Groupes

Deux exercices égarés de la feuille sur les anneaux

∆∘ **Exercice 1.** *Radical d'un idéal.* *X*

Soit A un anneau commutatif. Étant donné un idéal $I \trianglelefteq A$, on définit son *radical* $\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} : a^n \in I\}$.

1. Montrer que pour tout idéal $I \trianglelefteq A$, le radical $\sqrt{I}$ est un idéal de A.
2. Un idéal est dit *radiciel* s'il est égal à son radical. Déterminer les idéaux radiciels de $\mathbb{Z}$ et de K[X].

Étant donné deux idéaux $I, J \trianglelefteq A$, on définit leur *somme* $I + J = \{x + y \mid x \in I, y \in J\}$, qui est encore un idéal de A .

3. Soit $I, J \trianglelefteq A$. Démontrer une inclusion générale entre $\sqrt{I+J}$ et $\sqrt{I} + \sqrt{J}$ et produire un contre-exemple montrant que l'autre inclusion est en général fausse.

⋆ **Exercice 2.** *Anneaux noethériens.*

Soit A un anneau commutatif. Un idéal $I \trianglelefteq A$ sera dit *de type fini* s'il existe un nombre fini d'éléments $x_1, \dots, x_n \in A$ tels que $I = (x_1, \dots, x_n) := \{a_1 x_1 + \cdots + a_n x_n \mid a_1, \dots, a_n \in A\}$.

1. Montrer que les assertions suivantes sont équivalentes :
   (i) Tout idéal de A est de type fini.
   (ii) Toute suite croissante d'idéaux stationne.
   (iii) Tout ensemble non vide d'idéaux de A possède un élément maximal.

   Quand ces propriétés sont vraies, on dit que A est *noethérien.*
2. Donner un exemple d'anneau non noethérien.

Généralités et révisions

∆∘ **Exercice 3.** *2-groupe abélien élémentaire.*

Soit G un groupe tel que $\forall g \in G, g^2 = 1_G$. Montrer que G est abélien.

⋆ **Exercice 4.** *Une présentation étrange de* C_{10}.

Soit G un groupe et $x, y \in G$ tels que $xyx = y^3$ et $y^5 = 1_G$.

Montrer que x et y commutent, puis que $x^2 = y^2$.

Exercice 5. *Groupes n-abéliens.* *Mines*

Soit $k \in \mathbb{N}$ et G un groupe tel que $\forall a, b \in G, \forall \ell \in \{k, k+1, k+2\}, (ab)^\ell = a^\ell b^\ell$. Montrer que G est abélien.

◦ **Exercice 6.** *Produit de deux sous-groupes.*

Soit G un groupe et H_1, H_2 deux sous-groupes de G.

Montrer que H_1H_2 est un sous-groupe de G si et seulement si $H_1H_2 = H_2H_1$.

Exercice 7. *Une normalisation un peu cachée.*

Soit H, H', K trois sous-groupes d'un groupe G. On suppose H abélien et $H' \subseteq H$.

1. Donner un exemple où $H'K$ n'est pas un sous-groupe de G.
2. Montrer que $H \cap H'K$ est un sous-groupe de G.

Exercice 8. *Transport de structures.*

Montrer que tout ensemble fini non vide peut être muni d'une structure de groupe.

◦ **Exercice 9.** *Groupes additif et multiplicatif de* $\mathbb{R}$. *Lyon*

Montrer que le groupe additif $(\mathbb{R}, +)$ n'est pas isomorphe au groupe multiplicatif $(\mathbb{R}^*, \times)$.

Exercice 10. *Décomposition de* $\mathbb{C}^*$.

Montrer que le groupe multiplicatif $\mathbb{C}^*$ est isomorphe au groupe produit des groupes $(\mathbb{U}, \cdot)$ et $(\mathbb{R}, +)$.

Exercice 11. *Groupe des isométries linéaires du cube* $\{0,1\}^n$.

Soit $C = \{0,1\}^n$ et $G = \left\{ f \in \mathrm{GL}_n(\mathbb{C}) \,\middle|\, \forall x \in C, f(x) \in C \right\}$. Montrer que G est isomorphe à $\mathfrak{S}(n)$.

◦ **Exercice 12.** *Morphisme* $x \mapsto x^2$.

1. Soit $(G, \cdot)$ un groupe. Montrer que l'application $g \mapsto g^2$ est un morphisme de groupes si et seulement si G est abélien.
2. En déduire que dans un groupe abélien fini d'ordre impair, tout élément est un carré, c'est-à-dire que $\forall y \in G, \exists x \in G : x^2 = y$.
3. La propriété reste-t-elle vraie dans un groupe non abélien fini d'ordre impair ?

Exercice 13. *Morphismes.*

1. Décrire les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$.
2. Décrire les morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$.

Exercice 14. $\mathbb{Q}$ *n'est pas résiduellement fini.*

Soit F un groupe fini. Montrer que tout morphisme de groupes $\mathbb{Q} \to F$ est trivial.

Exercice 15. *Un ensemble fini de morphismes.*

Soit $n, m \in \mathbb{N}$.

1. Soit F un groupe fini. Montrer que $\mathrm{Hom}(\mathbb{Z}^n, F)$ est fini.
2. Plus précisément, montrer que $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}/2\mathbb{Z})$ possède 2^n éléments.
3. Déduire de la question précédente que $\mathbb{Z}^n$ et $\mathbb{Z}^m$ sont isomorphes si et seulement si $n = m$.

Exercice 16. *Isomorphismes entre groupes linéaires.*

Soit K un corps de caractéristique nulle.

1. Soit $n \geq 2$. À conjugaison près, combien $\mathrm{GL}_n(\mathrm{K})$ contient-il d'éléments d'ordre 2 ?
2. Soit $n, m \geq 2$ tels que $\mathrm{GL}_n(\mathrm{K})$ et $\mathrm{GL}_m(\mathrm{K})$ soient isomorphes. Montrer $n = m$.
3. Soit $n \geq 2$. Les groupes $\mathrm{GL}_n(\mathbb{R})$ et $\mathrm{GL}_n(\mathbb{C})$ sont-ils isomorphes ?

Exercice 17. *Sous-groupe des périodes.*

1. Soit $f : \mathbb{R} \to \mathbb{R}$. Montrer que *l'ensemble des périodes* de f
$$\mathrm{Pér}(f) = \left\{ \mathrm{T} \in \mathbb{R} \;\middle|\; \forall x \in \mathbb{R}, f(x + \mathrm{T}) = f(x) \right\}$$
est un sous-groupe de $\mathbb{R}$.
2. Réciproquement, soit G un sous-groupe de $\mathbb{R}$.
Construire une fonction $f : \mathbb{R} \to \mathbb{R}$ telle que $\mathrm{Pér}(f) = \mathrm{G}$.

♠ **Exercice 18.** *Sous-groupes de* $\mathbb{R}$.

Montrer que tout sous-groupe de $\mathbb{R}$ est soit monogène, soit dense.

Exercice 19. *Classes de conjugaison.*

1. On note $\Sigma = \left\{ \begin{pmatrix} \mathbb{C} \to & \mathbb{C} \\ z \mapsto & az + b \end{pmatrix} \;\middle|\; (a, b) \in \mathbb{C}^* \times \mathbb{C} \right\}$ l'ensemble des similitudes directes.
Montrer que $(\Sigma, \circ)$ est un groupe.
2. Déterminer les classes de conjugaison de Σ.

Exercice 20. *Point fixe global.* *X modifié*

Soit G l'ensemble des applications affines bijectives $\mathbb{R} \to \mathbb{R}$.

1. Montrer que $(\mathrm{G}, \circ)$ est un groupe.
2. Montrer que l'application $\varphi : \mathrm{G} \to \mathbb{R}^*$ qui associe à un élément de G son coefficient directeur est un morphisme de groupes et déterminer son noyau.
3. Soit Γ un sous-groupe de G tel que $\forall f \in \Gamma, \exists \omega \in \mathbb{R} : f(\omega) = \omega$.
Montrer que $\exists \omega \in \mathbb{R} : \forall f \in \Gamma, f(\omega) = \omega$.

⋆ **Exercice 21.** *Automorphismes d'un graphe.*

Pour les besoins de cet exercice,

- un *graphe* est un couple $(\mathrm{V}, \leftrightarrow)$ où V est un ensemble et $\leftrightarrow$ est une relation symétrique et *irréflexive* ($\forall v \in \mathrm{V}, v \not\leftrightarrow v$) sur V, appelée relation d'*adjacence* ;
- un *automorphisme* d'un graphe $(\mathrm{V}, \leftrightarrow)$ est une bijection $\varphi : \mathrm{V} \to \mathrm{V}$ telle que, pour tous $v_1, v_2 \in \mathrm{V}$, $v_1 \leftrightarrow v_2$ si et seulement si $\varphi(v_1) \leftrightarrow \varphi(v_2)$.

1. Vérifier que les automorphismes d'un graphe forment un groupe pour la composition.
2. **Exemples.** Soit $n \geq 3$.
   (a) On note K_n le graphe complet $\left(\llbracket 1, n \rrbracket, \neq\right)$. Déterminer son groupe d'automorphismes.
   (b) Montrer qu'il n'existe pas de relation d'adjacence $\leftrightarrow$ sur $\llbracket 1, n \rrbracket$ telle que le groupe des automorphismes de $(\llbracket 1, n \rrbracket, \leftrightarrow)$ soit $\mathfrak{A}(n)$.
   (c) Définir (avec le formalisme de l'exercice) le n-cycle C_n et montrer que son groupe d'automorphismes possède exactement $2n$ éléments.

3. Soit G un groupe. Construire un graphe dont le groupe des automorphismes contient un sous-groupe isomorphe à G.
4. **Cas particuliers du théorème de Frucht.**
   (a) Construire un graphe dont le groupe des automorphismes est isomorphe à $\mathbb{Z}$.
   (b) Construire un graphe possédant exactement trois automorphismes.

