EXERCICES SUR LES GROUPES

Exercice 1. Groupes diédraux. Soit P_n un polygone régulier du plan à n cotés (représenté par exemple par les racines n-ièmes de l'unité dans le plan complexe). On note D_n le groupe (appelé *n-ième groupe diédral*) des isométries *directes et indirectes* du plan préservant P_n.

(1) Montrer que D_n est d'ordre $2n$.

(2) Montrer que le sous-groupe D_n^+ constitué des isométries directes est cyclique d'ordre n : $D_n^+ \simeq \mathbb{Z}/n\mathbb{Z}$.

(3) Dresser la listes des classes de conjugaison dans D_n.

Exercice 2. Groupe des quaternions. On note $\mathbb{H}_8$ le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ (appelé *groupe des quaternions*) engendré par les trois matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Calculer l'ordre de $\mathbb{H}_8$, exhiber ses sous-groupes, ses sous-groupes distingués et ses quotients. Est-il isomorphe au groupe diédral D_4 ? Quel est le rapport avec le corps non commutatif des quaternions ?

Exercice 3. Groupes d'ordre 6. Montrer de façon élémentaire (aucun argument sophistiqué au-delà du théorème de Lagrange) que tout groupe d'ordre 6 non cyclique est isomorphe au groupe symétrique S_3. [Indication : on pourra montrer qu'un tel groupe contient un couple d'éléments d'ordre 2 et 3 ne commutant pas.]

Exercice 4. Signification de l'opération de conjugaison sur des exemples.

(1) Soit p un projecteur d'un sous-espace vectoriel F d'un espace vectoriel E sur un supplémentaire G, et $f \in \mathrm{GL}(E)$. Caractériser le conjugué $f \circ p \circ f^{-1}$.

(2) Même question pour une symétrie s par rapport à un sous-espace vectoriel F d'un espace vectoriel E, parallèlement à un supplémentaire G.

(3) Soit $n \in \mathbb{N}$, $\sigma \in S_n$ et $(a_1 \cdots a_k)$ un k-cycle de S_n. Calculer $\sigma(a_1 \cdots a_k)\sigma^{-1}$.

(4) soit G un groupe, E et F deux sous-ensembles de G, et $\sigma \in G$. Soit g un élément de G tel que $gE \subset F$. Quelle propriété vérifie son conjugué $\sigma g \sigma^{-1}$?

(5) Inventer des exos similaires...

Exercice 5. Exposant d'un groupe abélien et application.

(1) Soit G abélien et a, b d'ordres finis premiers entre eux. Montrer que ordre ab = ordre $a \cdot$ ordre b.

(2) Soit G un groupe abélien fini, et soit m le maximum parmi les ordres des éléments de G. Montrer que l'ordre de tout élément de G divise m. (m est appelé l'*exposant* de G).

(3) Soit $\mathbf{k}$ un corps, et $G \subset \mathbf{k}^*$ un sous-groupe fini du groupe multiplicatif $\mathbf{k}^*$. Montrer que G est cyclique. [Indication : on pourra considérer les racines du polynôme $X^m - 1 \in \mathbf{k}[X]$, où m est l'exposant de G.]

(4) Qu'en déduire pour le groupe $(\mathbb{Z}/p\mathbb{Z})^*$, où p est premier ? Et pour le groupe $\mathbb{C}^*$?

Exercice 6. Groupes abéliens infinis.

(1) Montrer que $(\mathbb{Z}, +)$ n'est pas isomorphe à $(\mathbb{Z}^2, +)$, et que $(\mathbb{Q}, +)$ n'est pas isomorphe à $(\mathbb{Q}^2, +)$.

(2) Montrer que le groupe abélien $(\mathbb{Q}, +)$ n'est pas de type fini.

(3) Soit G un sous-groupe de $(\mathbb{C}^*, \cdot)$ dont chaque élément est d'ordre fini. Est-il vrai que G est forcément fini ? et de type fini ?

(4) Montrer que les sous-groupes de $(\mathbb{R}, +)$ sont soit de la forme $a\mathbb{Z}$, soit denses.

(5) Que dire de $\mathbb{Z}[\sqrt{2}]$? Que dire d'une fonction réelle f continue, admettant 1 et $\sqrt{2}$ pour périodes ?

(6) Que dire des sous-groupes de $(\mathbb{C}, +)$?

Exercice 7. Une action bien utile. Soit G un groupe, et H un sous-groupe de G *d'indice fini* n. On fait opérer G par "translation" sur l'ensemble des classes à gauche G/H, c'est-à dire $g \cdot \sigma H := (g\sigma)H$ pour tout $\sigma \in G$.

(1) (La clé de nombreux exos) Montrer que le noyau du morphisme $\rho : G \to \mathrm{Bij}(G/H) \simeq S_n$ associé à cette action est le plus gros sous-groupe de H distingué dans G, et que de plus il est d'indice fini dans G.

(2) Application 1. Montrer qu'un groupe non-abélien d'ordre 6 est isomorphe à S_3.

(3) Application 2. Soit G un groupe infini, possédant deux sous-groupes d'indice fini H et K. Montrer qu'il y a un sous-groupe distingué dans G et d'indice fini, contenu dans H et dans K.

(4) Application 3. Soit G un groupe fini, et p le plus petit facteur premier de son ordre. Soit H un sous-groupe d'indice p dans G. Montrer que H est distingué dans G. [N.B. Le cas $p = 2$ est bien plus élémentaire...]

Exercice 8. Centre d'un groupe ; groupes d'ordre p^2. Si G est un groupe, on peut faire agir G par conjugaison sur lui même.

(1) Montrer que le centre $Z(G)$ de G est constitué des éléments dont l'orbite est réduite à un point.

(2) (*i*) Si G est un p-groupe (p premier), montrer que le centre de G n'est pas réduit à $\{1\}$.

(*ii*) Soit G un groupe tel que $G/Z(G)$ soit monogène. Montrer qu'alors G est abélien (et donc en particulier le groupe monogène $G/Z(G)$ était en fait trivial).

(*iii*) Montrer qu'un groupe d'ordre p^2 est nécessairement abélien.

(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Exercice 9. p-Sylow dans un sous-groupe. Soit G un groupe fini d'ordre $|G| = p^a m$ avec p premier et $p \wedge m = 1$. Soit $S \subset G$ un p-Sylow (c'est-à-dire de cardinal p^a), et $H \subset G$ un sous-groupe. Montrer qu'il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H. [Indication : faire agir G sur l'ensemble des classes à gauche de G modulo S, et montrer que l'une des orbites est de cardinal non multiple de p.]

Exercice 10. Existence des p-Sylow.

(1) Soit $\mathbf{k}$ un corps, et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{k})$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments, où p est premier. Montrer que le groupe des matrices triangulaires supérieures avec 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

(3) Soit G un groupe fini et p un diviseur premier de $|G|$. Montrer à l'aide de l'exercice 9 que G admet un p-Sylow.

Exercice 11. Calculs dans les groupes symétriques. Écrire la décomposition en produit de cycles à supports disjoints, et calculer l'ordre, la signature et la puissance 10ème de

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 2 & 9 & 5 & 6 & 1 & 7 & 3 \end{pmatrix}, \quad \text{de } (35)(142)(134)(45)(12345)$$

$$\text{et de } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 7 & 1 & 3 & 8 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 2 & 4 & 5 & 7 & 3 & 6 \end{pmatrix}$$

Exercice 12. Quelques propriétés du groupe symétrique. Soit $n \geqslant 2$.

(1) Montrer que A_n est le seul sous-groupe d'indice 2 de S_n.

(2) On admet que A_n est simple pour $n \geqslant 5$. Montrer que pour $n \geqslant 5$, les seuls sous-groupes distingués de S_n sont $\{\mathrm{id}\}$, A_n et S_n. Que devient le résultat pour $n = 2, 3$ ou 4 ?

(3) Soit H un sous-groupe de S_n, d'indice n avec $n \geqslant 3$. L'action de S_n sur S_n/H (ensemble des classes à gauche) par translation induit un morphisme φ de S_n dans $\mathrm{Bij}(S_n/H)$.

(*i*) Montrer que φ est injectif.

(*ii*) En déduire que $H \simeq S_{n-1}$.

