

Feuille d'exercices n° 3

Exercice 1

Soient \mathbb{k} un corps et $G \subset GL(2, \mathbb{k})$ le sous-groupe des matrices 2×2 triangulaires supérieures. Déterminer si chacune des conditions suivantes définit un sous-groupe distingué de G , et si oui, utiliser le théorème d'isomorphisme pour identifier le quotient :

- (i) $a_{11} = 1$;
- (ii) $a_{12} = 0$;
- (iii) $a_{11} = a_{22}$;
- (iv) $a_{11} = a_{22} = 1$.

Solution 1

Le groupe G est

$$G = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \mid a_{11}, a_{22} \in \mathbb{k}^*, a_{12} \in \mathbb{k} \right\}$$

La loi de composition sur G est :

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} \quad (1)$$

- (i) Le sous-groupe défini par la condition $a_{11} = 1$ est

$$K = \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \mid b \in \mathbb{k}, c \in \mathbb{k}^* \right\}$$

Posons

$$\varphi: G \rightarrow \mathbb{k}^*, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

La relation (1) assure que φ est un morphisme, et on constate que $K = \ker \varphi$; en particulier K est distingué dans G . De plus φ est surjectif, car étant donné $a \in \mathbb{k}^*$ la matrice $\begin{pmatrix} a & 0 \\ 1 & 0 \end{pmatrix}$ est un antécédent

de a par φ . Le théorème d'isomorphisme permet de conclure que le quotient G/K est isomorphe à \mathbb{k}^* .

Remarque : on peut vérifier directement avec la définition que K est distingué dans G (c'est-à-dire vérifier que pour toutes matrices $A \in K$ et $B \in G$ on a $BAB^{-1} \in K$) ; ceci étant il faut identifier K à un noyau pour utiliser le théorème d'isomorphisme...

On peut chercher à voir s'il existe un sous-groupe H de G tel que $G = K \rtimes H$. Posons

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{k}^* \right\}$$

On voit que $K \cap H = \{\text{id}\}$ et $KH = G$ (à nouveau par (1)) dont H convient.

Remarquons que H n'est pas uniquement déterminé ; par exemple

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{k}^* \right\}$$

convient aussi.

En fait il y a une infinité d'autres choix possibles pour H .

(ii) Le sous-groupe défini par la condition $a_{12} = 0$ est

$$K = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{k}^* \right\}.$$

Si $\mathbb{k} \neq \mathbb{F}_2$, alors ce groupe n'est pas distingué dans G : pour tout $b \neq 0$ et $a \neq c$ nous avons

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & bc \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b(c-a) \\ 0 & c \end{pmatrix} \notin K.$$

Si $\mathbb{k} = \mathbb{F}_2$, alors on ne peut pas choisir deux éléments $a \neq c$ dans \mathbb{k}^* , et donc le contre-exemple ne tient plus. Dans ce cas le groupe K est trivial, donc en particulier distingué dans G ...

(iii) Le sous-groupe défini par la condition $a_{11} = a_{22}$ est

$$K = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{k}^*, b \in \mathbb{k} \right\}.$$

Posons

$$\varphi: G \rightarrow \mathbb{k}^*, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \frac{a}{c}$$

La relation (1) montre que φ est un morphisme, et donc $K = \ker \varphi$ est distingué dans G . De plus φ est surjectif, donc le théorème d'isomorphisme permet de conclure que le quotient G/K est isomorphe à \mathbb{k}^* . Notons que $G = K \rtimes H$ pour le choix suivant de sous-groupe H :

$$K = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{k}^* \right\}.$$

À noter qu'il y a une infinité d'autres choix possibles pour H .

(iv) Le sous-groupe défini par la condition $a_{11} = a_{22} = 1$ est

$$K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{k} \right\}$$

Posons

$$\varphi: G \rightarrow \mathbb{k}^* \times \mathbb{k}^*, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

De nouveau la relation (1) assure que φ est un morphisme surjectif, donc $K = \ker \varphi$ est distingué ; d'après le théorème d'isomorphisme le quotient G/K est isomorphe à $\mathbb{k}^* \times \mathbb{k}^*$.

Notons que $G = K \rtimes H$ par exemple pour le choix suivant de sous-groupe H :

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{k}^* \right\}$$

À noter qu'il y a une infinité d'autres choix possibles pour H .

Les exemples dans cet exercice peuvent donner la fausse idée que dès que $K \subset G$ est un sous-groupe distingué, il existe un sous-groupe $H \subset G$ tel que $G = K \rtimes H$. C'est faux ; considérer par exemple $G = \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ et $K = \{\bar{0}, \bar{2}\}$ et se convaincre qu'un tel H n'existe pas dans ce cas...

Exercice 2

On se propose de montrer que le groupe alterné \mathcal{A}_4 ne contient aucun sous-groupe d'ordre 6.

- (1) En général, montrer que si $H \subset G$ est un sous-groupe d'indice 2, alors H est distingué dans G .
- (2) Rappeler la liste des classes de conjugaison de \mathcal{A}_4 et leurs cardinaux.
- (3) Conclure.

Solution 2

- (1) Soit $H \subset G$ d'indice 2. Si g appartient à H , alors $gH = Hg = H$ (l'hypothèse indice 2 est inutile ici). Si g n'appartient pas à H , alors puisque H est d'indice 2 nous avons

$$G = H \cup gH = H \cup Hg.$$

On voit que $gH = Hg = G \setminus H$; en particulier $gH = Hg$, autrement dit H est distingué dans G .