Remarque. Le théorème de Frucht (1939) affirme que tout groupe est isomorphe au groupe des automorphismes d'un graphe. Comme le montrent les cas particuliers de l'exercice, la difficulté est de trouver un graphe n'exhibant pas de symétries « parasites ».

Parties génératrices

◦ **Exercice 22.** $\langle i, j \rangle$.

Quel est le sous-groupe de $(\mathbb{C}^*, \times)$ engendré par les deux nombres complexes i et j ?

Exercice 23. *Groupe des quaternions* Q_8.

Dans cet exercice, on note 1 la matrice identité (habituellement notée I_2) et on définit les trois matrices $\mathrm{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\mathrm{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mathrm{K} = \mathrm{IJ}$, toutes trois éléments de $\mathrm{GL}_2(\mathbb{C})$.

1. Montrer que le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par I et J est $\mathrm{Q}_8 = \{1, -1, \mathrm{I}, -\mathrm{I}, \mathrm{J}, -\mathrm{J}, \mathrm{K}, -\mathrm{K}\}$.
2. Dresser la table de multiplication de Q_8.
3. Déterminer l'ordre de chaque élément, et les classes de conjugaison du groupe.

⋆ **Exercice 24.** *Les parties génératrices contraignent les morphismes : cas de* $\mathrm{GL}_n(\mathbb{R})$.

Soit $n, m \geq 2$. On admet/rappelle que $\mathrm{GL}_n(\mathbb{R})$ est engendré par les matrices de dilatation, d'échange et de transvection.

Déterminer les morphismes $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{U}_m$.

⋆ **Exercice 25.** *Sous-groupe d'un groupe de type fini.*

1. Montrer (par exemple par récurrence sur le nombre de générateurs) que tout sous-groupe d'un groupe abélien de type fini est encore de type fini.
2. Une permutation $\sigma \in \mathfrak{S}(\mathbb{Z})$ est dite être *une translation à l'infini* s'il existe une partie finie $\mathrm{F} \subseteq \mathbb{Z}$ telle que $\exists t \in \mathbb{Z} : \forall x \in \mathbb{Z} \setminus \mathrm{F}, \sigma(x) = x + t$. On note G l'ensemble des translations à l'infini.
   (a) Soit $\sigma \in \mathrm{G}$.
   Montrer que l'entier t apparaissant dans la définition est en fait unique : on le notera $\tau(\sigma)$.
   (b) Montrer que G est un sous-groupe de $\mathfrak{S}(\mathbb{Z})$ et que $\tau : \mathrm{G} \to \mathbb{Z}$ est un morphisme de groupes.
   (c) Montrer que G est engendré par la transposition (1 2) et la translation $x \mapsto x + 1$, mais que $\ker \tau$ ne possède pas de partie génératrice finie.

⋆ **Exercice 26.** *Vers le théorème de Higman-Neumann-Neumann (1949).*

Soit $(\mathrm{A}, +)$ un groupe abélien, et G un sous-groupe du groupe $\mathrm{Aut}(\mathrm{A})$ des automorphismes de A.

Pour tout $\varphi \in \mathrm{G}$ et tout $a \in \mathrm{A}$, on considère l'application « affine » $\mathrm{F}_{\varphi,a} : \begin{cases} \mathrm{A} \to \mathrm{A} \\ x \mapsto \varphi(x) + a \end{cases}$ et on note $\mathrm{A} \rtimes \mathrm{G} = \left\{ \mathrm{F}_{\varphi,a} \,\middle|\, \varphi \in \mathrm{G}, a \in \mathrm{A} \right\}$.

1. Montrer que $A \rtimes G$ est un sous-groupe de $\mathfrak{S}(A)$, et que $\left\{F_{\varphi,0} \,\middle|\, \varphi \in G\right\}$ et $\left\{F_{\mathrm{id}_A,a} \,\middle|\, a \in A\right\}$ en sont des sous-groupes, isomorphes à G et A, respectivement.
2. On suppose qu'il existe $x_1, \dots, x_r \in A$ tels que le seul sous-groupe de A stable sous les éléments de G et contenant $x_1, \dots, x_r$ soit A lui-même.
   Montrer que si G est engendré par des éléments $\varphi_1, \dots, \varphi_s$, alors $A \rtimes G$ est engendré par $r+s$ éléments.
3. On note $\mathbb{Z}[1/2] = \left\{\dfrac{a}{2^k} \,\middle|\, a \in \mathbb{Z}, k \in \mathbb{N}\right\}$.
   (a) Vérifier que $\mathbb{Z}[1/2]$ est un sous-groupe de $(\mathbb{Q}, +)$ qui ne possède aucune partie génératrice finie.
   (b) Construire un groupe engendré par deux éléments contenant un sous-groupe isomorphe à $\mathbb{Z}[1/2]$.
4. Dans cette question, on note $\mathbb{Q}^{(\mathbb{Z})}$ l'ensemble des familles presque nulles, indexées par $\mathbb{Z}$, de nombres rationnels. On considère les deux applications
   $$\sigma : \begin{cases} \mathbb{Q}^{(\mathbb{Z})} \to \mathbb{Q}^{(\mathbb{Z})} \\ v \mapsto (v_{n+1})_{n\in\mathbb{Z}} \end{cases} \quad \text{et} \quad \tau : \begin{cases} \mathbb{Q}^{(\mathbb{Z})} \to \mathbb{Q}^{(\mathbb{Z})} \\ u \mapsto \big(\max(1,n)\, u_n\big)_{n\in\mathbb{Z}}, \end{cases}$$
   dont on vérifie sans difficulté qu'il s'agit d'automorphismes de $\mathbb{Q}^{(\mathbb{Z})}$.
   (a) Déterminer les sous-groupes de $\mathbb{Q}^{(\mathbb{Z})}$ stables sous tous les éléments de $\langle \sigma, \tau \rangle$.
   (b) Construire un groupe engendré par trois éléments contenant un sous-groupe isomorphe à $\mathbb{Q}^{(\mathbb{Z})}$.

Exercice 27. *Rang d'un groupe fini.*

Étant donné un groupe fini G, on définit son *rang* $\mathrm{rg}(G)$ comme le minimum des cardinaux des parties génératrices de G.

1. Soit $n \geq 2$. Montrer $\mathrm{rg}(\mathbb{Z}/n\mathbb{Z}) = 1$, $\mathrm{rg}\left((\mathbb{Z}/n\mathbb{Z})^2\right) = \mathrm{rg}(\mathfrak{S}(3)) = 2$.
2. Soit G_1 et G_2 deux groupes finis.
   (a) Montrer $\mathrm{rg}(G_1 \times G_2) \leq \mathrm{rg}(G_1) + \mathrm{rg}(G_2)$.
   (b) Montrer que l'inégalité précédente est stricte dans le cas où $G_1 = \mathbb{Z}/2\mathbb{Z}$ et $G_2 = \mathbb{Z}/3\mathbb{Z}$.
3. Soit G un groupe fini. Montrer que $\mathrm{rg}(G) \leq \log_2(|G|)$.
4. Soit $d \in \mathbb{N}$. Donner un exemple de groupe de rang d et de cardinal 2^d.

Exercice 28. *Rang de $(\mathbb{Z}/n\mathbb{Z})^r$.*

Soit $n \geq 2$. Montrer que si une partie S engendre $(\mathbb{Z}/n\mathbb{Z})^r$, alors $|S| \geq r$.

⋆⋆ **Exercice 29.** *Do not generate.* *ÉNS*

Alice et Bob jouent à un jeu dans un groupe fini G. Ils choisissent à tour de rôle (en commençant par Alice) un élément du groupe, différent des choix précédents. À un moment, le choix d'un des joueurs entraîne que les éléments choisis engendrent le groupe G. Ce joueur est alors déclaré perdant.

1. Quel joueur a une stratégie gagnante si $G = \mathbb{Z}/n\mathbb{Z}$ $(n \geq 2)$?
2. Quel joueur a une stratégie gagnante si $G = \mathfrak{S}(n)$ $(n \geq 3)$?

⋆⋆ **Exercice 30.** *Generate.*

Alice et Bob jouent à un jeu dans un groupe fini G. Ils choisissent à tour de rôle (en commençant par Alice) un élément du groupe, différent des choix précédents. À un moment, le choix d'un des joueurs entraîne que les éléments choisis engendrent le groupe G. Ce joueur est alors déclaré gagnant.

1. Quel joueur a une stratégie gagnante si G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$?
2. Montrer que si G est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^r$, pour un certain $r \geq 3$, Alice a une stratégie gagnante si et seulement si n est impair.
3. Montrer que si G est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$, Alice a une stratégie gagnante si et seulement si n n'est pas multiple de 4.

⋆ **Exercice 31.** *Mots de longueur* $|G|$.

Étant donné une partie S d'un groupe G et un entier $k \in \mathbb{N}$, on note $S^k = \{s_1 s_2 \cdots s_k \,|\, s_1, \dots, s_k \in S\}$.

Soit G un groupe fini d'ordre n et $S \subseteq G$ contenant 1. Montrer que S^n est un sous-groupe de G.

⋆⋆ **Exercice 32.** *Lemme de Dicman.*

Soit G un groupe et $X \subseteq G$ un ensemble fini, stable par conjugaison, constitué d'éléments d'ordre fini.

1. Montrer que le sous-groupe engendré $\langle X \rangle$ est stable par conjugaison et fini.
2. Montrer que son cardinal est majoré par le produit des ordres des éléments de X, et que cette majoration est en général optimale.
3. Montrer que l'on ne peut pas se passer de l'hypothèse que X est stable par conjugaison.

Groupes cycliques, ordres des éléments

Exercice 33. *Produit de groupes monogènes ou cycliques.*

1. Soit G_1 et G_2 deux groupes cycliques. À quelle condition le groupe $G_1 \times G_2$ est-il cyclique ?
2. Soit K un groupe. À quelle condition le groupe produit $\mathbb{Z} \times K$ est-il monogène ?