Exercice 13. Isomorphismes exceptionnels et interprétation. Soit p un nombre premier. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments. On fait agir $\mathrm{GL}_2(\mathbb{F}_p)$ sur l'ensemble des droites vectorielles (au nombre de $p+1$, à vérifier !) du plan $\mathbb{F}_p^2$. Il en résulte un morphisme

$$\rho : \mathrm{GL}_2(\mathbb{F}_p) \longrightarrow S_{p+1}.$$

(1) Montrer que le noyau de ρ est constitué des homothéties non nulles, d'où une injection

$$\mathrm{PGL}_2(\mathbb{F}_p) := \mathrm{GL}_2(\mathbb{F}_p)/\text{homothéties non nulles} \hookrightarrow S_{p+1}.$$

(2) On se propose de voir que, lorsque p est petit, cela donne lieu à des isomorphismes "exceptionnels" :
   (*i*) Montrer que $\sharp\,\mathrm{GL}_2(\mathbb{F}_p) = (p^2-1)(p^2-p)$, et en déduire $\sharp\,\mathrm{PGL}_2(\mathbb{F}_p)$.
   (*ii*) Montrer que $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$.
   (*iii*) Montrer que $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$
   (*iv*) Soit $\mathbb{F}_4$ un corps fini à 4 éléments (par exemple $\mathbb{F}_4 = \mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$). Montrer que $\mathrm{PGL}_2(\mathbb{F}_4) \simeq A_5$.
   (*v*) Montrer que $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$.

(3) Interprétation : montrer que $\mathrm{PGL}_2(\mathbf{k})$ agit simplement 3-transitivement sur les droites vectorielles de $\mathbf{k}^2$, puis interpréter les isomorphismes exceptionnels.

Exercice 14. Groupes des isométries du tétraèdre et du cube.

(1) Montrer, en le faisant opérer sur les quatre sommets, que le groupe des isométries *directes* du tétraèdre est isomorphe au groupe alterné A_4.

(2) Montrer que le groupe des isométries (directes ou indirectes) d'un tétraèdre régulier est isomorphe à un produit semi-direct $A_4 \rtimes \{\pm 1\}$. (voir exercice 21 pour la définition.)

(3) Montrer, en le faisant opérer sur les quatre grandes diagonales, que le groupe des isométries *directes* du cube est isomorphe au groupe symétrique S_4.

(4) On considère un carré "équateur" du cube, et le sous-groupe S des isométries directes du cube stabilisant (i.e. laissant globalement fixe) cet équateur. Montrer que $S = D_4$, puis observer sur ce cas les conclusions du théorème de Sylow.

(5) Adapter la question précédente pour décrire les 2-Sylow (= sous-groupes d'ordre 4) de Isom^+(tétraèdre)...

(6) ... puis (plus facile) les 3-Sylow (= sous-groupes d'ordre 3) de Isom^+(tétraèdre) et Isom^+(cube).

Exercice 15. Groupes symétriques et alternés de petits ordres.

(1) Pour chacun des groupes suivants, dresser la liste des classes de conjugaison :

$$S_2, \qquad A_2, \qquad S_3, \qquad A_3, \qquad S_4, \qquad A_4, \qquad A_5.$$

(2) Interpréter géométriquement les résultats pour A_4 et A_5 en utilisant les isomorphismes avec les groupes de rotations préservant un tétraèdre (resp. un icosaèdre) régulier.

(3) Donner un exemple de groupe G, et de deux sous-groupes $H \subset K \subset G$, tels que H soit distingué dans K, que K soit distingué dans G, mais tels que H ne soit pas distingué dans G.

Exercice 16. Simplicité de A_5. Montrer à l'aide du théorème de Lagrange et de la liste des cardinaux des classes de conjugaison obtenue dans l'exercice 15 que le groupe alterné A_5 est simple.

Exercice 17. Propriétés du groupe alterné.

(1) Montrer que le groupe alterné A_n est engendré par les 3-cycles.

(2) Montrer que pour $n \geqslant 5$, les 3-cycles de A_n sont deux à deux conjugués.

Exercice 18. Générateurs de GL_n. On dit qu'une matrice $M \in \mathrm{GL}_n(\mathbf{k})$ est une *dilatation* de rapport $\lambda \in \mathbf{k}^*$ si M est conjugué à la matrice diagonale $\mathrm{diag}(\lambda, 1, \ldots, 1)$. Montrer que les dilatations engendrent $\mathrm{GL}_n(\mathbf{k})$, pour tout $n \geqslant 2$ et tout corps $\mathbf{k} \neq \mathbb{F}_2$. [Indication : on peut admettre, ou redémontrer, que les transvections engendrent $\mathrm{SL}_n(\mathbf{k})$, puis montrer que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est un produit de deux dilatations.]

Exercice 19. Automorphismes de certains groupes abéliens non cyclique. Soit p un nombre premier.

(1) Montrer qu'une application f de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ dans lui même est un morphisme de groupe si, et seulement si, c'est un morphisme de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

(2) En déduire la structure du groupe $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$ en terme de groupe linéaire.

Exercice 20. Produits directs internes.

(1) Soit G un groupe, et H, K deux sous groupes de G. On note $HK := \{hk \mid h \in H, k \in K\}$. Montrer que si au moins un des sous-groupes H ou K est distingué dans G alors HK est un sous-groupe de G. (La réciproque est-elle vraie ?)

(2) Dans la situation ci-dessus, on suppose que :

$$H \cap K = \{1\}, \qquad HK = G, \qquad H \text{ et } K \text{ sont distingués dans } G.$$

Montrer qu'alors $(h, k) \mapsto hk$ est un isomorphisme de $H \times K$ dans G.

(3) Donner un énoncé réciproque.

(4) Application : On considère le groupe G des isométries de l'espace euclidien $\mathbb{R}^3$ préservant un cube, et son sous-groupe G^+ constitué des isométries directes. Montrer que $G \simeq G^+ \times \{\pm 1\}$.

(5) Le groupe des isométries du plan euclidien préservant un carré est-il un produit direct de deux sous-groupes non triviaux ?

Exercice 21. Produits semi-directs internes. Soit G un groupe, et H, K deux sous groupes de G. On dit que $G = H \ltimes K$ est le *produit semi-direct* de H et K si $K \triangleleft G$, $HK = G$ et $H \cap K = \{1\}$.

(1) Si $G = H \ltimes K$, montrer que $H \simeq G/K$.

Montrer les isomorphismes suivants :

(2) $S_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

(3) Si $\mathbf{k}$ est un corps commutatif, $\mathrm{GL}_n(\mathbf{k}) \simeq \mathrm{SL}_n(\mathbf{k}) \rtimes \mathbf{k}^*$, où $\mathrm{SL}_n(\mathbf{k})$ désigne le groupe des matrices de déterminant 1.

(4) Si P est un polygone régulier à n côtés, et $\mathrm{Isom}^+(P)$ est le groupe des rotations préservant P, $\mathrm{Isom}(P) \simeq \mathrm{Isom}^+(P) \rtimes \mathbb{Z}/2\mathbb{Z}$. (Ici $\mathrm{Isom}(P)$ est le groupe diédral D_n de l'exercice 1.)

(5) Donner une structure de produit semi-direct pour le groupe des automorphismes d'un espace affine.

Exercice 22. Automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

(1) Soit $n \geqslant 1$ et $k \in \mathbb{Z}$ deux entiers. Montrer l'équivalence des assertions suivantes :

(*i*) $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ engendre $\mathbb{Z}/n\mathbb{Z}$.

(*ii*) n et k sont premiers entre eux.

(*iii*) $\bar{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(2) Montrer que $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \simeq ((\mathbb{Z}/n\mathbb{Z})^*, \times)$.

Exercice 23. Automorphismes intérieurs et centre d'un groupe. Montrer que le sous-groupe $\mathrm{Int}(G)$ des automorphisme intérieurs de G est un sous-groupe distingué du groupe $\mathrm{Aut}(G)$, et que $\mathrm{Int}(G) \simeq G/Z(G)$, où $Z(G)$ est le centre de G.

Exercice 24. Groupes abéliens d'ordre donné. Donner la liste des groupes abéliens d'ordre 72 à isomorphismes près, sous forme "facteurs invariants" et sous forme "facteurs élémentaires".

Exercice 25. Un théorème de simplification. Soit G, H, G', H' des groupes finis, tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$. On se propose de montrer que $H \simeq H'$.

(1) Montrer en donnant un contre-exemple que le résultat est faux pour des groupes infinis.

Étant donnés deux groupes finis G_1, G_2, notons $m(G_1, G_2) \geqslant 1$ le nombre de morphismes de G_1 vers G_2, et $i(G_1, G_2) \geqslant 0$ le nombre de morphismes injectifs.

