Révisions

Table des matières

1 Actions de groupes, sous-groupes distingués

Exercice 1

Soit G un groupe fini. Soient p le plus petit facteur premier de $|\mathrm{G}|$ et H un sous-groupe d'ordre p et distingué dans G. En faisant opérer G sur H par conjugaison montrer que H est contenu dans le centre de G.

Solution 1

Puisque H est distingué dans G l'application

$$\mathrm{G}\times\mathrm{H}\to\mathrm{H}, \qquad (g,h)\mapsto ghg^{-1}$$

définit une action du groupe G sur l'ensemble H. Puisque $|\mathrm{H}|\geqslant 2$ il existe $h\in\mathrm{H}\smallsetminus\{e\}$. Soit $\mathcal{O}_h$ l'orbite de h. D'une part $|\mathcal{O}_h|$ divise $|\mathrm{G}|$ et d'autre part H étant réunion des orbites nous avons $|\mathcal{O}_h|\leqslant|\mathrm{H}|=p$. Si $|\mathcal{O}_h|>1$, alors p étant le plus petit diviseur de $|\mathrm{G}|$ distinct de 1, nous avons $|\mathcal{O}_h|\geqslant p$ et par suite $|\mathcal{O}_h|=|\mathrm{H}|$. Il en résulte que $\mathcal{O}_h=\mathrm{H}$. En particulier e appartient à $\mathcal{O}_h$ et donc $h=e$: contradiction. Ainsi toutes les orbites sont des singletons et donc si (g,h) appartient à $\mathrm{G}\times\mathrm{H}\to\mathrm{H}$ alors $ghg^{-1}=h$, *i.e.* $gh=hg$ et $\mathrm{H}\subset Z(\mathrm{G})$.

Exercice 2

Soient $\Bbbk$ un corps et $\mathrm{G}\subset\mathrm{GL}(2,\Bbbk)$ 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 2

Le groupe G est

$$\mathrm{G}=\left\{\left(\begin{array}{cc}a_{11}&a_{12}\\0&a_{22}\end{array}\right)\,\middle|\,a_{11},\,a_{22}\in\Bbbk^*,\,a_{12}\in\Bbbk\right\}$$

La loi de composition sur G est :

$$\left(\begin{array}{cc}a&b\\0&c\end{array}\right)\left(\begin{array}{cc}a'&b'\\0&c'\end{array}\right)=\left(\begin{array}{cc}aa'&ab'+bc'\\0&cc'\end{array}\right) \qquad (1)$$

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

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

Posons

$$\varphi\colon \mathrm{G} \to \mathbb{k}^*, \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

La relation (1) assure que φ est un morphisme, et on constate que $\mathrm{K} = \ker \varphi$; en particulier K est distingué dans G. De plus φ est surjectif, car étant donné $a \in \mathbb{k}^*$ la matrice $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ est un antécédent de a par φ. Le théorème d'isomorphisme permet de conclure que le quotient ${}^{\mathrm{G}}\!/\!_{\mathrm{K}}$ 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 $A \in \mathrm{K}$ et $B \in \mathrm{G}$ on a $BAB^{-1} \in \mathrm{K}$) ; 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 $\mathrm{G} = \mathrm{K} \rtimes \mathrm{H}$. Posons

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

On voit que $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et $\mathrm{KH} = \mathrm{G}$ (à nouveau par (1)) dont H convient.
Remarquons que H n'est pas uniquement déterminé ; par exemple

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

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

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

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

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

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

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

Posons

$$\varphi\colon \mathrm{G} \to \mathbb{k}^*, \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \frac{a}{c}$$

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

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

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

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

Posons

$$\varphi \colon \mathrm{G} \to \Bbbk^* \times \Bbbk^*, \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

De nouveau la relation (1) assure que φ est un morphisme surjectif, donc $\mathrm{K} = \ker \varphi$ est distingué ; d'après le théorème d'isomorphisme le quotient G/K est isomorphe à $\Bbbk^* \times \Bbbk^*$.
Notons que $\mathrm{G} = \mathrm{K} \rtimes \mathrm{H}$ par exemple pour le choix suivant de sous-groupe H :

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

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 $\mathrm{K} \subset \mathrm{G}$ est un sous-groupe distingué, il existe un sous-groupe $\mathrm{H} \subset \mathrm{G}$ tel que . C'est faux ; considérer par exemple $\mathrm{G} = \mathbb{Z}/4\mathbb{Z} = \{\overline{0},\, \overline{1},\, \overline{2},\, \overline{3}\}$ et $\mathrm{K} = \{\overline{0},\, \overline{2}\}$ et se convaincre qu'un tel H n'existe pas dans ce cas...

Exercice 3 [Action par conjugaison]

Soit G un groupe fini.

1. On définit l'application suivante

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, x) \mapsto g \cdot x = gxg^{-1}$$

   Montrer qu'il s'agit d'une action du groupe G sur lui-même.
2. Lorsqu'un groupe G agit sur un ensemble X on appelle *points fixes* les éléments de X qui sont invariants sous l'action de G. Ils forment l'ensemble $\{x \in X \mid g \cdot x = x \quad \forall\, g \in \mathrm{G}\}$.
   Décrire les points fixes de l'action par conjugaison d'un groupe G sur lui-même.
3. Dans le cas $\mathrm{G} = \mathcal{S}_4$ décrire les orbites et les stabilisateurs.
4. Combien y a-t-il d'orbites pour l'action par conjugaison de $\mathcal{S}_{10}$ sur lui-même ?

Solution 3 Soit G un groupe fini.

1. On définit l'application suivante

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, x) \mapsto g \cdot x = gxg^{-1}$$

   Montrons qu'il s'agit d'une action du groupe G sur lui-même.
   Le neutre agit trivialement :

$$e \cdot x = exe^{-1} = exe = x.$$

   Pour tous g_1, g_2, x dans G nous avons

$$g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2) \cdot x.$$

2. Lorsqu'un groupe G agit sur un ensemble X on appelle *points fixes* les éléments de X qui sont invariants sous l'action de G. Ils forment l'ensemble $\{x \in X \mid g \cdot x = x \quad \forall\, g \in \mathrm{G}\}$.
   Un élément $x \in \mathrm{G}$ est un point fixe si et seulement si pour tout $g \in \mathrm{G}$ $g \cdot x = x$. Or $g \cdot x = x$ se réécrit $gxg^{-1} = x$ ou encore $gx = xg$. Les points fixes pour l'action par conjugaison d'un groupe sur lui-même sont donc les éléments qui commutent avec tous les autres, c'est-à-dire les éléments du centre de G.
3. Supposons $\mathrm{G} = \mathcal{S}_4$.
   Rappelons que $\mathcal{S}_4$ compte $24 = 4!$ éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Les différentes orbites sont
- ◇ $\mathcal{O}_{\mathrm{id}} = \{g \cdot \mathrm{id} \,|\, g \in \mathrm{G}\} = \{g\mathrm{id}g^{-1} \,|\, g \in \mathrm{G}\} = \{\mathrm{id} \,|\, g \in \mathrm{G}\} = \{\mathrm{id}\}$;
- ◇ $\mathcal{O}_{(1\ 2)} = \{g \cdot (1\ 2) \,|\, g \in \mathrm{G}\} = \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\}$;
- ◇ $\mathcal{O}_{(1\ 2)(3\ 4)} = \{g \cdot (1\ 2)(3\ 4) \,|\, g \in \mathrm{G}\} = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$;
- ◇ $\mathcal{O}_{(1\ 2\ 3)} = \{g \cdot (1\ 2\ 3) \,|\, g \in \mathrm{G}\} = \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2\ 4),\ (1\ 4\ 2)\}$;
- ◇ $\mathcal{O}_{(1\ 2\ 3\ 4)} = \{g \cdot (1\ 2\ 3\ 4) \,|\, g \in \mathrm{G}\} = \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}$.

Les stabilisateurs correspondants sont
- ◇ $\mathrm{G}_{\mathrm{id}} = \{g \in \mathrm{G} \,|\, g \cdot \mathrm{id} = \mathrm{id}\} = \{g \in \mathrm{G} \,|\, g\mathrm{id}g^{-1} = \mathrm{id}\} = \mathrm{G}$
- ◇ $\mathrm{G}_{(1\ 2)} = \{g \in \mathrm{G} \,|\, g \cdot (1\ 2) = (1\ 2)\} = \{g \in \mathrm{G} \,|\, g(1\ 2)g^{-1} = (1\ 2)\} = \{g \in \mathrm{G} \,|\, g(1\ 2) = (1\ 2)g\} = \{\mathrm{id},\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}$
- ◇ $\mathrm{G}_{(1\ 2)(3\ 4)} = \{g \in \mathrm{G} \,|\, g \cdot (1\ 2)(3\ 4) = (1\ 2)(3\ 4)\} = \{g \in \mathrm{G} \,|\, g(1\ 2)(3\ 4)g^{-1} = (1\ 2)(3\ 4)\} = \{g \in \mathrm{G} \,|\, g(1\ 2)(3\ 4) = (1\ 2)(3\ 4)g\} = \{\mathrm{id},\ (12),\ (3\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 3\ 2\ 4),\ (1\ 4\ 2\ 3)\}$
- ◇ $\mathrm{G}_{(1\ 2\ 3)} = \{g \in \mathrm{G} \,|\, g \cdot (1\ 2\ 3) = (1\ 2\ 3)\} = \{g \in \mathrm{G} \,|\, g(1\ 2\ 3)g^{-1} = (1\ 2\ 3)\} = \{g \in \mathrm{G} \,|\, g(1\ 2\ 3) = (1\ 2\ 3)g\} = \{\mathrm{id},\ (1\ 2\ 3),\ (1\ 3\ 2)\}$
- ◇ $\mathrm{G}_{(1\ 2\ 3\ 4)} = \{g \in \mathrm{G} \,|\, g \cdot (1\ 2\ 3\ 4) = (1\ 2\ 3\ 4)\} = \{g \in \mathrm{G} \,|\, g(1\ 2\ 3\ 4)g^{-1} = (1\ 2\ 3\ 4)\} = \{g \in \mathrm{G} \,|\, g(1\ 2\ 3\ 4) = (1\ 2\ 3\ 4)g\} = \{\mathrm{id},\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2)\}$

Notons que dans chaque cas nous avons $|\mathrm{G}| = |\mathrm{G}_x| \times |\mathcal{O}_x|$.

4. Déterminons le nombre d'orbites pour l'action par conjugaison de $\mathcal{S}_{10}$ sur lui-même.
   Toute permutation de $\mathcal{S}_n$ s'écrit de manière unique comme produit de cycles à support disjoint. Ici on compte aussi les cycles de longueur 1 et on note la liste des tailles des cycles. Par exemple à la permutation $(2\ 7)(1\ 3\ 4)(8\ 9\ 10) = (5)(6)(2\ 7)(1\ 3\ 4)(8\ 9\ 10)$ on associe le 5-uplet $(1, 1, 2, 3, 3)$. On ordonne toujours ce k-uplet par ordre croissant (les cycles à support disjoint commutent). La somme des éléments de ce k-uplet vaut n (ici 10). Un tel k-uplet est appelé une partition du nombre n. Il y a une bijection entre les partitions de 10 et les orbites de $\mathcal{S}_{10}$ sous l'action de lui-même par conjugaison. Et on a 42 partitions du nombre 10 donc 42 orbites pour l'action par conjugaison de $\mathcal{S}_{10}$ sur lui-même.

Exercice 4

Soit G un sous-groupe de $\mathcal{S}_4$ opérant sur $\{1,\ 2,\ 3,\ 4\}$ par l'action naturelle de $\mathcal{S}_4$. Pour $1 \leqslant i \leqslant 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i. Déterminer $\mathcal{O}_i$ et S_i pour les cas suivants :
- ◇ G est le groupe engendré par le 3-cycle (1 2 3).
- ◇ G est le groupe engendré par le 4-cycle (1 2 3 4).
- ◇ G est le groupe engendré par les double transpositions.

◇ $\mathrm{G} = \mathcal{A}_4$.

Solution 4

◇ Par symétrie il suffit d'étudier les cas $i = 1$ et $i = 4$.
Pour $i = 4$ c'est plus facile car aucun élément de G ne modifie 4. Ainsi $\mathcal{O}_4 = \{4\}$ et $S_4 = \mathrm{G}$.
Ensuite si $s = (1\ 2\ 3)$, alors $s(1) = 2$ et $s \circ s(1) = 3$ d'où

$$\mathcal{O}_1 = \{g \cdot 1 \,|\, g \in \mathrm{G}\} = \{g(1) \,|\, g \in \mathrm{G}\} = \{\mathrm{id}(1),\, s(1),\, s \circ s(1)\} = \{1,\, 2,\, 3\}.$$

Puisque $\mathrm{G} = \{\mathrm{id},\, s,\, s^2\}$ nous obtenons que

$$S_1 = \{g \in \mathrm{G} \,|\, g \cdot 1 = 1\} = \{g \in \mathrm{G} \,|\, g(1) = 1\} = \{\mathrm{id}\}$$

◇ Par symétrie il suffit d'étudier le cas $i = 1$. Par un raisonnement analogue au précédent nous constatons que

$$S_1 = \{g \in \mathrm{G} \,|\, g \cdot 1 = 1\} = \{g \in \mathrm{G} \,|\, g(1) = 1\} = \{\mathrm{id}\}$$

et

$$\mathcal{O}_1 = \{g \cdot 1 \,|\, g \in \mathrm{G}\} = \{g(1) \,|\, g \in \mathrm{G}\} = \{1,\, 2,\, 3,\, 4\}.$$

En effet si $s = (1\ 2\ 3\ 4)$, alors $\mathrm{G} = \{\mathrm{id},\, s,\, s^2,\, s^3\}$.

◇ Par symétrie il suffit d'étudier le cas $i = 1$.
Le produit de deux double transpositions est ou bien l'identité, ou bien une double transposition. Une double transposition ne fixe aucun élément de $\{1,\, 2,\, 3,\, 4\}$ et on peut trouver une double transposition qui envoie 1 sur n'importe quel élément de $\{2,\, 3,\, 4\}$. En résumé nous avons

$$\mathcal{O}_1 = \{1,\, 2,\, 3,\, 4\} \qquad\qquad S_1 = \{\mathrm{id}\}.$$

◇ Par symétrie il suffit d'étudier le cas $i = 1$.
Les éléments de $\mathcal{A}_4$ sont l'identité, les double transpositions et les 3-cycles. D'après la question précédente $\mathcal{O}_1 = \{1,\, 2,\, 3,\, 4\}$ puisque l'orbite de 1 par $\mathcal{A}_4$ contient au moins l'orbite de 1 par les double transpositions. Déterminons maintenant le stabilisateur de 1. Une double transposition ne peut pas être dans le stabilisateur de 1. D'après la première question les 3-cycles qui stabilisent 1 sont ceux qui n'ont pas 1 dans leur support, on a donc $S_1 = \big\{\mathrm{id},\, (2\ 3\ 4),\, (2\ 4\ 3)\big\}$.

Exercice 5

Soit $n \geqslant 3$ un entier. Considérons les matrices suivantes de $\mathrm{GL}(2, \mathbb{R})$

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad\qquad \tau = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

Notons G le sous-groupe de $\mathrm{GL}(2, \mathbb{R})$ engendré par σ et τ ; désignons par H le sous-groupe de G engendré par σ et K le sous-groupe de G engendré par τ :

$$\mathrm{G} = \langle \sigma,\, \tau \rangle, \qquad\qquad \mathrm{H} = \langle \sigma \rangle, \qquad\qquad \mathrm{K} = \langle \tau \rangle.$$

Posons $\mathrm{K}' = \big\{g \in \mathrm{G} \,|\, \det g = 1\big\}$ et définissons les vecteurs X_0 et Y_0 de $\mathbb{R}^2$ par

$$X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad\qquad Y_0 = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

1. Donner l'ordre de σ.
2. Donner une interprétation géométrique pour τ et donner son ordre.
3. Si G est d'ordre fini, que peut-on dire sur son ordre ?
4. Montrer que $\sigma\tau = \tau^{n-1}\sigma$.
5. Donner tous les éléments de G, H et K.
6. Combien y a-t-il de classes à gauche de G modulo H ?
7. Décrire ${}^{\mathrm{G}}\!\diagup_{\mathrm{H}}$.
8. A-t-on $\mathrm{H} \triangleleft \mathrm{G}$? Si oui décrire le groupe quotient ${}^{\mathrm{G}}\!\diagup_{\mathrm{H}}$.

9. A-t-on $\mathrm{K} \triangleleft \mathrm{G}$? Si oui décrire le groupe quotient ${}^{\mathrm{G}}\!/_{\mathrm{K}}$.
10. Le sous-ensemble K' de G est-il un sous-groupe de G ? Si oui, a-t-on $\mathrm{K}' \triangleleft \mathrm{G}$?
11. Comparer K et K'.
12. Existe-t-il un sous-groupe de G isomorphe à ${}^{\mathrm{G}}\!/_{\mathrm{K}}$?
13. Calculer $D(\mathrm{G})$. À quel groupe est isomorphe ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$?
14. Montrer que la multiplication des matrices définit une action

$$\mathrm{G} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, X) \mapsto M \cdot X = MX$$

15. L'action est-elle transitive ?
16. L'action est-elle fidèle ?
17. Quels sont les points fixes de l'action ?
18. Quel est le stabilisateur G_{X_0} du vecteur X_0 ?
19. Décrire l'orbite du vecteur X_0.
20. Quel est le stabilisateur G_S du segment $S = [X_0, Y_0]$?

Solution 5

1. Donnons l'ordre de σ.
Nous avons $\sigma \neq \mathrm{id}$ mais $\sigma^2 = \mathrm{id}$ donc σ est d'ordre 2.
2. Donnons une interprétation géométrique pour τ et donnons son ordre.
On voit que τ est la rotation de centre $O = (0, 0)$ et d'angle $\frac{2\pi}{n}$. En particulier τ est d'ordre n. On peut de plus déterminer τ^k :
$$\tau^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}$$
3. Si G est d'ordre fini, alors son ordre est divisible d'une part par 2 et d'autre part par n, donc par $\mathrm{ppcm}(2, n)$.
4. Montrons que $\sigma\tau = \tau^{n-1}\sigma$. Un calcul direct assure que $\sigma\tau\sigma^{-1} = \tau^{-1}$:
$$\sigma\tau\sigma^{-1} = \sigma\tau\sigma = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(-\frac{2\pi}{n}\right) & -\sin\left(-\frac{2\pi}{n}\right) \\ \sin\left(-\frac{2\pi}{n}\right) & \cos\left(-\frac{2\pi}{n}\right) \end{pmatrix} = \tau^{-1}$$
On en déduit que $\sigma\tau\sigma^{-1} = \tau^{n-1}$ puis que $\sigma\tau = \tau^{n-1}\sigma$.
5. Donnons tous les éléments de G, H et K.
Puisque σ est d'ordre 2, nous avons $\mathrm{H} = \{\mathrm{id}, \sigma\}$.
Comme τ est d'ordre n, nous avons $\mathrm{K} = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}\}$.
Nous avons $\mathrm{G} = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}, \sigma, \tau\sigma, \tau^2\sigma, \ldots, \tau^{n-1}\sigma\}$. En effet d'une part un élément de G s'écrit
$$(\sigma)\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}(\sigma)$$
d'autre part $\sigma\tau\sigma^{-1} = \tau^{n-1}$ implique $\sigma\tau^\ell\sigma^{-1} = \tau^{\ell(n-1)}$ et $\sigma\tau^\ell = \tau^{\ell(n-1)}\sigma$. En effet montrons par exemple par récurrence qu'un élément de la forme $(\sigma)\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}(\sigma)$ avec k pair est de la forme τ^ℓ ou $\tau^\ell\sigma$:
   - ◇ commençons par considérer un élément de la forme $\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$ avec k pair. Montrons par récurrence sur k qu'il s'écrit aussi τ^κ pour un certain κ. C'est vrai pour $k = 2$, en effet
   $$\underbrace{\sigma\tau^{i_1}}_{\tau^{i_1(n-1)}\sigma}\sigma\tau^{i_2} = \tau^{i_1(n-1)}\sigma\sigma\tau^{i_2} = \tau^{i_1(n-1)}\tau^{i_2} = \tau^{i_1(n-1)+i_2}$$
   Soit k un entier pair. Supposons que la propriéé soit vraie pour tout $j \leqslant k$ pair et montrons qu'alors c'est vrai pour $k + 2$
   $$\underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa_1}}\underbrace{\sigma\tau^{i_{k+1}}\sigma\tau^{i_{k+2}}}_{\tau^{\kappa_2}} = \tau^{\kappa_1}\tau^{\kappa_2} = \tau^{\kappa_1+\kappa_2}$$
   - ◇ considérons un élément de la forme $\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$ avec k pair, alors
   $$\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k} = \sigma\underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^\kappa} = \sigma\tau^\kappa = \tau^{\kappa(n-1)}\sigma$$

- ◇ finalement considérons un élément de la forme $\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma$ avec k pair ; d'après le premier point il s'écrit $\tau^\kappa\sigma$.

Un raisonnement analogue permet de conclure lorsque k est impair.

6. Déterminons le nombre de classes à gauche de G modulo H.
   L'ensemble des classes à gauche de G modulo H est l'ensemble G/H. Son cardinal est $\left|\mathrm{G}/\mathrm{H}\right| = [\mathrm{G}:\mathrm{H}] = \frac{|\mathrm{G}|}{|\mathrm{H}|}$.
   D'après la question précédente nous avons $|\mathrm{G}| = 2n$, $|\mathrm{H}| = 2$ et donc $\left|\mathrm{G}/\mathrm{H}\right| = \frac{|\mathrm{G}|}{|\mathrm{H}|} = n$.
7. Décrivons G/H.
   La description de G nous permet d'affirmer que
   $$\mathrm{G}/\mathrm{H} = \left\{\overline{\mathrm{id}},\, \overline{\tau},\, \ldots,\, \overline{\tau^{n-1}}\right\}.$$
8. Le sous-groupe H de G n'est pas distingué dans G ; en effet
   $$\tau^{-1}\sigma\tau = \tau^{-1}\tau^{n-1}\sigma = \tau^{n-2}\sigma \notin \mathrm{H}.$$
9. Nous avons $[\mathrm{G}:\mathrm{K}] = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{2n}{2} = 2$. Ainsi K est un sous-groupe d'indice 2 de G ; il est donc distingué dans G.
   Le groupe quotient G/K est d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Nous avons $\mathrm{G}/\mathrm{K} = \left\{\overline{\mathrm{id}},\, \overline{\sigma}\right\}$.
10. L'application $\det\colon \mathrm{G} \to \mathbb{R}^*$ est un morphisme de groupes et K' est son noyau. Ainsi K' est un sous-groupe distingué de G.
11. Comparons K et K'.
    Remarquons que $\det\tau = \cos^2\left(\frac{2\pi}{n}\right) + \sin^2\left(\frac{2\pi}{n}\right) = 1$ donc τ appartient à K'. Ainsi $\mathrm{K} = \langle\tau\rangle \subset \mathrm{K}'$.
    De plus $\det\sigma = -1$, par conséquent $\det(\tau^k\sigma) = -1$ et $\mathrm{K} = \mathrm{K}'$.
12. Les groupes H et G/K sont d'ordre 2, donc sont isomorphes. Il en résulte qu'il existe un sous-groupe de G (le sous-groupe H) isomorphe à G/K.
13. Calculons $D(\mathrm{G})$.
    Le groupe G n'est pas abélien : $\sigma\tau = \tau^{n-1}\sigma \neq \tau\sigma$ car $n \neq 2$. Par conséquent $D(\mathrm{G}) \neq \{\mathrm{id}\}$.
    De plus G/K est abélien ; $\mathrm{G}/D(\mathrm{G})$ étant le plus grand quotient abélien $D(\mathrm{G}) \subset \mathrm{K}$.
    Calculons $[\sigma,\tau]$:
    $$[\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \tau^{-1}\tau^{-1} = \tau^{-2}$$
    ainsi τ^{-2} appartient à $D(\mathrm{G})$ et τ^2 appartient à $D(\mathrm{G})$. Finalement $\langle\tau^2\rangle \subset D(\mathrm{G})$.
    Si n est impair, alors n est premier avec 2 et l'ordre de τ^2 est $\frac{n}{\mathrm{pgcd}(2,n)} = n$ donc $\langle\tau^2\rangle = \langle\tau\rangle$ et $\mathrm{K} = \langle\tau\rangle \subset D(\mathrm{G})$. Finalement $D(\mathrm{G}) = \mathrm{K} = \langle\tau\rangle = \langle\tau^2\rangle$. Dans ce cas nous avons $\mathrm{G}/D(\mathrm{G}) \simeq \mathbb{Z}/2\mathbb{Z}$.
    Si $n = 2m$ est pair, montrons que
    $$D(\mathrm{G}) = \langle\tau^2\rangle = \{\mathrm{id},\, \tau^2,\, \tau^4,\, \ldots,\, \tau^{n-2}\} = \{\mathrm{id},\, \tau^2,\, \tau^4,\, \ldots,\, \tau^{2(m-1)}\}.$$
    Nous avons vu que $\langle\tau^2\rangle \subset D(\mathrm{G})$. Montrons que $\langle\tau^2\rangle \lhd \mathrm{G}$. Soit $y = \tau^{2a} \in \langle\tau^2\rangle$ et $x \in \mathrm{G}$; nous avons $x = \tau^k$ ou $x = \tau^k\sigma$. Dans le premier cas nous obtenons
    $$xyx^{-1} = \tau^k\tau^{2a}\tau^{-k} = \tau k + 2a - k = \tau 2a = y \in \langle\tau^2\rangle.$$
    Dans le second cas nous obtenons
    $$xyx^{-1} = \tau^k\sigma\tau^{2a}(\tau^k\sigma)^{-1} = \tau^k\underbrace{\sigma\tau^{2a}}_{\tau^{2a(n-1)}\sigma}\sigma^{-1}\tau^{-k} = \tau^k\tau^{2a(n-1)}\sigma\sigma^{-1}\tau^{-k} = \tau^k\tau^{2a(n-1)}\tau^{-k} = \tau^{k+2a(n-1)-k} = \tau^{2a(n-1)} \in \langle\tau^2\rangle$$
    Ainsi $\langle\tau^2\rangle \lhd \mathrm{G}$.
    De plus τ^2 est d'ordre $\frac{n}{\mathrm{pgcd}(2,n)} = \frac{n}{2} = m$ donc $|\langle\tau^2\rangle| = m$. Ainsi le quotient $\mathrm{G}/\langle\tau^2\rangle$ est d'ordre $\frac{2n}{m} = 4$.
    Mais un groupe d'ordre 4 a ou bien un élément d'ordre 4 et est alors isomorphe à $\mathbb{Z}/4\mathbb{Z}$, ou bien n'a que des éléments d'ordre 2 et est isomorphe à un groupe de Klein. En particulier un groupe d'ordre 4 est abélien donc $\mathrm{G}/\langle\tau^2\rangle$ est abélien et $D(\mathrm{G}) \subset \langle\tau^2\rangle$. On obtient $D(\mathrm{G}) = \langle\tau^2\rangle$.

Il reste à déterminer ${}^{\mathrm{G}}\!/_{D(\mathrm{G})} = {}^{\mathrm{G}}\!/_{\langle\tau^2\rangle}$ qui est d'ordre 4. On peut décrire ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$:

$$ {}^{\mathrm{G}}\!/_{D(\mathrm{G})} = \{\overline{\mathrm{id}},\, \overline{\sigma},\, \overline{\tau},\, \overline{\tau\sigma}\}. $$

Mais $\overline{\tau}^2 = \overline{\tau^2} = \mathrm{id}$ (car on quotiente par τ^2), $\overline{\sigma}^2 = \overline{\sigma^2} = \overline{\mathrm{id}}$ (car σ est d'ordre 2) et $\overline{\tau\sigma}^2 = \overline{\tau}^2\overline{\sigma}^2 = \overline{\mathrm{id}}$ (car le groupe est abélien). Ainsi tous les éléments de ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ sont d'ordre 2 et ${}^{\mathrm{G}}\!/_{D(\mathrm{G})} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ est un groupe de Klein.

14. Montrons que la multiplication des matrices définit une action

$$ \mathrm{G} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, X) \mapsto M \cdot X = MX $$

D'une part $\mathrm{id} \cdot X = X$; d'autre part pour M, M' dans G nous avons

$$ (MM') \cdot X = MM'X = M \cdot (M' \cdot X) $$

par l'associativité du produit matriciel. Nous avons donc bien une action de G sur $\mathbb{R}^2$.

15. L'action n'est pas transitive. L'orbite d'un vecteur $X \in \mathbb{R}^2$ est l'ensemble

$$ \mathcal{O}_X = \{g \cdot X \,|\, g \in \mathrm{G}\} = \{gX \,|\, g \in \mathrm{G}\}; $$

en particulier $\mathcal{O}_X$ compte au plus $2n$ éléments alors que $\mathbb{R}^2$ est infini. Il s'en suit qu'aucune orbite ne peut être égale à $\mathbb{R}^2$ tout entier.

16. L'action est fidèle : soit $g \in \mathrm{G}$ tel que $g \cdot X = X$ pour tout $X \in \mathbb{R}^2$, *i.e.* tel que $gX = X$ pour tout $X \in \mathbb{R}^2$, alors $g = \mathrm{Id}$.

17. Déterminons les points fixes de l'action, *i.e.* déterminons

$$ \{X \in \mathbb{R}^2 \,|\, g \cdot X = X \quad \forall g \in \mathrm{G}\}. $$

Autrement dit nous cherchons les $X \in \mathbb{R}^2$ tels que $g \cdot X = X$ pour tout $g \in \mathrm{G}$. Remarquons que $X = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ est un point fixe. Montrons que c'est le seul. En effet si $X = \begin{pmatrix} x \\ y \end{pmatrix}$ est un point fixe, alors en particulier $\sigma \cdot X = X$, c'est-à-dire $(x, -y) = (x, y)$ d'où $y = 0$. De plus nous avons $\tau \cdot X = X$ soit $\tau \cdot \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$ qui se réécrit $\begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) x \\ \sin\left(\frac{2\pi}{n}\right) x \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$. En particulier $\sin\left(\frac{2\pi}{n}\right) x = 0$; mais pour $n \geqslant 3$, nous avons $\sin\left(\frac{2\pi}{n}\right) \neq 0$ donc $x = 0$ et $X = (0, 0)$. Finalement $(0, 0)$ est l'unique point fixe de l'action.

18. Déterminons le stabilisateur

$$ \mathrm{G}_{X_0} = \{g \in \mathrm{G} \,|\, g \cdot X_0 = X_0\} = \{g \in \mathrm{G} \,|\, gX_0 = X_0\} $$

du vecteur $X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Remarquons que $\sigma \cdot X_0 = \sigma X_0 = X_0$, *i.e.* σ appartient à G_{X_0}.

Par ailleurs $\tau^k \cdot X_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$; ainsi $\tau^k \cdot X_0 = X_0$ si et seulement si $\cos\left(\frac{2k\pi}{n}\right) = 1$ et $\sin\left(\frac{2k\pi}{n}\right) = 0$, c'est-à-dire si et seulement si $\frac{2k\pi}{n} \equiv 0 \pmod{2\pi}$, *i.e.* si et seulement si k est un multiple de n donc si et seulement si $\tau^k = \mathrm{id}$.

De même nous avons $\tau^k\sigma \cdot X_0 = X_0$ si et seulement si $\tau^k \cdot X_0 = X_0$ si et seulement si $\tau^k = \mathrm{id}$ si et seulement si $\tau^k\sigma = \sigma$.

Il en résulte que $\mathrm{G}_{X_0} = \{\mathrm{id},\, \sigma\} = \mathrm{H}$.

19. Décrivons l'orbite du vecteur X_0.

Puisque $\mathcal{O}_{X_0}$ et ${}^{\mathrm{G}}\!/_{\mathrm{G}_{X_0}}$ sont en bijection nous avons

$$ |\mathcal{O}_{X_0}| = \left| {}^{\mathrm{G}}\!/_{\mathrm{G}_{X_0}} \right|. $$

Or

$$\left|{}^{\mathrm{G}}\!/\!_{\mathrm{G}_{X_0}}\right| = [\mathrm{G} : \mathrm{G}_{X_0}] = [\mathrm{G} : \mathrm{H}] = \frac{|\mathrm{G}|}{|\mathrm{H}|} = \frac{2n}{2} = n.$$

Ainsi l'orbite du vecteur X_0 compte n éléments.

Les éléments $\tau^k \cdot X_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$, $0 \leqslant k \leqslant n-1$, sont 2 à 2 distincts. Ils forment donc l'orbite de X_0.

20. Quel est le stabilisateur G_S du segment $S = [X_0, Y_0]$?

Comme $Y_0 = -X_0$ nous voyons que

$$\sigma \cdot Y_0 = \sigma \cdot (-X_0) = \sigma(-X_0) = -\sigma(X_0) = -X_0 = Y_0$$

donc $\sigma[X_0, Y_0] = [X_0, Y_0]$ et σ appartient à G_S.

Si g appartient à G_S, alors comme g est linéaire, g doit envoyer X_0 sur un élément de la droite $\langle X_0 \rangle = (X_0, Y_0)$. Cherchons de tels $g \in \mathrm{G}$. On a ou bien $g = \tau^k$, ou bien $g = \tau^k \sigma$ avec dans les deux cas $0 \leqslant k \leqslant n-1$. Dans les deux éventualités

$$g \cdot X_0 = \tau^k X_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$$

Mais $\langle X_0 \rangle = \{(x, y) \in \mathbb{R}^2 \,|\, y = 0\}$ donc on veut que $\sin\left(\frac{2k\pi}{n}\right) \equiv 0 \pmod{\pi}$ c'est-à-dire $\frac{2k\pi}{n} \equiv 0 \pmod{\pi}$.

Si n est impair, alors la seule possibilité est $k = 0$ et $\mathrm{G}_S = \{\mathrm{id}, \sigma\} = \mathrm{H}$.

Si $n = 2m$ est pair, alors nous avons deux possibilités : $k = 0$ et $k = m$. Pour $k = m$ nous avons

$$\tau^m = \begin{pmatrix} \cos\left(\frac{2m\pi}{n}\right) & -\sin\left(\frac{2m\pi}{n}\right) \\ \sin\left(\frac{2m\pi}{n}\right) & \cos\left(\frac{2m\pi}{n}\right) \end{pmatrix}$$

Ainsi $\tau^m \cdot X_0 = Y_0$ et $\tau^m \cdot Y_0 = X_0$. Par suite $\tau^m \cdot S = S$. Finalement $\mathrm{G}_S = \{\mathrm{id}, \sigma, \tau^m, \tau^m\sigma\}$.

Exercice 6

Soit E un espace vectoriel de dimension finie n.

1. Montrer que le groupe $\mathrm{GL}(E)$ agit naturellement sur l'ensemble X des sous-espaces vectoriels de E.
2. Déterminer l'orbite de $F \in X$. Combien existe-t-il d'orbites ?
3. Déterminer le stabilisateur de $F \in X$.

Solution 6

1. Le groupe $\mathrm{GL}(E)$ est un sous-groupe du groupe $\mathcal{S}_E$ des bijections de E. Il agit à gauche sur E et donc sur $\mathcal{P}(E)$
$$\forall\, g \in \mathrm{G} \quad \forall\, X \in \mathcal{P}(E) \quad g \cdot X = \big\{g \cdot x \,|\, x \in X\big\}.$$
Soient $g \in \mathrm{GL}(E)$ et $F \in X$. Alors $g(F)$ est un sous-espace vectoriel de E. Donc X est une partie stable $\mathcal{P}(E)$ et $(g, F) \mapsto g(F)$ est une action de $\mathrm{GL}(E)$ sur X.
2. Soit $F \in X$ de dimension k. Pour tout $g \in \mathrm{GL}(E)$ nous avons $\dim g(F) = k$.
Réciproquement soit $F' \in X$ tel que $\dim F' = k$. Choisissons des bases $(e_1, e_2, \ldots, e_k)$ de F et $(e'_1, e'_2, \ldots, e'_k)$ de F'. On peut compléter ces familles libres de E et obtenir des bases $(e_1, e_2, \ldots, e_k, e_{k+1}, e_{k+2}, \ldots, e_n)$ et $(e'_1, e'_2, \ldots, e'_k, e'_{k+1}, e'_{k+2}, \ldots, e'_n)$ de E. Il existe g une unique forme linéaire de E dans E telle que $g(e_i) = e'_i$ pour $1 \leqslant i \leqslant n$. Puisque le rang de g est n et puisque $g(F) = F'$ nous avons : $g \in \mathrm{GL}(E)$. Ainsi F' appartient l'orbite de F. L'orbite de F est donc l'ensemble des sous-espaces vectoriels de E de même dimension que F. Il existe donc $n+1$ orbites pour cette action.
3. Le stabilisateur de F est l'ensemble des $g \in \mathrm{GL}(E)$ qui laissent F invariant. C'est l'ensemble des $g \in \mathcal{L}(E)$ qui ont, dans la base $(e_1, e_2, \ldots, e_k, e_{k+1}, e_{k+2}, \ldots, e_n)$ précédente, une matrice de la forme $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ avec $A \in \mathrm{M}_{k,k}$, $B \in \mathrm{M}_{k,n-k}$, $C \in \mathrm{M}_{n-k,n-k}$ et avec A et C inversibles car $\det A \det C = \det M \neq 0$.

Exercice 7

Soient $n \geqslant 2$ un entier et $d \geqslant 1$ un diviseur de n. Montrer que le groupe cyclique $\mathbb{Z}/_{n\mathbb{Z}}$ contient un unique sous-groupe d'ordre d. Est-il vrai que $\mathbb{Z}/_{n\mathbb{Z}}$ contient un unique élément d'ordre d ? (Commencer par expliciter les réponses dans le cas particulier $n = 6$, $d = 3$).

Solution 7

- Si $d = 1$, le seul sous-groupe d'ordre 1 de $\mathbb{Z}/_{n\mathbb{Z}}$ est $\{\overline{0}\}$.
- Supposons maintenant $d \geqslant 2$.

  Existence : soit q le quotient de n par d, c'est-à-dire $n = dq$. Alors le sous-groupe engendré par $\overline{q}$ est d'ordre d :
  $$\langle q\rangle = \left\{\overline{0},\, \overline{q},\, \overline{2q},\, \ldots,\, \overline{(d-1)q}\right\}.$$
  Unicité : Soit $\mathrm{H} \subset \mathbb{Z}/_{n\mathbb{Z}}$ un sous-groupe d'ordre $d \geqslant 2$. Soit $k > 0$ le plus petit entier positif tel que $\overline{k} \in \mathrm{H}$. Si $\overline{a}$ appartient à H pour un certain a dans $\mathbb{N}$, montrons que a est un multiple de k. En effet écrivons la division euclidienne de a par q : $a = qk + r$, $0 \leqslant r \leqslant k - 1$, on obtient alors $\overline{a} = \underbrace{\overline{k} + \overline{k} + \ldots + \overline{k}}_{q \text{ fois}} + \overline{r}$ d'où $\overline{r} \in \mathrm{H}$ et donc $r = 0$ par minimalité de k. En particulier puisque $\overline{d} = \overline{0} \in \mathrm{H}$, d est un multiple de k et donc $\mathrm{H} = \langle\overline{k}\rangle$ avec $n = kd$.

  Exemple : dans $\mathbb{Z}/_{6\mathbb{Z}}$, l'unique sous-groupe d'ordre 3 est $\{\overline{0},\, \overline{2},\, \overline{4}\}$, qui contient deux éléments d'ordre 3.

