

Exercice 1.

Considérons la fonction

$$\varphi: \mathbb{Z} \rightarrow \mathbb{N}, \quad n \mapsto \begin{cases} 2n & \text{si } n \geq 0 \\ -2n - 1 & \text{si } n < 0. \end{cases}$$

On vérifie aisément que φ est bijective, ce qui montre que $|\mathbb{N}| = |\mathbb{Z}|$.

Alternativement, on peut exhiber des fonctions injectives $\mathbb{N} \hookrightarrow \mathbb{Z}$ et $\mathbb{Z} \hookrightarrow \mathbb{N}$ puis conclure en utilisant le théorème de Cantor-Schröder-Bernstein.

Exercice 2.

Définissons $\eta: G/H \rightarrow F$ par

$$\eta(gH) := \phi(g), \quad \forall g \in G.$$

On vérifie que η a les propriétés désirées :

1. **η est bien définie.** En effet, supposons que $gH = g'H$. Cela implique qu'il existe $h \in H$ tel que $g' = gh$. On a alors

$$\begin{aligned} \eta(g'H) = \phi(g') &= \phi(gh) \\ &\stackrel{\phi \text{ morphisme}}{=} \phi(g)\phi(h) \\ &\stackrel{H \subseteq \ker \phi}{=} \phi(g)e_H \\ &= \phi(g) \\ &= \eta(gH). \end{aligned}$$

2. **η est un morphisme.** En effet,

$$\begin{aligned} \eta(gH \cdot g'H) = \eta(gg'H) &= \phi(gg') \\ &\stackrel{\phi \text{ morphisme}}{=} \phi(g)\phi(g') \\ &= \eta(gH)\eta(g'H). \end{aligned}$$

3. **η est unique avec la propriété que $\eta \circ \xi = \phi$.** En effet, si $\eta': G/H \rightarrow F$ est une fonction quelconque qui satisfait $\eta' \circ \xi = \phi$, alors pour tout $g \in G$ on a

$$\eta'(gH) = \eta'(\xi(g)) = \phi(g),$$

donc la restriction $\eta'|_{\text{im}(\xi)}: \text{im}(\xi) \rightarrow F$ satisfait

$$\eta'|_{\text{im}(\xi)} = \eta|_{\text{im}(\xi)}.$$

Mais ξ est surjective, donc $\eta' = \eta$.

Exercice 3.

Pour $i = 1, 2, 3$, prenons $h_i \in H$ et $f_i \in F$. On a d'une part :

$$\begin{aligned} [(h_1, f_1)(h_2, f_2)](h_3, f_3) &= (h_1\phi_{f_1}(h_2), f_1f_2)(h_3, f_3) \\ &= (h_1\phi_{f_1}(h_2)\phi_{f_1f_2}(h_3), f_1f_2f_3). \end{aligned}$$

On a d'autre part :

$$\begin{aligned} (h_1, f_1)[(h_2, f_2)(h_3, f_3)] &= (h_1, f_1)(h_2\phi_{f_2}(h_3), f_2f_3) \\ &= (h_1\phi_{f_1}(h_2\phi_{f_2}(h_3)), f_1f_2f_3). \end{aligned}$$

Remarquons maintenant que

$$\begin{aligned} h_1\phi_{f_1}(h_2\phi_{f_2}(h_3)) &\stackrel{\phi_{f_1} \text{ morphisme}}{=} h_1\phi_{f_1}(h_2)\phi_{f_1}(\phi_{f_2}(h_3)) \\ &= h_1\phi_{f_1}(h_1)(\phi_{f_1} \circ \phi_{f_2})(h_3) \\ &\stackrel{\phi \text{ morphisme}}{=} h_1\phi_{f_1}(h_1)\phi_{f_1f_2}(h_3). \end{aligned}$$

Grâce à ces égalités, on trouve que

$$[(h_1, f_1)(h_2, f_2)](h_3, f_3) = (h_1, f_1)[(h_2, f_2)(h_3, f_3)],$$

et donc que la loi de groupe est associative.

Exercice 4.

Soit G un groupe abélien d'ordre p^2 non-cyclique. On va montrer que $G \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$.

Par le théorème de Lagrange, pour tout $x \in G$ on a $o(x) \in \{1, p, p^2\}$. Or G n'est pas cyclique, donc $o(x) \neq p^2$. Puisque $o(x) = 1$ si et seulement si pour $x = e_G$, on peut trouver $x \in G$ tel que $o(x) = p$. Prenons ensuite $y \in G \setminus \langle x \rangle$ (ce qui est possible puisque $|G| = p^2 > p = |\langle x \rangle|$). Puisque $y \neq e_G$, on a aussi $o(y) = p$.

Notons $X := \langle x \rangle, Y := \langle y \rangle$. Ces deux sous-groupes sont de cardinal p . On a ainsi $X \cong \mathbb{Z}/p\mathbb{Z} \cong Y$ par le Corollaire 3.5.37. Par le théorème de Lagrange, le cardinal de l'intersection $X \cap Y$ divise p . Cette intersection est donc soit triviale, soit égale à X et à Y ; mais $X \neq Y$ par construction, donc $X \cap Y = \{e\}$.

