Groupes : énoncés

Exercices CCINP

1) Soit G un groupe. Montrer que l'ensemble des automorphismes de groupe de G (i.e. l'ensemble des isomorphismes de groupe de G sur lui-même) est un groupe pour la composition. C'est le *groupe des automorphismes* de G, noté $\mathrm{Aut}(G)$. À quels groupes simples sont isomorphes les groupes $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$, $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ et $\mathrm{Aut}(\mathfrak{S}_3)$?

2) Le groupe des permutations de $\{1,2,3\}$ est-il cyclique ?

3) On travaille ici dans le groupe $\mathfrak{S}_{12}$ des permutations de $\{1,2,\dots,12\}$. Un élément σ de ce groupe sera noté

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & 11 & 12 \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(11) & \sigma(12) \end{pmatrix}$$

et si $i_1, i_2, \dots, i_k$ sont des entiers distincts compris entre 1 et 12, nous noterons $(i_1, i_2, \dots, i_k)$ le cycle $i_1 \to i_2 \to i_3 \to \cdots \to i_k \to i_1$. Nous avons par exemple :

$$(1,3,7,5,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 2 & 7 & 4 & 6 & 1 & 5 & 8 & 9 & 10 & 11 & 12 \end{pmatrix}$$

Décomposer la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 3 & 8 & 4 & 9 & 5 & 10 & 1 & 11 & 2 & 12 \end{pmatrix}$ en produit de cycles disjoints. Quel est l'ordre de σ ? Calculer σ^{2022}.

4) Soit E un ensemble et $\bullet$, Δ les deux lois internes

$$\forall A, B \in \mathcal{P}(E), \begin{cases} A \bullet B = (A \cup (E \setminus B)) \cap (B \cup (E \setminus A)) \\ A \Delta B = (A \cup B) \setminus (A \cap B) \end{cases}$$

Montrer que $(\mathcal{P}(E), \bullet)$ et $(\mathcal{P}(E), \Delta)$ sont des groupes abéliens isomorphes.

5) Montrer que tout élément de $\mathfrak{S}_n$ se décompose de façon unique, à l'ordre près, en produit de cycles dont les supports sont deux à deux disjoints.

Décomposer les permutations :

$$s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 6 & 5 & 7 & 4 & 2 \end{pmatrix},\ s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \text{ et } s_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}$$

Calculer $(s_3)^{2023}$.

6) Soient $f : X \to Y$ une bijection. Montrer que les groupes de permutations $\mathfrak{S}_X$ et $\mathfrak{S}_Y$ sont isomorphes.

7) Soit $f : G \longrightarrow G'$ un morphisme de groupe et soit $x \in G$ d'ordre fini n. Montrer que $f(x)$ est d'ordre fini, et que cet ordre divise n. En déduire les morphismes de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/13\mathbb{Z}$, puis de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.

8) Trouver tous les morphismes de groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$.

9) Soit G un sous-groupe fini de $(\mathbb{C}^*, \cdot)$ de cardinal n. Montrer que G est l'ensemble des racines n-ièmes de l'unité.

10) Donner un exemple de groupe de cardinal infini dont tous les éléments sont d'ordre fini.

11) Soit $n \in \mathbb{N}^*$ et φ le morphisme de groupe de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui à un entier k associe sa classe modulo n, notée $\overline{k}$. On considère un sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer qu'il existe un entier naturel m tel que $\varphi^{-1}(H) = m\mathbb{Z}$.

b) Montrer que m divise n.

c) Montrer que H est monogène et donner un élément qui l'engendre.

12) Le groupe $(\mathbb{Q}, +)$ est-il engendré par une partie finie ?

Exercices Mines-Centrale

13) Soient G et H deux groupes finis ; le produit $G \times H$ est muni de sa structure de groupe produit. Soient $x \in G$ et $y \in H$, d'ordres respectifs n et m. Montrer que (x, y) est d'ordre $n \vee m$. En déduire une condition nécessaire et suffisante pour que $G \times H$ soit cyclique.

14) Théorème de Lagrange : soit G un groupe fini et H un sous-groupe de G. Pour tout élément g de G, on note $gH = \{x \in G,\ \exists h \in H,\ gh\}$.

a) Montrer que pour tout $g \in G$, gH a même cardinal que H.

b) Montrer que pour $g_1, g_2 \in G$, ou bien $g_1H = g_2H$, ou bien $g_1H \cap g_2H = \emptyset$. En déduire qu'il existe un entier $k \in \mathbb{N}^*$ et des éléments $g_1, g_2, \ldots, g_k$ de G tels que les parties $g_1H, g_2H, \ldots, g_kH$ forment une partition de G.

c) Montrer que le cardinal de H divise le cardinal de G.

d) En déduire que pour tout élément g de G, l'ordre de g est un diviseur du cardinal de G.

15) Soit G un groupe fini dont les éléments autres que le neutre sont d'ordre 2.

a) Montrer que G est abélien. La loi de G sera donc notée additivement.

b) Montrer que G possède une structure canonique d'espace vectoriel sur le corps $\mathbb{Z}/2\mathbb{Z}$. En déduire que G est isomorphe, en tant que groupe, à une puissance du groupe cyclique $\mathbb{Z}/2\mathbb{Z}$.

16) Soit $(G, +)$ un groupe abélien, A et B deux parties finies de G.

a) Montrer que si $\mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G)$, alors $A + B = G$.

b) Montrer que $H = \{x \in G,\ A = x + A\}$ est un sous-groupe de G.

c) Montrer que $\mathrm{Card}(A + B) = \mathrm{Card}(A)$ si et seulement s'il existe $b \in G$ tel que $B \subset b + H$.

17) Soit G un groupe. On note A l'ensemble des éléments de G d'ordre fini impair. Montrer que A est non vide et que $x \longmapsto x^2$ définit une bijection de A sur lui-même.

18) Soit G un groupe et $x, y \in G$. Montrer que xy et yx ont même ordre.

19) Montrer que dans un groupe de cardinal impair, tout élément est un carré.

20) (Centrale 2012) Soit G un groupe multiplicatif de cardinal n et p un diviseur premier de n. On pose :

$$E = \{(x_1, \ldots, x_p) \in G^p,\ x_1 x_2 \ldots x_p = 1\}.$$

Pour $X = (x_1, \ldots, x_p) \in G^p$ et pour toute permutation $\sigma \in \mathfrak{S}_p$, on note $\sigma \cdot X = (x_{\sigma(1)}, \ldots, x_{\sigma(p)})$.

a) Pour $\sigma_1, \sigma_2 \in \mathfrak{S}_p$ et $X \in G^p$, que vaut $\sigma_1 \cdot (\sigma_2 \cdot X)$?

On note σ le cycle $(1, 2, \ldots, p)$ et, pour tout $X \in E$, l'*orbite de* X est l'ensemble $o(X) = \{\sigma^k \cdot X,\ k \in \mathbb{Z}\}$.

b) Montrer que E est de cardinal n^{p-1} et que pour tout $X \in E$, $o(X) \subset E$.

c) Montrer que pour tous X, Y dans E, on a soit $o(X) = o(Y)$, soit $o(X) \cap o(Y) = \emptyset$.

d) Montrer que pour tout $X \in E$, le cardinal de $o(X)$ est soit 1, soit p.

e) En déduire que G possède un élément d'ordre p.

21) (Mines 2014) Soit $(G, .)$ un groupe fini. On note $Z = \{x \in G,\ \forall y \in G,\ xy = yx\}$: c'est le *centre* de G. Le cardinal de Z peut-il être égal à la moitié (resp. au tiers) de celui de G ?

22) Soit E un ensemble non vide muni d'une loi de composition interne associative notée multiplicativement. On suppose que pour tout $(a, b) \in E^2$, il existe $(x, y) \in E^2$ tel que $ax = b$ et $ya = b$. Montrer que $(E, .)$ est un groupe.

23) Soit E un ensemble fini non vide et $\cdot$ une loi de composition associative sur G. Montrer que E possède un élément idempotent (i.e. un élément x tel que $x \cdot x = x$).

24) (Centrale) Pour $\sigma \in \mathfrak{S}_n$, on note $O(\sigma)$ l'ordre de la permutation σ. On note M_n le maximum des ordres des éléments de $\mathfrak{S}_n$. Pour des raisons évidentes, nous verrons un élément de σ comme une permutation de l'ensemble $\{0, 1, \ldots, n-1\}$; un tel élément sera représenté en Python par la liste $[\sigma(0), \ldots, \sigma(n-1)]$.

a) Écrire une fonction `compose` qui calcule la composée de deux permutations.

b) Écrire une fonction `ordre` qui calcule l'ordre d'une permutation.

On classe les éléments de $\mathfrak{S}_n$ dans l'ordre lexicographique. Ainsi, quand $n = 3$, nous avons :

$$(0, 1, 2) < (0, 2, 1) < (1, 0, 2) < (1, 2, 0) < (2, 0, 1) < (2, 1, 0)$$

Si $\sigma \in \mathfrak{S}_n \setminus \{(n-1, n-2, \ldots, 1, 0)\}$, on note $s(\sigma)$ la permutation qui suit σ pour cet ordre.

c) Écrire une fonction `calcul_k` qui, appliquée à une permutation σ renvoie le plus petit entier k tel que la suite $(\sigma(k), \sigma(k+1), \ldots, \sigma(n-1))$ est décroissante. Cet entier sera noté k_σ.

d) Quand k_σ est différent de 0, comment peut-on transformer σ en $s(\sigma)$? En déduire une fonction `suivant` qui, appliquée à (σ, k_σ) avec $k_\sigma \neq 1$, transforme σ en $s(\sigma)$.

e) Écrire une fonction `calcul_M` qui, appliquée à une entier n, renvoie M_n.

25) (Mines 2019) Soit $n \in \mathbb{N}^*$. Déterminer les morphismes de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$

26) (Centrale Python 2021) On note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$. Une permutation $x \in \mathfrak{S}_n$ sera représentée par la liste $[x(1), x(2), \ldots, x(n)]$. On sait qu'une telle permutation se décompose de façon unique (à l'ordre près) en produit de cycles disjoints : $x = c_1 \circ c_2 \circ \cdots \circ c_k$. On notera $\ell(x)$ la suite croissante des longueurs des cycles c_i (sans oublier les cycles de longueur 1). Par exemple, si $n = 10$ et $x = [3, 9, 5, 6, 10, 4, 7, 8, 2, 1] = (1, 3, 5, 10) \circ (2, 9) \circ (4, 6) \circ (7) \circ (8)$, on a $\ell(x) = (1, 1, 2, 2, 4)$.

Pour G un groupe fini de cardinal N et $x \in G$, on pose

$$p_G = \frac{\text{Card}\left(\{(x, y) \in G^2, xy = yx\}\right)}{N^2},\ C_x = \{y \in G, xy = yx\} \text{ et } p_x = \frac{\text{Card}(C_x)}{N}.$$

On dit que x *est conjugué à* y *dans* G s'il existe $z \in G$ tel que $y = zxz^{-1}$.

On admet que la relation « être conjugué » est une relation d'équivalence sur G. On note $\overline{x}$ la classe d'équivalence d'un élément x de G et N_G le nombre de classes d'équivalence.

a) Calculer les valeurs de $p_{\mathfrak{S}_1}$, $p_{\mathfrak{S}_2}$ et $p_{\mathfrak{S}_3}$.

b) Coder une fonction qui, appliquée à n, renvoie une permutation aléatoire (suivant la loi uniforme) de $[\![1, n]\!]$.

c) Coder une fonction qui approxime $p_{\mathfrak{S}_n}$ et tracer $p_{\mathfrak{S}_n}$ pour $n \in [\![1, 9]\!]$.

d) Soient x et y conjugués. Montrer que $p_x = p_y$, puis que $\text{Card}\left(\left\{s \in G, y = sxs^{-1}\right\}\right) = \text{Card}(C_x)$. En déduire une relation entre p_x et le cardinal de C_x, puis que $p_G = \dfrac{N_G}{N}$.

e) Soit $c = (a_1, \ldots, a_r)$ un r-cycle de $[\![1, n]\!]$. Pour $\sigma \in \mathfrak{S}_n$, montrer que $\sigma c \sigma^{-1}$ est un r-cycle que l'on déterminera. En déduire que deux permutations $x, y \in \mathfrak{S}_n$ sont conjuguées si et seulement si $\ell(x) = \ell(y)$. Calculer $p_{\mathfrak{S}_n}$ pour $1 \leq n \leq 5$.

27) (Mines 22) Soit p un nombre premier. On note $G_p = \{z \in \mathbb{C},\ \exists k \in \mathbb{N},\ z^{p^k} = 1\}$.

a) Montrer que G_p est un sous-groupe multiplicatif de $\mathbb{C}^*$.

b) Montrer que tout sous-groupe strict de G_p est cyclique.

c) Montrer que G_p n'est pas engendré par une partie finie.

Exercices X-ENS

28) Montrer que si G est un sous-groupe strict de $(\mathbb{R}, +)$, $\mathbb{R} \setminus G$ est non dénombrable.

29) (ENS 2014) Soit G un sous-groupe abélien de $\mathfrak{S}_n$ tel que pour $a, b \in \{1, \ldots, n\}$, il existe $g \in G$ tel que $g(a) = b$. Montrer qu'un élément g de G distinct du neutre n'a aucun point fixe. En déduire que G est de cardinal n.

30) (P 2019) Le groupe symétrique $\mathfrak{S}_{\mathbb{N}}$ est-il dénombrable ?

31) Soit $(G, .)$ un groupe et $\sim$ une relation d'équivalence sur G. Pour $x \in G$, on note $\overline{x}$ la classe d'équivalence de x pour $\sim$. L'ensemble quotient est $G_{/\sim} = \{\overline{x},\ x \in G\}$ et l'application $p :\ x \longmapsto \overline{x}$ est appelée la *projection canonique*.

On note $\mathfrak{S}_n$ le groupe symétrique d'indice n, i.e. l'ensemble des bijection de $E_n = \{1, 2, \ldots, n\}$ sur lui-même muni de la composition. Une permutation x de $\mathfrak{S}_n$ est dite paire si sa signature est égale à 1 : on note $\mathfrak{A}_n$ l'ensemble des permutations paires de E_n. $\mathfrak{A}_n$ est le groupe alterné d'indice n (c'est le noyau du morphisme "signature").

a) On souhaite munir $G_{/\sim}$ d'une structure de groupe telle que p soit un morphisme de groupe. Montrer que c'est possible si et seulement si $\sim$ est compatible avec la loi de G, i.e. si :

$$\forall x, y, x', y' \in G,\ \left.\begin{array}{c} x \sim x' \\ y \sim y' \end{array}\right\} \Longrightarrow xy \sim x'y'.$$

b) Montrer que si $\sim$ est compatible avec la loi de G, la partie $H = \overline{1}$ vérifie :

(i) H est un sous-groupe de G ;

(ii) $\forall x \in G,\ \forall y \in H,\ x^{-1}yx \in H$ (on dit que H est *est stable par automorphisme intérieur*) ;

(iii) $\forall x, y \in G,\ x \sim y \Longleftrightarrow x^{-1}y \in H$.

Si H est un sous-groupe de G vérifiant (ii), on dit que c'est un *sous-groupe distingué de G*.

c) Montrer qu'un sous-groupe H de G est distingué si et seulement si $xH = Hx$ pour tout $x \in G$.

d) Soit H un sous-groupe distingué de G. Montrer que la relation $\sim$ définie par :

$$\forall x, y \in G,\ x \sim y \Longleftrightarrow x^{-1}y \in H$$

est une relation d'équivalence sur G compatible avec la loi de G et que pour tout $x \in G$, $\overline{x} = xH = Hx$.

e) Quels sont les sous-groupes distingués de $G = \mathfrak{S}_3$? Pour $n \in \mathbb{N}^*$, montrer que $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$. Donner un exemple de sous-groupe distingué de $GL_n(K)$ où K est un corps commutatif.

f) On travaille dans le groupe $G = \mathfrak{A}_5$. Calculer le cardinal de la classe de conjugaison $\mathcal{C}(x) = \{y^{-1}xy,\ y \in \mathfrak{A}_5\}$ dans les cas suivants :

- $x = (1,2)(3,4)$ (composée des transpositions $(1,2)$ et $(3,4)$) ;
- $x = (1,2,3)$ (3-cycle) ;
- $x = (1,2,3,4,5)$ (5-cycle).

En déduire que $\mathfrak{A}_5$ n'a pas d'autres sous-groupes distingués que $\{Id\}$ et lui-même. On dit que $\mathfrak{A}_5$ est *simple* : cette propriété prouve qu'il n'existe pas de méthode de résolution des équations polynomiales de degré 5 par radicaux.