Exercice 34. *Caractères d'un groupe cyclique.*

Étant donné un groupe G, on note $\widehat{G}$ l'ensemble des morphismes $G \to \mathbb{C}^\times$.

1. Montrer que, muni d'une loi de multiplication naturelle, $\widehat{G}$ est un groupe.
   Quelle propriété du groupe $\mathbb{C}^\times$ a-t-on utilisée au passage ?
2. Montrer que si G est cyclique, $\widehat{G}$ l'est aussi.
3. La question précédente reste-t-elle vraie avec le mot « cyclique » remplacé par le mot « monogène » ?

◦ **Exercice 35.** *Groupe sans sous-groupe propre.*

Soit G un groupe non trivial dont les seuls sous-groupes sont $\{1_G\}$ et G.

Montrer que G est cyclique, d'ordre premier.

◦ **Exercice 36.** *Égalités sur les ordres des éléments.*

Soit G un groupe et $x, y \in G$.

1. Montrer que si x est d'ordre fini, alors x^{-1} également, et que leurs ordres sont les mêmes.
2. Montrer que si x est d'ordre fini, alors yxy^{-1} également, et que leurs ordres sont les mêmes.
3. Montrer que si xy est d'ordre fini, alors yx également, et que leurs ordres sont les mêmes.

Exercice 37. *Ordres des éléments et des sous-groupes d'un groupe abélien.*

Soit G un groupe abélien. On note O(G) l'ensemble des ordres des éléments de G.

1. Montrer que O(G) est stable sous ppcm.
2. Montrer que la question précédente est fausse si l'on ne suppose pas G abélien.
3. Soit $E \subseteq \mathbb{N}^*$ un ensemble stable sous ppcm et par passage aux diviseurs. Construire un groupe abélien tel que $O(G) = E$.

Exercice 38. *Sous-groupes finis de* $\mathbb{C}^\times$. *Mines*

Montrer que tout sous-groupe fini du groupe multiplicatif $\mathbb{C}^\times$ est cyclique.

Exercice 39. *Groupes p-quasicycliques de Prüfer.*

Soit p un nombre premier et $G = \bigcup_{n\geq 1} \mathbb{U}_{p^n} \subseteq \mathbb{C}^\times$. Montrer que G est un sous-groupe de $\mathbb{C}^\times$ et en déterminer les sous-groupes. En déduire que G est *indécomposable*, c'est-à-dire qu'il n'est pas isomorphe à un produit $G_1 \times G_2$ avec $|G_i| > 1$.

Exercice 40. *Groupes divisibles.* *X*

Soit p premier. Un *p-groupe* est un groupe dont tous les éléments ont pour ordre une puissance de p.

Étant donné $k \in \mathbb{N}^*$, un groupe G est dit *k-divisible* si $\forall g \in G, \exists h \in G : g = h^k$.

1. Montrer que si G est un p-groupe p-divisible, alors G est soit trivial soit infini.
2. Donner un exemple de p-groupe non trivial qui soit p-divisible.
3. Montrer qu'un tel groupe est en fait k-divisible pour tout $k \in \mathbb{N}^*$.

⋆ **Exercice 41.** *Ordre multiplicatif.*

On fixe un nombre premier p, et un nombre entier k premier avec p. L'ordre d'un élément x dans un groupe sera noté $o(x)$, et on notera en particulier $\omega_n = o([k]_{p^n})$ l'ordre de $[k]_{p^n}$ dans le groupe multiplicatif $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

1. Soit $f : G \to G'$ un morphisme surjectif de groupes finis, et $x \in G$.
   Montrer que le quotient $\dfrac{o(x)}{o(f(x))}$ est un entier divisant $\dfrac{|G|}{|G'|}$.
2. En déduire $\forall n \in \mathbb{N}^*, \dfrac{\omega_{n+1}}{\omega_n} \in \{1, p\}$.
3. Montrer que la suite $\left(\dfrac{\omega_{n+1}}{\omega_n}\right)_{n\in\mathbb{N}}$ est stationnaire.
4. Montrer que le résultat de la question précédente reste vrai si l'on enlève l'hypothèse de primalité de p.

Exercice 42. *Produit de deux involutions.* *Lyon*

1. Montrer que toute rotation du plan est la composée de deux symétries orthogonales.
2. Soit X un ensemble fini.
   Montrer que toute permutation de X s'écrit $\sigma \circ \tau$, où $\sigma, \tau \in \mathfrak{S}(X)$ vérifient $\sigma^2 = \tau^2 = \mathrm{id}_X$.
3. Le résultat de la question précédente reste-t-il vrai pour un ensemble infini ?

Exercice 43. *Groupe diédral infini.*

Soit G un groupe infini engendré par deux éléments a, b d'ordre 2.

1. Montrer que $G = \langle ab\rangle \cup a\langle ab\rangle$, puis que ab est d'ordre infini.
2. Montrer que G est isomorphe au sous-groupe de $\mathfrak{S}(\mathbb{R})$ constitué des transformations affines de la forme $x \mapsto x + n$ et $x \mapsto n - x$, pour $n \in \mathbb{Z}$.

Exercice 44. *Groupe des homéomorphismes de* $[0, 1]$. *X*

On considère l'ensemble $\mathcal{H}$ des bijections continues $[0, 1] \to [0, 1]$.

1. Montrer qu'il s'agit d'un groupe pour la composition.
2. Soit G un sous-groupe fini de $\mathcal{H}$ fini. Montrer que $|G| \leq 2$.

Exercice 45. *Morphisme entre groupes cycliques.* *X*

Déterminer les morphismes $\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/13\mathbb{Z})$, où $\mathrm{Aut}(\mathbb{Z}/13\mathbb{Z})$ désigne les automorphismes du groupe additif $\mathbb{Z}/13\mathbb{Z}$.

Exercice 46. *Nilpotents dans un anneau commutatif fini.*

Soit A un anneau commutatif fini et $N \subseteq A$ l'ensemble des éléments nilpotents.

Montrer que $|N|$ divise $|A|$ et $|A^\times|$.

Exercice 47. *Sous-groupes d'indice fini.*

Soit G un groupe.

Un sous-groupe H de G est dit *d'indice fini* si l'ensemble G/H des classes à gauche modulo H est fini.

1. Montrer que si F est un groupe fini et que $f : G \to F$ est un morphisme de groupes, alors $\ker f$ est un sous-groupe d'indice fini qui est en outre *distingué*, c'est-à-dire que $\forall h \in \ker f, \forall g \in G, ghg^{-1} \in \ker f$.
2. Donner un exemple de groupe G possédant un sous-groupe d'indice fini H qui ne soit pas distingué.
3. Soit H un sous-groupe d'indice fini de G.
   Montrer qu'il existe un sous-groupe distingué d'indice fini N tel que $N \subseteq H$.
4. Montrer que l'intersection de deux sous-groupes d'indice fini est encore un sous-groupe d'indice fini.

Groupes finis

Exercice 48. *Classification des groupes de petit cardinal.*

1. Soit p un nombre premier et G un groupe d'ordre p. Montrer que G est cyclique.
2. Classer à isomorphisme près tous les groupes finis dont le cardinal est ≤ 7.

Exercice 49. *Groupes d'ordre* 8. *X (détaillé)*

Soit G un groupe de cardinal 8 non abélien.

1. Montrer qu'il existe un élément $x \in G$ d'ordre 4.
2. Soit $y \in G \setminus \langle x \rangle$. Montrer que x et y engendrent G, et en déduire que x et y ne commutent pas.
3. Montrer que $G = \langle x \rangle \sqcup y\langle x \rangle$, que $yxy^{-1} \in \langle x \rangle$, puis que $yxy^{-1} = x^{-1}$.
4. Montrer qu'il n'existe, à isomorphisme près, que deux groupes non abéliens d'ordre 8.

Exercice 50. *Sous-groupes d'indice 2.* *Lyon (détaillé)*

Soit G un groupe fini de cardinal $2n$.

1. Soit H un sous-groupe de G de cardinal n. Montrer que l'application
$$\varphi : \begin{cases} G \to & \mathbb{U}_2 \\ g \mapsto & \begin{cases} 1 & \text{si } g \in H \\ -1 & \text{si } g \notin H \end{cases} \end{cases}$$
   est un morphisme de groupes.
2. Utiliser la question précédente pour montrer que $(\mathbb{Z}/2\mathbb{Z})^d$ possède exactement $2^d - 1$ sous-groupes de cardinal 2^{d-1}.
3. Montrer qu'il est impossible que G possède exactement deux sous-groupes de cardinal n.

Δ **Exercice 51.** *Projecteur associé à un sous-groupe fini de* $GL_n(K)$.

Soit K un corps de caractéristique nulle.

1. Soit G un groupe fini.
   Montrer que, pour tout $g \in G$, l'ensemble $\{(h,k) \in G^2 \mid hk = g\}$ est de cardinal $|G|$.

2. Soit $G \subseteq GL_n(\mathbb{K})$ un sous-groupe fini. Montrer que la matrice $M = \frac{1}{|G|}\sum_{g\in G} g$ vérifie $M^2 = M$.
3. On note $I = \left\{v \in K^n \,\middle|\, \forall g \in G, g(v) = v\right\}$ l'ensemble des vecteurs *invariants sous* G. Montrer que $\operatorname{im} M = I$ et en déduire la valeur de $\frac{1}{|G|}\sum_{g\in G} \operatorname{tr}(g)$.

⋆ **Exercice 52.** *Groupes finis engendrant $M_n(\mathbb{C})$.*

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un sous-groupe fini $G \subseteq GL_n(\mathbb{C})$ tel que $\operatorname{Vect}(G) = M_n(\mathbb{C})$.

