Groupe diédral, groupe des quaternions, groupes d'ordre $\leqslant 8$

Exercice 1 (*Groupe d'automorphismes du groupe diédral*, [Delcourt, exercice 3.3.12])
Soit $n \geqslant 3$ un entier. Soit $G = \mathbb{D}_n$ le groupe diédral engendré par deux élements r, s satisfaisant les relations $r^n = s^2 = (rs)^2 = 1$.

1. Montrez que pour tout morphisme de groupes $f : G \to H$, les éléments $R = f(r)$ et $S = f(s)$ vérifient les relations $R^n = S^2 = (RS)^2 = 1$. Réciproquement, montrez que pour tout couple $(R, S) \in H^2$ tel que $R^n = S^2 = (RS)^2 = 1$ il existe un unique morphisme de groupes $f : G \to H$ tel que $f(r) = R$ et $f(s) = S$.
2. Déduisez de la question précédente que les automorphismes $f : G \to G$ sont les morphismes $f = f_{i,j}$ déterminés par $f(r) = r^i$ et $f(s) = sr^j$, pour $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $j \in \mathbb{Z}/n\mathbb{Z}$.
3. Cette question nécessite de connaître le concept de produit semi-direct. Montrez que

$$N := \{f_{1,j};\ j \in \mathbb{Z}/n\mathbb{Z}\} \simeq \mathbb{Z}/n\mathbb{Z} \quad , \quad H := \{f_{i,0};\ i \in (\mathbb{Z}/n\mathbb{Z})^\times\} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

   et que $\mathrm{Aut}(G)$ est le produit semi-direct $N \rtimes_\varphi H$ où φ est l'action naturelle de $(\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ sur $\mathbb{Z}/n\mathbb{Z}$.

Corrigé. 1. Comme f est un morphisme de groupes, en prenant les images par f des relations $r^n = s^2 = (rs)^2 = 1$ on trouve les relations $R^n = S^2 = (RS)^2 = 1$. Réciproquement soit $(R, S) \in H^2$ tel que $R^n = S^2 = (RS)^2 = 1$. On sait que chaque élément x de $G = \mathbb{D}_n$ peut s'écrire d'une manière unique sous la forme $x = s^\epsilon r^i$ avec $\epsilon \in \{0, 1\}$ et $i \in \{0, \ldots, n-1\}$. (On pourrait écrire $\epsilon \in \mathbb{Z}/2\mathbb{Z}$ et $i \in \mathbb{Z}/n\mathbb{Z}$ ce qui refléterait mieux les structures des sous-groupes en présence.) S'il existe un morphisme de groupes $f : G \to H$ tel que $f(r) = R$ et $f(s) = S$, nécessairement $f(x) = S^\epsilon R^i$ pour tout $x = s^\epsilon r^i$. L'unicité est donc acquise, et il nous suffit de vérifier que l'application f ainsi définie est bien un morphisme de groupes. Soit $y = s^\eta r^j$, avec $\eta \in \{0, 1\}$ et $j \in \{0, \ldots, n-1\}$, un second élément de G. La relation de commutation fondamentale $r^i s = sr^{-i}$ dans le groupe diédral implique que l'on a $r^i s^\eta = s^\eta r^{(1-2\eta)i}$. On calcule donc :

$$xy = s^\epsilon r^i \cdot s^\eta r^j = s^{\epsilon+\eta} r^{(1-2\eta)i+j}.$$

Il s'ensuit que $f(xy) = S^{\epsilon+\eta} R^{(1-2\eta)i+j}$. Or dans H, les relations $R^n = S^2 = (RS)^2 = 1$ impliquent de même que l'on a $R^i S = SR^{-i}$ donc $R^i S^\eta = S^\eta R^{(1-2\eta)i}$. On voit alors que

$$f(x)f(y) = S^\epsilon R^i \cdot S^\eta R^j = S^{\epsilon+\eta} R^{(1-2\eta)i+j}$$

donc $f(xy) = f(x)f(y)$ et f est bien un morphisme.