32) (X 2019) Soit $(G,.)$ un groupe fini de cardinal n. Pour $x \in G$, on note $\overline{x} = \{g^{-1}xg,\ g \in G\}$ la *classe de conjugaison* de x. On dit que x est *ambivalent* si $x^{-1} \in \overline{x}$.

a) Montrer que si une classe de conjugaison contient un élément ambivalent, tous ses éléments le sont.

b) Soit $x \in G$. En considérant la surjection $\varphi :\ g \in G \longmapsto g^{-1}xg \in \overline{x}$, montrer que pour tout $y \in \overline{x}$, $\mathrm{Card}\left(\left\{g \in G,\ g^{-1}xg = y\right\}\right) = \frac{n}{\mathrm{Card}(\overline{x})}$.

c) Pour $g \in G$, on note $\rho(g)$ le nombre de solutions de l'équation $x^2 = g$. Montrer que $\dfrac{1}{n}\displaystyle\sum_{g\in G}\rho(g)^2$ est le nombre de classes de conjugaison ambivalentes de G. On pourra écrire, pour $g \in G$, $\rho(g) = \displaystyle\sum_{x\in G}\mathbf{1}_{x^2=g}$.

33) (X 2020) a) Soit $(G,+)$ un groupe abélien fini. Déterminer la somme s des éléments de G.

b) On suppose que $G = \mathfrak{S}_3$. Quels sont les éléments de G que l'on peut écrire comme produits de tous les éléments de G dans un ordre quelconque, chaque élément apparaissant exactement une fois ?

34) (X 2020) a) Donner un exemple de triplet (G,x,y) où G est un groupe multiplicatif avec $x, y \in G$ d'ordres finis et xy d'ordre infini.

b) Soient G un groupe et $\leq$ une relation d'ordre total sur G telle que :

$$\forall x,y,z \in G,\ (x \leq y) \Longrightarrow (zx \leq zy \text{ et } xz \leq yz)\,.$$

Soient S une partie de G stable par conjugaison, $g \in G$, $r \in \mathbb{N}^*$ et $(s_1,\dots,s_r) \in S^r$ tels que $g = s_1 \dots s_r$. Montrer qu'il existe $(s'_1,\dots,s'_r) \in S^r$ tel que $g = s'_1 \cdot \dots \cdot s'_r$ et $s'_1 \leq \dots \leq s'_r$.

35) (L) Soit n un entier supérieur ou égal à 2.

a) Soit $\sigma \in \mathfrak{S}_n$ telle que $\sigma^2 = Id$. Dénombrer les $\theta \in \mathfrak{S}_n$ telles que $\sigma \circ \theta = \theta \circ \sigma$.

b) Montrer que, si $n \neq 6$, un automorphisme du groupe $\mathfrak{S}_n$ envoie une transposition quelconque sur une transposition.

c) Montrer que pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs, i.e. les automorphismes de la forme $\sigma \longmapsto \tau^{-1} \circ \sigma \circ \tau$ pour $\tau \in \mathfrak{S}_n$.

36) (X) Soit $(G,\cdot)$ un groupe fini de cardinal n. On note $\widehat{G}$ l'ensemble des morphismes de groupe de $(G,\cdot)$ dans $(\mathbb{C}^*,\times)$. Les éléments de $\widehat{G}$ sont appelés les *caractères* de G.

a) Montrer que $\widehat{G}$ est un groupe pour la multiplication ordinaire des fonctions.

b) Montrer que si $\chi \in \widehat{G}$ n'est pas le morphisme trivial, $\displaystyle\sum_{g\in G}\chi(g) = 0$.

c) Si χ est χ' sont deux éléments distincts de $\widehat{G}$, montrer que $\displaystyle\sum_{g\in G}\overline{\chi(g)}\chi'(g) = 0$.

d) Montrer que $\mathrm{Card}(\widehat{G}) \leq n$.

e) Pour $g \in G$, on note δ_g l'application qui à $\chi \in \widehat{G}$ associe $\chi(g)$. Montrer que l'application $\delta_g \in \widehat{\widehat{G}}$ et que $\delta :\ g \longmapsto \delta_g$ est un morphisme de G sur $\widehat{\widehat{G}}$.

f) On suppose maintenant que G est abélien. Montrer que δ est un isomorphisme et en déduire le cardinal de $\widehat{G}$.

37) (X 2023) L'objectif de l'exercice est de caractériser les groupes de cardinal 2023.

a) Montrez qu'il existe deux groupes non isomorphes G_1 et G_2 de cardinal 2023.

b) Prouvez le lemme suivant : tout groupe G de cardinal p^2 avec p premier est isomorphe soit à $(\mathbb{Z}/p\mathbb{Z})^2$, soit à $\mathbb{Z}/p^2\mathbb{Z}$.

c) Soit G un groupe de cardinal 2023. En supposant l'existence d'un morphisme surjectif $\phi : G \longrightarrow \mathbb{Z}/17\mathbb{Z}$, montrer que G est isomorphe à G_1 ou à G_2.

d) Montrez enfin qu'un tel morphisme existe et conclure.

Groupes : corrigés

Exercices CCINP

1) $\mathrm{Aut}(G)$ est un sous-groupe du groupe $(S_G, \circ)$ des permutations de G :

- l'application identité est un automorphisme ;
- la composée de deux automorphismes de groupe est un automorphisme de groupe ;
- l'inverse d'un automorphisme de groupe est un automorphisme de groupe.

Comme 1 engendre $\mathbb{Z}/3\mathbb{Z}$, un automorphisme φ de ce groupe est entièrement déterminé par $\varphi(1)$. Comme 1 est d'ordre 3, son image par φ est également d'ordre 3 ; on a donc *a priori* deux possibilités : $\varphi(1) = 1$ ou $\varphi(1) = 2 = -1$. Réciproquement, les applications $Id : x \longmapsto x$ et $-Id = x \longmapsto -x$ sont des automorphismes de$\mathbb{Z}/3\mathbb{Z}$. On en déduit que $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = \{Id, -Id\}$, qui est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (tout groupe de cardinal 2 est isomorphe à $\mathbb{Z}/2\mathbb{Z}$).

De la même façon, un automorphisme φ de $\mathbb{Z}/4\mathbb{Z}$ est déterminé par la donnée de $\varphi(1)$, qui ne peut valoir que 1 ou -1. Comme ci-dessus, $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = \{Id, -Id\} \sim \mathbb{Z}/2\mathbb{Z}$.

Notons $x_1 = (1,2,3)$ et $x_2 = (1,3,2)$ les deux éléments d'ordre 3 de $\mathcal{S}G_3$. De même, notons $y_1 = (1,2)$, $y_2 = (2,3)$ et $y_3 = (3,1)$ ses trois éléments d'ordre 2. Comme $\mathcal{S}G_3$ est engendré par $(x_1, y1)$, un morphisme φ de $\mathfrak{S}_3$ est entièrement caractérisé par $\varphi(x_1)$ et $\varphi(y_1)$. A priori, $\varphi(x_1)$ peut être égal soit à x_1, soit à x_2 ; de même, $\varphi(y_1)$ peut-être égal soit à y_1, soit à y_2, soit à y_3. On obtient fastidieusement 6 applications possibles, décrites par le tableau suivant (on fait le calcul en remarquant par exemple que $x_2 = x_1 \circ x_1$, $y_2 = x_2 \circ y_1$ et $y_3 = x_1 \circ y_1$) :

	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
1	1	1	1	1	1	1
x_1	x_1	x_1	x_1	x_2	x_2	x_2
x_2	x_2	x_2	x_2	x_1	x_1	x_1
y_1	y_1	y_2	y_3	y_1	y_2	y_3
y_2	y_2	y_3	y_1	y_3	y_1	y_2
y_3	y_3	y_1	y_2	y_2	y_3	y_1

Très fastidieusement, on montre que ces 6 applications sont des automorphismes. On peut aller un peu plus vite en reconnaissant ces applications : pour chaque $\sigma \in \mathfrak{S}_3$, l'application $\varphi_\sigma : x \longmapsto \sigma \circ x \circ \sigma^{-1}$ est un automorphisme de $\mathfrak{S}_3$. Un calcul encore fastidieux montre que ces six applications sont deux à deux distinctes : ce sont donc les sic applications répertoriées dans le tableau ci-dessus. Nous avons ainsi montré qu'il existe 6 automorphismes de $\mathfrak{S}_3$. On peut montrer que $\mathrm{Aut}(\mathfrak{S}_3)$ est isomorphe à $\mathfrak{S}_3$ de deux façons :

- c'est un groupe de cardinal 6 non commutatif : il est isomorphe à $\mathfrak{S}_3$ (un groupe de cardinal 6 est soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$, soit isomorphe à $\mathfrak{S}_3$) ;
- remarquer que l'application $\sigma \longmapsto \varphi_\sigma$ est un isomorphisme de groupe.

2) Le groupe $\mathfrak{S}_3$ n'est pas cyclique car il n'est pas commutatif : $(1,2,3) \circ (1,2) = (1,3)$ et $(1,2) \circ (1,2,3) = (2,3)$, en notant $(a_1, a_2, \ldots, a_k)$ le cycle qui envoie a_1 sur a_2, a_2 sur a_3, …, a_k sur a_1.

3) Nous obtenons les cycles suivant :

- σ envoie 1 sur 6, puis 6 sur 9 et 9 sur 1 ;
- σ envoie 2 sur 7, puis 7 sur 5, puis 5 sur 4, puis 4 sur 8, puis 8 sur 10, puis 10 sur 11 et 11 sur 2 ;

- σ laisse fixe les deux derniers points 3 et 12.

Cela donne $\sigma = (1,6,9) \circ (2,7,5,4,8,10,11)$. On en déduit que σ est d'ordre $3 \wedge 7$, soit 21, puis $\sigma^{2020} = \sigma^4$, car $2020 \equiv 4$ [mod] 21. Cela donne :

$$\begin{aligned}
\sigma^{2020} &= (1,6,9)^4 \circ (2,7,5,4,8,10,11)^4 \\
&= (1,6,9) \circ (2,8,7,10,5,11,4) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 8 & 3 & 2 & 11 & 9 & 10 & 7 & 1 & 5 & 4 & 12 \end{pmatrix}
\end{aligned}$$

4) Pour montrer que $(\mathcal{P}(E), \Delta)$ est un groupe, on va le mettre en isomorphisme avec un groupe simple : on remarque que $\mathcal{P}(E)$ est en bijection avec $\{0,1\}^E$, par le biais de l'application qui à une partie A de E associe sa fonction indicatrice 1_A. En identifiant $\{0,1\}$ à $\mathbb{Z}/2\mathbb{Z}$, $\{0,1\}^E$ devient un groupe commutatif. La loi $\bigtriangleup$ est alors la loi correspond à la somme dans $\{0,1\}^E$: pour A, B parties de E, on a :

$$\forall x \in E,\ (1_A + 1_B)(x) = \begin{cases} 1 & \text{si } 1_A(x) \neq 1_B(x) \\ 0 & \text{si } 1_A(x) = 1_B(x) \end{cases}$$

ce qui s'écrit bien $1_{A \bigtriangleup B} = 1_A + 1_B$.

Ainsi, comme $\left(\{0,1\}^E, +\right)$ est un groupe abélien, $(\mathcal{P}(E), \bigtriangleup)$ en est un.

L'application $A \longrightarrow E \setminus A$ est ensuite un isomorphisme de $(\mathcal{P}(E), \bigtriangleup)$ sur $(\mathcal{P}(E), \bullet)$, ce qui prouve que $(\mathcal{P}(E), \bullet)$ est également un groupe

5) C'est une question de cours ; $\sigma \in \mathfrak{S}_n$ étant fixée, on définit la relation d'équivalence $\sim$ sur $\{1, 2, \ldots, n\}$ par :

$$\forall i, j \in \{1, 2, \ldots, n\},\ i \sim j \iff \exists k \in \mathbb{N},\ \sigma^k(i) = j.$$

La classe de i est appelée l'orbite de i. La restriction de σ à une orbite est une permutation circulaire. En notant $C_1, \ldots, C_k$ les différentes orbites non réduites à un singleton, on pose :

$$\forall j \in \{1, \ldots, k\},\ \sigma_j(i) = \begin{cases} \sigma(i) & \text{si } i \in C_j \\ i & \text{sinon} \end{cases}$$

Chaque σ_j est un cycle de support C_j et σ est la composée de ces cycles.

Les orbites de s_1 sont les parties $\{1,8,2\}$, $\{3\}$, $\{4,6,7\}$ et $\{5\}$, donc :

$$s_1 = (1,8,2) \circ (4,6,7)$$

On trouve de la même façon :

$$s_2 = (1,6) \circ (2,5) \circ (3,4) \text{ et } s_3 = (1,5) \circ (2,8,6,4) \circ (3,9,7).$$

On en déduit :

$$(s_3)^{100} = (1,5)^{100} \circ (2,8,6,4)^{100} \circ (3,9,7)^{100} = (3,9,7)$$

puisque $(1,5)$, $(2,8,6,4)$ et $(3,9,7)$ sont d'ordres 2, 4 et 3. Plus généralement, l'ordre d'une permutations est le p.p.c.m. des longueurs des cycles de sa décomposition en produit de cycles disjoints : s_3 est donc d'ordre 12 et $(s_3)^{100} = (s_3)^4$.

6) L'application qui a σ associe $f \circ \sigma \circ f^{-1}$ est un isomorphisme de groupe de $\mathfrak{S}_X$ sur $\mathfrak{S}_Y$.

7) Les groupes G et H étant quelconques, nous noterons multiplicativement leurs lois.

On a $f(x)^n = f(x^n) = f(1) = 1$, donc $f(x)$ est d'ordre fini et son ordre divise n.

Soit f est un morphisme de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/13\mathbb{Z}$ (attention : les lois sont maintenant notées additivement). L'élément 1 de $\mathbb{Z}/7\mathbb{Z}$ est d'ordre 7 donc son image $f(1)$ est d'ordre un diviseur de 7. Comme tous les éléments non nuls de $\mathbb{Z}/13\mathbb{Z}$ sont d'ordre 13 et que 7 ne divise pas 13, on en déduit que $f(1) = 0$, puis que $f = 0$.

Réciproquement, l'application nulle est bien un morphisme de groupe de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/13\mathbb{Z}$.

Soit f est un morphisme de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$. L'élément 1 de $\mathbb{Z}/3\mathbb{Z}$ est d'ordre 3 donc son image est d'ordre un diviseur de 3. Les seuls éléments de $\mathbb{Z}/12\mathbb{Z}$ dont l'ordre divise 3 sont 0, 4 et 8. On a donc trois cas possibles :

- $f = 0$;
- $f(0) = 0$, $f(1) = 4$ et $f(2) = f(1) + f(1) = 8$;
- $f(0) = 0$, $f(1) = 8$ et $f(2) = f(1) + f(1) = 4$.

Réciproquement, ces trois applications sont des morphismes de groupe de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.

8) Pour tout $p \in \mathbb{Z}$, on note $\overline{p}$ la classe de p modulo n.

Si φ est un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^*$, $\varphi(\overline{1})^n = \varphi(n\,\overline{1}) = \varphi(\overline{0}) = 1$, donc $\varphi(\overline{1})$ est une racine n-ième de l'unité. Réciproquement, si ξ est l'une des n-racines n-ième de l'unité, on défini l'application φ_ξ par :

$$\forall p \in \mathbb{Z},\ \varphi_\xi(\overline{p}) = \xi^p.$$

Cette application est bien définie (si $p \equiv\ q \bmod n$, $\xi^p = \xi^q$) et c'est un morphisme :

$$\forall p, q \in \mathbb{Z},\ \varphi_\xi(\overline{p} + \overline{q}) = \varphi_\xi(\overline{p+q}) = \xi^{p+q} = \xi^p\,\xi^q = \varphi_\xi(\overline{p})\,\varphi_\xi(\overline{q}).$$

Il existe ainsi n morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^*$. L'ensemble G des morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^*$ est un groupe pour la loi produit et l'application $\xi \longmapsto \varphi_\xi$ est un isomorphisme de $\mathbb{U}_n$ (groupe des racines n-ièmes de l'unité) sur G. Ainsi, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

9) Notons n le cardinal de G. On a $z^n = 1$ pour tout $z \in G$ (les éléments d'un groupe fini sont d'ordre finis et leur ordre divise le cardinal du groupe). On en déduit que $G \subset \mathbb{U}_n$, puis que $G = \mathbb{U}_n$, puisque ces deux ensembles sont de même cardinal n.

10) L'ensemble $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est un groupe pour la loi + et tout élément de ce groupe est d'ordre 2 (sauf l'élément neutre qui est d'ordre 1) :

$$\forall (x_n)_{n\geq 0} \in G,\ (x_n)_{n\geq 0} + (x_n)_{n\geq 0} = (x_n + x_n)_{n\geq 0} = (0)_{n\geq 0}.$$

11) a) H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et φ est un morphisme de groupe, donc $\varphi^{-1}(H)$ est un sous-groupe de Z : il existe donc un entier $m \in \mathbb{N}$ tel que $\varphi^{-1}(H) = m\mathbb{Z}$.

b) Comme $\varphi(n) = \overline{0} \in H$, $n \in \varphi^{-1}(H)$, donc $m \,|\, n$.

c) Comme φ est surjective, $H = \varphi(\varphi^{-1}(H)) = \varphi(m\mathbb{Z}) = \{k\,\overline{m}, k \in \mathbb{Z}\}$. On en déduit que $\overline{m}$ engendre H, qui est donc cyclique.