- (2) Le groupe \mathcal{A}_4 compte quatre classes de conjugaison, qui sont :
- ◊ la classe de l'identité, de cardinal 1,
 - ◊ la classe des doubles transposition, de cardinal 3,
 - ◊ une première classe de 3-cycles, de cardinal 4,
 - ◊ une deuxième classe de 3-cycles, de cardinal 4.

Notons que dans \mathcal{S}_4 la réponse serait différente : les 3-cycles forment une seule classe de conjugaison dans \mathcal{S}_4 , de cardinal 8.

- (3) Supposons que $H \subset \mathcal{A}_4$ soit un sous-groupe d'ordre 6 ; il est ainsi d'indice 2 dans \mathcal{A}_4 . La question (1) assure que H est donc distingué dans \mathcal{A}_4 . Alors H devrait être union de classes de conjugaison, dont celle du neutre, mais il n'est pas possible d'obtenir 6 en sommant des nombres parmi $\{1, 3, 4, 4\}$: contradiction.

Remarque : d'après (2) les cardinaux possibles pour un sous-groupe distingué de \mathcal{A}_4 sont

- ◊ 1 (sous-groupe trivial),
- ◊ $4 = 1 + 3$ (c'est le groupe de KLEIN engendré par les double-transpositions),
- ◊ $5 = 1 + 4$ (en fait impossible par LAGRANGE),
- ◊ $8 = 1 + 3 + 4$ (en fait impossible par LAGRANGE),
- ◊ $9 = 1 + 4 + 4$ (en fait impossible par LAGRANGE),
- ◊ $12 = 1 + 3 + 4 + 4$ (groupe \mathcal{A}_4 entier).

Exercice 3

Soit p un nombre premier. Soit $n \geq 1$ un entier. Soient G un groupe d'ordre p^n et $Z(G)$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrer que $H \cap Z(G) \neq \{e\}$.
2. Montrer que l'ordre de $Z(G)$ est > 1 (sans utiliser le premier point).

Indication : faire agir G par conjugaison sur H .

Solution 3

Soit p un nombre premier. Soit $n \geq 1$ un entier. Soient G un groupe d'ordre p^n et $Z(G)$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrons que $H \cap Z(G) \neq \{e\}$. Faisons agir G par conjugaison sur H ; notons que c'est possible car H étant distingué dans G nous avons $\forall g \in G, gHg^{-1} \subset H$.

L'ordre de H est une puissance de p soit p^β car $|H|$ divise $|G|$ qui est une puissance de p . L'ordre de H est aussi somme des cardinaux des orbites pour cette action ; chacune de ces orbites a pour cardinal un diviseur de $|G|$, c'est-à-dire de p^n donc une puissance de p .

Raisonnons par l'absurde : supposons que $Z(G) \cap H = \{e\}$; alors une seule des orbites est réduite à un seul élément¹ : l'orbite de e . Nous avons alors

$$|H| = p^\beta = 1 + \text{somme de puissances de } p$$

contradiction. Par suite $Z(G) \cap H \neq \{e\}$.

2. Montrons que l'ordre de $Z(G)$ est > 1 . Nous allons encore appliquer la formule des classes. Remarquons que les orbites de G pour l'action de G par conjugaison sur lui-même ont pour cardinal des puissances de p ; en effet ces cardinaux sont des diviseurs de $|G| = p^n$.

Raisonnons par l'absurde : supposons que $|Z(G)| = 1$, alors

$$p^n = |G| = 1 + \text{somme de puissances de } p$$

contradiction. Il en résulte que $|Z(G)| > 1$.

Exercice 4

Soit G un groupe. Désignons par $\text{Aut}(G)$ le groupe des automorphismes de G . Si a appartient à G , notons $\varphi(a)$ l'application

$$\varphi(a): G \rightarrow G \qquad g \mapsto aga^{-1}.$$

- a) Montrer que pour tout a dans G l'application $\varphi(a)$ est un automorphisme de G (appelé automorphisme intérieur de G).

1. $\mathcal{O}_g = \{g\} \iff \{h \cdot g \mid g \in G\} = \{g\} \iff \{hgh^{-1} \mid g \in G\} = \{g\} \iff \forall h \in G \ hgh^{-1} = g$

- b) Montrer que $\varphi: G \rightarrow \text{Aut}(G)$, $g \mapsto \varphi(g)$ est un morphisme de groupes de G dans $\text{Aut}(G)$.
- c) Notons $\text{Int}(G)$ l'ensemble des automorphismes intérieurs de G . Montrer que $\text{Int}(G)$ est un sous-groupe distingué de $\text{Aut}(G)$.
- d) Notons $Z(G)$ le centre de G . Montrer que $\text{Int}(G) \simeq G/Z(G)$.

Solution 4

- a) Il faut montrer que $\varphi(a)$ est un morphisme de G dans G ; bien sûr $\varphi(a)(e) = e$. Il reste donc à montrer que $\varphi(a)(gg') = \varphi(a)(g)\varphi(a)(g')$. Or

$$\varphi(a)(gg') = agg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \varphi(a)(g)\varphi(a)(g').$$

Montrons que $\ker \varphi(a) = \{e\}$. Soit $g \in \ker \varphi(a)$, alors $\varphi(a)(g) = e$, autrement dit $aga^{-1} = e$ d'où $g = a^{-1}a = e$. Ainsi $\varphi(a)$ est un morphisme injectif.

Soit g dans G . On a $g = a(a^{-1}ga)a^{-1} = \varphi(a)(a^{-1}ga)$. Autrement dit $\varphi(a)$ est surjectif.

Il en résulte que $\varphi(a)$ est un automorphisme de G et $(\varphi(a))^{-1} = \varphi(a^{-1})$.