Exercice 8

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 $\mathrm{H} \subset \mathrm{G}$ 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 8

(1) Soit $\mathrm{H} \subset \mathrm{G}$ d'indice 2. Si g appartient à H, alors $g\mathrm{H} = \mathrm{H}g = \mathrm{H}$ (l'hypothèse indice 2 est inutile ici). Si g n'appartient pas à H, alors puisque H est d'indice 2 nous avons
$$\mathrm{G} = \mathrm{H} \cup g\mathrm{H} = \mathrm{H} \cup \mathrm{H}g.$$
On voit que $g\mathrm{H} = \mathrm{H}g = \mathrm{G} \setminus \mathrm{H}$; en particulier $g\mathrm{H} = \mathrm{H}g$, 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 $\mathrm{H} \subset \mathcal{A}_4$ 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 9

Soit $\mathrm{GL}\left(2, \mathbb{Z}/_{2\mathbb{Z}}\right)$ le groupe des matrices inversibles 2×2 à coefficients dans $\mathbb{Z}/_{2\mathbb{Z}}$.

1. Quel est l'ordre de $\mathrm{GL}\left(2, \mathbb{Z}/_{2\mathbb{Z}}\right)$?
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/_{2\mathbb{Z}}$. Définir une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/_{2\mathbb{Z}}\right)$ sur E.

3. En déduire que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

Solution 9

1. Les éléments de $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sont les matrices inversibles dans $\mathbb{Z}/2\mathbb{Z}$. En voici la liste
$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \qquad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \qquad \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \qquad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$$
Il en résulte que G est un groupe d'ordre 6.
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définissons une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.
À chaque base (v, w) de l'espace vectoriel E correspond une action de G sur E : pour $g \in \mathrm{G}$ et $u \in E$ on définit $g * u \in E$ comme l'image du vecteur u par l'application linéaire de matrice g dans la base (v, w).
3. Montrons que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.
Fixons une base de E et considérons l'action correspondante de G sur E. Pour tout $g \in \mathrm{G}$ l'application $\varphi_g \colon u \mapsto g * u$ est définie par les images des vecteurs non nuls de E ; en effet le vecteur nul a toujours pour image lui-même.
Ainsi à tout élément de G est associée une permutation de $E \smallsetminus \{0\}$. Or E compte $2^2 = 4$ éléments. Soient v_1, v_2 et v_3 les trois vecteurs non nuls de E. Alors
$$g \mapsto \big((v_1, v_2, v_3) \mapsto (g * v_1, g * v_2, g * v_3)\big)$$
définit un morphisme de groupes de G dans $\mathcal{S}_3$. Ce morphisme est injectif. Par suite G est isomorphe à un sous-groupe de $\mathcal{S}_3$. Puisque G et $\mathcal{S}_3$ ont même ordre, G est isomorphe à $\mathcal{S}_3$.

Exercice 10

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

1. Montrer que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$.
2. Montrer que l'ordre de $Z(\mathrm{G})$ est > 1.

Indication : faire agir G par conjugaison sur H.

Solution 10

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

1. Montrons que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$. Faisons agir G par conjugaison sur H ; notons que c'est possible car H étant distingué dans G nous avons $\forall\, g \in \mathrm{G}$, $g\mathrm{H}g^{-1} \subset \mathrm{H}$.
L'ordre de H est une puissance de p soit p^β car $|\mathrm{H}|$ divise $|\mathrm{G}|$ 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 $|\mathrm{G}|$, c'est-à-dire de p^n donc une puissance de p.
Raisonnons par l'absurde : supposons que $Z(\mathrm{G}) \cap \mathrm{H} = \{e\}$; alors une seule des orbites est réduite à un seul élément : l'orbite de e. Nous avons alors
$$|\mathrm{H}| = p^\beta = 1 + \text{ somme de puissances de } p$$
contradiction. Par suite $Z(\mathrm{G}) \cap \mathrm{H} \neq \{e\}$.
2. Montrons que l'ordre de $Z(\mathrm{G})$ 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 $|\mathrm{G}| = p^n$.
Raisonnons par l'absurde : supposons que $|Z(\mathrm{G})| = 1$, alors
$$p^n = |\mathrm{G}| = 1 + \text{ somme de puissances de } p$$
contradiction. Il en résulte que $|Z(\mathrm{G})| > 1$.

Exercice 11

Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \smallsetminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.
   Montrer que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).
2. En déduire que si G n'est pas abélien, alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier divisant l'ordre $|\mathrm{G}|$ de G.
3. Soit p un nombre premier. Soit n un entier.
   Quelles sont les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n ?
   Quel est le centre d'un groupe d'ordre p^2 ?
   Quel est le centre d'un groupe non abélien d'ordre p^3 ?
4. Donner un exemple de groupe d'ordre p^3 non abélien.
5. Montrer que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Solution 11

Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \smallsetminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.
   Montrons que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).
   L'inclusion $Z(\mathrm{G}) \subseteq \mathrm{Stab}(g)$ est claire.
   Soit $g \in \mathrm{G} \smallsetminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Remarquons que g appartient à $\mathrm{Stab}(g)$; en effet $ggg^{-1} = g$. Par suite $Z(\mathrm{G})$ est strictement inclus dans $\mathrm{Stab}(g)$.
   Soit $g \in \mathrm{G} \smallsetminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Puisque $g \notin Z(\mathrm{G})$ il existe un élément $h \in \mathrm{G}$ qui ne commute pas avec g donc qui n'appartient pas à $\mathrm{Stab}(g)$. Il en résulte que $\mathrm{Stab}(g)$ est un sous-groupe propre de G.
2. Supposons que G ne soit pas abélien, montrons qu'alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier p divisant l'ordre $|\mathrm{G}|$ de G.
   D'après 1. si G n'est pas abélien et si g appartient à $\mathrm{G} \smallsetminus Z(\mathrm{G})$, alors l'indice de $|\mathrm{G} : Z(\mathrm{G})| > |\mathrm{G} : \mathrm{Stab}(g)|$.
   Mais $|\mathrm{G} : \mathrm{Stab}(g)| \geqslant p$ car $|\mathrm{G} : \mathrm{Stab}(g)|$ divise $|\mathrm{G}|$. Par suite $|\mathrm{G} : Z(\mathrm{G})| > p$.
3. Soit p un nombre premier. Soit n un entier.
   Donnons les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n.
   Si G est abélien, alors $|Z(\mathrm{G})| = p^n$.
   Si G n'est pas abélien, alors $|\mathrm{G} : Z(\mathrm{G})| > p$ donc $|Z(\mathrm{G})| < p^{n-1}$. L'exercice précédent assure que $Z(\mathrm{G})$ n'est pas réduit à l'élément neutre donc $|Z(\mathrm{G})| \geqslant p$. Finalement lorsque G n'est pas abélien, nous avons
   $$|Z(\mathrm{G})| \in \{p,\, p^2,\, \ldots,\; p^{n-2}\}$$
   Si $n = 2$, le groupe G est nécessairement abélien.
   Déterminons le centre d'un groupe d'ordre p^2. Le centre d'un groupe G d'ordre p^2 est donc G tout entier.
   Déterminons le centre d'un groupe non abélien d'ordre p^3. Le centre d'un groupe non abélien d'ordre p^3 est d'ordre p.
4. Donnons un exemple de groupe d'ordre p^3 non abélien.
   Le groupe des quaternions est un groupe d'ordre 2^3 (ici $p = 2$) et n'est pas abélien.
5. Montrons que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
   Soit G un groupe d'ordre p^2. Il est abélien. Nous avons l'alternative suivante :
   — ou bien G contient un élément d'ordre p^2 auquel cas G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$;
   — ou bien tous les éléments de $\mathrm{G} \smallsetminus \{e\}$ sont d'ordre p. Soient x et y deux éléments de $\mathrm{G} \smallsetminus \{e\}$ tels que $y \notin \langle x \rangle$. Alors $\langle x \rangle \cap \langle y \rangle = \{e\}$. En effet le sous-groupe $\langle x \rangle \cap \langle y \rangle$ est d'ordre strictement inférieur à p et d'ordre divisant p donc d'ordre 1. Puisque tout sous-groupe du groupe abélien G est distingué G est isomorphe à $\langle x \rangle \times \langle y \rangle$. Or $\langle x \rangle \simeq \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 12

Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite.

Montrer que les stabilisateurs Stab_g et Stab_h sont des sous-groupes conjugués de G.

En déduire que Stab_g et Stab_h ont même ordre.

Solution 12

Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite. Alors il existe x dans G tel que $h = x \cdot g$.

Soit $y \in \mathrm{Stab}_g$. Alors $y \cdot g = g$. De plus d'une part $y \cdot g = y \cdot (x^{-1}h)$ et d'autre part $g = x^{-1}h$. Par conséquent $y \cdot (x^{-1}h) = x^{-1}h$, soit $xyx^{-1} \cdot h = h$ c'est-à-dire xyx^{-1} appartient à Stab_h. Autrement dit $x\mathrm{Stab}_g x^{-1} \subset \mathrm{Stab}_h$.

Un raisonnement similaire conduit à $\mathrm{Stab}_h \subset x\mathrm{Stab}_g x^{-1}$.

Il s'en suit que $\mathrm{Stab}_h = x\mathrm{Stab}_g x^{-1}$.

L'application $y \mapsto xyx^{-1}$ est un automorphisme de G. C'est donc une bijection et l'image de Stab_g par cet automorphisme est Stab_h. Ces deux ensembles ont donc même cardinal.

Exercice 13

Soit E un ensemble fini. Soit G un groupe fini qui opère sur E. Pour tout g dans G on définit

$$E^g = \big\{ s \in E \,|\, gs = s \big\}.$$

Autrement dit E^g est l'ensemble des points fixes de E sous l'action de g. Pour $s \in E$, on note G_s le fixateur de s pour l'action de G sur E.

1. Construire la table de l'opération

$$\varphi\colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$

définie par

$$\begin{cases} \varphi(g, s) = V \text{ si } gs = s \\ \varphi(g, s) = F \text{ sinon} \end{cases}$$

dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A,\, B,\, C\}$ où ABC est un triangle équilatéral.

2. Démontrer que $\displaystyle\sum_{s \in E} |\mathrm{G}_s| = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g)$.

3. En déduire la formule de Burnside

$$|\mathrm{G}| \times \text{ le nombre d'orbites } = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g).$$

Solution 13

1. Construisons la table de l'opération

$$\varphi\colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$

définie par

$$\begin{cases} \varphi(g, s) = V \text{ si } gs = s \\ \varphi(g, s) = F \text{ sinon} \end{cases}$$

dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A,\, B,\, C\}$ où ABC est un triangle équilatéral.

Désignons par O le centre de gravité du triangle équilatéral ABC et par ρ la rotation de centre O et d'angle $\frac{2\pi}{3}$. Soient s_A, s_B et s_C les symétries d'axes respectifs AO, BO et CO.

Nous obtenons la table suivante

	A	B	C
id	V	V	V
ρ	F	F	F
ρ^2	F	F	F
s_A	V	F	F
s_B	F	V	F
s_C	F	F	V

En effet

(a) $\mathrm{id}(A) = A$, $\mathrm{id}(B) = B$ et $\mathrm{id}(C) = C$;

(b) $\rho(A) \in \{B, C\}$, $\rho(B) \in \{A, C\}$ et $\rho(C) \in \{A, B\}$;

(c) $\rho^2(A) \in \{B, C\}$, $\rho^2(B) \in \{A, C\}$ et $\rho^2(C) \in \{A, B\}$;

(d) $s_A(A) = A$, $s_A(B) = C$ et $s_A(C) = B$;

(e) $s_B(B) = B$, $s_B(A) = C$ et $s_B(C) = A$;

(f) $s_C(C) = C$, $s_C(A) = B$ et $s_C(B) = A$.

2. Montrons que $\displaystyle\sum_{s\in E} |\mathrm{G}_s| = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$.

Posons $p = |\mathrm{G}|$. Notons $g_1, g_2, \ldots, g_p$ les éléments de G. Posons $q = \mathrm{card}(E)$. Notons $s_1, s_2, \ldots, s_q$ les éléments de E.

D'une part

$$\begin{array}{rcl}\varphi^{-1}(V) & = & \big\{(g,s) \in \mathrm{G}\times E \,|\, gs = s\big\}\\ & = & \big\{(g,s) \in \mathrm{G}\times E \,|\, s \in E^g\big\}\\ & = & \{g_1\}\times E^{g_1} \cup \{g_2\}\times E^{g_2} \cup \ldots \cup \{g_p\}\times E^{g_p}\end{array}$$

ce qui conduit à

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$$

D'autre part

$$\begin{array}{rcl}\varphi^{-1}(V) & = & \big\{(g,s) \in \mathrm{G}\times E \,|\, gs = s\big\}\\ & = & \big\{(g,s) \in \mathrm{G}\times E \,|\, g \in \mathrm{G}_s\big\}\\ & = & \mathrm{G}_{s_1}\times\{s_1\} \cup \mathrm{G}_{s_2}\times\{s_2\} \cup \ldots \cup \mathrm{G}_{s_q}\times\{s_q\}\end{array}$$

ce qui entraîne

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{s\in E} |\mathrm{G}_s|.$$

Il en résulte que

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = \sum_{s\in E} |\mathrm{G}_s|.$$

3. Si s est un élément de E, on désigne par $\mathcal{O}_s$ l'orbite de s sous l'action de G. On sait que $|\mathrm{G}_s| = \frac{|\mathrm{G}|}{\mathrm{card}(\mathcal{O}_s)}$. Par suite

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = |\mathrm{G}| \left(\frac{1}{\mathrm{card}(\mathcal{O}_{s_1})} + \frac{1}{\mathrm{card}(\mathcal{O}_{s_2})} + \ldots + \frac{1}{\mathrm{card}(\mathcal{O}_{s_q})}\right)$$

Soient $\sigma_1, \sigma_2, \ldots, \sigma_r$ des éléments de E tels que E est la réunion disjointe des $\mathcal{O}_{\sigma_i}$ pour $1 \leqslant i \leqslant r$. Nous avons

$$\sum_{s\in \mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_s)} = \sum_{s\in \mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} \sum_{s\in \mathcal{O}_{\sigma_i}} 1 = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} \times \mathrm{card}(\mathcal{O}_{\sigma_i}) = 1$$

d'où la formule de Burnside.

Exercice 14

Combien $(\mathbb{F}_2)^n$ admet-il de sous-espaces vectoriels de dimension k ?

Solution 14

Soit $0 \leqslant k \leqslant n$. Le groupe $\mathrm{GL}(n, \mathbb{F}_2)$ agit transitivement sur l'ensemble Λ_k des sous-espaces vectoriels de dimension k de $(\mathbb{F}_2)^n$. L'ordre du groupe $\mathrm{GL}(n, \mathbb{F}_2)$ est

$$\begin{aligned}&(2^n - 1) \times (2^n - 2) \times \ldots \times (2^n - 2^{n-1})\\ &\quad = (2^n - 1) \times 2 \times (2^{n-1} - 1) \times \ldots \times 2^{n-1} \times (2 - 1)\\ &\quad = 2 \times 2^2 \times \ldots \times 2^{n-1} \times (2^n - 1) \times (2^{n-1} - 1) \times \ldots \times (2 - 1)\\ &\quad = 2^{1+2+\ldots+(n-1)} \times (2^n - 1) \times (2^{n-1} - 1) \times \ldots \times (2 - 1)\\ &\quad = 2^{\frac{n(n-1)}{2}} \times (2^n - 1) \times (2^{n-1} - 1) \times \ldots \times (2 - 1)\end{aligned}$$

Le stabilisateur de $(\mathbb{F}_2)^k \times \{0_{n-k}\}$ sous l'action de $\mathrm{GL}(n,\mathbb{F}_2)$ sur Λ_k est d'ordre [1]

$$\underbrace{(2^k-1)(2^k-2)\dots(2^k-2^{k-1})}_{|\mathrm{GL}(k,\mathbb{F}_2)|}\times(2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1}).$$

Simplifions cette expression :

$$\begin{aligned}
&(2^k-1)(2^k-2)\dots(2^k-2^{k-1})(2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\\
&\quad=\Big((2^k-1)(2^k-2)\dots(2^k-2^{k-1})\Big)\Big((2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\Big)\\
&\quad=\Big((2^k-1)\times 2\times(2^{k-1}-1)\times\dots\times 2^{k-1}\times(2-1)\Big)\\
&\qquad\quad\Big(2^k\times(2^{n-k}-1)\times 2^{k+1}\times(2^{n-k-1}-1)\times\dots\times 2^{n-1}\times(2-1)\Big)\\
&\quad=2\times 2^2\times\dots 2^k\times 2^{k+1}\times\dots\times 2^{n-1}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\quad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times(2-1)\\
&\quad=2^{1+2+\dots+(n-1)}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\quad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)\\
&\quad=2^{\frac{n(n-1)}{2}}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\quad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)
\end{aligned}$$

Le ratio de ces deux quantités donne le cardinal recherché soit

$$\frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-k+1}-1)}{(2^k-1)(2^{k-1}-1)\dots(2-1)}.$$

Exercice 15

Soit G un groupe. Soient H et K deux sous-groupes distingués de G.

Montrer que le sous-groupe de G engendré par $\mathrm{H}\cup\mathrm{K}$ est aussi distingué dans G.

Solution 15

Soient $g\in\mathrm{G}$ et $x\in\langle\mathrm{H}\cup\mathrm{K}\rangle$. Il existe donc y_1, y_2, …, y_m dans $\mathrm{H}\cup\mathrm{K}$ tels que $x=y_1y_2\dots y_m$ et

$$gxg^{-1}=gy_1y_2\dots y_mg^{-1}.$$

Si y_1 appartient à H alors puisque H est distingué dans G il existe $y_1'\in\mathrm{H}$ tel que $gy_1=y_1'g$. Si y_1 appartient à K alors puisque K est distingué dans G il existe $y_1''\in\mathrm{K}$ tel que $gy_1=y_1''g$. Ainsi il existe $z_1\in\mathrm{H}\cup\mathrm{K}$ tel que $gy_1=z_1g$.

En fait pour tout $1\leqslant i\leqslant m$ il existe $z_i\in\mathrm{H}\cup\mathrm{K}$ tel que $gy_i=z_ig$.

Nous obtenons donc

$$\begin{aligned}
gxg^{-1}&=gy_1y_2\dots y_mg^{-1}\\
&=z_1gy_2\dots y_mg^{-1}\\
&=z_1z_2g\dots y_mg^{-1}\\
&=\dots\\
&=z_1z_2\dots z_mgg^{-1}\\
&=z_1z_2\dots z_m
\end{aligned}$$

Or $z_1z_2\dots z_m$ appartient à $\mathrm{H}\cup\mathrm{K}$ donc gxg^{-1} appartient à $\mathrm{H}\cup\mathrm{K}$. Ainsi $\langle\mathrm{H}\cup\mathrm{K}\rangle$ est distingué dans G.

Exercice 16

Soit G un groupe. Rappelons que le centralisateur d'un élément de G est l'ensemble des éléments de G qui commutent avec lui.

1. cela revient à choisir une matrice de $\mathrm{GL}(k,\mathbb{F}_2)$ puis à choisir un vecteur non nul linéairement indépendant avec les k premiers puis un vecteur non nul linéairement indépendant avec les $k+1$ premiers...

1. Montrer que le centralisateur d'un élément de G est un sous-groupe de G.
2. Dans $\mathcal{S}_4$ quel est le centralisateur de $(1\ 2)$? Est-ce un sous-groupe distingué de $\mathcal{S}_4$?

Solution 16

1. Soit G un groupe. Montrons que le centralisateur C_g d'un élément g de G est un sous-groupe de G.
   Notons que e appartient à C_g.
   Soit x dans C_g. Alors $gx = xg$ d'où $x^{-1}gxx^{-1} = x^{-1}xgx^{-1}$ c'est-à-dire $x^{-1}g = gx^{-1}$, autrement dit x^{-1} appartient à C_g.
   Soient x et y dans C_g. Alors
   $$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$
   i.e. xy appartient à C_g.
   Il en résulte que C_g est un sous-groupe de G.
2. Déterminons le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$.
   Soit σ un élément de $\mathcal{S}_n$. Si $(i\ j)$ est une transposition quelconque alors $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$. En effet soit $y \in \{1, 2, \ldots, n\}$;
   - si $y = \sigma(i)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(j)$;
   - si $y = \sigma(j)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(i)$;
   - si $y \notin \{\sigma(i), \sigma(j)\}$, alors $\big((i\ j)\sigma^{-1}\big)(y) = \sigma^{-1}(y)$ et $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = y$.

   Ainsi le centralisateur de $(i\ j)$ est constitué des permutations $\sigma \in \mathcal{S}_n$ qui laisse l'ensemble $\{i, j\}$ invariant, *i.e.* des permutations $\sigma \in \mathcal{S}_n$ telles que $\sigma(i) = i$ ou j et $\sigma(j) = j$ ou i. En particulier le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$ est $\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.
   Considérons la permutation $(3\ 4)$ qui appartient au centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$. Conjuguons là par la transposition $(2\ 3)$. Nous obtenons $(2\ 4)$, *i.e.* $(2\ 3)(1\ 2)(2\ 3) = (2\ 4)$. En particulier $(2\ 3)(1\ 2)(2\ 3)$ n'appartient pas au centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$. Le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$ n'est donc pas un sous-groupe distingué de $\mathcal{S}_4$.

Exercice 17

Soit G un groupe. Soient H et K deux groupes de G. Considérons un sous-groupe L de $\mathrm{H}\cap\mathrm{K}$ qui est distingué dans H et dans K.

Montrer que L est distingué dans le sous-groupe de G engendré par $\mathrm{H} \cup \mathrm{K}$.

Solution 17

Le sous-groupe L est un sous-groupe de $\langle \mathrm{H} \cup \mathrm{K}\rangle$. Soit z un élément de $\langle \mathrm{H} \cup \mathrm{K}\rangle$. Nous pouvons écrire z sous la forme $z_1z_2\ldots z_m$ les z_i, $1 \leqslant i \leqslant m$, appartenant à $\mathrm{H} \cup \mathrm{K}$.

Soit $\ell \in \mathrm{L}$; alors
$$z\ell z^{-1} = z_1z_2\ldots(z_m\ell z_m^{-1})\ldots z_2^{-1}z_1^{-1}.$$
L'élément $z_m\ell z_m^{-1}$ appartient à L ; en effet si z_m appartient à H (respectivement K), nous utilisons le fait que L est distingué dans H (respectivement K).

Nous en déduisons de la même façon que $z_{m-1}z_m\ell z_m^{-1}z_{m-1}^{-1}$ appartient à L. Par récurrence $z\ell z^{-1}$ appartient à L ce qui prouve que L est distingué dans $\langle \mathrm{H} \cup \mathrm{K}\rangle$.

Exercice 18

Montrer que dans un groupe tout sous-groupe d'indice 2 est distingué.

Solution 18

Soit G un groupe. Soit H un sous-groupe d'indice 2 de G. Nous avons donc $\mathrm{G}/\mathrm{H} = \big\{\mathrm{H}, x\mathrm{H}\big\}$ où $x \neq \mathrm{H}$ et $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $\mathrm{H} \cap x\mathrm{H} = \emptyset$.

Soit $g \in \mathrm{G}$. Ou bien $g \in \mathrm{H}$ et $g\mathrm{H}g^{-1} = \mathrm{H}$. Ou bien $g \notin \mathrm{H}$ et $g \in x\mathrm{H}$; il existe donc $h_0 \in \mathrm{H}$ tel que $g = xh_0$. Soit alors $h \in \mathrm{H}$; nous avons
$$ghg^{-1} = xh_0hh_0^{-1}x^{-1} = xh'x^{-1}$$
où $h' = h_0hh_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à $x\mathrm{H}$, *i.e.* $xh'x^{-1}$ s'écrit xh_1 avec h_1 dans H. Ceci implique que x appartient à H : contradiction. Par conséquent $xh'x^{-1}$ appartient à H, *i.e.* ghg^{-1} appartient à H. Autrement dit H est un sous-groupe distingué de G.

Exercice 19

Soit G un groupe. Soient H et K des sous-groupes de G. Supposons que

- H et K sont des sous-groupes distingués de G ;
- $\mathrm{H} \cap \mathrm{K} = \{e\}$;
- HK = G.

Considérons l'application

$$\varphi \colon \mathrm{H} \times \mathrm{K} \to \mathrm{G} \qquad\qquad \varphi(h, k) = hk.$$

1. Montrer que φ est une application injective.
2. Montrer que φ est un isomorphisme de groupes.

Solution 19

1. Montrons que φ est une application injective.
   Soient h et h' dans H, soient k et k' dans K. Supposons que $\varphi(h, k) = \varphi(h', k')$, *i.e.* $hk = h'k'$ ce que nous pouvons réécrire $h^{'-1}h = k'k^{-1}$. D'une part $h^{'-1}h$ appartient à H, d'autre part $k^{'-1}k$ appartient à K. Il en résulte que $h^{'-1}h = k'k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K} = \{e\}$. Ainsi $h = h'$, $k = k'$ et φ est injective.
2. Montrons que φ est un isomorphisme de groupes.
   Par hypothèse HK = G donc φ est surjective.
   Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk = k_1h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1h = h_1k_1$ pour un certain h_1 dans H. Or φ est injective donc $h = h_1$, $k = k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$ d'où
   - HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK ;
   - φ est un morphisme de groupes.

   Par suite φ est un isomorphisme de groupes.

Exercice 20

Soit G un groupe. Soient H et K deux sous-groupes propres de G. Supposons que
- H et K sont des sous-groupes d'indice 2 dans G ;
- $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution 20

Les groupes H et K sont d'indice 2 dans G ils sont donc distingués dans G.
De plus $\mathrm{H} \cap \mathrm{K} = \{e\}$ donc HK est un sous-groupe distingué de G. En effet
- Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk = k_1h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1h = h_1k_1$ pour un certain h_1 dans H. Or φ est injective donc $h = h_1$, $k = k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$. Ainsi HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK.
- Le groupe HK est distingué dans G ; en effet soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Comme H est distingué dans G l'éléement $ghkg^{-1}$ s'écrit aussi h_1gkg^{-1} avec h_1 dans H. Par ailleurs $h_1gkg^{-1} = h_1k_1gg^{-1} = h_1k_1$ avec k_1 dans K car K est distingué dans G. Il s'en suit que $ghkg^{-1}$ appartient à HK.
- Montrons que H et K sont d'ordre 2. Nous avons $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $x \notin \mathrm{H}$. Comme K est d'indice 2 il est d'ordre au moins 2 et contient donc au moins un élément k qui n'est pas dans H (en particulier $k \neq e$). Nous pouvons donc prendre pour x cet élément k. Ainsi $\mathrm{G} = \mathrm{H} \cup k\mathrm{H}$ avec $\mathrm{H} \cap k\mathrm{H} = \emptyset$. Soit $k' \in \mathrm{K} \setminus \{e\}$. Ainsi k' n'appartient pas à H et $k' \in k\mathrm{H}$. Il existe donc $h \in \mathrm{H}$ tel que $k' = kh$. Par suite $h = k^{-1}k'$ est aussi dans K donc $h = e$ et $k = k'$. Le groupe K contient donc seulement deux éléments : e et k.
  De même nous obtenons que H est d'ordre 2.
  Ainsi H et K sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$.
- Montrons que G = KH. Soit $g \in \mathrm{G}$. Alors ou bien g appartient à H et donc g appartient à HK, ou bien g appartient à $k\mathrm{H}$, *i.e.* $g = kh$ avec $h \in \mathrm{H}$. Or HK = KH donc g appartient à HK.

Finalement G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 21

Pour a et b réels on définit l'application

$$\tau_{a,b} \colon \mathbb{R} \to \mathbb{R} \qquad\qquad x \mapsto ax + b.$$

1. Soit $G = \{\tau_{a,b} \,|\, a \neq 0\}$.
   Montrer que G est un groupe pour la composition des applications.
2. Soit $H = \{\tau_{a,b} \,|\, a \neq 0,\, a \in \mathbb{Q}\}$.
   Montrer que H est un sous-groupe de G.
3. Décrire les classes à droite de H dans G.
   Montrer que toute classe à gauche (modulo H) est classe à droite (modulo H). (Indication : considérer l'application qui à l'élément $\tau_{a,b}$ de G associe la classe de a dans ${}^{\mathbb{R}^*}\!/_{\mathbb{Q}^*}$).
4. Donner un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.
5. Soit $N = \{\tau_{a,b} \,|\, a = 1\}$.
   Montrer que N est un sous-groupe distingué de G.

Solution 21

1. Soit $G = \{\tau_{a,b} \,|\, a \neq 0\}$.
   Montrons que G est un groupe pour la composition des applications.
   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de G. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite G est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.
2. Soit $H = \{\tau_{a,b} \,|\, a \neq 0,\, a \in \mathbb{Q}\}$.
   Montrons que H est un sous-groupe de G.
   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de H. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite H est un sous-groupe de G.
3. Décrivons les classes à droite de H dans G et montrons que toute classe à gauche (mod H) est classe à droite (modulo H).
   La classe à droite de l'élément $\tau_{\alpha,\beta}$ de G est l'ensemble des $\tau_{\alpha a,\alpha b+\beta}$ où $a \in \mathbb{Q}$.
   Pour montrer que toute classe à gauche est une classe à droite il suffit de montrer que H est distingué dans G. Considérons le morphisme de groupes
   $$\varphi\colon G \to {}^{\mathbb{R}^*}\!/_{\mathbb{Q}^*} \qquad\qquad \tau_{a,b} \mapsto \text{ la classe de } a \text{ dans } {}^{\mathbb{R}^*}\!/_{\mathbb{Q}^*}$$
   Son noyau est H qui est donc distingué dans G.
4. Donnons un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.
   Soit K le sous-groupe de G des éléments $\tau_{a,b}$ où a et b sont rationnels. Les classes à gauche et à droite de K dans G ne coïncident pas.
5. Soit $N = \{\tau_{a,b} \,|\, a = 1\}$.
   Montrons que N est un sous-groupe distingué de G.
   L'identité appartient à N. Soient $\tau_{1,b}$ et $\tau_{1,b'}$ deux éléments de N. Nous avons $\tau_{1,b} \circ \tau_{1,b'}^{-1} = \tau_{1,b-b'}$; en particulier $\tau_{1,b} \circ \tau_{1,b'}^{-1}$ appartient à N. Ainsi N est un sous-groupe de G.
   Soit $\tau_{\alpha,\beta}$ un élément quelconque de G et soit $\tau_{1,b}$ un élément quelconque de N. Alors
   $$\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1} = \tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{1/\alpha,-\beta/\alpha} = \tau_{1,\alpha b};$$
   ainsi $\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1}$ appartient à N ce qui prouve que N est un sous-groupe distingué de G.

Exercice 22

Soit H un sous-groupe d'un groupe G tel que toute classe à gauche modulo H soit classe à droite modulo H. Le sous-groupe H est-il distingué ?

Solution 22

Supposons que H ne soit pas distingué dans G. Cela signifie qu'il existe $g \in G \smallsetminus \{e\}$ tel que $gH \neq Hg$ ou encore qu'il existe $h \in H$ tel que gh n'appartient pas à Hg.

Ainsi gh appartient à une autre classe à droite que nous noterons Hg' ($Hg' \neq Hg$). Puisque toute classe à gauche est une classe à droite et que les classes à droite forment une partition de G la classe à droite qui est égale à gH est nécessairement Hg'.

Donc g appartient à $g\mathrm{H}$ et $\mathrm{H}g$. Comme $g\mathrm{H} = \mathrm{H}g'$ l'élément g appartient aussi à $\mathrm{H}g'$. Autrement dit g appartient à $\mathrm{H}g \cap \mathrm{H}g'$. Ceci n'est possible que si $g = e$ ou $\mathrm{H}g = \mathrm{H}g'$. Mais par hypothèse $g \neq e$ et $\mathrm{H}g \neq \mathrm{H}g'$.

Il en résulte que H est distingué dans G.

Exercice 23

Soit G un groupe fini. Soit H un sous-groupe de G. Soit N un sous-groupe distingué de G.

Montrer que si $|\mathrm{H}|$ et $[\mathrm{G} : \mathrm{N}]$ sont premiers entre eux, alors H est un sous-groupe de N.

Solution 23

Raisonnons par l'absurde : supposons que H ne soit pas un sous-groupe de N. Alors il existe $h \in \mathrm{H}$ qui n'est pas un élément de N. Il s'en suit que $h\mathrm{N}$ est un élément différent de l'élément neutre N de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$.

Soit q l'ordre de $h\mathrm{N}$ dans ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. On sait que $q \neq 1$ et que q divise $|{}^{\mathrm{G}}\!/_{\mathrm{N}}| = [\mathrm{G} : \mathrm{N}]$. Par ailleurs $h^{|\mathrm{H}|} = e$ donc $(h\mathrm{N})^{|\mathrm{H}|} = \mathrm{N}$. Par suite q divise $|\mathrm{H}|$. Ainsi $q \neq 1$ est un diviseur commun à $[\mathrm{G} : \mathrm{N}]$ et $|\mathrm{H}|$ qui sont premiers entre eux : contradiction. Il en résulte que H est un sous-groupe de N.

Exercice 24

Soit G un groupe qui ne contient qu'un seul sous-groupe H d'ordre n.

Montrer que H est distingué dans G.

Solution 24

Nous allons montrer que H est un sous-groupe caractérisque de G. Soit φ un automorphisme de G et $\varphi_{|\mathrm{H}} \colon \mathrm{H} \to \varphi(\mathrm{H})$ la restriction de φ à H et à son image. Comme φ est un automorphisme de G, $\varphi_{|\mathrm{H}}$ est bijective. C'est donc un isomorphisme de groupes. Étant donné que H est fini d'ordre n, $\varphi(\mathrm{H})$ est fini d'ordre n. Or H est l'unique sous-groupe de G d'ordre n donc $\varphi(\mathrm{H}) = \mathrm{H}$.

Puisque H est un sous-groupe caractéristique de G c'est un sous-groupe distingué de G.

Exercice 25

Soit H un sous-groupe de G tel que le produit de deux classes à gauche modulo H soit une classe à gauche modulo H.

Le sous-groupe H est-il distingué dans G ?

Solution 25

Comme le produit de deux classes à gauche est une classe à gauche pour tout couple (g, g') d'éléments de G il existe $g'' \in \mathrm{G}$ tel que $g\mathrm{H}g'\mathrm{H} = g''\mathrm{H}$. En particulier il existe g'' tel que $g\mathrm{H}g^{-1}\mathrm{H} = g''\mathrm{H}$. Et pour tout élément h de H il existe h' et h'' dans H tels que $ghg^{-1}h' = g''h''$. En particulier puisque e appartient à H il existe h'' dans H tel que $geg^{-1}e = g''h''$ ce qui se réécrit $e = g''h''$. Ainsi $g'' = h''^{-1} \in \mathrm{H}$ et $g\mathrm{H}g^{-1}\mathrm{H} = \mathrm{H}$, c'est-à-dire $g\mathrm{H}g^{-1} = \mathrm{H}$. Le sous-groupe H est donc distingué dans G.

Exercice 26

Soit G un groupe. Soit H un sous-groupe distingué de G.

Montrer que si H est cyclique tout sous-groupe de H est distingué dans G.

Solution 26

Soit h un générateur de H. Soit K un sous-groupe du groupe cyclique distingué H. Alors tous les éléments de K sont égaux à une puissance de h et K est lui-même cyclique engendré par une puissance de h : posons $p_0 = \inf\{p \in \mathbb{N}^* \mid h^p \in \mathrm{K}\}$. Soit h^p un élément de K. Nous avons $p = qp_0 + r$ avec $0 \leqslant r < p_0$. Par suite $h^p = (h^{p_0})^q h^r$ et $h^r = h^p(h^{-p_0})^q$ appartient à K. Puisque $p_0 = \inf\{p \in \mathbb{N}^* \mid h^p \in \mathrm{K}\}$ nous avons nécessairement $r = 0$ et $\mathrm{K} = \langle h^{p_0} \rangle$.

Puisque H est distingué dans G pour tout $g \in \mathrm{G}$ il existe q tel que $ghg^{-1} = h^q$. Par conséquent $gh^{p_0}g^{-1} = h^{qp_0}$ et K est distingué dans G.

Exercice 27

Soient A un groupe et C un sous-groupe distingué de A. Soient B un groupe et D un sous-groupe distingué de B.

Montrer que ${}^{\mathrm{A} \times \mathrm{B}}\!/_{\mathrm{C} \times \mathrm{D}} \simeq {}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Solution 27

Considérons le morphisme de groupes entre $A \times B$ et $A/_C \times B/_D$ donné par

$$\varphi((a,b)) = (aC, bD).$$

Le noyau de φ est égal à

$$\begin{aligned}\ker\varphi &= \big\{(a,b)\in A\times B \,|\, aC = C \text{ et } bD = D\big\}\\ &= \big\{(a,b)\in A\times B \,|\, a\in C \text{ et } b\in D\big\}\\ &= C\times D.\end{aligned}$$

Par ailleurs (aC, bD) est l'image de (a,b) par φ donc φ est surjectif. Il en résulte que φ induit un isomorphisme entre $A\times B/_{C\times D}$ et $A/_C \times B/_D$.

Exercice 28

Soient G_1 et G_2 deux groupes non isomorphes.

1. Montrer que $Z(G_1)\times Z(G_2)$ est isomorphe à $Z(G_1\times G_2)$.
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrer que $G_1\times G_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   (b) Montrer que si H est un sous-groupe distingué de $G_1\times G_2$, alors $H\cap H_1$ est distingué dans H_1 et $H\cap H_2$ est distingué dans H_2.
   (c) En déduire que H_1 et H_2 sont les seuls sous-groupes distingués de $G_1\times G_2$.

Solution 28

1. Montrons que $Z(G_1)\times Z(G_2)$ est isomorphe à $Z(G_1\times G_2)$.
   Soit $(x_1,x_2)\in G_1\times G_2$; alors (x_1,x_2) appartient à $Z(G_1\times G_2)$ si et seulement si

   $$\forall\,(y_1,y_2)\in G_1\times G_2 \qquad (x_1,x_2)(y_1,y_2) = (y_1,y_2)(x_1,x_2)$$

   si et seulement si

   $$\forall\,(y_1,y_2)\in G_1\times G_2 \qquad (x_1y_1, x_2y_2) = (y_1x_1, y_2x_2)$$

   si et seulement si

   $$\forall\,(y_1,y_2)\in G_1\times G_2 \qquad x_1y_1 = y_1x_1 \text{ et } x_2y_2 = y_2x_2.$$

   Par conséquent (x_1,x_2) appartient à $Z(G_1\times G_2)$ si et seulement si x_1 appartient à $Z(G_1)$ et x_2 appartient à $Z(G_2)$. Ainsi

   $$Z(G_1\times G_2)\simeq Z(G_1)\times Z(G_2).$$

2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrons que $G_1\times G_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   Soit $H_1 = G_1\times\{e_2\}$ où e_2 est l'élément neutre de G_2. Le groupe H_1 est un sous-groupe de $G_1\times G_2$ isomorphe à G_1. De plus H_1 est distingué dans $G_1\times G_2$ car pour tout $(x_1,x_2)\in G_1\times G_2$, pour tout $(x,e_2)\in H_1$ nous avons

   $$(x_1,x_2)(x,e_2)(x_1,x_2)^{-1} = (x_1,x_2)(x,e_2)(x_1^{-1},x_2^{-1}) = (x_1xx_1^{-1}, x_2x_2^{-1}) = (x_1xx_1^{-1}, e_2)$$

   et $(x_1,x_2)(x,e_2)(x_1,x_2)^{-1}$ appartient à H_1.
   De même $H_2 = \{e_1\}\times G_2$ est un sous-groupe distingué de $G_1\times G_2$.
   (b) Montrons que si H est un sous-groupe distingué de $G_1\times G_2$, alors $H\cap H_1$ est distingué dans H_1 et $H\cap H_2$ est distingué dans H_2.
   Soit $(x_1,e_2)\in H_1$ et soit $(x,e_2)\in H\cap H_1$; nous avons

   $$(x_1,e_2)(x,e_2)(x_1,e_2)^{-1} = (x_1,e_2)(x,e_2)(x_1^{-1},e_2) = (x_1xx_1^{-1},e_2)$$

   donc $(x_1,e_2)(x,e_2)(x_1,e_2)^{-1}$ appartient à H_1. Par ailleurs H est un sous-groupe distingué de $G_1\times G_2$ donc $(x_1,e_2)(x,e_2)(x_1,e_2)^{-1}$ appartient à H. Finalement $(x_1,e_2)(x,e_2)(x_1,e_2)^{-1}$ appartient à $H\cap H_1$ et $H\cap H_1$ est un sous-groupe distingué de H_1.
   De même $H\cap H_2$ est un sous-groupe distingué de H_2.