On peut remarquer, en écrivant $n = md$, que $\overline{m}$ est d'ordre d ; H est donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$ avec $d = \dfrac{n}{m}$. Ainsi, tout sous-groupe cyclique d'un groupe cyclique est cyclique. Plus précisément, un groupe cyclique de cardinal n possède un unique sous-groupe de cardinal m quand m divise n.

Pour les amateurs de quotient, on peut ensuite démontrer que tout quotient d'un groupe cyclique est cyclique : si G est cyclique de cardinal n et si H est un sous-groupe de cardinal m (m diviseur quelconque de n), le quotient de G par H est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

12) Si $A = \left\{ \dfrac{a_i}{b_i},\ 1 \leq i \leq k \right\}$ est une partie finie de $\mathbb{Q}$, le groupe qu'elle engendre s'écrit :

$$< A >= \left\{ \alpha_1 \frac{a_1}{b_1} + \alpha_2 \frac{a_2}{b_2} + \cdots + \alpha_k \frac{a_k}{b_k}, \alpha_1, \ldots, \alpha_k \in \mathbb{Z} \right\} \subset \left\{ \frac{\alpha}{b_1 b_2 \ldots b_k},\ \alpha \in \mathbb{Z} \right\}$$

et A n'engendre pas $\mathbb{Q}$: en choisissant un entier b premier avec $b_1 b_2 \ldots b_k$, le rationnel $\dfrac{1}{b}$ n'est pas élément de $< A >$.

Exercices Mines-Centrale

13) On a

$$\begin{aligned} (x,y)^p = 1_{G\times H} &\iff (x^p, y^p) = (1_G, 1_H) \iff \big(x_p = 1_G \text{ et } y^p = 1_H\big) \\ &\iff \big(n \,|\, p \text{ et } m \,|\, p\big) \iff n \vee m \,|p \end{aligned}$$

donc (x, y) est d'ordre $n \wedge m$.

Si G et H sont finis, de cardinaux respectifs N et M, on a en particulier :

$$\text{ordre}(x, y) = n \vee m \leq nm \leq NM.$$

Ainsi, $G \times H$ est cyclique si et seulement s'il contient un élément (x, y) d'ordre NM, c'est-à-dire si et seulement s'il existe $x \in G$ et $y \in H$ d'ordres n et m tels que $n \vee m = nm = NM$, ce qui signifie que $n = N$, $m = M$ et $N \wedge M = 1$.

Ainsi, $G \times H$ est cyclique si et seulement si G et H sont cycliques de cardinaux premiers entre eux.

14) a) L'application $h \longmapsto gh$ est une bijection de H sur gH, donc gH a même cardinal que H.

b) Si $g_1H \cap g_2H$ contient un élément g, on peut écrire $g = g_1h_1 = g_2h_2$ avec $h_1, h_2 \in H$. On a alors :

$$\forall h \in H,\ g_1 h = g_1 h_1 h_1^{-1} h = g_2 \underbrace{h_2 h_1^{-1} h}_{\in H} \in g_2 H$$

donc $g_1H \subset g_2H$, et par symétrie $g_1H = g_2H$. Ainsi, les parties g_1H et g_2H sont soient égales, soient disjointes.

On construit la famille $(g_1, \ldots, g_k)$ par itération : on pose $g_1 = 1$; si $P_1 = g_1H = G$, la construction est terminée. Sinon, on choisit $g_2 \in G \setminus P_1$: comme $g_2 \in g_2H$ et $g_2 \notin g_1H$, les parties g_1H et g_2H sont disjointes. Si $P_2 = g_1H \cup g_2H = G$, la construction est terminée. Sinon, on choisit $g_3 \in G \setminus P_2$ et g_1H, g_2H, g_3H sont des parties disjointes. Comme G est fini et que les cardinaux des P_i croissent strictement, cette construction s'arrête et la famille $(g_i)_{1\leq i\leq k}$ obtenue vérifie les conditions imposées.

c) On en déduit que $\text{Card}(G) = \displaystyle\sum_{i=1}^{k} \text{Card}(g_iH) = k\,\text{Card}(H)$: le cardinal de H divise celui de G.

d) Si $g \in G$, avec G fini, g est d'ordre fini k et le groupe engendré par g est de cardinal k, donc k divise le cardinal de G.

Remarque : on peut faire une preuve directe de ce résultat quand G est abélien ; en notant a le produit de tous les éléments de G (l'ordre n'intervient pas car G est abélien), on a (l'application $g \longmapsto g^{-1}$ est une bijection) :

$$a = \prod_{g\in G} g = \prod_{g\in G} g^{-1} = \left(\prod_{g\in G} g \right)^{-1} = a^{-1}$$

donc $a = 1$.

Pour $g_0 \in G$, l'application $g \longmapsto g_0 g$ est bijective, donc un nouveau changement d'indice donne :

$$1 = \prod_{g \in G} g = \prod_{g \in G} g_0 g = g_0^{\mathrm{Card}(G)} \prod_{g \in G} g = g_0^{\mathrm{Card}(G)}$$

Ainsi, l'ordre de g_0 divise $\mathrm{Card}(G)$.

15) a) Pour tout $x \in G$, on a $x^2 = 1$, donc $x^{-1} = x$. Ainsi, pour $x, y \in G$, $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$ et G est abélien. On note donc la loi $+$ à partir de maintenant.

b) $(G, +)$ est déjà un groupe abélien. On n'a pas le choix pour définir la loi externe ; on pose :

$$\forall \alpha \in \mathbb{Z}/2\mathbb{Z},\ \forall x \in G,\ \alpha\, x = \begin{cases} 0 & \text{si } \alpha = 0 \\ x & \text{si } \alpha = 1 \end{cases}$$

On a alors :

- pour tout $x \in G$, $1.x = x$;
- pour tous $\alpha \in \mathbb{Z}/2\mathbb{Z}$ et $x, y \in G$, $\alpha(x+y) = \left\{ \begin{array}{ll} 0 & \text{si } \alpha = 0 \\ x+y & \text{si } \alpha = 1 \end{array} \right\} = \alpha x + \alpha y$;
- pour tous $\alpha, \beta\mathbb{Z}/2\mathbb{Z}$ et $x \in G$, $\alpha(\beta x) = \left\{ \begin{array}{ll} 0 & \text{si } \alpha = 0 \text{ ou } \beta = 0 \\ x & \text{si } \alpha = \beta = 1 \end{array} \right\} = (\alpha\beta)x$;
- pour tous $\alpha, \beta \in \mathbb{Z}/2\mathbb{Z}$ et $x \in G$, $(\alpha + \beta)x = \alpha x + \beta x$ en distinguant les 4 cas possibles (et en utilisant $x + x = 0$).

Comme G est fini, G est de dimension finie d. On en déduit que l'espace vectoriel G est isomorphe à l'espace vectoriel $(\mathbb{Z}/2\mathbb{Z})^d$; en particulier, le groupe $(G, +)$ est isomorphe au groupe $\left((\mathbb{Z}/2\mathbb{Z})^d, +\right)$.

16) a) Soit $g \in G$. On cherche $a \in A$ et $b \in B$ tels que $a + b = g$, i.e. $a = g - b$. Ceci signifie que les parties A et $g - B$ ont un élément commun, ce qui est évident car $\mathrm{Card}(A) + \mathrm{Card}(g - B) = \mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G)$.

b) Il suffit de le vérifier :

- $0 \in H$ car $0 + A = A$;
- si $x, y \in H$, $(x - y) + A = (x - y) + (y + A) = x + (-y + y + A) = x + A = A$ donc $x - y \in H$.

c) Si $B = b + H$ avec $b \in G$, on $A + b = A + B$:

- $0 \in H$, donc $b \in B$ et $A + b \subset A + B$;
- si $c \in A + B$, on peut écrire $c = a + b + h$ avec $h \in H$, et donc $c = \underbrace{(a + h)}_{\in A} + b \in A + b$.

On en déduit que $\mathrm{Card}(A + B) = \mathrm{Card}(A + b) = \mathrm{Card}(A)$.

Supposons que $\mathrm{Card}(A + B) = \mathrm{Card}(A)$. Si B est vide, $A + B$ est vide et A est vide ; on a donc $H = G$ et on peut choisir b quelconque. Sinon, on peut choisir $b \in B$. Nous allons montrer que $B \subset b + H$. Les applications $a \longmapsto a + b$ et $a \longmapsto a + b'$ sont des bijections de A sur $A + B$ (elle sont injectives et les deux ensembles ont le même cardinal fini), l'application $a \longmapsto a + b' - b$ est une bijection de A sur lui-même, donc $b' - b \in H$, ce qui signifie que $b' \in b + H$.

17) 1 est d'ordre 1, donc A est non vide.

Soit x un élément de A, d'ordre $2p+1$. On a :

$$\forall q \in \mathbb{Z},\ (x^2)^q = 1 \iff x^{2q} = 1 \iff 2p+1 \,|\, 2q \iff 2p+1 \,|\, q$$

car 2 est premier avec $2p+1$. On en déduit que x^2 est d'ordre $2p+1$: il est élément de A. L'application $\varphi :\ x \longmapsto x^2$ est donc bien définie de A dans A.

On a d'autre part

$$x = x^{2p+1-2p} = x^{-2p} = \left(x^2\right)^{-p}.$$

Ainsi, si x (d'ordre $2p+1$) et y (d'ordre $2q+1$) sont deux éléments de A tels que $x^2 = y^2$, on a :

- $2p+1 = \text{ordre}(x^2) = \text{ordre}(y^2) = 2q+1$, donc $p = q$;
- $x = \left(x^2\right)^{-p} = \left(y^2\right)^{-p} = \left(y^2\right)^{-q} = y$

donc φ est injective.

Si $y \in A$, d'ordre $2p+1$, on a :

$$\forall q \in \mathbb{Z},\ (y^{-p})^q = 1 \iff y^{-pq} = 1 \iff 2p+1 \,|\, -pq \iff 2p+1 \,|\, q$$

car $2p+1$ et p sont premiers entre eux (on a la relation de Bézout $(2p+1) - 2p = 1$). Ainsi, $x = y^{-p}$ est d'ordre $2p+1$, donc $x \in A$, et $\varphi(x) = y^{-2p} = y$: φ est surjective.

La réciproque de $x \longmapsto x^2$ est l'application $y \longmapsto y^{-p}$, avec $p = \dfrac{\text{ordre}(y) - 1}{2}$.

18) On a $(yx)^{n+1} = y(xy)^n x$. On en déduit que si $(xy)^n = 1$, alors $(yx)^{n+1} = yx$, soit $(yx)^n = 1$ en simplifiant par yx. Ainsi, $\{n \in \mathbb{N},\ (xy)^n = 1\} \subset \{n \in \mathbb{N},\ (yx)^n = 1\}$, puis $\{n \in \mathbb{N},\ (xy)^n = 1\} = \{n \in \mathbb{N},\ (yx)^n = 1\}$ par symétrie, ce qui signifie que xy et yx ont même ordre (cet ordre pouvant être fini ou infini).

19) Si G est un groupe de cardinal $2n+1$ et si $x \in G$, x est d'ordre fini et son ordre divise $2n+1$, donc $x^{2n+1} = 1$. On en déduit que $\left(x^{n+1}\right)^2 = x^{2n+2} = x$ et x est un carré.

20) a) On a, pour $\sigma_1, \sigma_2 \in \mathfrak{S}_p$ et $X = (x_1, \ldots, x_p) \in G^p$:

$$\sigma_1 \cdot (\sigma_2 \cdot X) = \sigma_1 \cdot (\underbrace{x_{\sigma_2(1)}}_{=y_1}, \ldots, \underbrace{x_{\sigma_2(p)}}_{=y_p}) = (y_{\sigma_1(1)}, \ldots, y_{\sigma_1(p)}) = (x_{\sigma_2(\sigma_1(1))}, \ldots, x_{\sigma_1(\sigma_2(p))}) = (\sigma_2 \circ \sigma_1) \cdot X.$$

$$\sigma^i \cdot (\sigma^j \cdot X) = \sigma^{j+i} \cdot X = \sigma^{i+j} \cdot X.$$

b) L'application $(x_1, \ldots, x_p) \longmapsto (x_1, \ldots, x_{p-1})$ est un bijection de E sur G^{p-1} (l'unique antécédent de $(x_1, \ldots, x_{p-1})$ est $(x_1, \ldots, x_{p-1}, x_p)$ avec $x_p = x_{p-1}^{-1} \ldots x_1^{-1}$). Le cardinal de E est donc égal à n^{p-1}.

Si $X = (x_1, \ldots, x_n) \in E$, on a $\sigma \cdot X = (x_2, \ldots, x_p, x_1)$ et $x_2 x_3 \ldots x_p x_1 = x_1^{-1} \underbrace{x_1 x_2 \ldots x_p}_{=1} x_1 = 1$, donc $\sigma \cdot X \in E$.

Une récurrence immédiate donne $\forall k \in \mathbb{N},\ \sigma^k \cdot X \in E$, puis $\forall k \in \mathbb{Z},\ \sigma^k \cdot X \in E$ puisque $\{\sigma^k,\ k \in \mathbb{Z}\} = \{\sigma^k,\ 0 \leq k < p\}$ (σ est d'ordre p).

c) Soient $X, Y \in E$ tels que $o(X) \cap o(Y) \neq \emptyset$. Il existe donc $k_1, k_2 \in \mathbb{Z}$ tels que $\sigma^{k_1} \cdot X = \sigma^{k_2} \cdot Y$. Pour tout $Z = \sigma^k \cdot X \in o(X)$, on a :

$$Z = \sigma^k \cdot X = \sigma^{k-k_1+k_2} \cdot Y$$

donc $o(X) \subset o(Y)$, puis $o(X) = o(Y)$ par symétrie. Ainsi, soit $o(X) = o(Y)$, soit $o(X) \cap o(Y) = \emptyset$.

Comme chaque élément X de E appartient à $o(X)$, on en déduit que E est la réunion disjointe des orbites.

d) Soit $X \in E$. Comme $\sigma^p = Id$, on peut écrire $o(X) = \{\sigma^k \cdot X,\ 0 \leq k \leq p-1\}$. Si cette partie n'est pas de cardinal p, il existe i, j tels que $0 \leq i < j \leq p-1$ et $\sigma^i \cdot X = \sigma^j \cdot X$; on a alors $\sigma^q \cdot X = X$ avec $q = j - i$. Comme p est premier et

$1 \leq q \leq p-1$, p et q sont premier entre eux ; par le théorème de Bézout, il existe u, v dans $\mathbb{Z}$ tels que $up + vq = 1$. On en déduit que $\sigma = \sigma^{up+vq} = (\sigma^q)^v$, ce qui donne $\sigma \cdot X = X$. En effet, on montre facilement par récurrence le résultat :

$$\forall v \in \mathbb{N},\ (\sigma^q)^v \cdot X = X$$

puis

$$\forall v \in \mathbb{Z}^-,\ X = (\sigma^q)^v \cdot \left((\sigma^q)^{-v} \cdot X\right) = (\sigma^q)^v \cdot X$$

On a donc $\sigma \cdot X = X$, puis par récurrence $\sigma^k \cdot X = X$ pour tout $k \in \mathbb{N}$, soit $o(X) = \{X\}$. Ainsi, $o(X)$ est soit de cardinal p, soit de cardinal 1.

Autre preuve : prolongeons la suite finie X en une suite infinie $\widetilde{X} = (x_i)_{i \geq 1}$ de période p. La plus petite période de $\widetilde{X}$ est un diviseur de p, c'est donc soit 1, soit p. Dans le premier cas, X est constante et $o(X)$ est de cardinal 1 ; dans le second cas, $o(X)$ est de cardinal p (si on avait $\sigma^i \cdot X = \sigma^j \cdot X$ avec $0 \leq i < j \leq p-1$, on aurait $\widetilde{X}$ de période $j - i$).

e) Pour $x \in G$, notons X_x le p-uplet constant $(x, \ldots, x)$.

Les orbites sont deux à deux disjointes et leur réunion est égale à E (tout élément X de E est dans l'orbite $o(X)$) : elles forment donc une partition de E. Il existe ainsi $k \in \mathbb{N}^*$ et $X_1, \ldots, X_k \in E$ tels que $E = \bigsqcup_{k=i}^{k} o(X_i)$. Si $x_1, \ldots, x_N$ est l'ensemble des éléments d'ordre p de G, les éléments $X_1, X_{x_1}, X_{x_2}, \ldots, X_{x_N}$ sont exactement les éléments de E dont les orbites sont de cardinal 1 ($o(X)$ est un singleton si et seulement si X est de la forme X_x, et $X_x \in E$ si et seulement si $x^p = 1$, i.e. si et seulement si $x = 1$ ou x est d'ordre p). Comme les autres orbites sont de cardinal p, on en déduit :

$$n^{p-1} = \mathrm{Card}(E) \equiv (1 + N) \bmod p$$

Comme p divise n et $p - 1 \geq 1$, on a $N \equiv p - 1 \bmod p$, donc N est non nul (on a même $N \geq p - 1$, ce qui n'est pas très utile car si x est d'ordre p, les éléments x^i, pour $1 \leq i \leq p-1$ sont distincts et d'ordre p). Nous avons donc démontré que dans tout groupe de cardinal fini n, il existe un élément d'ordre p pour tout diviseur premier p de n.

