GROUPE OPÉRANT SUR UN ENSEMBLE

Soient $(G,\star)$ un groupe d'élément neutre e et X un ensemble non vide. On appelle opération de G sur X la donnée d'une application $\omega : \left\{ \begin{array}{ccc} G\times X & \longrightarrow & X \\ (g,x) & \longmapsto & g.x \end{array} \right.$ vérifiant les deux axiomes :

1. $\forall x\in X$, on a: $e.x=x$;
2. $\forall g,h\in G$ et $x\in X$, on a: $g.(h.x)=(g\star h).x$

Partie I: Orbites et stabilisateurs

On définit la relation $\mathcal{R}$ sur X par:

$$\forall (x,y)\in X^2,\quad x\mathcal{R}y \Longleftrightarrow \exists g\in G,\ y=g.x$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
   On note $\mathcal{O}_x=\{g.x\ ,\ g\in G\}$ la classe de $x\in X$ et $\mathcal{S}$ une section de la relation d'équivalence $\mathcal{R}$, c'est-à-dire une partie de X qui contient exactement un élément de chacune des classes d'équivalence de $\mathcal{R}$
2. Pour $x\in X$, on définit le stabilisateur $\mathcal{G}_x$ de x par

   $$\mathcal{G}_x=\{g\in G\ ,\ g.x=x\}$$

   Montrer que le stabilisateur est un sous-groupe de $(G,\star)$

Partie II: Exemples

1. **Opération par translation à gauche:**
   (a) Montrer que G opère sur lui-même par translation à gauche via l'action

   $$\omega : \left\{ \begin{array}{ccc} G\times G & \longrightarrow & G \\ (g,x) & \longmapsto & gx \end{array} \right.$$

   (b) Décrire les orbites et les stabilisateurs de $x\in G$ pour cette action
2. **Opération par conjugaison:**
   (a) Montrer que G opère sur lui-même par translation à gauche via l'action

   $$\omega : \left\{ \begin{array}{ccc} G\times G & \longrightarrow & G \\ (g,x) & \longmapsto & gxg^{-1} \end{array} \right.$$

   (b) Décrire les orbites et les stabilisateurs de $x\in G$ pour cette action
3. Soit $\mathcal{H}$ l'ensemble des sous-groupes de $(G,.)$
   (a) Soit $H\in\mathcal{H}$ et $g\in G$. Montrer que $gHg^{-1}=\{ghg^{-1}\ ,\ h\in H\}$ est un sous-groupe de $(G,.)$ (appelé sous-groupe conjugué de H)
   (b) Montrer que G opère sur $\mathcal{H}$ via l'action

   $$\omega : \left\{ \begin{array}{ccc} G\times \mathcal{H} & \longrightarrow & \mathcal{H} \\ (g,H) & \longmapsto & gHg^{-1} \end{array} \right.$$

GROUPE OPÉRANT SUR UN ENSEMBLE

Partie III: Équation aux classes

1. On suppose que G est fini.
   (a) Montrer que $\mathbf{Card}(G) = \mathbf{Card}(\mathcal{O}_x).\mathbf{Card}\,(\mathcal{G}_x)$
   (b) Si X est aussi fini. Montrer l'équation aux classes
$$\mathbf{Card}(X) = \sum_{x\in\mathcal{S}} \frac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$$
2. On fait agir G sur lui-même par les automorphismes intérieurs:
$$(s, x) \longmapsto s.x = sxs^{-1}$$
   Montrer que
$$\mathbf{Card}(G) = \mathbf{Card}\,(Z(G)) + \sum_{\substack{x\in\mathcal{S}\\ x\notin Z(G)}} \frac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$$
   où $Z(G)$ est le centre de G, c'est-à-dire $Z(G) := \{a \in G\ ,\ \forall x \in G\ ax = xa\}$

Partie IV: Applications

1. **APPLICATION 1:** Soit $(G, .)$ un groupe abélien d'ordre $m \in \mathbb{N}^s$. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que:
$$\forall x \in G, \quad x^n = e$$
   (a) Montrer que m divise une puissance de n
   (b) Montrer que le résultat reste encore vrai en ne supposant plus G abélien
2. **APPLICATION 2:** Soit $(G, .)$ un groupe abélien d'ordre mp^r, avec p premier et $m \wedge p = 1$
   (a) Montrer que G admet un sous-groupe d'odre p^r
   (b) Montrer que le résultat reste encore vrai en ne supposant plus G abélien
3. **APPLICATION 3:** Soit $(G, .)$ un groupe d'ordre p^r, avec p premier et $r \geqslant 2$
   (a) Montrer que $Z\,(G) \neq \{e\}$
   (b) Si $r = 2$, montrer que $(G, .)$ est abélien
4. **APPLICATION 4:** Soit $(G, .)$ un groupe non abélien d'ordre pq, avec p et q premiers et $r \geqslant 2$
   (a) Montrer que $Z\,(G) = \{e\}$
   (b) En déduire qu'il existe dans G des sous-groupes d'ordre p (resp. d'ordre q)

GROUPE OPÉRANT SUR UN ENSEMBLE

Soient $(G, \star)$ un groupe d'élément neutre e et X un ensemble non vide. On appelle opération de G sur X la donnée d'une application $\omega : \left\{ \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g.x \end{array} \right.$ vérifiant les deux axiomes :

