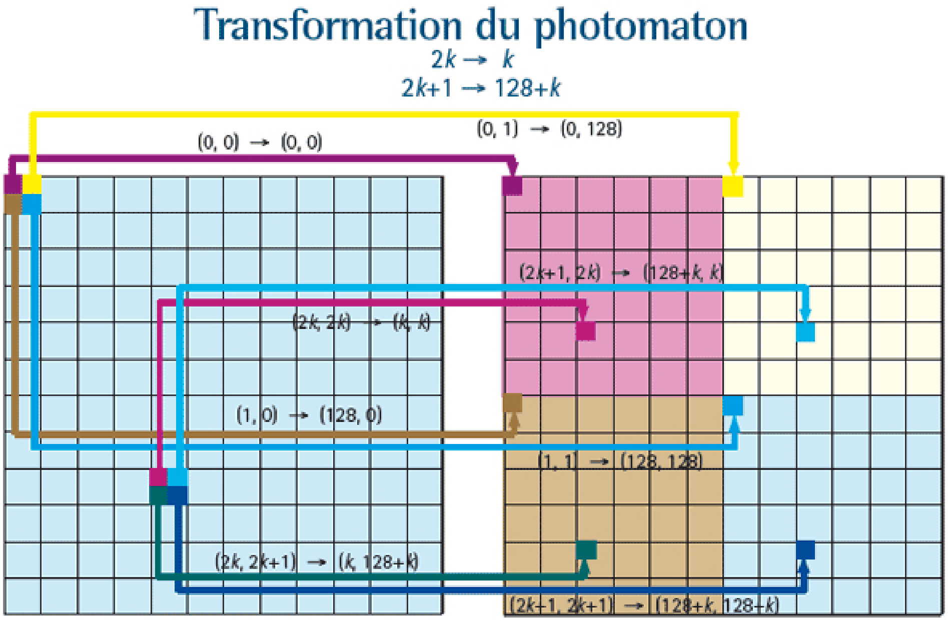
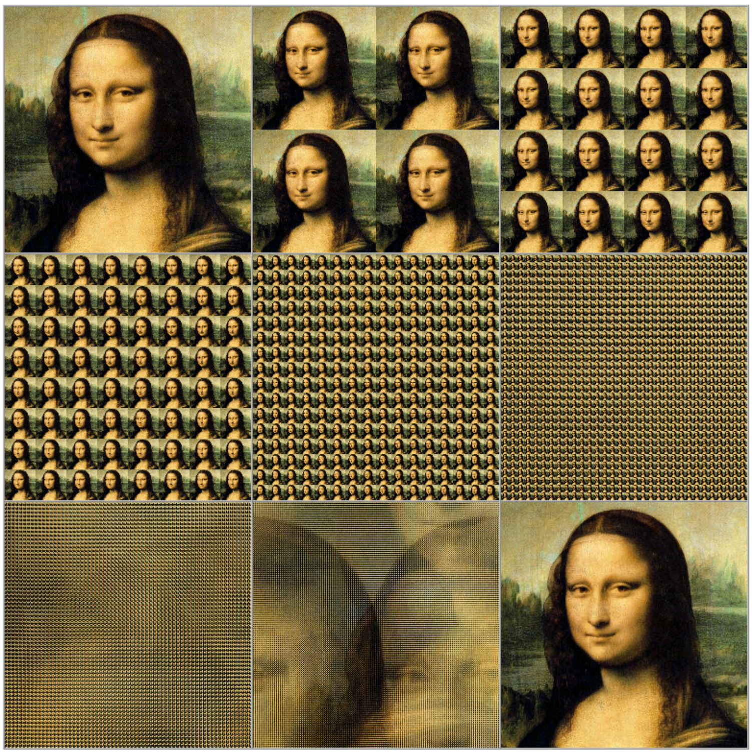
Enseignant : Rémi Molinier
remi.molinier@univ-grenoble-alpes.fr

Groupes et actions de groupes

Exercice 1 (En guise de mise en bouche : La transformation du photomaton)
On considère une image carré de 256×256 de la Joconde et on considère la transformation donnée sur l'image suivante[1].