Puisque G est abélien, Y est automatiquement contenu dans le normalisateur de X . De plus, $|G| = |X| \cdot |Y|$. Par le Théorème 3.8.13, on en déduit donc

$$G \cong X \rtimes_{\alpha} Y, \quad \text{pour un certain } \alpha: Y \rightarrow \text{Aut}(X).$$

Par la Remarque 3.8.11, puisque G est abélien, le morphisme α est trivial, et donc

$$G \cong X \times Y \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

comme annoncé.

Exercice 5. 1. Puisque σ fixe exactement deux éléments, son support $\text{Supp}(\sigma)$ possède exactement 3 éléments. Si $\sigma = \sigma_1 \cdots \sigma_r$ est la décomposition en cycles disjoints, alors

$$\text{Supp}(\sigma) = \bigcup_{i=1}^r \text{Supp}(\sigma_i).$$

Comme $|\text{Supp}(\sigma_i)| \geq 2$, on en déduit que $r = 1$ et que σ est un 3-cycle.

2. La permutation σ est uniquement déterminée par les 2 éléments fixés, et le 3-cycle induit sur les autres 3 éléments. Il y a $\binom{5}{2} = 10$ possibilités de choisir 2 éléments distincts parmi $\{1, \dots, 5\}$; et les 3-cycles sur un ensemble $\{x, y, z\}$ sont les deux suivants :

$$x \rightarrow y \rightarrow z \rightarrow x, \quad x \rightarrow z \rightarrow y \rightarrow x.$$

Il y a donc $10 \cdot 2 = 20$ permutations de S_5 qui fixent exactement 2 éléments.

Exercice 6. 1. On $o(\sigma) = \text{ppmc}\{o(\sigma_1), \dots, o(\sigma_r)\}$. Voir le corrigé de l'Exercice 5 de la série 4.

2. Prenons $H \leq S_4$ tel que $|H| = 6 = 2 \cdot 3$. Par le Corollaire 3.8.18 (que l'on peut appliquer, puisque $(\mathbb{Z}/3\mathbb{Z})^\times$ est d'ordre 2, donc cyclique car engendré par l'élément non-trivial), on a $H \cong \mathbb{Z}/6\mathbb{Z}$ ou $H \cong D_6$. On va d'abord écarter le premier cas. En effet, si $H \cong \mathbb{Z}/6\mathbb{Z}$, alors H est cyclique. Donc il existe $\sigma \in S_4$ d'ordre 6 qui engendre H . Par le point précédent, on a alors que σ est soit un 6-cycle, soit un produit d'un 2-cycle et d'un 3-cycle disjoint. En particulier $|\text{Supp}(\sigma)| \geq 5$. Mais $\sigma \in S_4$, c'est une contradiction.

Ainsi $H \cong D_6$. Or $D_6 \cong S_3$ par la Remarque 3.6.10, donc $H \cong S_3$.

Exercice 7. 1. Il est clair que $F := \{e, -e\}$ est un sous-groupe d'ordre 2.

Soit $H \leq Q_8$ un sous-groupe et supposons qu'il existe $x \in H$ tel que $x \notin F$. Alors $x \in \{i, i^3, j, j^3, k, k^3\}$, et dans tous les cas on trouve $x^2 = -e$. Donc $F \subsetneq H$. Ceci montre que F est l'unique sous-groupe d'ordre 2, et que F est contenu dans tous les sous-groupes d'ordre 4.

2. Supposons par l'absurde qu'on puisse écrire $Q_8 \cong A \rtimes_\alpha B$, pour des groupes A, B non-triviaux et un homomorphisme $\alpha: B \rightarrow \text{Aut}(A)$. Puisque l'ensemble sous-jacent de $A \rtimes_\alpha B$ est le produit cartésien $A \times B$, on a $8 = |Q_8| = |A| \cdot |B|$. Comme A et B ne sont pas triviaux, on a $|A|, |B| \geq 2$. Donc l'un des deux groupes est d'ordre 2 et l'autre est d'ordre 4.

Par la Proposition 3.8.10, les sous-ensembles

$$A \times \{e_B\} \subset A \rtimes_\alpha B, \quad \{e_A\} \times B \subset A \rtimes_\alpha B$$

sont des sous-groupes, isomorphes à A et B respectivement. Il est clair que

$$(A \times \{e_B\}) \cap (\{e_A\} \times B) = \{e_{A \rtimes_\alpha B}\}.$$

Donc $A \rtimes_\alpha B$ possède un sous-groupe d'ordre 2 et un sous-groupe d'ordre 4, et le premier n'est pas inclus dans le second. Or cela n'est pas possible dans Q_8 , comme on l'a vu au point précédent.