(c) Les sous-groupes H_1 et H_2 sont isomorphes à G_1 et G_2 respectivement. Les groupes G_1 et G_2 étant simples les groupes H_1 et H_2 sont aussi simples. Il y a donc quatre cas possibles qui sont les suivants :

i) $\mathrm{H} \cap \mathrm{H}_1 = \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_2 = \mathrm{H}_2$ auquel cas $\mathrm{H} = \mathrm{G}_1 \times \mathrm{G}_2$.

ii) $\mathrm{H} \cap \mathrm{H}_1 = \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_2 = \{(e_1, e_2)\}$ auquel cas $\mathrm{H} = \mathrm{H}_1$.

iii) $\mathrm{H} \cap \mathrm{H}_1 = \{(e_1, e_2)\}$ et $\mathrm{H} \cap \mathrm{H}_2 = \mathrm{H}_2$ auquel cas $\mathrm{H} = \mathrm{H}_2$.

iv) $\mathrm{H} \cap \mathrm{H}_1 = \{(e_1, e_2)\}$ et $\mathrm{H} \cap \mathrm{H}_2 = \{(e_1, e_2)\}$ auquel cas $\mathrm{H} = \{(e_1, e_2)\}$. En effet ${}^{\mathrm{HH}_1}\!/_{\mathrm{H}_1}$ (qui est isomorphe à H) est distingué dans ${}^{\mathrm{G}}\!/_{\mathrm{H}_1}$, groupe qui est lui-même isomorphe à G_2.
De la même façon nous obtenons que si H n'est pas trivial il est isomorphe à G_1.
Ainsi si H n'est pas trivial, il est isomorphe à G_1 et à G_2 et G_1 et G_2 sont isomorphes : contradiction.
Par conséquent $\mathrm{H} = \{(e_1, e_2)\}$.

Ainsi les seuls sous-groupes distingués propres de $\mathrm{G}_1 \times \mathrm{G}_2$ sont H_1 et H_2.

Exercice 29

Soient G un groupe et H un sous-groupe de G.

(a) Montrer qu'en posant $g \cdot a\mathrm{H} = (ga)\mathrm{H}$, où a, $g \in \mathrm{G}$, on définit une action de G sur l'ensemble ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ des classes à gauche modulo H.

(b) Montrer que cette action est transitive.
Déterminer le stabilisateur de $a\mathrm{H}$.

(c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Solution 29

(a) Posons $X = {}^{\mathrm{G}}\!/_{\mathrm{H}}$. Soient g dans G et x dans X. Désignons par a, a' deux représentants de la classe à gauche x. On a $a\mathrm{H} = a'\mathrm{H} = x$ ou encore $a^{-1}a' \in \mathrm{H}$. Or

$$(ga)^{-1}ga' = a^{-1}g^{-1}ga' = a^{-1}a' \in \mathrm{H}$$

donc $ga\mathrm{H} = ga'\mathrm{H}$.
Si on remplace a par un autre représentant a' de la classe $x = a\mathrm{H}$, alors $ga'\mathrm{H} = ga\mathrm{H}$. La formule a donc bien un sens et définit une application de $\mathrm{G} \times X \to X$.
C'est bien une action de G sur X puisque

- $\forall\, x = a\mathrm{H} \in X$ nous avons $e \cdot x = ea\mathrm{H} = a\mathrm{H} = x$,
- $\forall\, x = a\mathrm{H} \in X$, $\forall\, g \in \mathrm{G}$, $\forall\, g' \in \mathrm{G}$ nous avons

$$g \cdot (g' \cdot x) = g \cdot (g'a\mathrm{H}) = g(g'a)\mathrm{H} = (gg')a\mathrm{H} = gg' \cdot x$$

(b) Pour tous $x = a\mathrm{H} \in X$ et $y = b\mathrm{H} \in X$ il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ (prendre $g = ba^{-1}$). Il existe donc une seule orbite, égale à X.
Le stabilisateur de $x = a\mathrm{H}$ est $a\mathrm{H}a^{-1}$ car :

$$g \in \mathrm{G}_x \Longleftrightarrow ga\mathrm{H} = a\mathrm{H} \Longleftrightarrow a^{-1}ga\mathrm{H} = \mathrm{H} \Longleftrightarrow a^{-1}ga \in \mathrm{H} \Longleftrightarrow g \in a\mathrm{H}a^{-1}.$$

(c) Comme $\mathrm{G}_x = a\mathrm{H}a^{-1} = \mathrm{Ad}_a(\mathrm{H}) \simeq \mathrm{H}$, on retrouve le théorème de Lagrange

$$[\mathrm{G} : \mathrm{H}] = \mathrm{card}\Big({}^{\mathrm{G}}\!/_{\mathrm{H}}\Big) = \mathrm{card}(\mathrm{orb}(x)) = \frac{[\mathrm{G} : 1]}{[\mathrm{G}_x : 1]} = \frac{[\mathrm{G} : 1]}{[\mathrm{H} : 1]}.$$

Exercice 30

Soient p un nombre premier et $a > 1$. En utilisant une action de groupe que l'on précisera montrer que tout groupe G d'ordre p^a admet un élément central (*i.e.* qui commute avec tout élément de G) d'ordre p.

Solution 30

Faisons agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites on a donc $|Z(\mathrm{G})| \equiv 0 \bmod p$, ce qui interdit à $Z(\mathrm{G})$ d'être trivial. Soit $g \in Z(\mathrm{G}) \smallsetminus \{1\}$, alors g est d'ordre p^b pour un certain $1 \leqslant b \leqslant a$. Alors $g^{p^{b-1}}$ appartient à $Z(\mathrm{G})$ et est d'ordre p.

Exercice 31

Soit G un groupe. Soient H et K deux sous-groupes de G tels que $\mathrm{K} \subset \mathrm{H} \subset \mathrm{G}$.

a) Supposons que G soit fini. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}|\,.$$

b) On ne suppose plus que G est fini. On suppose par contre que H et K sont distingués dans G. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}|\,.$$

Solution 31

a) Comme G est fini, on a

$$|\mathrm{G}| = |\mathrm{G} : \mathrm{H}|\,|\mathrm{H}| \qquad |\mathrm{H}| = |\mathrm{H} : \mathrm{K}|\,|\mathrm{K}| \qquad |\mathrm{G}| = |\mathrm{G} : \mathrm{K}|\,|\mathrm{K}|$$

L'ordre d'un groupe n'est jamais nul donc $|\mathrm{K}| \neq 0$ et

$$|\mathrm{G} : \mathrm{K}| = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{|\mathrm{G} : \mathrm{H}|\,|\mathrm{H}|}{|\mathrm{K}|} = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}|\,.$$

b) Les groupes G/H et $(\mathrm{G}/\mathrm{K})/(\mathrm{H}/\mathrm{K})$ sont isomorphes donc $\left|\mathrm{G}/\mathrm{H}\right| = \left|(\mathrm{G}/\mathrm{K})/(\mathrm{H}/\mathrm{K})\right|$ soit $|\mathrm{G} : \mathrm{H}| = \left|\mathrm{G}/\mathrm{K} : \mathrm{H}/\mathrm{K}\right|$ d'où $|\mathrm{G} : \mathrm{H}|\left|\mathrm{H}/\mathrm{K}\right| = \left|\mathrm{G}/\mathrm{K}\right|$, *i.e.*

$$|\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| = |\mathrm{G} : \mathrm{K}|\,.$$

Exercice 32

Soit G un groupe. Les assertions suivantes sont-elles vraies ou fausses ? Justifier.

a) Si tout sous-groupe H de G est distingué dans G, alors G est abélien.

b) Si $\mathrm{H} \triangleleft \mathrm{G}$ et $\mathrm{K} \triangleleft \mathrm{H}$, alors $\mathrm{K} \triangleleft \mathrm{G}$.

c) Soient g et h dans G d'ordre fini. Alors gh est d'ordre fini.

d) Si G a un nombre fini de sous-groupes, alors G est fini.

e) Si H et K sont des sous-groupes de G, alors $\langle \mathrm{H} \cup \mathrm{K} \rangle = \mathrm{HK}$.

Solution 32

a) Faux. Considérons le groupe $\mathbb{H}_8$ des quaternions. Rappelons qu'il est défini de la façon suivante : $\mathbb{H}_8$ est l'ensemble

$$\mathbb{H}_8 = \big\{ \pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k} \big\}$$

et la loi de groupe est définie par

$$\begin{aligned}
&(-1)^2 = 1,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1\\
&(-1)\cdot\mathbf{i} = \mathbf{i}\cdot(-1) = -\mathbf{i},\ (-1)\cdot\mathbf{j} = \mathbf{j}\cdot(-1) = -\mathbf{j},\ (-1)\cdot\mathbf{k} = \mathbf{k}\cdot(-1) = -\mathbf{k}\\
&\mathbf{i}\cdot\mathbf{j} = -\mathbf{j}\cdot\mathbf{i} = \mathbf{k}.
\end{aligned}$$

Les sous-groupes de $\mathbb{H}_8$ sont
— le sous-groupe trivial $\{\mathrm{id}\}$ qui est distingué dans $\mathbb{H}_8$,
— le sous-groupe d'ordre 2 engendré par -1 qui est distingué dans $\mathbb{H}_8$ car contenu dans le centre de $\mathbb{H}_8$,
— les sous-groupes d'ordre 4 sont d'indice 2 dans $\mathbb{H}_8$ donc distingués dans $\mathbb{H}_8$,
— le sous-groupe $\mathbb{H}_8$ entier qui est distingué dans $\mathbb{H}_8$.
Les sous-groupes de $\mathbb{H}_8$ sont donc tous distingués dans $\mathbb{H}_8$ mais $\mathbb{H}_8$ n'est pas abélien.

b) Faux. Considérons par exemple $\mathrm{G} = \mathcal{S}_4$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 2)(3\ 4)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

c) Faux. Pour avoir un contre-exemple il faut que le groupe G soit infini et non abélien. Prenons par exemple $\mathrm{G} = \mathrm{GL}(2, \mathbb{Q})$, $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'élément g est d'ordre 2, l'élément h est d'ordre 3 mais $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

d) Vrai. Tout élément de G est d'ordre fini : si g est d'ordre infini, alors le sous-groupe engendré par g est isomorphe à $\mathbb{Z}$ et contient donc une infinité de sous-groupes distincts. Or G a un nombre fini de sous-groupes cycliques notés $\langle g_1\rangle, \ldots, \langle g_n\rangle$. Donc pour tout g dans G il existe i tel que $\langle g\rangle = \langle g_i\rangle$, autrement dit g est une puissance de g_i. Ceci assure que le cardinal de G est borné par la somme des ordres des g_i. Il s'en suit que G est fini.

e) Faux. L'inclusion $\mathrm{HK} \subset \langle \mathrm{H} \cup \mathrm{K}\rangle$ est toujours vérifiée. En revanche le sous-ensemble HK n'est en général pas un sous-groupe de G contrairement à $\langle \mathrm{H}\cup\mathrm{K}\rangle$. En effet prenons par exemple $\mathrm{G} = \mathcal{S}_3$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 3)\}$. Alors $\langle \mathrm{H}\cup\mathrm{K}\rangle$ coïncide avec G et $\mathrm{HK} = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$ n'est pas un sous-groupe de G.
La réponse est vraie si l'on suppose que H ou K est distingué dans G (exercice).

Exercice 33

Soit S un sous-ensemble non vide d'un groupe fini G. Soit $N(S) = \{g \in \mathrm{G} \mid gSg^{-1} = S\}$ le normalisateur de S dans G. Soit $C(S) = \{g \in \mathrm{G} \mid \forall s \in S,\ gsg^{-1} = s\}$ le centralisateur de S dans G.

Montrer que

a) $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$.

b) $N(S) = \mathrm{G}$ si et seulement si $S = \bigcup_{g\in\mathrm{G}} gSg^{-1}$.

c) Si $\mathrm{H} \lhd \mathrm{G}$, alors $C(\mathrm{H}) \lhd \mathrm{G}$.

d) Si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Solution 33

a) Montrons que $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$. Bien sûr e appartient à $N(S)$. Soient g et h dans $N(S)$. Alors

$$(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$$

donc gh appartient à $N(S)$. Si g appartient à $N(S)$ on a $gSg^{-1} = S$ donc en multipliant à gauche et à droite par g^{-1} et g respectivement on a $S = g^{-1}Sg$, autrement dit g^{-1} appartient à $N(S)$. Ainsi $N(S)$ est un sous-groupe de G.
De même $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons que $C(S)$ est distingué dans $N(S)$. Soient $g \in C(S)$ et $h \in N(S)$. Soit $s \in S$. Alors

$$(hgh^{-1})s(hgh^{-1})^{-1} = hg(h^{-1}sh)g^{-1}h^{-1}$$

et comme h appartient à $N(S)$, on a $h^{-1}sh$ appartient à S. Donc puisque g appartient à $C(S)$

$$g(h^{-1}sh)g^{-1} = h^{-1}sh$$

et finalement

$$(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s.$$

Ainsi hgh^{-1} appartient à $C(S)$ et $C(S) \lhd N(S)$.

b) Montrons que $N(S) = \mathrm{G}$ si et seulement si $S = \bigcup_{g\in\mathrm{G}} gSg^{-1}$.
Supposons que $N(S) = \mathrm{G}$. Alors pour tout $g \in \mathrm{G}$, on a $gSg^{-1} = S$ donc $S = \bigcup_{g\in\mathrm{G}} gSg^{-1}$.
Réciproquement supposons que $S = \bigcup_{g\in\mathrm{G}} gSg^{-1}$. Pour tout $g \in \mathrm{G}$ nous avons $g^{-1}Sg \subset S$ donc en multipliant par g et g^{-1} à gauche et à droite respectivement nous avons $S \subset gSg^{-1} \subset S$ d'où $S = gSg^{-1}$. Ainsi g appartient à $N(S)$ et $\mathrm{G} = N(S)$.

c) Montrons que si $\mathrm{H} \lhd \mathrm{G}$, alors $C(\mathrm{H}) \lhd \mathrm{G}$. Supposons que H soit distingué dans G. Soient g dans G, c dans $C(\mathrm{H})$ et h dans H. Nous avons

$$(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$$

puisque H est distingué dans G nous savons que $g^{-1}hg$ appartient à H. Or c appartient à $C(\mathrm{H})$ donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$ et finalement

$$(gcg^{-1})h(gcg^{-1})^{-1}$$

ce qui assure que gcg^{-1} appartient à $C(\mathrm{H})$. Le groupe $C(\mathrm{H})$ est donc distingué dans G.

d) Montrons que si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Par définition et a) $N(\mathrm{H})$ est un sous-groupe de G contenant H et H est distingué dans $N(\mathrm{H})$. Considérons un sous-groupe K de G contenant H tel que $\mathrm{H} \triangleleft \mathrm{K}$. Par définition nous avons $k\mathrm{H}k^{-1} = \mathrm{H}$ pour tout $k \in \mathrm{K}$. Par conséquent k appartient à $N(\mathrm{H})$ donc $\mathrm{K} \subset N(\mathrm{H})$ ce qui assure la maximalité de $N(\mathrm{H})$ parmi les sous-groupes de G concernés.

Exercice 34

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

$$\varphi(a)\colon \mathrm{G} \to \mathrm{G} \qquad\qquad g \mapsto aga^{-1}.$$

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

b) Montrer que $\varphi\colon \mathrm{G} \to \mathrm{Aut(G)}$, $g \mapsto \varphi(g)$ est un morphisme de groupes de G dans Aut(G).

c) Notons Int(G) l'ensemble des automorphismes intérieurs de G. Montrer que Int(G) est un sous-groupe distingué de Aut(G).

d) Notons $Z(\mathrm{G})$ le centre de G. Montrer que $\mathrm{Int(G)} \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Solution 34

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.* $\varphi(e) = \mathrm{id}$. 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 Aut(G).

c) Int(G) est l'image de G par le morphisme de groupes φ ; c'est donc un sous-groupe de 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 $\mathrm{Im}\,\varphi$. Le groupe Int(G) est distingué dans Aut(G).

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

Exercice 35

Soit G un groupe et soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ en fonction de ceux de G.

b) Soit K un sous-groupe de G.

   i) Si K est distingué dans G et contient H, montrer que

$$\frac{{}^{\mathrm{G}}\!/_{\mathrm{H}}}{{}^{\mathrm{K}}\!/_{\mathrm{H}}} \simeq {}^{\mathrm{G}}\!/_{\mathrm{K}}$$

   ii) Montrer que HK est un sous-groupe de G égal à KH.

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

iii) Montrer que H est distingué dans HK.

iv) Montrer que
$$\mathrm{K}/(\mathrm{K}\cap\mathrm{H}) \simeq \mathrm{HK}/\mathrm{H}.$$

Solution 35

Soit G un groupe et soit $H \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrivons les sous-groupes distingués de G/H en fonction de ceux de G. On note $\pi\colon \mathrm{G}\to\mathrm{G}/\mathrm{H}$ la projection canonique. La correspondance $K\mapsto\pi(K)$ établit une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de G/H donc la réciproque est donnée par $\overline{K}\mapsto\pi^{-1}(\overline{K})$. Cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de G/H.

b) Soit K un sous-groupe de G.

i) Supposons que K soit distingué dans G et que K contienne H. Montrons que
$$\mathrm{G}/\mathrm{H}\,\mathrm{K}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$$

Le morphisme $\pi\colon\mathrm{G}\to\mathrm{G}/\mathrm{H}$ composé avec la projection $\pi'\colon\mathrm{G}/\mathrm{H}\to(\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$ induit un morphisme surjectif $q\colon\mathrm{G}\to(\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$. Par construction un élément g de G appartient à $\ker q$ si et seulement si $\pi(g)$ appartient à $\ker\pi'=\mathrm{K}/\mathrm{H}$ si et seulement si g appartient à K. Ainsi $\ker q=\mathrm{K}$. Le théorème de factorisation assure alors que q induit un isomorphisme entre $\mathrm{G}/\ker q=\mathrm{G}/\mathrm{K}$ et $(\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$.

ii) Montrons que HK est un sous-groupe de G égal à KH.

Soient h, h' dans H et k, k' dans K. Le groupe H étant distingué dans G il existe h'' dans H tel que $k\cdot h'=h''\cdot k$. Par suite
$$(h\cdot k)\cdot(h'\cdot k')=(h\cdot h'')\cdot(k\cdot k')$$
appartient à HK et HK est un sous-groupe de G.

iv) Montrons que $\mathrm{K}/(\mathrm{K}\cap\mathrm{H})$ et $(\mathrm{HK})/\mathrm{H}$ sont isomorphes. L'inclusion $\mathrm{K}\to\mathrm{HK}$ induit un morphisme $p\colon\mathrm{K}\to(\mathrm{HK})/\mathrm{H}$. Montrons que p est surjectif : si h est dans H et k dans K, alors la classe $(h\cdot k)\mathrm{H}=k\mathrm{H}$ est l'image de k par p, donc p est surjectif. De plus un élément $k\in\mathrm{K}$ appartient à $\ker p$ si et seulement si il est dans H. Autrement dit $\ker p=\mathrm{K}\cap\mathrm{H}$. On conclut à l'aide du théorème de factorisation.

Exercice 36

Soit G un groupe fini. Soient H et K des sous-groupes de G. Supposons que

— H et K sont des sous-groupes distingués de G ;

— $\mathrm{H}\cap\mathrm{K}=\{e\}$.

Montrer que HK est un sous-groupe distingué de G d'ordre $|\mathrm{H}||\mathrm{K}|$.

Solution 36

Montrons tout d'abord que HK est un sous-groupe de G. On définit l'application φ par
$$\varphi\colon\mathrm{H}\times\mathrm{K}\to\mathrm{HK}\qquad\qquad (h,k)\mapsto hk.$$

Cette application est injective. En effet soient h, h' dans H et k, k' dans K tels que $f(h,k)=f(h',k')$, *i.e.* $hk=h'k'$. On en déduit que $hh'^{-1}=k'k^{-1}$; de plus $hh'^{-1}=k'k^{-1}$ appartient à $\mathrm{H}\cap\mathrm{K}=\{e\}$. Donc $hh'^{-1}=e$ et $kk'^{-1}=e$ c'est-à-dire $(h,k)=(h',k')$. Cette application est par définition surjective. Soient h, h' dans H et soient k, k' dans K. Puisque K est distingué il existe k_1 dans K tel que $hk=k_1h$. Comme H est distingué il existe h_1 dans H tel que $k_1h=h_1k_1$. Ainsi $hk=h_1k_1$. Mais φ est injective d'où $h=h_1$, $k=k_1$ et h et k commutent ($hk=kh$). Donc $hkh'k'=hh'kk'$. On en déduit que

— HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et si $g\in\mathrm{HK}$, alors $g^{-1}\in\mathrm{HK}$;

— φ est un morphisme de groupes.

En particulier φ est un isomorphisme de groupes.

Montrons que HK est distingué dans G. Soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Alors

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) = h_1(gkg^{-1})$$

avec h_1 dans H car H est distingué dans G. Par ailleurs $h_1gkg^{-1} = h_1k_1$ avec k_1 dans K car K est distingué dans G. Donc $ghkg^{-1}$ appartient à HK et HK est distingué dans G.

Montrons que HK est d'ordre $|\mathrm{H}||\mathrm{K}|$. Comme φ est un isomorphisme de groupes l'ordre de HK est celui de $\mathrm{H} \times \mathrm{K}$, *i.e.* $|\mathrm{H}||\mathrm{K}|$.

Exercice 37

Soit G un groupe de centre $Z(\mathrm{G})$.

a) Montrer que $Z(\mathrm{G})$ est un sous-groupe distingué de G.

b) Montrer que si ${}^{\mathrm{G}}/_{Z(\mathrm{G})}$ est monogène (*i.e.* ${}^{\mathrm{G}}/_{Z(\mathrm{G})}$ est engendré par un seul élément), alors G est abélien.

Solution 37

a) Le centre de G est un sous-groupe de G. En effet si $x \in Z(\mathrm{G})$ et $y \in Z(\mathrm{G})$, alors $y^{-1} \in Z(\mathrm{G})$ et pour tout élément g de G on a $xy^{-1}g = xgy^{-1} = gxy^{-1}$ ce qui implique que xy^{-1} appartient à $Z(\mathrm{G})$.
Par ailleurs soit $g \in \mathrm{G}$ et soit $c \in Z(\mathrm{G})$. Comme c commute avec tous les éléments de G nous avons

$$gcg^{-1} = cgg^{-1} = c.$$

Donc $gZ(\mathrm{G})g^{-1} = Z(\mathrm{G})$ et $Z(\mathrm{G})$ est un sous-groupe distingué dans G.

b) Si $\mathrm{G} = Z(\mathrm{G})$, alors G est abélien. Si $\mathrm{G} \neq Z(\mathrm{G})$ et si ${}^{\mathrm{G}}/_{Z(\mathrm{G})}$ est monogène non trivial, alors il existe un élément x de G tel que $x \notin Z(\mathrm{G})$ et ${}^{\mathrm{G}}/_{Z(\mathrm{G})} = \langle xZ(\mathrm{G})\rangle$. Soit y dans G. Ou bien $y \in Z(\mathrm{G})$ et $xy = yx$. Ou bien $y \notin Z(\mathrm{G})$ et il existe $n \in \mathbb{N}$ tel que $y \in (xZ(\mathrm{G}))^n = x^nZ(\mathrm{G})$, autrement dit $y = x^nc$ avec $c \in Z(\mathrm{G})$. Dans ce cas $xy = xx^nc = x^ncx = yx$. Ainsi x commute avec tous les éléments de G, *i.e.* $x \in Z(\mathrm{G})$: contradiction. Ainsi $\mathrm{G} = Z(\mathrm{G})$ et G est abélien.

Exercice 38

On note $\mathbb{H}_8$ le sous-groupe de $\mathrm{GL}(2,\mathbb{C})$, appelé *groupe des quaternions* engendré par les trois matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad K = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

1. Calculer l'ordre de $\mathbb{H}_8$.
2. Exhiber les sous-groupes de $\mathbb{H}_8$.
3. Exhiber les sous-groupes distingués de $\mathbb{H}_8$.
4. Est-il isomorphe au groupe diédral D_8 ?

Solution 38

1. On vérifie que

$$I^2 = J^2 = K^2 = -\mathrm{id} \qquad\qquad IJ = K.$$

Par conséquent le groupe des quaternions est

$$\mathbb{H}_8 = \{\mathrm{id},\, -\mathrm{id},\, I,\, -I,\, J,\, -J,\, K,\, -K\}.$$

En particulier il est d'ordre 8.

2. D'après le théorème de Lagrange les sous-groupes propres de $\mathbb{H}_8$ sont d'ordre 2 ou 4. Il y a un seul sous-groupe d'ordre 2 : $\langle -\mathrm{id}\rangle$ et trois sous-groupes d'ordre 4 : $\langle I\rangle$, $\langle J\rangle$, $\langle K\rangle$.
3. Tous les sous-groupes de $\mathbb{H}_8$ sont distingués.
4. Le groupe diédral D_8 compte 5 éléments d'ordre 2 donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.

Exercice 39

Soit Q_8 le groupe des matrices 2×2 inversibles engendré par $\begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$ et $\begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$. Ce groupe est appelé le groupe des quaternions.

a) Quel est l'ordre de Q_8 ?

b) Montrer que Q_8 n'a qu'un élément d'ordre 2.

c) Quel est le centre de Q_8 ?

d) Montrer que tous les sous-groupes de Q_8 sont distingués.

e) Peut-on trouver un isomorphisme entre Q_8 et un produit semi-direct de $\mathbb{Z}/4\mathbb{Z}$ avec $\mathbb{Z}/2\mathbb{Z}$?

Solution 39

Posons $\mathcal{I} = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$, $\mathcal{J} = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$, $\mathcal{K} = \mathcal{I}\mathcal{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

a) On vérifie que Id est l'élément neutre,

$$-\mathrm{Id}M = -M \quad \forall M \in \{\mathcal{I}, \mathcal{J}, \mathcal{K}\} \qquad \mathcal{I}^2 = \mathcal{J}^2 = \mathcal{K}^2 = -\mathrm{Id}$$
$$\mathcal{I}\mathcal{J} = \mathcal{K},\ \mathcal{J}\mathcal{K} = \mathcal{I},\ \mathcal{K}\mathcal{I} = \mathcal{J} \qquad \mathcal{J}\mathcal{I} = -\mathcal{K},\ \mathcal{K}\mathcal{J} = -\mathcal{I},\ \mathcal{I}\mathcal{K} = -\mathcal{J}$$

Il en résulte que Q_8 contient 8 élements.

b) D'après ce qui précède l'unique élément d'ordre 2 est $-\mathrm{Id}$.

c) D'après ce qui précède le centre de Q_8 est $\{\mathrm{Id}, -\mathrm{Id}\}$.

d) Les sous-groupes de Q_8 sont le groupe trivial, le centre de Q_8 et

$$\langle \mathcal{I} \rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{I}, -\mathcal{I}\} \qquad \langle \mathcal{J} \rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{J}, -\mathcal{J}\} \qquad \langle \mathcal{K} \rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{K}, -\mathcal{K}\}$$

e) Les groupes $\langle \mathcal{I} \rangle$, $\langle \mathcal{J} \rangle$ et $\langle \mathcal{K} \rangle$ sont tous trois cycliques d'ordre 4 donc isomorphes à $\mathbb{Z}/4\mathbb{Z}$ mais aucun d'entre eux ne peut être un facteur semi-direct de Q_8 car l'autre facteur serait d'ordre 2 et d'intersection réduite à $\{\mathrm{Id}\}$ avec le facteur d'ordre 4. Or tous ces sous-groupes d'ordre 4 contiennent le sous-groupe d'ordre 2. Par conséquent Q_8 ne peut s'obtenir comme produit semi-direct de deux de ses sous-groupes propres.

Exercice 40

Soit G un groupe d'ordre 55 possédant deux sous-groupes distingués d'ordre 5 et 11 respectivement. Montrer que G est isomorphe à $\mathbb{Z}/55\mathbb{Z}$.

Solution 40

Si H et K sont d'ordre respectif 5 et 11, alors $\mathrm{H} \cap \mathrm{K} = \{e\}$ (en effet tous les éléments de $\mathrm{H} \setminus \{e\}$ sont d'ordre 5 et tous les éléments de $\mathrm{K} \setminus \{e\}$ sont d'ordre 11.

L'exercice 1 assure que HK est un sous-groupe de G d'ordre $5 \times 11 = 55$ qui est l'ordre de G. Il en résulte que $\mathrm{G} = \mathrm{HK}$. Alors HK est isomorphe à $\mathrm{H} \times \mathrm{K}$. Par suite G est isomorphe à $\mathrm{H} \times \mathrm{K}$. Or H est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ et K est isomorphe à $\mathbb{Z}/11\mathbb{Z}$ donc G est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} = \mathbb{Z}/55\mathbb{Z}$ (théorème chinois).

Exercice 41

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
$$E^{\mathrm{G}} = \{x \in E \mid \forall g \in \mathrm{G},\ g \cdot x = x\}.$$
Montrer que $|E^{\mathrm{G}}| = |E| \bmod p$.
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 $x_1 x_2 \dots x_p = e$.
3. Soit H un groupe fini d'ordre n. Soit $m \in \mathbb{N}^*$ tel que pour tout $x \in \mathrm{H}$ on ait $x^m = e$. Montrer que n divise une puissance de m.

Solution 41

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 ω_1, ω_2, ..., ω_r les orbites de E de cardinal strictement supérieur à 1. Si x_i est un élément de ω_i, alors $|\omega_i| = [\mathrm{G} : \mathrm{Stab}_{\mathrm{G}}(x_i)]$, c'est donc une puissance de p. Il résulte de l'équation aux classes que

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

2. Soit $(x_1, x_2, \ldots, x_p)$ un élément de E. Nous avons $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \ldots x_p x_1 = e$, *i.e.* $(x_2, x_3, \ldots, x_p, x_1)$ appartient à E. Notons c le cycle $(1\ 2\ \ldots\ p)$ 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

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

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 $|E| \equiv |E^{\mathrm{K}}| \mod p$. Le cardinal de E est n^{p-1} (en effet on peut choisir x_1, x_2, ..., x_{p-1} quelconques, x_p est alors déterminé de manière unique). Comme p divise n, $|E^{\mathrm{K}}|$ est nul modulo p. Or les éléments de E^{K} sont justement les p-uplets $(x, x, \ldots, x)$ avec $x^p = e$. Notons que E^{K} contient le p-uplet $(e, e, \ldots, e)$; 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 $x \in \mathrm{H}$ d'ordre p. Or par hypothèse $x^m = e$ donc p divise m.

Exercice 42

Soit G un groupe fini. Soit p le plus petit nombre premier divisant $|\mathrm{G}|$. 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 G/H par $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ pour tout $h \in \mathrm{H}$ et pour tout $a \in \mathrm{G}$.
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 $\geqslant p$.

c) Conclure.

Solution 42

a) On peut vérifier que $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ est bien définie : si $a\mathrm{H} = b\mathrm{H}$, alors $(ha)\mathrm{H} = (hb)\mathrm{H}$ donc $h \cdot (a\mathrm{H})$ 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

$$\begin{aligned} \mathrm{G}_{a\mathrm{H}} &= \big\{h \in \mathrm{H} \,|\, h \cdot (a\mathrm{H}) = a\mathrm{H}\big\} \\ &= \big\{h \in \mathrm{H} \,|\, (ha)\mathrm{H} = a\mathrm{H}\big\} \\ &= \big\{h \in \mathrm{H} \,|\, a^{-1}ha \in \mathrm{H}\big\} \\ &= \big\{h \in \mathrm{H} \,|\, h \in a\mathrm{H}a^{-1}\big\} \\ &= \mathrm{H} \cap a\mathrm{H}a^{-1}. \end{aligned}$$

L'orbite de H est réduite à H :

$$\mathcal{O}_{\mathrm{H}} = \big\{h \cdot \mathrm{H} \,|\, h \in \mathrm{H}\big\} = \big\{h\mathrm{H} \,|\, h \in \mathrm{H}\big\} = \mathrm{H}.$$

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 $a \in \mathrm{G}$ et $h \in \mathrm{H}$ 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 $\geqslant 2$ de $|\mathrm{G}|$.

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 ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| \geqslant p+1$: contradiction avec le fait que $\underbrace{[\mathrm{G}:\mathrm{H}]}_{\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right|} = p$.

Exercice 43

Soit E un espace vectoriel de dimension finie n sur un corps $\Bbbk$.

a) Faisons opérer le groupe linéaire $\mathrm{G} = \mathrm{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par $g \cdot F := g(F)$ pour tout $g \in \mathrm{G}$ et tout sous-espace F de E. Quelles sont les orbites pour cette action ?

b) On prend $\Bbbk = {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}$ et $n = 5$. Combien E possède-t-il de sous-espaces vectoriels de dimension 3 ?

Solution 43

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 $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ 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 $d = 0, 1, \ldots, n$.

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 $\mathrm{GL}(E)$ ou encore l'ordre de $\mathrm{GL}(E)$ divisé par celui du stabilisateur S de F. Le cardinal de $\mathrm{GL}(E)$ 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 $A \in \mathrm{GL}(3, \mathbb{F}_7)$, $B \in \mathrm{M}_{3,2}(\mathbb{F}_7)$ et $C \in \mathrm{GL}(2, \mathbb{F}_7)$. 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

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

Exercice 44

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 $g \in \mathrm{G}$ 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 $\mathrm{G} = \left(\mathbb{Z}/_{3\mathbb{Z}}, +\right)$ et $X = \left(\mathbb{Z}/_{13\mathbb{Z}}, +\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

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

Solution 44

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 $f(\overline{1})$) 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 $\left(\mathbb{Z}/_{13\mathbb{Z}}\right)^\times$ sur $\mathrm{Aut}(X)$) 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 45

Soit E un espace euclidien. On fait opérer le groupe orthogonal $\mathrm{O}(E)$ de E sur l'ensemble des sous-espaces vectoriels de E.

a) Quelles sont les orbites pour cette action ?

b) Donner un énoncé analogue pour les espaces hermitiens.

c) Y a-t-il un énoncé analogue pour le groupe orthogonal $\mathrm{O}(q)$ d'un espace vectoriel de dimension finie muni d'une forme quadratique non dégénérée q ?

Solution 45

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 orthonormée $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base orthonormée $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base orthonormée $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base orthonormée $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ 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 $d = 0, 1, \ldots, n$.

b) Idem en remplaçant le groupe orthogonal de E par le groupe unitaire de E.

c) Il est clair que si F est un sous-espace une condition nécessaire pour qu'un autre sous-espace G soit dans l'orbite de F est que les restrictions de q à F et G soient des formes quadratiques isomorphes (ce qui entraîne en particulier $\dim F = \dim G$ mais n'est pas équivalent à cette condition. Cette condition est en fait suffisante mais c'est un énoncé difficile, le théorème de WITT ([**?**]).

Exercice 46

Soit G un groupe. Soit g un élément de G. On appelle *centralisateur* de g l'ensemble G_g des éléments h de G tels que $hg = gh$.

a) Montrer que G_g est un sous-groupe de G. Est-il toujours distingué ?

b) Supposons que G soit fini. Soit C la classe de conjugaison de g. Trouver une relation entre $|\mathrm{G}|$, $|C|$ et $|\mathrm{G}_g|$.

Solution 46

a) Il est immédiat que G_g est un sous-groupe de G mais il n'est pas toujours distingué : par exemple dans $\mathcal{S}_3$ le centralisateur d'une transposition τ n'est pas distingué dans $\mathcal{S}_3$.

b) La groupe G opère par conjugaison sur lui-même. Par définition C est l'orbite de g et G_{g_0} son stabilisateur d'où
$$|\mathrm{G}| = |C| \cdot |\mathrm{G}_g|.$$

Exercice 47

Soit G un groupe opérant sur un ensemble X. Si (g, x) appartient à $\mathrm{G} \times X$ quelle relation peut-on écrire entre $\mathrm{Stab}(x)$ et $\mathrm{Stab}(g \cdot x)$?

Solution 47

Nous avons $\mathrm{Stab}(g \cdot x) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

Exercice 48

Soit G un groupe d'ordre 33 agissant sur un ensemble X de cardinal 19. Montrer qu'il existe une orbite de cardinal 1.

Solution 48

Utiliser la formule des classes.

Exercice 49

Pour chaque polyèdre régulier et convexe $\mathcal{P}$ d'un espace euclidien $\mathcal{E}$ de dimension 3 déterminer le nombre d'isométries de $\mathcal{E}$ préservant $\mathcal{P}$.

Solution 49

Le groupe $\mathrm{Isom}(\mathcal{P})$ agit transitivement sur $\mathcal{P}$; il suffit donc de déterminer l'ordre du stabilisateur d'un sommet de $\mathcal{P}$.

Exercice 50

1. Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble
$$E = \big\{(g, x) \in \mathrm{G} \times X \mid g \cdot x = x\big\},$$
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 50

1. Désignons par $\mathrm{Fix}(g) = \big\{x \in X \mid g \cdot x = x\big\}$ 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 $g \in \mathrm{G}$ tel que $y = g \cdot x$. Soit $w \in \mathrm{G}_x$, 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 $g\mathrm{G}_x g^{-1} \subset \mathrm{G}_y$. Un raisonnement analogue conduit à $\mathrm{G}_y \subset g\mathrm{G}_x g^{-1}$. Il s'en suit que $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$.
   - ◇ D'après ce qui précède $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$ donc $|\mathrm{G}_y| = |\mathrm{G}_x|$ et
     $$\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = \sum_{y \in \mathcal{O}_x} |\mathrm{G}_x| = |\mathrm{G}_x| \sum_{y \in \mathcal{O}_x} 1 = |\mathrm{G}_x|\,|\mathcal{O}_x|.$$
     Or l'application
     $$\mathrm{G}/\mathrm{G}_x \to \mathcal{O}_x, \qquad \overline{g} \mapsto g \cdot x$$
     est bien définie et est une bijection ; par suite $\left|\mathrm{G}/\mathrm{G}_x\right| = |\mathcal{O}_x|$, *i.e.* $|\mathrm{G}| = |\mathcal{O}_x|\,|\mathrm{G}_x|$. Ainsi $\displaystyle\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$.