En itérant la transformation on observe ce qui suit.



Pourquoi retombe-t-on sur l'image initiale ?

[1]source : `https://images.math.cnrs.fr/Mona-Lisa-au-photomaton.html`

1 Avant propos (mais après mise en bouche)

Cette feuille propose des exercices pour un survol approximatif du programme d'agreg interne sur les groupes et les actions de groupes. Elle n'a pas l'ambition d'être exhaustive et est (très) biaisée par les goûts de l'auteur. Au vu du nombre d'exercices, Il n'est bien sûr pas attendu que vous résolviez l'ensemble de la feuille et d'ailleurs seul une toute petit fraction sera traitée en séance mais je vous invite à la parcourir dans sont intégralité et de piocher par-ci par-là les exercices qui vous titillent le plus. Vous y trouverez aussi quelques développements potentiels pour vos leçons (marqués d'un (Dev) dans le titre).
Notez aussi que la difficulté des exercices et questions est très variable (même parfois au sein d'un même exercice !) donc ne vous laissez pas décourager et n'hésitez pas à contacter l'auteur pour avoir des indices voir essayer de le soudoyer pour les solutions. La plupart des exercices sont aussi très classiques et se trouvent facilement dans des manuels ou sur internet pour les fanas de google ou autres moteurs de recherche. Enfin si vous êtes vraiment désespéré·e vous pouvez demander à chat GPT (ou votre IA favorite) qui vous donnera peut-être n'importe quoi comme réponse mais "hey, c'est une IA super intelligente donc c'est forcément vrai !" (cette avant propos part vraiment dans tous les sens...)
Enfin les erreurs, coquilles ou autres ne sont imputables qu'à l'auteur qui s'en excuse platement. Si vous en remarquez, n'hésitez surtout pas à lui signaler sévèrement son manque de sérieux et de rigueur dans la préparation de cette feuille.

2 Un vrai/faux pour se remuer les méninges

Exercice 2 (Vrai ou Faux ?)
Pour chaque item, la proposition est elle vraie ou fausse ? Justifier. Les questions avec un * demandent plus de réflexion et/ou d'astuce, en particulier pour les justifications, et peuvent être laissées de coté en première lecture.

(i) L'intersection de deux sous-groupes et un sous-groupe.

(ii) L'union de deux sous-groupes est un sous-groupe.

(iii) le produit de deux sous-groupes est un sous-groupe.

(iv) L'ordre du produit de deux éléments d'ordre finis est le ppcm des deux ordres.

(v) tout groupe d'exposant fini (i.e. il existe $N \in \mathbb{N}^*$ tel que pour tout $g \in G$, $g^N = 1$) est fini.

(vi) Si p est un nombre premier, alors il n'existe qu'un seul groupe d'ordre p à isomorphisme près.

(vii) Tout groupe d'ordre p^2 avec p un nombre premier est abélien.

(viii) Si G est un groupe dont tous les éléments distincts du neutre sont d'ordre 2 alors G est abélien.

(ix) Si G est un groupe dont tous les éléments distincts du neutre sont d'ordre 3 alors G est abélien.*

(x) Si G et H sont des groupes, $f : G \to H$ un morphisme de groupe et A est une partie de G, alors $f(\langle A \rangle) = \langle f(A) \rangle$.

(xi) Si G et H sont des groupes, $f : G \to H$ un morphisme de groupe et B est une partie de H, alors $f^{-1}(\langle B \rangle) = \langle f^{-1}(B) \rangle$.

(xii) Tout sous-groupe d'indice 2 est distingué.

(xiii) Tout sous-groupe d'indice 3 est distingué.*

(xiv) Tous les sous-groupes d'un groupe G sont distingués si et seulement si G est abélien.*

(xv) Tout morphisme non trivial $f : G \to H$ d'un groupe simple G vers un groupe H est injectif.

