Éléments de correction du partiel du 4 novembre 2019

Exercice 1.

Montrer que le groupe symétrique $\mathcal{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathcal{S}_3)$.

Éléments de solution 1.

L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathcal{S}_3$ dans $\mathrm{Aut}(\mathcal{S}_3)$, car le centre de $\mathcal{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathcal{S}_3)$ est déterminé par l'image des générateurs (1 2) et (1 3). Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathcal{S}_3$), donc en comparant les ordres on obtient que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 2.

Soient G un groupe et X un ensemble. Notons $\mathcal{S}_X$ l'ensemble des permutations de X. Soit $\phi\colon G \to \mathcal{S}_X$ un morphisme de groupes.

(1) Montrer que $g \cdot x = \phi(g)(x)$ définit une action du groupe G sur X.

(2) Considérons l'action de G sur lui-même par translation à gauche.
   i) Expliciter $\phi\colon \mathrm{G} \to \mathcal{S}_\mathrm{G}$ dans ce cas.
   ii) Montrer que cette action est fidèle.

(3) Supposons que $|\mathrm{G}| = n$.
   i) Montrer que $\mathcal{S}_\mathrm{G}$ est isomorphe au groupe des permutations $\mathcal{S}_n$.
   ii) Montrer que G est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Éléments de solution 2.

(1) Montrons que $g \cdot x = \phi(g)(x)$ définit une action du groupe G sur X.
   - pour tout $x \in X$, $1 \cdot x = \phi(1)(x) = \mathrm{id}(x) = x$;
   - pour tout $x \in X$ et pour tous G, $h \in H$, on a

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot \phi(h)(x) \\ &= [\phi(g) \circ \phi(h)](x) \\ &= \phi(gh)(x) \\ &= (gh) \cdot x \end{aligned}$$

   Ainsi $g \cdot x = \phi(g)(x)$ définit bien une action de groupe.

(2) Considérons l'action de G sur lui-même par translation à gauche.
   i) Explicitons $\phi\colon \mathrm{G} \to \mathcal{S}_\mathrm{G}$ dans ce cas.
   Pour tout $x \in X = \mathrm{G}$ $\phi(g)(x) = gx$.
   ii) Montrons que cette action est fidèle.
   Soit $g \in \mathrm{G}$. Si pour tout $x \in \mathrm{G}$ on a $g \cdot x = gx = x$, alors $g = 1$. L'action est donc fidèle.

(3) Supposons que $|\mathrm{G}| = n$.
   i) Montrons que $\mathcal{S}_\mathrm{G}$ est isomorphe au groupe des permutations $\mathcal{S}_n$.
   Soit $f\colon \mathrm{G} \to \{1, 2, \ldots, n\}$ une bijection. Alors

$$\Psi\colon \mathcal{S}_\mathrm{G} \to \mathcal{S}_n \qquad\qquad \sigma \mapsto f \circ \sigma \circ f^{-1}$$

est un morphisme de groupes (à vérifier). En définissant

$$\Phi\colon \mathcal{S}_n \to \mathcal{S}_{\mathrm{G}} \qquad\qquad \sigma \mapsto f^{-1} \circ \sigma \circ f$$

on vérifie que $\Phi \circ \Psi = \mathrm{id}_{\mathcal{S}_{\mathrm{G}}}$ et $\Psi \circ \Phi = \mathrm{id}_{\mathcal{S}_n}$. Par conséquent Ψ est bijective et donc un isomorphisme.

ii) Montrons que G est isomorphe à un sous-groupe de $\mathcal{S}_n$.
Le morphisme $\phi\colon \mathrm{G} \to \mathcal{S}_{\mathrm{G}}$ défini au (2) est un morphisme injectif de groupes (car l'action est fidèle). La composée $\Psi \circ \phi$ est donc un morphisme injectif de G dans $\mathcal{S}_n$. Il en résulte que G est isomorphe au sous-groupe $\mathrm{im}(\Psi \circ \phi)$ de $\mathcal{S}_n$.

Exercice 3.

Soit $\mathcal{A}_4$ l'ensemble des éléments du groupe des permutations $\mathcal{S}_4$ de signature 1.

(1) Faire la liste des éléments de $\mathcal{A}_4$ et donner leurs ordres.

(2) Soit H l'ensemble formé de l'identité et des permutations

$$(1\ 2)(3\ 4) \qquad (1\ 3)(2\ 4) \qquad (1\ 4)(2\ 3)$$

i) Montrer que H est un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

ii) Montrer que H est un sous-groupe distingué de $\mathcal{A}_4$.

(3) Montrer que les sous-groupes propres de H ne sont pas distingués dans $\mathcal{A}_4$.

(4) Montrer que tout sous-groupe d'indice 2 d'un groupe G est distingué.

(5) Déduire des questions précédentes que $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6 (on pourra raisonner par l'absurde et remarquer qu'une intersection de sous-groupes distingués est distinguée).

(6) Déterminer tous les sous-groupes de $\mathcal{A}_4$. Lesquels sont distingués ?

Éléments de solution 3.

(1) Listons les éléments de $\mathcal{A}_4$ et donnons leurs ordres :
- id est d'ordre 1 ;
- les produits de deux transpositions de supports disjoints $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ et $(1\ 4)(2\ 3)$ sont d'ordre 2.
- les cycles $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$ et $(2\ 4\ 3)$ sont d'ordre 3.

Remarquons que nouve avons listé tous les éléments. En effet on vient de lister 12 éléments et $|\mathcal{A}_4| = \frac{|\mathcal{S}_4|}{2} = \frac{4!}{2} = 4 \cdot 3 = 12$.