- b) D'une part $\varphi(e)(g) = ege^{-1} = g$, i.e. $\varphi(e) = \text{id}$. D'autre part

$$\varphi(a) \circ \varphi(a')(g) = a(a'ga'^{-1})a^{-1} = (aa')g(aa')^{-1} = \varphi(aa')(g)$$

c'est-à-dire $\varphi(a) \circ \varphi(a') = \varphi(aa')$. Par suite φ est un morphisme de groupes de G dans $\text{Aut}(G)$.

- c) $\text{Int}(G)$ est l'image de G par le morphisme de groupes φ ; c'est donc un sous-groupe de $\text{Aut}(G)$.

Soit τ un automorphisme de G ; alors

$$\tau \circ \varphi(a) \circ \tau^{-1}(g) = \tau(a\tau^{-1}(g)a^{-1}) = \tau(a)\tau(\tau^{-1}(g))\tau(a^{-1}) = \tau(a)g\tau(a^{-1})$$

Ainsi $\tau \circ \varphi(a) \circ \tau^{-1} = \varphi(\tau(a))$ appartient à $\text{Im } \varphi$. Le groupe $\text{Int}(G)$ est distingué dans $\text{Aut}(G)$.

- d) D'une part $\ker \varphi$ est le centre $Z(G)$ de G^2 , d'autre part $\text{Im } \varphi = \text{Int}(G)$ (voir c)). Le théorème d'isomorphisme assure que $\text{Int}(G) \simeq G/Z(G)$.

Exercice 5 [Formule de BURNSIDE et coloriage de polyèdres]

1. Soit G un groupe fini agissant sur un ensemble fini X . Pour tout $x \in X$ on désigne par \mathcal{O}_x l'orbite de x par l'action de G et par G_x son stabilisateur.

- a) Soient $x \in X$ et $y \in \mathcal{O}_x$. Trouvez $z \in G$ tel que

$$G_y = z^{-1}G_xz.$$

- b) Montrer que pour tout $x \in X$

$$|G| = \sum_{y \in \mathcal{O}_x} |G_y|.$$

- c) En déduire que

$$|\Omega| = \frac{1}{|G|} \sum_{x \in X} |G_x|$$

où $\Omega = \{\mathcal{O}_x \mid x \in X\}$ est l'ensemble des orbites dans X par l'action de G .

- d) En décomposant de deux façons différentes l'ensemble $F = \{(g, x) \in G \times X \mid g \cdot x = x\}$ déduire de la question précédente la formule de BURNSIDE

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

où $\text{Fix}(g)$ est l'ensemble des points $x \in X$ tels que $g \cdot x = x$.

2. On cherche maintenant à déterminer le nombre de façons de colorier les faces et les arêtes d'un tétraèdre régulier, où k couleurs sont disponibles, à chaque face et à chaque arête étant attribuée une couleur et une seule. Le tétraèdre T est vu comme un sous-ensemble de l'espace vectoriel \mathbb{R}^3 et on le suppose centré en 0.

Nous identifions deux coloriages du tétraèdre s'il existe une rotation R de l'espace euclidien \mathbb{R}^3 qui préserve le tétraèdre, i.e. $R(T) = T$, et qui envoie le premier coloriage sur le second.

2. $\ker \varphi = \{g \in G \mid \varphi(g) = \text{id}\} = \{g \in G \mid \forall h \in G, \varphi(g)(h) = h\} = \{g \in G \mid \forall h \in G, ghg^{-1} = h\} = \{g \in G \mid \forall h \in G, gh = hg\} = Z(G)$

- a) Soit X l'ensemble des coloriage où on interdit cette identification. Quel est le cardinal de X ?
- b) Montrer que l'ensemble des rotations préservant T , muni de la loi de composition, est un groupe. Notons G ce groupe. On admet qu'il est fini et plus précisément que $|G| = 12$:
- l'identité $\text{id}_{\mathbb{R}^3}$;
 - 3 rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π ;
 - 8 rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm 2\pi/3$.
- c) Le groupe G agit naturellement sur X , et chaque coloriage du tétraèdre correspond à une orbite \mathcal{O}_x dans X par l'action de G . Exprimer le nombre de coloriage du tétraèdre en fonction de k .

Solution 5

1. a) Soient $x \in X$ et $y \in \mathcal{O}_x$. Il existe $g \in G$ tel que $y = g \cdot x$. Soit $w \in G_x$, alors $w \cdot x = x$. D'une part $w \cdot x = w \cdot (g^{-1}y)$, d'autre part $x = g^{-1}y$. Par conséquent $w \cdot x = x$ se réécrit $w \cdot (g^{-1}y) = g^{-1}y$ ou encore $(gwg^{-1}) \cdot y = y$; autrement dit gwg^{-1} appartient à G_y et $gG_xg^{-1} \subset G_y$. Un raisonnement analogue conduit à $G_y \subset gG_xg^{-1}$. Il s'en suit que $G_y = gG_xg^{-1}$ et que $z = g^{-1}$ convient.
- b) D'après a) $G_y = gG_xg^{-1}$ donc $|G_y| = |G_x|$ et

$$\sum_{y \in \mathcal{O}_x} |G_y| = \sum_{y \in \mathcal{O}_x} |G_x| = |G_x| \sum_{y \in \mathcal{O}_x} 1 = |G_x| |\mathcal{O}_x|.$$