21) a) Supposons que $2\,\mathrm{Card}(Z) = \mathrm{Card}(G) = 2n$. En choisissant $y \in G \setminus Z$, les parties Z et yZ sont disjointes et de cardinal n, donc $G = Z \cup yZ$. L'élément y commute avec tous les éléments de Z et avec tous les éléments de yZ (si $x \in Z$, $xy = yx$ et $y(yx) = y(xy) = (yx)y$) : on en déduit que $y \in Z$, ce qui est absurde.

b) Supposons que $3\,\mathrm{Card}(Z) = \mathrm{Card}(G) = 3n$. On choisit une nouvelle fois $y \in G \setminus Z$; le sous-groupe H engendré par $Z \cup \{y\}$ est alors de cardinal au moins $2n$ (il contient les deux parties disjoints Z et yZ) ; comme le cardinal de H divise celui de G, on a $H = G$ ($3n$ est le seul diviseur de $3n$ supérieur ou égal à $2n$). L'ensemble

$$C = \{x \in G,\ xy = yx\}$$

est alors un sous-groupe de G contenant Z et y : il contient donc H ; ainsi, $C = G$ et $y \in Z$: c'est absurde.

Nous avons montré que $\dfrac{\mathrm{Card}(G)}{\mathrm{Card}(Z)}$ ne peut ni être égal à 2, ni être égal à 3. On peut avoir un quotient égal à 4 : c'est le cas pour le groupe des quaternions $(\mathbb{H}_8, \cdot)$, défini de la façon suivante :

- $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$;
- 1 est l'élément neutre neutre ;
- $i^2 = j^2 = k^2 = -1$;
- $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$;
- pour tous $x, y \in \{1, i, j, k\}$, $(-x)y = x(-y) = -(xy)$ et $(-x)(-y) = xy$.

On peut avec un peu de courage vérifier que $\mathbb{H}_8$ est un groupe de cardinal 8, dont le centre Z est réduit à $\{-1, 1\}$: le rapport des cardinaux est bien égal à 4.

22) Comme E est non vide, on peut choisir $a \in E$. En appliquant l'hypothèse avec $b = a$, il existe e et f dans E tels que $ae = a$ et $fa = a$.

Pour $b \in A$, il existe x et y dans E tels que $ax = b$ et $ya = b$. On a alors :

$$be = (ya)e = y(ae) = ya = b \text{ et } fb = f(ax) = (fa)x = ax = b$$

donc

$$\forall b \in E,\ be = b \text{ et } fb = b.$$

On en déduit (avec $b = f$ et $b = e$) que $fe = f$ et $fe = e$, d'où $e = f$. Ainsi e est neutre pour le produit de E.

Si $b \in E$, il existe x et y dans E tels que $bx = e$ et $yb = e$: il faut montrer que $x = y$; il suffit d'écrire :

$$y = ye = y(bx) = (yb)x = ex = x$$

Nous avons donc montré que tout élément est inversible : E est bien un groupe.

23) Nous pouvons définir :

$$\forall a \in E,\ \forall n \in \mathbb{N}^*,\ a^n = \begin{cases} a & \text{si } n = 1 \\ a \cdot a^{n-1} & \text{si } n \geq 2 \end{cases}$$

La loi $\cdot$ étant associative, nous avons :

$$\forall n, m \in \mathbb{N}^*,\ a^{n+m} = a^n \cdot a^m.$$

Fixons $a \in E$ (E est non vide). Comme $\mathbb{N}^*$ est infini et E fini, il existe $n \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$ tels que $a^{n+p} = a^n$. Nous avons alors, par récurrence immédiate :

$$\forall k, m \in \mathbb{N},\ a^{k+n+pm} = a^{k+n}.$$

Nous allons alors chercher deux entiers $k, m \geq 0$ tels que $k+n+pm = 2(k+n)$, ce qui donnera $x^2 = x$ en posant $x = a^{k+n}$. Cela revient donc à trouver (k, m) tels que $pm = k + n$. On choisit donc $p \in \mathbb{N}$ assez grand pour avoir $pm \geq n$, puis on pose $k = pm - n \in \mathbb{N}$: l'élément $x = a^{k+n}$ est idempotent.

24) a), b) et c) Ces trois fonctions ne posent pas de problème :

```
def compose(s,t):
    return([s[t[i]] for i in range (len(s))])

def ordre(s):
    Id = [i for i in range(len(s))]
    n = 1
    t = s
    while t != Id:
        t = compose(t,s)
        n += 1
    return(n)

def calcul_k(s):
    k = len(s)-1
    while k != 0 and s[k-1]>s[k]:
        k -= 1
    return(k)
```

d) Regardons l'exemple suivant :

$$\begin{array}{cccccccccccccc} [0 & , & 1 & , & 2 & , & 4 & , & 7 & , & 6 & , & 5 & , & 3 &] \\ & & & & & & k-1 & & k & & & & & & & \end{array}$$

La permutation suivante s'obtient en conservant le maximum de valeurs initiales commune et en augmentant la valeur suivante le moins possible. Il n'est pas possible de conserver le début jusqu'au rang $k-1$ car on ne peut pas remplacer le k-ième terme par une valeur strictement plus grande : toutes les valeurs qui viennent après 7 sont plus petites que 7. Par

contre, on peut conserver le début $[0,1,2]$ et remplacer le $(k-1)$-ième terme par une valeur plus grande. La plus petite de ses valeurs est 5, située à l'indice i :

$$\begin{array}{ccccccccccccccc} [0 & , & 1 & , & 2 & , & 4 & , & 7 & , & 6 & , & 5 & , & 3 &] \\ & & & & & & k-1 & & k & & & & i & & & \end{array}$$

Nous commençons par échanger les contenus des cases $k-1$ et i :

$$\begin{array}{ccccccccccccccc} [0 & , & 1 & , & 2 & , & 5 & , & 7 & , & 6 & , & 4 & , & 3 &] \\ & & & & & & k-1 & & k & & & & & & & \end{array}$$

et il reste à inverser la fin de la liste, pour obtenir la plus petite permutation commençant par $[0,1,2,5]$

$$\begin{array}{ccccccccccccccc} [0 & , & 1 & , & 2 & , & 5 & , & 3 & , & 4 & , & 6 & , & 7 &] \\ & & & & & & k-1 & & k & & & & & & & \end{array}$$

Cela se fait en échangeant les contenus des cases k et $n-1$, $k+1$ et $n-2$), et ainsi de suite jusqu'à $k+j-1$ et $n-j$ où $j = \left\lfloor \frac{n-k}{2} \right\rfloor$ (il y a $n-k$ valeurs entre la k-ième et la $n-1$-ième, donc le nombre ce j est bien le nombre de couples à échanger).

Cela donne :

```
def echange(s,i,j):
    s[i],s[j] = s[j],s[i]

def suivant(s,k):
    n = len(s)
    i = k
    while i < n-1 and s[i+1] > s[k-1]:
        i += 1
    echange(s,i,k-1)
    for j in range((n-k)//2):
        echange(s,k+j,n-1-j)
```

d) Il n'y a pas de difficulté : `s` est la permutation courante, k sa valeur k_σ et `M` est le maximum des ordres déjà trouvés. On initiale avec la permutation identité, dont le `k` vaut $n-1$ et l'ordre 1 ; tant que `k` est non nul (i.e. tant que l'on n'a pas étudié toutes les permutations), on passe à la permutation suivante et on met à jour `k` et `M`. Cela donne :

```
def calcul_M(n):
    s = [i for i in range(n)]
    M = 1
    k = n-1
    while k != 0:
        suivant(s,k)
        k = calcul_k(s)
        M = max(N,ordre(s))
    return(N)
```

On obtient ainsi les premières valeurs de la suite :

$$(M_n)_{n\geq 1} = (1,2,3,4,6,6,12,15,20,\dots)$$

mais il est difficile d'aller plus loin avec cette fonction de type "force brute".

Il est facile de transformer la fonction pour qu'elle renvoie une permutation d'ordre maximal :

```
def calcul_bis(n):
    s = [i for i in range(n)]
    smax = [i for i in range(n)]
```

```
    M = 1
    k = rang(s)
    while k != 0:
        suivant(s,k)
        k = rang(s)
        o = ordre(s)
        if M<o:
            copier(s,smax)
            M = o
    return(M,smax)
```

On obtient par exemple :

```
>>> calcul_bis(5)
    (6, [1, 0, 3, 4, 2])

>>> calcul_bis(6)
    (6, [0, 2, 1, 4, 5, 3])

>>> calcul_bis(7)
    (12, [1, 2, 0, 4, 5, 6, 3])

>>> calcul_bis(8)
    (15, [1, 2, 0, 4, 5, 6, 7, 3])

>>> calcul_bis(9)
    (20, [1, 2, 3, 0, 5, 6, 7, 8, 4])
```

25) Si $n = 1$, $\mathfrak{S}_n$ est réduit à $\{Id\}$ et le seul morphisme de groupe de $\mathfrak{S}_n$ sur $\mathbb{C}^*$ est le morphisme constant $\sigma \longmapsto 1$.

Supposons que $n \geq 2$ et soit φ un morphisme de groupe de $\mathfrak{S}_n$ sur $\mathbb{C}^*$. Pour toute transposition τ, nous avons $\tau^2 = Id$, donc $\varphi(\tau)^2 = 1$, soit $\varphi(\tau) \in \{-1, 1\}$. Nous allons montrer que soit $\varphi(\tau) = 1$ pour toute transposition τ, soit $\varphi(\tau) = -1$ pour toute transposition τ. Ce résultat est une conséquence du lemme classique :

Lemme : deux transpositions de $\mathfrak{S}_n$ sont conjuguées, i.e. que si $(i, j, i', j') \in [\![1, n]\!]$ avec $i \neq j$ et $i' \neq j'$, il existe $\sigma \in \mathfrak{S}_n$ telle que $(i', j') = \sigma^{-1} \circ (i, j) \circ \sigma$.

Il suffit en effet de choisir $\sigma \in \mathfrak{S}_n$ telle que $\sigma(i) = i'$ et $\sigma(j) = j'$ (il suffit d'utiliser une bijection de $[\![1, n]\!] \setminus \{i, j\}$ sur $[\![1, n]\!] \setminus \{i', j'\}$) pour avoir la relation voulue.

Nous pouvons donc conclure : si τ et τ' sont deux transpositions, il existe $\sigma \in \mathfrak{S}_n$ telle que $\tau' = \sigma^{-1} \circ \tau \circ \sigma$ et on a $\varphi(\tau') = \varphi(\sigma^{-1})\varphi(\tau)\varphi(\sigma) = \varphi(\tau)\varphi(\sigma^{-1})\varphi(\sigma) = \varphi(\tau)\varphi(Id) = \varphi(\tau)$ car $\mathbb{C}^*$ est un groupe abélien.

Enfin, comme les permutations engendrent $\mathfrak{S}_n$, soit φ est le morphisme constant égal à 1, soit φ est le morphisme *signature*.

26) a) $\mathfrak{S}_1$ est $\mathfrak{S}_2$ sont commutatifs, donc $p_{\mathfrak{S}_1} = p_{\mathfrak{S}_2} = 1$. $\mathfrak{S}_3$ contient les 6 éléments Id, $(1, 2)$, $(2, 3)$, $(3, 1)$, $(1, 2, 3)$ et $(1, 3, 2)$. Id commute avec les 6 éléments, chacune des trois transpositions commutent avec deux éléments (Id et elle-même) et chaque 3-cycles σ commute avec Id, σ et σ^2. On en déduit que $p_{\mathfrak{S}_3} = \dfrac{6 + 2 + 2 + 2 + 3 + 3}{36} = \dfrac{1}{2}$.

b) Première méthode : on construit la liste $L = [1, 2, \ldots, n]$, on initialise une liste vide σ puis, pour i variant de 0 à $n - 1$, on choisit un indice j entre 0 et $len(L) - 1$, puis on ajoute $L[j]$ à σ et on supprime $L[j]$ de L.

```
import numpy.random as rd
import math
import matplotlib.pyplot as plt

def permutation(n):
    L = [i for i in range(1,n+1)]
    sigma = []
    for i in range(n):
```

```
        j = rd.randint(0,len(L))
        sigma.append(L[j])
        del L[j]
    return(sigma)
```

Deuxième méthode : on peut aussi écrire une fonction récursive. Si $n = 1$, on renvoie $[1]$; sinon, on calcule une permutation aléatoire σ de $\mathfrak{S}_{n-1}$ et on insère n dans σ, en position aléatoire $i \in \{0, \dots, n-1\}$.

```
def permutation_rec(n):
    if n == 1:
        return([1])
    else:
        sigma = permutation_rec(n-1)
        j =  rd.randint(0,n-1)
        sigma.insert(j,n)
        return(sigma)
```

Troisième méthode (mélange de Fisher-Yatesalgorithme ou de Knuth) : on crée la liste $\sigma = [1, 2, \dots, n]$ puis, pour i allant de $n-1$ à 1, on choisit aléatoirement un indice $j \in \{0, \dots, i\}$ et on échange les éléments $\sigma[i]$ et $\sigma[j]$.

```
def permutation_knuth(n):
        sigma = [i for i in range(1,n+1)]
        for i in range(n-1,0,-1):
            j = rd.randint(0,i)
            sigma[i],sigma[j] = sigma[j],sigma[i]
        return(sigma)
```

c) p_G est la probabilité que deux éléments de G choisis uniformément et indépendamment commutent. Si X et Y désignent deux variables aléatoires indépendantes et de même loi uniforme sur $\mathfrak{S}_n$, on peut noter Z la variable aléatoire qui prend la valeur 1 si X et Y commutent et 0 sinon : Z suit alors une loi de Bernoulli de paramètre $p_{\mathfrak{S}_n}$. On peut donc approximer $p_{\mathfrak{S}_n}$ par $\frac{1}{m}, \sum_{k=1}^{m} Z_i$ où $(Z_1, \dots, Z_m)$ est une suite de v.a.i.i.d de même loi que Z, avec m choisi « assez grand ». Cela donne :

```
def Z(n): # simule une variable de type Z
    x,y = permutation(n),permutation(n)
    for i in range(n):
        if x[y[i]-1] != y[x[i]-1]: #x et y ne commutent pas
            return 0
    return 1  # si on sort de la boucle, x et y commutent

    for i in range(n):
        if s[t[i]-1] != t[s[i]-1]:
            return(0)
    return(1)

def proba(n,m):
    c = 0
    for i in range(m):
        c += Z(n)
    return(c/m)
```

Il reste ensuite à faire le tracé (j'ai choisi $m = 1000$: il pourrait être utile de donner des intervalles de confiance précis).

```
x = [i for i in range(1,10)]
y = [proba(i,1000) for i in x]
plt.plot(x,y)
```

On remarque que $p_{\mathfrak{S}_n}$ converge assez vite vers 0.

d) Supposons que x et y sont conjugués ; il existe $z \in G$ tel que $y = zxz^{-1}$ et l'application $a \longmapsto zaz^{-1}$ est une bijection de C_x sur C_y. On en déduit que les deux ensembles ont même cardinal, ce qui donne $p_x = p_y$.

En notant $A_{x,y} = \{s \in G,\ y = sxs^-1\}$, nous avons :

$$s \in A \iff zxz^{-1} = sxs^{-1} \iff s^{-1}zx = xs^{-1}z \iff s^{-1}z \in C_x.$$

Comme l'application $s \longmapsto s^{-1}z$ est une bijection de G sur lui-même, $\mathrm{Card}(A_{x,y}) = \mathrm{Card}(C_x) = N\,p_x$.

Cette propriété permet de relier p_x au cardinal de la classe de x : l'application $\varphi :\ s \longmapsto sxs^{-1}$ est une bijection de G sur $\overline{x}$ et chaque élément y de $\overline{x}$ a exactement p_x antécédents ($A_{x,y} = \varphi^{-1}(y)$ est de cardinal $N\,p_x$). On en déduit que $N\,p_x\,\mathrm{Card}(\overline{x}) = N$, soit $p_x\,\mathrm{Card}(\overline{x}) = 1$.

Choisissons un élément x_i dans chaque classe d'équivalence (avec $1 \leq i \leq N_G$). Nous pouvons écrire :

$$p_G = \frac{1}{N^2}\sum_{x\in G}\mathrm{Card}(C_x) = \frac{1}{N}\sum_{x\in G}p_x = \frac{1}{N}\sum_{i=1}^{N_G}p_{x_i}\mathrm{Card}(\overline{x_i}) = \frac{N_G}{N}.$$

e) Nous avons directement $\sigma c\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_r))$. Ceci prouve que deux r-cycles sont conjugués : pour tout r-cycle $(b_1, \ldots, b_r)$, il existe une permutation σ telle que $b_i = \sigma(a_i)$ pour tout i, ce qui donne $\sigma(a_1, \ldots, a_r)\sigma^{-1} = (b_1, b_2, \ldots, b_r)$.