(2) i) Montrons que H est un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Posons

$$\sigma_1 = (1\ 2)(3\ 4) \qquad \sigma_2 = (1\ 3)(2\ 4) \qquad \sigma_3 = (1\ 4)(2\ 3)$$

On constate que $\mathrm{H} = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$ est un groupe et que

$$\Phi\colon \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to H \\ (0,0) \mapsto \mathrm{id} \\ (1,0) \mapsto \sigma_1 \\ (0,1) \mapsto \sigma_2 \\ (1,1) \mapsto \sigma_3 \end{cases}$$

est un isomorphisme de groupes.

ii) Montrons que H est un sous-groupe distingué de $\mathcal{A}_4$.
Remarquons que $\mathrm{H} \setminus \{\mathrm{id}\}$ est l'ensemble des permutations de la forme $(a\ b)(c\ d)$ où $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Soit $\sigma_i = (a\ b)(c\ d)$ une telle permutation. Pour toute permutation σ on a

$$\sigma\sigma_i\sigma = (\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$$

et comme σ est une bijection de $\{1, 2, 3, 4\}$ on a bien encore un élément de $\mathrm{H} \setminus \{\mathrm{id}\}$.

(3) Montrons que les sous-groupes propres de H ne sont pas distingués dans $\mathcal{A}_4$.

Le théorème de Lagrange assure que les sous-groupes de H sont de cardinal 1, 2 ou 4. Les sous-groupes non triviaux et propres sont donc d'ordre 2. Ces sous-groupes de cardinal 2 sont les $\langle\sigma_i\rangle$ pour $i = 1, 2, 3$. Ils sont donc de la forme

$$\big\{\mathrm{id},\, \sigma_i = (a\ b)(c\ d)\big\}$$

où $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Or si $\sigma = (b\ c\ d)$, alors

$$\sigma\sigma_i\sigma^{-1} = (a\ \sigma(b))(\sigma(c)\ \ \sigma(d)) \notin \big\{\mathrm{id},\, \sigma_i = (a\ b)(c\ d)\big\}$$

Ainsi $\langle\sigma_i\rangle$ n'est pas distingué dans $\mathcal{A}_4$.

(4) Montrons que tout sous-groupe d'indice 2 d'un groupe G est distingué.

Soit G un groupe. Soit H un sous-groupe d'indice 2 de G. Nous avons donc ${}^{\mathrm{G}}\!/_{\mathrm{H}} = \big\{\mathrm{H},\, x\mathrm{H}\big\}$ où $x \neq \mathrm{H}$ et $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $\mathrm{H} \cap x\mathrm{H} = \emptyset$.

Soit $g \in \mathrm{G}$. Ou bien $g \in \mathrm{H}$ et $g\mathrm{H}g^{-1} = \mathrm{H}$. Ou bien $g \notin \mathrm{H}$ et $g \in x\mathrm{H}$; il existe donc $h_0 \in \mathrm{H}$ tel que $g = xh_0$. Soit alors $h \in \mathrm{H}$; nous avons

$$ghg^{-1} = xh_0hh_0^{-1}x^{-1} = xh'x^{-1}$$

où $h' = h_0hh_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à $x\mathrm{H}$, *i.e.* $xh'x^{-1}$ s'écrit xh_1 avec h_1 dans H. Ceci implique que x appartient à H : contradiction. Par conséquent $xh'x^{-1}$ appartient à H, *i.e.* ghg^{-1} appartient à H. Autrement dit H est un sous-groupe distingué de G.

(5) Montrons que $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6.

Supposons par l'absurde que $\mathcal{A}_4$ ait un sous-groupe K d'ordre 6. Le théorème de Lagrange assure que $|\mathrm{K} \cap \mathrm{H}|$ divise $|\mathrm{K}|$ et $|\mathrm{H}|$; par suite $|\mathrm{K} \cap \mathrm{H}|$ appartient à $\{1, 2\}$. Si $\mathrm{K} \cap \mathrm{H} = \{e_{\mathrm{G}}\}$, alors $|\mathrm{KH}| = |\mathrm{H}| \cdot |\mathrm{K}|$: absurde. Par conséquent $\mathrm{K} \cap \mathrm{H}$ est un sous-groupe d'ordre 2 dans H. D'après (2) et (4) H et K sont distingués dans $\mathcal{A}_4$, donc $\mathrm{K} \cap \mathrm{H}$ est distingué dans $\mathcal{A}_4$: contradiction avec (3).

(6) Déterminons tous les sous-groupes de $\mathcal{A}_4$ et précisons lesquels sont distingués.

D'après le théorème de Lagrange et (5) les sous-groupes de $\mathcal{A}_4$ sont d'ordre 1, 2, 3, 4 ou 12.

— Les groupes triviaux $\{\mathrm{id}\}$ et $\mathcal{A}_4$ sont distingués.

— 2 et 3 sont premiers donc les groupes d'ordre 2 et 3 sont monogènes. Or on a listé en (1) les éléments d'ordre 2 et 3.

- les groupes d'ordre 2 sont donc les $\langle\sigma_i\rangle$ pour $i = 1, 2, 3$. Ils ne sont pas distingués (voir (3)).
- les groupes d'ordre 3 sont $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, $\langle(1\ 3\ 4)\rangle$, $\langle(2\ 3\ 4)\rangle$. Un argument similaire à celui donné dans (3) assure que ces groupes ne sont pas distingués dans $\mathcal{A}_4$.
- Soit K un groupe d'ordre 4. Ce groupe ne peut pas être cyclique car $\mathcal{A}_4$ ne contient pas d'élément d'ordre 4. Ainsi les éléments de $\mathrm{K} \setminus \{\mathrm{id}\}$ sont d'ordre 2. Or il n'y a que trois éléments d'ordre 2 : les σ_i. Ainsi $\mathrm{K} = \mathrm{H}$ est l'unique groupe d'ordre 4. D'après (2)(ii) il est distingué.

Exercice 4.

Soit $n \geq 2$ un entier.

(1) Montrer que les transpositions sont conjuguées dans $\mathcal{S}_n$, *i.e.* montrer que pour tout couple (τ_1, τ_2) de transpositions il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$.

(2) En déduire que le seul morphisme de groupes non trivial de $\mathcal{S}_n$ dans $(\mathbb{C}^*, \cdot)$ est la signature.

(3) En déduire que le seul sous-groupe de $\mathcal{S}_n$ d'indice 2 est le groupe $\mathcal{A}_n$ des permutations de signature 1 (on pourra utiliser le fait que tout sous-groupe d'indice 2 d'un groupe G est distingué).