Or l'application

$$G/G_x \rightarrow \mathcal{O}_x, \quad \bar{g} \mapsto g \cdot x$$

est bien définie et est une bijection ; par suite $|G/G_x| = |\mathcal{O}_x|$, i.e. $|G| = |\mathcal{O}_x| |G_x|$. Ainsi $\sum_{y \in \mathcal{O}_x} |G_y| = |G|$.

c) Nous avons

$$\sum_{x \in X} |G_x| = \sum_{\mathcal{O}_x \subset \Omega} \sum_{y \in \mathcal{O}_x} |G_y|.$$

D'après b) $\sum_{y \in \mathcal{O}_x} |G_y| = |G|$ d'où

$$\sum_{x \in X} |G_x| = \sum_{\mathcal{O}_x \subset \Omega} |G| = |G| \sum_{\mathcal{O}_x \subset \Omega} 1 = |G| |\Omega|.$$

Finalement

$$|\Omega| = \frac{1}{|G|} \sum_{x \in X} |G_x|.$$

d) Le groupe G est fini ; désignons par g_1, g_2, \dots, g_p ses éléments. L'ensemble X est fini ; désignons par x_1, x_2, \dots, x_q ses éléments. D'une part

$$\begin{aligned} F &= \{(g, x) \in G \times X \mid g \cdot x = x\} \\ &= \{(g, x) \in G \times X \mid x \in \text{Fix}(g)\} \\ &= \left(\{g_1\} \times \text{Fix}(g_1) \right) \cup \left(\{g_2\} \times \text{Fix}(g_2) \right) \cup \dots \cup \left(\{g_p\} \times \text{Fix}(g_p) \right) \end{aligned}$$

d'où $|F| = \sum_{g \in G} |\text{Fix}(g)|$.

D'autre part

$$\begin{aligned} F &= \{(g, x) \in G \times X \mid g \cdot x = x\} \\ &= \{(g, x) \in G \times X \mid g \in G_x\} \\ &= \left(G_{x_1} \times \{x_1\} \right) \cup \left(G_{x_2} \times \{x_2\} \right) \cup \dots \cup \left(G_{x_q} \times \{x_q\} \right) \end{aligned}$$

d'où $|F| = \sum_{x \in X} |G_x|$. Par conséquent $\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |G_x|$. Mais c) assure que $|\Omega| |G| = \sum_{x \in X} |G_x|$.

donc

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

2. On cherche maintenant à déterminer le nombre de façons de colorier les faces et les arêtes d'un tétraèdre régulier, où k couleurs sont disponibles, à chaque face et à chaque arête étant attribuée une couleur et une seule. Le tétraèdre T est vu comme un sous-ensemble de l'espace vectoriel \mathbb{R}^3 et on le suppose centré en 0.

Nous identifions deux coloriage du tétraèdre s'il existe une rotation R de l'espace euclidien \mathbb{R}^3 qui préserve le tétraèdre, *i.e.* $R(T) = T$, et qui envoie le premier coloriage sur le second.

a) Soit X l'ensemble des coloriage où on interdit cette identification. Quel est le cardinal de X ?
 Un tétraèdre régulier a quatre faces S_1, S_2, S_3, S_4 et six arêtes A_1, A_2, \dots, A_6 . En particulier il y a dix objets à colorier. On a donc $|X| = k^{10}$.

b) Montrons que l'ensemble des rotations préservant T , muni de la loi de composition, est un groupe. Voir cours.

Notons G ce groupe. On admet qu'il est fini et plus précisément que $|G| = 12$:

- l'identité $\text{id}_{\mathbb{R}^3}$;
- 3 rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π ;
- 8 rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm 2\pi/3$.

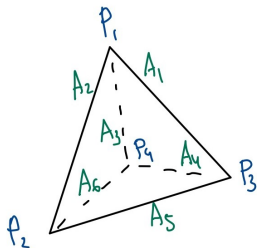
c) Le groupe G agit naturellement sur X , et chaque coloriage du tétraèdre correspond à une orbite \mathcal{O}_x dans X par l'action de G . Exprimons le nombre de coloriage du tétraèdre en fonction de k .

Appliquons la formule de BURNSIDE : soit n le nombre de coloriage, ou de manière équivalente le nombre d'orbites de G sur X . Alors

$$n = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Trois cas sont à distinguer :

- Si $g = \text{id}$, alors $\text{Fix}(g) = X$; par suite $|\text{Fix}(g)| = |X| = k^{10}$.
- Si g est l'une des trois rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π . Alors $|\text{Fix}(g)| = k^6$.



$g : P_1 \rightarrow P_2 \rightarrow P_1$
 une fois A_1, A_2 & A_3 fixés A_1, A_4 & A_5 le sont $\Rightarrow k^3$ choix

$g : P_3 \rightarrow P_4 \rightarrow P_3$
 aucune contrainte sur $A_6 \Rightarrow k$ choix

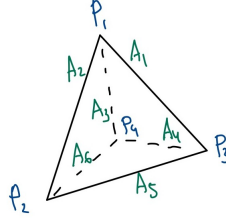
$g : P_1 P_2 P_3 \rightarrow P_1 P_2 P_4 \rightarrow P_1 P_2 P_3$
 autrement dit les faces $P_1 P_2 P_3$ & $P_1 P_2 P_4$ ont même couleur
 $\Rightarrow k$ choix

$g : P_2 P_3 P_4 \rightarrow P_1 P_3 P_4 \rightarrow P_2 P_3 P_4$

Par exemple si g est la rotation d'axe passant par le milieu de l'arête A_2 et le milieu de l'arête A_4 alors