Exercice 53. *Extensions simples de sous-groupes de $\mathbb{C}^\times$.* *Mines modifié*

1. Soit G un sous-groupe fini de $GL_n(\mathbb{C})$ tel que $G \cap SL_n(\mathbb{C}) = \{I_n\}$.
   Montrer que G est cyclique.
2. Dans la suite de l'exercice, on considère des sous-groupes G de $GL_2(\mathbb{C})$ de cardinal 8.
   (a) Donner un exemple de tel groupe qui ne soit pas cyclique.
   (b) On suppose que $G \cap SL_2(\mathbb{C})$ a deux éléments. Montrer que G est abélien.
   (c) Construire un exemple où G n'est pas abélien et $|G \cap SL_2(\mathbb{C})| = 4$.
   (d) Peut-on construire un tel exemple vérifiant en outre $G \subseteq GL_2(\mathbb{R})$?

Exercice 54. *Théorème de Cauchy en 2.*

Soit G un groupe fini.

1. Montrer que $i : x \mapsto x^{-1}$ est une involution $G \to G$. Quels sont ses points fixes ?
2. Montrer que si l'ordre de G est pair, alors G possède un élément d'ordre 2.

♠ **Exercice 55.** *Théorème de Cauchy (1845).*

1. Soit G un groupe fini d'ordre n et p un nombre premier divisant n.
   (a) On considère l'ensemble $X = \left\{(g_0, g_1, \dots, g_{p-1}) \in G^p \,\middle|\, g_0 g_1 \cdots g_{p-1} = 1\right\}$. Quel est son cardinal ?
   (b) Deux p-uplets $(g_0, \dots, g_{p-1}), (h_0, \dots, h_{p-1}) \in X$ sont dits *cycliquement équivalents* s'il existe $k \in \mathbb{Z}$ tel que $\forall j \in \mathbb{Z}, g_j = h_{j+k}$, les indices étant à comprendre modulo p.
   Montrer que toutes les classes d'équivalence cyclique sont de cardinal 1 ou p.
   (c) En déduire le théorème de Cauchy : G contient des éléments d'ordre p.
2. Montrer que le théorème de Cauchy devient faux sans l'hypothèse de primalité de p.

♠ **Exercice 56.** *Indice du centre.*

Soit G un groupe fini et $Z(G) = \left\{g \in G \,\middle|\, \forall h \in G, gh = hg\right\}$ son *centre*.

Montrer que le quotient de cardinaux $\frac{|G|}{|Z(G)|}$ ne peut pas être un nombre premier.

Exercice 57. *Théorème de Jordan.*

1. Soit G un groupe fini et H un sous-groupe de G.
   Majorer le cardinal de $\bigcup_{x\in G} xHx^{-1}$ et en déduire $\bigcup_{x\in G} xHx^{-1} \neq G$.
2. **Application.** Soit H un sous-groupe de $\mathfrak{S}(d)$ tel que $\forall x, y \in [\![1, d]\!], \exists \sigma \in H : \sigma(x) = y$ (on dit que H est *transitif*). Montrer que si $H \neq \mathfrak{S}(d)$, alors il existe des éléments de H sans point fixe.
3. Constater que l'application est fausse pour les sous-groupes de $\mathfrak{S}(\mathbb{N})$ et en déduire que l'on ne peut pas enlever l'hypothèse de finitude de la première question.

Exercice 58. *Groupes d'ordre 2n (n impair).* *X*

Soit n un nombre impair, et G un groupe fini d'ordre $2n$.

1. Montrer que G possède un élément d'ordre 2.
2. En considérant $\varphi : \begin{cases} G \to & \mathfrak{S}(G) \\ g \mapsto & (x \mapsto gx), \end{cases}$ montrer que G possède un sous-groupe d'ordre n.
3. Montrer que la question précédente devient fausse si on ne suppose plus n impair.

Exercice 59. $|\mathrm{Aut}(G)| \neq 3$.

Soit G un groupe fini, dont on suppose (par l'absurde) qu'il possède exactement trois automorphismes.

1. On suppose provisoirement G abélien.
   (a) Montrer que $x \mapsto x^{-1}$ est un automorphisme, et en déduire $\forall x \in G, x^2 = 1$.
   (b) Montrer qu'il existe $r \in \mathbb{N}^*$ tel que G soit isomorphe au groupe additif $(\mathbb{Z}/2\mathbb{Z})^r$.
   (c) Aboutir à une absurdité.
2. On note $Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$ le centre de G. Montrer qu'il est impossible que $|G| = 3\,|Z(G)|$.
3. Vérifier que $\varphi : \begin{cases} G \to & \mathrm{Aut}(G) \\ g \mapsto & x \mapsto gxg^{-1} \end{cases}$ est un morphisme de groupes dont on déterminera le noyau, et en déduire que G est automatiquement abélien, ce qui conclut la démonstration.

Exercice 60. *Groupes d'ordre pq.*

1. Soit $p < q$ deux nombres premiers. Montrer que tout groupe abélien de cardinal pq est cyclique.
2. En exhibant un contre-exemple (avec p, q bien choisis), montrer que le résultat est faux si le groupe n'est plus supposé abélien.

♠ **Exercice 61.** *Groupe diédral.*

Soit $n \geq 3$. On note $D_{2n} = \{z \mapsto \omega z \mid \omega \in \mathbb{U}_n\} \cup \{z \mapsto \omega \overline{z} \mid \omega \in \mathbb{U}_n\}$.

1. Montrer que D_{2n} est un sous-groupe non abélien du groupe des similitudes du plan complexe, d'ordre $2n$.
2. Montrer que D_{2n} est l'ensemble des similitudes qui stabilisent $\mathbb{U}_n$.
3. Soit $\zeta_n = \exp\left(i\frac{2\pi}{n}\right)$. Déterminer l'ordre de $\rho : z \mapsto \zeta_n z$ et de $\sigma : z \mapsto \overline{z}$ et vérifier que $D_{2n} = \langle \rho, \sigma \rangle$.
4. Montrer que D_{2n} est engendré par deux éléments d'ordre 2.
5. On suppose que $p \geq 3$ est premier.
   Montrer que tout groupe d'ordre $2p$ est soit cyclique, soit isomorphe à D_{2p}.

⋆ **Exercice 62.** *Noyaux de Frobenius.* *X*

Soit N un groupe fini et $\varphi \in \mathrm{Aut}(N)$ tel que $\forall g \in N, \varphi(g) = g \Rightarrow g = 1$. On note n l'ordre de φ dans $\mathrm{Aut}(N)$.

1. Montrer que $\forall x \in N, x\varphi(x)\,\varphi^2(x) \cdots \varphi^{n-1}(x) = 1$.
2. Si $n = 2$, que peut-on dire de N ? Donner un exemple.
3. Si $n = 3$, montrer que pour tout $x \in N$, on a $x\varphi(x) = \varphi(x)\,x$.

Exercice 63. *Théorème de Frobenius sur les sous-groupes d'indice minimal (1895).*

Soit G un groupe fini. On note p le plus petit facteur premier de $|G|$ et on suppose qu'il existe un sous-groupe H de G de cardinal $|G|/p$.

1. Construire un morphisme de groupes $\varphi : G \to \mathfrak{S}(p)$ tel que $\forall g \in G, g \in H \Leftrightarrow \varphi(g) \in \mathrm{Stab}(1)$, où l'on a noté $\mathrm{Stab}(1) = \{\sigma \in \mathfrak{S}(p) \mid \sigma(1) = 1\}$ le *stabilisateur* de 1.
2. Montrer que $H = \ker \varphi$.

Δ **Exercice 64.** *Le « lemme préhistorique ».*

Soit A et B deux parties d'un groupe fini G. On suppose $|A| + |B| > |G|$.

1. Montrer que $G = \{ab \mid a \in A, b \in B\}$.
2. Montrer que la question précédente devient fausse si on remplace, dans l'hypothèse, l'inégalité stricte par une inégalité large.

Δ **Exercice 65.** *Inégalité de Dixon.*

Soit G un groupe fini non abélien. On note $Z(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ son *centre*.

1. Montrer que $|G| \geq 4\,|Z(G)|$.
2. Montrer que $\left|\{(x,y) \in G^2 \mid xy = yx\}\right| \leq \frac{5}{8}|G|^2$.
3. Interpréter cette inégalité en termes de variables aléatoires.

⋆⋆ **Exercice 66.** *Lemme de Brauer et Fowler (1955).* *ÉNS*

Soit G un groupe fini. On note I l'ensemble des éléments de G dont l'ordre est exactement 2.

1. Soit $\sigma, \tau \in I$. Montrer que σ et τ sont conjuguées, ou qu'il existe $\gamma \in I$ commutant à la fois avec σ et τ.
2. On suppose que I contient deux éléments non conjugués.
   Montrer qu'il existe $\delta \in I$ dont le *centralisateur* $C_G(\delta) = \{x \in G \mid x\delta = \delta x\}$ soit de cardinal $> |G|^{1/3}$.

Exercice 67. *Constante de doublement égale à* 1. *Ulm*

Soit G un groupe et $X \subseteq G$ une partie finie non vide telle que X et XX aient le même cardinal.

Montrer qu'il existe un sous-groupe H de G et un élément $x \in G$ tels que $X = xH$ et $H = x^{-1}Hx$.

Exercice 68. *Sous-groupe approximatif.* *ÉNS enrichi*

Soit G un groupe fini.

1. Soit X une partie de G telle que $|XX| < 2|X|$. Montrer que $XX^{-1} = X^{-1}X$.
2. Soit X une partie de G telle que $|XX^{-1}| < \frac{3}{2}|X|$. Montrer que $X^{-1}X$ est un sous-groupe de G.
3. Soit X une partie de G telle que $|XX| < \frac{3}{2}|X|$. Montrer que XX^{-1} est un sous-groupe de G.

Groupe symétrique

Exercice 69. *Carrés dans $\mathfrak{S}(n)$.*

Soit $n \geq 3$.

1. Le n-cycle $(1\ 2\ \cdots\ n)$ est-il le carré d'un élément de $\mathfrak{S}(n)$?
2. Vérifier que pour $n \leq 5$, $\{\sigma^2 \mid \sigma \in \mathfrak{S}(n)\} = \mathfrak{A}(n)$.
3. Pour $n \geq 6$, montrer que l'égalité précédente est fausse.