(xvi) Si $n \geq 2$, alors le groupe alterné $\mathfrak{A}_n$ est simple.

(xvii) Dans le groupe symétrique $\mathfrak{S}_n$, deux éléments de même ordre sont conjugués.

(xviii) Dans le groupe alterné A_n, deux éléments de même type sont conjugué.

(xix) Si G est un groupe d'ordre $n \geq 1$ agissant transitivement sur un ensemble fini X alors n divise le cardinal de X.

3 Des groupes à connaître

Les petits

Exercice 3 (Les tout petits groupes)
Donner, à isomorphisme près, la liste de tout les groupes d'ordre au plus 8. Pour chacun expliciter les éléments avec leurs ordres, donner la liste des sous-groupes sous forme d'un treillis, identifier le centre et les sous-groupes distingués.

Les monogènes

Exercice 4 (Groupes cycliques et monogènes)
On considère l'ensemble des entiers $\mathbb{Z}$ muni de la loi additive.

1. Quels sont les sous-groupes de $\mathbb{Z}$?
2. Quels sont les générateurs de $\mathbb{Z}$?
3. Quel est le groupe des automorphismes de $\mathbb{Z}$?
4. Montrer que tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

On fixe maintenant $n \in \mathbb{N}^*$ et on considère l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes modulo n d'entiers muni de la loi additive.

5. Quels sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$?
6. Quels sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$?
7. Quel est le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$?
8. Montrer que tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 5
Soit n et m deux entier non nuls. Donner une condition nécessaire et suffisante pour avoir $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ isomorphes. Dans les cas où ils sont isomorphes exhiber un isomorphisme et son inverse.

Exercice 6
Soit G un groupe fini (ou pas*).

1. Montrer que si $G/Z(G)$ est cyclique (ou monogène), alors G est abélien.
2. en déduire que $\mathrm{Aut}(G)$ ne peut être cyclique d'ordre impair .

Les groupes symétriques et alternés

Exercice 7 (Parties génératrices de $\mathfrak{S}_n$)

1. Montrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1,2),(2,3),\dots,(n-1,n)$. En déduire une famille génératrice de $\mathfrak{A}_n$.
2. Montrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1,2),(1,3),\dots,(1,n)$. En déduire une famille génératrice de $\mathfrak{A}_n$.
3. Montrer que $\mathfrak{A}_n$ est engendré par les carrés des éléments de S_n.

Exercice 8
Quels sont les sous-groupes d'indice 2 de $\mathfrak{S}_n$?

Exercice 9
Soit $\sigma \in \mathfrak{S}_n$ et soit $c = (i_1,\dots,i_l)$ un l-cycle, montrer que $\sigma c \sigma^{-1} = (\sigma(i_1),\dots,\sigma(i_l))$. Quel est le stabilisateur de c (pour l'action de conjugaison)? Quel est le cardinal de ce stabilisateur?

Exercice 10 (Les groupes $\mathfrak{S}_4, \mathfrak{A}_4$)

1. Déterminer tous les éléments de $\mathfrak{S}_4$. Pour chaque élément calculer son centralisateur. Pour chaque type de décomposition en produit de cycles disjoints calculer le nombre de classes de conjugaison. Pour les éléments de $\mathfrak{A}_4$ comparer le centralisateur et les orbites pour l'action de $\mathfrak{S}_4$ avec ceux pour l'action de $\mathfrak{A}_4$.

2. Effectuer le même travail pour les sous-groupes de $\mathfrak{S}_4$.

Les groupes linéaires

Exercice 11
Soit k un corps et E un k-espace vectoriel.

1. Quel est le centre de $\mathrm{GL}(E)$? de $\mathrm{SL}(E)$?

2. Donner une famille de générateurs de $\mathrm{GL}(E)$ et de $\mathrm{SL}(E)$.

Exercice 12 (Groupes linéaires sur un corps finis)
Soit $\mathbb{F}_q$ est un corps fini à q éléments.