Éléments de solution 4.

Soit $n \geq 2$ un entier.

(1) Montrons que les transpositions sont conjuguées dans $\mathcal{S}_n$, *i.e.* montrer que pour tout couple (τ_1, τ_2) de transpositions il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$.

Soient deux transpositions $\tau_1 = (a\ b)$ et $\tau_2 = (c\ d)$. Soit σ une permutation qui envoie a sur c et b sur d. Alors $\sigma\tau_1\sigma^{-1} = (\sigma(a)\ \sigma(b)) = \tau_2$.

(2) Montrons que le seul morphisme de groupes non trivial de $\mathcal{S}_n$ dans $(\mathbb{C}^*, \cdot)$ est la signature.

Soit $\phi\colon \mathcal{S}_n \to \mathbb{C}^*$ un morphisme de groupes. D'après (1) pour toutes transpositions τ_1, τ_2 il existe une permutation σ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$. Par suite

$$\phi(\tau_2) = \phi(\sigma\tau_1\sigma^{-1}) = \phi(\sigma)\phi(\tau_1)\phi(\sigma)^{-1} = \phi(\tau_1).$$

Or si τ est une transposition $\big(\phi(\tau)\big)^2 = \phi(\tau^2) = \phi(\mathrm{id}) = 1$ d'où $\phi(\tau) = \pm 1$. Il en résulte l'alternative suivante :

— toutes les transpositions sont envoyées sur 1 et comme les transpositions engendrent $\mathcal{S}_n$ ϕ est identiquement égal à 1 ;

— toutes les transpositions sont envoyées sur -1 et puisque les transpositions engendrent $\mathcal{S}_n$ nous avons $\mathrm{Im}\phi \subset \langle -1\rangle = \{-1, 1\}$. Ce morphisme est la signature.

(3) Montrons que le seul sous-groupe de $\mathcal{S}_n$ d'indice 2 est le groupe $\mathcal{A}_n$ des permutations de signature 1 (on pourra utiliser le fait que tout sous-groupe d'indice 2 d'un groupe G est distingué).

Soit H un sous-groupe de $\mathcal{S}_n$ d'indice 2. Alors H est distingué dans $\mathcal{S}_n$. Par conséquent $\mathcal{S}_n/\mathrm{H}$ est un groupe de cardinal 2 et donc isomorphe à $\{-1, 1\}$. La surjection canonique $s\colon \mathcal{S}_n \to \mathcal{S}_n/\mathrm{H}$ donne un morphisme non trivial de $\mathcal{S}_n$ vers $\{-1, 1\}$. D'aprés (2) c'est la signature. Son noyau H est donc $\mathcal{A}_n$. Ainsi le seul sous-groupe de $\mathcal{S}_n$ d'indice 2 est le groupe $\mathcal{A}_n$.

Exercice 5.

Soit G un groupe fini. Soit p un facteur premier de G.

(1) Montrer que le sous-ensemble

$$\Sigma = \big\{(x_1, \ldots, x_p) \in \mathrm{G}^p \,|\, x_1 \ldots x_p = \mathrm{e_G}\big\}$$

de G^p est en bijection avec G^{p-1}.

(2) Notons "n mod p" le reste de la division euclidienne de n par p. Montrer que l'application

$$\phi\colon \mathbb{Z}/p\mathbb{Z} \times \Sigma \to \Sigma \quad (\overline{k}, (x_1, \ldots, x_p)) \mapsto \overline{k} \cdot (x_1, \ldots, x_p) = (x_{1+k \bmod p}, \ldots, x_{p+k \bmod p})$$

est bien définie et que c'est une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble Σ.

(3) Montrer que le stabilisateur de $(x_1, x_2, \ldots, x_p)$ est $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x_1 = x_2 = \ldots = x_p$.

(4) En appliquant l'équation aux classes, en déduire que G contient au moins un élément d'ordre p.

Éléments de solution 5.

(1) Montrons que le sous-ensemble

$$\Sigma = \left\{(x_1, \ldots, x_p) \in \mathrm{G}^p \,|\, x_1 \ldots x_p = \mathrm{e}_G\right\}$$

de G^p est en bijection avec G^{p-1}.

Remarquons que

$$\Sigma = \left\{((x_2 x_3 \ldots x_p)^{-1}, \ldots, x_p) \in \mathrm{G}^p \,|\, x_2, \ldots, x_p \in \mathrm{G}\right\}$$

donc Σ est en bijection avec G^{p-1}.

(2) Notons "n mod p" le reste de la division euclidienne de n par p. Montrons que l'application

$$\phi\colon \mathbb{Z}/p\mathbb{Z} \times \Sigma \to \Sigma \quad (\overline{k}, (x_1, \ldots, x_p)) \mapsto \overline{k} \cdot (x_1, \ldots, x_p) = (x_{1+k \bmod p}, \ldots, x_{p+k \bmod p})$$

est bien définie et que c'est une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble Σ.

Si k et k' sont des éléments de $\mathbb{Z}$ tels que $\overline{k} = \overline{k'}$ dans $\mathbb{Z}/p\mathbb{Z}$ alors K mod $p = k'$ mod p. L'application ϕ est donc bien définie.

De plus $\overline{0} \cdot (x_1, \ldots, x_p) = (x_1, \ldots, x_p)$ et pour tous k, k' dans $\mathbb{Z}$ on a

$$\begin{aligned} \overline{k'} \cdot (\overline{k} \cdot (x_1, \ldots, x_p)) &= \\ &= \overline{k + k'} \cdot (\overline{k} \cdot (x_1, \ldots, x_p)) \\ &= (\overline{k} + \overline{k'}) \cdot (\overline{k} \cdot (x_1, \ldots, x_p)) \end{aligned}$$

On a donc bien une action de groupes.

(3) Montrons que le stabilisateur de $(x_1, x_2, \ldots, x_p)$ est $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x_1 = x_2 = \ldots = x_p$.