Exercice 70. *Partie génératrice de $\mathfrak{S}(n)$.*

Soit $n \geq 3$ et $k \in [\![2, n]\!]$. À quelle condition les permutations $(1\ 2\ \cdots\ n)$ et $(1\ k)$ engendrent-elles $\mathfrak{S}(n)$?

Exercice 71. *Transpositions engendrant le groupe symétrique.*

Montrer que si k transpositions engendrent $\mathfrak{S}(n)$, alors $k \geq n - 1$.

Exercice 72. *Les parties génératrices contraignent les morphismes : cas de $\mathfrak{S}(n)$.*

Soit $n \geq 3$.

1. Montrer que la signature est le seul morphisme $\mathfrak{S}(n) \to \mathbb{C}^\times$ envoyant $(1\ 2)$ sur -1.
2. Plus généralement, montrer qu'il n'y a que deux morphismes $\mathfrak{S}(n) \to \mathbb{C}^\times$.
3. Soit A un groupe abélien. Combien y a-t-il de morphismes $\mathfrak{S}(n) \to \mathrm{A}$?

Exercice 73. *Sous-groupe maximal.* *ÉNS*

On considère le sous-groupe $\mathrm{G} \subseteq \mathfrak{S}(n)$ constitué des permutations σ telles que $\sigma(1) = 1$.

Montrer que G est un sous-groupe maximal de $\mathfrak{S}(n)$, c'est-à-dire qu'il n'existe pas de sous-groupe H de $\mathfrak{S}(n)$ tel que $\mathrm{G} \subsetneq \mathrm{H} \subsetneq \mathfrak{S}(n)$.

Exercice 74. *Groupe de permutations abélien et transitif.* *ÉNS*

Soit $\mathrm{G} \subseteq \mathfrak{S}(n)$ abélien et *transitif* $(\forall 1 \leq i, j \leq n, \exists \sigma \in \mathrm{G} : \sigma(i) = j)$. Montrer que $|\mathrm{G}| = n$.

Exercice 75. *Isomorphismes exceptionnels.*

Étant donné un corps K et un entier $n \geq 2$, on note $\mathrm{P}^{n-1}(\mathrm{K})$ l'ensemble des droites vectorielles de K^n (c'est *l'espace projectif de dimension $n-1$ sur* K).

1. Construire un morphisme $\mathrm{GL}_n(\mathrm{K}) \to \mathfrak{S}\big(\mathrm{P}^{n-1}(\mathrm{K})\big)$ dont le noyau est $\big\{\lambda \mathrm{I}_n \,\big|\, \lambda \in \mathrm{K}^*\big\}$.
2. Montrer que $\mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe à $\mathfrak{S}(3)$.
3. Construire un morphisme surjectif $\mathrm{GL}_2(\mathbb{F}_3) \to \mathfrak{S}(4)$ dont le noyau est $\{\pm \mathrm{I}_2\}$.

Exercice 76. *Tout automorphisme de $\mathfrak{S}(4)$ est intérieur.* *Lyon*

Soit $f : \mathfrak{S}(4) \to \mathfrak{S}(4)$ un automorphisme de groupes. Montrer qu'il existe $g \in \mathfrak{S}(4)$ tel que

$$\forall x \in \mathfrak{S}(4), f(x) = gxg^{-1}.$$

Exercice 77. *Un comportement exceptionnel de $\mathfrak{S}(4)$.*

Construire un morphisme surjectif $\mathfrak{S}(4) \to \mathfrak{S}(3)$ et déterminer son noyau.

♠ **Exercice 78.** *Conjugaison des stabilisateurs.*

1. Soit X un ensemble et G un sous-groupe de $\mathfrak{S}(\mathrm{X})$.
   Pour tout $x \in \mathrm{X}$, on définit son *stabilisateur* $\mathrm{Stab}(x) = \big\{\sigma \in \mathrm{G} \,\big|\, \sigma(x) = x\big\}$.
   Montrer qu'il s'agit d'un sous-groupe de G.
2. Soit $x \in \mathrm{X}$ et $\sigma \in \mathrm{G}$. Montrer que $\mathrm{Stab}\big(\sigma(x)\big) = \sigma \mathrm{Stab}(x) \sigma^{-1}$.

♠ **Exercice 79.** *Formule noyau-image.*

Soit $f : \mathrm{G}_1 \to \mathrm{G}_2$ un morphisme de groupes, avec G_1 fini.

1. Montrer $|\mathrm{G}_1| = |\ker f| \times |\mathrm{im}\, f|$.
2. Donner un exemple où le groupe G_1 n'est pas isomorphe au groupe produit $(\ker f) \times (\mathrm{im}\, f)$.

Exercice 80. *Formule stabilisateur-orbite pour les sous-groupes de $\mathfrak{S}(\mathrm{X})$.*

Soit X un ensemble fini et G un sous-groupe de $\mathfrak{S}(\mathrm{X})$. Pour $x \in \mathrm{X}$, on définit

- son *orbite* $\mathrm{G}x = \big\{\sigma(x) \,\big|\, \sigma \in \mathrm{G}\big\}$;
- son *stabilisateur* $\mathrm{Stab}(x) = \big\{\sigma \in \mathrm{G} \,\big|\, \sigma(x) = x\big\}$.

1. Soit $x \in \mathrm{X}$. Montrer la *formule stabilisateur-orbite* $|\mathrm{G}| = |\mathrm{Stab}(x)| \cdot |\mathrm{G}x|$.

2. Expliquer pourquoi il existe $x_1, \dots, x_r \in X$ tels que $X = \bigsqcup_{j=1}^{r} Gx_j$ et en déduire *l'équation aux classes*

$$|X| = \sum_{j=1}^{r} \frac{|G|}{|\mathrm{Stab}(x_j)|}.$$

3. **Application aux p-groupes.** On suppose que le cardinal de G est une puissance d'un nombre premier p et on note $X^G = \{x \in X \mid \forall \sigma \in G, \sigma(x) = x\}$ l'ensemble des *points fixes globaux*.
Montrer $|X| \equiv |X^G| \pmod{p}$.

♠ **Exercice 81.** *Formule stabilisateur-orbite pour les actions de groupes.*

Cet exercice reprend le résultat principal du précédent, dans un cadre un peu plus général.

On considère un groupe fini G, un ensemble fini X, et un morphisme de groupes $\alpha : G \to \mathfrak{S}(X)$. On dit alors que le groupe G *agit* (ou *opère*) sur l'ensemble X. Pour plus de commodité, on notera, pour tout $g \in G$ et tout $x \in X$, $g \cdot x = \alpha(g)(x)$.

Soit $x \in X$, on définit

- son *orbite* $Gx = \{g \cdot x \mid g \in G\}$;
- son *stabilisateur* $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$.

Montrer la *formule stabilisateur-orbite* $|G| = |\mathrm{Stab}(x)| \cdot |Gx|$.

Exercice 82. *Applications théoriques de la formule stabilisateur-orbite.*

Soit G un groupe fini.

1. **Centralisateur d'un élément.** Soit $g \in G$.
Le *centralisateur* de g est le sous-groupe $C_G(g) = \{h \in G \mid gh = hg\}$.
Montrer que le nombre d'éléments de G conjugués à g est $\dfrac{|G|}{|C_G(g)|}$.
2. **Normalisateur d'un sous-groupe.** Soit H un sous-groupe de G.
Son *normalisateur* est $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.
   (a) Montrer que $N_G(H)$ est un sous-groupe de G contenant H.
   (b) Montrer que le nombre de sous-groupes conjugués à H est $\dfrac{|G|}{|N_G(H)|}$.

Exercice 83. *Le lemme qui n'est pas de Burnside.*

Soit X un ensemble fini et G un sous-groupe de $\mathfrak{S}(X)$.

1. Montrer que la relation $\sim$ définie sur X par $x_1 \sim x_2 \Leftrightarrow \exists \sigma \in G : \sigma(x_1) = x_2$ est une relation d'équivalence.

On appelle G-*orbite* toute classe d'équivalence pour cette relation d'équivalence.

2. Pour tout $\sigma \in G$, on note $\mathrm{Fix}(\sigma) = \{x \in X \mid \sigma(x) = x\}$. Montrer que le nombre moyen de points fixes d'un élément de G, c'est-à-dire $N = \dfrac{1}{|G|} \displaystyle\sum_{\sigma \in G} |\mathrm{Fix}(\sigma)|$, est exactement le nombre de G-orbites.
3. **Applications matricielles.** Pour toute permutation $\sigma \in \mathfrak{S}(n)$, on note $P_\sigma = \left(\mathbb{1}_{i=\sigma(j)}\right)_{1 \le i,j \le n} \in \mathrm{M}_n(\mathbb{Z})$ la *matrice de permutation associée*. Calculer $\displaystyle\sum_{\sigma \in \mathfrak{S}(n)} \mathrm{tr}(P_\sigma)$ et $\displaystyle\sum_{\sigma \in \mathfrak{S}(n)} \mathrm{tr}(P_\sigma)^2$.

Exercice 84. *Introduction à la structure des p-groupes.*

Soit p un nombre premier et G un *p-groupe* fini, c'est-à-dire un groupe fini dont l'ordre est une puissance de p.

On suppose G non trivial et on note $Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$ le *centre* de G.