◇ Nous avons

$$\sum_{x\in X} |\mathrm{G}_x| = \sum_{\mathcal{O}_x\subset\Omega}\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y|$$

où $\Omega = \{\mathcal{O}_x \,|\, x\in X\}$ est l'ensemble des orbites de l'action de G sur X. D'après b) $\displaystyle\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$ d'où

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

Finalement

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

◇ D'une part

$$\begin{aligned} E &= \{(g,x)\in \mathrm{G}\times X \,|\, g\cdot x = x\} \\ &= \{(g,x)\in \mathrm{G}\times X \,|\, x\in \mathrm{Fix}(g)\} \\ &= \Big(\{g_1\}\times\mathrm{Fix}(g_1)\Big)\cup\Big(\{g_2\}\times\mathrm{Fix}(g_2)\Big)\cup\ldots\cup\Big(\{g_p\}\times\mathrm{Fix}(g_p)\Big) \end{aligned}$$

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

D'autre part

$$\begin{aligned} E &= \{(g,x)\in \mathrm{G}\times X \,|\, g\cdot x = x\} \\ &= \{(g,x)\in \mathrm{G}\times X \,|\, g\in \mathrm{G}_x\} \\ &= \Big(\mathrm{G}_{x_1}\times\{x_1\}\Big)\cup\Big(\mathrm{G}_{x_2}\times\{x_2\}\Big)\cup\ldots\cup\Big(\mathrm{G}_{x_q}\times\{x_q\}\Big) \end{aligned}$$

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

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

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 $\mathrm{G} = \mathcal{S}_n$ agit (via l'action évidente) sur $X = \big\{1,\,2,\,\ldots,\,n\big\}$, 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, …, 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 $\mathrm{G} = \mathrm{D}_{18}$ des isométries d'un polygône régulier à neuf côtés. Ce groupe G est donc un sous-groupe de $\mathrm{SO}(2,\mathbb{R})$, il est d'ordre 18 et ses éléments sont les suivants

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

   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.

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

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

- ◇ Si $g = \mathrm{id}$, alors $\mathrm{Fix}(g) = X$.
- ◇ Si $g \in \{r, r^2, r^4, r^5, r^7, r^8\}$, 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 $\mathrm{Fix}(g) = \emptyset$.
- ◇ Si $g \in \{r^3, r^6\}$, 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 $\mathrm{Fix}(g) = \emptyset$.
- ◇ 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

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

Enfin le cardinal de X est

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

On en déduit que

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

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

Exercice 51

Montrer que nous avons les isomorphismes suivants

$$\mathrm{PGL}(2, \mathbb{F}_2) \simeq \mathcal{S}_3, \qquad \mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathcal{S}_4, \qquad \mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4, \qquad \mathrm{PGL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5.$$

Solution 51

Le groupe $\mathrm{PGL}(n, \mathbb{F}_q)$ agit fidèlement sur les droites de $\mathbb{F}_q^n$.

Exercice 52

Soit $\Bbbk$ un corps commutatif. Considérons l'action du groupe $\mathrm{GL}(m, \Bbbk) \times \mathrm{GL}(n, \Bbbk)$ sur $\mathrm{M}_{m,n}(\Bbbk)$ définie par $\big((P,Q), M\big) \mapsto PMQ^{-1}$.

Déterminer le nombre d'orbites de cette action.

Solution 52

Il s'agit de classer les matrices à équivalence près. On en déduit qu'il y a $\min(m, n) + 1$ orbites.

Exercice 53

Soit $\Bbbk$ un corps commutatif. Considérons l'action de $\mathrm{GL}(n, \Bbbk)$ sur $\mathrm{Sym}(n, \Bbbk)$ définie par

$$(P, S) \mapsto PS{}^{\mathrm{t}}P$$

a) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{C}$.
b) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{R}$.
c) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{F}_p$ lorsque p désigne un nombre premier impair.

Solution 53

Il s'agit de classer les formes bilinéaires sur $\Bbbk^n$.

— Si $\Bbbk = \mathbb{C}$, alors il y a $n + 1$ orbites.
— Si $\Bbbk = \mathbb{R}$, alors il y a $\frac{(n+2)(n+1)}{2}$ orbites.
— Si $\Bbbk = \mathbb{F}_p$, alors il y a $2n + 1$ orbites.

Exercice 54

Soit G un groupe d'ordre $n \in \mathbb{N}^*$ et soit $\Bbbk$ un corps commutatif. Montrer qu'il existe un morphisme de groupes injectif de G dans $\mathrm{GL}(n, \Bbbk)$.

Solution 54

Utiliser le théorème de Cayley.

Exercice 55

Soit G un groupe d'ordre $2m$ avec $m \in \mathbb{N}^*$ impair. Montrer que G admet un sous-groupe d'indice 2.

Solution 55

Utiliser le théorème de Cayley.

Exercice 56

Déterminer les groupes finis admettant exactement deux classes de conjugaison.

Solution 56

Avec la formule des classes on trouve $\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 57

Déterminer les groupes finis admettant exactement trois classes de conjugaison.

Solution 57

La formule des classes assure qu'il existe un couple (a, b) dans $\mathbb{N}^2$ tel que $1 \leqslant b \leqslant a \leqslant |\mathrm{G}|$ et

$$1 = \frac{1}{|\mathrm{G}|} + \frac{1}{a} + \frac{1}{b}.$$

Nous en déduisons que $1 \leqslant b \leqslant 3$ puis en étudiant les différents cas nous obtenons que $\mathrm{Card}(\mathrm{G}) \leqslant 6$. Finalement nous obtenons que $\mathrm{G} \simeq \mathbb{Z}/3\mathbb{Z}$ ou $\mathrm{G} \simeq \mathcal{S}_3$.

Exercice 58

Soit G un groupe d'ordre p^n où n appartient à $\mathbb{N}^*$ et p est un nombre premier. Montrer que le centre de G n'est pas trivial.

Solution 58

Faire agir G sur lui-même et utiliser la formule des classes.

Exercice 59

Soit G un groupe d'ordre infini. Supposons que G admette un sous-groupe propre H d'indice fini. Montrer que G n'est pas simple.

Solution 59

Faire agir G sur G/H par translation des classes.

Exercice 60

Soit G un groupe fini d'ordre $n \geqslant 2$. Soit p le plus petit facteur premier de n. Montrer que si H est un sous-groupe de G d'ordre p alors H est central.

Solution 60

Faire agir G sur H par conjugaison. Étudier le cardinal de chaque orbite pour obtenir qu'elles sont des singletons.

Exercice 61

Soit G un groupe opérant sur un ensemble E. On note pour $g \in \mathrm{G}$ et $x \in E$ l'action de g sur x par : $g \cdot x$.

1. Montrer que pour tout x dans le E le stabilisateur

$$\mathrm{Stab}_{\mathrm{G}}(x) = \mathrm{G}_x = \big\{g \in \mathrm{G} \,|\, g \cdot x = x\big\}$$

de x est un sous-groupe de G.
Soit maintenant $n \in \mathbb{N}$, $n \geqslant 2$. Notons G le groupe orthogonal $(\mathrm{O}(n, \mathbb{R}), \circ)$. Posons

$$\forall\, f \in \mathrm{G},\ \forall\, v \in \mathbb{R}^n \qquad f \cdot v = f(v).$$

Désignons par $\mathcal{C} = (e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$.

2. Montrer que

$$\mathrm{G} \times \mathbb{R}^n \to \mathbb{R}^n \qquad\qquad (f, v) \mapsto f \cdot v$$

définit une action du groupe G sur l'ensemble $\mathbb{R}^n$.

3. Déterminer l'orbite
$$\mathcal{O}_v^{\mathrm{G}} = \big\{f \cdot v \,|\, f \in \mathrm{G}\big\}$$
d'un élément v de $\mathbb{R}^n$ sous l'action de G.

4. Montrer que f appartient à G_{e_1} si et seulement si la matrice représentative de f dans $\mathcal{C}$ est du type

$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$

où P désigne un élément de $\mathrm{O}(n-1, \mathbb{R})$.

5. En déduire que $\mathrm{G}_{e_1} \simeq \mathrm{O}(n-1, \mathbb{R})$ en explicitant un isomorphisme entre $\mathrm{O}(n-1, \mathbb{R})$ et G_{e_1}.
6. Soit $x \in \mathbb{R}^n \smallsetminus \{0\}$. Donner un isomorphisme de groupes $\phi_x \colon \mathrm{G}_x \xrightarrow{\simeq} \mathrm{G}_{e_1}$.
7. Pour quels $x \in \mathbb{R}^n$ a-t-on $\mathrm{G}_x \triangleleft \mathrm{O}(n, \mathbb{R})$?
8. Soit $x \in \mathbb{R}^n \smallsetminus \{0\}$. Nous restreignons l'action de G sur $\mathbb{R}^n$ à celle de G_x. Donner l'orbite

$$\mathcal{O}_v^{\mathrm{G}_x} = \big\{f \cdot v \,|\, f \in \mathrm{G}_x\big\}$$

d'un élément v de $\mathbb{R}^n$ sous cette action (peut-être s'aider d'un dessin).

Solution 61

1. Soit x dans E. Par définition d'une action $e \cdot x = x$ ce qui conduit à $e \in \mathrm{G}_x$.
Si g et g' appartiennent à G_x nous avons

$$(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$$

donc gg' appartient à G_x.
Enfin si g appartient à G_x, alors $x = g \cdot x$ et en faisant agir g^{-1} de part et d'autre de l'égalité nous obtenons
$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$
ce qui montre que g^{-1} appartient à G_x.
En conclusion G_x est un sous-groupe de G.

2. Soit v dans $\mathbb{R}^n$. Nous avons
$$\mathrm{id}_{\mathbb{R}^n} \cdot v = \mathrm{id}_{\mathbb{R}^n}(v) = v$$
et si f, g appartiennent à $\mathrm{O}(n, \mathbb{R})$

$$(f \circ g) \cdot v = (f \circ g)(v) = f(g(v)) = f \cdot g(v) = f \cdot (g \cdot v).$$

3. Soit v dans $\mathbb{R}^n$.
Si $v = 0$, quel que soit $f \in \mathrm{O}(n, \mathbb{R})$ $f(v) = 0$ et

$$\mathcal{O}_0^{\mathrm{G}} = \big\{f \cdot 0 \,|\, f \in \mathrm{G}\big\} = \{0\}.$$

Si $v \neq 0$, alors du fait que les éléments $f \in \mathrm{O}(n, \mathbb{R})$ conservent la norme pour le produit scalaire standard de $\mathbb{R}^n$ nous avons $||f(v)|| = ||v||$ et donc $\mathcal{O}_v^{\mathrm{G}}$ est contenue dans la sphère $S(0, ||v||)$ de centre 0 et de rayon $||v||$. Réciproquement soit u dans $\mathbb{R}^n$ tel que $||v|| = ||u||$, soient $\mathcal{B}_u = \left(\frac{u}{||u||}, u_2, u_2, \ldots u_n\right)$ et $\mathcal{B}_v = \left(\frac{v}{||v||}, v_2, v_2, \ldots v_n\right)$ deux bases orthonormées de $\mathbb{R}^n$ (on peut compléter par le procédé de Gram-Schmidt un vecteur de norme 1 en une base orthonormée en dimension finie) et soit f l'application linéaire qui transforme $\mathcal{B}_v$ en $\mathcal{B}_u$. Puisque $\mathcal{B}_v$ et $\mathcal{B}_u$ sont deux bases orthonormées, f appartient à $\mathrm{O}(n, \mathbb{R})$. De plus $f\left(\frac{v}{||v||}\right) = \frac{u}{||u||}$ et $||u|| = ||v||$ entraînent $f(v) = u$. Finalement u appartient à $\mathcal{O}_v^{\mathrm{G}}$ et $\mathcal{O}_v^{\mathrm{G}} = S(0, ||v||)$ si $v \neq 0$.

4. Si f appartient à G_{e_1}, alors $f(e_1) = e_1$ et donc la première colonne de la matrice M représentant f dans la base canonique est : $\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. D'autre part $f(e_1) = e_1$ étant orthogonal à $f(e_2)$, $f(e_3)$, ..., $f(e_n)$ puisque f préserve le produit scalaire la première ligne de M est $(1\ 0\ 0\ \ldots\ 0)$. Par suite $M = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$. Puisque ${}^{\mathrm{t}}MM = \mathrm{id}_n$ nécessairement ${}^{\mathrm{t}}PP = \mathrm{id}_{n-1}$; anisi P appartient à $\mathrm{O}(n-1, \mathbb{R})$.
   Réciproquement si
   $$M = \mathrm{mat}(f, \mathcal{C}_n) = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$
   avec P dans $\mathrm{O}(n-1, \mathbb{R})$ nous avons bien : f appartient à $\mathrm{O}(n-1, \mathbb{R})$ (car ${}^{\mathrm{t}}MM = \begin{pmatrix} 1 & 0 \\ 0 & {}^{\mathrm{t}}PP \end{pmatrix} = \mathrm{id}_n$) et $f(e_1) = e_1$.

5. D'après 4. l'application $\Psi \colon \mathrm{O}(n-1, \mathbb{R}) \to \mathrm{G}_{e_1}$ définie par $\Psi(g) = f$ où $\mathrm{mat}(f, \mathcal{C}_n) = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$ et $\mathrm{mat}(g, \mathcal{C}_{n-1}) = P$ est bien à valeurs dans G_{e_1}. L'application Ψ est bien un morphisme de groupes : à la composition des applications correspond le produit des matrices. De plus g appartient à $\ker \Psi$ si et seulement si $\mathrm{mat}(g, \mathcal{C}_{n-1}) = \mathrm{id}_{n-1}$ si et seulement si $g = \mathrm{id}_{\mathbb{R}^{n-1}}$ ce qui prouve que Ψ est injective. La surjectivité de Ψ résulte directement de 4.

6. Soit x dans $\mathbb{R}^n \smallsetminus \{0\}$. Soit h dans $\mathrm{O}(n-1, \mathbb{R})$ tel que $h(e_1) = \frac{x}{||x||}$ (une telle application existe d'après 3.) Considérons
   $$\phi_x \colon \mathrm{G}_x \to \mathrm{G}_{e_1} \qquad\qquad f \mapsto h \circ f \circ h^{-1}.$$
   Notons que $\phi_x(f)$ appartient à $\mathrm{O}(n-1, \mathbb{R})$ puisque f et h appartiennent à $\mathrm{O}(n-1, \mathbb{R})$. D'autre part
   $$\phi_x(f)(e_1) = h(f(h^{-1}(e_1))) = h\left(f\left(\frac{x}{||x||}\right)\right) = h\left(\frac{x}{||x||}\right) = e_1$$
   ainsi ϕ_x est bien à valeurs dans G_{e_1}. Le fait que ϕ_x est un isomorphisme de groupes se vérifie directement.

7. Soit x dans $\mathbb{R}^n$.
   Si $x = 0$, alors $\mathrm{G}_0 = \mathrm{O}(n, \mathbb{R})$ et $\mathrm{G}_0 \lhd \mathrm{O}(n, \mathbb{R})$.
   Supposons $x \neq 0$. Soit f dans $\mathrm{G}_x \smallsetminus \{\mathrm{id}_{\mathbb{R}^n}\}$ (rappelons que d'après 3. G_x n'est pas réduit à $\mathrm{id}_{\mathbb{R}^n}$). Il existe y dans $\mathbb{R}^n$ tel que $||y|| = ||x||$ et $f(y) \neq y$. D'après 3. on peut alors construire h dans $\mathrm{O}(n, \mathbb{R})$ tel que $h(y) = x$. Alors $h(f(h^{-1}(x))) \neq x$ (en effet $h^{-1}(x) = y$ donc $f(h^{-1}(x)) = f(y) \neq y$). Ainsi G_x n'est pas distingué dans $\mathrm{O}(n, \mathbb{R})$.
   Finalement $\mathrm{G}_x \lhd \mathrm{O}(n, \mathbb{R})$ si et seulement si $x = 0$.

8. D'après 4. un élément f de G_x s'identifie à une application orthogonale de $\mathrm{O}(n-1, \mathbb{R})$ qui agit sur $x^\perp$ (en identifiant $\mathbb{R}^{n-1}$ et $x^\perp$) en laissant fixe la direction x. Écrivons v dans une base orthonormée commençant par $\frac{x}{||x||}$; on voit que l'image par f de v appartient à $S(0, ||v||)$ (car f conserve la norme) et aussi à l'hyperplan affine $\mathcal{H}$ de $\mathbb{R}^n$ orthogonal à x et passant par la projection orthogonale π de v sur la droite x (car f préserve la coordonnée suivant $\frac{x}{||x||}$). L'intersection de $S(0, ||v||)$ et de $\mathcal{H}$ est la sphère $S_{\mathcal{H}}$ de $\mathcal{H}$ centrée en $\pi(v)$ et de rayon $\mathrm{dist}(v, \mathrm{vect}(x))$. Réciproquement si u appartient à $S_{\mathcal{H}}$ la projection orthogonale $p(u)$ de u sur $x^\perp$ est de même norme que la projection orthogonale $p(v)$ de v sur $x^\perp$. Il existe donc une

application orthogonale f de $\mathrm{O}(n-1,\mathbb{R})$ qui envoie $p(u)$ sur $p(v)$ (nous avons identifié $\mathbb{R}^{n-1}$ et $x^{\perp}$). Nous étendons alors f à $\widetilde{f}$ sur $\mathbb{R}^n$ tout entier en imposant que $\widetilde{f}$ laisse fixe la direction x. L'application $\widetilde{f}$ appartient à G_x et envoie u sur v. Il s'en suit que $\mathcal{O}_v^{\mathrm{G}_x} = S_{\mathcal{H}}$.

Exercice 62

Soient G un p-groupe et H un sous-groupe non trivial distingué de G.

Montrer que $\mathrm{H} \cap Z(\mathrm{G})$ n'est pas réduit à l'élément neutre.

Solution 62

Le sous-groupe H de G étant distingué G agit par conjugaison sur H. Puisque G est un p-groupe H l'est aussi et les orbites non triviales de cette action sont de cardinal divisible par p. On en déduit que la réunion des orbites triviales, c'est-à-dire l'ensemble $\mathrm{H} \cap Z(\mathrm{G})$ des points fixes, est aussi de cardinal divisible par p. Comme il contient l'élément neutre il contient au moins p éléments et n'est donc pas réduit à l'élément neutre.

Exercice 63

1. Soit G un groupe fini. Soit H un sous-groupe strict de G. Montrer qu'il existe $x \in \mathrm{G}$ tel que la classe de conjugaison de x ne rencontre pas H.
2. Donner un contre-exemple si G n'est pas fini.

Solution 63

1. Soient x et g dans G. Nous avons $gxg^{-1} \in \mathrm{H} \Longleftrightarrow x \in g^{-1}\mathrm{H}g$. On est donc ramené à montrer que la réunion $\bigcup\limits_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ des conjugués de H n'est pas égale à G. Pour cela on va majorer le cardinal de $\bigcup\limits_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ et montrer que cette réunion contient strictement moins d'éléments que G. Notons que si g_1 et g_2 sont dans la même classe à gauche modulo H, *i.e.* s'il existe $h \in \mathrm{H}$ tel que $g_2 = g_1 h$, alors

$$g_2\mathrm{H}g_2^{-1} = g_1(h\mathrm{H}h^{-1})g_1^{-1} = g_1\mathrm{H}g_1^{-1}.$$

   Dans la réunion ci-dessus on peut donc prendre un système de représentants des classes à gauche modulo H. Soit g_1, g_2, …, g_k un tel système de représentants, $k = \frac{|\mathrm{G}|}{|\mathrm{H}|}$ étant l'indice de H dans G. Les conjugués de H ayant au moins l'élément neutre en commun il vient

$$\left|\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}\right| = \left|\bigcup_{i=1}^{k} g_i\mathrm{H}g_i^{-1}\right| \leqslant 1 + (|\mathrm{H}|-1)k = |\mathrm{G}| + 1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < |\mathrm{G}|$$

   car par hypothèse $|\mathrm{H}| < |\mathrm{G}|$ donc $1 < \frac{|\mathrm{G}|}{|\mathrm{H}|}$ et $1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < 0$.
2. Le résultat précédent ne s'étend pas à un groupe infini. Prenons par exemple $\mathrm{G} = \mathrm{GL}(n,\mathbb{C})$ et H le sous-groupe de G formé des matrices triangulaires supérieures inversibles. Toute matrice de G étant trigonalisable la classe de conjugaison de toute matrice de G rencontre H.

Exercice 64

Soit $\Bbbk = \mathbb{F}_q$ un corps fini de cardinal q. Considérons le groupe linéaire $\mathrm{GL}(n,\Bbbk)$ et son sous-groupe $\mathrm{SL}(n,\Bbbk)$.

a) Montrer que le centre de $\mathrm{GL}(n,\Bbbk)$ (respectivement de $\mathrm{SL}(n,\Bbbk)$) est constitué des matrices scalaires de ce groupe.

b) Notons $\mathrm{PGL}(n,\Bbbk)$ (respectivement $\mathrm{PSL}(n,\Bbbk)$) le quotient de $\mathrm{GL}(n,\Bbbk)$ (respectivement $\mathrm{SL}(n,\Bbbk)$) par son centre. Calculer les ordres de $\mathrm{SL}(n,\Bbbk)$, $\mathrm{PGL}(n,\Bbbk)$ et $\mathrm{PSL}(n,\Bbbk)$.
   Soit n un entier. Soit E le $\Bbbk$-espace vectoriel $\Bbbk^n$. Désignons par $\mathbb{P}(E)$ l'ensemble des droites vectorielles de $\Bbbk^n$ (espace projectif de dimension $n-1$).

c) Montrer qu'il existe un morphisme injectif Φ de $\mathrm{PGL}(n,\Bbbk)$ dans le groupe symétrique $\mathcal{S}_{\mathbb{P}(E)}$.
   Dans la suite on suppose que $n = 2$.

d) Montrer que $\mathbb{P}(E)$ est de cardinal $q+1$; on identifie Φ à un morphisme de $\mathrm{PGL}(2,\Bbbk)$ dans $\mathcal{S}_{q+1}$.

e) Supposons que $q = 2$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}(2,\mathbb{F}_2)$ et $\mathrm{PSL}(2,\mathbb{F}_2)$ sur $\mathcal{S}_3$.

f) Supposons que $q = 3$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2,\mathbb{F}_3)$ sur $\mathcal{S}_4$ et de $\mathrm{PSL}(2,\mathbb{F}_3)$ sur $\mathcal{A}_4$. Les groupes $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathrm{SL}(2,\mathbb{F}_3)$ sont-ils isomorphes ?

g) Supposons que $q = 4$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}(2,\mathbb{F}_4)$ et $\mathrm{PSL}(2,\mathbb{F}_4)$ sur $\mathcal{A}_5$.

h) Supposons que $q = 5$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2, \mathbb{F}_5)$ sur $\mathcal{S}_5$ et de $\mathrm{PSL}(2, \mathbb{F}_5)$ sur $\mathcal{A}_5$ (rappelons une conséquence non triviale de la simplicité des groupes alternés : tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$ pour $n \geqslant 5$).

Solution 64

a) Montrons plus généralement (sur un corps $\Bbbk$ quelconque) que si un endomorphisme f de $\Bbbk^n$ commute avec tous les endomorphismes de déterminant 1, alors f est une homothétie. Pour cela montrons que tout vecteur $v \neq 0$ de $\Bbbk^n$ est vecteur propre pour f. Complétons v en une base $(v, e_1, e_2, \ldots, e_{n-1})$ de $\Bbbk^n$. Soit M la matrice de f dans cette base. Alors M commute avec la matrice de Jordan J_n donc laisse stable le noyau de J_n qui est $\Bbbk \cdot v$. Ainsi v est bien vecteur propre pour f.

b) Nous avons
$$|\mathrm{GL}(n, \Bbbk)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}).$$
Par définition $\mathrm{SL}(n, \Bbbk)$ est le noyau du morphisme de groupes surjectif
$$\det \colon \mathrm{GL}(n, \Bbbk) \to \Bbbk^*;$$
son cardinal est celui de $\mathrm{GL}(n, \Bbbk)$ divisé par $q - 1$, soit
$$|\mathrm{SL}(n, \Bbbk)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-2})q^{n-1}.$$
De plus $\mathrm{PGL}(n, \Bbbk)$ est le quotient de $\mathrm{GL}(n, \Bbbk)$ par un groupe isomorphe à $\Bbbk^*$ (les matrices scalaires non nulles) donc $|\mathrm{PGL}(n, \Bbbk)| = |\mathrm{SL}(n, \Bbbk)|$.

Pour finir $|\mathrm{PSL}(n, \Bbbk)| = \frac{|\mathrm{SL}(n,\Bbbk)|}{|Z(\mathrm{SL}(n,\Bbbk))|}$ et $Z(\mathrm{SL}(n, \Bbbk)) = \{\lambda \mathrm{Id} \mid \lambda^n = 1\}$. Or il y a $\mathrm{pgcd}(n, q-1)$ racines $n$ièmes de l'unité dans un corps $\Bbbk$ de cardinal q [3] donc
$$|\mathrm{PSL}(n, \Bbbk)| = \frac{(q^n - 1)(q^n - q) \ldots (q^n - q^{n-2})q^{n-1}}{\mathrm{pgcd}(n, q-1)}.$$

c) Faisons opérer $\mathrm{PGL}(n, \Bbbk)$ sur l'ensemble $\mathbb{P}(E)$ des droites vectorielles de E par $\overline{g} \cdot D = g(D)$ où g appartient à $\mathrm{GL}(n, \Bbbk)$ et $\overline{g}$ est son image dans $\mathrm{PGL}(n, \Bbbk)$. Ceci est bien défini car si $\overline{g_1} = \overline{g_2}$, alors g_1 et g_2 sont proportionnels et $g_1(D) = g_2(D)$. L'opération est fidèle car les seuls éléments g de $\mathrm{GL}(n, \Bbbk)$ qui stabilisent toutes les droites sont les homothéties. Nous obtenons donc un morphisme injectif Φ de $\mathrm{PGL}(n, \Bbbk)$ dans $\mathcal{S}_{\mathbb{P}(E)}$.

d) Les droites vectorielles de E sont données par une équation $y = ax$ dans le plan, avec $a \neq 0$, ou par l'équation $x = 0$. Il y a donc $q + 1$ droites, *i.e.* $|\mathbb{P}(E)| = q + 1$.

e) D'après c) les groupes $\mathrm{PGL}(2, \mathbb{F}_2)$ et $\mathrm{PSL}(2, \mathbb{F}_2)$ coïncident et sont d'ordre 6. De plus $\mathcal{S}_3$ est d'ordre 6. Ainsi le morphisme injectif Φ est aussi surjectif d'où le résultat.

f) D'une part $|\mathrm{PGL}(2, \mathbb{F}_3)| = (3^2 - 1) \times 3 = 24$ d'autre part $|\mathcal{S}_4| = 24$. Ainsi Φ réalise un isomorphisme entre entre $\mathrm{PGL}(2, \mathbb{F}_3)$ et $\mathcal{S}_4$. Comme $\mathrm{pgcd}(2, 3 - 1) = 2$ le groupe $\mathrm{PSL}(2, \mathbb{F}_3)$ est, d'après c), un sous-groupe d'indice 2 de $\mathrm{PGL}(2, \mathbb{F}_3)$. Puisque le seul sous-groupe d'indice 2 de $\mathcal{S}_4$ est $\mathcal{A}_4$ [4] nous obtenons que Φ induit un isomorphisme entre $\mathrm{PSL}(2, \mathbb{F}_3)$ et $\mathcal{A}_4$.

Les groupes $\mathrm{PGL}(2, \mathbb{F}_3)$ et $\mathrm{SL}(2, \mathbb{F}_3)$ ne sont pas isomorphes. En effet $Z(\mathrm{SL}(2, \mathbb{F}_3))$ est d'ordre 2 alors que le centre de $\mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathcal{S}_4$ est trivial.

g) D'une part $|\mathrm{PGL}(2, \mathbb{F}_4)| = (4^2-1) \times 4 = 60$, d'autre part comme $\mathrm{pgcd}(2, 4-1) = 1$ nous avons $\mathrm{PGL}(2, \mathbb{F}_4) = \mathrm{PSL}(2, \mathbb{F}_4)$. Par suite Φ induit un des isomorphismes de $\mathrm{PGL}(2, \mathbb{F}_4)$ et $\mathrm{PSL}(2, \mathbb{F}_4)$ sur un sous-groupe d'indice 2 de $\mathcal{S}_5$ qui ne peut être que $\mathcal{A}_5$ [5].

h) L'ordre de $\mathrm{PGL}(2, \mathbb{F}_5)$ est $(5^2 - 1) \times 5 = 120$ donc Φ induit un isomorphisme de $\mathrm{PGL}(2, \mathbb{F}_5)$ sur un sous-groupe d'indice 6 de $\mathcal{S}_6$ lequel est isomorphe à $\mathcal{S}_5$ d'après le résultat rappelé. Étant donné que $\mathrm{pgcd}(2, 5 - 1) = 2$, le groupe $\mathrm{PSL}(2, \mathbb{F}_5)$ est un sous-groupe d'indice 2 de $\mathrm{PGL}(2, \mathbb{F}_5) \simeq \mathcal{S}_5$ et est donc isomorphe, via Φ, à $\mathcal{A}_5$.

Exercice 65

Donner des applications de l'équation aux classes.

3. En effet $\Bbbk^*$ est un groupe cyclique d'ordre $q - 1$. Nous sommes donc ramenés à compter le nombre de solutions x de $nx = 0$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$ ce qui donne le résultat.

4. En effet, dès que $m \geqslant 2$ le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

5. En effet, dès que $m \geqslant 2$ le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

Solution 65

Applications de l'équation aux classes : le centre d'un p-groupe n'est pas trivial, théorème de Wedderburn.

Exercice 66

Donner des applications de la formule de Burnside.

Solution 66

Applications de la formule de Burnside : petit théorème de Fermat, les colliers de Polya.

Exercice 67

Trouver un groupe fini $\mathrm{G} \neq \{e\}$ tel que le centre de G est $\{e\}$, le sous-groupe dérivé de G est G mais G n'est pas simple.

Solution 67

Considérons $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2$ où G_1 et G_2 sont deux groupes simples non abéliens, par exemple $\mathrm{G}_1 = \mathrm{G}_2 = \mathcal{A}_5$. Le groupe G n'est pas simple : il contient par exemple le sous-groupe distingué non trivial $\mathrm{G}_1 \times \{e\}$. De plus d'une part $Z(\mathrm{G}) = Z(\mathrm{G}_1) \times Z(\mathrm{G}_2)$, d'autre part $Z(\mathrm{G}_1) = Z(\mathrm{G}_2) = \{e\}$. Et enfin d'une part $[\mathrm{G}, \mathrm{G}] = [\mathrm{G}_1, \mathrm{G}_1] \times [\mathrm{G}_2, \mathrm{G}_2]$ et d'autre part $[\mathrm{G}_i, \mathrm{G}_i] = \mathrm{G}_i$ pour $i = 1, 2$.

Exercice 68

Soit D le groupe diédral d'ordre 8 (groupe des isométries du carré). Calculer le centre, le sous-groupe dérivé et l'abélianisé de D.

Soit $\mathbb{H}_8$ le groupe des quaternions d'ordre 8. Calculer le centre, le sous-groupe dérivé et l'abélianisé de $\mathbb{H}_8$.

Solution 68

Le centre $Z(\mathrm{D})$ de D est $\{\pm \mathrm{id}\}$. Puisque le quotient ${}^{\mathrm{D}}\!/_{Z(\mathrm{D})}$ est abélien (il est d'ordre 4) son sous-groupe dérivé est inclus dans $Z(\mathrm{D})$. Étant donné que D n'est pas abélien, le groupe dérivé de ${}^{\mathrm{D}}\!/_{Z(\mathrm{D})}$ ne peut pas être trivial et coïncide donc avec $Z(\mathrm{D})$. On peut vérifier que tout élément g de D satisfait $g^2 \in Z(\mathrm{D})$. Ainsi tous les éléments non triviaux de ${}^{\mathrm{D}}\!/_{Z(\mathrm{D})}$ sont d'ordre 2. Par suite ce groupe d'ordre 4 n'est pas cyclique ; il est donc isomorphe à $\left({}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\right)^2$.

Les règles de calcul dans $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ sont

$$ij = -ji = k, \qquad ki = -ik = j, \qquad jk = -kj = i, \qquad i^2 = j^2 = k^2 = -1.$$

Le centre $Z(\mathbb{H}_8)$ est donc réduit à $\{\pm 1\}$. Comme pour D nous en déduisons que le groupe dérivé de $\mathbb{H}_8$ est $Z(\mathbb{H}_8)$ et que l'abélianisé ${}^{\mathbb{H}_8}\!/_{Z(\mathbb{H}_8)}$ de $\mathbb{H}_8$ est isomorphe à $\left({}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\right)^2$.

Notons que D et $\mathbb{H}_8$ ne sont pas isomorphes pour autant : D possède 5 éléments d'ordre 2 alors que $\mathbb{H}_8$ n'en possède qu'un.

Exercice 69

Soit G un groupe fini tel que le quotient de G par son centre soit abélien. Le groupe G est-il toujours abélien ?

Solution 69

Non. Considérons par exemple un groupe non abélien G d'ordre 8 comme le groupe diédral. Son centre $Z(\mathrm{G})$ est non trivial car G est un 2-groupe. Par conséquent le quotient ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est d'ordre au plus 4 et ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est abélien.

Exercice 70

Quels sont les groupes finis G tels que tout élément g de G vérifie $g^2 = e$?

Solution 70

Un tel groupe G est abélien ; en effet si g et h sont deux éléments de G alors $g = g^{-1}$ et $h = h^{-1}$ mais aussi $(gh) = (gh)^{-1}$ soit $gh = h^{-1}g^{-1}$ ou encore $gh = hg$. Notons alors G additivement. Nous avons alors $2g = 0$ pour tout $g \in \mathrm{G}$. Le groupe G est alors isomorphe au groupe additif $\left({}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\right)^r$ pour un certain $r \in \mathbb{N}$. Réciproquement un tel groupe convient.

Exercice 71

Soit p un nombre premier, soit G un groupe d'ordre p^2. Montrer que G est abélien.

Solution 71

L'équation aux classes pour l'action de G sur lui-même par conjugaison assure que le centre $Z(\mathrm{G})$ de G n'est pas réduit à l'élément neutre. En faisons agir G sur lui-même par conjugaison

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, h) \mapsto hgh^{-1}.$$

Notons que g appartient à $Z(\mathrm{G})$ si et seulement si l'orbite $\mathcal{O}_g$ de g sous cette action est réduite à $\{g\}$. L'équation aux classes assure que

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|.$$

D'après le théorème de Lagrange $|\mathcal{O}_{g_i}|$ divise p donc

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|$$

conduit à

$$|\mathrm{G}| \equiv |Z(\mathrm{G})| \bmod p$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Mais e_G appartient à $Z(\mathrm{G})$ donc $|Z(\mathrm{G})| \geqslant p$. Par suite $Z(\mathrm{G})$ est de cardinal p ou p^2.

Si $|Z(\mathrm{G})| = p^2$, alors $\mathrm{G} = Z(\mathrm{G})$ est abélien.

Si $|Z(\mathrm{G})| = p$, alors ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est de cardinal p premier, ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est cyclique et G est, d'après a), abélien.

Exercice 72

Soit G un groupe. On note e l'élément neutre de G. Étant donnés deux sous-groupes A et B de G nous désignons par AB le sous-ensemble de G formé des éléments de G de la forme ab où a est dans A et b est dans B.

Considérons désormais deux sous-groupes H et K de G.

1. Montrer que HK = KH si et seulement si HK est un sous-groupe de G.
2. Montrer que si H est distingué dans G nous avons HK = KH (et donc HK est un sous-groupe de G).
3. Montrer que si H est distingué dans G l'application $\varphi\colon \mathrm{K} \to {}^{\mathrm{HK}}\!/_{\mathrm{H}}$ définie par $\varphi(k) = k\mathrm{H}$ réalise (par passage au quotient) un isomorphisme de ${}^{\mathrm{K}}\!/_{\mathrm{H} \cap \mathrm{K}}$ sur ${}^{\mathrm{HK}}\!/_{\mathrm{H}}$.
4. Montrer que si H et K sont distingués dans G et si $\mathrm{H} \cap \mathrm{K} = \{e\}$, l'application $\psi\colon \mathrm{H} \times \mathrm{K} \to \mathrm{HK}$ définie par $\psi((h,k)) = hk$ est un isomorphisme de groupes.

   Soit $\mathrm{SL}(2,\mathbb{Z})$ le groupe des matrices carrées de taille 2×2 à coefficients dans $\mathbb{Z}$ dont le déterminant est 1. Posons

   $$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad N = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

5. Déterminer l'ordre de M, l'ordre de N et l'ordre de MN dans $\mathrm{SL}(2,\mathbb{Z})$.
6. Soient H (resp. K) le sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ engendré par M (resp. par N). Montrer que HK n'est pas un groupe.

Solution 72

1. Supposons que HK soit un sous-groupe de G. Soit hk un élément de HK. Cet élément possède un inverse uv dans HK. On a donc $hk = (uv)^{-1} = v^{-1}u^{-1}$ qui est donc dans KH. Cela montre que HK est contenu dans KH. Par ailleurs soit kh un élément de KH. L'inverse de kh qui est $h^{-1}k^{-1}$ appartient à HK. Puisque HK est un sous-groupe de G, kh est donc aussi dans HK. D'où l'inclusion $\mathrm{KH} \subset \mathrm{HK}$, et l'égalité HK = KH.

   Réciproquement supposons HK = KH. D'abord $e \in \mathrm{HK}$ et si x est dans HK, il est clair que x^{-1} aussi. Considérons par ailleurs, deux éléments $u = ab$ et $v = cd$ dans HK. On a $bc = fg$ avec f dans H et g dans K. D'où $uv = (af)(gd) \in \mathrm{HK}$. Cela prouve que HK est un sous-groupe de G.

2. Soit hk un élément de HK. On a $hk = k(k^{-1}hk)$, ce qui prouve que hk appartient à KH (rappelons que H est distingué dans G). Par suite $\mathrm{HK} \subset \mathrm{KH}$.

   Réciproquement, soit kh dans KH. L'élément $khk^{-1} = h$ est dans H. D'où $kh = hk$ appartient à HK et $\mathrm{KH} \subset \mathrm{HK}$. D'où le résultat.

3. L'ensemble quotient HK/H est un groupe car H est distingué dans G (donc aussi dans HK) et φ est un morphisme de groupes (car $kk'\mathrm{H} = (k\mathrm{H})(k'\mathrm{H})$). Par ailleurs φ est surjective ; en effet, soit $a = hk\mathrm{H}$ un élément de HK/H : on a $a = k'h'\mathrm{H}$ où $k' \in \mathrm{K}$ et $h' \in \mathrm{H}$ (car KH = HK). D'où $a = k'\mathrm{H}$ et $\varphi(k') = a$. Enfin étant donné un élément k de K, on a $k\mathrm{H} = \mathrm{H}$ si et seulement si k appartient à H. Le théorème de factorisation des morphismes de groupes entraîne alors notre assertion.

4. Par définition l'application ψ est surjective. Elle est injective car $\mathrm{H} \cap \mathrm{K}$ est réduit à l'élément neutre de G. Tout revient à vérifier que ψ est un morphisme de groupes. Considérons pour cela deux éléments (h, k) et (h', k') de $\mathrm{H} \times \mathrm{K}$. Nous avons

$$\psi((h,k)(h',k')) = \psi((hh',kk')) = (hh')(kk')$$

   Par ailleurs tout élément de H commute avec tout élément de K ; en effet si $h \in \mathrm{H}$ et $k \in \mathrm{K}$, alors l'élément $hkh^{-1}k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K}$ (par hypothèse H et K sont distingués dans G). Il en résulte que $hkh^{-1}k^{-1} = e$ et que $hk = kh$. Par conséquent $\psi((h,k)(h',k')) = (hk)(h'k')$, c'est-à-dire $\psi((h,k)(h',k')) = \psi((h,k))\psi((h',k'))$.

5. Soit id la matrice identité de $\mathrm{SL}(2,\mathbb{Z})$. On vérifie que $M^2 \neq \mathrm{id}$ et les égalités $M^4 = \mathrm{id}$, et $N^3 = \mathrm{id}$. Il s'ensuit que l'ordre de M est 4 et celui de N est 3. Par ailleurs, pour tout entier $n \geqslant 0$ nous avons

$$(MN)^{2n} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \qquad (MN)^{2n+1} = \begin{pmatrix} -1 & -1-2n \\ 0 & -1 \end{pmatrix}$$

   Il en résulte que MN n'est pas d'ordre fini (MN est donc d'ordre infini).