Si le stabilisateur de $(x_1, x_2, \ldots, x_p)$ est $\mathbb{Z}/p\mathbb{Z}$, alors en particulier $\overline{1}$ appartient au stabilisateur de $(x_1, x_2, \ldots, x_p)$ et donc $x_1 = x_2$, $x_2 = x_3$, …, $x_{p-1} = x_p$.

Réciproquement si $x_1 = x_2 = \ldots = x_p$, alors $\overline{k} \cdot (x_1, \ldots, x_p) = (x_1, \ldots, x_p)$ pour tout k.

Ainsi le stabilisateur de $(x_1, x_2, \ldots, x_p)$ est $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x_1 = x_2 = \ldots = x_p$.

(4) Montrons que G contient au moins un élément d'ordre p.

L'équation aux classes assure que

$$|\mathrm{G}|^{p-1} = |\Sigma| = \sum_{\mathcal{O} \in \{ \text{ orbites } \}} |\mathcal{O}|$$

Comme p divise $|\mathrm{G}|$ et $p \geq 2$, p divise $|\mathrm{G}|^{p-1}$. De plus le cardinal de l'orbite d'un point divise $\left|\mathbb{Z}/p\mathbb{Z}\right|$, donc vaut p ou 1. Par suite le nombre d'orbites de cardinal 1 divise p.

L'orbite de $(1, \ldots, 1)$ est une orbite de cardinal 1 qui appartient à Σ. Il en résulte qu'il y en a donc au moins p. En particulier il existe $x = (x_1, \ldots, x_p)$ dans $\Sigma \smallsetminus \{(1, \ldots, 1)\}$ dont l'orbite est de cardinal 1. La question (3) assure alors que $x_1 = x_2 = \ldots = x_p$.

Il existe donc un élément x_1 dans $\mathrm{G} \smallsetminus \{1\}$ tel que $x_1 x_2 \ldots x_p = x_1^p = 1$. Puisque p est premier x_1 est d'ordre p.

Exercice 6. Produit semi-direct

(1) Soient H et K deux groupes multiplicatifs. Désignons par Aut(H) le groupe des automorphismes de H. Soit

$$\varphi\colon \mathrm{K} \to \mathrm{Aut(H)}, \qquad k \mapsto \varphi_k$$

un morphisme de groupes.

a) Montrer que l'ensemble $\mathrm{H} \times \mathrm{K}$ muni de la loi

$$(h,k)\cdot(h',k') = (h\varphi_k(h'), kk')$$

est un groupe. Le groupe ainsi obtenu est appelé produit semi-direct de H par K relativement à φ et est noté $\mathrm{H} \rtimes_\varphi \mathrm{K}$. Si φ est le morphisme trivial (*i.e.* si $\varphi_k = 1_{\mathrm{Aut(H)}} = \mathrm{id}_\mathrm{H}$ pour tout $k \in \mathrm{K}$), on retrouve le produit direct de H et K.

b) Supposons que H et K sont abéliens. Montrer que $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est abélien si et seulement si φ est le morphisme trivial.

c) Soient

$$\mathrm{H}' = \mathrm{H}\times\{1\} = \big\{(h,1)\,|\,h\in\mathrm{H}\big\} \qquad \mathrm{K}' = \{1\}\times\mathrm{K} = \big\{(1,k)\,|\,k\in\mathrm{K}\big\}$$

Montrer que H' et K' sont deux sous-groupes de $\mathrm{H} \rtimes_\varphi \mathrm{K}$.
Montrer que $\mathrm{H}' \subset \mathrm{H} \rtimes_\varphi \mathrm{K}$ est distingué.
Remarquer que $\mathrm{H}'\cdot\mathrm{K}' = \mathrm{H}\rtimes\mathrm{K}$ et $\mathrm{H}'\cap\mathrm{K}' = \{(1,1)\}$ et montrer que le groupe quotient $\mathrm{H}\rtimes\mathrm{K}/\mathrm{H}'$ est isomorphe à K.

(2) Réciproquement soient G un groupe et E, F deux sous-groupes de G. Supposons que E est distingué dans G, que $\mathrm{E}\cdot\mathrm{F} = \mathrm{G}$ et que $\mathrm{E}\cap\mathrm{F} = \{1\}$. On définit

$$\psi\colon \mathrm{F} \to \mathrm{Int(E)}, \qquad x \mapsto \psi_x$$

où ψ_x est l'automorphisme intérieur $y \mapsto xyx^{-1}$ de E. Montrer que G et $\mathrm{E}\rtimes_\psi \mathrm{F}$ sont isomorphes.

(3) a) Soit $n \geq 1$ un entier. Exhiber un isomorphisme entre le groupe diédral D_{2n} et un produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$. A-t-on $\mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

b) À l'aide de la question 1. b) construire un groupe non abélien d'ordre $21 = 3\times 7$.

Éléments de solution 6.

(1) Soient H et K deux groupes multiplicatifs. Désignons par Aut(H) le groupe des automorphismes de H. Soit

$$\varphi\colon \mathrm{K} \to \mathrm{Aut(H)}, \qquad k \mapsto \varphi_k$$

un morphisme de groupes.

a) Montrons que l'ensemble $\mathrm{H} \times \mathrm{K}$ muni de la loi

$$(h,k)\cdot(h',k') = (h\varphi_k(h'), kk')$$

est un groupe. Le groupe ainsi obtenu est appelé produit semi-direct de H par K relativement à φ et est noté $\mathrm{H} \rtimes_\varphi \mathrm{K}$. Si φ est le morphisme trivial (*i.e.* si $\varphi_k = 1_{\mathrm{Aut(H)}} = \mathrm{id}_\mathrm{H}$ pour tout $k \in \mathrm{K}$), on retrouve le produit direct de H et K.
Vérification directe.

b) Supposons que H et K soient abéliens. Montrons que $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est abélien si et seulement si φ est le morphisme trivial.
Soient $(h,k), (h',k') \in \mathrm{H}\rtimes\mathrm{K}$, on a

$$(h,k)\cdot(h',k') = (h\varphi_k(h'), kk') \qquad \text{et} \qquad (h',k')\cdot(h,k) = (h'\varphi_{k'}(h), k'k)$$

Puisque H et K sont abéliens $(h,k)\cdot(h',k') = (h',k')\cdot(h,k)$ si et seulement $h\varphi_k(h') = h'\varphi_{k'}(h)$.