1. En considérant le morphisme $\begin{cases} G \to & \mathfrak{S}(G) \\ g \mapsto & (x \mapsto gxg^{-1}), \end{cases}$ montrer que Z(G) est un groupe non trivial.
2. Montrer que tout groupe d'ordre p^2 est abélien.
3. Montrer que tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

Exercice 85. *Dénombrement déterminantal dans $\mathfrak{S}(n)$.*

1. En utilisant un déterminant, trouver les valeurs de $n \geq 1$ telles que $|\mathfrak{A}(n)| = |\mathfrak{S}(n) \setminus \mathfrak{A}(n)|$.
2. Calculer le déterminant $P(x) = \begin{vmatrix} x & 1 & \cdots & 1 \\ 1 & x & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & x \end{vmatrix}_{[n]}$ en fonction de $x \in \mathbb{R}$.
3. Étant donné $\sigma \in \mathfrak{S}(n)$, on note $\chi(\sigma)$ le nombre de points fixes de σ.
   Calculer $\sum_{\sigma \in \mathfrak{S}(n)} \varepsilon(\sigma)\chi(\sigma)$ et $\sum_{\sigma \in \mathfrak{S}(n)} \frac{\varepsilon(\sigma)}{\chi(\sigma)+1}$ à l'aide du déterminant précédent.
4. Interpréter et démontrer de façon combinatoire le résultat sur $\sum_{\sigma \in \mathfrak{S}(n)} \varepsilon(\sigma)\chi(\sigma)$.

Exercice 86. *Dénombrement de centralisateurs.*

On se place dans $\mathfrak{S}(9)$.

1. Combien de permutations commutent avec $(1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$?
2. Combien de permutations commutent avec $(1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$?

Exercice 87. *Permutations d'ordre p.* *Ulm*

Soit p un nombre premier. Combien y a-t-il d'éléments de $\mathfrak{S}(2p)$ d'ordre p ?

Exercice 88. *Permutations sans cycle long.* *Lyon*

On pose a_n le nombre d'éléments de $\mathfrak{S}(2n)$ dont tous les cycles sont de longueur $\leq n$.

Donner une expression pour a_n et trouver une constante $c > 0$ telle que $a_n \underset{n\to+\infty}{\sim} c(2n)!$.

Exercice 89. *Fonction g de Landau : asymptotique.* *ÉNS*

Pour $n \geq 1$, on note $g(n)$ l'ordre maximal d'un élément de $\mathfrak{S}(n)$. Montrer $\forall \varepsilon > 0, g(n) = O(e^{\varepsilon n})$.

Indications

Exercice 1.

1. On pourra commencer par vérifier que si $a^2, b^2 \in \mathrm{I}$, alors $(a+b)^3 \in \mathrm{I}$.
2. Commencer par déterminer $\sqrt{n\mathbb{Z}}$, en ne se laissant pas impressionner par la notation, trompeuse.
3. On pourra vérifier que l'inclusion problématique est vraie dans un anneau principal (grâce à la décomposition en facteurs irréductibles). Il faut donc chercher ailleurs...

Exercice 2.

1. On rappelle qu'un élément maximal (pour l'inclusion) dans un ensemble de parties $\mathscr{F}$ est une partie $\mathrm{X} \in \mathscr{F}$ telle que $\forall \mathrm{Y} \in \mathscr{F}, \mathrm{X} \subseteq \mathrm{Y} \Rightarrow \mathrm{X} = \mathrm{Y}$.
   - (i) ⇒ (ii) : montrer que l'union d'une suite croissante d'idéaux est un idéal ;
   - (ii) ⇒ (iii) : procéder par contraposée, et construire par récurrence une suite strictement croissante d'idéaux ;
   - (iii) ⇒ (i) : regarder l'ensemble des idéaux de type fini contenus dans I.
2. Dans un anneau de fonctions A (définies sur un ensemble E), on a un idéal $\mathrm{I}_\mathrm{V} = \left\{ f \in \mathrm{A} \,\middle|\, \forall p \in \mathrm{V}, f(p) = 0 \right\}$. Il n'est alors pas si difficile d'imaginer des suites strictement croissantes d'idéaux.

Exercice 3. C'est un calcul direct. Une manière de le faire (assurément pas la seule) est de remarquer que l'hypothèse équivaut à $\forall g \in \mathrm{G}, g^{-1} = g$.

Exercice 4. On pourra chercher à exprimer x et y comme des puissances du produit xy.

Exercice 5. On pourra commencer par exprimer $(ab)^{\ell+1}$ en fonction de $(ba)^\ell$.

Exercice 6. On peut montrer que $\mathrm{H}_1\mathrm{H}_2 = \mathrm{H}_2\mathrm{H}_1$ si et seulement si $\mathrm{H}_1\mathrm{H}_2$ est stable par $x \mapsto x^{-1}$. La stabilité par produit est alors un bonus.

Exercice 7.

1. On vérifie que $\mathrm{H}'\mathrm{K}$ est bel et bien un sous-groupe si les éléments de H' et de K commutent. On cherchera alors des exemples (très) simples où ça n'est pas le cas.
2. Un élément de $\mathrm{H} \cap \mathrm{H}'\mathrm{K}$ s'écrit sous la forme $h'k$, où $h' \in \mathrm{H}'$ et $k \in \mathrm{H} \cap \mathrm{K}$.

Exercice 8. On pourra montrer que si un ensemble est en bijection avec un groupe, il peut être lui aussi muni d'une structure de groupe.

Exercice 9. On pourra par exemple raisonner sur l'ordre des éléments.

Exercice 10. La décomposition est loin d'être exotique, mais il peut être rassurant de remplacer $\mathbb{R}$ par un groupe multiplicatif qui lui est isomorphe, pour éviter de mélanger des lois notées si différemment.

Exercice 11. Il est facile de construire un morphisme $\mathrm{G} \to \mathfrak{S}(n)$, et l'algèbre linéaire peut aider à montrer qu'il est bijectif.

Exercice 13. À chaque fois, tout morphisme f est trivial, les éléments de im f héritant du domaine de f des propriétés que les éléments non triviaux de $\mathbb{Z}$ ne possèdent pas.

Exercice 14. Quels sont les $g \in \mathrm{F}$ tels que $\forall n \in \mathbb{N}^*, \exists h \in \mathrm{F} \,:\, h^n = g$?

Exercice 15.

1. Trouver n éléments engendrant $\mathbb{Z}^n$. Ensuite, à l'aide de ces éléments, expliquer comment une « quantité d'information finie » permet de connaître entièrement un morphisme de groupes $\varphi : \mathbb{Z}^n \to \mathrm{F}$.
3. Montrer que $|\mathrm{Hom}(\mathrm{G},\mathrm{F})|$ est un *invariant d'isomorphisme*, c'est-à-dire que si G_1 et G_2 sont deux groupes isomorphes, alors $|\mathrm{Hom}(\mathrm{G}_1,\mathrm{F})| = |\mathrm{Hom}(\mathrm{G}_2,\mathrm{F})|$.

Exercice 16. La première question est une question de cours bien cachée : elle exploite directement la classification des symétries vectorielles vues en sup.

Pour la dernière question, on pourra commencer par déterminer le centre des deux groupes, et chercher à comparer leurs propriétés de théorie des groupes.

Exercice 17. Si le groupe est trop riche (par exemple $\mathrm{G} = \mathbb{Q}$), on se convaincra facilement que la fonction f ne peut pas être continue. On cherchera donc une construction très « théorie des ensembles ».

Exercice 18. On pourra considérer $\alpha = \inf\left(\mathrm{G} \cap \mathbb{R}_+^*\right)$ et distinguer suivant que cette borne inférieure est atteinte ou non.

Exercice 19. Le slogan est que deux éléments dans un groupe sont conjugués s'ils sont les mêmes à un changement de point de vue près. Autrement dit, ils doivent avoir les mêmes caractéristiques, avec éventuellement les « éléments caractéristiques » déplacés par l'élément qui effectue la conjugaison.

Dans cet esprit, on pourra par exemple vérifier que toutes les rotations du même angle (mais de centres différents) sont conjuguées.

Dans l'autre sens, il est facile de trouver un morphisme $\pi : \Sigma \to \mathbb{C}^*$, et le caractère abélien de $\mathbb{C}^*$ forcera π à valoir la même chose sur deux éléments conjugués.

Exercice 20. Dans la dernière question, on pourra utiliser le morphisme φ pour montrer que Γ est abélien.

Exercice 21.

2. Le point-clef est que $\mathfrak{A}(n)$ « mélange beaucoup » les éléments de $[\![1,n]\!]$. Par exemple, pour $n \geq 4$, il peut envoyer n'importe quel couple d'éléments distincts sur n'importe quel autre (on dit qu'il est 2-*transitif*).
3. On pourra munir G lui-même d'une structure de graphe.
4. Il faut faire des dessins, et ajouter des « fioritures » pour empêcher les symétries parasites. On pourra aussi contempler le drapeau de l'île de Man.

Exercice 22. On pourra commencer par trouver $n \in \mathbb{N}^*$ tel que $i, j \in \mathbb{U}_n$.

Exercice 23. Les classes de conjugaison de ce groupe sont étonnantes (et petites) : alors que I, J et K jouent des rôles complètement interchangeables, on peut vérifier qu'elles ne sont pas conjuguées.

Exercice 24. On pourra vérifier que tout morphisme $\mathbb{R} \to \mathbb{U}_m$, et tout morphisme $\mathbb{R}_+^* \to \mathbb{U}_m$ est trivial. La théorie des symétries vectorielles permet également de vérifier que $r = \mathrm{diag}(-1, 1, \dots, 1)$ et la matrice associée à la permutation $(1\ 2)$ sont semblables, c'est-à-dire conjuguées dans $\mathrm{GL}_n(\mathbb{R})$.

Le morphisme est alors entièrement déterminé par l'image de r, pour laquelle il n'y a qu'une ou deux possibilités suivant la parité de m.

Pour vérifier qu'il y a bel et bien un morphisme non trivial quand m est pair, on pensera au déterminant.

Exercice 25.

1. On pourra utiliser un morphisme surjectif $\mathbb{Z}^n \to \mathbb{Z}$, dont le noyau est isomorphe à $\mathbb{Z}^{n-1}$, pour mener à bien le « dévissage » nécessaire dans l'hérédité.

2. On pourra vérifier que toutes les transpositions $(k\ k+1)$ appartiennent au sous-groupe engendré par les deux éléments. Quel est le groupe que ces transpositions engendrent ?