6. Supposons que HK soit un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$; c'est alors un groupe fini (car par exemple l'application

$$\mathrm{H} \times \mathrm{K} \to \mathrm{HK}, \qquad (h,k) \mapsto hk$$

   est surjective). Mais cela conduit à une contradiction car MN appartient à HK et MN est d'ordre infini. D'où l'assertion.

Exercice 73

1. Soit G un groupe non abélien d'ordre 10. Montrer que G contient un élément d'ordre 5.
2. Montrer que G contient un sous-groupe distingué H d'ordre 5 et que tout élément $x \in \mathrm{G} \setminus \mathrm{H}$ est d'ordre deux (considérer le groupe quotient G/H).
3. Montrer que G est isomorphe au groupe diédral D_{10} (considérer l'ordre d'un élément xh).

Solution 73

1. On rappelle que dans un groupe fini G, l'ordre de tout élément est un diviseur du cardinal de G. Ainsi, si dans un groupe d'ordre 10 il n'y avait aucun élément d'ordre 5, il n'y aurait aucun élément g d'ordre 10 car sinon g^2 serait d'ordre 5, de sorte que tout élément $g \neq 1$ serait d'ordre 2 ce qui est impossible car 10 n'est pas une puissance de 2 [6].

2. Soit g un élément d'ordre 5 ; le sous-groupe H qu'il engendre est d'indice 2 et est donc distingué [7] dans G. Soit alors $x \in \mathrm{H}$. Dans le groupe quotient G/H, nous avons $(\overline{x})^2 = 1$ de sorte que x^2 appartient à H. Si nous avions $x^2 \neq 1$, alors x^2 serait d'ordre 5 et x d'ordre 10 ; le groupe G serait alors cyclique donc abélien.

6. Soit G un groupe dont tous les éléments non triviaux sont d'ordre 2 ; l'ordre de G est de la forme 2^n. En effet supposons, par récurrence, que si l'ordre de G est inférieur à r alors il est de la forme 2^n. La récurrence est vérifiée pour $r = 1$ et $r = 2$, supposons-la vraie jusqu'au rang r et traitons le cas $r+1$. Soit $g_1 \neq 1$ un élément de G qui engendre, par hypothèse, un sous-groupe d'ordre 2 qui est distingué dans G car $gg_1g^{-1} = g_1$. Considérons alors le groupe quotient $\mathrm{G}/\langle g_1 \rangle$ qui est d'ordre $\binom{r}{2}$ et dont tous les éléments sont d'ordre 2. Par récurrence $\binom{r}{2}$ est de la forme 2^n d'où le résultat

7. Si G est un groupe et si H est un sous-groupe d'indice 2 de G, alors H est distingué dans G.

3. Supposons pour commencer que G est non abélien. Soit $x \in \mathrm{H}$ de sorte que tout élément de G s'écrit de manière unique sous la forme $g^k x^i$ avec $0 \leqslant k < 5$ et $i = 0, 1$. Considérons alors l'application $f \colon \mathrm{G} \to \mathrm{D}_{10}$ qui envoie $g^k x^i$ sur $r^k \circ s^i$ où r est la rotation d'angle $\frac{2\pi}{5}$ et s la réflexion d'axe (Ox). Montrons que f est un morphisme de groupes, *i.e.* $f(g^k x^i g^{k'} x^{i'}) = r^k s^i r^{k'} s^{i'}$. Pour $i = 0$ ou $k' = 0$ le résultat découle de la définition. Dans le cas $i = i' = 1$ comme $(g^{k'} x)^2 = 1$ (resp. $(r^{k'} x)^2 = 1$), nous avons $g^k x g^{k'} x = g^{k-k'}$ (resp. $r^k s r^{k'} s = r^{k-k'}$) d'où le résultat. Si $i' = 0$ nous écrivons $g^k x g^{k'}$ (resp. $r^k s r^{k'}$) sous la forme $g^k x g^{k'} x x$ (resp. $r^k s r^{k'} s s$) et nous appliquons le calcul précédent.
   Nous obtenons ainsi un morphsime de G dans D_{10} qui est injectif par définition et qui réalise donc étant l'égalité des ordres de G et D_{10} un isomorphisme.
   Si G est abélien nous reprenons le raisonnement de 2. Si $x^2 \neq 1$, x est d'ordre 10 et G est cyclique. Si $x^2 = 1$, x est alors d'ordre 2. Considérons alors $y = xg$ et soit n tel que $y^n = x^n g^n = 1$ soit $x^{-n} = x^n = g^n$. Si n était impair, nous aurions $x \in \mathrm{H}$: impossible car H ne contient pas d'élément d'ordre 2. Ainsi n est pair et $g^n = 1$ soit 5 divise n et donc 10 divise n de sorte que y est d'ordre 10 d'où le résultat.

Exercice 74

Soit G un groupe fini d'ordre 21 opérant sur un ensemble fini E ayant n éléments.

1. Supposons que $n = 19$. Supposons aussi qu'il n'existe pas de point fixe dans E sous l'action de G. Combien y a-t-il d'orbites dans E ? Quel est le nombre d'éléments dans chacune de ces orbites ?
2. Supposons que $n = 11$. Montrer qu'il existe au moins un point fixe dans E sous l'action de G.
3. Soit n un entier > 11. Montrer qu'il existe un ensemble ayant n éléments sur lequel G opère sans point fixe.

Solution 74

1. L'équation aux classes s'écrit
$$n = a_1 + 3a_2 + 7a_3 + 21a_4$$
   où a_1 (resp. a_2, resp. a_3, resp. a_4) désigne le nombre de classes de cardinal 1 (resp. 3, resp. 7, resp. 21). Pour $n = 19$, l'entier a_4 est nécessairement nul et si par ailleurs on impose a_1 nul alors l'équation aux classes se réécrit $3a_2 + 7a_3 = 19$. Par conséquent $a_3 = 1$ et $a_2 = 4$; autrement dit il y a cinq orbites dont une de cardinal 7 et quatre de cardinal 3.
2. L'équation aux classes s'écrit encore
$$n = a_1 + 3a_2 + 7a_3 + 21a_4$$
   où a_1 (resp. a_2, resp. a_3, resp. a_4) désigne le nombre de classes de cardinal 1 (resp. 3, resp. 7, resp. 21). Pour $n = 11$, l'entier a_4 est nécessairement nul. Par ailleurs l'équation $3a_2 + 7a_3 = 11$ n'a pas de solution entière de sorte que a_1 ne peut pas être nul ; autrement dit il existe au moins un point fixe dans E sous l'action de G.
3. Il suffit de montrer que tout entier $n \geqslant 12$ peut s'écrire $3a + 7b$ avec $a, b \geqslant 0$. Or c'est vrai pour 12, 13 et 14 donc pour tout entier plus grand en ajoutant un multiple de 3.

2 Groupe des permutations

Exercice 75

Dans le groupe symétrique $\mathcal{S}_5$, combien y a-t-il de 5-cycles distincts ? de 4-cycles distincts ?

Solution 75

L'ensemble des 5-cycles est en bijection avec les 5-uplets (a, b, c, d, e) d'éléments distincts modulo permutation circulaire, c'est-à-dire :
$$(a, b, c, d, e) \sim (b, c, d, e, a) \sim (c, d, e, a, b) \sim (d, e, a, b, c) \sim (e, a, b, c, d)$$
de sorte que chaque classe est constituée de 5 éléments. On obtient alors $\binom{5}{5}(5-1)!$ tels cycles, où $\binom{5}{5}$ est le coefficient binomial.

Pour les 4-cycles le même raisonnement donne $\binom{4}{5}3!$.

Plus généralement le nombre de r-cycles dans $\mathcal{S}_n$ est $\binom{n}{r}(r-1)!$.

Exercice 76

Soient $p \geqslant 5$ un nombre premier et $\mathrm{H} \subset \mathcal{S}_p$ un sous-groupe tel que $1 < [\mathcal{S}_p : \mathrm{H}] < p$.

1. Montrer que tout cycle d'ordre p est contenu dans H.
2. Montrer que tout cycle d'ordre 3 est produit de deux cycles d'ordre p.
3. Montrer que $\mathrm{H} = \mathcal{A}_p$.
4. Montrer que $\mathcal{S}_5$ ne contient aucun sous-groupe d'ordre 30, 40.

Solution 76

1. Soit c un p-cycle et soit $\overline{c}$ son image dans ${}^{\mathcal{S}_p}\!/\!_{\mathrm{H}}$ qui n'est qu'un ensemble et n'est pas muni de structure de groupe car H n'est pas distingué dans $\mathcal{S}_p$. L'ensemble ${}^{\mathcal{S}_p}\!/\!_{\mathrm{H}}$ étant de cardinal strictement inférieur à p, on en déduit qu'il existe $0 \leqslant i < j < p$ tel que $\overline{c^i} = \overline{c^j}$ de sorte qu'il existe $h \in \mathrm{H}$ tel que $c^j = c^i h$ soit $c^{j-i} \in \mathrm{H}$. Or p étant premier, il existe u et v tel que $u(j-i) + vp = 1$ de sorte que $c^{(j-i)u} = c \in \mathrm{H}$ (car $c^p = \mathrm{id}$ puisque c est un p-cycle).
2. On remarque que
$$(1\ 3\ 2\ 4\ \ldots\ p)^{-1} \circ (1\ 2\ 3\ \ldots\ p) = (1\ 3\ 2)$$
de sorte que pour un 3-cycle quelconque $(a\ b\ c)$ nous avons
$$(a\ b\ c) = (a\ b\ c\ i_1\ \ldots\ i_{p-3})^{-1} \circ (a\ c\ b\ i_1\ \ldots\ i_{p-3})$$
où $\{i_1, \ldots, i_{p-3}\} = \{1, \ldots, n\} \smallsetminus \{a, b, c\}$.
3. Le groupe $\mathcal{A}_p$ étant engendré par les 3-cycles qui d'après la question précédente appartiennent à H, nous obtenons que $\mathcal{A}_p \subset \mathrm{H} \subset \mathcal{S}_p$ de sorte que $\frac{p!}{2}$ divise l'ordre de H qui est lui-même un diviseur de $p!$. Comme H est un sous-groupe strict de $\mathcal{S}_p$, nous en déduisons que H est d'ordre $\frac{p!}{2}$ et donc que $\mathcal{A}_p = \mathrm{H}$.
4. Appliquons ce qui précède au cas $p = 5$. Si H était un sous-groupe de $\mathcal{S}_5$ de cardinal 30 (resp. 40), il serait d'indice 4 (resp. 3) de sorte qu'il devrait contenir $\mathcal{A}_5$ ce qui n'est pas possible.

Exercice 77

Quel est l'ordre maximal d'un élément de $\mathcal{S}_5$?

Solution 77

Soit σ un élément de $\mathcal{S}_5$. Soit $\sigma = c_1 \circ c_2 \circ \ldots \circ c_r$ la décomposition en cycles à supports disjoints de σ. Chaque cycle est d'ordre sa longueur et ces cycles commutent car leurs supports sont disjoints de sorte que l'ordre de σ est le ppcm des longueurs des cycles c_i pour $1 \leqslant i \leqslant r$. En particulier dans $\mathcal{S}_5$ on trouve que l'ordre maximal d'un élément est 6.

Exercice 78

Le groupe $\mathcal{A}_4$ est-il simple ? le groupe $\mathcal{S}_4$ est-il simple ?

Solution 78

Le groupe $\mathcal{A}_4$ n'est pas simple : le groupe
$$\mathcal{K} \simeq \big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$$
est un sous-groupe distingué non trivial et strict de $\mathcal{A}_4$.

Le groupe $\mathcal{S}_4$ n'est pas simple : le groupe $\mathcal{A}_4$ est un sous-groupe distingué non trivial et strict de $\mathcal{S}_4$.

Exercice 79

Décomposer la permutation $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2)$ en produit de cycles à support disjoint.

Solution 79

On a $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2) = (2\ 1\ 4\ 5)$.

Exercice 80

Exprimer comme produit de cycles disjoints :

1. $(1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$;
2. $(1\ 2)(1\ 2\ 3)(1\ 2)$.

Quelle est la signature de ces permutations ?

Solution 80

1. Posons $\sigma_1 = (1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$. Explicitons σ_1 :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 1\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 6\ 7\ 8\ 9\ 1 \\ 4\ 2\ 3\ 5\ 6\ 7\ 8\ 9\ 1 \\ 4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2 \end{array}$$

Donc $\sigma_1 = (4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2)$.
C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

2. Posons $\sigma_2 = (1\ 2)(1\ 2\ 3)(1\ 2)$. Explicitons σ_2 :

$$\begin{array}{c} 1\ 2\ 3 \\ 2\ 1\ 3 \\ 3\ 2\ 1 \\ 3\ 1\ 2 \end{array}$$

Ainsi $\sigma_2 = (3\ 1\ 2)$.
C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

Exercice 81

Calculer aba^{-1} pour

1. $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$;
2. $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$.

Solution 81

1. Calcul de aba^{-1} pour $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$.
Explicitons a :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 1\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 3\ 5\ 4\ 1\ 6\ 7\ 8\ 9 \end{array}$$

autrement dit $a = (1\ 2\ 3\ 5)$. Il s'en suit que

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 1\ 2\ 4\ 3\ 6\ 7\ 8\ 9 \end{array}$$

Finalement nous obtenons

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 1\ 2\ 4\ 3\ 6\ 7\ 8\ 9 \\ 7\ 5\ 2\ 4\ 3\ 6\ 9\ 8\ 1 \\ 7\ 1\ 3\ 4\ 5\ 6\ 9\ 8\ 2 \end{array}$$

2. Calcul de aba^{-1} pour $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$. Les cycles a et b sont à supports disjoints donc commutent.
Ainsi $aba^{-1} = aa^{-1}b = b$, autrement dit $aba^{-1} = b$.

Exercice 82

Déterminer la parité des permutations suivantes et les écrire comme produits de transpositions :

$$\sigma_1 = (1\ 3\ 5)(5\ 4\ 3\ 2)(5\ 6\ 7\ 8), \qquad \sigma_2 = (1\ 2)(2\ 4)(1\ 7)(7\ 6\ 8).$$

Solution 82

L'application signature est un morphisme de $\mathcal{S}_8$ dans le groupe multiplicatif $\{-1, 1\}$.

La permutation σ_1 est le produit d'un cycle pair avec deux cycles impairs, elle est donc paire.

La permutation σ_2 est le produit de 3 cycles impairs et d'un cycle pair, elle est donc impaire.

Autre méthode :

$$\sigma_1 = (3\ 5)(5\ 1)(2\ 3)(4\ 2)(2\ 5)(7\ 8)(6\ 8)(5\ 8)$$

donc $\text{sgn}(\sigma_1) = (-1)^8 = 1$ et

$$\sigma_2 = (1\ 2)(2\ 4)(1\ 7)(6\ 8)(7\ 8)$$

donc $\text{sgn}(\sigma_1) = (-1)^5 = -1$.

Exercice 83

Soit σ la permutation de $\{1, 2, \ldots, 12\}$ définie par

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

Calculer σ^{2000}.

Solution 83

Posons $\sigma_1 = (1\ 10\ 5\ 7\ 2\ 9\ 12)$, $\sigma_2 = (3\ 8\ 6)$ et $\sigma_3 = (4\ 11)$.

Ces trois permutations sont à supports disjoints deux à deux donc commutent. Il en résulte que $\sigma^{2000} = \sigma_1^{2000}\sigma_2^{2000}\sigma_3^{2000}$.

Par ailleurs σ_1 est d'ordre 7 et $2000 = 285 \times 7 + 5$ d'où $\sigma_1^{2000} = \sigma_1^5$.

De plus σ_2 est d'ordre 3 et $2000 = 666 \times 3 + 2$ d'où $\sigma_2^{2000} = \sigma_2^2$.

Enfin σ_3 est d'ordre 2 et $2000 = 1000 \times 2$ d'où $\sigma_3^{2000} = \text{id}$.

Par suite

$$\sigma^{2000} = \sigma_1^5\sigma_2^2 = (1\ 9\ 7\ 10\ 12\ 2\ 5)(3\ 8\ 6)$$

Exercice 84

Soit n un entier, soit σ une permutation de $\{1, 2, \ldots, n\}$ et soit $(x_1\ x_2\ \ldots\ x_k)$ un cycle de $\mathcal{S}_n$.

Calculer $\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}$.

Solution 84

Pour $1 \leqslant i \leqslant j$ posons $\sigma(x_i) = y_i$. Alors $\sigma^{-1}(y_i) = x_i$ et $\big((x_1\ x_2\ \ldots\ x_k)\sigma^{-1}\big)(y_i) = \big((x_1\ x_2\ \ldots\ x_k)\big)(x_i) = x_{i+1}$ donc $\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}(y_i) = \sigma(x_{i+1}) = y_{i+1}$.

Par ailleurs si $y \notin \{y_1, y_2, \ldots, y_k\}$, alors $\big(\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}\big)(y) = y$.

Il en résulte que

$$\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \ldots\ \sigma(x_k))$$

Exercice 85

Dans le groupe $\mathcal{S}_7$ calculer le produit

$$(4\ 5\ 6)(5\ 6\ 7)(6\ 7\ 1)(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

Solution 85

Nous avons

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7 \\ 1\ 2\ 4\ 5\ 3\ 6\ 7 \\ 1\ 3\ 2\ 5\ 4\ 6\ 7 \\ 2\ 1\ 3\ 5\ 4\ 6\ 7 \\ 2\ 6\ 3\ 5\ 4\ 7\ 1 \\ 2\ 7\ 3\ 6\ 4\ 5\ 1 \\ 2\ 7\ 3\ 4\ 5\ 6\ 1 \end{array}$$

Exercice 86

Soit n un entier. Construire des morphismes injectifs de $\mathcal{S}_n$ dans $\mathcal{S}_{n+1}$.

Solution 86

Soit x un élément de $\{1, 2, \ldots, n+1\}$. Posons $E_x = \{1, 2, \ldots, n+1\} \smallsetminus \{x\}$. Il existe un isomorphisme φ entre $\mathcal{S}_n$ et $\mathcal{S}_{E_x}$. Le morphisme $f_x\colon \mathcal{S}_n \to \mathcal{S}_{n+1}$ défini par

$$\left\{\begin{array}{l} f_x(\sigma)(i) = \varphi(\sigma)(i) \text{ pour } i \in E_x \\ f_x(\sigma)(x) = x \end{array}\right.$$

est injectif.

Exercice 87

Montrer que si c et γ sont des n-cycles de $\mathcal{S}_n$ qui commutent entre eux, il existe un entier r tel que $\gamma = c^r$.

Solution 87

Soient $c = (1\ c(1)\ c^2(1)\ \ldots\ c^{n-1}(1))$ et $\gamma = (1\ \gamma(1)\ \gamma^2(1)\ \ldots\ \gamma^{n-1}(1))$ deux n-cycles de $\mathcal{S}_n$ qui commutent entre eux, *i.e.* $c\gamma = \gamma c$.

L'ensemble $\{1, 2, \ldots, n\}$ coïncide avec $\{1, c(1), c^2(1), \ldots, c^{n-1}(1)\}$. Par conséquent il existe $0 \leqslant r \leqslant n-1$ tel que $\gamma(1) = c^r(1)$. De plus si $i \in \{1, \ldots, n\}$, alors il existe $0 \leqslant s \leqslant n-1$ tel que $i = c^s(1)$. Il en résulte que

$$\gamma(i) = \gamma(c^s(1)) = c^s(\gamma(1)) = c^s(c^r(1)) = c^r(c^s(1)) = c^s(i).$$

Par suite $\gamma = c^s$.

Autre méthode : faisons agir $\mathcal{S}_n$ sur l'ensemble des n-cycles par conjugaison (c'est possible car les n-cycles sont dans la même orbite pour cette action). Cet ensemble est de cardinal $(n-1)!$ En effet un n-cycle σ s'écrit $(1\ \sigma(1)\ \sigma(2)\ \ldots\ \sigma(n-1))$ et nous avons $(n-1)$ choix pour $\sigma(1)$ puis $(n-2)$ choix pour $\sigma(2)$ etc. Le groupe $\mathcal{S}_n$ agit transitivement sur cet ensemble. L'indice du stabilisateur de c pour cette action est $(n-1)!$ et son cardinal est n. Ce stabilisateur est le centralisateur de c qui contient au moins les n puissances de c et tout n-cycle qui commute avec c est donc égal à une puissance de c.

Exercice 88

Soit $n \geqslant 3$ un entier. Sachant que le groupe $\mathcal{S}_n$ est engendré par l'ensemble des transpositions de $\{1, 2, \ldots, n\}$ montrer que $\mathcal{S}_n$ est engendré par les ensembles suivants de permutations :

1. $(1\ 2), \ldots, (1\ n)$;
2. $(1\ 2), (2\ 3), \ldots, (n-1\ n)$;
3. $(1\ 2), (2\ 3\ \ldots\ n)$.

Solution 88

1. Notons que $(i\ j) = (i\ 1)(j\ 1)(i\ 1)$ lorsque $i \neq j$;
2. Soit $i < j$.
   Si $j > i+1$, alors
   $$(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j) \tag{2}$$
   Si $j-1 = i+1$, alors $(i\ j) \in \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle$.
   Sinon nous appliquons (2) en remplaçant $(i\ j)$ par $(i\ j-1)$ et nous arrivons de proche en proche au résultat.

3. Nous avons
$$(2\ 3\ \ldots\ n)(1\ 2)(2\ 3\ \ldots\ n)^{-1} = (1\ 3).$$
Par suite par récurrence pour $i > 2$ nous avons
$$(1\ i) = (2\ 3\ \ldots\ n)^{i-2}(1\ 2)(2\ 3\ \ldots\ n)^{-i+2}$$
d'où le résultat (en utilisant la première question).

Exercice 89

Soit G un sous-groupe de $\mathcal{S}_4$ opérant sur $\{1, 2, 3, 4\}$ par l'action induite par l'action naturelle de $\mathcal{S}_4$.
Pour $i = 1, 2, 3, 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i.
Déterminer $\mathcal{O}_i$ et S_i pour $i = 1, 2, 3, 4$ dans chacun des cas suivants :

1. $\mathrm{G} = \langle(1\ 2\ 3)\rangle$;
2. $\mathrm{G} = \langle(1\ 2\ 3\ 4)\rangle$;
3. $\mathrm{G} = \big\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}$;
4. $\mathrm{G} = \big\{e, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\big\}$;
5. $\mathrm{G} = \mathcal{A}_4$.

Solution 89

1. Supposons que $\mathrm{G} = \langle(1\ 2\ 3)\rangle$.
   Si $i = 1$, alors $\mathcal{O}_i = \big\{1, 2, 3\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \big\{1, 2, 3\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \big\{1, 2, 3\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{4\}$ et $S_i = \mathrm{G}$.
2. Supposons que $\mathrm{G} = \langle(1\ 2\ 3\ 4)\rangle$.
   Si $i = 1$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
3. Supposons que $\mathrm{G} = \big\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \mathrm{id}$.
4. Supposons que $\mathrm{G} = \big\{\mathrm{id}, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\big\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \big\{1, 2\big\}$ et $S_i = \big\{\mathrm{id}, (3\ 4)\big\}$.
   Si $i = 2$, alors $\mathcal{O}_i = \big\{1, 2\big\}$ et $S_i = \big\{\mathrm{id}, (3\ 4)\big\}$.
   Si $i = 3$, alors $\mathcal{O}_i = \big\{3, 4\big\}$ et $S_i = \big\{\mathrm{id}, (1\ 2)\big\}$.
   Si $i = 4$, alors $\mathcal{O}_i = \big\{3, 4\big\}$ et $S_i = \big\{\mathrm{id}, (1\ 2)\big\}$.
5. Supposons que $\mathrm{G} = \mathcal{A}_4$.
   Si $i = 1$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \langle(2\ 3\ 4)\rangle$.
   Si $i = 2$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \langle(1\ 3\ 4)\rangle$.
   Si $i = 3$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \langle(1\ 2\ 4)\rangle$.
   Si $i = 4$, alors $\mathcal{O}_i = \big\{1, 2, 3, 4\big\}$ et $S_i = \langle(1\ 2\ 3)\rangle$.

Exercice 90

Établir la table de $\mathcal{S}_3$ et de $\mathbb{Z}/6\mathbb{Z}$.
Quels sont les sous-groupes de $\mathcal{S}_3$?
Quels sont les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$?

Solution 90

La table de $\mathcal{S}_3$ est

	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

La table de $\mathbb{Z}/6\mathbb{Z}$ est

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[4]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Les sous-groupes de $\mathcal{S}_3$ sont :

- un sous-groupe d'ordre 1 ;
- trois sous-groupes d'ordre 2 : $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$;
- un sous-groupe d'ordre 3 : $\langle(1\ 2\ 3)\rangle$.

Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont :

- un sous-groupe d'ordre 1 ;
- un sous-groupes d'ordre 2 : $\langle[3]\rangle$;
- un sous-groupes d'ordre 3 : $\langle[2]\rangle$.

Exercice 91

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Solution 91

a) Soit $c = (a_1\ \dots\ a_k)$ un k-cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1)\ \dots\ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geqslant 1$ tels que

$$m_1 \leqslant \ldots \leqslant m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1\ \dots\ a_{2k+1}) \qquad\qquad c' = (a'_1\ \dots\ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1\ a'_1)\ldots(a_{2k+1}\ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leqslant i < j \leqslant n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i\ j)\sigma(i\ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 92

Considérons les deux éléments suivants du groupe symétrique $\mathcal{S}_9$

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in \mathcal{S}_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$.

Quel est le cardinal (une expression sous forme de produit d'entiers suffit) de la classe de conjugaison de σ_1 dans $\mathcal{S}_9$?

Solution 92

Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de même longueur (2, 3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (8\ 9)(5\ 6\ 7)(1\ 2\ 3\ 4)$$

nous trouvons parmi de nombreux choix possibles $\omega = (1\ 8\ 3\ 5\ 7\ 2\ 9\ 4\ 6)$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de $\mathcal{S}_9$ de type 2, 3, 4 :

- $(9 \cdot 8)/2 = 9 \cdot 4$ choix possibles pour la transposition ;
- $2 \cdot (7 \cdot 6 \cdot 5)/6 = 7 \cdot 5 \cdot 2$ choix possibles pour le 3-cycle ;
- 6 choix possibles pour le 4-cycle.

soit finalement $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ choix possibles.

Exercice 93

Montrer que le groupe symétrique $\mathcal{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathcal{S}_3)$.

Solution 93

L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathcal{S}_3$ dans $\mathrm{Aut}(\mathcal{S}_3)$, car le centre de $\mathcal{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathcal{S}_3)$ est déterminé par l'image des générateurs $(1\,2)$ et $(1\,3)$. Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathcal{S}_3$), donc en comparant les ordres nous obtenons que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 94

Montrer que tout sous-groupe d'indice n dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

Solution 94

Soit H un sous-groupe d'indice n dans $\mathcal{S}_n$.

Si $n \geqslant 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors si $\mathrm{H} \not\simeq \mathcal{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q-1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geqslant 5$. Le groupe $\mathcal{S}_n$, et donc aussi H, opère par translation à gauche sur $E = {}^{\mathcal{S}_n}\!/_{\mathrm{H}}$ d'où un morphisme

$$\varphi \colon \mathcal{S}_n \to \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a \in \mathcal{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathcal{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geqslant 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$.

Exercice 95

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Solution 95

a) Soit $c = (a_1 \ \dots \ a_k)$ un k-cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geqslant 1$ tels que

$$m_1 \leqslant \ldots \leqslant m_r \qquad \qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \dots \ a_{2k+1}) \qquad \qquad c' = (a'_1 \ \dots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \dots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leqslant i < j \leqslant n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i \ j)\sigma(i \ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 96

Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathcal{S}_n$ formé par les permutations paires.

a) Montrer que le produit de deux transpositions distinctes de $\mathcal{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathcal{S}_n$.

b) i) Montrer que pour $n \geqslant 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles $(1\ 2\ 3)$, …, $(1\ 2\ n)$. En déduire que $\mathcal{A}_n$ est pour $n \geqslant 3$ stable par tout automorphisme ϕ de $\mathcal{S}_n$ (autrement dit $\mathcal{A}_n$ est un sous-groupe caractéristique de $\mathcal{S}_n$).

ii) Montrer que $\mathcal{A}_n$ est engendré
— si n est impair $\geqslant 5$ par $(1\ 2\ 3)$ et $(3\ 4\ \dots\ n)$;
— si n est pair $\geqslant 4$ par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \dots\ n)$.

c) Montrer que pour $n \geqslant 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathcal{S}_n$ de la forme $(a\ b)(c\ d)$ avec a, b, c, d deux à deux distincts.

Solution 96

a) Soient $i < j < k < l$. Nous avons

$$(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l)$$

Or $(i\ j)(j\ k) = (i\ j\ k)$ donc

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l).$$

Tout élément σ de $\mathcal{A}_n$ est le produit d'un nombre pair de transpositions donc un produit de 3-cycles. Le sous-groupe de $\mathcal{A}_n$ engendré par les 3-cycles contient donc $\mathcal{A}_n$, c'est donc $\mathcal{A}_n$.

b) i) Soient i, j et k des éléments de $\{1, \ldots, n\}$ tels que $i < j < k$. Nous avons

$$(i\ j\ k) = (1\ 2\ i)(2\ j\ k)(1\ 2\ i)^{-1}$$

et

$$(2\ j\ k) = (1\ 2\ j)(1\ 2\ k)(1\ 2\ j)^{-1}$$

donc $\mathcal{A}_n \subset \langle (1\ 2\ 3), \ldots, (1\ 2\ n) \rangle$. Il en résulte que

$$\mathcal{A}_n = \langle (1\ 2\ 3), \ldots, (1\ 2\ n) \rangle.$$

Soient ϕ un automorphisme de $\mathcal{S}_n$ et σ un 3-cycle. L'ordre de $\phi(\sigma)$ est 3. Donc $\phi(\sigma)$ est un produit de 3-cycles car son ordre est le ppcm des longueurs des cycles qui interviennent dans sa décomposition en cycles. Le groupe $\mathcal{A}_n$ est donc caractéristique dans $\mathcal{S}_n$.

ii) Pour $i \geqslant 4$ et $n \geqslant 4$ nous avons

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

Par ailleurs si $n \geqslant 5$ est impair, $(3\ 4\ \ldots\ n)$ est une permutation paire car c'est un cycle de longueur impaire $n-2$. Ainsi pour $n \geqslant 5$ impair on a

$$\mathcal{A}_n = \langle (1\ 2\ 3), (3\ 4\ \ldots\ n) \rangle$$

Nous avons

$$(1\ 2)^\alpha (1\ 2\ i)(1\ 2)^\alpha = \begin{cases} (1\ 2\ i) \text{ pour } \alpha \text{ pair} \\ (1\ 2\ i)^{-1} \text{ pour } \alpha \text{ impair} \end{cases}$$

Donc puisque pour $i \geqslant 4$ et $n \geqslant 4$

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

alors pour $i \geqslant 4$ impair et $n \geqslant 4$

$$(1\ 2\ i) = [(1\ 2)(3\ 4\ \ldots\ n)]^{i-3}(1\ 2\ 3)[(1\ 2)(3\ 4\ \ldots\ n)]^{-3+i}.$$

Et pour $i \geqslant 4$ pair et $n \geqslant 4$

$$(1\ 2\ i) = \big[\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{i-3}(1\ 2\ 3)\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{-3+i}\big]^{-1}.$$

Or si $n \geqslant 4$ est pair $(1\ 2)(3\ 4\ \ldots\ n)$ est une pemutation paire. Par conséquent le groupe $\mathcal{A}_n$ est engendré par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Il suffit de montrer que tout 3-cycle $(i\ j\ k)$ (avec $i < j < k$) est produit de permutations de la forme $(a\ b)(c\ d)$ où a, b, c et d sont deux à deux distincts. Puisque $n \geqslant 5$ il existe ℓ et m dans $\{1, 2, \ldots, n\}$ tels que i, j, k, ℓ et m soient 2 à 2 distincts. Or nous avons

$$(i\ j\ k) = (m\ \ell)(j\ k)(m\ \ell)(i\ k)$$

d'où le résultat.

Exercice 97

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.

Solution 97

Considérons l'application $\psi\colon \mathcal{S}_n \to \mathcal{A}_{n+2}$ définie par

$$\begin{cases} \psi(\sigma) = \sigma \text{ si } \sigma \text{ est une permutation paire} \\ \psi(\sigma) = \sigma \circ (n+1\ n+2) \text{ si } \sigma \text{ est une permutation impaire} \end{cases}$$

L'application ψ est injective par unicité de la décomposition en cycles à supports disjoints.

On peut vérifier que ψ est un morphisme de groupes.

Exercice 98

Construire un morphisme surjectif de $\mathcal{S}_4$ sur $\mathcal{S}_3$.

Solution 98

Faire agir $\mathcal{S}_4$ par conjugaison sur les éléments d'ordre 2 de $\mathcal{S}_4$ qui ne sont pas des transpositions.

Exercice 99

On rappelle que le groupe symétrique $\mathcal{S}_n$ agit par applications linéaires sur $\mathbb{R}^n$ muni de sa base canonique (e_i), en posant pour tout $\sigma \in \mathcal{S}_n$ et tout vecteur e_i de la base canonique $\sigma \cdot e_i = e_{\sigma(i)}$. Pour $\sigma = (1\ 2\ 3) \in \mathcal{S}_3$ expliciter la matrice associée et calculer $\sigma \cdot (x_1, x_2, x_3)$.

Solution 99

L'action de $\mathcal{S}_3$ par applications linéaires sur $\mathbb{R}^3$ correspond à un morphisme de $\mathcal{S}_3$ vers le groupe $\mathrm{GL}(3, \mathbb{R})$ des bijections linéaires de $\mathbb{R}^3$. Il s'agit de trouver l'image de $\sigma = (1\ 2\ 3) \in \mathcal{S}_3$. L'application linéaire est entièrement déterminée par l'image d'une base : puisque $e_1 \mapsto e_2$, $e_2 \mapsto e_3$, $e_3 \mapsto e_1$ nous obtenons la matrice

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

et finalement l'image de (x_1, x_2, x_3) est (x_3, x_1, x_2) car

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}.$$

Remarque : une erreur classique est de croire que l'action est donnée par

$$\sigma(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}).$$

Ce n'est pas le cas, cette définition donnerait une action à droite, pas à gauche ! En fait on peut vérifier que la formule correcte pour l'action exprimée en coordonnées est

$$\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

3 Autour des théorèmes de Sylow

Exercice 100

Donner un p-Sylowde $\mathrm{GL}(n, \mathbb{F}_p)$.

Solution 100

Le sous-groupe des matrices triangulaires supérieures strictes de $\mathrm{GL}(n, \mathbb{F}_p)$ est un p-Sylowde $\mathrm{GL}(n, \mathbb{F}_p)$.

Exercice 101

Montrer qu'il n'existe pas de groupe simple d'ordre 30.

Solution 101

Supposons qu'il existe un groupe simple G d'ordre 30. Considérons les p-Sylowde G. Désignons par n_p le nombre de p-Sylow de G.

Rappelons que $30 = 2 \times 3 \times 5$.

Les théorèmes de Sylowassurent que

$$\begin{aligned} n_2 &\equiv 1 \bmod 2, & n_2 &\,|\, 3 \times 5 = 15 \\ n_3 &\equiv 1 \bmod 3, & n_3 &\,|\, 2 \times 5 = 10 \\ n_5 &\equiv 1 \bmod 5, & n_5 &\,|\, 2 \times 3 = 6 \end{aligned}$$

i.e.

$$n_2 \in \{1,\ 3,\ 5\,15\}, \qquad n_3 \in \{1,\ 10\}, \qquad n_5 \in \{1,\ 6\}$$

Mais G est simple donc $n_2 \neq 1$, $n_3 \neq 1$ et $n_5 \neq 1$; finalement

$$n_2 \in \{3,\, 5,\, 15\}, \qquad\qquad n_3 = 10, \qquad\qquad n_5 = 6.$$

On en déduit que le groupe G contient 24 éléments d'ordre 5 (les intersections des 5-Sylowsont restreintes à l'élément neutre) et au moins 20 éléments d'ordre 3. En particulier d'une part $|\mathrm{G}| = 30$, d'autre part $|\mathrm{G}| \geqslant 44$.

Exercice 102

Montrer qu'un groupe d'ordre 200 n'est pas simple.

Solution 102

Soit G un groupe d'ordre 200. Notons que $200 = 2^3 \times 5^2$. D'après les Théorèmes de Sylow le nombre de 5-Sylow de G est congru à 1 modulo 5 et divise $2^3 = 8$ donc vaut 1. L'unique 5-Sylow de G est donc nécessairement distingué dans G ; en particulier G n'est pas simple.

Exercice 103

Soit G un groupe d'ordre 15.

1. Combien G possède-t-il d'éléments d'ordre 3 ?
2. Combien G possède-t-il d'éléments d'ordre 5 ?
3. Démontrer que G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Solution 103

1. Soit n_3 le nombre de 3-Sylow de G. D'après les théorèmes de Sylow, $n_3 \equiv 1 \mod 3$ et $n_3|5$, *i.e.* $n_3 = 1$. Soit H l'unique 3-Sylow de G. Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si $\mathrm{H} = \big\{\mathrm{id},\, g,\, h\big\}$, alors ces éléments sont g et h.
2. De la même façon, on montre que G possède quatre éléments d'ordre 5. Soit n_5 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \mod 5$ et $n_5|3$ soit que $n_5 = 1$. Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.
3. L'ordre d'un élément de G est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a huit éléments d'ordre 15. Ainsi G possède un élément d'ordre son cardinal ; G est donc le groupe cyclique engendré par cet élément, *i.e.* G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 104

(1) Quel est le nombre de 2-Sylow dans le groupe symétrique $\mathcal{S}_4$?

(2) Rappelons que $\mathcal{S}_4$ est isomorphe au groupe des rotations de $\mathbb{R}^3$ préservant un cube. Interpréter géométriquement la réponse à la question précédente.

Solution 104

(1) Le groupe $\mathcal{S}_4$ est d'ordre $24 = 2 \times 3 \times 3$. Le nombre n de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $8 = 2^3$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n = 1$ ou $n = 3$. Montrons que $n = 1$ est impossible. Si $n = 1$, alors l'unique 2-Sylow serait un sous-groupe distingué de $\mathcal{S}_4$. Mais les classes de conjugaison de $\mathcal{S}_4$ sont de cardinaux 1, 3 et 8, et il est impossible d'obtenir 8 en sommant 1 et 3 ou 8 (rappelons qu'un sous-groupe contient le neutre, donc la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : $\mathcal{S}_4$ contient 3 sous-groupes d'ordre 8.

(2) Cherchons géométriquement un sous-groupe d'ordre 8 dans $\mathcal{S}_4$ vu comme le groupe des rotations préservant un cube. Il y a cinq groupes d'ordre 8 à isomorphisme près, dont le groupe diédral D_8. Comme il y a un air de famille entre le cube et le carré, cela incite à chercher un sous-groupe de $\mathcal{S}_4$ isomorphe à D_8. Effectivement il y en a : on tranche le cube suivant un "carré équateur" et on considère le sous-groupe des rotations préservant à la fois le cube et ce carré : il y en a 8.

Exercice 105

Montrer que tout groupe d'ordre 217 est cyclique (Indication : commencer par calculer le nombre de p-Sylow pour chaque diviseur premier p de 217).

Solution 105

Soit G un groupe d'ordre 217. Notons que $217 = 7 \times 31$ et que 7 et 31 sont premiers. Le nombre de 7-Sylow de G est congru à 1 modulo 7 et divise 31 : la seule possibilité est donc 1. D'autre part le nombre de 31-Sylow est congru à 1 modulo 31 et divise 7 ; de nouveau la seule possibilité est 1. Ainsi G contient un unique 7-Sylow $S_7 \subset$ G, qui est donc distingué, et de même contient un unique 31-Sylow $S_{31} \subset$ G, lui-aussi distingué.

