ACTIONS DE GROUPES

Trois niveaux de difficulté/longueur :

— Piste bleue : questions **1)** à **5)**.

— Piste rouge : questions **1)** à **7)**.

— Piste noire : tout le devoir.

1 ACTIONS DE GROUPES

Pour tout groupe G et tout ensemble X, on appelle *action de G sur X* toute application $(g,x) \longmapsto g \cdot x$ de $G \times X$ dans X pour laquelle pour tout $x \in X$: $1_G \cdot x = x$ et pour tous $g, g' \in G$ et $x \in X$: $(gg') \cdot x = g \cdot (g' \cdot x)$.

Attention, aucun symbole ne désigne la loi de G, le produit de deux éléments x et y de G est simplement noté xy. En revanche, dans la notation $g \cdot x$, le point $\cdot$ désigne l'action d'un élément g de G sur un élément x de X.

On ADMET le *théorème de Lagrange* selon lequel pour tout groupe fini G et tout sous-groupe H de G, $|H|$ divise $|G|$.

1) a) Soit G un groupe. Vérifier que l'application $(g,x) \longmapsto gx$ est une action de G sur lui-même. On l'appelle l'*action de G sur lui-même par translation à gauche*.

b) Soit G un groupe. Vérifier que l'application $(g,x) \longmapsto gxg^{-1}$ est une action de G sur lui-même. On l'appelle l'*action de G sur lui-même par conjugaison*.

c) Soient E un ensemble. Vérifier que l'application $(\sigma,x) \longmapsto \sigma(x)$ est une action du groupe symétrique S_E sur E.

Soient G un groupe, X un ensemble et $\cdot$ une action de G sur X.

2) Pour tous $x, y \in X$, on dit que $x \sim y$ si $y = g \cdot x$ pour un certain $g \in G$.

a) Montrer que $\sim$ est une relation d'équivalence sur X.

Pour tout $x \in X$, la classe d'équivalence de x pour $\sim$ est notée $\mathrm{cl}_G(x)$ et appelée l'*orbite de x sous G*.

b) Montrer que $G_x = \left\{ g \in G \mid \quad g \cdot x = x \right\}$ est un sous-groupe de G pour tout $x \in X$. On l'appelle le *stabilisateur de x dans G*.

3) On suppose G fini. Soit $x \in X$ fixé. On note φ_x l'application $g \longmapsto g \cdot x$ de G dans $\mathrm{cl}_G(x)$.

a) Montrer que pour tous $g, g' \in G$: $\quad \varphi_x(g) = \varphi_x(g') \quad \Longleftrightarrow \quad g' \in gG_x$.

b) En déduire que pour tout $y \in \mathrm{cl}_G(x)$: $\quad \left|\varphi_x^{-1}\big(\{y\}\big)\right| = |G_x|, \quad$ puis que $|G| = \left|\mathrm{cl}_G(x)\right| \times |G_x|$.

4) On suppose que $|G| = p^n$ pour certains $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$. On pose $\mathrm{Fix}_G(X) = \left\{ x \in X \mid \quad \forall g \in G, \quad g \cdot x = x \right\}$.

a) Montrer que $\left|\mathrm{cl}_G(x)\right|$ est divisible par p pour tout $x \in X \setminus \mathrm{Fix}_G(X)$.

b) En déduire que : $\quad |X| \equiv \left|\mathrm{Fix}_G(X)\right| \ [p]$.

2 QUELQUES EXEMPLES

Différentes actions de groupes sont exploitées dans cette partie. Les notations $\sim$, $\mathrm{cl}_G(x)$ et G_x de la question **2)** pourront être utilisées librement, mais leur signification dépend dans chaque question de l'action de groupe étudiée.

5) Soient $p \in \mathbb{P}$ et G un groupe fini de cardinal p^2. On ADMET que l'ensemble des éléments de G qui commutent à tout élément de G, appelé le *centre de G* et noté $\mathrm{Z}(G)$, est un sous-groupe de G.

a) Montrer, en exploitant l'action de G sur lui-même par conjugaison de la question **1)b)**, que le cardinal de $\mathrm{Z}(G)$ est divisible par p.

b) Montrer que l'ensemble $\left\{ x^k z \mid \quad k \in \mathbb{Z}, \quad z \in \mathrm{Z}(G) \right\}$ est un sous-groupe commutatif de G pour tout $x \in G$.

c) En déduire que G est commutatif.

Ce résultat de commutativité est très spécifique aux groupes de cardinal p^2 et faux en toute généralité des groupes de cardinaux $p^3, p^4 \ldots$ comme le montre le résultat de la question suivante.

6) Soit $m \in \mathbb{N}^*$. On pose $\theta = \dfrac{2\pi}{m}$, puis $R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ et $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, et enfin $D_m = \left\{ R^i S^j \mid \quad i, j \in \mathbb{Z} \right\}$.

a) Calculer R^k et S^k pour tout $k \in \mathbb{Z}$ et vérifier que $SR = R^{-1}S$.

b) Montrer que D_m est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$, non commutatif si $m \geqslant 3$.

c) Que vaut $|D_m|$? Attention, on ne veut pas une majoration de $|D_m|$, mais une égalité.