1. Quel sont les cardinaux de $\mathrm{GL}_n(\mathbb{F}_q)$ et $\mathrm{SL}_n(\mathbb{F}_q)$?

2. Montrer qu'il existe un homomorphisme de $\mathrm{GL}_n(\mathbb{F}_q)$ vers $\mathfrak{S}_{n_q}$ où $n_q = q^n + q^{n-1} + \cdots + 1$ dont le noyau est le centre $Z(\mathrm{GL}_n(\mathbb{F}_q))$. en déduire un isomorphisme entre $\mathrm{GL}_2(\mathbb{F}_2)$ et $\mathfrak{S}_3$.

Exercice 13 (Un théorème de Burnside (Dev))
Soit $n \geq 1$ et G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. On suppose que G est d'exposant fini: il existe $N \in \mathbb{N}^*$ tel que $g^N = 1$ pour tout $g \in G$. Le but de l'exercice est de démontrer que G est fini.

1. Montrer que tous les éléments de G sont diagonalisable. Quelles sont les valeurs propres possibles ?

2. Montrer que l'ensemble T des traces des éléments de G est fini.

On note $\varphi_g : G \to T$ l'application définie par $\varphi_g(h) = Tr(gh)$.

3. Soit $g \in G$. Montrer que si $Tr(g) = Tr(\mathrm{I}_n)$, alors $g = 1$.

4. En déduire que l'application $g \mapsto \varphi_g$ est injective.

5. En déduire que G est fini.

6. Est-ce vrai si on remplace $\mathbb{C}$ par n'importe quel corps de caractéristique nulle ?

7. Et en caractéristique p ? *

Des groupes d'isométries

Exercice 14 (Isométries d'un espace Euclidien)
Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension n et $\mathrm{O}(E)$ le groupe des isométries vectoriel de E (i.e. une application linéaire $u \in \mathrm{O}(E)$ si et seulement si, pour tout $x, y \in E$, $\langle u(x), u(y) \rangle = \langle x, y \rangle$).

1. Soit u un endomorphisme de E. Montrer qu'on a équivalence entre
   (i) $u \in \mathrm{O}(E)$;
   (ii) pour tout $x \in E$, $\|u(x)\|_2 = \|x\|_2$;
   (iii) pour toute base orthonormée e, la matrice de u dans la base e est orthogonale ;
   (iv) Il existe une base orthonormée e telle que la matrice de u dans cette base est orthogonale.

2. Montrer que pour tout $u \in \mathrm{O}(E)$, $\det(u) \in \pm 1$.

3. Montrer que les valeurs propres réelles de u, s'il y en a, sont 1 ou -1.

4. Montrer que l'ensemble $\mathrm{SO}(E)$ des isométries positive (i.e. telles que $\det(u) = 1$) forme un sous-groupe distingué de $\mathrm{O}(E)$ d'indice 2.

5. On veut montrer que $\mathrm{O}(E)$ est engendré par les réflexions orthogonales. On rappelle qu'une isométrie u est une **réflexion orthogonale** s'il existe un hyperplan $F \subseteq E$ tel que $u|_F = \mathrm{id}_F$ et $u|_{F^\perp} = -\mathrm{id}_{F^\perp}$.
   (a) Vérifier ce qu'il se passe si la dimension est $n = 1$.
   (b) Soit $u \in \mathrm{O}(E)$ et $a \in E$ tel que $u(a) \neq a$. Montrer qu'il existe une réflexion orthogonale qui envoie $u(a)$ sur a.
   (c) En effectuant une récurrence sur la dimension n de E, montrer que toute isométrie de E est le produit d'au plus n réflexions.

Exercice 15 ($\mathrm{SO}_2(\mathbb{R})$ ET ANGLES ORIENTÉS)
Soit $\mathrm{SO}_2(\mathbb{R})$ le sous groupes des isométries positives du plan euclidien $\mathbb{R}^2$ muni du produit scalaire usuel.