(2) Pour tous groupes finis G_1, G_2, montrer que $m(G_1, G_2) = \sum_{N \triangleleft G_1} i(G_1/N, G_2)$.

(3) Pour tout groupe fini F, montrer que $m(F, H) = m(F, H')$, puis $i(F, H) = i(F, H')$, et conclure.

Exercice 26. Deux groupes non isomorphes de cardinal 24.

(1) Montrer que $\mathrm{SL}_2(\mathbb{F}_3)$ et $\mathrm{PGL}_2(\mathbb{F}_3)$ sont tous deux de cardinal 24.

(2) Montrer que $\mathrm{SL}_2(\mathbb{F}_3)$ admet un sous-groupe d'ordre 8 isomorphe à $\mathbb{H}_8$.

(3) En déduire que $\mathrm{SL}_2(\mathbb{F}_3)$ et $\mathrm{PGL}_2(\mathbb{F}_3)$ ne sont pas isomorphes.

Exercice 27. Un groupe d'ordre pq. Soient $p < q$ deux nombres premiers, tel que p divise $q - 1$. Donner un exemple de groupe non-abélien G d'ordre pq, constitué de matrices triangulaires dans $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$.

Solution de l'exercice 1

On note O le centre du polygone.

(1) Soit AB et CD deux arêtes du polygone. Il existe une rotation qui envoie l'arête AB sur l'arête non orientée CD. En composant éventuellement par la symétrie d'axe la médiatrice de CD, on obtient un élément $f \in D_n$ tel que $f(A) = C$ et $f(B) = D$. De plus f est entièrement déterminé par cette propriété, car une application linéaire de $\mathbb{R}^2$ est déterminée par l'image d'une base (ici les vecteurs OA et OB forment une base). Comme P_n compte $2n$ arêtes orientées distinctes (n arêtes, chacune avec 2 orientations possibles), on obtient $\text{ordre}(D_n) = 2n$.

(2) Le groupe engendré par la rotation r de centre O et d'angle $2\pi/n$ est cyclique d'ordre n. De plus toute symétrie d'axe passant par un sommet et par O est un élément de $D_n \setminus D_n^+$. Donc D_n^+ est un sous-groupe strict de D_n de cardinal au moins n, par Lagrange on en déduit qu'il est de cardinal exactement n, et donc $D_n^+ = \langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

(3)
- Cas n impair.
  Pour chacun des n couples de sommet et milieu d'arête opposée on a un axe et une symétrie associés : ces n symétries forment une classe de conjugaison.
  Deux rotations sont conjugués ssi elles ont même angles orienté, on a donc une classe singleton pour l'identité, et $(n-1)/2$ classes de paires de rotations.
- Cas n pair.
  On a deux classes de conjugaison de $n/2$ symétries, celles d'axe reliant deux sommets opposés, et celles d'axe reliant les milieux de côtés opposés. Outre l'identité, on a également la rotation d'angle π (que l'on peut aussi voir comme une symétrie centrale) qui commutent avec tous les éléments de D_n : cela donne deux classes de conjugaison singleton. On a ensuite $(n-2)/2$ classes de paires de rotations comme précédemment.

Solution de l'exercice 2

On vérifie que

$$I^2 = J^2 = K^2 = -\,\mathrm{id} \text{ et } IJ = K.$$

On en déduit que le groupe des quaternions est

$$\mathbb{H}_8 = \{\mathrm{id}, -\mathrm{id}, I, -I, J, -J, K, -K\}$$

Les sous-groupes propres sont d'ordre 2 ou 4 par Lagrange. Il y a un seul sous-groupes d'ordre 2 : $\langle -\mathrm{id} \rangle$, et trois sous-groupes d'ordre 4 : $\langle I \rangle$, $\langle J \rangle$, $\langle K \rangle$.
Tous les sous-groupes sont distingués (fait rarissime !).
Le groupe diédral D_4 compte 5 éléments d'ordre 2, donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.
NB :

(1) On peut montrer que D_4 et $\mathbb{H}_8$ sont les seuls groupes non-abéliens d'ordre 8 à isomorphismes près. Les abéliens sont $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, $\mathbb{Z}/2 \times \mathbb{Z}/4$ et $\mathbb{Z}/8$.

(2) $\mathbb{H}_8$ n'est pas cyclique, par contre il suffit de deux éléments pour l'engendrer, par exemple $\mathbb{H}_8 = \langle I, J \rangle$.

(3) le corps des quaternions s'identifie aux matrices de la forme

$$\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}, a, b \in \mathbb{C},$$

le groupe $\mathbb{H}_8$ correspond aux intersections des 4 axes de coordonnées canoniques avec la sphère unité.

A noter que les notations I, J, K dans cet énoncé sont peut-être un peu exotiques, il semble plus usuel d'utiliser

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

mais alors la relation devient $IJ = -K$...

Solution de l'exercice 3

Soit G un groupe d'ordre 6 non cyclique, et $g \in G$ distinct de l'élément neutre. Par Lagrange, et comme on suppose G non cyclique, l'ordre de g est 2 ou 3. G ne peut pas contenir deux éléments a, b d'ordre 2 tel que le produit ab soit aussi d'ordre 2, car alors $\{1, a, b, ab\}$ serait un sous-groupe, contradiction avec Lagrange. Donc G contient au moins un élément d'ordre 3, et comme les éléments d'ordre 3 arrivent par paire g, g^{-1}, il y en a au plus 4 dans G. Bilan : G contient un élément τ d'ordre 2, et un élément γ d'ordre 3. On a $G = \langle \tau, \gamma \rangle$, par

Lagrange à nouveau. Les éléments τ et γ ne commutent pas, sinon $\tau\gamma$ serait d'ordre $\mathrm{PPCM}(2,3)=6$ et on a exclu ce cas. Donc $\gamma\tau\gamma^{-1}$ est d'ordre 2 et distinct de τ, donc il y a exactement 2 éléments d'ordre 3 dans G qui sont τ et τ^{-1} (plus la place pour deux autres...). Finalement $\sigma\tau\sigma=\tau^{-1}$ (seul élément d'ordre 3 distinct de τ), et cette identité permet de reconstruire entièrement la table de G, qui coïncide donc avec celle de S_3, via l'isomorphisme $\varphi(\tau)=(12)$ et $\varphi(\gamma)=(123)$.
Autre façon de conclure : faire agir G sur les 3 éléments d'ordre 2, cela donne un morphisme $G\to S_3$ dont on vérifie qu'il est injectif, et donc par égalité des cardinaux c'est un isomorphisme.
Encore une autre variante : voir exercice 7(2).
NB : il convient de savoir aussi démontrer de façon élémentaire qu'il n'y a que deux groupes d'ordre 4 à isomorphisme près, qui sont $\mathbb{Z}/4$ et $\mathbb{Z}/2\times\mathbb{Z}/2$ (c'est en fait plus facile).

Solution de l'exercice 4

(1) $f\circ p\circ f^{-1}$ est le projecteur du sous-espace $f(F)$ sur le supplémentaire $f(G)$.

(2) $f\circ s\circ f^{-1}$ est la symétrie par rapport au sous-espace $f(F)$, parallèlement au supplémentaire $f(G)$.

(3) $\sigma(a_1\cdots a_k)\sigma^{-1}$ est le k-cycle $(\sigma(a_1)\cdots\sigma(a_k))$.

(4) $(\sigma g\sigma^{-1})\sigma(E)\subset\sigma(F)$.

(5) Par exemple, dans $\mathbb{R}^2$, que donne le conjugué d'une translation par une rotation ? Et le conjugué d'une rotation par une translation ? Et une rotation par un élément quelconque de $\mathrm{GL}_2(\mathbb{R})$ (piège !) ?

Solution de l'exercice 5

(1) Notons $m=$ ordre a, $n=$ ordre b. On a $(ab)^{mn}=(a^m)^n(b^n)^m=1$, donc mn est un multiple de $d=\mathrm{ordre}(ab)$.

Par ailleurs on a $(ab)^d=1$. Alors $a^d=b^{-d}$ sont de même ordre p divisant à la fois m et n (car $a^d\in\langle a\rangle$ et $b^{-d}\in\langle b\rangle$), donc $p=1$. Autrement dit $a^d=b^{-d}=1$ (dans un groupe le neutre est l'unique élément d'ordre 1). Donc d est un multiple commun de $m=$ ordre a et $n=$ ordre b, et donc un multiple de $\mathrm{PPCM}(m,n)=mn$. On conclut $d=mn$.