- ◇ g envoie P_1 sur P_2 et P_2 sur P_1 donc une fois A_1, A_2 et A_3 fixés, A_1, A_4 et A_5 le sont $\rightsquigarrow k^3$ choix,
- ◇ g envoie P_3 sur P_4 et P_4 sur P_3 , il n'y a donc aucune contrainte sur $A_6 \rightsquigarrow k$ choix,
- ◇ g envoie $P_1 P_2 P_3$ sur $P_1 P_2 P_4$ et $P_1 P_2 P_4$ sur $P_1 P_2 P_3$, autrement dit les faces $P_1 P_2 P_4$ et $P_1 P_2 P_3$

- ont même couleur $\rightsquigarrow k$ choix,
 $\diamond g$ envoie $P_2P_3P_4$ sur $P_1P_3P_4$ et $P_1P_3P_4$ sur $P_2P_3P_4$, autrement dit les faces $P_1P_3P_4$ et $P_2P_3P_4$ ont même couleur $\rightsquigarrow k$ choix
 soit au total k^6 choix.
- Si g est l'une des huit rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm \frac{2\pi}{3}$. Par conséquent $|\text{Fix}(g)| = k^4$.



g rotation d'axe passant par un sommet et le centre de la face opposée d'angle $\pm \frac{2\pi}{3}$

$$g: A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow A_1$$

$$g: A_4 \rightarrow A_6 \rightarrow A_5 \rightarrow A_4$$

\Rightarrow les arêtes $A_1, A_2 \& A_3$ sont de même couleur, k choix
 les arêtes $A_4, A_5 \& A_6$ sont de même couleur, k choix

- Par exemple si g est une rotation d'axe passant par P_1 et le centre de la face $P_2P_3P_4$, alors
- $\diamond g$ envoie A_1 sur A_2 , A_2 sur A_3 et A_3 sur A_1 donc les arêtes A_1, A_2 et A_3 sont de même couleur $\rightsquigarrow k$ choix,
 - $\diamond g$ envoie A_4 sur A_6 , A_6 sur A_5 et A_5 sur A_4 donc les arêtes A_4, A_5 et A_6 sont de même couleur $\rightsquigarrow k$ choix,
 - $\diamond g$ laisse fixe la face $A_4A_5A_6 \rightsquigarrow k$ choix,
 - $\diamond g$ envoie la face $A_1A_2A_5$ sur la face $A_1A_3A_4$, la face $A_1A_3A_4$ sur la face $A_2A_3A_6$ et la face $A_2A_3A_6$ sur la face $A_1A_2A_5$ donc les faces $A_1A_2A_5, A_1A_3A_4$ et $A_2A_3A_6$ sont de même couleur $\rightsquigarrow k$ choix
- soit au total k^4 choix

Finalement

$$n = \frac{1}{12} (k^{10} + 3 \cdot k^6 + 8 \cdot k^4)$$

Exercice 6

1. Soit G un groupe fini qui opère sur un ensemble fini non vide E . Supposons que G soit d'ordre p^m avec p premier et $m \in \mathbb{N}^*$. Posons

$$E^G = \{x \in E \mid \forall g \in G, g \cdot x = x\}.$$

Montrer que $|E^G| = |E| \pmod{p}$.

2. Soit H un groupe fini d'ordre n . Soit p un diviseur premier de n . Montrer que H contient un élément d'ordre p (lemme de CAUCHY). Indication : faire agir $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble E des (x_1, x_2, \dots, x_p) de H^p tels que $x_1x_2 \dots x_p = e$.
3. Soit H un groupe fini d'ordre n . Soit $m \in \mathbb{N}^*$ tel que pour tout $x \in H$ on ait $x^m = e$. Montrer que n divise une puissance de m .

Solution 6

1. Si x appartient à E , nous notons $\mathcal{O}(x)$ l'orbite de x sous l'action de G . Les éléments de E^G sont exactement les éléments x de E tels que $\mathcal{O}(x) = \{x\}$. Notons $\omega_1, \omega_2, \dots, \omega_r$ les orbites de E de cardinal strictement

supérieur à 1. Si x_i est un élément de ω_i , alors $|\omega_i| = \left| \mathbb{G} / \mathbb{G}_{x_i} \right| = \frac{|\mathbb{G}|}{|\mathbb{G}_{x_i}|}$, c'est donc une puissance de p . Il résulte de l'équation aux classes que

$$|E| = |E^{\mathbb{G}}| + \sum_{i=1}^r |\omega_i| \equiv |E^{\mathbb{G}}| \pmod{p}$$

2. Soit (x_1, x_2, \dots, x_p) un élément de E . Nous avons $x_1 x_2 \dots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \dots x_p x_1 = e$, i.e. $(x_2, x_3, \dots, x_p, x_1)$ appartient à E . Notons c le cycle $(1 \ 2 \ \dots \ p)$ de \mathcal{S}_p . Il s'agit d'un élément d'ordre p qui engendre un sous-groupe cyclique K isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Nous définissons une opération de K sur l'ensemble H^p par

$$c \cdot (x_1, x_2, \dots, x_p) = (x_{c(1)}, x_{c(2)}, \dots, x_{c(p)}) = (x_2, x_3, \dots, x_p, x_1).$$

La remarque ci-dessus montre que E est stable par cette opération. Appliquons alors le résultat de la question précédente à l'opération induite sur E . Nous avons $|E| \equiv |E^K| \pmod{p}$. Le cardinal de E est n^{p-1} (en effet on peut choisir x_1, x_2, \dots, x_{p-1} quelconques, x_p est alors déterminé de manière unique). Comme p divise n , $|E^K|$ est nul modulo p . Or les éléments de E^K sont justement les p -uplets (x, x, \dots, x) avec $x^p = e$. Notons que E^K contient le p -uplet (e, e, \dots, e) ; en particulier E^K est non vide et par suite E^K a un cardinal supérieur à p . Il y a donc au moins $(p-1)$ éléments d'ordre p dans H .