1. Montrer que pour tout élément $g \in \mathrm{SO}_2(\mathbb{R})$ il existe $\theta \in \mathbb{R}$ tel que la matrice de g dans n'importe quel base orthonormée directe est
$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$
2. En déduire que les isométries positives sont exactement les rotations.
3. Montrer que $SO_2(\mathbb{R})$ agit transitivement sur l'ensemble des vecteur de norme 1 (pour la norme euclidienne). Est-ce que l'action est fidèle ? libre ?
4. Comment définir proprement la notion d'angle orienté entre deux vecteurs $u \in \mathbb{R}^2$ et $v \in \mathbb{R}^2$?

Exercice 16 (LES GROUPES DIÉDRAUX)
Soit $n \geq 2$ et soit P_n un polygone régulier du plan à n cotés (représenté par exemple par les racines n-ièmes de l'unité dans le plan complexe). On note D_{2n} le groupe (appelé n-ième groupe diédral) des isométries directes et indirectes du plan préservant P_n.

1. Montrer que D_{2n} est d'ordre $2n$.
2. Montrer que le sous-groupe D_{2n}^+ constitué des isométries directes est cyclique d'ordre n : $D_{2n}^+ \cong \mathbb{Z}/n\mathbb{Z}$.
3. Montrer que D_{2n} est un sous-groupe de $\mathcal{S}_n$.
4. Dresser la listes des classes de conjugaison dans D_{2n}.

4 Morphismes et quotients en pagaille

Exercice 17 (CONSTRUCTION DE MORPHISMES)
Soit G un groupe. Pour $n \in \mathbb{N}$, on note $G_n = \{x \in G, x^n = 1_G\}$ l'ensemble des éléments de G dont l'ordre divise n.

1. Montrer que les applications suivantes sont bien définies et des bijections réciproques l'un de l'autre
$$\begin{aligned} \mathrm{Hom}(\mathbb{Z}, G) &\longrightarrow G \\ \varphi &\longmapsto \varphi(1) \end{aligned} \qquad \text{et} \qquad \begin{aligned} G &\longrightarrow \mathrm{Hom}(\mathbb{Z}, G) \\ x &\longmapsto (n \mapsto x^n) \end{aligned}$$

Morale (à retenir) : *se donner un morphisme de groupes issu de $\mathbb{Z}$, c'est la même chose que se donner un élément du groupe.*

2. Montrer que les applications suivantes sont bien définies et des bijections réciproques l'un de l'autre
$$\begin{aligned} \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G) &\longrightarrow G_n \\ \varphi &\longmapsto \varphi(\overline{1}) \end{aligned} \qquad \text{et} \qquad \begin{aligned} G_n &\longrightarrow \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \\ x &\longmapsto (n \mapsto x^k) \end{aligned}$$
où $\overline{1}$ désigne la classe de 1 modulo n.

Morale (à retenir): *se donner un morphisme de groupes issu de $\mathbb{Z}/n\mathbb{Z}$, c'est la même chose que se donner un élément du groupe d'ordre divisant n.*
On pourra remarquer que les bijections des deux questions ci-dessus dépendent du "choix" d'un générateur de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$.

3. D'après la propriété universelle du quotient, $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$ s'identifie à un sous-ensemble de $\mathrm{Hom}(\mathbb{Z}, G)$ (lequel ?). Montrer que cette identification est compatible aux bijections ci-dessus.

4. à quel sous-ensemble de G s'identifie les morphismes injectifs de $\mathbb{Z}$ dans G ? les morphismes injectifs de $\mathbb{Z}/n\mathbb{Z}$ dans G ?

5. Soit G un groupe. Dénombrer les morphismes injectifs de $\mathbb{Z}/2\mathbb{Z}$ dans G. Qu'obtient-on si $G = \mathfrak{S}_n$?