(2) Soit $x\in G$ réalisant l'ordre maximal m, et supposons qu'il existe $y\in G$ dont l'ordre q ne divise pas m. Ceci implique qu'il existe un premier p et des entiers $b>a$ tels que

$$m=p^a m' \quad\text{et}\quad q=p^b q',$$

avec m',n' premiers avec p. Alors par le point précédent $\mathrm{ordre}(y^{q'}x^{p^a})=p^bm'>m$, absurde.

(3) Par le point précédent tous les éléments de G sont des racines de X^m-1. Mais un polynôme de degré m sur un corps a au plus m racines, et les m éléments du groupe $\langle x\rangle$ fournissent déjà m racines. Donc ce sont les seules et $G=\langle x\rangle$ est cyclique.

(4) Pour tout premier p le groupe $(\mathbb{Z}/p)^*$ est cyclique. Par exemple $(\mathbb{Z}/7)^*$ est cyclique d'ordre 6, on pourra vérifier que $\bar{5}$ est un générateur mais pas $\bar{2}$.

Tout sous-groupe fini de $\mathbb{C}^*$ est un groupe cyclique engendré par une racine de l'unité.

Solution de l'exercice 6

(1) Soit $\varphi\colon\mathbb{Z}\to\mathbb{Z}^2$ un morphisme, et $(a,b)=\varphi(1)$. Alors pour tout $n\in\mathbb{Z}$ on a $\varphi(n)=(na,nb)$, donc l'image de φ est contenu dans une droite et φ n'est pas surjective.

Pour tout $a/b,c/d\in\mathbb{Q}\setminus\{0\}$ il existe $m,n\in\mathbb{Z}\setminus\{0\}$ tel que (poser $m=-bc,n=ad$)

$$m\frac{a}{b}+n\frac{c}{d}=0,$$

mais cette propriété n'est pas vrai dans $\mathbb{Q}^2$ (prendre $(1,0)$ et $(0,1)$...), donc $\mathbb{Q}$ et $\mathbb{Q}^2$ ne sont pas isomorphes.

(2) Soit $G=\langle\frac{a_1}{b_1},\dots,\frac{a_s}{b_s}\rangle$ un sous-groupe de type fini dans $\mathbb{Q}$. Alors tout élément de G peut s'écrire comme une fraction avec dénominateur égal au produit des b_i. En particulier G ne peut pas être égal à $\mathbb{Q}$ tout entier.

(3) Le groupe de toutes les racines de l'unité donne un contre-exemple aux deux assertions.

(4) Soit G un sous-groupe de $\mathbb{R}$, que l'on peut supposer non trivial (sinon $G=0\mathbb{Z}$ et il n'y a rien à montrer). On pose $a=\inf\{x\in G\mid x>0\}$. Si $a=0$, on montre que G est dense dans $\mathbb{R}$, et si $a>0$, on montre que $G=a\mathbb{Z}$.

Détail pour le cas $a = 0$: on considère $I =]x, x + \varepsilon[$ un intervalle ouvert de diamètre ε, on veut montrer que I contient un élément de G. Par hypothèse il existe $y \in]0, \varepsilon/2[$, et l'un des multiples ny, $n \in \mathbb{N}$ convient.

Détail pour le cas $a > 0$: Dans ce cas l'inf est atteint, c'est-à-dire $a \in G$. Soit $x \in G$, on veut montrer que $x \in a\mathbb{Z}$. On écrit $x = na + r$ avec n entier et $0 \leqslant r < a$. Mais alors $r = x - na \in G$, donc est nul par minimalité de a.

(5) Si le groupe $\mathbb{Z}[\sqrt{2}]$ était de la forme $a\mathbb{Z}$, alors 1 et $\sqrt{2}$ seraient tous deux multiples entiers de a, donc a, puis $\sqrt{2}$, seraient des rationnels : absurde.

Le groupe $\mathbb{Z}[\sqrt{2}]$ est donc dense dans $\mathbb{R}$, et toute fonction continue admettant 1 et $\sqrt{2}$ pour périodes est constante.

(6) Six possibilités pour un sous-groupe G de $\mathbb{C}$: trivial, isomorphe à $\mathbb{Z}$, isomorphe à $\mathbb{Z}^2$, dense dans une droite, produit direct dense dans une droite $\times$ discret dans une droite, dense dans $\mathbb{C}$.

Détails : soit $G \subset \mathbb{C}$ un sous-groupe additif, on considère V le plus petit sous-espace vectoriel (réel) contenant G. On a $V = \{0\}$ ssi $G = \{0\}$. Si V est une droite, alors V est isomorphe à $\mathbb{R}$ et on est ramené à la question (4). Reste le cas $V = \mathbb{C}$. Supposons G non dense dans $\mathbb{C}$.

S'il existe des éléments de G arbitrairement proches de 0, alors ils sont tous sur une même droite D (si on a des bases formées d'éléments de G arbirairement petits, G est dense). Soit $z \in G \setminus D$ de module minimal. Alors $G = D \oplus z\mathbb{Z}$.

Enfin s'il existe une boule autour de 0 qui ne contient aucun autre élément de G, alors on prend $z_1 \in G \setminus \{0\}$ de module minimal, et $z_2 \in G \setminus z_1\mathbb{Z}$ de module minimal, et $G = z_1\mathbb{Z} + z_2\mathbb{Z}$.

Solution de l'exercice 7

(1) $g \in \operatorname{Ker}\rho$ ssi pour toute classe σH on a $(g\sigma)H = \sigma H$, ce qui équivaut à $\sigma^{-1}g\sigma \in H$, ou encore $g \in \sigma H\sigma^{-1}$. On a donc

$$\operatorname{Ker}\rho = \bigcap_{\sigma \in G} \sigma H \sigma^{-1},$$

et tout sous-groupe distingué $K \lhd G$ inclu dans H est inclu dans cette intersection, puisque $K = \sigma K \sigma^{-1} \subset \sigma H \sigma^{-1}$ pour tout $\sigma \in G$.

Puisque $G/\operatorname{Ker}\rho \simeq \rho(G)$, l'indice de $\operatorname{Ker}\rho$ est l'ordre de l'image de ρ, qui est d'ordre fini puisque sous-groupe du groupe fini S_n.

(2) On reprend le début de la solution de l'exercice 3, pour obtenir l'existence d'un élément τ d'ordre 2, et on pose $H = \langle\tau\rangle$ qui est donc d'indice 3. Comme τ ne commute pas avec au moins un élément γ d'ordre 3, on obtient $\operatorname{Ker}\rho = H \cap \gamma H \gamma^{-1} = \{\mathrm{id}\}$. Ainsi ρ est un morphisme injectif de G vers S_3, et donc un isomorphisme par égalité des cardinaux.

(3) Il suffit de prendre l'intersection des deux sous-groupes distingués d'indice fini associés respectivement à H et K.

(4) La restriction de ρ à H donne un morphisme $\rho|_H \colon H \to S_p$, puis, en oubliant la classe $\mathrm{id}\, H$ qui est fixée par l'action de tout $h \in H$, un morphisme $\rho|_H \colon H \to S_{p-1}$. Soit K son noyau. L'indice $[H : K]$ d'une part est égal à l'ordre de l'image de $\rho|_H$ donc divise $(p-1)!$, d'autre part il divise l'ordre de H et donc tous ses facteurs premiers sont $\geqslant p$. On en déduit que $[H : K] = 1$, autrement dit $H = \operatorname{Ker}\rho|_H = \operatorname{Ker}\rho$ est distingué dans G.

Solution de l'exercice 8

(1) C'est la définition du centre :

$$Z(G) = \{x \in G \mid gxg^{-1} = x \text{ pour tout } g \in G\}.$$

(2) (*i*) Notons Ω_i, $i \in I$ les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|G|$ on obtient que chaque $|\Omega_i|$ est une puissance de p (non égale à 1). En écrivant G comme une union disjointe d'orbites on obtient

$$|G| = |Z(G)| + \sum_i |\Omega_i|$$

et en réduisant modulo p :

$$0 \equiv |Z(G)| \mod p.$$

Ceci montre que $|Z(G)| \neq 1$.

(*ii*) Par hypothèse, il existe $a \in G$ dont la classe $\bar{a} \in G/Z(G)$ engendre $G/Z(G)$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(G)$, et G est commutatif car

$$a^k h \cdot a^{k'} h' = a^{k+k'} hh' = a^{k+k'} h'h = a^{k'} h' a^k h.$$

(Une autre façon de terminer est de dire que a commute avec tout élément de la forme $a^k h$, et donc $a \in Z(G)$, et $G/Z(G)$ est trivial).

