}$. On voit que les éléments de H^- sont les sr^j tels que $j \equiv k \mod d$, si bien que $H_{d,k}$ ne dépend de k que par sa classe modulo d. Explicitement, si l'on fixe d et on fait varier k, on trouve d'abord d sous-groupes distincts

$$\begin{aligned}
H_{d,0} &= H^+ \cup \{s, sr^d, \dots, sr^{(m-1)d}\} \\
H_{d,1} &= H^+ \cup \{sr, sr^{1+d}, \dots, sr^{1+(m-1)d}\} \\
&\vdots \\
H_{d,d-1} &= H^+ \cup \{sr^{d-1}, sr^{d-1+d}, \dots, sr^{d-1+(m-1)d}\}
\end{aligned}$$

mais ensuite on trouve $H_{d,d} = H_{d,0}$ et l'énumération prend fin ici. On obtient la liste du tableau récapitulatif ci-dessous.

► L'exercice demandait aussi de trouver les sous-groupes qui sont distingués. D'abord justifions le fait que les sous-groupes cycliques $H = \langle r^d \rangle$ sont distingués. En effet, si $g \in G$, alors gHg^{-1} est un sous-groupe de G^+ car G^+ est distingué, et il est de cardinal m. Or dans le groupe cyclique G^+, il y a un seul sous-groupe de cardinal m, donc $gHg^{-1} = H$.

Regardons maintenant les conjugués de $H = H_{d,k}$ avec $k \in \mathbb{Z}/d\mathbb{Z}$ (on va en fait trouver la liste des conjugués de $H_{d,k}$, et celui-ci sera distingué exactement lorsqu'il est son seul conjugué.) Soit $g \in G$. Par le même argument que celui déjà donné, on a $gH^+g^{-1} = H^+ \subset H$. Il reste à regarder l'effet des conjugaisons sur les éléments de H^-, qui sont les $x = sr^j$ tels que $j \equiv k \mod d$.

Une rotation $g = r^i$ agit par $r^i \cdot sr^j \cdot r^{-i} = r^{j-2i}$. Prenant $j = k$, on voit que dans ce cas $gH_{d,k}g^{-1} = H_{d,k-2i}$. L'ensemble des conjugués de $H_{d,k}$ par des rotations est donc l'ensemble des $H_{d,k'}$ tels que $k' \equiv k \mod 2$ dans $\mathbb{Z}/d\mathbb{Z}$. Il est paramétré par l'ensemble $E = \{k' \in \mathbb{Z}/d\mathbb{Z} \ ; \ k' \equiv k \mod 2\}$.

Une réflexion $g = sr^i$ agit par $sr^i \cdot sr^j \cdot sr^i = r^{2i-j}$. Prenant $j = k$, on voit que dans ce cas $gH_{d,k}g^{-1} = H_{d,2i-k}$. L'ensemble des conjugués de $H_{d,k}$ par des réflexions est donc paramétré par $E' = \{k' \in \mathbb{Z}/d\mathbb{Z} \ ; \ k' \equiv -k \mod 2\}$. Or $-k \equiv k \mod 2$ entraîne que $E' = E$, et on n'obtient donc pas ainsi de nouveaux conjugués.

Si d est impair, c'est-à-dire si 2 est inversible modulo d, alors $E = \mathbb{Z}/d\mathbb{Z}$ et tous les $H_{d,k}$, $k \in \mathbb{Z}/d\mathbb{Z}$, sont conjugués. On obtient une classe de conjugaison à d éléments ; cette classe n'est ponctuelle que lorsque $d = 1$, c'est-à-dire $H = G$ qui est le seul sous-groupe distingué de la famille.

Si $d = 2e$ est pair (ce qui impose que n soit pair également !), alors les sous-groupes $H_{d,k}$ tels que $H^+ = \langle r^d \rangle$ se répartissent en deux classes de conjugaison : la classe « paire » composée des $H_{d,2i}$ et la classe « impaire » composée des $H_{d,2i+1}$. Chacune de ces classes contient e éléments. Elles ne sont ponctuelles que lorsque $e = 1$, c'est-à-dire $d = 2$ et dans ce cas $H = H_{2,0}$ et $H_{2,1}$ sont les seuls sous-groupes distingués de la famille.

► Voici un tableau récapitulatif. On note que $\mathbb{D}_1 = \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{D}_2 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ qui sont les deux seuls groupes diédraux commutatifs. Dans le tableau, lorsque $d|n$ on note $n = md$.

Sous-groupes de $G = \mathbb{D}_n = \langle r, s \ ; r^n = s^2 = (rs)^2 = 1 \rangle$			
Paramètre	Sous-groupe H	Classe d'isom.	Distingué ?
d diviseur de n	$C_d = \langle r^d \rangle$	$\mathbb{Z}/m\mathbb{Z}$	oui, et $G/H \simeq \mathbb{D}_d$
couple (d, k) avec $d\|n$ et $k \in \mathbb{Z}/d\mathbb{Z}$	$H_{d,k} = \langle r^d, sr^k \rangle$	$\mathbb{D}_m$	non si $d > 2$ oui si $d = 1$, et $G/H \simeq \{1\}$ oui si $d = 2$, et $G/H \simeq \mathbb{Z}/2\mathbb{Z}$