6. Soit G un groupe. Dénombrer les morphismes surjectifs de G dans $\mathbb{Z}/2\mathbb{Z}$ puis les morphismes surjectifs de G dans $\mathbb{Z}/p\mathbb{Z}$ pour p un nombre premier. Plus généralement, soit G et H deux groupes. Dénombrer les morphismes surjectifs de G dans H dont le noyau est fixé. étudier le cas $G = \mathfrak{S}_4$ et $H = \mathfrak{S}_3$.

7. Soient H et K deux groupes. On note $p_1 : H \times K \to H$ la projection sur la première coordonnée et $p_2 : H \times K \to K$. Montrer que les applications suivantes sont bien définies et des bijections réciproques l'un de l'autre
$$\begin{aligned} \mathrm{Hom}(G, H \times K) &\longrightarrow \mathrm{Hom}(G, H) \times \mathrm{Hom}(G, K) \\ \varphi &\longmapsto (p_1 \circ \varphi, p_2 \circ \varphi) \end{aligned}$$
$$\begin{aligned} \mathrm{Hom}(G, H) \times \mathrm{Hom}(G, K) &\longrightarrow \mathrm{Hom}(G, H \times K) \\ (\varphi_1, \varphi_2) &\longmapsto (x \mapsto (\varphi_1(x), \varphi_2(x)))\,. \end{aligned}$$

Morale (à retenir): *se donner un morphisme de groupes à valeurs dans un groupe produit, c'est la même chose que se donner un morphisme à valeurs dans chacun des facteurs.*

8. Soit G un groupe. Pour $g \in G$, montrer que l'application
$$\begin{aligned} c_g \colon G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$
est un automorphisme de groupes. Décrire l'automorphisme inverse. On dit que c_g est l'*automorphisme intérieur de G associé à g.*

9. Montrer que l'application
$$\begin{aligned} \mathrm{Int} \colon G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto c_g \end{aligned}$$
est un morphisme de groupes. En déduire une action de G sur lui-même appelée *action de G par conjugaison.* L'image de ce morphisme est l'ensemble des automorphismes intérieurs et noté $\mathrm{Int}(G)$. Quel est le noyau de Int ?

10. Montrer que $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$.

11. Soit $N \triangleleft G$ un sous-groupe distingué. Vérifier que par restriction, l'automorphisme intérieur de G associé à g définit un automorphisme de N **qui n'est plus nécessairement un automorphisme intérieur de** N (considérer le cas d'une transposition de $\mathfrak{S}_3$ agissant sur $\mathfrak{A}_3$). Ainsi, on a un morphisme de groupes de $\mathrm{Int}(G)$ dans $\mathrm{Aut}(N)$ et même un morphisme de groupes de G dans $\mathrm{Aut}(N)$. Quel est le noyau ?

Exercice 18

1. À quoi est isomorphe $\mathbb{C}/\mathbb{R}$?

2. À quoi est isomorphe $\mathbb{R}^*/\mathbb{R}_+^*$?

3. Montrer que l'ensemble des doubles transpositions et du neutre forme un sous-groupe distingué de $\mathfrak{S}_4$. À quoi est isomorphe le quotient ?

4. Montrer que $\mathrm{SL}_n(\mathbb{R})$ est distingué dans $\mathrm{GL}_n(\mathbb{R})$. À quoi est isomorphe le quotient ?

5. Montrer que $\mathrm{GL}^+(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid \det(M) > 0\}$ est distingué. À quoi est isomorphe le quotient ?

6. Soit $\mu_\infty = \{z \in \mathbb{C} \mid \exists n \geq 0,\ z^n = 1\}$ l'ensemble des complexes d'ordre finis. Montrer que $\mu_\infty \cong \mathbb{Q}/\mathbb{Z}$.