Exercice 26. Pour la question 4(a), on pourra vérifier que si un tel sous-groupe contient une suite non nulle, il contient une suite qui est nulle partout, sauf en un point de $\mathbb{Z}$.

Exercice 27. La troisième question demande concrètement de construire une famille pas trop grande qui engendre le groupe G. Pour cela, on imposera une condition de non-redondance finalement assez faible. Il peut par ailleurs être utile de faire d'abord la dernière question.

Exercice 28. Il serait possible de se ramener à la théorie de la dimension en fixant un diviseur premier p de n et en considérant un morphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^r \to \mathbb{F}_p^r$ induit par la réduction modulo p. Il est cependant plus simple de montrer que pour toute partie finie $S \subseteq (\mathbb{Z}/n\mathbb{Z})^r$, $|\langle S\rangle| \leq n^{|S|}$.

Exercice 29. Un *sous-groupe maximal* $M \subseteq G$ est un sous-groupe strict de G tel que tout sous-groupe N vérifiant $M \subseteq N \subseteq G$ vérifie $N = M$ ou $N = G$.

1. Que se passe-t-il si Alice joue au premier coup un générateur d'un sous-groupe maximal d'ordre impair ?
2. Que se passe-t-il si tous les sous-groupes maximaux de G sont d'ordre pair ?

Pour le groupe symétrique, il est étonnamment facile de montrer que tous les sous-groupes maximaux sont d'ordre pair (pour $n \geq 4$), et cela donne une stratégie gagnante à Bob.

Exercice 30. On dira qu'un coup est *tranquille* si l'élément choisi appartient au sous-groupe engendré par les éléments choisis précédemment. On peut alors vérifier que si un joueur a toujours la possibilité de jouer un coup tranquille, il a une stratégie gagnante.

Si n est impair, on vérifiera que c'est le cas pour Alice. Sinon, Bob aura envie de jouer rapidement un élément d'ordre pair, et dans presque tous les cas, il pourra alors ne plus jouer que des coups tranquilles.

Exercice 31. Remarquer que le théorème redonne (la forme faible du) théorème de Lagrange, et qu'il pourrait donc être utile, mais aussi qu'il suffit de montrer la stabilité par produit de S^n : comment faire cela ? On pourra également considérer la suite croissante $(S^k)_{k\in\mathbb{N}}$ d'ensembles finis.

Exercice 32.

1. On pourra montrer que si un mot « $x_1^{m_1}x_2^{m_2}\cdots x_r^{m_r}$ » représentant un élément de G (avec $x_1, \dots, x_r \in X$) est le plus court possible (sans compter les exposants, c'est-à-dire que r est minimal) alors les lettres x_i sont distinctes.
2. En plus de l'argument de la question précédente, on pourra munir X d'un certain ordre et représenter les éléments de $\langle X\rangle$ par des mots « lexicographiquement minimaux ».

Exercice 33. Théorème chinois.

Exercice 34. Pour la dernière question, on pourra montrer que le groupe des morphismes $\mathbb{Z} \to \mathbb{C}^\times$ est en fait isomorphe à $\mathbb{C}^\times$ lui-même.

Exercice 35. On pourra montrer que tous les éléments non triviaux de G en sont des générateurs.

Exercice 36. Les deux premières questions sont immédiates. La troisième peut être vue comme une conséquence de la deuxième.

Exercice 37. On pourra chercher comme exemple un sous-groupe de $\mathbb{C}^\times$.

Exercice 38. Les théorèmes du cours permettent de montrer $G = \mathbb{U}_{|G|}$ sans trop se salir les mains.

Exercice 39. On pourra classer les sous-groupes de G et montrer qu'ils sont *totalement ordonnés* : étant donné deux tels sous-groupes H_1, H_2, on a $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.

Exercice 40. La troisième question est une conséquence d'un résultat plus général et plus simple : si k et p sont premiers entre eux, tout p-groupe est k-divisible.

Exercice 41.

3. Si $n \geq 1$ (ou $n \geq 2$ dans le cas exceptionnel $p = 2$), si $\omega_{n+1} = p\omega_n$, la puissance k^{ω_n} est congrue à 1 modulo p^n mais pas modulo p^{n+1}. On pourra en déduire que sa puissance p-ième $k^{\omega_{n+1}}$ est congrue à 1 modulo p^{n+1} mais pas modulo p^{n+2}.
4. Il faut s'armer de courage et du théorème chinois...

Exercice 42.

1. Faire un dessin.
2. S'inspirer du dessin précédent.
3. S'inspirer encore du dessin, et être un peu optimiste sur la généralisation de la décomposition en cycles disjoints à un élément de $\mathfrak{S}(X)$.

Exercice 43. Pour la deuxième question, on cherche deux involutions α et β sur lesquelles envoyer a et b, telles que $\alpha\beta$ soit d'ordre infini. Deux réflexions $x \mapsto m - x$ dont la composée est $x \mapsto x + 1$ conviennent. Il reste à montrer que cette définition peut donner naissance à un morphisme.

Exercice 44. On pourra montrer que $\mathscr{H}_+ := \{f \in \mathscr{H} \mid f \text{ croissante}\}$ est un sous-groupe de $\mathscr{H}$ *sans torsion*, c'est-à-dire qu'à part l'identité, tous ses éléments sont d'ordre infini.

Exercice 45. On pourra relier le groupe des automorphismes du groupe additif $\mathbb{Z}/13\mathbb{Z}$ et le groupe $(\mathbb{Z}/13\mathbb{Z})^\times$ des inversibles de l'anneau $\mathbb{Z}/13\mathbb{Z}$. On en déduira que $\mathrm{Aut}(\mathbb{Z}/13\mathbb{Z})$ est isomorphe au groupe additif $\mathbb{Z}/12\mathbb{Z}$.

Exercice 46. Il s'agit deux fois du théorème de Lagrange, en faisant un peu d'efforts pour identifier N à un sous-groupe de $A^\times$.

Exercice 47.

2. Il suffit de trouver un exemple avec G fini !
3. On pourra utiliser une numérotation $G/H = \{H, g_2H, \dots, g_rH\}$ pour définir un morphisme de groupes $f : G \to \mathfrak{S}(r)$ envoyant H dans $\mathrm{Stab}(1) = \{\sigma \in \mathfrak{S}(r) \mid \sigma(1) = 1\}$.
4. On peut utiliser la question précédente, ou montrer à la main l'inégalité $|G/(H_1 \cap H_2)| \leq |G/H_1| \times |G/H_2|$.

Exercice 48.

1. Pour la première question, on utilisera le théorème de Lagrange.
2. La première question traite tous les cardinaux sauf $n = 4$ et $n = 6$ mais, même dans ces cas, le théorème de Lagrange donne des contraintes.
   Dans le cas $n = 6$, on pourra par exemple montrer que si le groupe n'est pas cyclique, il existe un élément x d'ordre 3 et un élément y d'ordre 2 qui ne commutent pas. Dans ce cas, que vaut yxy^{-1} ?

Exercice 49. La question 3 entraîne que tout élément de G est un x^i ou yx^i, avec $i \in \{0, 1, 2, 3\}$. Mauvaise nouvelle : ces expressions se combinent mal. Bonne nouvelle : la connaissance de $yxy^{-1} = x^{-1}$ permet de comprendre comment elles se combinent, en la réécrivant $yx = x^{-1}y$ et en pratiquant allègrement un jeu de « saute-moutons ».

Exercice 50.

1. La difficulté (réelle) est de montrer que le produit de deux éléments de $G \setminus H$ est un élément de H (ce qui est très faux si on n'a pas l'hypothèse sur les cardinalités). Cela vient du fait que le complémentaire $G \setminus H$ est ici également une classe latérale gH.
2. Il est facile de dénombrer les morphismes $(\mathbb{Z}/2\mathbb{Z})^d \to \mathbb{U}_2$, en faisant attention à la notation : additive à gauche, multiplicative à droite.
3. L'ensemble $\mathrm{Hom}(G, \mathbb{U}_2)$ n'est pas juste un ensemble !

Exercice 51. On pourra se souvenir, voire redémontrer, que la trace d'un projecteur est son rang.

Exercice 52. Il y a plein de possibilités. Une d'entre elles est de remarquer que si G est le groupe des matrices de permutations, alors Vect(G) y est presque : il s'identifie à l'espace vectoriel (et même l'algèbre) produit $\mathscr{L}(H) \times \mathscr{L}(D)$, où $H = \left\{(x_1, \dots, x_n) \in \mathbb{C}^n \,\middle|\, x_1 + \cdots + x_n = 0\right\}$ est « l'hyperplan standard » de $\mathbb{C}^n$ et où $D = \mathrm{Vect}\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$.
On peut alors chercher à ruser et à trouver un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ isomorphe à $\mathfrak{S}(n+1)$.

Exercice 53.

1. L'hypothèse permet de trouver un morphisme de groupes injectif $\delta : G \to \mathbb{C}^\times$.
2. En (b), en reprenant le même morphisme que dans la première question, on montrera qu'il existe un morphisme de groupes surjectif $G \to \mathbb{U}_4$ dont le noyau est $G \cap \mathrm{SL}_2(\mathbb{C})$.
   Pour le dernier exemple, on pourra représenter le groupe diédral D_8 (groupe des symétries du carré) comme un groupe de matrices.

Exercice 54. Quand on a une involution i sur un ensemble fini X, on peut vérifier $|X| \equiv |X^i| \pmod 2$, où X^i est l'ensemble des points fixes de i.

Exercice 55. On va en fait montrer que le nombre de $g \in G$ tels que $g^p = 1$ est un multiple de p. Mais ils ne sont pas tous d'ordre p !

Exercice 56. Si le quotient de cardinaux était premier, on pourrait montrer que tout élément de G peut s'écrire sous la forme $g^i z$, avec $g \in G$ bien choisi et $z \in Z(G)$.

Exercice 57.