On en déduit que si $x = c_1c_2\ldots c_k$ (décomposition en produit de cycle disjoints) et si $\sigma \in \mathfrak{S}_n$, on a $\sigma x\sigma^{-1} = \underbrace{(\sigma c_1\sigma^{-1})}_{=c'_1}\underbrace{(\sigma c_2\sigma^{-1})}_{=c'_2}\ldots\underbrace{(\sigma c_k\sigma^{-1})}_{=c'_k}$ et les c'_i sont des cycles disjoints de même longueurs que les c_i : deux permutations x et y conjuguées vérifient donc $\ell(x) = \ell(y)$.

Réciproquement, si $\ell(x) = \ell(y) = (n_1, n_2, \ldots, n_k)$, on peut écrire $x = \prod_{i=1}^k(a_{i,1}, \ldots a_{i,n_i})$ et $y = \prod_{i=1}^k(b_{i,1}, \ldots b_{i,n_i})$ (décompositions en produits de cycles disjoints). L'application σ qui envoie chaque $a_{i,j}$ sur $b_{i,j}$ est alors une permutation qui vérifie $\sigma y\sigma^{-1}x : x$ et y sont conjuguées.

On en déduit que le nombre de classes $N_{\mathfrak{S}_n}$ est égal au nombre P_n de *partitions (ou partages)* de n, i.e. au nombre suites croissantes $(n_1, \ldots, n_k)$ d'entiers naturels non nuls telles que $n_1 + \cdots + n_k = n$. On obtient facilement les premières valeurs de cette suite :

$$1 = 1 \text{ donc } P_1 = 1$$

$$2 = 2 = 1 + 1 \text{ donc } P_2 = 2$$

$$3 = 3 = 1 + 2 = 1 + 1 + 1 \text{ donc } P_3 = 3$$

$$4 = 4 = 1 + 3 = 2 + 2 = 1 + 1 + 2 = 1 + 1 + 1 + 1 \text{ donc } P_4 = 5$$

$$5 = 5 = 1 + 4 = 2 + 3 = 1 + 1 + 3 = 1 + 2 + 2 = 1 + 1 + 1 + 2 = 1 + 1 + 1 + 1 + 1 \text{ donc } P_5 = 7$$

On peut vérifier la cohérence des résultats obtenus à la question c) par le biais de l'instruction :

```
[proba(i,5000)*math.factorial(i) for i in range(1,5)]
```

dont voici différents résultats :

```
In[1]: [[proba(i,5000)*math.factorial(i) for i in range(1,6)] for j in range(5)]

Out[1]:
[[1.0, 2.0, 3.0108, 4.6608, 7.08],
 [1.0, 2.0, 2.9448, 4.9536, 6.744],
 [1.0, 2.0, 3.0023999999999997, 5.0784, 7.296],
 [1.0, 2.0, 3.0588, 5.04, 6.96],
 [1.0, 2.0, 3.0408, 4.9344, 7.008]]
```

27) Pour tout $n \in \mathbb{N}$, notons U_n le sous-groupe multiplicatif des racines n-ièmes de l'unité. On sait que U_n est un groupe cyclique de cardinal n.

a) On a clairement $1 \in G_p \subset \mathbb{C}^*$; si z_1, z_2 sont deux éléments de G_p, il existe $(k_1, k_2) \in \mathbb{N}^*$ tel que z_1 (resp. z_2) est une racine p^{k_1}-ième (resp. p^{k_2}-ième) de l'unité. En notant $k = \max(k_1, k_2)$, z_1 et z_2 sont racines p^k-ième de l'unité, donc $z_1z_2^{-1}$ l'est également (U_{p^k} est un sous-groupe). On en déduit que $z_1z_2^{-1} \in G_p$, qui est ainsi un sous-groupe multiplicatif de $\mathbb{C}^*$.

b) Soit H un sous-groupe strict et $z \in G_p \setminus H$. Notons p^k l'ordre de z. Si H contenait un élément h d'ordre p^q avec $q \geq k$, alors H contiendrait $< h >$, qui est de cardinal p^q et contenu dans U_{p^q} : on aurait donc $U_{p^q} =< h > \subset H$, ce qui serait absurde car $z \in U_{p^k} \subset U_{p^q}$ et $z \notin H$.

On en déduit que tout élément de H est d'ordre p^q avec $q < k$: H est donc contenu dans $U_{p^{k-1}}$. Il reste à montrer que tout sous-groupe d'un groupe cyclique est cyclique : H sera donc cyclique car $U_{p^{k-1}}$ l'est.

Supposons donc que G est un groupe cyclique de cardinal n, engendré par un élément z, et que H est un sous-groupe de G. L'application $\varphi : \mathbb{Z} \to G$ qui à $q \in \mathbb{Z}$ associe z^q est alors un morphisme (surjectif) de groupe. On en déduit que $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$: il est donc de la forme $m\mathbb{Z}$ pour un certain $m \in \mathbb{N}$. Comme φ est surjective, on a $H = \varphi(\varphi^{-1}(H)) = \varphi(m\mathbb{Z}) = \{z^{mq}, q \in \mathbb{Z}\} =< z^m >$: H est cyclique.

c) Si A est une partie finie de G_p, il existe $k \in \mathbb{N}$ tel que $g^{p^k} = 1$ pour tout $g \in A$ (il suffit de choisir le maximum des entiers k associés aux éléments de A). A est donc contenu dans le sous-groupe U_{p^k} : on en déduit que le sous-groupe $< A >$ engendré par A est contenu dans U_{p^k}, qui est strictement contenu dans G_p (le complexe $z = \exp\left(\frac{2i\pi}{p^{k+1}}\right)$ appartient à $G_p \setminus < A >$). G_p n'est donc pas finement engendré.

Exercices X-ENS

28) Si G est dénombrable, $\mathbb{R} \setminus G$ ne l'est pas (dans le cas contraire, $\mathbb{R}$ serait dénombrable). Sinon, on peut fixer $a \in \mathbb{R} \setminus G$ et $a + G$ est une partie non dénombrable (elle est en bijection avec G) contenue dans $\mathbb{R} \setminus G$, qui est donc non dénombrable.

29) Soit $g \in G \setminus \{Id\}$. Il existe donc $a \in [\![1, n]\!]$ tel que $g(a) \neq a$. Pour $b \in [\![1, n]\!]$, il existe $g' \in G$ tel que $g'(a) = b$. On a alors :

$$g(b) = g \circ g'(a) = g' \circ g(a) \neq g'(a) = b$$

car g' est injective ($g(a) \neq a$ implique $g'(g(a)) \neq g'(a)$). On en déduit que g n'a pas de point fixe.

On définit sur $\mathfrak{S}_n$ la relation d'équivalence :

$$\forall \sigma, \sigma' \in \mathfrak{S}_n,\ \sigma \sim \sigma' \iff \sigma^{-1} \circ \sigma' \in G$$

et on note X l'ensemble quotient. On a alors :

- pour $\sigma \in \mathfrak{S}_n$, la classe d'équivalence $\overline{\sigma}$ de σ est la partie σG : elle a donc même cardinal que G ;
- comme les classes d'équivalence partitionnent $\mathfrak{S}_n$, on en déduit que $\mathrm{Card}(X) \times \mathrm{Card}(G) = \mathrm{Card}(\mathfrak{S}_n)$.

Si $\sigma \in \mathfrak{S}_n$, il existe une et une seule permutation $\tau \in \mathfrak{S}_n$ telle que $\sigma \sim \tau$ et $\tau(n) = n$. En effet :

- il existe $g \in G$ tel que $g(n) = \sigma^{-1}(n)$; en posant $\tau = \sigma \circ g$, on a $\sigma^{-1} \circ \tau = g \in G$ et $\tau(n) = \sigma(g(n)) = n$, donc τ est solution ;
- si τ et τ' sont deux solutions, on a $\tau \sim \tau'$, donc $g = \tau^{-1} \circ \tau' \in G$; on a d'autre part

  $$g(n) = \tau^1(\tau'(n)) = \tau^{-1}(n) = n.$$

  Ainsi, g est élément de G et possède un point fixe, c'est donc l'application identité et $\tau = \tau'$.

L'ensemble $Y = \{\tau \in \mathfrak{S}_n,\ \tau(n) = n\}$ est alors une partie de $\mathfrak{S}_n$ de cardinal $(n-1)!$ (c'est un sous-groupe isomorphe à $\mathfrak{S}_{n-1}$) et l'application $\tau \longmapsto \overline{\tau}$ est une bijection de Y sur X. On en déduit :

$$\mathrm{Card}(G) = \frac{\mathrm{Card}(\mathfrak{S}_n)}{\mathrm{Card}(X)} = \frac{\mathrm{Card}(\mathfrak{S}_n)}{\mathrm{Card}(Y)} = n.$$

Remarque : on pourrait croire que G est cyclique, engendré par un n-cycle, mais c'est faux. Par exemple, quand $n = 4$, $G = \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ est un sous-groupe de $\mathfrak{S}_4$ vérifiant les conditions imposées. En particulier, G

est abélien (comme tous les groupes de cardinal 4) non cyclique (il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$). Pour aller un peu plus loin, on peut remarquer que si σ est un élément de G différent de l'identité et si $a \in [\![1, n]\!]$, il existe un plus petit entier non nul k tel que $\sigma^k(a) = a$. Comme $\sigma^k \in G$ et possède un point fixe, $\sigma^k = Id$ et par minimalité de k, σ est d'ordre k. Ainsi, la décomposition de σ en cycles disjoints ne donne que des cycles de même longueur k (qui est un diviseur de n).

30) Nous allons démontrer que $\mathfrak{S}_{\mathbb{N}}$ n'est pas dénombrable. Nous avons pour cela trois méthodes : construire une bijection entre $\mathfrak{S}_{\mathbb{N}}$ et un ensemble non dénombrable connu X, construire une injection d'un ensemble non dénombrable X dans $\mathfrak{S}_{\mathbb{N}}$ ou construire une surjection de $\mathfrak{S}_{\mathbb{N}}$ dans un ensemble non dénombrable X.

La première méthode est souvent difficile à mettre en place, car il est en général difficile d'obtenir une bijection ; c'est pourquoi on préfère se contenter de construire une injection ou une surjection. On a besoin d'un ensemble X non dénombrable qui soit assez proche de $\mathfrak{S}_{\mathbb{N}}$; on peut penser à $\mathbb{N}^{\mathbb{N}}$ ou $\{0,1\}^{\mathbb{N}}$. On peut rapidement rappeler une preuve de la non dénombrabilité de $\{0,1\}^{\mathbb{N}}$: si f est une application de $\mathbb{N}$ dans $\{0,1\}^{\mathbb{N}}$, elle n'est pas surjective car la suite $(u_n)_{n\in\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N},\ u_n = \begin{cases} 0 & \text{si } (f(n))_n = 1 \\ 1 & \text{si } (f(n))_n = 0 \end{cases}$$

n'est pas dans l'image de f (on a noté $f(n) = (f(n)_p)_{p\geq 0}$ la suite $f(n)$). Cette preuve est connu sous le nom d'*argument diagonal de Cantor*. Elle se généralise pour démontrer que pour tout ensemble X, il n'existe pas de surjection de X dans $\mathcal{P}(X)$; si $f :\ X \longmapsto \mathcal{P}(X)$, la partie :

$$U = \{x \in X,\ x \notin f(x)\}$$

n'appartient pas à l'image de f (on peut identifier $\mathcal{P}(X)$ à $\{0,1\}^X$ en associant à chaque partie de X sa fonction indicatrice : cela donne bien le résultat précédent quand $X = \mathbb{N}$).

Méthode 1 : construction d'une bijection

Il semble assez naturel d'essayer de construire une permutation σ de $\mathbb{N}$ à partir d'une application $\varphi :\ \mathbb{N} \longrightarrow \mathbb{N}$: on pose $A_0 = \mathbb{N}$ et $\sigma(0)$ est le $\varphi(0)$-ième élément de A_0 ; on pose ensuite $A_1 = A_0 \setminus \{\sigma(0)\}$, puis on note $\sigma(1)$ le $\varphi(1)$-ième élément de A_1, et ainsi de suite. Plus formellement, nous définissons une application F qui, à une partie infinie $A = \{n_0 < n_1 < \cdots < n_i < \ldots\}$ de $\mathbb{N}$ et à un entier $i \in \mathbb{N}$ associe $F(A, i) = n_i$ (ce que j'ai appelé le i-ième élément de A) et on définit par récurrence :

$$\forall n \in \mathbb{N},\ \sigma(n) = F(\mathbb{N} \setminus \{\sigma(0), \ldots, \sigma(n-1)\}, \varphi(n))$$

L'application $\varphi \longmapsto \sigma$ est injective de $\mathbb{N}^{\mathbb{N}}$ dans $\mathbb{N}^{\mathbb{N}}$, mais son image n'est pas tout à fait $\mathfrak{S}_{\mathbb{N}}$. En effet, σ est bien injective (par construction, $\sigma(n) \neq \sigma(k)$ pour tout $0 \leq k < n$) mais elle n'est surjective que si φ ne prend pas des valeurs ≥ 1 à partir d'un certain rang. En effet, si $\varphi(n) \geq 1$ pour tout $n \geq n_0$, le premier élément de A_{n_0} ne sera jamais choisi. Réciproquement, si nous supposons que σ n'est pas surjective, soit p le plus petit entier tel que $p \notin \sigma(\mathbb{N})$. Il existe donc $n_0, \ldots, n_{p-1}$ tels que

$$\sigma(n_0) = 0,\ \sigma(n_1) = 1,\ \ldots, \sigma_(n_{p-1}) = p-1$$

En notant $N = \max(n_0, n_1, \ldots, n_{p-1})$, p est le premier élément de A_n pour tout $n \geq N$, ce qui prouve que $\varphi(n) \geq 1$ pour tout $n \geq N$.

Nous avons ainsi démontré qu'il existait une bijection entre $X = \{\varphi \in \mathbb{N}^{\mathbb{N}},\ \forall p \in \mathbb{N},\ \exists n \geq p,\ \varphi(n) = 0\}$ et $\mathfrak{S}_{\mathbb{N}}$. X est non dénombrable : on peut par exemple construire une injection de $\{0,1\}^{\mathbb{N}}$ dans X :

$$(u_n)_{n\geq 0} \longmapsto (0, u_0, 0, u_1, 0, u_2, 0, \ldots).$$

Ceci prouve que $\mathfrak{S}_{\mathbb{N}}$ est non dénombrable. Il a en fait le même cardinal que $\mathbb{N}^{\mathbb{N}}$, i.e. que $\mathbb{R}$: $\mathfrak{S}_{\mathbb{N}}$ a la *puissance du continu*.

Méthode 2 : construction d'une injection

Une fois cette preuve faite, on peut aller plus vite et construire simplement une injection d'un ensemble non dénombrable dans $\mathfrak{S}_{\mathbb{N}}$: pour $u = (u_n)_{n\geq 0} \in \{0,1\}^{\mathbb{N}}$, on définit par récurrence :

- $A_0 = \mathbb{N}$, $\sigma(0) = F(A_0, 0) = 0$, $A_1 = \mathbb{N} \setminus \{\sigma(0)\}$ et $\sigma(1) = F(A_1, u_0)$;
- pour tout $n \geq 1$, $A_{2n} = \mathbb{N} \setminus \sigma(0), \sigma(1), \ldots, \sigma(2n-1)$, $\sigma(2n) = F(A_{2n}, 0)$, $A_{2n+1} = \mathbb{N} \setminus \sigma(0), \sigma(1), \ldots, \sigma(2n)$ et $\sigma(2n+1) = F(A_{2n+1}, u_n)$.

et l'application $u \longmapsto \sigma$ est une injection de $\{0,1\}^{\mathbb{N}}$ dans $\mathfrak{S}_{\mathbb{N}}$.

Méthode 3 : construction d'une surjection

Une autre idée consiste à associer à chaque permutation σ de $\mathbb{N}$ une partie de $\mathbb{N}$, de façon surjective ($\mathcal{P}(\mathbb{N})$ n'est pas dénombrable). Une idée naturelle est d'associer à $\sigma \in \mathfrak{S}_{\mathbb{N}}$ l'ensemble $A_\sigma = \{n \in \mathbb{N},\ \sigma(n) \neq n\}$. On a bien l'impression que $\sigma \longmapsto A_\sigma$ est surjective, mais on va voir qu'il y a un petit défaut : si A est une partie quelconque de $\mathbb{N}$, on cherche à construire $\sigma \in \mathfrak{S}_{\mathbb{N}}$ telle que $A = A_\sigma$. On doit donc construire σ de sorte que σ_A soit une permutation de A sans point fixe, puisqu'on impose $\sigma(n) = n$ pour $n \in \mathbb{N} \setminus A$. Ceci est possible, sauf si A est un singleton :

- si $A = \emptyset$, $\sigma = Id$ convient ;
- si $A = \{a_1, a_2, \ldots, a_n\}$ est fini, avec $n \geq 2$, on choisit pour σ une permutation circulaire :

$$\forall i \in \{1, \ldots, n-1\},\ \sigma(a_i) = a_{i+1},\ \sigma(a_n) = a_1 \text{ et } \forall n \in \mathbb{N} \setminus A,\ \sigma(n) = n.$$

- si $A = \{a_0, a_1, a_2, \ldots\}$ est infini, σ échange deux à deux les éléments de A :

$$\forall i \in \mathbb{N},\ \sigma(a_{2i}) = a_{2i+1}, \sigma(a_{2i+1}) = a_{2i} \text{ et } \forall \forall n \in \mathbb{N} \setminus A,\ \sigma(n) = n.$$

Dans chaque cas σ est un antécédent de A. Ainsi, l'application $\sigma \longmapsto A_\sigma$ est surjective de $\mathfrak{S}_{\mathbb{N}}$ sur $X = \{A \in \mathcal{P}(\mathbb{N})\} \setminus \{\{n\},\ n \in \mathbb{N}\}$. Comme X est non dénombrable (on a enlevé une partie dénombrable à un ensemble non dénombrable), on a une nouvelle preuve de la non dénombrabilité de $\mathfrak{S}_{\mathbb{N}}$.