3. Il suffit de montrer que tous les facteurs premiers de n sont des facteurs premiers de m . Soit p un premier divisant n . Le lemme de CAUCHY garantit l'existence d'un élément $x \in H$ d'ordre p . Or par hypothèse $x^m = e$ donc p divise m .

Exercice 7 Soit G un groupe fini. Soit p le plus petit nombre premier divisant $|G|$. Soit H un sous-groupe de G d'indice p . On se propose de montrer que H est distingué dans G .

- a) Montrer que H opère sur l'ensemble des classes à gauche \mathbb{G}/\mathbb{H} par $h \cdot (aH) = (ha)H$ pour tout $h \in H$ et pour tout $a \in G$.
 Quel est le stabilisateur de aH ?
 Quelle est l'orbite de la classe H ?
- b) Montrer que si H n'était pas distingué dans G , alors au moins une des orbites aurait un cardinal $\geq p$.
- c) Conclure.

Solution 7

- a) On peut vérifier que $h \cdot (aH) = (ha)H$ est bien définie : si $aH = bH$, alors $(ha)H = (hb)H$ donc $h \cdot (aH)$ ne dépend pas du représentant a choisi dans une même classe à gauche), et que ceci définit une opération de groupe.

Le stabilisateur de aH est

$$\begin{aligned} G_{aH} &= \{h \in H \mid h \cdot (aH) = aH\} \\ &= \{h \in H \mid (ha)H = aH\} \\ &= \{h \in H \mid a^{-1}ha \in H\} \\ &= \{h \in H \mid h \in aHa^{-1}\} \\ &= H \cap aHa^{-1}. \end{aligned}$$

L'orbite de H est réduite à H :

$$\mathcal{O}_H = \{h \cdot H \mid h \in H\} = \{hH \mid h \in H\} = H.$$

- b) Si H n'est pas distingué dans G , alors il y a au moins une orbite dont le cardinal n'est pas 1 puisque cela signifie qu'il existe $a \in G$ et $h \in H$ tel que $a^{-1}(ha)$ n'appartient pas à H . Puisque le cardinal de cette orbite divise celui de H (donc aussi celui de G par le théorème de LAGRANGE) ce cardinal est au moins p étant donné que p est le plus petit diviseur ≥ 2 de $|G|$.

- c) Si H n'est pas distingué dans G , alors il y a au moins une orbite de cardinal au moins p mais il y a aussi une orbite de cardinal 1 (celle de H).

Rappel : soit K un groupe agissant sur un ensemble X ; X est réunion disjointe des orbites de X sous l'action de G , i.e. $|X| = \sum_{i=1}^p |\mathcal{O}_i|$ où les \mathcal{O}_i sont les orbites de X sous l'action de G .

Puisque H opère sur l'ensemble des classes à gauche, nous avons $|\mathbb{G}/\mathbb{H}| \geq p + 1$: contradiction avec le fait que $|\mathbb{G} : \mathbb{H}| = p$.

$$|\mathbb{G}/\mathbb{H}|$$

Exercice 8

Soit E un espace vectoriel de dimension finie n sur un corps \mathbb{k} .

- a) Faisons opérer le groupe linéaire $G = \text{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par $g \cdot F := g(F)$ pour tout $g \in G$ et tout sous-espace F de E . Quelles sont les orbites pour cette action ?
- b) On prend $\mathbb{k} = \mathbb{Z}/7\mathbb{Z}$ et $n = 5$. Combien E possède-t-il de sous-espaces vectoriels de dimension 3 ?

Solution 8

- a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d . Réciproquement si F et G sont des sous-espaces de dimension d , on choisit une base (f_1, f_2, \dots, f_d) de F que l'on complète en une base $(f_1, f_2, \dots, f_d, f_{d+1}, \dots, f_n)$ de E . De même on peut prendre une base (g_1, g_2, \dots, g_d) de F que l'on complète en une base $(g_1, g_2, \dots, g_d, g_{d+1}, \dots, g_n)$ de E . L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0, 1, \dots, n$.
- b) Fixons un sous-espace F de dimension 3 (on sait qu'il y en a au moins 1). D'après a) le nombre cherché est le cardinal de l'orbite de F sous l'action de $\text{GL}(E)$ ou encore l'ordre de $\text{GL}(E)$ divisé par celui du stabilisateur S de F . Le cardinal de $\text{GL}(E)$ est obtenu en comptant le nombre de bases de E , il vaut

$$(7^5 - 1)(7^5 - 7)(7^5 - 7^2)(7^5 - 7^3)(7^5 - 7^4).$$

En prenant une base de F que l'on complète en une base de E on voit que S est isomorphe au groupe des matrices-bloc de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où $A \in \text{GL}(3, \mathbb{F}_7)$, $B \in \text{M}_{3,2}(\mathbb{F}_7)$ et $C \in \text{GL}(2, \mathbb{F}_7)$. Ainsi

$$|S| = (7^3 - 1)(7^3 - 7)(7^3 - 7^2)(7^2 - 1)(7^2 - 7)7^6.$$

Par suite le cardinal cherché est

$$\begin{aligned} & \frac{(7^5 - 1)(7^5 - 7)(7^5 - 7^2)(7^5 - 7^3)(7^5 - 7^4)}{(7^3 - 1)(7^3 - 7)(7^3 - 7^2)(7^2 - 1)(7^2 - 7)7^6} \\ &= \frac{7 \times 7^2 \times 7^3 \times 7^4 \times (7^5 - 1)(7^4 - 1)(7^3 - 1)(7^2 - 1)(7 - 1)}{7 \times 7^2 \times 7 \times 7^6 \times (7^3 - 1)(7^2 - 1)(7 - 1)(7^2 - 1)(7 - 1)} \\ &= \frac{(7^5 - 1)(7^4 - 1)}{(7^2 - 1)(7 - 1)} \\ &= 140050 \end{aligned}$$