(*iii*) On sait que le centre $Z(G)$ est non trivial, il est donc d'ordre p ou p^2. Si l'ordre est p^2, on a $G = Z(G)$ et G est abélien. Si l'ordre est p, alors $G/Z(G)$ serait d'ordre p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$, c'est impossible par la question précédente.

(3) Chacun des coefficients $*$ est un élément arbitraire de $\mathbb{F}_p$, d'où p^3 choix possibles. Il suffit ensuite de constater que

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas (calculer le coefficient en haut à droite).

Solution de l'exercice 9

On note comme ci-dessus $|G| = p^a m$, et de même $|H| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Noter que $g' \in \mathrm{Stab}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble X est de cardinal m, qui n'est pas multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal non multiple de p. Soit $x = gS \in \Omega$. Le stabilisateur $\mathrm{Stab}(x)$ est de la forme $H \cap gSg^{-1}$, donc de cardinal p^c pour un certain $c \leqslant b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |H| = p^b n$ et $|\Omega| \wedge p = 1$, on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu.

Solution de l'exercice 10

(1) Tout groupe fini G se plonge dans un groupe symétrique S_n, en faisant agir G sur lui-même par translation, ce qui montre que $n = |G|$ convient. De plus le groupe symétrique S_n se plonge dans $\mathrm{GL}_n(\mathbf{k})$, pour tout corps $\mathbf{k}$, en faisant agir S_n sur les vecteurs d'une base de $\mathbf{k}^n$.

(2) Le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$ est (compter les bases de $(\mathbb{F}_p)^n$) :

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\cdots+(n-1)} m,$$

avec $m \wedge p = 1$. Or $p^{1+2+\cdots+(n-1)}$ est le cardinal du groupe T des matrices triangulaires unipotentes (c'est-à-dire, avec des 1 sur la diagonale).

(3) Application directe. Le point intéressant est que dans de nombreuses sources on trouve une preuve bien plus abstraite de l'existence des p-Sylow, cette preuve rend les choses un peu plus concrète via l'exemple "canonique" celui des matrices triangulaires donné à la question précédente.

Solution de l'exercice 11

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 2 & 9 & 5 & 6 & 1 & 7 & 3 \end{pmatrix} = (187)(2493),$$

d'ordre 12 = PPCM(3,4), signature -1, et

$$\sigma^{10} = (187)(2493)^2 = (187)(29)(43)$$

$$(35)(142)(134)(45)(12345) = id.$$

d'ordre 1, signature 1, et puissance 10 = id.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 7 & 1 & 3 & 8 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 2 & 4 & 5 & 7 & 3 & 6 \end{pmatrix} = (164)(35)$$

d'ordre 6 = PPCM(2,3), signature -1 et $\sigma^{10} = (164)$.

Solution de l'exercice 12

(1) Soit H un sous-groupe d'indice 2 dans S_n, autrement dit $S_n/H \simeq \mathbb{Z}/2$. Pour tout $h \in H$, si $h \notin H$ alors $h^2 \in H$. En appliquant cette remarque à un 3-cycle $h = (ijk)$, on obtient que l'un au moins de h ou $h^2 = h^{-1}$ est dans H, et donc les deux. Finalement H contient tous les 3-cycles, et ceux-ci engendrent A_n, donc H contient A_n, et donc $H = A_n$ par égalité des cardinaux.

(2) Soit H un sous-groupe distingué de S_n, $n \geqslant 5$. Alors $H \cap A_n$ est un sous-groupe distingué du groupe simple A_n. Le cas $H \cap A_n = A_n$ implique que $H = A_n$ ou S_n. On se concentre maintenant sur le cas $H \cap A_n = \{\mathrm{id}\}$, et on veut montrer $H = \{\mathrm{id}\}$. Par l'absurde, supposons que $\sigma \in H$ soit non trivial. Alors pour tout γ non trivial dans H, on a $\sigma\gamma \in H \cap A_n = \{\mathrm{id}\}$. Donc σ est d'ordre 2 et $H = \{\mathrm{id}, \sigma\}$. Mais ceci voudrait dire que la classe de conjugaison de σ est un singleton, contredit le fait que $\sigma \neq \mathrm{id}$.

Le résultat reste vrai pour $n = 3$ (par inspection, ou si on veut avec la même preuve, puisque $A_3 \simeq \mathbb{Z}/3$ est simple). Pour $n = 2$, S_2 est le groupe a deux éléments, et donc A_2 est le groupe trivial. Pour $n = 4$, on a un groupe distingué supplémentaire d'ordre 4.

(3) (*i*) Soit $\sigma \in S_n$ tel que pour tout classe γH on a $\sigma\gamma H = \gamma H$, ce qui équivaut à $\sigma \in \gamma H \gamma^{-1}$. On voit que le noyau du morphisme φ est égal à $\cap_{\gamma \in S_n} \gamma H \gamma^{-1}$, et en particulier est contenue dans H donc d'indice $\geqslant n \geqslant 3$. Par la question précédente on en déduit que le groupe distingué $\ker \varphi$ est trivial, donc φ est injectif.

(*ii*) Pour $n = 3$, le résultat est vrai par inspection (la liste des sous-groupes de S_3 n'est pas bien longue...)

Pour $n = 4$, un sous-groupe d'indice 4 est d'ordre 6, et n'est pas cyclique car S_4 ne contient aucun élément d'ordre 6. On conclut par l'exercice 3.

Supposons maintenant $n \geqslant 5$. Le sous-groupe F de $\mathrm{Bij}(S_n/H) \simeq S_n$ fixant la classe $\mathrm{id}\, H$ est isomorphe à S_{n-1}. Par la question précédente, H s'injecte dans F, et donc est isomorphe à F par comparaison des cardinaux.

Solution de l'exercice 13

(1) L'espace vectoriel $(\mathbb{F}_p)^2$ compte $p+1$ droites vectorielles, qui sont engendrées par le vecteur $(1,0)$ et les vecteurs de la forme $(a,1)$, $a \in \mathbb{F}_p$.

Pour tout corps $\mathbf{k}$, $M \in \mathrm{GL}_2(\mathbf{k})$ préserve les droites engendrées par $(1,0)$ et $(0,1)$ ssi M est diagonale. Si de plus M préserve la droite engendrée par $(1,1)$, alors M est une matrice scalaire. Réciproquement, une matrice scalaire $M \in \mathrm{GL}_2(\mathbf{k})$ correspond à une homothétie de rapport non nulle et préserve toutes les droites vectorielles.

(2) (*i*) On compte les bases de $(\mathbb{F}_p)^2$. Il y a $p^2 - 1$ choix pour le premier vecteur colonne (qui doit être non nul), puis $p^2 - p$ choix pour le second vecteur colonne (qui ne doit pas être proportionnel au premier). On a donc

$$\sharp\, \mathrm{GL}_2(\mathbb{F}_p) = (p^2-1)(p^2-p), \qquad \sharp\, \mathrm{PGL}_2(\mathbb{F}_p) = (p^2-1)p.$$

(*ii*) $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2)$ est de cardinal 6 et s'injecte dans S_3, d'où $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$.

(*iii*) $\mathrm{PGL}_2(\mathbb{F}_3)$ est de cardinal 24 et s'injecte dans S_4, d'où $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$.

(*iv*) $\mathrm{PGL}_2(\mathbb{F}_4)$ est de cardinal 60 et s'injecte dans S_5, d'où $\mathrm{PGL}_2(\mathbb{F}_4) \simeq A_5$ en utilisant l'exercice 12(1).

(*v*) $\mathrm{PGL}_2(\mathbb{F}_5)$ est de cardinal 120 et s'injecte dans S_6, d'où $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$ en utilisant l'exercice 12(3).

(3) On peut envoyer deux droites vectorielles distinctes sur les axes de coordonnées, en envoyant une base de vecteurs directeurs sur $(1,0)$ et $(0,1)$, puis on remarque que les matrices diagonales agissent transitivement sur les droites distinctes des axes de coordonnée.

Pour $\mathbb{F}_2$ et $\mathbb{F}_3$, l'image de trois droites détermine entièrement la permutation des (3 ou 4) droites. Pour $\mathbb{F}_4$, l'image de trois droites détermine la permutation à une transposition près. Pour $\mathbb{F}_5$, l'image de trois droites détermine la permutation à une permutation près des trois droites restantes.