31) a) Supposons qu'il existe un loi de groupe sur $G_{/\sim}$, notée $\odot$, telle p soit un morphisme. Si $x \sim x'$ et $y \sim y'$, nous pouvons donc écrire :

$$\overline{xy} = \overline{x} \odot \overline{y} = \overline{x'} \odot \overline{y'} = \overline{x'y'}$$

donc $xy \sim x'y'$.

Supposons réciproquement que $\sim$ est compatible avec la loi de G. Nous pouvons alors définir la loi $\odot$ par :

$$\forall \alpha, \beta \in G_{/\sim},\ \alpha \odot \beta = \overline{xy} \text{ avec } x, y \in G \text{ tels que } \overline{x} = \alpha \text{ et } \overline{y} = \beta$$

Cette définition est cohérente car $\overline{(xy)}$ ne dépend pas des choix des représentants x et y des classes α et β. Il reste à vérifier que $(G_{/\sim}, \odot)$ est un groupe et que p est un morphisme de groupe :

- $\odot$ est associative :

$$\forall x, y, z \in G,\ \overline{x} \odot (\overline{y} \odot \overline{z}) = \overline{x} \odot \overline{yz} = \overline{x(yz)} = \overline{(xy)z} = (\overline{x} \odot \overline{y}) \odot \overline{z};$$

- $\overline{1}$ est neutre :

$$\forall x \in G,\ \overline{1} \oplus \overline{x} = \overline{1x} = \overline{x} = \overline{x1} = \overline{x} \odot \overline{1};$$

- tout élément $\overline{x}$ possède pour inverse $\overline{x^{-1}}$:

$$\forall x \in G,\ \overline{x} \odot \overline{x^{-1}} = \overline{xx^{-1}} = \overline{1} = \overline{x^{-1}x} = \overline{x^{-1}} \odot \overline{x};$$

- p est un morphisme de groupe :

$$\forall x, y \in G,\ p(xy) = \overline{xy} = \overline{x} \odot \overline{y} = p(x) \odot p(y).$$

b) Il suffit de vérifier ces propriétés :

(i) On munit $G_{/\sim}$ de la loi de groupe $\odot$ et $H = p^{-1}(\{\overline{1}\})$ est un sous-groupe de G, comme image réciproque d'un sous-groupe par un morphisme de groupe ;

(ii) Soient $x \in G$ et $y \in H$. On a $x \sim x$ et $y \sim 1$, donc $xy \sim x$; comme $x^{-1} \sim x^{-1}$, on en déduit $xyx^{-1} \sim xx^{-1} = 1$, soit $xyx^{-1} \in H$;

(iii) Soient $x, y \in G$. Si $x \sim y$, on a $x^{-1} \sim x^{-1}$ donc $1 = x^{-1}x \sim x^{-1}y$, soit $x^{-1}y \in H$; réciproquement, si $x^{-1}y \in H$, on a $x^{-1}y \sim 1$ et $x \sim x$, donc $y = xx^{-1}y \sim y$.

c) Soit H un sous-groupe distingué. Nous avons :

$$\forall x \in G,\ \forall \in H, xy = \underbrace{xyx^{-1}}_{\in H} x \in Hx$$

donc $xH \subset Hx$, puis $Hx = x(x^{-1}H)x \subset x(Hx^{-1})x = xH$. On a donc $xH = Hx$ (on vient de montrer que si $xH \subset Hx$ pour tout x, alors $xH = Hx$ pour tout x).

Réciproquement, supposons que $xH = Hx$ pour tout $x \in G$. Pour $x \in G$ et $y \in H$, on a $xy \in xH$, donc il existe $y' \in H$ tel que $xy = y'x$, ce qui donne $xyx^{-1} = y' \in H$: H est un sous-groupe distingué.

d) Il s'agit une nouvelle de vérifications évidentes :

- $\sim$ est réflexive car pour $x \in G$, $x^{-1}x = 1 \in H$;
- $\sim$ est symétrique car pour $x, y \in G$, $x^{-1}y \in H$ implique $y^{-1}x = \left(x^{-1}y\right)^{-1} \in H$;
- $\sim$ est transitive car pour $x, y, z \in G$, $x^{-1}y \in H$ et $z^{-1}y \in H$ implique $z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$;
- $\sim$ est compatible avec la loi de g : pour $x_1, x_2, y_1, y_2 \in G$ tels que $x_1 \sim x_2$ et $y_1 \sim y_2$, nous avons

$$(x_2y_2)^{-1}(x_1y_1) = y_2^{-1}x_2^{-1}x_1y_1 = \underbrace{y_2^{-1}\underbrace{x_2^{-1}x_1}_{\in H}y_2}_{\in H}\underbrace{y_2^{-1}y_1}_{\in H} \in H$$

- pour $x \in G$, on a (en utilisant le c) :

$$\overline{x} = \{y \in G,\ x^{-1}y \in H\} = \{y \in G,\ \exists h \in H,\ y = xh\} = xH = Hx$$

Notation : une permutation $x \in \mathfrak{S}_n$ sera notée :

$$x = \begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ x(1) & x(2) & \ldots\ldots & x(n) \end{pmatrix}$$

Pour $i_1, \ldots, i_k$ éléments distincts de $\{1, 2, \ldots, n\}$, nous utiliserons aussi la notation usuelle $(i_1, i_2, \ldots, i_k)$ pour représenter le k-cycle qui envoie i_1 sur i_2, i_2 sur i_3, …, i_{k-1} sur i_k, i_k sur i_1 et qui laisse les autres éléments de $\{1, 2, \ldots, n\}$ en place. Nous utiliserons également la décomposition des permutations en produits de cycles disjoints. Par exemple :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix} = (1,3)(2,5).$$

e) $\mathfrak{S}_3$ contient les 6 éléments Id, $(1,2)$, $(1,3)$, $(2,3)$, $(1,2,3)$ et $(1,3,2)$. Chaque transposition engendre un sous-groupe de cardinal 2, les 3-cycles engendrent chacune le même sous-groupe de cardinal 3 et si un sous-groupe contient une transposition et un 3-cycle, c'est le groupe entier. $\mathfrak{S}_3$ a donc 5 sous-groupes :

$$H_1 = \{Id\},\ H_2 = \{Id, (1,2)\},\ \{Id, (1,2)\},\ H_3 = \{Id, (1,2)\},\ \{Id, (1,3)\},$$

$$H_4 = \{Id, (1,2)\},\ \{Id, (2,4)\},\ H_5 = \{Id, (1,23), (1,3,2)\} = \mathfrak{A}_3 \text{ et } H_6 = \mathfrak{S}_3.$$

H_1 et H_6 sont trivialement distingués, ainsi que H_5 (voir preuve générale ci-dessous). Par contre, H_2, H_3 et H_4 ne le sont pas (les trois cas sont symétriques) : $(1,2) \in H_2$, $(1,3) \in G$ mais $(1,3)^{-1}(1,2)(1,3) = (2,3) \notin H_2$.

Notons $\sigma(x)$ la signature d'un élément de x de SG_n. Nous avons :

$$\forall x \in \mathfrak{S}_n,\ \forall y \in \mathfrak{A}_n,\ \sigma(x^{-1}yx) = \sigma(x^{-1})\underbrace{\sigma(y)}_{=1}\sigma(x) = \sigma(x^{-1}x) = \sigma(Id) = 1$$

donc $\mathfrak{A}_n$ est un sous-groupe distingué de G.

Remarque : on a $\mathfrak{A}_n = \mathrm{Ker}(\sigma)$ et on montre facilement que le noyau d'un morphisme de groupe $\sigma : G \longrightarrow G'$ est un sous-groupe distingué de G.

On obtient donc un sous-groupe distingué de $GL_n(K)$ en introduisant un morphisme de groupe ... on pense au déterminant : $SL_n(K) = \{M \in \mathcal{M}_n(K),\ \det(M) = 1\}$ est un sous-groupe distingué de $GL_n(K)$.

f) Commençons par rappeler que $\mathfrak{A}_5$ est partitionné en 4 parties :

- $A_1 = \{Id\}$, de cardinal 1 ;
- $A_{2,2}$, ensemble des permutations qui se décomposent en produit de deux transpositions à supports disjoints, de cardinal 15 (5 choix pour l'élément qui ne bouge pas, puis 3 choix pour séparer les 4 éléments qui restent en deux paquets de 2) ;
- A_3, ensemble des 3 cycles, de cardinal 20 ($\binom{5}{3}$ pour choisir les 3 éléments du cycle puis 2 choix pour le "sens" du 3-cycle) ;
- A_5, ensemble des 5 cycles, de cardinal 24 (il y a 120 permutations $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$ et chaque 5-cycle a 5 écritures, puisque $(a,b,c,d,e) = (b,c,d,e,a) = \cdots = (e,a,b,c,d)$).

Chacune de ces parties est stable par automorphisme intérieur : par exemple, si $y = (i,j,k)$ est un élément de $\mathbb{A}_3$ (i, j et k sont donc des éléments distincts de $\{1,2,3,4,5\}$ et si $x \in \mathfrak{S}_5$ (et à plus forte raison si $x \in \mathfrak{A}_5$), $xyx^{-1} = (a,b,c)$ avec $a = x(i)$, $b = x(j)$ et $c = x(k)$. Nous avons alors :

- $\mathcal{C}(Id) = \{Id\} = A_1$;
- $\mathcal{C}((1,2)(3,4)) = A_{2,2}$: si $(a,b)(c,d) \in A_{2,2}$, notons e le dernier des 5 éléments de $\{1,2,3,4,5\}$. Nous avons $x(1,2)(3,4)x^{-1} = (a,b)(c,d)$ pour $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$. Si $x \in \mathfrak{A}_5$, nous avons montré que $(a,b)(c,d)$ est dans la classe de conjugaison de $(1,2)(3,4)$. Sinon, la permutation $y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ b & a & c & d & e \end{pmatrix}$ est dans $\mathfrak{A}_5$ et vérifie $y(1,2)(3,4)y^{-1} = (b,a)(c,d) = (a,b)(c,d)$: nous avons donc démontré que $(a,b)(c,d)$ est dans tous les cas élément de $\mathcal{C}((1,2)(3,4))$.
- $\mathcal{C}((1,2,3)) = A_3$: si $(a,b,c) \in A_3$, notons e et f les deux derniers éléments de $\{1,2,3,4,5\}$. Nous avons $x(1,2,3)x^{-1} = (a,b,c)$ pour $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$ et $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & e & f \end{pmatrix}$. Comme l'une de ces deux permutations est paire, $(1,2,3)$ et (a,b,c) sont conjugués.
- Soient $(a,b,c,d,e) \in A_5$ et $x \in \mathfrak{S}_5$; on a :

$$\begin{aligned} & x(1,2,3,4,5)x^{-1} = (a,b,c,d,e) \Longleftrightarrow (x(1),x(2),x(3),x(4),x(5)) = (a,b,c,d,e) \\ \Longleftrightarrow\ & x \in \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ b & c & d & e & a \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & d & e & a & b \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ d & e & a & b & c \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ e & a & b & c & d \end{pmatrix} \right\} \end{aligned}$$

  Comme ces 5 permutations ont toutes la même parité, on en déduit que la classe de conjugaison de $(1,2,3,4,5)$ est l'ensemble des 5-cycles (a,b,c,d,e) tels que $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$ est pair. Comme $\mathfrak{A}_5$ contient 60 éléments et que chaque 5-cycle est atteinte 5 fois, la classe de conjugaison de $(1,2,3,4,5)$ contient 12 éléments. Comme A_5 contient 24 élément, il sera réunion de deux classes de conjugaison : celles des 5-cycles $(1,2,3,4,5)$ et $(2,1,3,4,5)$.

Si H est un sous-groupe distingué de $\mathfrak{A}_5$, il est réunion de classes de conjugaison. Comme $\mathfrak{A}_5$ continent 5 classes, de cardinaux respectifs 1, 15, 20, 12 et 12, le cardinal de H est de la forme $1 + 15a + 20b + 12c$ avec $a, b \in \{0, 1\}$ et $c \in \{0, 1, 2\}$. Les valeurs possibles pour ce cardinal sont donc 1, 13, 16, 21, 25, 28, 33, 36, 40, 45, 48 et 60. Si on sait que le cardinal de H divise celui de $\mathfrak{A}_5$ (théorème de Lagrange), i.e. 60, on obtient que les deux seuls valeurs possibles sont 1 et 60 : $\mathfrak{A}_5$ ne possède donc que les sous-groupes distingués triviaux $\{Id\}$ et $\mathfrak{A}_5$.

Démonstration du théorème de Lagrange : soit G un groupe fini et H un sous-groupe de G. On définit la relation $\sim$ sur G par :

$$\forall x, y \in G,\ x \sim y \Longleftrightarrow x^{-1}y \in H.$$

On montre facilement que $\sim$ est une relation d'équivalence sur G et que $\overline{x} = xH$ pour tout $x \in G$ (on n'a pas besoin que h soit un sous-groupe distingué). Le cardinal de G est alors la somme des cardinaux des classes d'équivalence (ces classes forment une partition de G). Comme $\overline{x} = xH$, chaque classe a le même cardinal que H, ce qui donne $\mathrm{Card}(G) = k\mathrm{Card}(H)$ où k est le nombre de classes d'équivalence : nous avons prouvé que $\mathrm{Card}(H)$ divise $\mathrm{Card}(G)$.

32) a) Remarquons que $\overline{x}$ est la classe d'équivalence pour la relation d'équivalence définie par :

$$\forall x, y \in G,\ x \sim y \Longleftrightarrow \exists g \in G,\ g^{-1}xg = y.$$

Si x est ambivalent et si $y = h^{-1}xh$ est un élément quelconque de $\overline{x}$, on a

$$y^{-1} = (h^{-1}xh)^{-1} = h^{-1}x^{-1}h \sim x^{-1} \sim x \sim y$$

donc y est ambivalent.

b) L'application φ est clairement surjective et pour $y = g_0^{-1}xg_0 \in \overline{x}$, $\varphi^{-1}(y)$ a le même cardinal que $\varphi^{-1}(x)$. En effet, on a :

$$\forall g \in G,\ g \in \varphi^{-1}(y) \Longleftrightarrow g^{-1}xg = g_0^{-1}xg_0 \Longleftrightarrow (gg_0)^{-1}x(gg_0^{-1}) = x \Longleftrightarrow gg_0^{-1} \in \varphi^{-1}(x)$$

donc l'application $g \longmapsto gg_0^{-1}$ est une bijection de $\varphi^{-1}(y)$ sur $\varphi^{-1}(x)$. En notant k ce cardinal commun, on en déduit que $n = k \times \mathrm{Card}(\overline{x})$, ce qui donne le résultat(demandé.

c) On a $\rho(g) = \sum_{\substack{x \in G \\ x^2 = g}} 1 = \sum_{x \in G} \mathbf{1}_{(x^2=g)}$. On obtient donc :

$$\begin{aligned}
\frac{1}{n}\sum_{g\in G}\rho(g)^2 &= \frac{1}{n}\sum_{g\in G}\left(\sum_{x\in G}\mathbf{1}_{(x^2=g)}\right)^2 \\
&= \frac{1}{n}\sum_{g\in G}\sum_{x\in G}\sum_{y\in G}\mathbf{1}_{(x^2=g)}\mathbf{1}_{(y^2=g)} \\
&= \frac{1}{n}\sum_{g\in G}\sum_{x\in G}\sum_{y\in G}\mathbf{1}_{(x^2=g \text{ et } y^2=g)} \\
&= \frac{1}{n}\sum_{x\in G}\sum_{y\in G}\underbrace{\sum_{g\in G}\mathbf{1}_{(x^2=g \text{ et } y^2=g)}}_{=\mathbf{1}_{(x^2=y^2)}} \\
&= \frac{1}{n}\sum_{x\in G}\sum_{y\in G}\mathbf{1}_{(x^2=y^2)} \\
&= \frac{1}{n}\sum_{x\in G}\sum_{z\in G}\mathbf{1}_{(x^2=(xz)^2)} \qquad \text{car, à } x \text{ fixé, } z \longmapsto zx \text{ est une bijection de } G \text{ sur lui-même.} \\
&= \frac{1}{n}\sum_{z\in G}\sum_{x\in G}\mathbf{1}_{(z^{-1}=x^{-1}zx)}
\end{aligned}$$

Notons A l'ensemble des éléments ambivalents de G. Si $z \notin A$, $\mathbf{1}_{(z^{-1}=x^{-1}zx)} = 0$ pour tout x. On peut donc restreindre la somme pour $z \in G$ à la somme pour $z \in A$. Nous obtenons donc :

$$\frac{1}{n}\sum_{g\in G}\rho(g)^2 = \frac{1}{n}\sum_{z\in A}\left|\{x \in G,\ z^{-1} = x^{-1}zx\}\right| = \sum_{z\in A}\frac{1}{|\overline{z}|}$$

en utilisant le résultat du b).