L'intersection $S_7 \cap S_{31}$ est triviale par Lagrange.

Puisque S_7 est distingué dans G, S_7S_{31} est un sous-groupe de G [8]. Comme il contient strictement S_7 et S_{31}, son ordre est un mutliple strict de 7 et de 31, la seule possibilité est donc 217 et on conclut que G $= S_7 \times S_{31}$.

Puisque S_7 et S_{31} sont d'ordre premiers ils sont cycliques et G $\simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z}$; par le théorème chinois on conclut que G $\simeq \mathbb{Z}/217\mathbb{Z}$.

Exercice 106

Soient p un nombre premier et n un entier naturel avec $p > n$. Considérons un groupe G d'ordre pn et H un sous-groupe de G d'ordre p. Montrer que H est un sous-groupe distingué de G.

Indication : compter les p-Sylow de G.

Solution 106 D'après les hypothèses, $\mathrm{pgcd}(p, n) = 1$, donc H est un p-Sylow de G. Notons n_p le nombre de p-Sylow de G. Alors par les théorèmes de Sylow, $n_p \equiv 1 \bmod p$ et $n_p | n$. Si $n_p \neq 1$, alors $n_p \geqslant p + 1$, ce qui contredit que n_p divise n puisque $n < p$. Ainsi, $n_p = 1$ et H est l'unique p-Sylow de G donc est distingué dans G.

Exercice 107

Déterminer à isomorphisme près tous les groupes d'ordre 33.

Solution 107 Soit G un groupe d'ordre 33.

Les éléments de G sont d'ordre 1, 3, 11 ou 33. Une application directe des théorèmes de Sylow montre que G contient un unique 3-Sylow et un unique 11-Sylow. En effet soit n_p le nombre de p-Sylow de G ; d'une part $n_3 \equiv 1 \bmod 3$ et $n_3|11$, d'autre part $n_{11} \equiv 1 \bmod 11$ et $n_{11}|3$, *i.e.* $n_{11} = 1$. Les éléments d'ordre 3 et 11 sont contenus dans ces deux groupes. On a au plus $1 + (3 - 1) + (11 - 1) = 1 + 2 + 10 = 13$ éléments d'ordre 1, 3 ou 11. Il existe donc un élément d'ordre 33 dans G qui est donc cyclique isomorphe à $\mathbb{Z}/33\mathbb{Z}$.

Exercice 108

1. Quels sont les sous-groupes de Sylow de $\mathcal{A}_4$?
2. Déterminer l'ordre de tous les éléments de $\mathcal{A}_4$.
   Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.
   Montrer que H contient au moins trois éléments d'ordre 3.
   Peut-il être isomorphe à $\mathcal{S}_3$?
   En déduire qu'il n'y a pas de sous-groupe d'ordre 6 dans $\mathcal{A}_4$.
4. Donner la liste des sous-groupes de $\mathcal{A}_4$.

Solution 108

8. On utilise la propriété suivante : si K $\subset$ G est un sous-groupe distingué, et H $\subset$ G est un sous-groupe, alors KH $= \{kh \mid k \in$ K, $h \in$ H$\}$ est un sous-groupe de G ; cela découle de :

$$\forall k_1, k_2 \in \mathrm{K}, \forall h_1, h_2 \in \mathrm{H} \qquad (k_1h_1)(k_2h_2) = \underbrace{k_1h_1k_2h_1^{-1}}_{\in \mathrm{K}}\underbrace{h_1h_2}_{\in \mathrm{H}} \in \mathrm{KH}$$

1. Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$.

   L'ordre de $\mathcal{A}_4$ est $12 = 2^2 \times 3$. Soient n_2 le nombre de sous-groupes de Sylow d'ordre $2^2 = 4$ et n_3 le nombre de sous-groupes de Sylow d'ordre 3. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2|3$$

   $$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3|2^2 = 4$$

   autrement dit que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$.

   Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois donc $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4 isomorphe au groupe de Klein, *i.e.* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (en effet d'après le théorème de Lagrange un sous-groupe K de $\mathcal{A}_4$ d'ordre 4 contient des éléments d'ordre 1, 2 ou 4 ; mais $\mathcal{A}_4$ ne contient pas d'élément d'ordre 2 donc K contient des éléments d'ordre 1 ou 4. Comme $\mathcal{A}_4$ contient un seul élément d'ordre 1 et trois éléments d'ordre 4 il contient un seul sous-groupe d'ordre 4).

   Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.
2. Déterminons l'ordre de tous les éléments de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?

   Le groupe $\mathcal{A}_4$ contient trois éléments d'ordre 2, huit éléments d'ordre 3 et un élément d'ordre 1. Le groupe $\mathcal{A}_4$ ne contient donc aucun élément d'ordre 6 et ne contient donc pas de sous-groupe cyclique d'ordre 6.
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.

   Notons que
   $$(a\ b)(c\ d)(a\ b\ c) = (b\ d\ c)$$
   Le groupe H contient les 3-cycles : $(a\ b\ c)$, $(a\ c\ b)$ et $(b\ d\ c)$ donc les trois sous-groupes d'ordre 3
   $$\langle(a\ b\ c)\rangle, \qquad \langle(a\ c\ b)\rangle, \qquad \langle(b\ d\ c)\rangle.$$
   Un groupe d'ordre 6 ne contient qu'un sous-groupe d'ordre 3 (en effet soit K un sous-groupe d'ordre $6 = 2 \times 3$. Désignons par n_3' le nombre de 3-Sylow de K ; d'une part $n_3' \equiv 1 \bmod 3$ d'autre part $n_3'|2$ donc $n_3' = 1$). Par conséquent le groupe H n'est pas d'ordre 6. En particulier H ne peut pas être isomorphe à $\mathcal{S}_3$ qui est d'ordre 6.
4. Le groupe $\mathcal{A}_4$ contient :
   — un sous-groupe d'ordre 1 : $\{\mathrm{id}\}$;
   — trois sous-groupes d'ordre 2 :
   $$\langle(1\ 2)(3\ 4)\rangle \qquad \langle(1\ 3)(2\ 4)\rangle \qquad \langle(1\ 4)(2\ 3)\rangle;$$
   — quatre sous-groupes d'ordre 3 :
   $$\langle(1\ 2\ 3)\rangle \qquad \langle(1\ 2\ 4)\rangle \qquad \langle(1\ 3\ 4)\rangle \qquad \langle(2\ 3\ 4)\rangle;$$
   — un sous-groupe d'ordre 4 :
   $$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Exercice 109 [Simplicité de $\mathcal{A}_n$, $n \geqslant 5$]

I) Commençons par démontrer que le groupe $\mathcal{A}_5$ est simple.

Soit G un groupe. Un sous-groupe H de G est caractéristique si pour tout automorphisme φ de G on $\varphi(\mathrm{H}) \subset \mathrm{H}$.

I) a) Montrer que tout p-Sylow distingué d'un groupe d'ordre fini est caractéristique.

I) b) Montrer que tout groupe d'ordre 15 est cyclique.

I) c) Montrer que tout groupe d'ordre 30 contient un sous-groupe distingué d'ordre 15.

I) d) Montrer que tout groupe d'ordre 30 ne contient qu'un seul 5-Sylow (d'ordre 5).

I) e) Montrer que tout groupe d'ordre 20 contient un seul sous-groupe d'ordre 5.

I) f) Montrer que tout groupe d'ordre 12 contient un sous-groupe caractéristique.

I) g) Montrer que tout groupe d'ordre 6 contient un sous-groupe caractéristique.

I) h) Montrer que tout groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow est simple.

I) i) Montrer que le groupe $\mathcal{A}_5$ est simple.

II) Soit $n \geqslant 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué de $\mathcal{A}_n$ non trivial.

II) a) Montrer qu'il existe $\tau \in \mathrm{H}$ distinct de l'identité qui a au moins un point fixe.

II) b) Montrer que pour tout $1 \leqslant j \leqslant n$ le sous-groupe $\mathrm{G}_j = \mathrm{Stab}_{\mathcal{A}_n}(\{j\})$ est inclus dans H.

II) c) Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$. Montrer que $\mathcal{A}_n = \mathrm{H}$.

II) d) En déduire que $\mathcal{A}_n$ est simple pour $n \geqslant 5$.

Solution 109

I) a) Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué dans G. Soit φ un automorphisme de G. L'image de H par φ est un sous-groupe de même ordre que H, *i.e.* $\varphi(\mathrm{H})$ est un p-Sylow de G. Mais H est l'unique p-Sylow de G car H est distingué dans G. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$.

I) b) Soit H un groupe d'ordre 15. Il a exactement un sous-groupe d'ordre 5 et un sous-groupe d'ordre 3. Ces deux sous-groupes sont distingués dans H. Par suite $\mathrm{H} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ et est donc cyclique.

I) c) Soit G un groupe d'ordre 30. Remarquons tout d'abord que tout sous-groupe d'ordre 15 de G est distingué dans G car il est d'indice 2 dans G.

Il suffit donc de démontrer l'existence d'un sous-groupe d'ordre 15 dans le groupe G.

— Supposons que G contienne plus d'un seul 5-Sylow, *i.e.* $n_5 > 1$. Puisque

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \,|\, 6$$

on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant id fait 25 éléments de G. Il y a donc exactement un seul 3-Sylow que nous noterons K (sinon il y en aurait 10 donc 20 éléments d'ordre 3 soit 45 éléments au moins dans G). En particulier K est distingué dans G. Si H est l'un des sous-groupes d'ordre 5, $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 de G.

— Supposons que G contienne un seul 5-Sylow H ; il est alors distingué dans G. Si K est l'un des sous-groupes d'ordre 3 de G (il y en a au moins un) $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

I) d) Au I) c) on a vu d'une part que tout groupe G d'ordre 30 contient un sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 5 et d'autre part que K ou H est distingué dans G.

Les groupes K et H sont distingués dans KH et sont donc caractéristiques (voir I)a)) dans le groupe KH qui est cyclique et distingué dans G (car d'indice 2 dans G). Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow.

I) e) Soit G un groupe d'ordre $20 = 2^2 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 4$$

d'où $n_5 = 1$.

I) f) Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

— Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué dans G ; ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (cf I) a)).

— Si $n_3 = 4$, on dénombre $4 \times 2 = 8$ éléments d'ordre 3 ; en ajoutant le neutre on compte donc 9 éléments. Considérons maintenant les 2-Sylow de G. D'après les théorèmes de Sylow on a

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \,|\, 3$$

Ainsi n_2 appartient à $\{1, 3\}$. Si $n_2 = 3$, on a trois sous-groupes d'ordre 4, soit trop d'éléments. Ainsi $n_2 = 1$, l'unique 2-Sylow est distingué dans G et donc caractéristique dans G (cf I) a)).

I) g) Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ses 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et I) b) permet de conclure.

I) h) Soit G un groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow. D'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 12$$

d'où $n_5 \in \{1, 6\}$. Par hypothèse $n_5 \neq 1$ donc $n_5 = 6$.
Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G. Notons que

$$|\mathrm{H}| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

- ◇ Si $|\mathrm{H}|$ est divisible par 5 alors H contient au moins un 5-Sylow de G. Mais H est distingué et les 5-Sylow se déduisent les uns des autres par conjugaison ; ainsi H contient tous les 5-Sylow de G. On en déduit que H contient déjà 6×4 éléments d'ordre 5. Par ailleurs $|\mathrm{H}|$ divise 60 donc $|\mathrm{H}| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|\mathrm{H}| < 60$). Mais dans ce cas H ne contient qu'un seul sous-groupe d'ordre 5 (voir I)d)) : contradiction avec le fait qu'il en contient 6. Par suite $|\mathrm{H}|$ n'est pas divisible par 5.
- ◇ Si $|\mathrm{H}|$ appartient à $\{6, 12\}$, alors il existe un sous-groupe caractéristique de H d'ordre 2, 3 ou 4 (d'après I)f) et I)g)). Ce sous-groupe caractéristique de H, qui est lui-même distingué dans G, est distingué dans G.
- ◇ Nous pouvons donc maintenant supposer que H est d'ordre 2, 3 ou 4. Dans ce cas G/H est d'ordre 30, 20 ou 15 (on renvoie à I)d) si G/H est d'ordre 30, à I)e) si G/H est d'ordre 20 ; enfin si G/H est d'ordre $15 = 3 \times 5$ et si n_5 est le nombre de 5-Sylow de G/H, les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et n_5 divise 3 donc $n_5 = 1$). Donc G/H contient un sous-groupe K distingué d'ordre 5. Considérons la surjection canonique $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$. Le sous-groupe $\pi^{-1}(\mathrm{K})$ contient H et est distingué dans G. Or $\pi^{-1}(\mathrm{K})/\mathrm{H}$ est isomorphe à $\mathrm{K} = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction (voir le premier ◇ du I)h)).

I) i) Le groupe $\mathcal{A}_5$ est d'ordre 60 et contient au moins deux 5-Sylow distincts engendrés par les 5-cycles $(1\ 2\ 3\ 4\ 5)$ et $(1\ 3\ 2\ 4\ 5)$. D'après I) h) le groupe $\mathcal{A}_5$ est simple.

II) a) **Remarque**. Supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Alors si τ_1 et τ_2 sont deux éléments de H qui coïncident en un point i, ils sont égaux. En effet si $\tau_1(i) = \tau_2(i)$ alors $\tau_2^{-1}\tau_1(i) = i$. De plus $\tau_2^{-1}\tau_1$ appartient à H donc par hypothèse $\tau_2^{-1}\tau_1 = \mathrm{id}$, *i.e.* $\tau_1 = \tau_2$.

Raisonnons par l'absurde : supposons qu'aucun élément non trivial de H n'a de point fixe, *i.e.* supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$.

- ◇ Montrons dans un premier temps qu'aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre $\geqslant 3$. Raisonnons par l'absurde : supposons qu'il existe τ dans H tel que la décomposition de τ en produit de cycles disjoints contient un cycle d'ordre $\geqslant 3$ alors on peut écrire

$$\tau = (a_1\ a_2\ a_3\ \ldots)(b_1\ b_2\ \ldots)\ldots$$

Puisque $n \geqslant 6$ il existe σ dans $\mathcal{A}_n$ tel que $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ et $\sigma(a_3) \neq a_3$. Alors

$$\sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ \ldots)(\sigma(b_1)\ \sigma(b_2)\ \ldots)\ldots$$

Ainsi $\sigma\tau\sigma^{-1}(a_1) = \tau(a_1) = a_2$. À noter que $\sigma\tau\sigma^{-1}$ appartient à H car H est distingué. La remarque qui précède assure donc que $\sigma\tau\sigma^{-1} = \tau$. Mais $\sigma\tau\sigma^{-1}(a_2) = \sigma(a_3) \neq a_3$ et $a_3 = \tau(a_2)$ donc $\sigma\tau\sigma^{-1}(a_2) \neq \tau(a_2)$: contradiction. Ainsi aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre $\geqslant 3$. Les éléments de H sont donc des produits de transpositions disjointes.
- ◇ Considérons un élément τ de H. D'après ce qui précède τ est un produit de transpositions disjointes. À noter que si τ est une double transposition alors elle laisse fixe un élément ce qui est contraire à l'hypothèse. Ainsi τ s'écrit

$$\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\ldots$$

Soit $\sigma = (a_1\ a_2)(a_3\ a_5)$. Alors on a

$$\sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\ldots$$

D'une part $\sigma\tau\sigma^{-1}(a_2) = \tau(a_2)$ donc $\sigma\tau\sigma^{-1} = \tau$ (cf Remarque). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction.

Le groupe H contient donc au moins un élément non trivial qui possède un point fixe.

II) b) Soit τ un élément de $\mathrm{H} \setminus \{\mathrm{id}\}$ pour lequel il existe $1 \leqslant i \leqslant n$ tel que $\tau(i) = i$ (l'existence d'un tel τ est assurée par II) a)). Ainsi τ appartient à $\mathrm{G}_i \cap \mathrm{H}$ qui est un sous-groupe distingué de G_i. Or G_i est isomorphe à $\mathcal{A}_{n-1}$ donc l'hypothèse de récurrence implique que G_i est simple donc ou bien $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$ ou bien $\mathrm{G}_i \cap \mathrm{H} = \{\mathrm{id}\}$. Or τ est un élément non trivial de $\mathrm{G}_i \cap \mathrm{H}$ donc $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$, c'est-à-dire G_i est inclus dans H.

Par ailleurs pour tout σ dans $\mathcal{S}_n$ on a $\sigma \mathrm{G}_i \sigma^{-1} = \mathrm{G}_{\sigma(i)}$ d'où $\mathrm{G}_i \subset \mathrm{H}$ donc $\mathrm{G}_{\sigma(i)} = \sigma \mathrm{G}_i \sigma^{-1} \subset \sigma \mathrm{H} \sigma^{-1} = \mathrm{H}$. Autrement dit pour tout $1 \leqslant j \leqslant n$ on a l'inclusion $\mathrm{G}_j \subset \mathrm{H}$.

II) c) Bien sûr $\mathrm{H} \subset \mathcal{A}_n$ donc pour montrer que $\mathcal{A}_n = \mathrm{H}$ il suffit de montrer que $\mathcal{A}_n \subset \mathrm{H}$. Considérons un élément g de $\mathcal{A}_n$. C'est un produit d'un nombre pair de transpositions, il s'écrit donc

$$g = t_1 t_2 \ldots t_k$$

où chaque t_j est un produit de deux transpositions. Le support de chaque t_j contient au plus quatre éléments donc t_j appartient à G_i pour un i extérieur à ce support. Par suite $\mathcal{A}_n \subset \mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n$. Mais $\mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n \subset \mathrm{H}$ (cf II) b)). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$.

II) d) Le groupe $\mathcal{A}_5$ est simple (I)i)). Pour $n \geqslant 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (cf II) c)).

Exercice 110

Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_2)$ le groupe des matrices à coefficients dans le corps à deux éléments et de déterminant 1.

1. Quel est l'ordre de G ? Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
2. Soit X l'ensemble des 2-Sylow de G. Donner la liste de ses éléments.

   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}$$

   Montrer par un calcul direct que cette action est transitive.

   Quel est le stabilisateur de

   $$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\} ?$$

3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.

   Montrer que

   $$\phi \colon \mathrm{G} \to \mathcal{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.

Solution 110

1. Déterminons l'ordre de G. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de G. Nous avons $ad + bc = \overline{1}$ donc

   — ou bien $ad = \overline{1}$ et $bc = \overline{0}$;
   — ou bien $ad = \overline{0}$ et $bc = \overline{1}$.

   On a $ad = \overline{1}$ et $bc = \overline{0}$ si et seulement si $(a, b, c, d) = (1, 0, 1, 1)$ ou $(a, b, c, d) = (1, 1, 0, 1)$ ou $(a, b, c, d) = (1, 0, 0, 1)$ ce qui donne 3 possibilités.

   De même $ad = \overline{0}$ et $bc = \overline{1}$ donne 3 possibilités.

   Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?

   Soient n_2 le nombre de 2-Sylow de G et n_3 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \qquad n_2 | 3$$

et

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3|2$$

Par conséquent $n_3 = 1$, *i.e.* G contient un unique 3-Sylow qui est donc distingué dans G. Le seul sous-groupe d'ordre 3 est constitué de l'identité, de $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $D^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Les éléments d'ordre 2 sont

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

2. Soit X l'ensemble des 2-Sylow de G. La liste des éléments de X est : $\{\langle A\rangle, \langle B\rangle, \langle C\rangle\}$.
   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \,|\, h \in S\}$$

   Montrons par un calcul direct que cette action est transitive :

   $$B \cdot \langle A\rangle = \langle C\rangle \qquad A \cdot \langle C\rangle = \langle B\rangle \qquad C \cdot \langle B\rangle = \langle A\rangle$$

   Quel est le stabilisateur de

   $$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}?$$

   Déterminons le stabilisateur de $\langle A\rangle$. C'est un sous-groupe de G dont l'ordre divise $|\mathrm{G}|$. Il contient Id et A mais ni B, ni C. Par ailleurs $B \cdot \langle A\rangle = \langle C\rangle$. Ce stabilisateur est donc $\langle A\rangle$.
3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.
   Montrer que

   $$\phi\colon \mathrm{G} \to \mathcal{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.
   Puisque G agit sur X le morphisme ϕ est un morphisme de groupes. Il est injectif car

   $$\begin{aligned} \ker \phi &= \{g \in \mathrm{G} \,|\, \phi(g) = \mathrm{id}_X\} \\ &= \{g \in \mathrm{G} \,|\, g \cdot S = S \quad \forall S \in X\} \\ &= \bigcap_{S \in X} \mathrm{G}_S \\ &= \{e_{\mathrm{G}}\}. \end{aligned}$$

   Comme $\mathcal{S}_X$ et G ont même ordre (6) nous obtenons que ϕ est un isomorphisme.

Exercice 111

Montrer que $\mathcal{S}_4$ possède trois 2-sous-groupes de Sylow isomorphes à D_8.

Solution 111

Le groupe $\mathcal{S}_4$ est d'ordre $24 = 2^3 \times 3$. Par ailleurs D_8 est le groupe des isométries du plan qui conservent un carré donc $\mathrm{D}_8 \subset \mathcal{S}_4$.

Soit n_2 le nombre de 2-Sylow de $\mathcal{S}_4$. Le groupe D_8 est l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathcal{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation $(1\ 2\ 3\ 4)$. Notons que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathcal{S}_4$. Il y a donc 3 sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathcal{S}_4$.

Exercice 112

Soit G un groupe. Soit p un nombre premier divisant $|\mathrm{G}|$.

Montrer que si H est un p-sous-groupe de G distingué dans G, alors H est contenu dans tout p-sous-groupe de Sylow de G.

Solution 112

Si H est un p-sous-groupe de G, il existe un p-Sylow de G qui contient H. Puisque $H \triangleleft G$ et que les p-Sylow sont conjugués entre eux, H se trouve dans tous les p-Sylow de G.

Exercice 113

Montrer qu'un groupe d'ordre 56 n'est pas simple.

Solution 113

Soit G un groupe d'ordre $56 = 2^3 \times 7$. Soit n_2 le nombre de 2-Sylow et n_7 le nombre de 7-Sylow.

D'après les théorèmes de Sylow

$$n_2 \equiv 1 \pmod 2 \qquad\qquad n_2|7$$

$$n_7 \equiv 1 \pmod 7 \qquad\qquad n_7|8$$

Par conséquent $n_2 \in \{1,\, 7\}$ et $n_7 \in \{1,\, 8\}$.

Si $n_7 = 1$, alors d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Supposons que $n_7 \neq 1$, alors $n_7 = 8$ et G compte huit sous-groupes d'ordre 7, c'est-à-dire déjà $8(7-1) = 48$ éléments d'ordre 7 (remarque : $7-1 =$ nombre d'éléments non triviaux d'un sous-groupe d'ordre 7). En ajoutant l'élément neutre nous avons donc "listé" 49 éléments du groupe G. Nous allons les noter $g_1 = e,\, g_2,\, \ldots,\, g_{49}$. Supposons que $n_2 = 7$. Soit S un 2-Sylow de G ; il est d'ordre 8. Notons $e,\, h_2,\, \ldots,\, h_8$ ses éléments. Pour des raisons d'ordre les h_i n'appartiennent pas $\{g_1,\, g_2,\, \ldots,\, g_{49}\}$. Donc G contient les éléments distincts $g_1,\, g_2,\, \ldots,\, g_{49},\, h_2,\, h_3,\, \ldots,\, h_8$; en particulier $|G| \geqslant 49 + 7 = 56$. Par hypothèse $n_2 = 7$ donc G contient un 2-Sylow T distinct de S. Soit k dans $T \smallsetminus S$. Pour des raisons d'ordre k n'appartient pas $\{g_1,\, g_2,\, \ldots,\, g_{49}\}$. Par suite G contient les éléments distincts $g_1,\, g_2,\, \ldots,\, g_{49},\, h_2,\, h_3,\, \ldots,\, h_8,\, k$. En particulier $|G| \geqslant 49 + 7 + 1 = 57$: contradiction. Par conséquent $n_2 \neq 7$ et $n_2 = 1$; d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Exercice 114

Montrer qu'un groupe d'ordre pq, où p et q sont premiers et distincts, ne peut être simple.

Solution 114

Soit G un groupe d'ordre pq. Quitte à renommer p et q nous pouvons supposer que $p > q$. Soit n_p le nombre de p-Sylow de G.

Les théorèmes de Sylow assurent que $n_p \equiv 1 \pmod p$ et n_p divise q, autrement dit que $n_p \equiv 1 \pmod p$ et $n_p \in \{1,\, q\}$. Mais comme $p > q$, $q \not\equiv 1 \pmod p$. Par suite $n_p = 1$, *i.e.* il y a un seul p-Sylow dans G qui est un sous-groupe d'ordre p distingué dans G et propre. Il s'en suit que G n'est pas simple.

Exercice 115

Soit $G = SL(2, \mathbb{F}_3)$ le groupe des matrices 2×2 de déterminant égal à 1 et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

1. Montrer que G est d'ordre 24.
2. Quel est l'ordre des éléments $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de G ?
3. Combien G a-t-il de 3-sous-groupes de Sylow ?
4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.
5. Montrer que G est produit semi-direct de H par un sous-groupe K d'ordre 3.
6. Montrer que le centre de $Z(G)$ de G est égal à $\{\mathrm{id},\, -\mathrm{id}\}$.
7. Montrer que $G/Z(G) \simeq \mathcal{A}_4$ (rappelons que les éléments $(1\ 2\ 3)$, $(1\ 2)(3\ 4)$ et $(1\ 3)(2\ 4)$ engendrent le groupe $\mathcal{A}_4$).

Solution 115

1. Montrons que G est d'ordre 24.

   Une matrice de G s'écrit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = \overline{1}$ et a, b, c et d dans $\mathbb{Z}/3\mathbb{Z}$. Cela donne 24 cas possibles pour M.

2. Les ordres cherchés sont des diviseurs de 24 bien sûr. La matrice $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 6. Les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sont d'ordre 3.

3. Soit n_3 le nombre de 3-Sylow de G qui est d'ordre $24 = 2^3 \times 3$. Notons que les 3-Sylow sont donc d'ordre 3. Les théorèmes de Sylow assurent que $n_3 \equiv 1 \pmod 3$ et que n_3 divise $2^3 = 8$. Il s'en suit que $n_3 \in \{1, 4\}$. D'après 2. il y a au moins deux sous-groupes de G d'ordre 3. Par conséquent $n_3 = 4$.

4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.

   Vérifions dans un premier temps que H est d'ordre 8. En effet $A^2 = B^2 = -\mathrm{id}$ donc A et B sont d'ordre 4. Posons $C = AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. On vérifie que

   $$\mathrm{H} = \big\{\mathrm{id},\, -\mathrm{id},\, A,\, -A,\, B,\, -B,\, C,\, -C\big\}$$

   (le groupe H est le groupe des quaternions).

   Soit $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors $N^{-1} = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}$.

   Posons $M = NAN^{-1}$ et $L = NBN^{-1}$. Remarquons que si x appartient à $\mathbb{Z}/3\mathbb{Z}$ et $x \neq \overline{O}$, alors $x^2 = \overline{1}$.

   Un calcul montre que

   $$M = \begin{pmatrix} bd + ac & -(a^2 + b^2) \\ (c^2 + d^2) & -(bd + ac) \end{pmatrix}$$

   Comme N appartient à G, nous avons $ad - bc = \overline{1}$.

   Si $a = \overline{0}$, alors $-bc = \overline{1}$ et $b = -c$. Si $d = \overline{0}$, alors $M = A$ appartient à H. Si $d \neq \overline{0}$, alors $M = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -C$ ou $M = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = -M$; dans les deux cas M appartient à H.

   Si maintenant $abcd \neq \overline{0}$, alors $a = -d$ et $b = c$ donc $M = -A$ appartient à H.

   On démontre de manière analogue que L appartient à H. Ainsi H est distingué dans G. Or H est un 2-Sylow de G. Par suite il n'y a qu'un seul 2-Sylow dans G puisque par conjugaison à partir d'un 2-Sylow on obtient tous les 2-Sylow. Or les 2-Sylow sont les sous-groupes d'ordre 8 de G. Il y a donc un unique sous-groupe d'ordre 8 dans G qui est H.

5. Montrons que G est produit semi-direct de H par un sous-groupe K d'ordre 3.

   Soit K l'un des sous-groupes d'ordre 3 de G. Nous avons les propriétés suivantes : $\mathrm{H} \cap \mathrm{K} = \{e\}$, H est distingué dans G et $3 \times 8 = 24$. Il s'en suit que G est un produit semi-direct de H par K.

   Nous avons $\mathrm{G} = \mathrm{H} \rtimes_\rho \mathrm{K}$ où $\rho \colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ est tel que $\rho(k)$ est l'automorphisme intérieur associé à l'élément $k \in \mathrm{K}$.

6. Montrons que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.

   Un élément M de G appartient à $Z(\mathrm{G})$ si en particulier $MA = AM$ et $MB = BM$.

   Or $AM = MA$ si et seulement si

   $$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

   et $BM = MB$ si et seulement si

   $$\begin{pmatrix} a+b & b+d \\ a+c & b-d \end{pmatrix} = \begin{pmatrix} a+b & a-b \\ c+d & c-d \end{pmatrix}.$$

   Ces deux égalités conduisent à $a = d$, $b = -c$, $b + d = a - b$, $a = d$ et $b = c$, soit à $a = d$ et $b = c = 0$, *i.e.* à $M = \pm\mathrm{id}$. Par suite $Z(\mathrm{G}) = \{\mathrm{id}, \mathrm{id}\}$.

7. Montrons que ${}^{\mathrm{G}}\!\diagup_{Z(\mathrm{G})} \simeq \mathcal{A}_4$.

   Considérons ici G comme produit semi-direct de H par K. Définir un morphisme φ de G dans $\mathcal{A}_4$ c'est définir φ sur H et K en respectant l'action de K sur H. Définir φ sur H c'est le définir sur les générateurs A et B en s'assurant que leurs images vérifient les mêmes relations, c'est-à-dire $A^2 = B^2 = (AB)^2$. On vérifie que φ défini par

$$\varphi(A) = (1\ 2)(3\ 4) \qquad \varphi(B) = (1\ 3)(2\ 4) \qquad \varphi(C) = (1\ 2\ 3)$$

   convient et que $\ker\varphi = \{\mathrm{id}, -\mathrm{id}\}$. Par suite ${}^{\mathrm{G}}\!\diagup_{Z(\mathrm{G})} = {}^{\mathrm{G}}\!\diagup_{\ker\varphi} \simeq \mathcal{A}_4$.

Exercice 116

Si G est un groupe, on peut faire agir G par conjugaison sur lui-même.

(1) Montrer que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

(2) (i) Si G est un p-groupe, p premier, montrer que le centre de G n'est pas réduit à $\{1\}$.

(ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!\diagup_{Z(\mathrm{G})}$ soit cyclique. Montrer qu'alors G est abélien.

(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Solution 116

(1) Montrons que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.
C'est la définition du centre :

$$Z(\mathrm{G}) = \{x \in \mathrm{G} \,|\, gxg^{-1} = x \text{ pour tout } g \in \mathrm{G}\}.$$

(2) (i) Si G est un p-groupe, p premier, montrons que le centre de G n'est pas réduit à $\{1\}$.
Notons Ω_i, $i \in I$, les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|\mathrm{G}|$ chaque $|\Omega_i|$ est une puissance de p distincte de 1. En écrivant G comme une union disjointe d'orbites on obtient

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_i |\Omega_i|$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Ceci montre que $|Z(\mathrm{G})| \neq 1$.

(ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!\diagup_{Z(\mathrm{G})}$ soit cyclique. Montrons qu'alors G est abélien.
Par hypothèse il existe un élément a de G dont la classe $\overline{a} \in {}^{\mathrm{G}}\!\diagup_{Z(\mathrm{G})}$ engendre ${}^{\mathrm{G}}\!\diagup_{Z(\mathrm{G})}$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(\mathrm{G})$. Puisque

$$a^k h \cdot a^{k'} h' = a^{k+k'} h h' = a^{k+k'} h' h = a^{k'} h' a^k h$$

le groupe G est aélien.

(3) Montrons que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.
Chacun des coefficients $*$ est un élément arbitraire de $\mathbb{F}_p$ d'où p^3 choix possibles ; de plus

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas d'où le résultat.

Exercice 117

Soit G un groupe fini d'ordre $|G| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $S \subset G$ un p-SYLOW et H un sous-groupe de G. Montrer qu'il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-SYLOW de H.

Solution 117

On a $|G| = p^a m$ et $|H| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Notons que $g' \in \mathrm{Stab}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble X est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal p^c pour un certain $c \leqslant b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |H| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu.

Exercice 118

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}(n, \Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-SYLOW de $\mathrm{GL}(n, \mathbb{F}_p)$.

Solution 118

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathcal{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |G|$ convient. De plus le groupe symétrique $\mathcal{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathcal{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.

(2) Le cardinal de $\mathrm{GL}(n, \mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1}) = p^{1+2+\dots+(n-1)}m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.

Exercice 119

Supposons qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente six 5-SYLOW.

b) Montrer que G contient dix 3-SYLOW. Montrer que deux 3-SYLOW distincts ne peuvent pas contenir un même élément $g \neq e_G$ (Indication : considérer les ordres possibles pour le centralisateur de g, observer qu'un groupe d'ordre 18 admet un unique 3-SYLOW).

c) Conclure.

Solution 119

a) Montrons que G contient trente six 5-SYLOW. Pour tout premier p qui divise $|G|$ notons n_p le nombre de p-SYLOW de G. Les théorèmes de SYLOW assurent que n_5 divise 36 et $n_5 \equiv 1 \pmod 5$. Ceci implique que n_5 appartient à $\{1, 6, 36\}$. Puisque par hypothèse G est simple on ne peut avoir $n_5 = 1$ (sinon l'unique 5-SYLOW serait distingué dans G). Il en résulte que n_5 appartient à $\{6, 36\}$. Supposons que $n_5 = 6$. Alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-SYLOW induit un morphisme non trivial $G \to \mathcal{S}_6$. Le groupe G étant par hypothèse simple, le noyau de ce morphisme est trivial, *i.e.* ce morphisme est injectif. Le morphisme $G \to \mathbb{Z}/2\mathbb{Z}$ donné par la signature a nécessairement un noyau trivial donc G est un sous-groupe de $\mathcal{A}_6$. D'une part $|\mathcal{A}_6| = \frac{|\mathcal{S}_6|}{2} = \frac{6!}{2} = 360$, d'autre part $|G| = 180$, autrement dit G est d'indice 2 dans $\mathcal{A}_6$. Le groupe G est donc un sous-groupe distingué non trivial et propre de $\mathcal{A}_6$: contradiction avec le fait que $\mathcal{A}_6$ est simple. Par conséquent $n_5 = 36$.

b) Montrons que G contient dix 3-SYLOW. Pour tout premier p qui divise $|G|$ notons n_p le nombre de p-SYLOW de G. Les théorèmes de SYLOW assurent que n_3 divise 20 et $n_3 \equiv 1 \pmod 3$. Ceci implique que n_3 appartient à $\{1, 4, 10\}$. Puisque par hypothèse G est simple on ne peut avoir $n_3 = 1$ (sinon l'unique 3-SYLOW serait distingué dans G). Si n_3 était égal à 4, on en déduirait comme au a) un morphisme injectif de G dans $\mathcal{S}_4$ ce qui est impossible car $180 = |G| > |\mathcal{S}_4| = 4! = 24$. Ainsi $n_3 = 10$.

Montrons que deux 3-SYLOW distincts ne peuvent pas contenir un même élément $g \neq e_G$.
Soient S et T deux 3-SYLOW de G distincts. Soit $g \in S \cap T$. Notons $Z = \{x \in G \mid xg = gx\}$ le centralisateur de g dans G. Supposons que $g \neq e_G$. Un groupe d'ordre 9 étant abélien, Z contient S et T. Par conséquent $|Z| \in \{18, 36, 45, 90\}$. L'action transitive de G sur G/Z induit un morphisme injectif de G vers $\mathcal{S}_{G/Z}$. Or $|G| = 180$ et $|\mathcal{S}_{G/Z}| \in \{2, 4! = 24, 5! = 120, 10!\}$ donc $\left|\mathcal{S}_{G/Z}\right| = 10!$ et $|Z| = 18$. Ainsi S et T sont des

3-Sylow de Z et un groupe d'ordre 18 admet un unique 3-Sylow d'où $S = T$: contradiction. Finalement $S \cap T = \{e_{\mathrm{G}}\}$.

c) D'après a) le groupe G contient exactement $36 \times 4 = 144$ éléments d'ordre 5.

D'après b) le groupe G contient dix 3-Sylow dont les intersections deux à deux sont triviales. Par suite il y a dans G exactement $10 \times 8 = 80$ éléments distincts de e_{G} d'ordre divisant 9.

Ainsi G possède au moins $144 + 80 = 224 > 180$ éléments distincts : contradiction.

Il n'existe donc pas de groupe simple d'ordre 180.

Exercice 120

Expliciter les sous-groupes de Sylow des groupes alternés $\mathcal{A}_4$ et $\mathcal{A}_5$.

Solution 120

Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.

Les théorèmes de Sylow assurent que

— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;

— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.

Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. Si c'est 4 l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathcal{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathcal{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_5$ ne contient pas d'élément d'ordre 4. En effet les éléments d'ordre 4 du groupe symétrique $\mathcal{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de $\{1, 2, 3, 4, 5\}$. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à $\{\mathrm{e}\}$. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.

Exercice 121

Expliciter les sous-groupes de Sylow des groupes diédraux D_8 et D_{10}.

Solution 121

i) Déterminons les sous-groupes de Sylow du groupe D_8. Le groupe D_8 est d'ordre $2^3 = 8$. Les 2-Sylow sont d'ordre 2^3, il n'y en a donc qu'un, c'est D_8.

ii) Déterminons les sous-groupes de Sylow du groupe D_{10}. Le groupe D_{10} est le groupe des isométries du plan qui conservent un pentagone régulier, il est d'ordre $2 \times 5 = 10$.

Soit n_2 le nombre de ses 2-Sylow, *i.e.* le nombre de ses sous-groupes d'ordre 2. D'après les théorèmes de Sylow $n_2 \equiv 1 \pmod 2$ et n_2 divise 5. Ainsi $n_2 \in \{1, 5\}$. Par ailleurs les sous-groupes de D_{10} engendrés par les cinq symétries par rapport aux médiatrices de chacun des côtés du pentagone sont cinq groupes d'ordre 2. Il s'en suit que $n_2 = 5$.

Soit n_5 le nombre de 5-Sylow de D_{10}, *i.e.* le nombre de sous-groupes d'ordre 5 de D_{10}. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \pmod 2$ et n_5 divise 2. Il n'y a donc qu'un unique 5-Sylow, le sous-groupe engendré par la rotation d'angle $\frac{2\pi}{5}$ dont le centre est le centre du pentagone.

Exercice 122

a) Quel est l'ordre d'un p-Sylow de $\mathcal{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathcal{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire

$$(p-1)! \equiv -1 \bmod p.$$

Solution 122

a) L'ordre de $\mathcal{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathcal{S}_p$ est d'ordre p.

b) Pour déterminer le nombre de p-Sylow de $\mathcal{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathcal{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \dots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \dots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \dots\ \sigma(p)) = (s(1)\ s(2)\ \dots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathcal{S}_p$ car ${\mathcal{S}_p}/{C}$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathcal{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathcal{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 123

On cherche à montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathcal{A}_5$.

b) Montrer que $\mathcal{A}_5$ est simple.

c) Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geqslant 1$ et m non divisible par p. Notons n_p le nombre de p-Sylow de G. Montrer que $|\mathrm{G}|$ divise $n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

e) En déduire que G contient un sous-groupe d'ordre 12.

f) Conclure.