Solution de l'exercice 14

(1) Le groupe G des isométries directe d'un tétraèdre régulier est de cardinal 12 (car une telle isométrie est entièrement déterminée par l'image d'une base formée d'un sommet s, d'un milieu d'arête a et d'un milieu de face f, avec $s \in a \subset f$). L'action de G sur les 4 sommets donne un morphisme $G \to S_4$. Ce morphisme est injectif, car si une application linéaire fixe une base (donnée ici par 3 sommets) alors c'est l'identité. L'image de G est donc un sous-groupe d'ordre 12 dans S_4, et cete image est égale à A_4 par l'exercice 12.

(2) Le même argument montre que le groupe Isom(tétraèdre) est isomorphe à S_4. Il s'agit ici d'observer géométriquement dans le cas $n = 4$ le produit semi-direct $S_n = A_n \rtimes \{\pm 1\}$. Il suffit de prendre le groupe d'ordre 2 engendré par une symétrie orthogonale préservant le tétraèdre (de plan passant par une arête et le milieu de l'arête opposée).

(3) Le morphisme $\mathrm{Isom}^+(\text{cube}) \to S_4$ induit par l'action sur les 4 grandes diagonales est injectif (car déjà 3 grandes diagonales donnent une base de $\mathbb{R}^3$ est donc leurs images déterminent une application linéaire), et donc bijectif par égalité des cardinaux (on peut aussi montrer la surjectivité en vérifiant que les transpositions, qui engendrent S_4, sont dans l'image).

Donner les détails peut constituer un début de développement, à compléter par exemple en interprétant géométriquement les deux sous-groupes distingués V_4 et A_4 de S_4, voire même en faisant aussi le lien avec la table de caractère de S_4. Voir §1.4 de mes notes.

(4) Le morphisme $S \to D_4$ est surjectif. Le théorème de Sylow prévoit que le nombre de 2-Sylow dans un groupe d'ordre 24 est impair et divise 3, ici on en trouve bien 3 correspondant aux 3 possibles carrés "équateur".

(5) On se sert des carrés obtenus en reliant les milieux de deux paires d'arêtes opposées (3 possibilités pour la paire d'arêtes qui ne sert pas), pour obtenir un isomorphisme $S \to \mathrm{Isom}^+(\text{carré}) \simeq \mathbb{Z}/4$.

(6) On trouve un 3-Sylow pour chaque paires g, g^{-1} d'éléments d'ordre 3, on en trouve 4 pour le carré et 4 pour le tétraèdre.

Solution de l'exercice 15

(1)
- $A_2 = \{\mathrm{id}\}$, $S_2 = \{\mathrm{id}, (12)\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $A_3 = \{\mathrm{id}, (123), (132)\} \simeq \mathbb{Z}/3\mathbb{Z}$ sont abéliens (donc les classes de conjugaison sont des singletons), et n'admettent aucun sous-groupes propres (c'est-à-dire distincts des deux cas extrêmes $\{\mathrm{id}\}$ et le groupe entier).
- $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ est le plus petit sous-groupe non abélien. Il admet trois classes de conjugaison qui sont $\{\mathrm{id}\}$, $\{(123), (132)\}$ et $\{(12), (13), (23)\}$. Ses 4 sous-groupes propres sont A_3, $\{\mathrm{id}, (12)\}$, $\{\mathrm{id}, (13)\}$, $\{\mathrm{id}, (23)\}$.
- S_4 admet 24 éléments répartis en 5 classes de conjugaison
  - $\{\mathrm{id}\}$ de cardinal 1 ;
  - Classe des transpositions (ij), de cardinal 6 ;
  - Classe des 3-cycles (ijk), de cardinal 8 ;
  - Classe des 4-cycles $(ijkl)$, de cardinal 6 ;
  - Classe des double-transpositions $(ij)(kl)$, de cardinal 3.
- Montrons que dans A_4 la classe de conjugaison des 3-cycles se coupent en deux (deux classes d'ordre 4).

  Soit X l'ensemble des huit 3-cycles, et considérons d'abord l'action par conjugaison

  $$S_4 \times X \to X$$
  $$\sigma \ , \ \gamma \to \sigma\gamma\sigma^{-1}$$

  On sait que l'action est transitive, donc pour tout $\gamma \in X$ on a

  $$|\operatorname{Stab}(\gamma)| = \frac{|S_4|}{|\operatorname{Orb}(\gamma)|} = \frac{24}{8} = 3.$$

  Donc $\operatorname{Stab}(\gamma) = \langle\gamma\rangle$.

  Maintenant restreignons l'action à A_4. Le stabilisateur $\operatorname{Stab}(\gamma)$ est toujours égal $\langle\gamma\rangle$ (car il ne peut que diminuer quand on passe à une restriction, et il contient γ). On en déduit que pour l'action de A_4,

  $$|\operatorname{Orb}(\gamma)| = \frac{|A_4|}{|\operatorname{Stab}(\gamma)|} = \frac{12}{3} = 4.$$

- Par ailleurs, si γ est une double transposition, le stabilisateur de γ pour l'action de S_4 est d'ordre 8 et contient au moins un 4-cycle (prendre un 4-cycle dont le carré est γ), donc le stabilisateur pour l'action de A_4 est un sous-groupe strict, donc d'indice 2, et l'orbite reste la même.
- Dans A_5 la classe de conjugaison des 5-cycles se coupent en deux (deux classes d'ordre 12). L'argument est similaire.

  La classe des 20 3-cycles, de stabilisateur d'ordre 6 dans S_4, reste la même (le stabilisateur est $\mathbb{Z}/3 \times \mathbb{Z}/2$ engendré par le 3-cycle et la transposition de support disjoint).

  La classe des 15 double transpositions, de stabilisateur d'ordre 8 dans S_4, reste la même (pas possible de couper en deux, elle est de cardinal impair).

(2) Il s'agit de comprendre pourquoi les deux assertions suivantes sont vraies :
- Si $G = \mathrm{Isom}^+(\text{tétraèdre}) \simeq A_4$, et si $g \in G$ est d'ordre 3, alors g n'est PAS conjugué à g^{-1} dans G.

- Si $G = \mathrm{Isom}^+(\text{icosaèdre}) \simeq A_5$, et si $g \in G$ est d'ordre 5, alors g EST conjugué à g^{-1} dans G (mais PAS à g^2...).

La raison est que $g = \varphi g^{-1} \varphi^{-1}$ dans $\mathrm{SO}_3(\mathbb{R})$ ssi φ est une rotation préservant l'axe de g et renversant son orientation, c'est-à-dire φ est d'angle π et d'axe orthogonal à celui de g. Dans le cas du tétraèdre, il n'existe pas un tel φ dans G (car l'axe de g passe par un sommet et le milieu de la face opposée), alors que dans le cas de l'icosaèdre, un tel g existe (l'axe passe par deux sommets opposés).

(3)
$$\{\mathrm{id}, (12)(34)\} \lhd \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \lhd A_4,$$
mais $\{\mathrm{id}, (12)(34)\}$ n'est pas distingué dans A_4.

NB : Le groupe intermédiaire d'ordre 4 est souvent appelé "groupe de Klein" et noté V_4, il est isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Solution de l'exercice 16

Les classes de conjugaison sont de cardinaux $1, 12, 12, 15, 20$. Un sous-groupes est distingué ssi il est union de classes de conjugaison, donc pour produire un candidat il faudrait qu'une union de classes de conjugaison (dont celle du neutre) soit de cardinal divisant 60. On vérifie que c'est impossible, sauf les cas extrêmes de cardinaux 1 et 60.

Solution de l'exercice 17

(1) Soit $\sigma \in A_n$. Comme S_n est engendré par les transpositions, on peut écrire σ comme la composée d'un nombre pair de transpositions. Reste à remarquer que le produit de deux transpositions τ_1, τ_2 peut également s'écrire à l'aide de 3-cycles : on distingue trois cas suivant que les supports de τ_1 et τ_2 ont 2, 1 ou 0 éléments commun.
   - $(ij)(ij) = \mathrm{id}$;
   - $(ij)(jk) = (ijk)$;
   - $(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$.

(2) Soit (ijk) un 3-cycle, il existe une permutation $\sigma \in S_n$ telle que $\sigma(1) = i$, $\sigma(2) = j$, $\sigma(3) = k$. On peut de plus supposer $\sigma \in A_n$, quitte à remplacer σ par $\sigma \circ (45)$. Alors $(ijk) = \sigma(123)\sigma^{-1}$, ainsi tous les 3-cycles sont conjugués à (123) dans A_n, et donc également entre eux.