2. On note d'abord que d'après la question 1, l'application $f_{i,j}$ donnée dans l'énoncé est un morphimsme de groupes. De plus, si $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ alors r^i engendre le sous-groupe des rotations, en particulier r est dans l'image de $f_{i,j}$. Comme sr^j est dans l'image de $f_{i,j}$, on déduit que s aussi est dans l'image. Donc $f_{i,j}$ est surjectif ce qui démontre que $f_{i,j}$ est bien un automorphisme. Il est clair que les $f_{i,j}$ sont tous différents, lorsque i et j varient dans les ensembles indiqués.

Soit $f : G \to G$ un automorphisme quelconque. La question 1 fournit des relations sur $f(r)$ et $f(s)$, et le fait que f soit un *auto*morphisme implique que son seulement $f(r)$ a sa puissance n-ième égale à 1 mais il est en fait d'ordre exactement n. De même $f(s)$ est d'ordre 2. Or on connait les ordres des éléments dans $G = \mathbb{D}_n$: chaque rotation r^i est d'ordre $n/\operatorname{pgcd}(n,i)$, et une symétrie sr^i est d'ordre 2. Comme on a supposé $n \geqslant 3$, les éléments d'ordre n se trouvent uniquement parmi les rotations, donc $f(r) = r^i$ avec $\operatorname{pgcd}(n,i) = 1$ c'est-à-dire $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. De plus $f(s)$ ne peut être une rotation (attention : si n est pair la rotation $r^{n/2}$ est d'ordre 2 !), car sinon l'image de f serait incluse dans le sous-groupe cyclique engendré par r en contradiction avec la surjectivité de f. Donc $f(s) = sr^j$ pour un $j \in \mathbb{Z}/n\mathbb{Z}$. Alors f est le morphisme $f_{i,j}$ donné dans l'énoncé.

3. Soient $i, k \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $j, l \in \mathbb{Z}/n\mathbb{Z}$. Posons $g = f_{i,j} \circ f_{k,l}$ (dans la suite on omettra le signe $\circ$ de composition). On calcule :

$$g(r) = f_{i,j}(r^k) = r^{ik} \qquad \text{et} \qquad g(s) = f_{i,j}(sr^l) = sr^j r^{il} = sr^{j+il}.$$

Ceci démontre que $f_{i,j} f_{k,l} = f_{ik,j+il}$. En particulier on voit que les ensembles N et H de l'énoncé sont bien des sous-groupes. De plus $N \cap H = \{1\}$ et $NH = G$ car $f_{i,j} = f_{1,j} f_{i,0}$. Ceci démontre que $\operatorname{Aut}(G)$ est le produit semi-direct interne de ses sous-groupes N et H. Finalement la formule $f_{i,j} f_{k,l} = f_{ik,j+il}$ montre exactement que dans le groupe $\operatorname{Aut}(G)$, qui est produit semi-direct de $N \simeq \mathbb{Z}/n\mathbb{Z}$ et $H \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, la multiplication est celle du produit semi-direct correspondant à l'action naturelle de $(\mathbb{Z}/n\mathbb{Z})^\times = \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ par multiplication sur $\mathbb{Z}/n\mathbb{Z}$: en effet on reconnait dans $j + il$ le produit de j avec il (ce « produit » est noté avec un signe $+$ car dans le groupe abélien $\mathbb{Z}/n\mathbb{Z}$ on utilise naturellement la notation additive), qui est « i agissant sur l » ce qui est exactement la définition de $N \rtimes_\varphi H$ telle qu'on la trouve par exemple dans le livre de Perrin.

Références

[Alessandri] M. Alessandri, *Thèmes de géométrie – groupes en situation géométrique*, Dunod.

[Delcourt] J. Delcourt, *Théorie des groupes*, Dunod.

[Ortiz] P. Ortiz, *Exercices d'algèbre*, Ellipses.

[Perrin] D. Perrin, *Cours d'algèbre*, Ellipses.