On peut enfin choisir $z_1, \dots, z_k$ dans A tels que $A = \overline{z_1} \bigsqcup \overline{z_2} \bigsqcup \dots \bigsqcup \overline{z_k}$ et on obtient :

$$\frac{1}{n} \sum_{g \in G} \rho(g)^2 = \sum_{i=1}^{k} \sum_{z \in \overline{z_i}} \frac{1}{|\overline{z}|} = \sum_{i=1}^{k} \sum_{z \in \overline{z_i}} \frac{1}{|\overline{z_i}|} = \sum_{i=1}^{k} 1 = k$$

33) a) Commençons par regarder quelques exemples :

G	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/10\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z}$
s	$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{5}$	$(\overline{0}, \overline{0}, \overline{0})$

On peut plus généralement remarquer que pour $G = \mathbb{Z}/n\mathbb{Z}$, on a $s = \overline{0 + 1 + \dots + (n-1)} = \overline{\frac{n(n-1)}{2}}$. Ainsi, si $n = 2p$, $s = \overline{p(n-1)} = \overline{-p} = \overline{p}$ et si $n = 2p+1$, $s = \overline{np} = \overline{0}$.

On peut aussi penser à calculer s quand G est le groupe multiplicatif d'un corps fini commutatif K (la loi de G est alors multiplicative et on remplace la somme par le produit) : si n est le cardinal de K, on a $a^{n-1} = 1$ pour tout $a \in G$, donc le polynôme $X^{n-1} - 1$ est scindé à racines simples : ses $n-1$ racines sont les éléments de G. On en déduit que $X^{n-1} - 1 = \prod_{a \in G}(X - a)$, ce qui donne $\displaystyle\prod_{a \in G} a = (-1)^n$: le produit est donc égal à 1 si n est pair et à -1 si n est impair.

Il semble donc qu'il y ait deux cas : ou bien s est le neutre 0 (ou 1 quand le groupe est noté multiplicativement), ou bien un élément d'ordre 2. Revenons donc au cas général. Dans la somme s, nous allons regrouper chaque élément avec son opposé. Notons donc $A = \{a \in G,\ a = -a\}$ et $B = G \setminus A$. A est l'ensemble des $a \in G$ tels que $2a = 0$: on montre facilement que c'est un sous-groupe de G. Il existe une partie B est de cardinal pair et est réunion disjointe de parties de la forme $\{b, -b\}$. On a donc $s = \sum_{x \in G} x = \sum_{a \in A} a$. Si A est réduit à $\{0\}$, $s = 0$. Sinon, A est un groupe fini non trivial vérifiant $\forall a \in A,\ 2a = 0$: A est isomorphe à une puissance de $\mathbb{Z}/2\mathbb{Z}$. En effet, on peut munir A du produit externe

$$\begin{array}{rcl} \mathbb{Z}/2\mathbb{Z} \times A & \longrightarrow & A \\ (\lambda, a) & \longmapsto & \lambda \cdot a = \begin{cases} 0 & \text{si } \lambda = \overline{0} \\ a & \text{si } \lambda = \overline{1} \end{cases} \end{array}$$

qui donne à A la structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension finie $d \geq 1$ (car A est fini) : A est donc isomorphe (en tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel) à $(\mathbb{Z}/2\mathbb{Z})^d$, donc également en tant que groupe. Par cet isomorphisme, s est identifié à

$$\sum_{a_1 \in \mathbb{Z}/2\mathbb{Z}} \sum_{a_2 \in \mathbb{Z}/2\mathbb{Z}} \dots \sum_{a_d \in \mathbb{Z}/2\mathbb{Z}} (a_1, \dots, a_d) = (2^{d-1} \cdot \overline{1}, \dots, 2^{d-1} \cdot \overline{1}).$$

Ainsi, $s = 0$ si $d > 1$ et s est l'unique élément non nul de A si $d = 1$ (dans ce cas, a est de cardinal 2).

En conclusion, nous avons :

- si G possède un unique élément d'ordre 2, s est cet élément d'ordre 2 ;
- sinon, $s = 0$.

b) Notons A l'ensemble cherché. Comme $\mathfrak{S}_3$ contient trois permutations paires (l'identité et les cycles $(1,2,3)$ et $(1,3,2)$) et trois permutations impaires (les transpositions $(1,2)$, $(2,3)$ et $(3,1)$), les éléments de A sont des permutations impaires, donc A est contenu dans $\{(1,2), (2,3), (3,1)\}$. Comme A est non vide, il contient au moins une de ces transpositions : il les contient toutes par symétrie. On peut aussi écrire :

$$(2,3) = Id \circ (1,2,3) \circ (1,3,2) \circ (1,2) \circ (2,3) \circ (3,1) \in A$$

donc en remplaçant $1, 2, 3$ respectivement par $2, 1, 3$, puis par $3, 2, 1$, nous obtenons :

$$\begin{cases} (1,3) = Id \circ (2,1,3) \circ (2,3,1) \circ (2,1) \circ (1,3) \circ (3,2) \in A \\ (2,1) = Id \circ (3,2,1) \circ (3,1,2) \circ (3,2) \circ (2,1) \circ (1,3) \in A \end{cases}$$

34) a) Soit G le groupe des permutations de $\mathbb{C}$, f la rotation de centre 0 et d'angle $\pi/4$ et g la rotation de centre 1 et d'angle $-\pi/4$. Nous avons :

$$\forall z \in \mathbb{C},\ f(z) = iz \text{ et } g(z) = -i(z-1)+1 = -iz+1+i.$$

f et g sont d'ordre 4 et $f \circ g :\ z \longmapsto i(-iz+1+i) = z-1+i$ est une translation d'ordre infini.

b) Nous allons la propriété par récurrence sur r. La construction décrire est comparable à celle du tri par insertion.

- Quand $r = 1$, il n'y a rien à démontrer.
- Pour $r \geq 2$, supposons la propriété démontrée au rang $r-1$ et soient $s_1, \ldots, s_r \in S$. Par hypothèse de récurrence, il existe $s'_1, \ldots, s'_{r-1} \in S$ tels que $s_1 \cdot \cdots \cdot s_{r-1} = s'_1 \cdots s'_{r-1}$ et $s'_1 \leq \cdots \leq s'_{r-1}$. Si $s'_{r-1} \leq s_r$, il sufit de poser $s'_r = s_r$ pour avoir la décomposition voulue. Sinon, on a $s_r \leq s'_{r-1}$ (car l'ordre est total) et on peut écrire :

  $$s_1 \cdot \cdots \cdot s_r = s'_1 \cdots s'_{r-2} s'_{r-1} s_r = s'_1 \cdots s'_{r-2} \left(s'_{r-1} s_r (s'_{r-1})^{-1}\right) s'_{r-1}$$

  On a $s'_{r-1} s_r (s'_{r-1})^{-1} \in S$ car S est stable par automorphisme intérieur et $s'_{r-1} s_r (s'_{r-1})^{-1} \leq s'_{r-1} s'_{r-1} (s'_{r-1})^{-1} = s'_{r-1}$ par compatibilité de l'ordre et du produit. On a donc obtenu une décomposition de la forme :

  $$s_1 \cdot \cdots \cdot s_r = s'_1 \cdot \cdots \cdot s'_{r-2} t_1 s'_{r-1}$$

  avec $t_1 \in S$ et $t_1 \leq s'_{r-1}$. Si $r = 2$ ou $s'_{r-2} \leq t_1$, cette décomposition convient. Sinon, la même méthode que précédemment donne une décomposition :

  $$s_1 \cdot \cdots \cdot s_r = s'_1 \cdot \cdots \cdot s'_{r-3} t_2 s'_{r-2} s'_{r-1}$$

  avec $t_2 \in S$ et $t_2 \leq s'_{r-2}$. On arrive ainsi en un nombre fini d'étapes à une décomposition

  $$s_1 \cdot \cdots \cdot s_r = s'_1 \cdot \cdots \cdot s'_{r-k-1} t_k s'_{r-k} \cdots s'_{r-1}$$

  avec $0 \leq k \leq r-1$, $t_k \in S$ et $s'_1 \leq \cdots \leq s'_{r-k-1} \leq t_k \leq s'_{r-k} \leq \cdots \leq s_{k-1}$: cela prouve le résultat au rang r.

35) a) La décomposition de σ en produit de cycles disjoints s'écrit $\sigma = (x_1, y_1) \circ \cdots \circ (x_k, y_k)$ avec $0 \leq 2k \leq n$ et $x_1, y_1, \ldots, x_k, y_k$ éléments distincts de $[\![1, n]\!]$. Si θ est une permutation quelconque, la décomposition de $\theta^{-1} \circ \sigma \circ \theta$ en produit de cycles disjoints est $(\theta^{-1}(x_1), \theta^{-1}(y_1)) \circ \cdots \circ (\theta^{-1}(x_k), \theta^{-1}(y_k))$. Par unicité de cette décomposition, on aura donc $\sigma \circ \theta = \theta \circ \sigma$ si et seulement s'il existe une permutation τ de $[\![1, k]\!]$ telle que $\theta(\{x_i, y_i\}) = \{x_{\tau(i)}, y_{\tau(i)}\}$.

Il existe ainsi $(n-2k)!k!2^k$ permutations qui commutent avec σ (on peut permuter indifféremment les $n-2k$ éléments autres que les x_i, y_i, puis on choisit une permutation quelconque $\tau \in \mathfrak{S}_k$ et pour chaque $i \in [\![1, k]\!]$, on a encore deux choix, selon que $\theta(x_i) = x_{\tau(i)}$ ou $\theta(x_i) = y_{\tau(i)}$).

b) Soit f un automorphisme de $\mathfrak{S}_n$ et σ une transposition. Comme σ est d'ordre 2, $f(\sigma)$ est également d'ordre 2. Si on note k le nombre de 2-cycles dans la décomposition de $f(\sigma)$ en produit de cycles disjoints, on a $\mathrm{Card}(\mathcal{C}(f(\sigma))) = (n-2k)!k!2^k$ et $k \geq 1$ ($f(\sigma) \neq Id$ car f est un automorphisme). D'autre part, f étant un automorphisme, $\mathcal{C}(f(\sigma)) = f(\mathcal{C}(\sigma))$, d'où :

$$(n-2k)!k!2^k = \mathrm{Card}(\mathcal{C}(f(\sigma))) = \mathrm{Card}(\mathcal{C}(\sigma)) = 2\,(n-2)!$$

Cela donne :

$$\binom{n-2}{n-2k} = \frac{2^{k-1}k!}{(2k-2)!} = \frac{k}{(2k-3)(2k-5)\ldots 1}.$$

Si $k = 2$, on obtient $\dfrac{(n-2)(n-3)}{2} = 2$: c'est absurde car les racines de $X^2 - 5X + 2$ ne sont pas entières.

Si $k = 3$, on obtient $\dbinom{n-2}{n-6} = 1$, ce qui n'est possible que si $n = 6$, valeur interdite.

Si $k \geq 4$, $\dfrac{k}{(2k-3)(2k-5)\ldots 1} \leq \dfrac{k}{2k-3} < 1$ et $\dbinom{n-2}{n-2k} \geq 1$: nous obtenons une nouvelle absurdité.

Nous avons donc $k = 1$, ce qui signifie que $f(\sigma)$ est également une transposition.

c) Il est évident que pout tout $\tau \in \mathfrak{S}_n$, f_τ est un automorphisme de $\mathfrak{S}_n$.

Soit f un automorphisme de $\mathfrak{S}_n$. D'après la question précédente, pour tout $1 \leq i < j \leq n$ il existe $1 \leq a < b \leq n$ tel que $f((i,j)) = (a,b)$. S'il existe $\tau \in \mathfrak{S}_n$ tel que f_τ, nous avons : $f((i,j)) = (\tau(i), \tau(j))$, soit $\{a,b\} = \{\tau(i), \tau(j)\}$. Nous allons donc atteindre τ en étudiant les images par f des transpositions (i,j).

Si $n = 2$, le résultat est évident car Id est le seul automorphisme de $\mathfrak{S}_2$: c'est bien un automorphisme intérieur.

Si $n \geq 3$ et si i, j, k sont trois éléments distincts de $[\![1, n]\!]$, les transpositions $f((i,j)) = (a,b)$ et $f((i,k)) = (c,d)$ sont distinctes (car f est injective) et à supports non disjoints (car (i,j) et (i,k) ne commutent pas, donc (a,b) et (c,d) ne commutent pas non plus). Il existe donc a, b, c distincts tels que $f(i,j) = (a,b)$ et $f(i,k) = (a,c)$. Nous pouvons donc définir τ :

- il existe a_1, a_2, a_3 distincts tels que $f((1,2)) = (a_1, a_2)$ et $f((1,3)) = (a_1, a_3)$;
- pour tout $i \geq 4$, il existe (a,b) tels que $f((1,i)) = (a,b)$; $\{a,b\}$ et $\{a_1, a_2\}$ ont un élément en commun et sont distincts, ainsi que $\{a,b\}$ et $\{a_1, a_3\}$: cet élément commun est donc nécessairement a_1. On en déduit qu'il existe a_i tel que $f((1,i)) = (a_1, a_i)$;
- les éléments $a_1, \ldots, a_n$ sont des éléments distincts de $[\![1, n]\!]$, on définit $\tau \in \mathfrak{S}_n$ en posant :

$$\forall i \in [\![1, n]\!],\ \tau(i) = a_i.$$

On a alors $f((1,i)) = f_\tau((1,i))$ pour tout $i \in [\![2, n]\!]$, donc $f = f_\tau$ puisqu'elle coïncident sur la famille génératrice $\big((1,i)\big)_{2 \leq i \leq n}$. a) La décomposition de σ en produit de cycles disjoints s'écrit $\sigma = (x_1, y_1) \circ \cdots \circ (x_k, y_k)$ avec $0 \leq 2k \leq n$ et $x_1, y_1, \ldots, x_k, y_k$ éléments distincts de $[\![1, n]\!]$. Si θ est une permutation quelconque, la décomposition de $\theta^{-1} \circ \sigma \circ \theta$ en produit de cycles disjoints est $(\theta^{-1}(x_1), \theta^{-1}(y_1)) \circ \cdots \circ (\theta^{-1}(x_k), \theta^{-1}(y_k))$. Par unicité de cette décomposition, on aura donc $\sigma \circ \theta = \theta \circ \sigma$ si et seulement s'il existe une permutation τ de $[\![1, k]\!]$ telle que $\theta(\{x_i, y_i\}) = \{x_{\tau(i)}, y_{\tau(i)}\}$.

Il existe ainsi $(n-2k)!k!2^k$ permutations qui commutent avec σ (on peut permuter indifféremment les $n - 2k$ éléments autres que les x_i, y_i, puis on choisit une permutation quelconque $\tau \in \mathfrak{S}_k$ et pour chaque $i \in [\![1, k]\!]$, on a encore deux choix, selon que $\theta(x_i) = x_{\tau(i)}$ ou $\theta(x_i) = y_{\tau(i)}$).

b) Soit f un automorphisme de $\mathfrak{S}_n$ et σ une transposition. Comme σ est d'ordre 2, $f(\sigma)$ est également d'ordre 2. Si on note k le nombre de 2-cycles dans la décomposition de $f(\sigma)$ en produit de cycles disjoints, on a $\mathrm{Card}(\mathcal{C}(f(\sigma))) = (n-2k)!k!2^k$ et $k \geq 1$ ($f(\sigma) \neq Id$ car f est un automorphisme). D'autre part, f étant un automorphisme, $\mathcal{C}(f(\sigma)) = f(\mathcal{C}(\sigma))$, d'où :

$$(n-2k)!k!2^k = \mathrm{Card}(\mathcal{C}(f(\sigma))) = \mathrm{Card}(\mathcal{C}(\sigma)) = 2\,(n-2)!$$

Cela donne :

$$\binom{n-2}{n-2k} = \frac{2^{k-2}k!}{(2k-2)!} = \frac{k}{(2k-3)(2k-5)\ldots 1}.$$

Si $k = 2$, on obtient $\dfrac{(n-2)(n-3)}{2} = 2$: c'est absurde car les racines de $X^2 - 5X + 2$ ne sont pas entières.

Si $k = 3$, on obtient $\dbinom{n-2}{n-6} = 1$, ce qui n'est possible que si $n = 6$, valeur interdite.

Si $k \geq 4$, $\dfrac{k}{(2k-3)(2k-5)\ldots 1} \leq \dfrac{k}{2k-3} < 1$ et $\dbinom{n-2}{n-2k} \geq 1$: nous obtenons une nouvelle absurdité.

Nous avons donc $k = 1$, ce qui signifie que $f(\sigma)$ est également une transposition.

c) Il est évident que pout tout $\tau \in \mathfrak{S}_n$, f_τ est un automorphisme de $\mathfrak{S}_n$.