1. Tous les sous-groupes xHx^{-1} ont le même cardinal, mais l'union n'est pas disjointe.
2. Appliquer la question précédente au *stabilisateur* de 1 : $S = \mathrm{Stab}(1) = \left\{\sigma \in S \,\middle|\, \sigma(1) = 1\right\}$, après avoir identifié les $\rho S \rho^{-1}$ dans ce cas.

Exercice 58.

1. C'est le théorème de Cauchy pour $p = 2$.
2. En notant $\varepsilon : \mathfrak{S}(G) \to \{\pm 1\}$, montrer que $\ker(\varepsilon \circ \varphi)$ est bien d'ordre n.
3. On peut par exemple montrer que $\mathfrak{A}(4)$ n'a pas de sous-groupe d'ordre 6.

Exercice 59. Pour la question 1(a), on remarquera que l'hypothèse entraîne que l'identité est le seul automorphisme de carré trivial. Pour la question 1(b), le plus efficace est de munir le groupe d'une structure de $\mathbb{F}_2$-espace vectoriel.

Exercice 60. On utilisera le théorème de Cauchy pour considérer deux éléments, d'ordre p et q, respectivement. Comment interagissent les sous-groupes cycliques engendrés par ces deux éléments ?

Exercice 61. Pour la deuxième question, on pourra commencer par montrer que l'identité est la seule

similitude directe qui fixe 1 et ζ_n. Pour la dernière, on pourra utiliser le théorème de Cauchy.

Exercice 62. Pour la première question (la plus difficile), on pourra commencer par montrer que $x \mapsto x^{-1}\varphi(x)$ est une bijection $\mathrm{N} \to \mathrm{N}$, puis que si un élément de N est conjugué à son image par φ, il est en fait conjugué à un point fixe de φ, ce qui laisse peu de choix.

Exercice 63. Pour la première question, on pourra se souvenir de l'ensemble G/H des classes latérales. Pour la deuxième, on utilisera l'information arithmétique sur le cardinal de G pour montrer que $\ker\varphi$, qui est évidemment inclus dans H, lui est en fait égal.

Exercice 64. Pour la première question, on pourra montrer que $\forall g \in \mathrm{G}, \mathrm{A} \cap \left\{gb^{-1} \,\middle|\, b \in \mathrm{B}\right\} \neq \emptyset$.

Exercice 65.

1. On notera que le théorème de Lagrange montre l'inégalité avec 4 remplacé par 2. Il s'agit donc d'améliorer un peu l'argument.
2. La première question et le théorème de Lagrange montrent qu'au moins trois quarts des éléments de G ne commutent qu'avec une minorité (au sens large) des éléments de G...

Exercice 66.

1. La question porte en fait sur le groupe engendré $\langle\sigma,\tau\rangle$ (car elle doit être vraie si $\mathrm{G} = \langle\sigma,\tau\rangle$, et les autres cas sont plus faciles). Si l'on connait le groupe diédral, on se rend compte que l'élément $\sigma\tau \in \mathrm{G}$ va être crucial. Concrètement, on pourra faire une disjonction de cas suivant que l'ordre de cet élément est pair ou impair.
2. En posant M le cardinal maximal du centralisateur d'une involution, on pourra appliquer la question à deux involutions non conjuguées σ et τ, ou plutôt à σ et τ' parcourant la classe de conjugaison de τ. Cela permet de montrer l'inégalité $|\mathrm{G}| \leq (\mathrm{M}-1)\mathrm{M}^2$.

Exercice 67. On pourra commencer par le cas où $1 \in \mathrm{X}$.

L'inégalité $|\mathrm{X}| \leq |\mathrm{XX}|$ est évidente : le cas d'égalité force énormément d'égalités entre ensembles.

Exercice 68.

1. Pour $x, y \in \mathrm{X}$, que dire de $x\mathrm{X}$ et $y\mathrm{X}$?
2. On pourra minorer le nombre d'écritures de la forme $a^{-1}b$ que possède un élément de $\mathrm{X}^{-1}\mathrm{X}$. Cela permettra ensuite d'en choisir des « compatibles » pour montrer la stabilité par produit.

Exercice 69. Pour la première question, on pourra avantageusement prendre connaissance de la deuxième. Pour les deux dernières, on pensera à la décomposition en cycles disjoints.

Exercice 70. On pourra par exemple remarquer que si l'on colorie les six entiers de $[\![1,6]\!]$ de façon répétitive : bleu, blanc, rouge, bleu, blanc, rouge, alors $(1\ 4)$ et $(1\ 2\ \cdots\ 6)$ respectent le coloriage, au sens où deux éléments de la même couleur sont encore envoyés sur deux éléments de la même couleur. Ils ne peuvent donc pas engendrer $\mathfrak{S}(6)$.

Exercice 71. On pourra (montrer et) utiliser que si un graphe à n sommets est connexe, alors il a au moins $n-1$ arêtes.

Exercice 72. On utilisera le fait que toutes les transpositions sont conjuguées dans $\mathfrak{S}(n)$.

Exercice 73. On pourra commencer par montrer qu'un sous-groupe H tel que $\mathrm{G} \subsetneq \mathrm{H} \subseteq \mathfrak{S}(n)$ vérifie automatiquement $\forall i \in [\![1,n]\!], \exists\sigma \in \mathrm{H} \,:\, \sigma(1) = i$.

Exercice 74. Pour un sous-groupe transitif $\mathrm{H} \subseteq \mathfrak{S}(n)$, on peut vérifier que les *stabilisateurs* $\mathrm{S}_i = \left\{\sigma \in \mathrm{H} \,\middle|\, \sigma(i) = i\right\}$

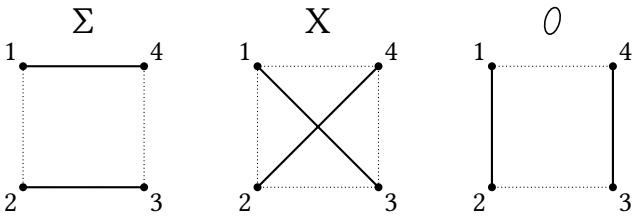
sont conjugués. C'est ici particulièrement contraignant.

Exercice 75. Étant donné $A \in GL_2(\mathbb{F}_p)$, il s'agit déjà de trouver $p+1$ « objets » que la matrice permute...

Exercice 76. À chaque élément $j \in [\![1,4]\!]$ correspond son *stabilisateur* $S_j \subseteq \mathfrak{S}(4)$: on pourra commencer par trouver $g \in \mathfrak{S}(4)$ tel que $\forall j \in [\![1,4]\!], f[S_j] = S_{g(j)}$.

En composant par la conjugaison par g^{-1}, il reste à montrer qu'un automorphisme de $\mathfrak{S}(4)$ stabilisant tous les S_j est en fait l'identité.

Exercice 77. On pourra contempler le dessin suivant, qui explique les trois façons de séparer en deux équipes les éléments de $[\![1,4]\!]$ ou, en jargon de théorie des graphes, les 1-*facteurs* du graphe K_4 :



- Σ : les équipes ont été faites pour que dans les deux cas, la somme vaille 5 ;
- X : les équipes ont été faites pour évoquer la lettre X ;
- *0* : les équipes ont été faites en respectant l'*0*rdre usuel des entiers.

Exercice 79.

1. C'est une application directe du lemme des bergers.
2. L'exemple minimal se fait avec $G_1 = \mathbb{Z}/4\mathbb{Z}$.

Exercice 80.

1. On appliquera le lemme des bergers à une application naturelle $G \to Gx$.
3. On remarquera que, modulo p, la plupart des termes de l'équation aux classes disparaissent.

Exercice 81. Le plus simple est de suivre la démonstration du cas $G \subseteq \mathfrak{S}(X)$, c'est-à-dire d'appliquer le lemme des bergers à une application naturelle $G \to Gx$.

Exercice 82. Dans les deux cas, on définira un ensemble X et un morphisme $G \to \mathfrak{S}(X)$ bien choisis. Il suffira alors d'appliquer la formule stabilisateur-orbite.

Exercice 83.

2. On pourra dénombrer de deux façons différentes $\{(\sigma, x) \in G \times X \mid \sigma(x) = x\}$ en utilisant au passage la formule stabilisateur-orbite.
3. Les deux calculs sont des applications directes de la question précédente à $G = \mathfrak{S}(n)$: dans un cas, $X = [\![1,n]\!]$; dans l'autre, $X = [\![1,n]\!]^2$.

Exercice 84.

1. On utilisera l'équation aux classes pour montrer un résultat plus fort : $|Z(G)|$ est un multiple de p.
2. On utilisera un exercice précédent (et classique) sur le centre d'un groupe fini.

Exercice 85. Pour le développement du déterminant, on pourra par exemple utiliser le caractère multilinéaire alterné.

Exercice 86. On pourra utiliser la formule de conjugaison dans $\mathfrak{S}(n)$:

$$\begin{aligned}\sigma \circ (i_{1,1}\ i_{1,2}\ \cdots\ i_{1,\ell_1})(i_{2,1}\ i_{2,2}\ \cdots\ i_{2,\ell_2}) \cdots (i_{r,1}\ i_{r,2}\ \cdots\ i_{r,\ell_r}) \circ \sigma^{-1} \\ = (\sigma(i_{1,1})\ \sigma(i_{1,2})\ \cdots\ \sigma(i_{1,\ell_1}))(\sigma(i_{2,1})\ \sigma(i_{2,2})\ \cdots\ \sigma(i_{2,\ell_2})) \cdots (\sigma(i_{r,1})\ \sigma(i_{r,2})\ \cdots\ \sigma(i_{r,\ell_r}))\end{aligned}$$

Exercice 87. Utiliser la décomposition en cycles disjoints.

Exercice 88. Il est plus facile de trouver une expression pour $(2n)! - a_n$: en effet, une permutation peut avoir au plus un cycle long, ce qui évite de commettre « l'erreur standard » en dénombrement.

Exercice 89. On pourra commencer par remarquer que le nombre de cycles **de longueurs différentes** d'une permutation de $\mathfrak{S}(n)$ est nécessairement $O(\sqrt{n})$.