— Supposons que $H \rtimes K$ soit abélien c'est-à-dire $h\varphi_k(h') = h'\varphi_{k'}(h)$ pour tous H, $h' \in$ H et K, $k' \in$ K. En prenant $h = 1 \in$ H on a

$$\varphi_k(h') = h'\varphi_{k'}(1) = 1 \qquad \forall\, k \in \mathrm{K},\, \forall\, h' \in \mathrm{H}.$$

En particulier $\varphi_k = \mathrm{id}_\mathrm{H} \in \mathrm{Aut(H)}$. Le morphisme $\varphi\colon \mathrm{K} \to \mathrm{Aut(H)}$ est donc trivial.

— Réciproquement supposons que $\varphi\colon \mathrm{K} \to \mathrm{Aut(H)}$ soit trivial, c'est-à-dire $\varphi_k = \mathrm{id}_\mathrm{H}$ pour tout $k \in$ K. On a $h\varphi_k(h') = hh'$ et $h'\varphi_{k'}(h) = h'h$ d'où

$$h\varphi_k(h') = h'\varphi_{k'}(h) = hh'.$$

Autrement dit le groupe H $\rtimes$ K est abélien.

c) Soient

$$\mathrm{H}' = \mathrm{H} \times \{1\} = \big\{(h,1) \,|\, h \in \mathrm{H}\big\} \qquad \mathrm{K}' = \{1\} \times \mathrm{K} = \big\{(1,k) \,|\, k \in \mathrm{K}\big\}$$

Montrons que H′ et K′ sont deux sous-groupes de H $\rtimes_\varphi$ K.
Montrons que H′ $\subset$ H $\rtimes_\varphi$ K est distingué.
Remarquons que H′ · K′ = H $\rtimes$ K et H′ $\cap$ K′ = $\{(1,1)\}$ et montrons que le groupe quotient $^{\mathrm{H} \rtimes \mathrm{K}}\!/_{\mathrm{H}'}$ est isomorphe à K.
Vérification directe.

(2) Réciproquement soient G un groupe et E, F deux sous-groupes de G. Supposons que E est distingué dans G, que E · F = G et que E $\cap$ F = $\{1\}$. On définit

$$\psi\colon \mathrm{F} \to \mathrm{Int(E)}, \qquad x \mapsto \psi_x$$

où ψ_x est l'automorphisme intérieur $y \mapsto xyx^{-1}$ de E. Montrons que G et E $\rtimes_\psi$ F sont isomorphes.

Considérons l'application

$$\alpha\colon \mathrm{E} \rtimes_\psi \mathrm{F} \to \mathrm{G} \qquad (e,f) \mapsto e \cdot f$$

Montrons que c'est un morphisme de groupes. En effet soient (e,f), (e',f') dans E $\rtimes_\psi$ F. On a

$$\alpha((e,f)(e',f')) = \alpha(e\psi_f(e'), ff') = e\psi_f(e')ff'.$$

Par définition $\psi_f(e') = fe'f^{-1}$. On en déduit que

$$\alpha((e,f)(e',f')) = e\psi_f(e')ff' = efe'f^{-1}ff' = efe'f'.$$

D'autre part $\alpha(e,f)\cdot\alpha(e',f') = efe'f'$ par suite $\alpha((e,f)(e',f')) = \alpha(e,f)\cdot\alpha(e',f')$. Autrement dit α est un morphisme de groupes.

Vérifions que ce morphisme α est un isomorphisme : puisque G = E · F pour tout $g \in$ G il existe $e \in$ E et $f \in$ F tels que $g = ef$. Par suite $\alpha(e,f) = g$, *i.e.* α est surjective. Pour vérifier l'injectivité de α il suffit d'étudier son noyau $\ker\alpha$. Soit $(e,f) \in \ker\alpha = \mathrm{E} \rtimes_\psi \mathrm{F}$. Alors $1 = \alpha(e,f) = ef$. Ainsi $e^{-1} \in \mathrm{E} \cap \mathrm{F} = \{1\}$. D'où $e = f = 1$.

(3) a) Soit $n \geq 1$ un entier. Exhibons un isomorphisme entre le groupe diédral D_{2n} et un produit semi-direct de $^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ par $^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. A-t-on $\mathrm{D}_{2n} \simeq {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$?
Par définition $\mathrm{D}_{2n} = \langle \alpha, \tau \,|\, \alpha^n = 1,\, \tau^2 = 1,\, \sigma\tau = \tau\sigma^{-1}\rangle$. Considérons $\phi\colon {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \to \mathrm{Aut}\Big({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\Big)$ tel que $\phi(\overline{0}) = \mathrm{id}$ et

$$\phi(\overline{1})\colon {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, \qquad \overline{m} \mapsto \overline{-m}.$$

On vérifie que ϕ ainsi défini est un morphisme de groupes.
Considérons l'application

$$\beta\colon {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \rtimes {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \to \mathrm{D}_{2n}, \qquad (\overline{m},\overline{i}) \mapsto \sigma^m\tau^i$$

C'est un isomorphisme de groupes.

Remarquons que si $n \geq 3$, alors D_{2n} n'est pas isomorphe à $\mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ car D_{2n} n'est pas abélien dès que $n \geq 3$.

b) À l'aide de la question 1. b) construisons un groupe non abélien d'ordre $21 = 3 \times 7$.

Puisque 7 est premier le groupe $\mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right) = \left(\mathbb{Z}/7\mathbb{Z}\right)^*$ est cyclique d'ordre 6. Soit σ un générateur de $\mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right)$ qui est donc d'odre 6. Considérons l'application

$$\gamma \colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right), \qquad \bar{i} \mapsto \sigma^{2i}$$

qui est un morphisme de groupes. Comme $\sigma \in \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right)$ est d'ordre 6, l'application γ est non triviale. Il en résulte par $(1)b)$ que le produit semi-direct $\mathbb{Z}/7\mathbb{Z} \rtimes_\gamma \mathbb{Z}/3\mathbb{Z}$ n'est pas abélien.