Exercice 19 (Sous-groupe dérivé)
Soit G un groupe et $D(G)$ le sous-groupe de G engendré par les commutateurs
$$D(G) = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle.$$

1. Montrer que $D(G)$ est distingué dans G.

2. Montrer que $G/D(G)$ est abélien.

3. Montrer que si H est un groupe abélien et $f\colon G \to H$ un morphisme de groupe, alors il existe un unique $\varphi\colon G/D(G) \to H$ tel que $f = \varphi \circ \pi$ où $\pi\colon G \to G/D(G)$ est la projection canonique.

4. Montrer que pour tout sous-groupe H de G, G/H est abélien si et seulement si H contient $D(G)$.

5 Des groupes en action

Exercice 20 (Où est l'action ?)
Dans les questions suivantes, identifier le groupe et l'action qui sont en jeu et démontrer l'assertion.

1. Soit $n \geq 1$. Il y a $q^n + q^{n-1} + \cdots + q + 1$ droites dans $\mathbb{F}_q^n$.

2. Soient X un ensemble fini et p un nombre premier ne divisant pas le cardinal de S. Tout élément d'ordre une puissance de p de $\mathfrak{S}(X)$ admet un point fixe.

3. Soit G un groupe fini. Si H un sous groupe de G alors l'ordre de H divise l'ordre de G. (Lagrange)

4. Soit $1 \leq k \leq n$. Il y a $\frac{n!}{(n-k)!}$ k-uplets d'éléments distincts de $\{1, 2, \ldots, n\}$.

5. Soit $1 \leq k \leq n$. Il y a $\frac{n!}{k!(n-k)!}$ parties à k-éléments de $\{1, 2, \ldots, n\}$.

6. Dans un groupe fini G, le nombre de conjugués d'un élément $g \in G$ est un diviseur de l'ordre de G.

7. Si G un groupe infini admettant un sous groupe strict d'indice fini alors G n'est pas simple.

8. Tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

9. Soit A, B, C trois points de $\mathbb{R}^n$. Montrer que $\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}$. (Chasles)

Exercice 21 (L'incontournable théorème de Cayley)
Soit G un groupe fini d'ordre $n \geq 1$. Montrer que G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.
Corollaire : En déduire que G est un sous-groupe de $\mathrm{GL}_n(k)$ pour k un corps quelconque.

Exercice 22 (Action par conjugaison)
Soit G un groupe. On considère l'action de G sur lui-même par conjugaison.

1. Montrer que l'action par conjugaison induit un morphisme de groupe $G \to \mathrm{Aut}(G)$.
   Quel est son noyau ? est-ce que le morphisme est surjectif ?

2. Quel est le stabilisateur d'un élément pour cette action ?

3. Quels sont les points fixes de l'action ?

4. Montrer que si G est d'ordre fini le cardinal d'une classe de conjugaison divise l'ordre de G.

5. Application au p-groupes : on suppose ici que G est d'ordre fini une puissance de p.
   (a) Montrer que le cardinal du centre de G est un multiple de p.
   (b) En déduire que le centre d'un p-groupe n'est pas trivial.

Exercice 23 (une petite généralisation des sous-groupes d'indice 2)
Soit G un groupe fini, p le plus petit nombre premier divisant l'ordre de G et H un sous groupe d'indice p. On va montrer que H est distingué. On considère l'action de H sur G/H par multiplication à gauche.

1. Montrer que cette action induit un morphisme $\varphi\colon H \to \mathfrak{S}_{p-1}$.

2. En considérant les nombres premiers divisant l'ordre de H, montrer que le morphisme φ est forcément trivial.

3. Conclure que H est distingué.

4. Donner un exemple où le résultat est faux si on suppose que p est un diviseur premier de l'ordre de G sans être le plus petit.

Exercice 24 (Le théorème de Cauchy)
Soit G un groupe fini d'ordre n et soit p un nombre premier divisant n. On considère l'ensemble

$$X = \{(g_0, g_1, \dots, g_{p-1}) \in G^p \mid g_0 g_1 \cdots g_{p-1} = 1\}.$$

1. Quel est le cardinal de X ?

   On munit X de l'action de $\mathbb{Z}/p\mathbb{Z}$ suivante

$$(k, (g_0, g_1, \dots, g_{p-1})) \in \mathbb{Z}/p\mathbb{Z} \times X \longmapsto (g_{0+k}, g_{1+k}, \dots, g_{p-1+k}) \in X.$$

2. Écrire l'équation aux classes pour cette action.
3. Montrez que G admet un élément d'ordre p.