Solution 123

a) Faisons la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif.

Les 60 éléments de $\mathcal{A}_5$ sont les suivants :

- l'identité d'ordre 1 qui forme une classe de conjugaison ;

- les double transpositions $(a\ b)(c\ d)$ où $\{a, b, c, d\}$ est de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2 et elles forment une classe de conjugaison ;
- les 3-cycles $(a\ b\ c)$ où $\{a, b, c\}$ est de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3 et forment une classe de conjugaison ;
- les 5-cycles $(a\ b\ c\ d\ e)$ où $\{a, b, c, d, e\}$ est de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5 et forment deux classes de conjugaison : celle de $(1\ 2\ 3\ 4\ 5)$ et $(2\ 1\ 3\ 4\ 5)$.

Nous avons bien énuméré tous les éléments de $\mathcal{A}_5$: $1 + 15 + 20 + 24 = 60$.

b) Montrons que $\mathcal{A}_5$ est simple. Soit $\mathrm{H} \neq \{e\}$ un sous-groupe distingué de $\mathcal{A}_5$. Puisque H est distingué, H est réunion de classes de conjugaison dans $\mathcal{A}_5$. Comme aucun des entiers $1+15 = 16$, $1+12 = 13$, $1+24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 20 + 15 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$ ne divise $60 = |\mathcal{A}_5|$, le théorème de LAGRANGE assure que H contient nécessairement toutes les classes de conjugaison de $\mathcal{A}_5$, donc $\mathrm{H} = \mathcal{A}_5$.

c) Regardons l'action transitive de G par conjugaison sur l'ensemble Syl_p de ses p-SYLOW. Comme G est simple $n_p > 1$. On obtient donc un morphisme non trivial $\mathrm{G} \to \mathcal{S}_{\mathrm{Syl}_p} \simeq \mathcal{S}_{n_p}$. Puisque G est simple ce morphisme est injectif. Il en résulte que $|\mathrm{G}|$ divise $|\mathcal{S}_{n_p}| = n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrons que le nombre de 2-SYLOW de G est égal à 5 ou à 15.

Soit n_2 le nombre de 2-SYLOW. Les théorèmes de SYLOW assurent que n_2 est impair et divise 15 ; par suite n_2 appartient à $\{1, 3, 5, 15\}$. Le groupe G étant simple, $n_2 \neq 1$, *i.e.* n_2 appartient à $\{3, 5, 15\}$. Le groupe G est d'ordre $2^2 \cdot 15$; d'après le c) $|\mathrm{G}|$ divise $n_2!$ donc $n_2 \neq 3$. Ainsi n_2 vaut 5 ou 15.

e) Montrons que G contient un sous-groupe d'ordre 12.

Supposons dans un premier temps que $n_2 = 5$; alors le normalisateur d'un 2-SYLOW de G est de cardinal $60/5 = 12$ d'où le résultat.

Supposons désormais que $n_2 = 15$. Montrons qu'il existe deux 2-SYLOW distincts S et T tels que $|\mathrm{S}\cap\mathrm{T}| = 2$. Sinon on aurait exactement $15 \cdot 3 + 1 = 46$ éléments d'ordre divisant 4. De plus les théorèmes de SYLOW assurent que $n_5 = 6$ donc que G contient $6 \cdot 4 = 24$ éléments d'ordre 5. Ainsi d'une part G contient au moins $46 + 24 = 70$ éléments et d'autre par $|\mathrm{G}| = 60$: contradiction. On dispose donc de deux 2-SYLOW distincts S et T tels que $\mathrm{S} \cap \mathrm{T} = \{e, g\}$ avec g d'ordre 2. Désignons par H le centralisateur de g dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6. Ainsi $|\mathrm{H}|$ appartient à $\{12, 20, 60\}$. Si $|\mathrm{H}| = 20$, alors l'action transitive de G sur G/H induit un morphisme injectif $\mathrm{G} \to \mathcal{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathcal{S}_3$: contradiction. Si $|\mathrm{H}| = 60$, alors g est dans le centre de G ce qui assure que le centre $Z(\mathrm{G})$ de G est non trivial : contradiction avec le fait que G est simple. Il s'en suit que $|\mathrm{H}| = 12$.

f) Soit H le sous-groupe de G d'ordre 12 construit au e). L'action transitive de G sur G/H induit un morphisme injectif $\varphi\colon \mathrm{G} \to \mathcal{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathcal{S}_5$. Ainsi G est isomorphe à un sous-groupe d'ordre 60 de $\mathcal{S}_5$ qui est nécessairement $\mathcal{A}_5$.

Exercice 124

Soit $n \geqslant 1$. On note $\mathrm{Int}(\mathcal{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathcal{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathcal{S}_n)$ tel que ϕ transforme toute transposition en une transposition.
Montrer que ϕ est intérieur.

b) Soit $\sigma \in \mathcal{S}_n$. Déterminer le cardinal du commutant

$$Z(\sigma) = \left\{\tau \in \mathcal{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\right\}$$

de σ.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$.

d) Soit $n \geqslant 5$ tel que $\mathrm{Int}(\mathcal{S}^n) = \mathrm{Aut}(\mathcal{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathcal{S}_n$ sont conjugués.

e) En utilisant les 5-SYLOW de $\mathcal{S}_5$ montrer qu'il existe un sous-groupe H d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Soit q une puissance D'un nombre premier et $n \geqslant 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}(n, \mathbb{F}_q) \to \mathcal{S}_N$ avec $N = \frac{q^n-1}{q-1}$.

g) Construire géométriquement un sous-groupe H' d'indice 6 dans $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

h) En déduire que $\mathrm{Aut}(\mathcal{S}_6) \neq \mathrm{Int}(\mathcal{S}_6)$.

Solution 124

a) Soit $\phi \in \mathrm{Aut}(\mathcal{S}_n)$ tel que ϕ transforme toute transposition en une transposition.
Montrons que ϕ est intérieur.
Puisque tout automorphisme de $\mathcal{S}_i$ est intérieur dès que $i \leqslant 3$ (à vérifier) on peut supposer que $n \geqslant 4$.
Le groupe symétrique est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geqslant 2$. Comme τ_i et τ_j ne commutent pas si $i \neq j$ les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun noté α_1. Puisque $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ils ont nécessairement tous α_1 en commun. Écrivons $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. L'application φ étant injective $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{1, 2 \ldots, n\}$. Définissons la permutation $\alpha \in \mathcal{S}_n$ par $\alpha(i) = \alpha_i$ pour tout $1 \leqslant i \leqslant n$. Ainsi φ est la conjugaison par α et φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.

b) Soit $\sigma \in \mathcal{S}_n$. Déterminons le cardinal du commutant

$$Z(\sigma) = \{\tau \in \mathcal{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\}$$

de σ. Décomposons σ en produit de cycles à supports disjoints, k_1 cycles de longueur 1, …, k_n cycles de longueur n, avec $n = \sum_i ik_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ et donc envoyer le support d'un k-cycle sur celui d'un autre k-cycle, en respectant l'ordre cyclique du support de ces cycles pour tout k. Ainsi le commutant d'un n-cycle de $\mathcal{S}_n$ est composé des puissances de ce dernier. Finalement on obtient

$$|Z(\sigma)| = \prod_i k_i!i^{k_i}.$$

c) Montrons que si $n \neq 6$, on a $\mathrm{Int}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$. Soit φ un automorphisme de $\mathcal{S}_n$. Si τ est une transposition de $\mathcal{S}_n$, alors $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de k transpositions à supports disjoints. On a $|Z(\tau)| = |Z(\varphi(\tau))|$ ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Puisque $n \neq 6$ on a $k = 1$. D'après a) φ est donc intérieur.

d) Soit $n \geqslant 5$ tel que $\mathrm{Int}(\mathcal{S}^n) = \mathrm{Aut}(\mathcal{S}_n)$. Montrons que tous les sous-groupes d'indice n de $\mathcal{S}_n$ sont conjugués. Soit H un sous-groupe d'indice n de $\mathcal{S}_n$. L'action transitive de $\mathcal{S}_n$ sur $\mathcal{S}_n/\mathrm{H}$ induit un morphisme de groupes

$$\phi\colon \mathcal{S}_n \to \mathcal{S}_{\mathcal{S}_n/\mathrm{H}} \simeq \mathcal{S}_n.$$

Puisque $\ker\phi$ est un sous-groupe distingué de $\mathcal{S}_n$, $\ker\phi \in \{\{\mathrm{id}\}, \mathcal{A}_n, \mathcal{S}_n\}$. Le groupe $\ker\phi$ agit trivialement sur la classe de H dans $\mathcal{S}_n/\mathrm{H}$, d'où $\ker\phi \subset \mathrm{H}$. Il en résulte que $\ker\phi = \{\mathrm{id}\}$, *i.e.* que ϕ est injective. Ainsi φ appartient à $\mathrm{Aut}(\mathcal{S}_n)$. Par hypothèse il existe une permutation σ telle que ϕ soit la conjugaison par σ. Or par construction ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathcal{S}_{\mathcal{S}_n/\mathrm{H}} \simeq \mathcal{S}_n$. Enfin dans $\mathcal{S}_n$ les stabilisateurs d'un point de $\{1, 2, \ldots, n\}$ sont tous conjugués.

e) En utilisant les 5-Sylow de $\mathcal{S}_5$ montrons qu'il existe un sous-groupe H d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$. Les théorèmes de Sylow assurent que $\mathcal{S}_5$ admet un ou six 5-Sylow. Comme $\mathcal{A}_5$ est simple $\mathcal{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5 et $\mathcal{S}_5$ admet exactement six 5-Sylow. Notons X l'ensemble des 5-Sylow de $\mathcal{S}_5$. L'action de $\mathcal{S}_5$ sur X par conjugaison est transitive et induit un morphisme de groupes

$$\mu\colon \mathcal{S}_5 \to \mathcal{S}_X \simeq \mathcal{S}_6$$

dont le noyau est trivial (les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$). Le groupe $\mathrm{H} = \mu(\mathcal{S}_5) \subset \mathcal{S}_6$ est un sous-groupe d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Preuve géométrique, par récurrence sur n : l'espace projectif $\mathbb{P}^{n-1}(\Bbbk)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur $\Bbbk$ (disons $\Bbbk^n$) et d'un hyperplan projectif de dimension $n-2$, *i.e.* isomorphe à un $\mathbb{P}^{n-2}(\Bbbk)$, appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(\Bbbk) = \Bbbk^{-1} \sqcup \mathbb{P}^{n-2}(\Bbbk)$. On en déduit par récurrence la formule suivante

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + \ldots + q + 1.$$

Autre preuve : le groupe $\mathrm{PGL}(\mathbb{F}_q^n)$ agit fidèlement sur $\mathbb{P}(\mathbb{F}_q^n)$ d'où le morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathcal{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = \mathbb{F}_q^n \smallsetminus \{0\}/\mathbb{F}_q^*$ donc $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1}$. Par conséquent il existe un morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathcal{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

g) Construisons géométriquement un sous-groupe H' d'indice 6 dans $\mathcal{S}_6$ opérant transitivement sur $\{1,\,2,\,\ldots,\,6\}$.
Le groupe $\mathrm{H}' = \mathrm{PGL}(2,\mathbb{F}_5)$ vu comme sous-groupe de $\mathcal{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ n'est pas conjugué à $\mathcal{S}_5 = \mathrm{Stab}(6) \subset \mathcal{S}_6$ puisqu'il ne fixe aucun point.

h) Montrons que $\mathrm{Aut}(\mathcal{S}_6) \neq \mathrm{Int}(\mathcal{S}_6)$.
Les d), e) et g) assurent que le groupe $\mathcal{S}_6$ possède au moins un automorphisme extérieur.

Exercice 125 [Simplicité de $\mathcal{A}_n$, $g \geqslant 5$, version 2]

a) Montrer que le groupe $\mathcal{A}_5$ est simple.
b) Soit $n \geqslant 3$. Montrer que les 3-cycles engendrent $\mathcal{A}_n$.
c) Montrer que $\mathcal{A}_n$ est simple dès que $n \geqslant 5$.
d) Montrer que $\mathcal{A}_4$ n'est pas simple.
e) Soit $n \geqslant 3$. Soient a, b dans $\{1,\,2,\,\ldots,\,n\}$ et $\sigma \in \mathcal{S}_n$. Montrer que

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

f) Soit $n \geqslant 3$. Montrer que le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.
g) Soit $n \geqslant 5$. Montrer que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

Solution 125

a) Le groupe $\mathcal{A}_5$ a 60 éléments :
— le neutre ;
— 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;
— 20 éléments d'ordre 3 (3-cycles) ;
— 24 éléments d'ordre 5 (5-cycles).
Les 3-cycles sont conjugués dans $\mathcal{A}_5$ [9]. Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.
Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (respectivement 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément donc tous les 5-sous-groupes de Sylow puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.
Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|\mathrm{H}| \geqslant 15 + 20 + 1 + 36.$$

Comme $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$ on obtient $|\mathrm{H}| = 60$ et $\mathrm{H} = \mathcal{A}_5$.

b) Puisque le groupe $\mathcal{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

9. Le groupe $\mathcal{A}_5$ est 3 fois transitif sur $\{1,\,2,\,\ldots,\,5\}$, *i.e.* si a_1, a_2, a_3 sont distincts et b_1, b_2, b_3 sont distincts il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1,\,2,\,\ldots,\,5\} = \{a_1,\,a_2,\,\ldots,\,a_5\} = \{b_1,\,b_2,\,\ldots,\,b_5\}$$

et considérons $\sigma \in \mathcal{S}_5$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1,\,2,\,\ldots,\,5$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_4\ a_5)$.
Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_5$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

c) Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.

Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geqslant 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.

Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes

— $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;

— $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \,|\, \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. Alors

— $\mathrm{H}_0 \triangleleft \mathcal{A}(F)$;

— $\rho_{|F} \in \mathrm{H}_0$;

— $\rho_{|F} \neq \mathrm{id}_F$.

Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $\mathrm{H}_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ [10] ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (cf b)) on a $\mathrm{H} = \mathcal{A}_n$.

d) Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\big\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

e) Calcul direct.

f) Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite d'après e)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

g) Soit $\mathrm{H} \triangleleft \mathcal{S}_n$. Alors $\mathrm{H} \cap \mathcal{A}_n \triangleleft \mathcal{A}_n$ donc $\mathrm{H} \cap \mathcal{A}_n \in \big\{\mathrm{id}, \mathcal{A}_n\big\}$.

Si $\mathrm{H} \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathrm{H} = \mathcal{A}_n$ ou $\mathrm{H} = \mathcal{S}_n$.

Si $\mathrm{H} \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(\mathrm{H}) \subset \{1, -1\}$. Par suite $|\mathrm{H}| \leqslant 2$. Si $|\mathrm{H}| = 2$, alors $\mathrm{H} = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathcal{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$. Autrement dit σ appartient au centre de $\mathcal{S}_n$ d'où $\sigma = \mathrm{id}$ (f)) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$.

Exercice 126

Soit G un groupe d'ordre 2009.

1. Montrer que $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$ où P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. En déduire que chaque groupe d'ordre 2009 est abélien.

10. Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$, *i.e.* si $a_1, a_2, \ldots, a_{n-2}$ sont distincts et b_1, b_2, b_{n-2} sont distincts il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, b_2, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et considérons $\sigma \in \mathcal{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, n$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_{n-1}\ a_n)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ \ldots\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_n$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

2. Classifier à isomorphisme près tous les groupes d'ordre 2009.
3. Soient P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. Montrer que $\mathrm{Aut(G)} \simeq \mathrm{Aut(P)} \times \mathrm{Aut(Q)}$.
4. Montrer que
   a) si Q est cyclique, alors Aut(Q) est cyclique aussi. Quel est l'ordre de Aut(Q) quand Q est cyclique ?
   b) si Q n'est pas cyclique, alors Aut(Q) est isomorphe à $\mathrm{GL}(2, \mathbb{F}_7)$ où $\mathbb{F}_7$ est le corps à 7 éléments. Quel est l'ordre de $\mathrm{GL}(2, \mathbb{F}_7)$?

Solution 126

1. Notons que $|\mathrm{G}| = 2009 = 7^2 \times 41$. D'après le premier théorème de Sylow le groupe G possède un 41-Sylow P d'ordre 41 et un 7-Sylow Q d'ordre 49. Notons n_p le nombre de p-Sylow de G. D'après le troisième théorème de Sylow
   - n_{41} est congru à 1 modulo 41 et divise 49 donc est égal à 1 ;
   - n_7 est congru à 1 modulo 7 et divise 41 donc est égal à 1.

   Nous en déduisons que $\mathrm{P} \triangleleft \mathrm{G}$ et $\mathrm{Q} \triangleleft \mathrm{G}$.

   Nous constatons aussi que $\mathrm{P} \cap \mathrm{Q} = \{e\}$, que $\mathrm{G} = \mathrm{PQ}$ et que les deux sous-groupes dans le produit sont distingués dans G. Tout ceci revient à dire $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$.

   Reste à montrer que G est abélien. Notons que P et Q sont abéliens puisque P est d'ordre premier et que Q est d'ordre premier au carré. Par ailleurs les éléments de P commutent avec ceux de Q. Ainsi G est abélien.
2. D'après 1. tous les groupes d'ordre 2009 sont abéliens, il suffit donc pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupe non isomorphes d'ordre 2009

   $$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$$

   soit encore

   $$\mathbb{Z}/2009\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z}$$
3. **Remarque**. Si φ est un automorphisme de G, alors $\varphi(\mathrm{P}) = \mathrm{P}$ et $\varphi(\mathrm{Q}) = \mathrm{Q}$. En effet comme dans tout groupe et pour tout p premier l'image par un morphisme d'un p-élément est un p-élément et que P et Q sont les seuls 41-Sylow et 7-Sylow de G respectivement, $\varphi(\mathrm{P}) \subset \mathrm{P}$ et $\varphi(\mathrm{Q}) \subset \mathrm{Q}$. Comme φ est une bijection ces deux inclusions sont en fait des égalités.

   Il découle de la Remarque précédente que la restriction de tout automorphisme $\varphi \in \mathrm{Aut(G)}$ au sous-groupe P (respectivement Q) est un automorphisme qu'on appellera φ_P (respectivement φ_Q) de P (respectivement Q). Les automorphismes de φ_P et φ_Q ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes P et Q respectivement.

   Considérons l'application

   $$\Phi \colon \mathrm{Aut(G)} \to \mathrm{Aut(P)} \times \mathrm{Aut(Q)}, \qquad \varphi \mapsto (\varphi_\mathrm{P}, \varphi_\mathrm{Q})$$

   Remarquons que $\Phi(\mathrm{id}) = (\mathrm{id}, \mathrm{id})$. Soient φ et ϕ deux éléments de Aut(G). Alors d'une part

   $$\begin{aligned} (\varphi \circ \phi)_\mathrm{P}(\mathrm{P}) &= (\varphi \circ \phi)(\mathrm{P}) \\ &= \varphi(\phi(\mathrm{P})) \\ &= \varphi_\mathrm{P}(\phi_\mathrm{P}(\mathrm{P})) \\ &= (\varphi_\mathrm{P} \circ \phi_\mathrm{P})(\mathrm{P}) \end{aligned}$$

   et d'autre part

   $$\begin{aligned} (\varphi \circ \phi)_\mathrm{Q}(\mathrm{Q}) &= (\varphi \circ \phi)(\mathrm{Q}) \\ &= \varphi(\phi(\mathrm{Q})) \\ &= \varphi_\mathrm{Q}(\phi_\mathrm{Q}(\mathrm{Q})) \\ &= (\varphi_\mathrm{Q} \circ \phi_\mathrm{Q})(\mathrm{Q}) \end{aligned}$$

   Autrement dit Φ est un morphisme de groupes.

Montrons maintenant que Φ est un isomorphisme.

Commençons par montrer que Φ est injective. Un automorphisme φ de $\mathrm{Aut(G)}$ appartient à $\ker \Phi$ si et seulement si $\varphi_{\mathrm{P}} = \mathrm{id}_{\mathrm{P}}$ et $\varphi_{\mathrm{Q}} = \mathrm{id}_{\mathrm{Q}}$. Or tout élément de G s'écrit sous la forme xy avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. Ainsi

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi_{\mathrm{P}}(x)\varphi_{\mathrm{Q}}(y) = \mathrm{id}_{\mathrm{P}}(x)\mathrm{id}_{\mathrm{Q}}(y) = xy.$$

Montrons que Φ est surjective. Soient φ_1 dans $\mathrm{Aut(P)}$ et φ_2 dans $\mathrm{Aut(Q)}$. Considérons l'application

$$\varphi \colon \mathrm{G} \to \mathrm{G}, \qquad\qquad xy \mapsto \varphi_1(x)\varphi_2(y)$$

avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. L'application φ est définie sans ambiguïté puisque G étant la somme directe de P et de Q chacun de ses éléments s'écrit de manière unique comme produit d'un élément de P et d'un autre de Q Montrons que φ est un automorphisme de G dont l'image sous l'action de Φ est (φ_1, φ_2).

Le fait que φ_1 et φ_2 soient des morphismes de groupes entraîne que φ est un morphisme de groupes. Il en est de même pour la surjectivité de φ. Supposons que $\varphi(xy) = 1$ pour $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. La définition de φ implique que $\varphi_1(x)\varphi_2(x) = 1$. Or $\varphi_1(x)$ appartient à P, $\varphi_2(y)$ appartient à Q et $\mathrm{P} \cap \mathrm{Q} = \{e\}$ donc $\varphi_1(x) = \varphi_2(y) = 1$. Puisque φ_1 est un automorphisme de P et φ_2 un automorphisme de Q nous obtenons $x = y = 1$. Comme $\mathrm{G} = \mathrm{PQ}$ tout élément de $\ker \varphi$ s'écrit comme produit d'un $x \in \mathrm{P}$ et d'un $y \in \mathrm{Q}$. Ainsi $\ker \varphi = \{e\}$.

Finalement φ est un automorphisme de G. Il s'ensuit de la définition de φ que $\varphi_{\mathrm{P}} = \varphi_1$ et $\varphi_{\mathrm{Q}} = \varphi_2$. Par conséquent $\Phi(\varphi) = (\varphi_1, \varphi_2)$. Ainsi Φ est surjective.

4. a) Si Q est cyclique, il est isomorphe à $\left(\mathbb{Z}/_{49\mathbb{Z}}, +\right)$. Alors $|\mathrm{Aut(Q)}| = \varphi(49) = 7 \times 6 = 42$ où φ est la fonction indicatrice d'Euler. Comme $42 = 2 \times 3 \times 7$ le théorème chinois assure que $\mathrm{Aut(Q)}$ est cyclique d'ordre 42.

   b) Supposons maintenant que Q soit non cyclique. Alors $\mathrm{Q} \simeq \left(\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}}, +\right)$. Ce dernier groupe peut aussi être considéré comme l'espace vectoriel de dimension 2 sur le corps $\mathbb{F}_7$ avec la base canonique $e_1 = (1,0)$ et $e_2 = (0,1)$. La loi externe induite par $\mathbb{F}_7$ est décrite par les identités

$$\lambda e_1 = \underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}} \qquad\qquad \lambda e_2 = \underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}$$

   avec $\lambda \in \mathbb{F}_7$, identités qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.
   Soit $\varphi \in \mathrm{Aut(Q)}$, alors

$$\begin{aligned}
\varphi(\lambda e_1) &= \varphi(\underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}}) \\
&= \underbrace{\varphi(1,0) + \varphi(1,0) + \ldots + \varphi(1,0)}_{\lambda \text{ fois}} \\
&= \lambda\varphi((1,0)) \\
&= \lambda\varphi(e_1)
\end{aligned}$$

   et

$$\begin{aligned}
\varphi(\lambda e_2) &= \varphi(\underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}) \\
&= \underbrace{\varphi(0,1) + \varphi(0,1) + \ldots + \varphi(0,1)}_{\lambda \text{ fois}} \\
&= \lambda\varphi((0,1)) \\
&= \lambda\varphi(e_2)
\end{aligned}$$

   Ainsi φ est une application linéaire. Étant bijectif $\varphi \in \mathrm{GL}(2, \mathbb{F}_7)$. Par suite $\mathrm{Aut(Q)} \subset \mathrm{GL}(2, \mathbb{F}_7)$. L'autre inclusion est claire car chaque bijection linéaire de $\mathbb{F}_7 \times \mathbb{F}_7$ est aussi un automorphisme du groupe $\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}}$. Finalement $|\mathrm{GL}(2, \mathbb{F}_7)| = (7^2 - 1)(7^2 - 7)$.

Exercice 127

1. Soit H un sous-groupe distingué de $\mathcal{S}_4$ qui contient un 4-cycle. Montrer que $\mathrm{H} = \mathcal{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathcal{S}_4$. Supposons que $\mathrm{P}_1 \cap \mathrm{P}_2$ contienne un 4-cycle. Montrer que $\mathrm{P}_1 = \mathrm{P}_2$ (indication : on montre que le normalisateur de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathcal{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$, on considère le sous-groupe engendré par $\mathrm{P}_1 \cup \mathrm{P}_2$ et on utilise 1.)
3. D'après ce qui précède un 4-cycle est dans un unique sous-groupe d'ordre 8 de $\mathcal{S}_4$. En déduire le nombre de sous-groupes d'ordre 8 de $\mathcal{S}_4$ en comptant le nombre de 4-cycles.

Solution 127

1. Les sous-groupes distingués de $\mathcal{S}_4$ sont id, $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\mathcal{A}_4$ et $\mathcal{S}_4$. Le seul de ces sous-groupes qui contient un 4-cycle est $\mathcal{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathcal{S}_4$. Si $\mathrm{P}_1 \neq \mathrm{P}_2$, alors $\mathrm{P}_1 \cap \mathrm{P}_2$ contient un 4-cycle et est donc d'ordre 4. Par conséquent $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_1 donc distingué dans P_1. De même $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_2 donc distingué dans P_2. Par suite le normalisateur N de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathcal{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$. Ainsi N est un sous-groupe de $\mathrm{P}_1 \cap \mathrm{P}_2$ d'ordre un diviseur de 24 qui est un multiple de 8 et > 8. Il en résulte que $|\mathrm{N}| = 24$ et donc que $\mathrm{N} = \mathcal{S}_4$. Ainsi $\mathrm{P}_1 \cap \mathrm{P}_2 \triangleleft \mathcal{S}_4$ et $\mathrm{P}_1 \cap \mathrm{P}_2 = \mathcal{S}_4$: absurde.
3. Déterminons le nombre de 4-cycles de $\mathcal{S}_4$. Un 4-cycle s'écrit de manière unique $(1\ i\ j\ k)$ où i, j et k sont trois entiers distincts parmi $\{2, 3, 4\}$. Il y a donc $3 \times 2 \times 1 =$ six 4-cycles dans $\mathcal{S}_4$. Soit n_2 le nombre de sous-groupes d'ordre 8. Ils sont tous isomorphes car ce sont les 2-Sylow qui sont tous conjugués. Soit k le nombre de 4-cycles dans un 2-Sylow. Nous avons donc $n_2 k = 6$ car un 4-cycle engendre un 2-groupe forcément contenu dans un 2-Sylow. De plus $k \geqslant 2$ car si c est un 4-cycle dans un sous-groupe P d'ordre 8, alors c^{-1} appartient à P. Si n_2 vaut 1 l'unique 2-Sylow contient un 4-cycle et est distingué dans $\mathcal{S}_4$ donc est $\mathcal{S}_4$: contradiction. Par suite $n_2 = 3$ et $k = 2$.

Exercice 128

Soit $n \geqslant 5$.

a) Montrer qu'un sous-groupe H d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

b) En utilisant les théorèmes de Sylow sur les 5-Sylow de $\mathcal{S}_5$ construire un sous-groupe de $\mathcal{S}_6$ d'indice 6 qui n'est pas de la forme
$$\mathcal{S}_6(i) = \{\sigma \in \mathcal{S}_6 \mid \sigma(i) = i\}$$
avec $1 \leqslant i \leqslant 6$.

Solution 128

a) Faire agir $\mathcal{S}_n$ sur $\mathcal{S}_n/\mathrm{H}$ par translation. Comme nous connaissons les sous-groupes distingués de $\mathcal{S}_n$ nous obtenons que le morphisme
$$\varphi\colon \mathrm{H} \to \mathrm{Bij}\left(\mathcal{S}_n/\mathrm{H}\right)$$
est injectif. De plus les éléments de $\varphi(\mathrm{H})$ fixent la classe H d'où le résultat.

b) Le troisième théorème de Sylow assure que $\mathcal{S}_5$ compte six 5-Sylow. Faisons agir $\mathcal{S}_5$ par conjugaison sur l'ensemble X des 5-Sylow. On obtient un morphisme de groupes
$$\varphi\colon \mathcal{S}_5 \to \mathrm{Bij}(X).$$
Le premier théorème de Sylow assure que cette action est transitive. Puisque nous connaissons les sous-groupes distingués de $\mathcal{S}_n$ nous obtenons que φ est injective. Finalement l'image de φ répond à la question.

Exercice 129

1. Soit G un groupe fini. Notons $\mathrm{Syl}_p(\mathrm{G})$ l'ensemble des p-sous-groupes de Sylowde G. Supposons que $|\mathrm{Syl}_p(\mathrm{G})| = m$. Montrons qu'il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathcal{S}_m$.
2. Soit G un groupe de cardinal 36. Montrer qu'il n'est pas simple.

Solution 129

1. D'après les théorèmes de Sylowl'action par conjugaison
$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}) \qquad\qquad (g, P) \mapsto gPg^{-1}$$
est transitive et détermine donc un morphisme non trivial $\rho\colon \mathrm{G} \to \mathrm{Bij}\big(\mathrm{Syl}_p(\mathrm{G})\big) \simeq \mathcal{S}_m$.

2. Remarquons que $|G| = 2^2 \times 3^2$. Soit n_p le nombre de p-SYLOWde G. Les théorèmes de SYLOWassurent que n_3 divise $2^2 = 4$ et que $n_3 \equiv 1 \bmod 3$, autrement dit que n_3 appartient à $\{1, 4\}$.
   Si $n_3 = 1$, alors G contient un unique 3-SYLOWqui est forcément distingué dans G ; en particulier G n'est pas simple.
   Si $n_3 = 4$, alors d'après 1. il existe un morphisme non trivial $\rho\colon G \to \mathcal{S}_4$. Puisque $|G| = 36$ ne divise pas $|\mathcal{S}_4| = 24$ ce morphisme n'est pas injectif et $\ker \rho$ est un sous-groupe distingué non trivial et propre de G.

Exercice 130

Soit G un groupe d'ordre 231.

1. Montrer que G admet un seul 7-SYLOWet un seul 11-SYLOW.
2. Montrer que si P est le 11-Sylow de G, alors P est contenu dans le centre de G (indication : on considère l'action d'un 3-SYLOWet l'action d'un 7-Sylow de G sur P par conjugaison).
3. Montrer que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G. Est-ce que ce sous-groupe d'ordre 77 est cyclique ? Justifier.
4. Montrer que G admet un sous-groupe cyclique d'ordre 33.

Solution 130

1. Montrons que G admet un seul 7-SYLOWet un seul 11-SYLOW.
   Soit n_p le nombre de p-SYLOWde G.
   Le troisième théorème de SYLOW assure que $n_7 \equiv 1 \bmod 7$ et que n_7 divise 33, soit que $n_7 = 1$.
   Le troisième théorème de SYLOW assure que $n_{11} \equiv 1 \bmod 11$ et que n_{11} divise 21, soit que $n_{11} = 1$.
2. Montrons que si P est le 11-Sylow de G, alors P est contenu dans le centre de G.
   Comme $n_{11} = 1$ nous avons $P \lhd G$. Soit Q un 3-Sylow ; il agit sur P par conjugaison.
   L'équation aux classes s'écrit $|P| = \displaystyle\sum_i \mathcal{O}_i$. Chaque orbite est de cardinal $\frac{|Q|}{|\mathrm{Stab}\mathcal{O}_i|}$ et $\frac{|Q|}{|\mathrm{Stab}\mathcal{O}_i|} \in \{1, 3\}$.
   C'est 1 si l'orbite est réduite à un point x_i tel que pour tout $g \in Q$ $gx_ig^{-1} = x_i$. Par suite
   $$|P| = |P^Q| \bmod 3$$
   où
   $$\begin{aligned} P^Q &= \{p \in P \,|\, \forall q \in Q,\, q \cdot p = p\} \\ &= \{p \in P \,|\, \forall q \in Q,\, qpq^{-1} = p\} \\ &= \{p \in P \,|\, \forall q \in Q,\, qp = pq\}. \end{aligned}$$
   Comme $|P^Q|$ divise 11 et $11 \neq 1 \bmod 3$, $P^Q = P$, *i.e.* le sous-groupe des éléments qui commutent à tous les éléments de P contient Q. De même les éléments qui commutent à tous les éléments de P contient un 7-SYLOW et bien entendu P car P est cyclique. Le sous-groupe des éléments qui commutent à tous les éléments de P est d'ordre un multiple de 3, 7 et 11, c'est donc G.
3. Montrons que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G.
   Commençons par montrer l'existence d'un tel sous-groupe. Soit Q un 7-SYLOW. Puisque $P \lhd G$ et $P \cap Q = \{\mathrm{id}\}$, PQ est un sous-groupe de G d'ordre 77. Comme $Q \lhd G$, $PQ \lhd G$.
   Montrons maintenant l'unicité. Soit H un sous-groupe de G d'ordre 77. Alors H contient un 11-SYLOW et un 7-SYLOW. Donc H = PQ. Soit p dans P d'ordre 11 et soit q dans Q d'ordre 7. Puisque $pq = qp$ (rappelons que p appartient à P et que $P \subset Z(G)$) pq est d'ordre 77 donc PQ est cyclique.
4. Montrons que G admet un sous-groupe cyclique d'ordre 33.
   Soit R un 3-SYLOW. Alors PR est un sous-groupe distingué de G d'ordre 33. En effet soient p d'ordre 11 dans P et r d'ordre 3 dans R. Puisque P est contenu dans le centre de G nous avons $pr = rp$ et pr est d'ordre 33.

Exercice 131

Rappelons que D_{2n} désigne le groupe à $2n$ éléments des isométries d'un polygone régulier à n côtés. On se propose de montrer que si G est un groupe de cardinal 70, alors G est isomorphe à l'un des groupes suivants

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Partie I

Soit G un groupe. Notons n_p le nombre de p-sous-groupes de SYLOW de G et $o(n)$ le nombre d'éléments d'ordre n.

1. Soit p un premier impair. Montrer pourquoi un groupe de cardinal $2p$ est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou D_{2p}.
2. Que valent n_2 et n_p lorsque $\mathrm{G} = \mathrm{D}_{2p}$?
   Si S et T sont deux sous-groupes de G tels que $\mathrm{S} \cap \mathrm{T} = \{e\}$, alors on considère $\mathrm{ST} = \{st \mid s \in \mathrm{S},\, t \in \mathrm{T}\}$.
3. Montrer que si S est distingué dans G, alors ST = TS est un sous-groupe de cardinal $|\mathrm{S}||\mathrm{T}|$.
4. Montrer que si S et T sont distingués dans G, alors ST est un sous-groupe isomorphe à $\mathrm{S} \times \mathrm{T}$. En déduire qu'un groupe de cardinal 35 est cyclique.

Partie II

Soit G un groupe de cardinal 70.

1. Exprimer $o(p)$ en terme de n_p et énumérer les valeurs possibles a priori pour n_2, n_5 et n_7.
2. Déduire de ce qui précède que G possède un sous-groupe K d'ordre 35. Montrer que K est distingué dans G.
3. En déduire que G contient un sous-groupe distingué $\mathrm{H} \simeq \mathbb{Z}/35\mathbb{Z}$.
4. Calculer n_2 dans le cas des quatre groupes
$$\mathbb{Z}/70\mathbb{Z} \qquad \mathrm{D}_{70} \qquad \mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad \mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}$$
   En déduire qu'ils ne sont pas isomorphes.
5. Inversement montrer en considérant les valeurs possibles de n_2 que G est isomorphe à l'un des quatre groupes
$$\mathbb{Z}/70\mathbb{Z} \qquad \mathrm{D}_{70} \qquad \mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad \mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Solution 131

Partie I

1. Si $|\mathrm{G}| = 2p$, les théorèmes de Sylow assurent l'existence d'un sous-groupe distingué H de cardinal p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et un sous-groupe d'ordre 2 disons $\mathrm{K} = \{e,\, s\}$. Soit r un générateur de H. Alors srs^{-1} appartient à H donc est égal à r^a pour un certain a. Alors d'une part $sr^a s^{-1} = r^{a^2}$ et d'autre part $r = s^{-1}r^a s$ qui se réécrit $r = sr^a s^{-1}$ puisque $s^2 = e$. On en déduit que $r^{a^2} = r$ et donc $a^2 \equiv 1 \mod p$ et donc $a \equiv \pm 1 \mod p$. Si $a = 1$, l'élément s commute avec r donc rs est d'ordre $2p$ et $\mathrm{G} \simeq \mathbb{Z}/2p\mathbb{Z}$. Si $a = -1$, alors $srs^{-1} = r^{-1}$ ce qui caractérise le groupe diédral.
2. Nous avons $n_p = 1$ (il n'y a qu'un seul p Sylow qui est distingué dans G) et $n_2 = p$ (en effet il y a p éléments d'ordre 2, les symétries).
3. Si S est distingué dans G, alors pour tout $t \in \mathrm{G}$ nous avons $\mathrm{S}t = t\mathrm{S}$ d'où l'égalité ST = TS. Si $g = st$ et $g' = s't'$, alors $gg' = sts't' = s(ts't^{-1})tt'$ appartient à ST. Si $g = st$, alors $g^{-1} = t^{-1}s^{-1}$ appartient à TS = ST. Par suite ST est bien un sous-groupe de G.
   Montrons que l'application
$$\phi\colon \mathrm{S} \times \mathrm{T} \to \mathrm{G} \qquad\qquad (s,t) \mapsto st$$
   est injective. Soient (s,t) et (s',t') dans $\mathrm{S} \times \mathrm{T}$ tels que $\phi(s,t) = \phi(s',t')$. L'égalité $\phi(s,t) = \phi(s',t')$ se réécrit $st = s't'$ dont on déduit $(s')^{-1}s = t't^{-1}$. En particulier $(s')^{-1}s = t't^{-1}$ est un élément de $\mathrm{S} \cap \mathrm{T}$; comme $\mathrm{S} \cap \mathrm{T} = \{e\}$, on obtient que $(s')^{-1}s = t't^{-1} = e$, soit que $s = s'$ et $t = t'$. Ainsi l'application ϕ est injective ; de plus son image est par définition ST. Par conséquent $|\mathrm{S} \times \mathrm{T}| = |\mathrm{ST}|$. Mais $|\mathrm{S} \times \mathrm{T}| = |\mathrm{S}| \cdot |\mathrm{T}|$ d'où $|\mathrm{S}| \cdot |\mathrm{T}| = |\mathrm{ST}|$.
4. D'une part $sts^{-1}t^{-1} = s(ts^{-1}t^{-1})$ donc $sts^{-1}t^{-1}$ appartient à S (par hypothèse $\mathrm{S} \lhd \mathrm{G}$), d'autre part $sts^{-1}t^{-1} = (sts^{-1})t^{-1}$ donc $sts^{-1}t^{-1}$ appartient à T (par hypothèse $\mathrm{T} \lhd \mathrm{G}$). Ainsi $sts^{-1}t^{-1}$ appartient à $\mathrm{S} \cap \mathrm{T} = \{e\}$, donc $sts^{-1}t^{-1} = e$ autrement dit s et t commutent. Ceci entraîne que ϕ est un morphisme ; en effet
$$\phi\big((s,t) \cdot (s',t')\big) = \phi(ss',tt') = ss'tt' = sts't' = \phi(s,t)\phi(s',t').$$
   D'après ce qui précède $\phi\colon \mathrm{S} \times \mathrm{T} \to \mathrm{ST}$ est donc un isomorphisme.