Exercice 7. Sous-groupes transitifs de $\mathcal{S}_4$

Soit $n \geq 1$.

Rappelons qu'un sous-groupe G de $\mathcal{S}_n$ est dit transitif si son action sur $\{1, 2, \ldots, n\}$ est transitive, c'est-à-dire si pour tous i, $j \in \{1, 2, \ldots, n\}$ il existe $g \in \mathrm{G}$ tel que $g(i) = j$.

Rappelons aussi que le commutant d'un élément γ d'un groupe Γ est le sous-groupe de Γ des éléments qui commutent avec γ.

(1) Montrer que n divise l'ordre de tout sous-groupe transitif de $\mathcal{S}_n$.

(2) Déterminer les sous-groupes transitifs de $\mathcal{S}_3$.

(3) Soit H le sous-groupe de $\mathcal{S}_4$ engendré par (1 2 3 4) et (1 3).
   a) Déterminer les sous-groupes de H qui sont transitifs.
   b) Déterminer le commutant de chaque élément d'ordre 2 de $\mathcal{S}_4$, et réaliser H de cette manière.
   c) Soit G un sous-groupe transitif de $\mathcal{S}_4$ d'ordre un diviseur de 8. Montrer qu'il est conjugué à l'un de ceux déterminés au a).
   d) Établir, à conjugaison près, la liste des sous-groupes transitifs de $\mathcal{S}_4$.

Éléments de solution 7.

(1) Montrons que n divise l'ordre de tout sous-groupe transitif de $\mathcal{S}_n$.

Soit G un sous-groupe transitif de $\mathcal{S}_n$. Désignons par $\mathrm{G}_1 \subset G$ le stabilisateur de l'élément 1, alors $|\mathrm{G}| = |\mathrm{G}_1| \cdot |\mathcal{O}_1|$ où $\mathcal{O}_1$ est l'orbite de l'action de G sur $\{1, 2, \ldots, n\}$ contenant 1. Puisque G agit transitivement sur $\{1, 2, \ldots, n\}$ il n'y a qu'une seule orbite pour cette action. Ainsi $\mathcal{O}_1 = \{1, 2, \ldots, n\}$ par suite $|\mathcal{O}_1| = n$. Ainsi $n = |\mathcal{O}_1|$ divise $|\mathrm{G}|$.

(2) Déterminons les sous-groupes transitifs de $\mathcal{S}_3$.

Soit G un sous-groupe transitif de $\mathcal{S}_3$. En particulier la formule de Lagrange assure que $|\mathrm{G}| \in \{1, 2, 3, 6\}$. D'après (1) 3 divise $|\mathrm{G}|$, par suite $|\mathrm{G}| = 3$ ou 6.

Si $|\mathrm{G}| = 3$, alors G est l'unique sous-groupe d'ordre 3 de $\mathcal{S}_3$:

$$\mathrm{G} = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

et on vérifie que G est transitif.

Si $|\mathrm{G}| = 6$, alors on a forcément $\mathrm{G} = \mathcal{S}_3$ qui est également transitif.

(3) Soit H le sous-groupe de $\mathcal{S}_4$ engendré par (1 2 3 4) et (1 3).

a) Déterminons les sous-groupes de H qui sont transitifs. Un calcul explicite montre que

$$\mathrm{H} = \big\{\mathrm{id},\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2),\ (1\ 3),\ (1\ 4)(2\ 3),\ (2\ 4),\ (1\ 2)(3\ 4)\big\}$$

En particulier H est d'ordre 8.

b) Déterminons le commutant de chaque élément d'ordre 2 de $\mathcal{S}_4$, et réalisons H de cette manière.
Posons $\sigma = (1\ 3)(2\ 4)$. Désignons par $C(\sigma)$ le commutant de σ dans $\mathcal{S}_4$. Un calcul explicite conduit à

$$(1\ 2\ 3\ 4)\sigma = \sigma(1\ 2\ 3\ 4) \qquad\qquad (1\ 3)\sigma = \sigma(1\ 3)$$

Autrement dit les deux générateurs de H sont contenus dans $C(\sigma)$. Puisque $C(\sigma)$ est un sous-groupe de $\mathcal{S}_4$ on en déduit que $\mathrm{H} \subset C(\sigma)$. En particulier $8 = |\mathrm{H}| \leq |C(\sigma)|$.
D'autre part $\mathcal{S}_4$ agit sur lui-même par conjugaison

$$\mathcal{S}_4 \times \mathcal{S}_4 \to \mathcal{S}_4, \qquad\qquad (\tau, x) \mapsto \tau x \tau^{-1}$$

On note $\mathcal{O}_\sigma \subset \mathcal{S}_4$ l'orbite de $\sigma \in \mathcal{S}_4$ sous cette action. On a

$$\mathcal{O}_\sigma = \big\{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$$

En particulier $|\mathcal{O}_\sigma| = 3$.
Par définition $C(\sigma)$ est le stabilisateur de σ sous l'action par conjugaison ; il en résulte que

$$|\mathcal{S}_4| = |C(\sigma)||\mathcal{O}_\sigma|$$

Par suite $|C(\sigma)| = 8$. Il s'en suit que $\mathrm{H} = C(\sigma)$.

c) Soit G un sous-groupe transitif de $\mathcal{S}_4$ d'ordre un diviseur de 8. D'après (1) 4 divise |K|. Par conséquent |K| appartient à $\{4, 8\}$.
Supposons que $|\mathrm{K}| = 4$. Alors l'action de K sur $\{1, 2, 3, 4\}$ est simplement transitive. On distingue deux possibilités :
— si K est cyclique d'ordre 4, alors K est conjugué à $\langle(1\ 2\ 3\ 4)\rangle$.
— Si K n'est pas cyclique, alors comme K agit transitivement sur $\{1, 2, 3, 4\}$ on peut trouver un élément τ dans K tel que $\tau(1) = 2$. Ainsi $\tau = (1\ 2)(3\ 4)$. De même on montre que K contient $(1\ 3)(2\ 4)$ et $(1\ 4)(2\ 3)$. Par suite $K = \big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$.