Exercice 9

- a) Combien y a-t-il d'opérations du groupe $\mathbb{Z}/4\mathbb{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?
- b) Soient G et X deux groupes. On dit que G opère par automorphismes sur X si on s'est donné une opération $(g, x) \mapsto g \cdot x$ de G sur X telle que pour tout $g \in G$ l'application $x \mapsto g \cdot x$ soit un automorphisme de X . L'opération de G sur lui-même par translation est-elle une opération par automorphismes ? L'opération de G sur lui-même par conjugaison est-elle une opération par automorphismes ?

- c) Si $G = (\mathbb{Z}/3\mathbb{Z}, +)$ et $X = (\mathbb{Z}/13\mathbb{Z}, +)$ combien y a-t-il d'actions de G sur X par automorphismes ?
- d) Si $G = (\mathbb{Z}/3\mathbb{Z}, +)$ et $X = (\mathcal{S}_3, \circ)$ combien y a-t-il d'actions de G sur X par automorphismes ?

Solution 9

- a) On cherche le nombre de morphismes de $\mathbb{Z}/4\mathbb{Z}$ dans le groupe des permutations \mathcal{S}_5 . Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\bar{1})$) dans \mathcal{S}_5 . Or \mathcal{S}_5 contient
- un élément d'ordre 1 (l'identité),
 - $\binom{5}{2} = 10$ transpositions,
 - $5 \cdot 3 = 15$ doubles transpositions (cinq façons de choisir le point fixe puis trois double transpositions avec les quatre éléments restants),
 - $5 \cdot 6 = 30$ 4-cycles (cinq façons de choisir le point fixe et six 4-cycles dans le groupe des permutations des quatre éléments restants).
- Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.
- b) L'opération de G sur lui-même par translation n'est pas une opération par automorphismes. L'opération de G sur lui-même par conjugaison est une opération par automorphismes.
- c) Le groupe des automorphismes de X est isomorphe au groupe multiplicatif de l'anneau $\mathbb{Z}/13\mathbb{Z}$ (en effet si on pose $\varphi_a(x) = ax$ on peut vérifier que $a \mapsto \varphi_a$ est un isomorphisme de $(\mathbb{Z}/13\mathbb{Z})^\times$ sur $\text{Aut}(X)$) lequel est isomorphe au groupe additif $\mathbb{Z}/12\mathbb{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ ou encore le nombre d'éléments de $\mathbb{Z}/12\mathbb{Z}$ d'ordre divisant 3. Il y a ainsi 3 possibilités.
- d) Les seuls automorphismes de \mathcal{S}_3 sont intérieurs. Le groupe des automorphismes de \mathcal{S}_3 est donc isomorphe à \mathcal{S}_3 quotienté par son centre, c'est-à-dire à \mathcal{S}_3 . On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans \mathcal{S}_3 et il y a 3 possibilités.

Exercice 10

1. Soit G un groupe fini agissant sur un ensemble fini X . En considérant l'ensemble

$$E = \{(g, x) \in G \times X \mid g \cdot x = x\},$$

calculer le nombre moyen de points fixes d'un élément de G . Que dire en particulier si l'action est transitive ? Que dire de la moyenne du nombre de points fixes d'une permutation aléatoire ?

2. Combien de colliers de 9 perles différents peut-on faire avec 4 perles bleues, 3 perles blanches et 2 perles oranges ?

Solution 10

1. Désignons par $\text{Fix}(g) = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points fixes de g dans X .

◇ Soient $x \in X$ et $y \in \mathcal{O}_x$. Montrons que G_y et G_x sont conjugués.

Il existe $g \in G$ tel que $y = g \cdot x$. Soit $w \in G_x$, alors $w \cdot x = x$. D'une part $w \cdot x = w \cdot (g^{-1}y)$, d'autre part $x = g^{-1}y$. Par conséquent $w \cdot x = x$ se réécrit $w \cdot (g^{-1}y) = g^{-1}y$ ou encore $(gwg^{-1}) \cdot y = y$; autrement dit gwg^{-1} appartient à G_y et $gG_xg^{-1} \subset G_y$. Un raisonnement analogue conduit à $G_y \subset gG_xg^{-1}$. Il s'en suit que $G_y = gG_xg^{-1}$.

◇ D'après ce qui précède $G_y = gG_xg^{-1}$ donc $|G_y| = |G_x|$ et

$$\sum_{y \in \mathcal{O}_x} |G_y| = \sum_{y \in \mathcal{O}_x} |G_x| = |G_x| \sum_{y \in \mathcal{O}_x} 1 = |G_x| |\mathcal{O}_x|.$$

Or l'application

$$G/G_x \rightarrow \mathcal{O}_x, \quad \bar{g} \mapsto g \cdot x$$

est bien définie et est une bijection ; par suite $|G/G_x| = |\mathcal{O}_x|$, i.e. $|G| = |\mathcal{O}_x| |G_x|$. Ainsi $\sum_{y \in \mathcal{O}_x} |G_y| = |G|$.