   Si $|\mathrm{G}| = 35$ le groupe contient un unique 5-Sylow $\mathrm{S} \simeq \mathbb{Z}/5\mathbb{Z}$ et un unique 7-Sylow $\mathrm{T} \simeq \mathbb{Z}/7\mathbb{Z}$. Comme ils sont tous les deux distingués dans G d'intersection triviale nous obtenons d'après les questions précédentes que
$$\mathrm{ST} = \mathrm{S} \times \mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$
   Enfin $|\mathrm{ST}| = 35 = |\mathrm{G}|$ conduit à ST = G.

Partie II

Soit G un groupe de cardinal 70.

1. Comme les p-Sylow sont de cardinal p (pour $p = 2$, 5 ou 7) ils sont deux à deux disjoints hormis l'élément e bien sûr qui est présent dans chacun d'entre eux. Ainsi si H_1, H_2, …, H_{n_p} désignent les p-Sylow de G nous avons
$$\Big|\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}\Big| = n_p(p-1)$$
Par ailleurs d'après les théorèmes de Sylow $\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}$ est l'ensemble des éléments d'ordre p. Ainsi $o(p) = n_p(p-1)$.
D'après les théorèmes de Sylow n_7 divise 10 et $n_7 \equiv 1 \bmod 7$ donc $n_7 = 1$.
D'après les théorèmes de Sylow n_5 divise 14 et $n_5 \equiv 1 \bmod 5$ donc $n_5 = 1$.
D'après les théorèmes de Sylow n_2 divise 35 et $n_2 \equiv 1 \bmod 2$ donc $n_2 \in \{1, 5, 7, 35\}$.
2. Soient S l'unique 5-Sylow de G et T l'unique 7-Sylow de G. Ils sont tous les deux distingués dans G donc $\mathrm{K} = \mathrm{ST}$ est un sous-groupe de cardinal 35 qui est automatiquement distingué dans G (on peut aussi remarquer que $[\mathrm{G} : \mathrm{K}] = 2$ donc K est distingué dans G).
3. D'après les questions qui précèdent nous avons
$$\mathrm{K} = \mathrm{ST} \simeq \mathrm{S} \times \mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}.$$
4. Désignons par $n_2(\mathrm{G})$ le nombre de 2-Sylow du groupe G.
Le groupe $\mathbb{Z}/70\mathbb{Z}$ étant abélien nous avons $n_2\big(\mathbb{Z}/70\mathbb{Z}\big) = 1$.
Le groupe D_{2n} contient n symétries d'ordre 2. Par conséquent $n_2(\mathrm{D}_{70}) = 35$. De plus si B est de cardinal impair, un 2-Sylow de $\mathrm{A} \times \mathrm{B}$ est contenu dans $\mathrm{A} \times \{e\}$ donc $n_2(\mathrm{A} \times \{e\}) = n_2(\mathrm{A})$; par suite
$$n_2\big(\mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}\big) = n_2(\mathrm{D}_{14}) = 7 \qquad\qquad n_2\big(\mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z}\big) = n_2(\mathrm{D}_{10}) = 5.$$
5. Choisissons un générateur r de $\mathrm{ST} = \mathrm{K} \simeq \mathbb{Z}/35\mathbb{Z}$ et s un élément d'ordre 2. Posons $\mathrm{R} = \{e, s\}$. Observons que $srs^{-1} = r^a$ avec $a \in \mathbb{Z}/35\mathbb{Z}$ et $a^2 = 1$. Comme $a^2 \equiv 1 \bmod 35$ équivaut par le Lemme chinois à $a^2 \equiv 1 \bmod 5$ et $a^2 \equiv 1 \bmod 7$ on a quatre solutions :
— $a \equiv 1 \bmod 35$,
— $a \equiv -1 \bmod 35$,
— $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$,
— $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$.
Intéressons-nous à chacune de ces éventualités :
— si $a \equiv 1 \bmod 35$, alors R commute avec K et $\mathrm{G} \simeq \mathrm{K} \times \mathrm{R} \simeq \mathbb{Z}/35\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/70\mathbb{Z}$.
— si $a \equiv -1 \bmod 35$, alors s commute avec S mais pas avec T ainsi S commute avec T et R donc avec le sous-groupe RT qui est d'ordre 14. Puisqu'il est non abélien RT doit être isomorphe à D_{14}. Par conséquent $\mathrm{G} \simeq \mathrm{S} \times \mathrm{RT} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathrm{D}_{14}$.
— le cas $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$ se traite de la même façon que le cas précédent et on obtient $\mathrm{G} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathrm{D}_{10}$.
— si $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$ alors $\mathrm{G} \simeq \mathrm{D}_{70}$.

Exercice 132

1. Soit G un groupe fini d'ordre n. Soit p un facteur premier de n. Soit n_p le nombre de p-Sylowde G. Montrer que si n ne divise pas $n_p!$, alors le groupe G n'est pas simple.
2. Soit G un groupe fini d'ordre n. Montrer que si n est de la forme $p^\alpha q^\beta$ et si n ne divise pas $p^\alpha!$ ou $q^\beta!$, alors G n'est pas simple.
3. Montrer qu'il n'existe pas de groupe simple d'ordre 72.

Solution 132

1. Si $n_p = 1$, alors l'unique p-Sylowde G est distingué. Sinon G opère transitivement sur l'ensemble à $n_p > 1$ éléments de ses p-Sylow. On obtient aussi un morphisme

$$\varphi\colon \mathrm{G} \to \mathcal{S}_{n_p}$$

qui n'est pas trivial (*i.e.* n'envoie pas G sur $\{\mathrm{id}\}$) car l'opération est transtive et $n_p > 1$. Puisque n ne divise pas $n_p!$, le morphisme φ ne peut être injectif. Son noyau $\ker\varphi$ est donc un sous-groupe distingué non trivial de G.

2. Supposons par exemple que n ne divise pas $q^\beta!$. D'après les théorèmes de Sylow n_p divise q^β donc est plus petit que q^β. Comme n ne divise pas $q^\beta!$ il ne divise pas non plus [11] $n_p!$ et on conclut par 1.
3. Soit G un groupe d'ordre 72. Notons que $72 = 2^3 \times 3^2$. Soit n_3 le nombre de 3-Sylow. D'après les théorèmes de Sylow d'une part n_3 divise $2^3 = 8$, d'autre part $n_3 \equiv 1 \bmod 3$. Par suite n_3 vaut 1 ou 4. Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué ; en particulier G n'est pas simple. Si $n_3 = 4$, alors 72 ne divise pas $n_3! = 24$ et G n'est pas simple d'après 1.

Exercice 133 Soit G un groupe fini simple non abélien.

1. Soit H un sous-groupe propre de G. Montrer que $|\mathrm{G}|$ divise $[\mathrm{G} : \mathrm{H}]!$ (indication : montrer que G est isomorphe à un sous-groupe du groupe alterné $\mathcal{A}_{\mathrm{G}/\mathrm{H}}$). Puisque H est distinct de G on peut même dire que G divise $\frac{1}{2}[\mathrm{G} : \mathrm{H}]!$.
2. Soit p un diviseur premier de $|\mathrm{G}|$. Désignons par n_p le nombre de p-Sylow de G. L'entier $|\mathrm{G}|$ divise alors $n_p!$.

Solution 133

1. Notons φ le morphisme de G dans $\mathcal{S}_{\mathrm{G}/\mathrm{H}}$ induit par l'action de G sur l'ensemble G/H des classes à droite de G modulo H. Le noyau de cette action est exactement l'intersection des conjugués de H dans G. C'est un sous-groupe propre de G car H l'est par hypothèse. Puisque G est simple $\ker\varphi = \{\mathrm{id}\}$, *i.e.* φ est injectif. Intéressons-nous alors au morphisme $\mathrm{sgn}\circ\varphi\colon \mathrm{G} \to \{-1,\, 1\}$ obtenu à partir de φ par composition par la signature $\mathrm{sgn}\colon \mathcal{S}_{\mathrm{G}/\mathrm{H}} \to \{-1,\, 1\}$. Si $\mathrm{sgn}\circ\varphi$ pouvait prendre la valeur -1, le groupe G possèderait un sous-groupe distingué d'indice 2 et ne serait pas simple non abélien. Par conséquent le morphisme $\mathrm{sgn}\circ\varphi$ est trivial et φ plonge donc G dans $\mathcal{A}_{\mathrm{G}/\mathrm{H}}$. En particulier $|\mathrm{G}|$ divise $|\mathcal{S}_{\mathrm{G}/\mathrm{H}}| = [\mathrm{G} : \mathrm{H}]!$.
2. Soit P un p-Sylow de G. Puisque G est simple non abélien, le normalisateur [12] $N_{\mathrm{G}}(\mathrm{P})$ de P dans G est un sous-groupe propre de G. D'après le 1. nous avons donc : $|\mathrm{G}|$ divise $[\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]!$. Les théorèmes de Sylowassure que $[\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]! = n_p!$ d'où le résultat.

4 Structure des groupes abéliens de type fini

Exercice 134

Soit G un groupe de type fini.

Un sous-groupe H de G est-il nécessairement de type fini ? Justifiez votre réponse.

Solution 134

Soit G est un groupe de type fini ; G peut contenir un sous-groupe H qui n'est pas de type fini.

Considérons le sous-groupe G de $\mathrm{GL}(2, \mathbb{Q})$ engendré par les matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Soit H le sous-groupe de G formé des matrices de G avec des 1 sur la diagonale. Raisonnons par l'absurde : supposons que H soit de type fini, *i.e.* $\mathrm{H} = \langle M_1,\, M_2, \ldots, M_r\rangle$ avec $M_i = \begin{pmatrix} 1 & m_i \\ 0 & 1 \end{pmatrix}$. Puisque $M_i^{-1} = \begin{pmatrix} 1 & -m_i \\ 0 & 1 \end{pmatrix}$

11. Si $a < b$, alors $a!$ divise $b!$.
12. dans un groupe G, le normalisateur d'une partie X est l'ensemble, noté $N_{\mathrm{G}}(X)$, des éléments g de G qui normalisent X, c'est-à-dire qui vérifient $gXg^{-1} = X$: $N_{\mathrm{G}}(X) = \left\{g \in \mathrm{G} \,|\, gXg^{-1} = X\right\} = \left\{g \in \mathrm{G} \,|\, gX = Xg\right\}$

et $M_iM_j = \begin{pmatrix} 1 & m_i + m_j \\ 0 & 1 \end{pmatrix}$, il existe un entier $N \geqslant 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}(2, \mathbb{Q})$ formé des matrices de la forme

$$\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$$

Or $A^{-N}BA^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$: contradiction ($2^N > N$). Ainsi H n'est pas de type fini alors que G l'est.

Considérons par exemple le groupe libre G sur deux générateurs a et b. Soit H le sous-groupe engendré par tous les éléments de la forme ab^n avec $n \in \mathbb{N}$. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H le nombre de b consécutifs soit toujours strictement inférieur à N. Or ab^N appartient à H : contradiction. Le sous-groupe H de G n'est donc pas de type fini.

Exercice 135

Soit G un groupe abélien.

Montrer que $T(\mathrm{G}) = \{g \in \mathrm{G} \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Donner un exemple explicite pour lequel $T(\mathrm{G})$ n'est pas un sous-groupe de G si G n'est pas abélien.

Solution 135

Soit G un groupe abélien.

Montrons que $T(\mathrm{G}) = \{g \in G \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Clairement $T(\mathrm{G})$ est contenu dans G. On a

- $o(e) = 1 < \infty$ donc $e \in T(\mathrm{G})$;
- soient g et h dans $T(\mathrm{G})$. Notons n (respectivement m) l'ordre de g (respectivement h). Par hypothèse $n < \infty$ et $m < \infty$. On a bien sûr $o(h^{-1}) = m$. Puisque G est abélien on a

$$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn}$$

  Par suite $(gh^{-1})^{mn} = (g^n)^m((h^{-1})^m)^n = e^me^n = e$. Ainsi $o(gh^{-1}) \leqslant mn < \infty$ et gh^{-1} appartient à $T(\mathrm{G})$.

Ainsi $T(\mathrm{G})$ est un sous-groupe de G.

Montrons que si G n'est pas abélien, alors $T(\mathrm{G})$ n'est pas forcément un sous-groupe de G.

Considérons $\mathrm{G} = \mathrm{O}(2)$. Soit ρ la rotation d'angle θ où θ/π est irrationnel. Alors ρ n'appartient pas à $T(\mathrm{G})$. Mais $\rho = s_2 \circ s_1$ avec s_1, s_2 réflexions ; en particulier $o(s_1) = o(s_2) = 2$ et donc s_1, s_2 appartiennent à $T(\mathrm{G})$.

Exercice 136

Soit $n \in \mathbb{N}$, $n \geqslant 2$. Trouver le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Montrer que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Solution 136

Soit $n \in \mathbb{N}$, $n \geqslant 2$. Déterminons le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} T\left(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right) &= \left\{(a, \overline{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, o(a, b) < \infty\right\} \\ &= \left\{(a, \overline{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, \exists\, k \in \mathbb{N}^*,\, o(a, b) = k\right\} \\ &= \left\{(a, \overline{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, (ka, kb) = (0, \overline{0})\right\} \\ &= \left\{(a, \overline{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, a = 0 \text{ et } b \in \mathbb{Z}/n\mathbb{Z}\right\} \\ &= \{0\} \times \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Montrons que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Soient $(1, 1)$ et $(-1, 0)$ deux éléments de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ils sont d'ordre infini mais $(1, 1) + (-1, 0) = (0, 1)$ est d'ordre fini.

Exercice 137

a) Donner un exemple de groupe abélien qui n'est pas de type fini.

b) Si p est un nombre premier, quel est le groupe sous-jacent au corps $\mathbb{F}_{p^n}$?

c) Soient n, $m \geqslant 1$ deux entiers. Posons $\delta := \text{pgcd}(n,m)$ et $\mu := \text{ppcm}(n,m)$.
Montrer que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

d) Montrer qu'un groupe abélien de type fini et de torsion est fini (ceci n'est plus vrai pour les groupes non-abéliens : voir par exemple [Calais, p. 294]).

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Solution 137

a) $(\mathbb{Q},+)$ est un groupe abélien qui n'est pas de type fini (pour le vérifier raisonner par l'absurde).

b) Soit p un nombre premier.
Si $n=1$, alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et le groupe sous-jacent est $\mathbb{Z}/p\mathbb{Z}$.
Si $n=2$, alors le groupe sous-jacent à $\mathbb{F}_{p^2}$ est $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ car $\mathbb{Z}/p^2\mathbb{Z}$ possède un élément d'ordre p^2 alors que $\mathbb{F}_{p^2}$ est de caractéristique p donc sans élément d'ordre p^2.
De même pour n quelconque le groupe sous-jacent à $\mathbb{F}_{p^n}$ est $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

c) Soient n, $m \geqslant 1$ deux entiers. Posons $\delta := \text{pgcd}(n,m)$ et $\mu := \text{ppcm}(n,m)$. Montrons que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.
Écrivons les décompositions de m et n en nombre premiers :

$$m = \prod_i p_i^{\alpha_i} \qquad\qquad n = \prod_i p_i^{\beta_i}$$

Alors

$$\delta = \prod_i p_i^{\min(\alpha_i,\beta_i)} \qquad\qquad \mu = \prod_i p_i^{\max(\alpha_i,\beta_i)}$$

D'une part

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d'autre part

$$\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

Si $\min(\alpha_i,\beta_i) = \alpha_i$, alors $\max(\alpha_i,\beta_i) = \beta_i$; réciproquement si $\min(\alpha_i,\beta_i) = \beta_i$ alors $\max(\alpha_i,\beta_i) = \alpha_i$. Par conséquent tous les α_i et β_i apparaissent une fois et une seule dans le produit

$$\prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

qui est donc isomorphe à

$$\prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d) Montrons qu'un groupe abélien de type fini et de torsion est fini.
Soit G un groupe abélien de type fini et sans torsion. Puisque G est abélien de type fini on a

$$\mathrm{G} \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

où $r \geqslant 0$, $n_j \geqslant 0$ pour tout $1 \leqslant j \leqslant s$ et n_{i+1} divise n_i pour tout $1 \leqslant i \leqslant s-1$.
De plus G est de torsion, *i.e.* tout élément est d'ordre fini. Il en résulte que $r=0$, c'est-à-dire que

$$\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

En particulier $|\mathrm{G}| = n_1 n_2 \ldots n_s < \infty$.

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Soient G un groupe abélien et $(\mathrm{H}_i)_{1\leqslant i\leqslant r}$ une famille de sous-groupes d'ordre 2 à 2 premiers entre eux. Alors ces groupes sont en somme directe dans G. En effet soit d_i l'ordre de H_i. Rappelons que dans un groupe abélien si G est d'ordre m et h d'ordre n avec n, m premiers entre eux, alors gh est d'ordre mn. Ainsi pour tout i l'ordre de tout élément de $\displaystyle\sum_{j\neq i}\mathrm{H}_j$ divise $\mathrm{ppcm}_{j\neq i}(d_j)$ donc est premier avec d_i. Il en résulte que nous avons pour tout i

$$\mathrm{H}_i\cap\Big(\sum_{j\neq i}\mathrm{H}_j\Big)=\{1\}$$

Par conséquent les H_i, $1\leqslant i\leqslant r$, sont en somme directe.

D'après ce qui précède les différents p-Sylow d'un groupe abélien fini G sont en somme directe. L'égalité des cardinaux assure que G est la somme directe de ses sous-groupes de Sylow.

Exercice 138

Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G.

Solution 138

Soit G un groupe abélien fini. Montrons qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G. Le théorème de structure assure que

$$\mathrm{G}\simeq\mathbb{Z}/d_1\mathbb{Z}\times\mathbb{Z}/d_2\mathbb{Z}\times\ldots\times\mathbb{Z}/d_r\mathbb{Z}$$

où d_i divise d_{i+1} pour tout $1\leqslant i\leqslant r-1$.

L'exposant de G est d_r et $(0,0,\ldots,0,1)$ est d'ordre d_r.

Exercice 139

Montrer qu'il existe exactement 20 groupes abéliens d'ordre $\leqslant 15$ à isomorphisme près. On donnera leur forme canonique successivement sous forme "facteurs invariants" et sous forme "facteurs élémentaires".

Solution 139

Il y a 15 groupes cycliques d'ordre $n\leqslant 15$. Pour chacun

- ◇ la décomposition en facteurs invariants consiste juste à écrire $\mathbb{Z}/n\mathbb{Z}$;
- ◇ la décomposition en facteurs élémentaires consiste à écrire la décomposition en facteurs premiers de n.

Par exemple

Exercice 140

a) Donner la décomposition primaire du groupe $\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$. En déduire ses facteurs invariants.

b) Donner la décomposition primaire du groupe $\mathbb{Z}/54\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$. En déduire ses facteurs invariants.

Solution 140

a) Donnons la décomposition primaire du groupe $\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$.
Notons que $8=2^3$, $12=2^2\times 3$ et $24=2^3\times 3$. Ainsi

$$\mathrm{G}\simeq\mathbb{Z}/2^3\mathbb{Z}\times\mathbb{Z}/2^2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2^3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2^3, 2^2, 3, 2^3 et 3.
Déterminons les facteurs invariants de G. Réordonnons les diviseurs élémentaires comme suit

$$\begin{array}{c} 2^2\mid 2^3\mid 2^3\\ \quad\;\; 3\mid 3\end{array}$$

Les facteurs invariants de G sont donc $2^2\times 1=4$, $2^3\times 3=24$ et $2^3\times 3=24$.
Par conséquent

$$\mathrm{G}\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}.$$

b) Donnons la décomposition primaire du groupe $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.
Notons que $54 = 2 \times 3^3$, $26 = 2 \times 13$ et $15 = 3 \times 5$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2, 3^3, 2, 13, 3 et 5.
Donnons ses facteurs invariants. On ordonne les diviseurs élémentaires comme suit

$$\begin{array}{r} 2 \mid 2 \\ 3 \mid 3^3 \\ 5 \\ 13 \end{array}$$

Les facteurs invariants de G sont donc $2 \times 3 = 6$ et $2 \times 3^3 \times 5 \times 13 = 3510$.

Exercice 141

a) Le nombre de classes de conjugaison dans $\mathcal{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?

b) Généraliser au nombre de classes de conjugaison dans $\mathcal{S}_n$.

Solution 141

a) Le nombre de classes de conjugaison dans $\mathcal{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Expliquons pourquoi. Le nombre de classes de conjugaison dans $\mathcal{S}_5$ et le nombre de groupes abéliens de cardinal 32 à isomorphisme près sont chacun en bijection avec l'ensemble des partitions de 5 (rappelons qu'une partition d'un entier est une décomposition de cet entier en une somme d'entiers strictement positifs à l'ordre près des termes).

b) Généralisons au nombre de classes de conjugaison dans $\mathcal{S}_n$. Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphismes de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathcal{S}_n$. Considérons

$$\varphi\colon P_n \to G_n \qquad (n_1, n_2, \ldots, n_r) \mapsto \text{ classe d'isomorphisme de } \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

et

$$\psi\colon P_n \to C_n \qquad \begin{array}{l}(n_1, n_2, \ldots, n_r) \mapsto \text{ classe de conjugaison de la permutation} \\ (1, 2, \ldots, n_1)(n_1+1, \ldots, n_1+n_2)\ldots(n_1+n_2+n_{r-1}+1, \ldots, n)\end{array}$$

φ et ψ sont des bijections donc $|C_n| = |G_n|$: il y a autant de classes de conjugaison dans $\mathcal{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 142

◇ Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(1,3)$ et $(2,0)$. Déterminer la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$.

◇ Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(1,1)$ et $(1,-1)$. Déterminer la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$.

Solution 142

◇ Déterminons la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$. On a

$$\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Par suite $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/6\mathbb{Z}$.

◇ On a

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Par conséquent $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 143

Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(2,5)$, $(5,-1)$ et $(1,-2)$. Déterminer une base de H et décrire le quotient ${\mathbb{Z}^2}\!/\!_{\mathrm{H}}$.

Solution 143

On a

$$\begin{pmatrix} 2 & 5 & 1 \\ 5 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 9 & 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 0 & 9 & -2 \end{pmatrix}$$

donc $\mathrm{H} = \langle (0,9), (1,-2) \rangle$ est de rang 2.

De plus $\begin{pmatrix} 0 & 1 \\ 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 9 & 0 \end{pmatrix}$; par suite ${\mathbb{Z}^2}\!/\!_{\mathrm{H}} \simeq \mathbb{Z}/_{9\mathbb{Z}}$.

Exercice 144

Trouver une base du groupe suivant :

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \,\middle|\, \begin{cases} 2x + 3y + 5z = 0 \\ 3x - 6y + 2z = 0 \end{cases} \right\}$$

Solution 144

Soit G le groupe donné par :

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \,\middle|\, \begin{cases} 2x + 3y + 5z = 0 \\ 3x - 6y + 2z = 0 \end{cases} \right\}$$

On a

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \,\middle|\, \begin{cases} 2x + 3y + 5z = 0 \\ 7x + 12z = 0 \end{cases} \right\}$$

Comme $7x + 12z = 0$ on écrit $x = 12k$ et $z = -7k$. Alors $2x + 3y + 5z = 0$ conduit à $3y = 11k$. On pose donc $k = 3l$ alors

$$x = 36\ell, \qquad y = 11\ell, \qquad z = -21\ell$$

Finalement

$$\mathrm{G} = \left\{ \ell(36, 11, -21) \mid \ell \in \mathbb{Z} \right\} = \mathrm{Vect}(36, 11, -21)$$

et $\{(36, 11, -21)\}$ est une base de G.

Exercice 145

Soit G un groupe abélien fini.

Supposons que pour tout diviseur d de l'ordre n de G, il existe un et un seul sous-groupe d'ordre d dans G. Montrer que G est cyclique.

Solution 145

Raisonnons par l'absurde. Supposons que G ne soit pas cyclique. Alors G est isomorphe à $\mathbb{Z}/_{q_1\mathbb{Z}} \times \mathbb{Z}/_{q_2\mathbb{Z}} \times \ldots \times \mathbb{Z}/_{q_k\mathbb{Z}}$ où $q_1 | q_2 | \ldots | q_k$ sont les facteurs invariants de G et $k \geqslant 2$. Il y a alors (au moins) deux sous-groupes distincts d'ordre q_1 : d'une part le facteur $\mathbb{Z}/_{q_1\mathbb{Z}}$ et d'autre part l'unique sous-groupe d'ordre q_1 du facteur $\mathbb{Z}/_{q_2\mathbb{Z}}$ associé au diviseur q_1 de q_2.

Exercice 146

1. Les groupes $\mathbb{Z}/_{12\mathbb{Z}} \times \mathbb{Z}/_{72\mathbb{Z}}$ et $\mathbb{Z}/_{18\mathbb{Z}} \times \mathbb{Z}/_{48\mathbb{Z}}$ sont-ils isomorphes ?
2. Les groupes $\mathbb{Z}/_{72\mathbb{Z}} \times \mathbb{Z}/_{84\mathbb{Z}}$ et $\mathbb{Z}/_{36\mathbb{Z}} \times \mathbb{Z}/_{168\mathbb{Z}}$ sont-ils isomorphes ?

Solution 146

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ ne sont pas isomorphes. En effet posons

$$\mathrm{G}_1 = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}.$$

   Nous avons $12 = 2^2 \times 3$, $72 = 2^3 \times 3^2$, $18 = 2 \times 3^2$ et $48 = 2^4 \times 3$. Les groupes G_1 et G_2 sont tous deux d'ordre $2^5 \times 3^3$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i$ pour $i = 1,\ 2$ où A_i est un groupe abélien d'ordre 2^5 et B_i un groupe abélien d'ordre 3^3. Le groupe A_1 est associé à la partition $(3, 2)$ de 5 et le groupe A_2 est associé à la partition $(4, 1)$ de 5 ; ils ne sont donc pas isomorphes. Par suite les groupes G_1 et G_2 ne sont pas isomorphes.
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont isomorphes. En effet posons

$$\mathrm{G}_1 = \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}.$$

Nous avons $72 = 2^3 \times 3^2$, $84 = 2^2 \times 3 \times 7$, $36 = 2^2 \times 3^2$ et $168 = 2^3 \times 3 \times 7$. Les groupes G_1 et G_2 sont donc de même ordre $2^5 \times 3^3 \times 7$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i \times \mathrm{C}_i$ où A_i est un groupe abélien d'ordre 2^5, B_i est un groupe abélien d'ordre 3^3 et C_i est un groupe abélien d'ordre 7. Les groupes A_1 et A_2 sont associés à la partition $(3, 2)$ de 5, ils sont isomorphes. Les groupes B_1 et B_2 sont associés à la partition $(2, 1)$ de 3 ; ils sont donc isomorphes. Les groupes C_1 et C_2 sont isomorphes. Il en résulte que G_1 et G_2 sont isomorphes.

Exercice 147

Soient a, b, c et d quatre entiers deux à deux premiers entre eux.
Montrer que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.

Solution 147

Soient a, b, c et d quatre entiers deux à deux premiers entre eux.
Montrons que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.
Les nombres a, b, c et d étant premiers entre deux à deux nous avons

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$
$$\mathbb{Z}/cd\mathbb{Z} \simeq \mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$
$$\mathbb{Z}/ac\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$$
$$\mathbb{Z}/bd\mathbb{Z} \simeq \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$

Par suite les deux groupes $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ et $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$ sont isomorphes.

Exercice 148

Soit $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Considérons les deux sous-groupes suivants de G :

$$\mathrm{H} = \mathbb{Z}/2\mathbb{Z} \times \{0\} \qquad \mathrm{K} = \{0\} \times \{0,\ 6\}.$$

Remarquons que $\mathrm{H} \simeq \mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z}$ mais avons-nous $\mathrm{G}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$?

Solution 148

D'une part $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, d'autre part $\mathrm{G}/\mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \times \mathbb{Z}/3\mathbb{Z}$.
Les deux premiers facteurs ne sont pas isomorphes donc les deux groupes ne sont pas isomorphes.

Exercice 149

Soient G, H et K des groupes abéliens finis.

1. Montrer que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq \mathrm{H}$.
2. Montrer que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

Solution 149

Soient G, H et K des groupes abéliens finis. Montrons que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq$ Het que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

La décomposition primaire de G est $\prod_{i=1}^{s} \mathrm{A}_i$, celle de $\mathrm{G} \times \mathrm{G}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \mathrm{A}_i$.

La décomposition primaire de H est $\prod_{i=1}^{t} \mathrm{B}_i$, celle de $\mathrm{H} \times \mathrm{H}$ est donc $\prod_{i=1}^{t} \mathrm{B}_i \times \mathrm{B}_i$.

La décomposition primaire de K est $\prod_{i=1}^{u} \mathrm{C}_i$, celle de $\mathrm{G} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \prod_{i=1}^{u} \mathrm{C}_i$ et celle de $\mathrm{H} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{B}_i \times \prod_{i=1}^{u} \mathrm{C}_i$.

Si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par suite $\mathrm{G} \simeq \mathrm{H}$.

Si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par conséquent $\mathrm{G} \simeq \mathrm{H}$.

Exercice 150

1. Exprimer tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.
2. Exprimer tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques.

Solution 150

1. Exprimons tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.
   Les groupes abéliens d'ordre $99 = 3^2 \times 11$ sont isomorphes
   - soit à $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$,
   - soit à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.
2. Exprimons tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques. Les groupes abéliens d'ordre $100 = 2^2 \times 5^2$ sont isomorphes
   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice 151

Combien existe-t-il, à isomorphisme près, de groupes abéliens d'ordre 10^6 ?

Solution 151

Nous avons $10^6 = 2^6 \times 5^6$. Les partitions de 6 sont

$$\begin{array}{l}(6)\\(5,1)\\(4,2)\\(4,1,1)\\(3,3)\\(3,2,1)\\(3,1,1,1)\\(2,2,2)\\(2,2,1,1)\\(2,1,1,1,1)\\(1,1,1,1,1,1)\end{array}$$

Elles sont donc au nombre de 11. Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 152

a) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 12 et 72.

b) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Solution 152

a) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 12.
Nous avons $12 = 2^2 \times 3$. De plus les partitions de 2 sont

$$2 \qquad\qquad 1,\ 1$$

Par conséquent il y a à isomorphisme près 2 groupes abéliens d'ordre 12 :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \qquad\qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Déterminons à isomorphisme près tous les groupes abéliens d'ordre 72.
Nous avons $72 = 2^3 \times 3^2$. De plus les partitions de 2 sont

$$2 \qquad\qquad 1,\ 1$$

et celles de 3 sont

$$3 \qquad\qquad 2,\ 1 \qquad\qquad 1,\ 1,\ 1$$

Par conséquent il y a à isomorphisme près $2 \times 3 = 6$ groupes abéliens d'ordre 72 :

$$\begin{array}{ll}
\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\text{é}\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, & \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\text{é}\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.
\end{array}$$

b) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 10^6.
Nous avons $10^6 = 2^6 \times 5^6$. De plus les partitions de 6 sont

6
5, 1
4, 2
4, 1, 1
3, 3
3, 2, 1
3, 1, 1, 1
2, 2, 2
2, 2, 1, 1
2, 1, 1, 1, 1, 1
1, 1, 1, 1, 1, 1

Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 153

Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Solution 153

Nous utilisons le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}\right) \times \left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}\right)$$

Notons que cette écriture est la décomposition en composantes p-primaires. En effet $12 = 2^2 \times 3$, $90 = 2 \times 3^2 \times 5$, $25 = 5^2$, $100 = 2^2 \times 5^2$, $30 = 2 \times 3 \times 5$ et $9 = 3^2$.

Nous pouvons aussi écrire la décomposition en facteurs invariants de ces deux groupes, nous trouvons

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}.$$

Exercice 154

Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Solution 154

Montrons qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Soit G un groupe abélien fini non cyclique. Il est isomorphe à un produit

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_i \geqslant 2$ et $d_i \mid d_{i+1}$. Puisque G n'est pas cyclique, $r \geqslant 2$. Soit p un facteur premier de d_1 alors p disvise tous les d_i et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Le sous-groupe de p torsion de G est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^r$ qui contient un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 155

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.
b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Solution 155

a) La décomposition de 360 en facteurs premiers est $2^3 \times 3^2 \times 5$. Ainsi si G est un groupe de cardinal 360, alors le sous-groupe
$$T_2(\mathrm{G}) = \left\{g \in \mathrm{G} \mid \exists n \in \mathbb{N} \quad 2^n g = 0\right\}$$
de 2-torsion de G est un groupe abélien de cardinal 2^3, il y a donc trois classes d'isomorphisme de tels groupes : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. De même il y a exactement deux classes d'isomorphisme possibles pour $T_3(\mathrm{G})$ à savoir $\mathbb{Z}/9\mathbb{Z}$ et $\left(\mathbb{Z}/3\mathbb{Z}\right)^2$. Par ailleurs $T_5(\mathrm{G})$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Il y a donc exactement six classes d'isomorphisme de groupes abéliens d'ordre 360 donc les décompositions p-primaires et les décompositions en facteurs invariants sont les suivantes :
$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/360\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times 4\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$$

b) Plus généralement, pour tout entier n, déterminons le nombre de groupes abéliens de cardinal n. Nous utilisons la classification des classes d'isomorphisme de groupes abéliens finis. Soit $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. La classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, d_2, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i \mid d_{i+1}$ et $d_1 d_2 \dots d_s = n$. Par suite chaque d_i se décompose comme suit : $d_i = p_1^{\alpha_{1,i}} p_2^{\alpha_{2,i}} \dots p_r^{\alpha_{r,i}}$ avec les contraintes suivantes : $\alpha_{i,j} \leqslant \alpha_{i+1,j}$ pour tout j, pour tout i et $\displaystyle\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$ et $\displaystyle\sum_{i=1}^{q} \alpha_{i,j} = \alpha_j$.

Il s'en suit que le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$ où $p(\alpha)$ désigne le nombre de partitions de α, *i.e.* le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 156

a) On considère $\mathrm{H} = \{(a,b) \in \mathbb{Z}^2 \,|\, a-b \text{ est divisible par } 10\}$. Montrer que H est un sous-groupe de $\mathbb{Z}^2$. Calculer le rang de H. Donner une base de H. Décrire le quotient ${\mathbb{Z}^2}/{\mathrm{H}}$.

b) On note H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4,8,10)$ et $(6,2,0)$. Déterminer la structure du groupe H.

Solution 156

a) Soit φ le morphisme de groupes donné par

$$\varphi\colon \mathbb{Z}^2 \to {\mathbb{Z}}/{10\mathbb{Z}}, \qquad (a,b) \mapsto a-b$$

Son noyau est H. En particulier H est un sous-groupe distingué de $\mathbb{Z}^2$.
D'une part H contient $(1,1)$ et $(0,10)$ donc $\mathrm{rg}\,\mathrm{H} \geqslant 2$. D'autre part $\mathrm{H} \subset \mathbb{Z}^2$ donc $\mathrm{rg}\,\mathrm{H} \leqslant 2$. Finalement $\mathrm{rg}\,\mathrm{H} = 2$.
Soit (a,b) dans H. Il existe n dans $\mathbb{Z}$ tel que $a = b + 10n$ et

$$(a,b) = (a, a-10n) = a(1,1) + (-n)(0,10).$$

Autrement dit $((1,1),(0,10))$ est une base de H.
Par ailleurs

$${\mathbb{Z}^2}/{\mathrm{H}} = \langle (g_1,g_2) \,|\, g_1 + g_2 = 0,\ 10g_2 = 0\rangle.$$

Puisque $\begin{pmatrix} 1 & 0 \\ 1 & 10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$ les facteurs invariants de ${\mathbb{Z}^2}/{\mathrm{H}}$ sont 1 et 10 et ${\mathbb{Z}^2}/{\mathrm{H}} \simeq {\mathbb{Z}}/{10\mathbb{Z}}$.

b) Notons H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4,8,10)$ et $(6,2,0)$. Déterminons la structure du groupe H. Nous avons

$$\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix}$$

Ainsi les facteurs invariants de $\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix}$ sont 2 et 10 et $\mathrm{H} \simeq \mathbb{Z} \times {\mathbb{Z}}/{2\mathbb{Z}} \times {\mathbb{Z}}/{10\mathbb{Z}}$.

Exercice 157

Déterminer les facteurs invariants des matrices suivantes à coefficients dans $\mathbb{Z}$:

a) $\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}$;

b) $\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix}$;

c) $\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}$.

Solution 157

Nous pouvons procéder de deux manières différentes :

- soit en calculer le pgcd des coefficients de la matrice puis le pgcd des mineurs de taille 2, etc
- soit en appliquant l'algorithme de réduction des matrices à coefficients entiers via des opérations élémentaires sur les lignes et les colonnes.

Dans les deux cas nous obtenons ($\sim$ désigne l'équivalence des matrices à coefficients entiers) :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Les facteurs invariants sont donc respectivement $(1,6)$, $(3,9)$ et $(1,2,16)$.

Détaillons la première équivalence :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Détaillons la seconde équivalence :

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 12 & -27 \\ 69 & -153 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & -27 \\ 9 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & -3 \\ 9 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & 3 \\ 9 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 12 \\ 0 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}.$$

Détaillons la dernière équivalence :

$$\begin{aligned}
\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} &\rightsquigarrow \begin{pmatrix} -75 & 41 & -13 \\ 12 & -6 & 2 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -3 & 5 & -1 \\ 12 & -6 & 2 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -12 & 6 & -2 \\ -3 & 5 & -1 \\ 19 & -3 & 3 \end{pmatrix} \\
&\rightsquigarrow \begin{pmatrix} 0 & -14 & 2 \\ -3 & 5 & -1 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -19 & 3 & -3 \\ -3 & 5 & -1 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & -27 & 3 \\ -3 & 5 & -1 \\ 0 & -14 & 2 \end{pmatrix} \\
&\rightsquigarrow \begin{pmatrix} 3 & -5 & 1 \\ -1 & -27 & 3 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & -86 & 10 \\ -1 & -27 & 3 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 27 & -3 \\ 0 & -86 & 10 \\ 0 & -14 & 2 \end{pmatrix} \\
&\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -86 & 10 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -2 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & -2 \\ 0 & -2 & -2 \end{pmatrix} \\
&\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -16 \\ 0 & -2 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -16 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -16 \end{pmatrix} \\
&\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}
\end{aligned}$$

Exercice 158

Soit $\Bbbk$ un corps commutatif. Soit G un sous-groupe fini du groupe multiplicatif $\Bbbk^\times = \Bbbk \smallsetminus \{0\}$ de $\Bbbk$. Montrer que G est cyclique.

Solution 158

Nous utilisons le théorème de structure des groupes abéliens finis. Si $|\mathrm{G}| > 1$, alors il existe une suite d'entiers $1 < a_1 \,|\, a_2 \,|\, \ldots \,|\, a_r$ tels que

$$\mathrm{G} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_r\mathbb{Z}$$

Montrons que $r = 1$. Puisque $a_r\mathrm{G} = \{0\}$ nous avons

$$\#\{z \in \Bbbk \,|\, z^{a_r} = 1\} \geqslant |\mathrm{G}| = a_1 a_2 \ldots a_r.$$

Par ailleurs le nombre de racines dans $\Bbbk$ du polynôme $X^{a_r} - 1 \in \Bbbk[X]$ est inférieur ou égal à son degré parce que $\Bbbk$ est commutatif. Il en résulte l'inégalité $a_1 a_2 \ldots a_r \leqslant a_r$ qui conduit à $r = 1$.