Exercice 25
Combien existe-t-il d'anagramme du mot "ABRACADABRA" ?

Exercice 26 (Un petit casse-tête)
On considère le jeu suivant. On choisit un entier $n \geq 1$. et on écrit une et une seule fois tous les nombres de 1 à n dans un ordre quelconques à la suite les un des autres (un exemple pour $n = 5 :\ 2, 1, 5, 4, 3$). Les opérations qu'on s'autorise sont les suivantes : on choisit k tel que $1 \leq k \leq n$ et on fait tourner vers la droite les k premiers nombres de la suite (par exemple, dans l'exemple précédent en prenant $k = 3$ on obtient la suite $5, 2, 1, 3$). Est-il toujours possible après un nombre fini d'opération d'obtenir la suites ordonnées $1, 2, \dots, n$.

Exercice 27 (Un classique : les colliers de perles (Dev))
Combien existe-t-il de collier de perles différents avec 10 perles et 3 couleurs de perles différentes (On s'autorise à ne pas utiliser toutes les couleurs).

Exercice 28 (Un autre classique : groupe du cube et coloriage (Dev))
Soit $\mathcal{C}$ un cube dans un espace affine de dimension 3. Soit G le groupe des isométries positives préservant le cube.

1. Monter que G est isomorphe à $\mathfrak{S}_4$.
2. En déduire le nombre de coloriages différents de $\mathcal{C}$ avec 6 couleurs.

Exercice 29 (Un peu de géométrie affine)
On rappel qu'un **espace affine** est un ensemble $\mathcal{A}$ muni d'une action d'un espace vectoriel E qui est *simplement transitive* (pour tout $A, B \in \mathcal{A}$, il existe un unique $u \in E$ tel que $u \cdot A = B$). Pour $A, B \in \mathcal{A}$ et $u \in E$, on notera $A + u$ l'image de A sous l'action de u et $\overrightarrow{AB}$ l'unique vecteur qui envoie A sur B.

1. Montrer la relation de Chasles : pour tout $A, B, C \in \mathcal{A}$, $\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}$.
2. Définir la notion de sous-espace affine en terme d'orbite pour l'action.

Une application $f \colon \mathcal{A} \to \mathcal{A}$ est une **application affine** s'il existe $\varphi \colon E \to E$ linéaire telle que pour tout $A, B \in \mathcal{A}$, $\overrightarrow{f(A)f(B)} = \varphi\left(\overrightarrow{AB}\right)$.

3. Montrer qu'une application affine préserve l'alignement (la réciproque est vraie lorsqu'on travaille avec des $\mathbb{R}$-espaces vectoriels mais c'est plus compliqué à démontrer).
4. Montrer qu'une application affine envoie un barycentre de $A_1, \dots, A_n \in \mathcal{A}$ sur le barycentre des images avec les mêmes poids.
5. Montrer que la composée de deux applications affines est aussi une application affine.

On notera $\mathrm{GA}(\mathcal{A})$ l'ensemble des applications affines bijectives.

6. Montrer que $\mathrm{GA}(\mathcal{A})$ forme un groupe pour la composition.

7. Montrer que l'application qui envoie une élément $f \in \mathrm{GA}(\mathcal{A})$ sur l'application linéaire associée φ défini un morphisme de groupe surjectif $L\colon \mathrm{GA}(\mathcal{A}) \to \mathrm{GL}(E)$ dont le noyau est isomorphe à E.

8. soit G un sous groupe fini de $\mathrm{GA}(\mathcal{A})$. Montrer qu'il existe un point fixe commun à tous les éléments de G.