◇ Nous avons

$$\sum_{x \in X} |G_x| = \sum_{\mathcal{O}_x \subset \Omega} \sum_{y \in \mathcal{O}_x} |G_y|.$$

D'après b) $\sum_{y \in \mathcal{O}_x} |G_y| = |G|$ d'où

$$\sum_{x \in X} |G_x| = \sum_{\mathcal{O}_x \subset \Omega} |G| = |G| \sum_{\mathcal{O}_x \subset \Omega} 1 = |G| |\Omega|.$$

Finalement

$$|\Omega| = \frac{1}{|G|} \sum_{x \in X} |G_x|.$$

◇ D'une part

$$\begin{aligned} E &= \{(g, x) \in G \times X \mid g \cdot x = x\} \\ &= \{(g, x) \in G \times X \mid x \in \text{Fix}(g)\} \\ &= \left(\{g_1\} \times \text{Fix}(g_1) \right) \cup \left(\{g_2\} \times \text{Fix}(g_2) \right) \cup \dots \cup \left(\{g_p\} \times \text{Fix}(g_p) \right) \end{aligned}$$

d'où $|E| = \sum_{g \in G} |\text{Fix}(g)|$.

D'autre part

$$\begin{aligned} E &= \{(g, x) \in G \times X \mid g \cdot x = x\} \\ &= \{(g, x) \in G \times X \mid g \in G_x\} \\ &= \left(G_{x_1} \times \{x_1\} \right) \cup \left(G_{x_2} \times \{x_2\} \right) \cup \dots \cup \left(G_{x_q} \times \{x_q\} \right) \end{aligned}$$

d'où $|E| = \sum_{x \in X} |G_x|$. Par conséquent $\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |G_x|$. Mais d'après ce qui précède $|\Omega| |G| = \sum_{x \in X} |G_x|$. donc

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Cela signifie que le nombre moyen de points fixes d'un élément de G est exactement $|\Omega|$, *i.e.* le nombre d'orbites de l'action.

En particulier si l'action est transitive ce nombre vaut 1.

Par exemple si $G = \mathcal{S}_n$ agit (via l'action évidente) sur $X = \{1, 2, \dots, n\}$, alors le nombre moyen de points fixes d'une permutation est exactement 1.

2. On représente un collier par un cercle du plan euclidien orienté \mathbb{R}^2 (de centre O et de rayon 1) muni de neuf points A_1, A_2, \dots, A_9 disposés à intervalles réguliers.

Deux colliers sont dits équivalents si et seulement si on peut obtenir l'un à partir de l'autre en effectuant une rotation plane du collier ou en le retournant (comme une crêpe) dans l'espace de dimension 3.

Autrement dit l'ensemble X de tous les colliers possibles à 9 perles dont 4 bleues, 3 blanches et 2 rouges, est muni d'une action du groupe diédral $G = D_{18}$ des isométries d'un polygone régulier à neuf côtés. Ce groupe G est donc un sous-groupe de $SO(2, \mathbb{R})$, il est d'ordre 18 et ses éléments sont les suivants

$$G = \{\text{id}, r, r^2, r^3, r^4, r^5, r^6, r^7, r^8, s, r \circ s, r^2 \circ s, r^3 \circ s, r^4 \circ s, r^5 \circ s, r^6 \circ s, r^7 \circ s, r^8 \circ s\}$$

où r est la rotation de centre O et d'angle $\frac{2\pi}{9}$ et s est la symétrie orthogonale d'axe $\Delta = (OA_1)$. En particulier G contient neuf rotations et neuf symétries orthogonales.

Le nombre de colliers est exactement le nombre d'orbites dans l'action de G sur X , *i.e.* $|\Omega|$.

On calcule ce nombre à l'aide de la formule obtenue en 1.

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

Déterminons $\text{Fix}(g)$ pour tout g dans G . Soit $g \in G$.

- ◇ Si $g = \text{id}$, alors $\text{Fix}(g) = X$.
- ◇ Si $g = r, r^2, r^4, r^5, r^7, r^8$, alors le sous-groupe de G engendré par g est constitué des 9 rotations (r^k engendre ce groupe si et seulement si k est premier avec 9). Donc un collier fixe par g est fixe par r ce qui implique que toutes les perles sont de la même couleur. Ceci n'est pas possible. Par suite $\text{Fix}(g) = \emptyset$.
- ◇ Si $g = r^3, r^6$, alors dans un collier fixe par g le nombre de perles d'une couleur donnée doit être un multiple de 3, ce qui n'est pas le cas dans l'ensemble X , donc $\text{Fix}(g) = \emptyset$.
- ◇ Si g est une symétrie, nous pouvons supposer que $g = s$, les autres cas étant identiques. Puisque l'axe Δ de g ne contient que la perle A_1 , dans un collier fixe par g , les perles $A_i, i \neq 1$, vont par paire de même couleur. Cela assure que la perle A_1 est nécessairement blanche. Se donner un collier fixe par g revient alors à se donner les couleurs des perles A_2, A_3, A_4, A_5 de sorte que 2 soient bleues, 1 blanche et 1 rouge. Il est clair que le nombre de tels colliers vaut

$$|\text{Fix}(g)| = \binom{4}{2} \binom{2}{1} = 6 \times 2 = 12.$$

Enfin le cardinal de X est

$$|X| = \binom{9}{4} \binom{5}{3} = 126 \times 10 = 1260.$$

On en déduit que

$$|\Omega| = \frac{1}{18} (1260 + 9 \times 12) = 76.$$

Il y a donc 76 colliers distincts (à équivalence près) satisfaisant les contraintes de l'énoncé.