7) Soient $p \in \mathbb{P}$ et G un groupe fini de cardinal divisible par p.

a) Montrer que si $p = 2$, G contient un élément $x \neq 1_G$ pour lequel $x^{-1} = x$, i.e. $x^2 = 1_G$.

On suppose à présent $p \geqslant 3$ et on pose $X = \left\{ (x_1, \ldots, x_p) \in G^p \mid \quad x_1 x_2 \ldots x_p = 1_G \right\}$.

b) Montrer que $|X| = |G|^{p-1}$.

c) Montrer que l'application $(x_1, \ldots, x_p) \overset{\pi}{\longmapsto} (x_p, x_1, \ldots, x_{p-1})$ est une permutation de X, puis que $\pi \neq \mathrm{Id}_X$ — c'est ici que l'hypothèse $p \geqslant 3$ est censée servir !

On **ADMET** pour gagner du temps que $A = \left\{ \pi^k \mid \quad k \in \mathbb{Z} \right\}$ est un sous-groupe de S_X.

d) Montrer que $\pi^k \neq \mathrm{Id}_X$ pour tout $k \in [\![1, p-1]\!]$, puis que $|A| = p$.

e) Montrer, en exploitant l'action $\big(\alpha, (x_1, \ldots, x_p)\big) \longmapsto \alpha(x_1, \ldots, x_p)$ de A sur X, que G contient un élément $x \neq 1_G$ pour lequel $x^p = 1_G$ (*théorème de Cauchy*).

3 Sous-groupes finis de $\mathrm{GL}_n(\mathbb{R})$ et $\mathrm{GL}_n(\mathbb{Z})$

8) Montrer que pour tout $n \geqslant 2$, $\mathrm{GL}_n(\mathbb{R})$ possède des sous-groupes finis de cardinal aussi grand qu'on veut.

Soit $n \in \mathbb{N}^*$ désormais fixé. On **ADMET** que l'ensemble $\mathcal{M}_n(\mathbb{Z})$ des matrices carrées de taille n à coefficients dans $\mathbb{Z}$ est un sous-anneau de $\mathcal{M}_n(\mathbb{R})$. Son groupe des inversibles est noté $\mathrm{GL}_n(\mathbb{Z})$. Attention, une matrice de $\mathrm{GL}_n(\mathbb{Z})$ n'est pas seulement une matrice inversible à coefficients dans $\mathbb{Z}$, mais une matrice inversible à coefficients dans $\mathbb{Z}$ dont l'inverse est aussi à coefficients dans $\mathbb{Z}$.

On notera $\mathbb{F}_3$ le corps $\dfrac{\mathbb{Z}}{3\mathbb{Z}} = \left\{ \overline{0}, \overline{1}, \overline{2} \right\}$ à 3 éléments. On **ADMET** que la théorie des matrices qu'on a commencé à développer sur les corps $\mathbb{R}$ et $\mathbb{C}$ aurait pu être développée à l'identique sur n'importe quel corps, notamment $\mathbb{F}_3$.

Pour tout $k \in \mathbb{Z}$, l'image de k dans $\mathbb{F}_3$ est notée $\overline{k}$ et l'application $k \longmapsto \overline{k}$ est un morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{F}_3$. Pour toute matrice $M \in \mathcal{M}_n(\mathbb{Z})$, on note $\overline{M}$ l'image de M dans $\mathcal{M}_n(\mathbb{F}_3)$, i.e. la matrice $\left(\overline{m_{ij}}\right)_{1 \leqslant i,j \leqslant n}$. On **ADMET** que l'application $M \overset{\rho}{\longmapsto} \overline{M}$ est un morphisme d'anneaux de $\mathcal{M}_n(\mathbb{Z})$ dans $\mathcal{M}_n(\mathbb{F}_3)$ et que sa restriction $\rho|_{\mathrm{GL}_n(\mathbb{Z})}$ est un morphisme de groupes de $\mathrm{GL}_n(\mathbb{Z})$ dans $\mathrm{GL}_n(\mathbb{F}_3)$.

Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$.

9) Montrer que si $G \cap \mathrm{Ker}\,\rho = \left\{ I_n \right\}$, alors $|G| \leqslant 3^{n^2}$.

On suppose désormais que $G \cap \mathrm{Ker}\,\rho \neq \left\{ I_n \right\}$. L'entier $\left| G \cap \mathrm{Ker}\,\rho \right|$ est ainsi supérieur à 2, donc possède un diviseur premier p. D'après le théorème de Cauchy de la question **7)e)**, $G \cap \mathrm{Ker}\,\rho$ contient une matrice $M \neq I_n$ pour laquelle $M^p = I_n$.

10) **a)** Montrer que $M = I_n + 3A$ pour une certaine matrice non nulle $A \in \mathcal{M}_n(\mathbb{Z})$.

On note d le PGCD des coefficients de A, non nul car $A \neq 0$, et B la matrice de $\mathcal{M}_n(\mathbb{Z})$ pour laquelle $A = dB$.

b) Montrer par un raisonnement arithmétique que $p = 3$ et $d = 1$, puis dénicher une contradiction.

En résumé, les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$ sont tous de cardinal inférieur à 3^{n^2}.