NB : Ces deux propriétés du groupe A_n sont les deux premières étape d'une preuve du fait classique que A_n est un groupe simple pour $n \geqslant 5$: je suggère la référence Ramis-Warusfel (aka "gros pavé"), page 19.

Solution de l'exercice 18

Rappelons qu'une *transvection* est une matrice conjuguée à
$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & & 0 & \ddots & \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$
Si $M \in \mathrm{GL}_n(\mathbf{k})$, en faisant des opérations sur les lignes et les colonnes (autrement dit en multipliant à droite et à gauche par des matrices de transvections) on peut se ramener à une matrice par bloc
$$\begin{pmatrix} 1 & 0 \\ 0 & M' \end{pmatrix}$$
avec $M' \in \mathrm{GL}_{n-1}(\mathbf{k})$ de même déterminant que M. Par récurrence sur la dimension de M, on en déduit que M est un produit de transvections et d'une dilatation.
Par ailleurs, on remarque qu'une matrice 2×2 est une dilatation ssi elle admet 1 et $\lambda \neq 1$ comme valeurs propres. Alors pour tout $a \neq 1$ on peut écrire :
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & a^{-1} \end{pmatrix}$$
Ceci implique que toute transvection (en toute dimension, en travaillant par blocs) est un produit de deux dilatations, d'où le résultat.
NB : Dans le cas $\mathbf{k} = \mathbb{F}_2$, l'ensemble des dilatations est vide, par contre $\mathrm{GL}_n(\mathbb{F}_2) = \mathrm{SL}_n(\mathbb{F}_2)$ et on peut appliquer le résultat qui dit que $\mathrm{SL}_n(\mathbf{k})$ est engendré par les transvections pour tout corps $\mathbf{k}$.

Solution de l'exercice 19

(1) Un morphisme de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel est en particulier un morphisme de groupe. Montrons la réciproque dans la situation de l'exercice.

Soit $(\bar{a},\bar{b},\bar{c}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ et $1 \leqslant \lambda \leqslant p$. On a :

$$\begin{aligned} f(\bar{\lambda}(\bar{a},\bar{b},\bar{c})) &= f(\underbrace{(\bar{a},\bar{b},\bar{c}) + \cdots + (\bar{a},\bar{b},\bar{c})}_{\lambda \text{ fois}}) \\ &= \underbrace{f(\bar{a},\bar{b},\bar{c}) + \cdots + f(\bar{a},\bar{b},\bar{c})}_{\lambda \text{ fois}} \\ &= \bar{\lambda} f(\bar{a},\bar{b},\bar{c}). \end{aligned}$$

(2) On en déduit

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z}).$$

NB : Ce résultat se généralise à un nombre quelconque de facteurs. On obtient par exemple

$$\mathrm{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2) \simeq \mathrm{GL}_2(\mathbb{Z}/2) \simeq S_3.$$

Solution de l'exercice 20

(1) Supposons K distingué (le cas H distingué est similaire). Pour tous $h_1, h_2 \in H$, $k_1, k_2 \in K$, on a

$$(h_1k_1)(h_2k_2) = (h_1h_2)h_2^{-1}k_1h_2k_2 \in HK, \quad (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h^{-1}hk_1^{-1}h_1^{-1} \in HK,$$

ainsi HK est un sous-groupe.

(La réciproque est fausse, pour un contre-exemple prendre $H = K$ un sous-groupe non-distingué de G, comme par exemple $H = \{\mathrm{id}, (12)\}$ dans $G = S_3$).

(2) Notons

$$\begin{aligned} \varphi\colon H \times K &\to G \\ (h\ ,\ k) &\mapsto hk. \end{aligned}$$

La condition $H \cap K = \{1\}$ assure que φ est injective, en effet si $hk = 1$ alors $h = k^{-1} \in H \cap K$.

La condition $HK = G$ assure que φ est surjective.

Enfin, la condition H et K distingué assure que φ est un morphisme, car pour tout $h \in H, k \in K$, on a

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1} \in H \cap K = \{1\}.$$

(3) Si G, H', K' sont des groupes tel que $H' \times K'$ est isomorphe à G, alors en notant H, K les images respectives de H', K' dans G, on a

$$H \cap K = \{1\}, \qquad HK = G, \qquad H \text{ et } K \text{ distingués dans } G.$$

(4) Notons σ la symétrie centrale de $\mathbb{R}^3$, ou autrement dit $\sigma = -\mathrm{id}$. σ est dans le centre de $\mathrm{GL}_3(\mathbb{R})$ et donc commute avec tout élément de G, de plus $\sigma \notin G^+$.

(5) Le groupe des isométries du carré est le groupe diédral D_4 d'ordre 8, en particulier tous ses sous-groupes propres sont abéliens. Si D_4 était un produit direct non-trivial alors il serait abélien, ce qui n'est pas le cas (voir exercice 1, où on a vu que les classes de conjugaison n'étaient pas toutes des singletons).

Solution de l'exercice 21

(1) On a déja vu (exercice 20) que les conditions $HK = G$ et $H \cap K = \{1\}$ assurent que l'application $(h,k) \in H \times K \mapsto hk \in G$ est bijective.

Donc tout $g \in G$ s'écrit de façon unique $g = hk$ avec $h \in H, k \in K$, et $gK = hK$. Ainsi les éléments de H forment un système de représentants des classes du quotient G/K.

(2) Il suffit de prendre $\mathbb{Z}/2\mathbb{Z} \simeq \langle (1\ 2) \rangle$.

(3) Il suffit de prendre $K^* \simeq \{\mathrm{diag}(\lambda, 1, \ldots, 1)\}$.

(4) Il suffit de prendre le groupe d'ordre 2 engendré par une symétrie orthogonale préservant le polygone.

(5) On prend H le groupe des automorphisme fixant un point (H est isomorphe au groupe linéaire), et K le groupe distingué des translations (caratérisées par le fait de ne pas avoir de point fixe, et cette propriété est préservée par conjugaison).

NB : La notation $G = K \rtimes H$ semble la plus courante, mais on trouve aussi parfois $G = H \ltimes K$. Dans les deux cas, le groupe qui agit "tient la poignée du ciseau". On trouve souvent des notations inversées (H pour le groupe distingué), mais je trouve plus naturel que ce soit K qui dénote le groupe distingué (car K comme "Ker").

Solution de l'exercice 22

NB : Dans cet exercice on décrit les automorphismes de *groupe* de $\mathbb{Z}/n\mathbb{Z}$, en se servant de sa structure d'anneau...

(1) $(i) \iff (iii)$. Si $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$, alors il existe $a \geqslant 1$ tel que $\bar{k} + \cdots + \bar{k} = \bar{1}$ (a fois), et donc $\bar{a}$ est l'inverse de $\bar{k}$ modulo n. Réciproquement si $\bar{k}$ est inversible modulo n on peut choisir décrire l'inverse sous la forme $\bar{a}$ avec $a \geqslant 1$.

$(ii) \iff (iii)$: $\bar{a}\bar{k} = \bar{1}$ équivaut à l'existence d'un $u \in \mathbb{Z}$ tel que $ak + un = 1$, et par Bézout ceci équivaut à k et n premiers entre eux.

(2) Comme $\mathbb{Z}/n\mathbb{Z}$ est monogène, un morphisme φ est entièrement déterminé par l'image d'un générateur (disons l'image de $\bar{1}$), et φ est un automorphisme ssi $\varphi(\bar{1})$ est aussi un générateur. Par la question précédente on associe donc à chaque $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ un élément inversible $\bar{a} = \varphi(\bar{1}) \in (\mathbb{Z}/n\mathbb{Z})^*$. Montrons qu'en fait φ est l'homothétie de rapport $\bar{a}$. On peut supposer $a \geqslant 1$, et pour tout $0 \leqslant x \leqslant n-1$ on écrit (toutes les sommes sont répétées x fois) :

$$\varphi(\bar{x}) = \varphi(\bar{1} + \cdots + \bar{1}) = \varphi(\bar{1}) + \cdots + \varphi(\bar{1}) = \bar{a} + \cdots + \bar{a} = \bar{a}\bar{x}.$$

Ceci implique que la bijection $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \mapsto \varphi(\bar{1}) \in (\mathbb{Z}/n\mathbb{Z})^*$ est un morphisme de groupe, et donc un isomorphisme.