Soit f un automorphisme de $\mathfrak{S}_n$. D'après la question précédente, pour tout $1 \leq i < j \leq n$ il existe $1 \leq a < b \leq n$ tel que $f((i,j)) = (a,b)$. S'il existe $\tau \in \mathfrak{S}_n$ tel que f_τ, nous avons : $f((i,j)) = (\tau(i), \tau(j))$, soit $\{a,b\} = \{\tau(i), \tau(j)\}$. Nous allons donc atteindre τ en étudiant les images par f des transpositions (i,j).

Si $n = 2$, le résultat est évident car Id est le seul automorphisme de $\mathfrak{S}_2$: c'est bien un automorphisme intérieur.

Si $n \geq 3$ et si i, j, k sont trois éléments distincts de $[\![1, n]\!]$, les transpositions $f((i,j) = (a,b)$ et $f((i,k)) = (c,d)$ sont distinctes (car f est injective) et à supports non disjoints (car (i,j) et (i,k) ne commutent pas, donc (a,b) et (c,d) ne commutent pas non plus). Il existe donc a, b, c distincts tels que $f(i,j) = (a,b)$ et $f(i,k) = (a,c)$. Nous pouvons donc définir τ :

- il existe a_1, a_2, a_3 distincts tels que $f((1,2)) = (a_1, a_2)$ et $f((1,3)) = (a_1, a_3)$;
- pour tout $i \geq 4$, il existe (a,b) tels que $f((1,i)) = (a,b)$; $\{a,b\}$ et $\{a_1, a_2\}$ ont un élément en commun et sont distincts, ainsi que $\{a,b\}$ et $\{a_1, a_3\}$: cet élément commun est donc nécessairement a_1. On en déduit qu'il existe a_i tel que $f((1,i)) = (a_1, a_i)$;
- les éléments $a_1, \ldots, a_n$ sont des éléments distincts de $[\![1, n]\!]$, on définit $\tau \in \mathfrak{S}_n$ en posant :

$$\forall i \in [\![1, n]\!],\ \tau(i) = a_i.$$

On a alors $f((1,i)) = f_\tau((1,i))$ pour tout $i \in [\![2, n]\!]$, donc $f = f_\tau$ puisqu'elle coïncident sur la famille génératrice $\big((1,i)\big)_{2 \leq i \leq n}$.

36) a) Remarquons que l'ensemble des applications de G dans $\mathbb{C}^*$ est trivialement un groupe pour le produit de fonctions $\times$. Nous allons montrer que $\widehat{G}$ en est un sous-groupe :

- l'élément neutre est la fonction constante $g \longmapsto 1$: c'est bien un morphisme de G dans $\mathbb{C}^*$;
- si φ_1 et φ_2 sont deux morphismes G dans $\mathbb{C}^*$, $\varphi_1 \times \varphi_2^{-1}$ est bien un morphisme de groupe :

$$\forall g, h \in G,\ \varphi_1 \times \varphi_2^{-1}(gh) = \frac{\varphi_1(gh)}{\varphi_2(gh)} = \frac{\varphi_1(g)\varphi_1(h)}{\varphi_2(g)\varphi_2(h)} = \frac{\varphi_1(g)}{\varphi_2(g)}\frac{\varphi_1(h)}{\varphi_2(h)} = \varphi_1 \times \varphi_2^{-1}(g)\varphi_1 \times \varphi_2^{-1}(h)$$

b) Notons $S = \sum_{g \in G} \chi(g)$. Nous avons :

$$S^2 = \sum_{g,h \in G} \chi(g)\chi(h) = \sum_{g \in G} \left(\sum_{h \in G} \chi(gh) \right) = \sum_{g \in G} \left(\sum_{k \in G} \chi(k) \right)$$

car l'application $h \longmapsto gh$ est une bijection de g sur lui-même. On en déduit que $S^2 = nS$, soit $S = n$ ou $S = 0$.

Pour tout $g \in G$, on a $g^n = 1$, donc $\chi(g)^n = 1$: on en déduit que les $\chi(g)$ sont de module 1. Si $S = n$, on peut écrire :

$$n = \mathrm{Re}\left(\sum_{g \in G} \chi(g) \right) = \sum_{g \in G} \mathrm{Re}(\chi(g)) \leq \sum_{g \in G} |\chi(g)| = n.$$

On en déduit que ces inégalités sont des égalités, ce qui impose :

$$\forall g \in G,\ \mathrm{Re}(\chi(g)) = 1$$

et χ est le morphisme constant égal à 1 (le seul complexe de module 1 et de partie réelle égale à 1 est 1). Ainsi, $S = 0$ si χ n'est pas le morphisme trivial.

c) L'application $\chi'' :\ g \longmapsto \overline{\chi(g)}\chi'(g)$ est un élément non trivial de $\widehat{G}$ (il existe g tel que $\chi(g) \neq \chi'(g)$, donc $\chi''(g) = \chi(g)^{-1}\chi'(g) \neq 1$) : la question précédente donne le résultat attendu.

d) On peut voir les caractères de G comme des éléments du $\mathbb{C}$-espace vectoriel $\mathbb{C}^G$. Nous allons montrer que la famille $(\chi)_{\chi \in \widehat{G}}$ est libre : cela prouvera que $\widehat{G}$ contient au plus n éléments, puisque $\mathbb{C}^G$ est de dimension n.

Soit $(\alpha_\chi)_{\chi \in \widehat{G}}$ une famille de complexe telle que $\sum_{\chi \in \widehat{G}} \alpha_\chi \chi = 0$. Pour tout $\chi' \in G$, on peut écrire :

$$0 = \sum_{g \in G} \overline{\left(\sum_{\chi \in \widehat{G}} \alpha_\chi \chi \right)(g)}\, \chi'(g) = \sum_{\chi \in \widehat{G}} \overline{\alpha_\chi} \underbrace{\sum_{g \in G} \overline{\chi(g)}\chi'(g)}_{\substack{=0 \text{ si } \chi \neq \chi' \\ \text{et } \ n \text{ sinon}}} = \overline{\alpha}_{\chi'}$$

ce qui prouve que tous les coefficients α_χ sont nuls.

e) Pour tous $\chi, \chi' \in \widetilde{G}$, on a $\delta_g(\chi \times \chi') = (\chi \times \chi')(g) = \chi(g) \times \chi'(g) = \delta_g(\chi) \times \delta_g(\chi')$ donc δ_g est élément de $\widetilde{\widetilde{G}}$.

On a ensuite :

$$\forall g, h \in G,\ \forall \chi \in \widetilde{G},\ \delta_{gh}(\chi) = \chi(gh) = \chi(g)\chi(h) = \delta_g(\chi)\delta_h(\chi) = (\delta(g) \times \delta_h)(\chi)$$

donc $g \longmapsto \delta_g$ est un morphisme de G dans $\widetilde{\widetilde{G}}$.

f) On sait d'après la question d) que $n = \mathrm{Card}(G) \geq \mathrm{Card}(\widehat{G}) \geq \mathrm{Card}(\widehat{\widehat{G}})$. Il suffit donc de prouver que δ est injective pour montrer qu'elle est bijective. Cela revient à montrer que pour tout $g \neq 1$, il existe un caractère χ de G tel que $\chi(g) \neq 1$.

Fixons donc $g \in G \setminus \{1\}$ et considérons le sous-groupe G_1 engendré par g ; soit k l'ordre de g. Il existe alors un isomorphisme χ_1 du groupe G_1 sur le groupe $\mathbb{U}_k$ des racines k-ièmes de l'unité (ces deux groupes sont isomorphes à $\mathbb{Z}/k\mathbb{Z}$) et χ_1 est un caractère de G_1 tel que $\chi_1(g) \neq 1$.

Si $G_1 = G$, nous avons terminé. Sinon, on peut choisir $g_2 \in G \setminus G_1$. Nous allons prolonger le caractère χ_1 en un caractère χ_2 sur le sous-groupe G_2 engendré par $G_1 \cup \{g_2\}$. Remarquons pour cela que :

- G_2 est l'ensemble des éléments de la forme $x_1 g_2^i$ avec $x_1 \in G_1$ et $i \in \mathbb{Z}$ (car G est abélien) ;
- il existe un plus petit entier $k \geq 1$ tel que $g_2^k \in G_1$ (comme g_2 est d'ordre fini, l'ensemble des $k \in \mathbb{N}^*$ tel que $g_2^k \in G_1$ est non vide : il contient l'ordre de g_2) ; on montre facilement ensuite que $g_2^i \in G_1$ si et seulement si k divise i.

On peut alors choisir α, racine k-ième de $\chi_1(g_2^k)$ (on travaille dans $\mathbb{C}$) ; pour $x \in G_2$, on peut écrire $x = x_1 g_2^i$ avec $x_1 \in G_1$ et $k \in \mathbb{Z}$: montrons que $\chi_1(x_1)\alpha^i$ ne dépend que de x et pas des éléments x_1 et i choisis. Supposons donc que $x_1 g_2^i = x_1' g_2^{i'}$ avec $x_1, x_1' \in G_1$ et $i, i' \in \mathbb{Z}$. Nous avons :

$$g_2^{i'-i} = x_1 (x_1')^{-1} \in G_1$$

donc $i' - i$ est un multiple de k et on peut écrire $i' - i = kj$ avec $j \in \mathbb{Z}$. On en déduit que $x_1 = x_1' g_2^{(i'-i)} = x_1' (g_2^k)^j$, puis :

$$\chi_1(x_1) = \chi_1(x_1') \left(\chi_1(g_2^k)\right)^j = \chi_1(x_1')\alpha^{kj} = \chi_1(x_1')\alpha^{i'-i},$$

ce qui donne l'égalité cherchée : $\chi_1(x_1)\alpha^i = \chi_1(x_1')\alpha^{i'}$.

Nous pouvons ainsi définir l'application $\chi_2 : \quad G_2 \longrightarrow \mathbb{C}^*$ en posant , pour tout $x = x_1 g_2^i \in G_2$ avec $x_1 \in G_1$ et $i \in \mathbb{Z}$, $\chi_2(x) = \chi_1(x_1)\alpha^i$. Cette application prolonge χ_1 et est un caractère de G_2 : si $x = x_1 g_2^i$ et $y = y_1 g_2^j$ sont deux éléments de G_2, avec $x_1, y_1 \in G_1$ et $i, j \in \mathbb{Z}$, nous avons :

$$\chi_2(xy) = \chi_2(\underbrace{x_1 y_1}_{\in G_1} g_2^{i+j}) = \chi_1(x_1 y_1)\alpha^{i+j} = \chi_1(x_1)\alpha^i \chi_1(y_1)\alpha^j = \chi_2(x)\chi_2(y).$$

Par itération, nous pouvons donc prolonger χ_1 est un caractère χ de G, ce qui prouve que le noyau de δ ne contient pas g : δ est injective.

Nous avons donc montré que δ était un isomorphisme de groupe : on en déduit que G et $\widehat{\widehat{G}}$ ont même cardinal, ce qui prouve que $\widetilde{G}$ contient aussi n éléments (son cardinal est compris entre celui de g et celui de $\widehat{\widehat{G}}$).

Remarque : nous avons évidemment utilisé plusieurs fois la commutativité de la loi de G et le résultat ne subsiste pas quand G n'est pas abélien. Ainsi, avec $G = \mathfrak{S}_n$ (avec $n \geq 3$), on peut montrer qu'il n'existe que deux caractères : le caractère constant égal à 1 et la signature.

37) a) On a $2023 = 7 \times 17^2$. On peut donc choisir $G_1 = \mathbb{Z}/2023\mathbb{Z}$ et $G_2 = \mathbb{Z}/119\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. En effet, $119 \times 17 = 2023$ et G_2 n'est pas isomorphe à G_1 car G_1 est cyclique alors que tout élément de G_2 est d'ordre un diviseur de 119.

b) Cette question est très délicate. La méthode habituelle utilise un théorème classique : le centre d'un p-groupe n'est pas trivial, qui demande un assez long développement. Tout d'abord, on appelle p-groupe tout groupe fini dont le cardinal est une puissance de p (où p est un nombre premier) et on appelle *centre* d'un groupe $(G, \cdot)$ la partie $Z(G) = \{g \in G,\ \forall h \in G,\ gh = hg\}$ (cette partie est trivialement un sous-groupe de G). Il faut ensuite utiliser la notion d'action de groupe. En se restreignant à l'action qui nous intéresse, nous pouvons nous contenter de définir, pour tout $h \in G$, les parties $O_h = \{g^{-1}hg,\ g \in G\}$ et $G_h = \{g \in G,\ hg = gh\}$ (ce sont respectivement *l'orbite* et le *stabilisateur* de h). On montre facilement :

- pour tout $h \in G$, l'application $g \longmapsto g^{-1}hg$ est surjective de G sur O_h et chaque élément a le même nombre d'antécédent, qui est le cardinal de G_h ; ainsi, nous avons

$$\mathrm{Card}(O_h) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(G_h)};$$

- pour tout $h \in G$, G_h est un sous-groupe de G et $h \in Z(G) \Longleftrightarrow G_h = G \Longleftrightarrow O_h = \{h\}$;

- les orbites O_h forment une partition de G.

Avec le théorème de Lagrange, on en déduit que pour $h \notin Z(G)$, $\mathrm{Card}(O_h)$ est un multiple de p (car G est de cardinal p^k et G_h est de cardinal un diviseur de p^k différent de p^k). Ainsi, toutes les orbites sont de cardinaux multiples de p, sauf les orbites réduites à un singleton : on en déduit que $\mathrm{Card}(Z(G)) \equiv \mathrm{Card}(G) \equiv 0 \bmod p$. Comme $Z(G)$ est non vide (il contient 1), $Z(G)$ contient au moins p éléments : il n'est pas réduit à $\{1\}$.

La preuve est maintenant élémentaire ; si G est de cardinal p^2, deux cas sont possibles :

- soit G possède un élément d'ordre p^2 et G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$;

- soit tous les éléments de G (autre que 1) sont d'ordre p ; comme $Z(G)$ est non trivial, on peut alors choisir un élément $x \in Z(G) \setminus \{1\}$ puis un élément $y \in G \setminus < x >$ (en notant $< x_1, \ldots, x_k >$ le groupe engendré par une partie $\{x_1, \ldots, x_k\}$). Comme $< x, y >$ contient au moins $p+1$ élément et est de cardinal un diviseur de p^2, $< x, y >= G$ et $xy = yx$. On en déduit que G est commutatif. Ainsi, G est un groupe abélien et en définissant la loi externe : $(\overline{k}, g) \in \mathbb{Z}/p\mathbb{Z} \times G \longmapsto g^k \in G$, on donne à G la structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel : comme G est de cardinal p^2, il est de dimension 2 : G est donc isomorphe (en tant que $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel donc à plus forte raison en tant que groupe) à $(\mathbb{Z}/p\mathbb{Z})^2$.

Nous allons maintenant donner une preuve qui évite l'étude du centre de G, mais qui oblige à s'intéresser à une autre notion hors programme, celle de *sous-groupe distingué*. Supposons que G n'est pas cyclique, i.e. que $x^p = 1$ pour tout $x \in G$. On peut alors choisir $x \in G \setminus \{1\}$ puis $y \in G \setminus < x >$: il suffit de démontrer que x et y commutent et on pourra terminer comme précédemment. La preuve va se faire en deux temps :

a) Montrons qu'il existe $k \in \mathbb{Z}$ tel que $yx = x^k y$ (cette propriété revient à dire que $< x >$ est un sous-groupe distingué de G) ; tout d'abord, $\mathcal{X} = \{g < x >,\ g \in G\}$ est une partition de G en p parties de même cardinal p (c'est la preuve du théorème de Lagrange) et l'application $\sigma : \mathcal{X} \to \mathcal{X}$ qui à une partie X de $\mathcal{X}$ associe xX est une permutation de $\mathcal{X}$. Comme l'élément $< x >$ de X est invariant par σ, la restriction σ' de σ à $\mathcal{X}' = \mathcal{X} \setminus \{< x >\}$ est une permutation de $\mathcal{X}'$; comme $x^p = 1$, $(\sigma')^p = Id$, donc l'ordre de σ' divise p ; d'autre part, cet ordre divise $(p-1)!$, qui est le cardinal du groupe symétrique de $\mathcal{X}'$: on en déduit que σ' est d'ordre 1 (p est premier avec $(p-1)!$), i.e. que $xg < x >= g < x >$ pour tout $g \in G$. Ainsi, avec $g = y^{-1}$, on a $xy^{-1} \in xy^{-1} < x >= y^{-1} < x >$ et il existe $k \in \mathbb{Z}$ tel que $yx = x^k y$.

b) Comme $yx \neq y$, i n'est pas divisible par p ; on obtient ensuite par récurrence immédiate :

$$\forall q \in \mathbb{N},\ y^q x y^{-q} = x^{k^q}$$

ce qui donne, avec $q = p-1$, $y^{-1}xy = x^{k^{q-1}}$. Comme k est premier avec p, le petit théorème de Fermat donne $k^{p-1} \equiv 1 \bmod p$, d'où $y^{-1}xy = x$ et x et y commutent.

c)