Enfin supposons que $|\mathrm{K}| = 8$. Le stabilisateur de tout élément de $\{1, 2, 3, 4\}$ est d'ordre 2 donc est, en particulier, non trivial. Quitte à renuméroter les 1, 2, 3 et 4 (ce qui revient à remplacer K par un conjugué de K) on peut supposer que $(1\ 3)$ et $(2\ 4)$ appartiennent à K. En particulier $(1\ 3)$ et $(2\ 4)$ engendent un sous-groupe K' de K d'ordre 4. Puisque K est d'ordre 8, K' est d'indice 2 dans K et est donc distingué dans K. En particulier l'élément $(1\ 3)(2\ 4)$ engendre un sous-groupe de K d'ordre 2 qui est également distingué dans K. Il s'en suit que $(1\ 3)(2\ 4)$ appartient au centre de K. Par conséquent K est contenu dans le commutant de $(1\ 3)(2\ 4)$ dans $\mathcal{S}_4$. Mais d'après (3)b) le commutant de $(1\ 3)(2\ 4)$ dans $\mathcal{S}_4$ est le sous-groupe de $\mathcal{S}_4$ engendré par $(1\ 2\ 3\ 4)$ et $(1\ 3)$. Ainsi $\mathrm{K} = \mathrm{H} = \langle(1\ 2\ 3\ 4)\,(1\ 3)\rangle$.

d) Établissons, à conjugaison près, la liste des sous-groupes transitifs de $\mathcal{S}_4$.
Soit K un sous-groupe transitif de $\mathcal{S}_4$. D'après (1) 4 divise |K|. Donc |K| appartient à $\{4, 8, 12, 24\}$.
Si $|\mathrm{K}| = 4$, alors il y a deux possibilités à conjugaison près

$$\langle(1\ 2\ 3\ 4)\rangle \qquad\qquad \big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}.$$

Si $|\mathrm{K}| = 8$, alors il n'y a qu'une possibilité à conjugaison près

$$\mathrm{K} = \langle (1\ 2\ 3\ 4),\ (1\ 3) \rangle$$

Si $|\mathrm{K}| = 12$, alors K est d'indice 2 dans $\mathcal{S}_4$ donc distingué dans $\mathcal{S}_4$. Par conséquent $\mathrm{K} = \mathcal{A}_4 \subset \mathcal{S}_4$.
Si $|\mathrm{K}| = 24$, alors $\mathrm{K} = \mathcal{S}_4$.

Exercice 8. Classification des groupes non abéliens d'ordre 8

Le but de cet exercice est de déterminer tous les groupes non abéliens d'ordre 8 à isomorphisme près.

Soit G un group fini ; on désigne par $Z(\mathrm{G})$ le centre de G.

(1) Montrer que $Z(\mathrm{G})$ est un sous-groupe distingué de G. Si G est d'ordre 8, quels sont les ordres possibles pour $Z(\mathrm{G})$?

(2) Montrer que si $\mathrm{G}/Z(\mathrm{G})$ est un groupe cyclique, alors G est abélien.

(3) Soit p un nombre premier. Supposons que le cardinal de G soit une puissance de p. Montrer que $Z(\mathrm{G}) \neq \{e_{\mathrm{G}}\}$ (indication : on pourra considérer l'action de G sur lui-même par conjugaison puis utiliser l'équation aux classes pour trouver une formule du type suivant

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{n} \frac{|\mathrm{G}|}{|\mathrm{H}_i|}$$

les $\mathrm{H}_i \subsetneq \mathrm{G}$ désignant certains sous-groupes de G).

(4) Supposons désormais que G est non abélien d'ordre $8 = 2^3$.
   a) Montrer que $Z(\mathrm{G}) \subset \mathrm{G}$ est un sous-groupe d'ordre 2 et que $\mathrm{G}/Z(\mathrm{G}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   b) Montrer que G contient au moins un élément d'ordre 4.
   c) Montrer que tout sous-groupe de G d'ordre 4 est distingué dans G.
   Soit $\mathrm{H} \subset \mathrm{G}$ un sous-groupe cyclique d'ordre 4 de G.
   cas 1 Il existe dans $\mathrm{G} \setminus \mathrm{H}$ un élément d'ordre 2. Montrer alors que $\mathrm{G} = \langle \mathrm{H}, x \rangle$.
   Montrer que l'automorphisme

$$\mathrm{H} \to \mathrm{H} \qquad\qquad g \mapsto xgx^{-1}$$

   est égal à $g \mapsto g^{-1}$. En déduire que G est isomorphe au groupe diédral D_8.
   cas 2 Tout élément de $\mathrm{G} \setminus \mathrm{H}$ est d'ordre 4. Montrer alors que G n'a qu'un seul élément d'ordre 2 et qu'il engendre $Z(\mathrm{G})$. On le note par -1. Soit i un générateur de H et soit $j \in \mathrm{G} \setminus \mathrm{H}$. On pose $k = ij$. Montrer que $i^2 = j^2 = k^2 = -1$. On note alors $-i$ pour i^3, $-j$ pour j^3 et $-k$ pour k^3. Écrire la table de Cayley de G.

Éléments de solution 8.

(1) Montrons que $Z(\mathrm{G})$ est un sous-groupe distingué de G.

Voir cours.

D'après le Théorème de Lagrange $Z(\mathrm{G})$ est d'ordre 1, 2, 4 ou 8.

(2) Montrons que si $\mathrm{G}/Z(\mathrm{G})$ est un groupe cyclique, alors G est abélien.