Solution de l'exercice 23

Soit $\varphi, \psi \in \mathrm{Aut}(G)$, avec φ l'automorphisme intérieur associé à la conjugaison par $y \in G$:

$$\forall x \in G, \varphi(x) = yxy^{-1}.$$

On a, pour tout $x \in G$:

$$\psi\varphi\psi^{-1}(x) = \psi(y\psi^{-1}(x)y^{-1}) = \psi(y)x\psi(y)^{-1}.$$

Ainsi $\psi\varphi\psi^{-1}$ est encore un automorphisme intérieur, associé à la conjugaison par $\psi(y)$. Ceci montre que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.
D'autre part, via l'action par conjugaison de G sur lui-même on obtient un morphisme surjectif de G vers $\mathrm{Int}(G)$, dont le noyau est le centre de G. On conclut par le théorème d'isomorphisme que $\mathrm{Int}(G) \simeq G/Z(G)$.

Solution de l'exercice 24

Donnons la liste des groupes abéliens d'ordre $72 = 2^3 \cdot 3^2$, que l'on cherche dans un premier temps sous la formes "facteurs élémentaires".
Il y a trois possibilités pour le 2-Sylow (d'ordre $8 = 2^3$), que l'on peut visualiser (c'est facultatif, mais pourra être recyclé en algèbre linéaire pour passer de la décomposition "Jordan" à la décomposition "Frobenius" et vice-versa) avec les colonnes d'un "tableau de Young" :

$\mathbb{Z}/8$ 

$\mathbb{Z}/4 \times \mathbb{Z}/2$ 

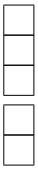
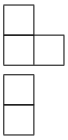
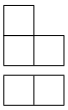
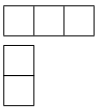
$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ 

Par ailleurs il y a deux possibilités pour le 3-Sylow (d'ordre $9 = 3^2$) :

$\mathbb{Z}/9$ 

$\mathbb{Z}/3 \times \mathbb{Z}/3$ 

En combinant ces possibilités, on obtient donc six groupes abéliens d'ordre 72 à isomorphisme près. En superposant les diagrammes et en lisant colonne par colonne, on trouve la décomposition en "facteurs invariants" :

$\mathbb{Z}/72 \simeq \mathbb{Z}/8 \times \mathbb{Z}/9$	
$\mathbb{Z}/24 \times \mathbb{Z}/3 \simeq \mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/3$	
$\mathbb{Z}/36 \times \mathbb{Z}/2 \simeq \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/9$	
$\mathbb{Z}/12 \times \mathbb{Z}/6 \simeq \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3$	
$\mathbb{Z}/18 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9$	
$\mathbb{Z}/6 \times \mathbb{Z}/6 \times \mathbb{Z}/2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3$	

Solution de l'exercice 25

(1) Prendre $G = G' = \oplus_{\mathbb{N}}\mathbb{Z}$ (on peut y penser comme le groupe additif $\mathbb{Z}[X]$ des polynômes à coefficients entiers), $H = \mathbb{Z}$, $H' = \mathbb{Z}^2$. Les groupes H et H' ne sont pas isomorphes (exercice 6), pourtant

$$G \times H \simeq G \times H' \simeq G.$$

(2) Pour tout morphisme $\varphi\colon G_1 \to G_2$ le théorème de factorisation donne un diagramme

$$\begin{array}{ccccc} G_1 & \longrightarrow & \varphi(G_1) & \hookrightarrow & G_2 \\ \downarrow & \nearrow & & & \\ G_1/\ker\varphi & & & & \end{array}$$

Réciproquement, le morphisme φ est uniquement déterminé par le choix d'un sous-groupe distingué $N = \ker\varphi$ dans G_1 et le choix d'un morphisme injectif $G_1/N \to G_2$. Cela implique immédiatement que

$$m(G_1, G_2) = \sum_{N \lhd G_1} i(G_1/N, G_2).$$

(3) Pour tout groupe fini F, on a

$$m(F, G) \cdot m(F, H) = m(F, G \times H) = m(F, G' \times H') = m(F, G') \cdot m(F, H').$$

On en déduit, puisque $m(F, G) = m(F, G') \geqslant 1$, que

$$m(F, H) = m(F, H').$$

Par récurrence sur l'ordre de F, on déduit de la question précédente que $i(F, H) = i(F, H')$, et en particulier en prenant $F = H$:

$$1 \leqslant i(H, H) = i(H, H').$$

Ainsi il existe un morphisme injectif de H vers H', et ces deux groupes ayant même cardinal, ce morphisme est un isomorphisme.

NB : Ce résultat permet de déduire très simplement la partie "unicité" dans le théorème de structure des groupes abéliens. Malheureusement, il ne se trouve dans aucun livre de ma connaissance... Pour la partie "existence" si on veut en faire un développement qui tienne dans les 15 minutes je suggère de suivre Colmez, voir §2 de mes notes.

Solution de l'exercice 26

(1) De façon générale on a $\sharp\,\mathrm{GL}_2(\mathbb{F}_p) = (p^2-1)((p^2-p)$, donc ici $\sharp\,\mathrm{GL}_2(\mathbb{F}_3) = 8\cdot 6 = 48$. De plus $\sharp\mathbb{F}_3^* = 2$, d'où le résultat.

(2) Ce point n'est pas facile, et fait appel à un peu de théorie de réduction des endomorphimes. Soit G un sous-groupe d'ordre 8 dans $\mathrm{SL}_2(\mathbb{F}_3)$ (G est un 2-Sylow, il en existe au moins un par l'exercice 10). Les matrices dans G sont annulées par le polynôme X^8-1, qui est à racine simple en caractéristique 3 (ses racines sont les éléments non nuls du corps $\mathbb{F}_9$). Une telle matrice M est donc diagonalisable, et de polynôme caractéristique $X^2-(\mathrm{tr}\,M)X+1$. Si $\mathrm{tr}\,M = \pm 1$, on a une racine double, car sur $\mathbb{F}_3$ on a
$$X^2-X+1 = (X+1)^2 \text{ et } X^2+X+1 = (X-1)^2.$$
Dans ce cas $M = \pm\,\mathrm{id}$. Sinon $\mathrm{tr}\,M = 0$, or il y a exactement 6 matrices de trace nulle dans $\mathrm{SL}_2(\mathbb{F}_3)$. Ainsi $\mathrm{SL}_2(\mathbb{F}_3)$ admet un seul sous-groupe d'ordre 8, on vérifie qu'il est non abélien et contient un élément d'ordre 2 central, il est donc isomorphe à $\mathbb{H}_8$.

(3) On a vu que $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$, et S_4 ne contient pas de sous-groupe isomorphe à $\mathbb{H}_8$. Une façon de le voir est de vérifier que l'on ne peut pas trouver trois éléments d'ordre 4 dans S_4 avec le même carré.

NB : on pourrait aussi court-circuiter la question précédente et constater que
$$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$
est d'ordre 6 dans $\mathrm{SL}_2(\mathbb{F}_3)$, or $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ ne contient aucun élément d'ordre 6.

Solution de l'exercice 27

On sait (voir exercice 5) que $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$, et comme p divise $q-1$ par hypothèse, il existe un sous-groupe H d'ordre p dans $\mathbb{F}_q^*$: écrire $\mathbb{F}_q^* = \langle \bar{a}\rangle$, et poser $H = \langle \bar{a}^k\rangle$ où $kp = q-1$ Alors le groupe d'ordre pq recherché est
$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in H, b \in \mathbb{F}_q \right\}$$
Cet exemple est tiré de Ramis-Warusfel, p.25. Attention : si on prend des matrices de la forme $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, on obtient le groupe abélien $\mathbb{Z}/p \times \mathbb{Z}/q$...

NB : C'est un résultat classique (et un développement possible) de montrer qu'il y a exactement deux groupes d'ordre pq à isomorphisme près quand $p|(q-1)$, qui sont $\mathbb{Z}/p\times\mathbb{Z}/q$ et le groupe non abélien de l'exercice (si p ne divise pas $q-1$ il n'y a que le groupe abélien). Cependant ce développement nécessite la notion de produit semi-direct *externe*, version abstraite de celle vue dans l'exercice 21. Souvent les candidats qui présentent ce développement ambitieux ne savent pas donner un exemple concret de groupe non-abélien d'ordre pq, voilà qui est réparé avec cet exercice (on pourra aussi penser au groupe diédral dans le cas $p = 2$).