On a obtenu une contradiction, ce qui signifie que Q_8 n'est pas un produit semi-direct non-trivial.

Exercice 8.

On prétend d'abord que $G \cong \mathbb{F}_2^{\oplus 2}$. En effet, on a

$$\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a+x \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix}$$

et il s'ensuit que la fonction

$$\varphi: \mathbb{F}_2^{\oplus 2} \longrightarrow G, \quad (x, y) \mapsto \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

est un isomorphisme. En particulier, le groupe G est 2-torsion.

Ecrivons $\sigma \in D_{10}$ le cycle d'ordre 5, $\tau \in D_{10}$ l'involution d'ordre 2, avec $D_{10} = \langle \sigma, \tau \rangle$. Prenons $f \in \text{Hom}(D_{10}, G)$. Alors $f(\sigma)^2 = e_G$ car G est 2-torsion, et $f(\sigma)^5 = e_G$ car $\sigma^5 = e_{D_{10}}$. Donc

$$e_G = f(\sigma)^5 = f(\sigma)^2 f(\sigma)^2 f(\sigma) = f(\sigma).$$

Donc $\langle \sigma \rangle \subseteq \ker f$ pour tout $f \in \text{Hom}(D_{10}, G)$. En particulier, par l'Exercice 2, on obtient une bijection

$$\text{Hom}(D_{10}, G) \xrightarrow{\sim} f \in \text{Hom}(D_{10}/\langle \sigma \rangle, G), \quad f \mapsto \bar{f}$$

où $\bar{f}$ est l'unique morphisme qui fait commuter le diagramme

$$\begin{array}{ccc} D_{10} & \xrightarrow{\text{quotient}} & D_{10}/\langle \sigma \rangle \\ & \searrow f & \swarrow \bar{f} \\ & G & \end{array}$$

Puisque $o(\sigma) = 5$, on a $|D_{10}/\langle \sigma \rangle| = 10/5 = 2$. Donc $D_{10}/\langle \sigma \rangle \cong \mathbb{Z}/2\mathbb{Z}$. On a vu en cours (et en série d'exercice) qu'il y a autant de morphismes $\mathbb{Z}/2\mathbb{Z} \rightarrow G$ qu'il y a d'éléments de 2-torsion dans G . Or G est 2-torsion, et donc

$$|\text{Hom}(D_{10}, G)| = |\text{Hom}(D_{10}/\langle \sigma \rangle, G)| = |\text{Hom}(\mathbb{Z}/2\mathbb{Z}, G)| = |G| = 4.$$

Exercice 9. 1. Prenons $f \in F$ et $h \in Z(G)$. Alors

$$fhf^{-1} = hff^{-1} = h.$$

Donc la fonction

$$\text{Ad}_f^{Z(G)}: Z(G) \rightarrow Z(G), \quad h \mapsto fhf^{-1} = h$$

est l'identité sur $\text{Ad}_f^{Z(G)}$. En particulier $\text{Ad}_F^{Z(G)}: F \rightarrow \text{Aut}(Z(G))$ est le morphisme trivial.

2. Supposons que $|G| = p^2$ et que $|Z(G)| = p$. Alors $Z(G) \subsetneq G$, et donc G n'est pas abélien. Prenons $x \in G \setminus Z(G)$; alors $o(x) \in \{p, p^2\}$, et puisque G n'est pas abélien il n'est pas cyclique, donc on a forcément $o(x) = p$. Posons $F := \langle x \rangle$.

L'intersection $I := F \cap Z(G)$ est un sous-groupe de F . Par le théorème de Lagrange, on a $|I| \in \{1, |F| = p\}$. Si $\{e_G\} \subsetneq I$, alors $|I| = p = |F|$ et donc $I = F$. Mais dans ce cas $x \in I \subseteq Z(G)$, contradiction avec le choix de x . Donc $I = \{e_G\}$.

De plus $N_G(Z(G)) = G$ car $Z(G)$ est normal, et donc $F \subset N_G(Z(G))$.

Finalement $|G| = p^2 = p \cdot p = |F| \cdot |Z(G)|$.

On peut ainsi appliquer le Théorème 3.8.13 pour trouver

$$G \cong Z(G) \rtimes_{\text{Ad}_F^{Z(G)}} F.$$

Or on a vu au premier point que $\text{Ad}_F^{Z(G)}$ est trivial, et donc

$$G \cong Z(G) \times F.$$

Les groupes $Z(G)$ et F sont d'ordres p , donc abéliens (voir le Corollaire 3.5.37), et donc G est abélien. Mais on a vu plus haut que G ne pouvait être abélien, on obtient donc une contradiction.

3. Considérons le groupe

$$U(3, \mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{F}_p \right\}$$

On vérifie aisément que

$$Z(U(3, \mathbb{F}_p)) = \left\{ \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid y \in \mathbb{F}_p \right\}.$$

Ainsi $|U(3, \mathbb{F}_p)| = p^3$ et $|Z(U(3, \mathbb{F}_p))| = p$.