Rappelons que le centre $Z(\mathrm{G})$ de G est distingué (voir (1)). Considérons le morphisme quotient $\pi\colon \mathrm{G} \to \mathrm{G}/Z(\mathrm{G})$. Par hypothèse $\mathrm{G}/Z(\mathrm{G})$ est engendré par un élément $\overline{g_0}$. Puisque π est surjective il existe $g_0 \in \mathrm{G}$ tel que $\pi(g_0) = \overline{g_0}$. Soient

G, H dans G. Il existe n, $m \in \mathbb{Z}$ tels que $\pi(g) = \overline{g_0}^n$ et $\pi(h) = \overline{g_0}^m$. Par suite $\pi(gg_0^{-n}) = \pi(hg_0^{-m}) = e$ et $y = gg_0^{-n}$, $z = gg_0^{-m}$ appartiennent à $Z(\mathrm{G})$. Alors

$$gh = yg_0^n z g_0^m = yz g_0^{n+m} = z g_0^m y g_0^n = hg$$

c'est-à-dire G est abélien.

(3) Soit p un nombre premier. Supposons que le cardinal de G soit une puissance de p. Montrons que $Z(\mathrm{G}) \neq \{e_\mathrm{G}\}$.

Voir TD.

(4) Supposons désormais que G est non abélien d'ordre $8 = 2^3$.

a) Montrons que $Z(\mathrm{G}) \subset \mathrm{G}$ est un sous-groupe d'ordre 2 et que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Puisque $Z(\mathrm{G}) \neq \{e_\mathrm{G}\}$ et G n'est pas abélien d'ordre 8, $Z(\mathrm{G})$ est d'ordre 2 ou 4.

Si $|Z(\mathrm{G})| = 4$ alors ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est d'ordre 2 donc cyclique. D'après (2) le groupe G est abélien : contradiction.

Ainsi $Z(\mathrm{G})$ est d'ordre 2.

Pour la même raison ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est un groupe d'ordre 4 non cyclique. Par conséquent

$${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$$

b) Montrons que G contient au moins un élément d'ordre 4.

Le théorème de Lagrange assure qu'un élément de G est d'ordre 1, 2, 4 ou 8. Comme G n'est pas cyclique (d'ordre 8) il n'y a pas d'élément d'ordre 8 dans G. Si tous les éléments sont d'ordre divisant 2, le groupe G est abélien : contradiction. Le groupe G contient donc au moins un élément d'ordre 4.

c) Montrons que tout sous-groupe de G d'ordre 4 est distingué dans G.

Comme G est d'ordre 8 les sous-groupes d'ordre 4 de G sont d'indice 2 dans G. Par suite ils sont tous distingués dans G.

Soit $\mathrm{H} \subset \mathrm{G}$ un sous-groupe cyclique d'ordre 4 de G.

cas 1 : Il existe dans $\mathrm{G} \smallsetminus \mathrm{H}$ un élément d'ordre 2. Montrons alors que $\mathrm{G} = \langle \mathrm{H}, x \rangle$.

Soit $x \in \mathrm{G} \smallsetminus \mathrm{H}$ un élément d'ordre 2. Comme $x \notin \mathrm{H}$, la réunion disjointe

$$\mathrm{H} \sqcup x\mathrm{H} \subset \mathrm{G}$$

fournit un sous-ensemble d'ordre 8. Ainsi on a $\mathrm{G} = \mathrm{H} \sqcup x\mathrm{H} = \langle \mathrm{H}, x \rangle$.

Montrons que l'automorphisme

$$\mathrm{H} \to \mathrm{H} \qquad\qquad g \mapsto xgx^{-1}$$

est égal à $g \mapsto g^{-1}$.

Soit $h_0 \in \mathrm{H}$ un générateur. Puisque H est un sous-groupe distingué de G, xh_0x^{-1} appartient à H. De plus comme h_0 et xh_0x^{-1} ont le même prdre et comme H est cyclique d'ordre 4 engendré par h_0, on a alors ou bien $xh_0x^{-1} = h_0$, ou bien $xh_0x^{-1} = h_0^3 = h_0^{-1}$ (car h_0 et $h_0^{-1} = h_0^3$ sont les seuls deux éléments d'ordre 4 de H). Or $\mathrm{G} = \langle \mathrm{H}, x \rangle$ et comme G est non abélien, l'éventualité $xh_0x^{-1} = h_0$ est impossible. Par suite $xh_0x^{-1} = h_0^{-1}$. Puisque $h_0 \in \mathrm{H}$ est un générateur il s'ensuit que pour tout $g \in \mathrm{H}$ on a $xgx^{-1} = g^{-1}$.

En déduire que G est isomorphe au groupe diédral D_8.

Ainsi $\mathrm{G} = \langle \mathrm{H}, x \rangle = \langle h_0, x \rangle$ avec

$$h_0^4 = 1, \qquad x^2 = 1, \qquad h_0 x = x h_0^{-1}$$

Donc $\mathrm{G} \simeq \mathrm{D}_8$.

cas 2 : Tout élément de $\mathrm{G} \setminus \mathrm{H}$ est d'ordre 4. Montrons alors que G n'a qu'un seul élément d'ordre 2 et qu'il engendre $Z(\mathrm{G})$.

Notons par $i \in \mathrm{H}$ un générateur. Si tout élément de $\mathrm{G} \setminus \mathrm{H}$ est d'ordre 4 et comme $\mathrm{H} = \langle i \rangle$ est cyclique d'ordre 4, le seul élément d'ordre 2 de G est alors i^2 qui sera par la suite noté -1.

Comme il n'y a qu'un seul élément d'ordre 2 pour tout $g \in \mathrm{G}$ on a $g \cdot (-1) \cdot g^{-1}$, c'est-à-dire $-1 \in Z(\mathrm{G})$.

Soit $j \in \mathrm{G} \setminus \mathrm{H}$ qui est alors d'ordre 4. Comme j est d'ordre 4, j^2 est d'ordre 2. Par suite on a forcément $j^2 = -1$.

Posons ensuite $k = ij$. Comme $j \notin \mathrm{H} = \langle i \rangle$, on a $k = ij \neq 1$. De plus $k \neq -1$; sinon on aurait $i^2 = ij$ d'où $i = j$: contradiction. Par suite $k \in \mathrm{G}$ est d'ordre 4. Il en résulte que k^2 est d'ordre 2, par suite $k^2 = -1$. On note ensuite i^3 par $-i$, j^3 par $-j$ et k^3 par $-k$.

Reste à écrire la table de Cayley.