1. $\forall x \in X$, on a: $e.x = x$;
2. $\forall g, h \in G$ et $x \in X$, on a: $g.(h.x) = (g \star h).x$

Partie I: Orbites et stabilisateurs

On définit la relation $\mathcal{R}$ sur X par:

$$\forall (x,y) \in X^2, \quad x\mathcal{R}y \Longleftrightarrow \exists g \in G,\ y = g.x$$

1. Montrons que $\mathcal{R}$ est une relation d'équivalence.
   - $\mathcal{R}$ est réflèxive car $e.x = x$
   - $\mathcal{R}$ est symétrique car: Si $x\mathcal{R}y$, alors il existe $g \in G$ tel que $y = g.x$, donc
     $$g^{-1}.y = g^{-1}.(g.x) = \left(g^{-1} \star g\right).x = e.x = x$$
     Donc $y\mathcal{R}x$
   - $\mathcal{R}$ est transitive car: Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors il existe $s, t \in G$ tels que $y = s.x$ et $z = t.y$, alors $z = (ts).x$, avec $ts \in G$ on tire que $x\mathcal{R}z$
2. Soit $x \in X$. $\mathcal{G}_x$ est une partie de G
   - $\mathcal{G}_x \neq \emptyset$, car $e \in \mathcal{G}_x$
   - Soit $s, t \in \mathcal{G}_x$, alors
     $$(s^{-1} \star t).x = s^{-1}.(t.x) = s^{-1}.x = s^{-1}.(s.x) = \left(s^{-1} \star s\right).x = e.x = x$$
     Donc $s^{-1}t \in \mathcal{G}_x$. Ce qui montre que $\mathcal{G}_x$ est un sous-groupe de $(G, \star)$

Partie II: Exemples

Accessible

Partie III: Équation aux classes

1. On suppose que G est fini.
   (a) On considère l'application $\psi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathcal{O}_x \\ g & \longmapsto & g.x \end{array} \right.$. ψ est bien définie, surjective par construction et pour tout $g \in G$, on a $\psi^{-1}(\{g.x\}) = g.\mathcal{G}_x$ qui a le même cardinal que $\mathcal{G}_x$, par le principe des bergers $\mathbf{Card}(G) = \mathbf{Card}(\mathcal{O}_x).\mathbf{Card}\,(\mathcal{G}_x)$
   (b) $\mathcal{S}$ est une section de $\mathcal{R}$, alors la famille $(\mathcal{O}_x)_{x \in \mathcal{S}}$ forme une partition de X et puisque X est fini, alors
   $$\mathbf{Card}(X) = \sum_{x \in \mathcal{S}} \mathbf{Card}\,(\mathcal{O}_x) = \sum_{x \in \mathcal{S}} \frac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$$
2. On fait agir G sur lui-même par les automorphismes intérieurs. Pour tout $x \in G$, on a $x \in Z(G) \Longleftrightarrow \mathcal{O}_x = \{x\}$. Donc $Z(G) \subset \mathcal{S}$ et l'équation aux classes devient alors:
   $$\mathbf{Card}(G) = \mathbf{Card}\,(Z(G)) + \sum_{\substack{x \in \mathcal{S} \\ x \notin Z(G)}} \frac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$$

Groupe opérant sur un ensemble

Partie IV: Applications

1. **Application 1:**

   (a) Par récurrence forte sur $m \in \mathbb{N}^*$

   - Pour $m = 1$, rien à démontrer
   - Soit G un groupe d'ordre $\leqslant m+1$ et vérifiant $x^n = e$ pour tout $x \in G$.
     Si G est d'ordre 1 alors c'est fini, sinon soit $x \in G \setminus \{e\}$ et considérons le groupe quotient $G/\mathrm{gr}(x)$. On a $\mathbf{Card}(G/\mathrm{gr}(x)) < \mathbf{Card}(G) \leqslant m+1$; en appliquant l'hypothèse de récurrence, on déduit que $\mathbf{Card}(G/\mathrm{gr}(x))$ divise une puissance de n. De plus, l'ordre de x divise n (car $x^n = e$) et $\mathbf{Card}(\mathrm{gr}(x)) = O(x) \mid n$. Maintenant, comme
     $$\mathbf{Card}(G) = \mathbf{Card}(G/\mathrm{gr}(x)) \times \mathbf{Card}(\mathrm{gr}(x))$$
     Alors $\mathbf{Card}(G)$ divise une puissance de n.

   La récurrence est terminée

   (b) On suppose G quelconque. On fait un raisonnement par récurrence forte sur $m \in \mathbb{N}^*$

   - Pour $m = 1$, rien à démontrer
   - Soit G un groupe d'ordre $\leqslant m+1$ et vérifiant $x^n = e$ pour tout $x \in G$. On écrit $\mathbf{Card}(G) = ab$ avec $a \wedge n = 1$ et b divise une puissance de n. Soit $\mathcal{S}$ une section de la classe d'équivalence $\mathcal{R}$ et $x \in S$ tel que $x \notin Z(G)$, alors $\mathcal{G}_x \neq G$ et par suite $\mathbf{Card}(\mathcal{G}_x) < \mathbf{Card}(G)$. Comme $\mathcal{G}_x$ est un sous-groupe de G, alors $\mathcal{G}_x$ vérifie les conditions de l'hypothèse de récurrence, c'est-à-dire $\mathbf{Card}(\mathcal{G}_x)$ divise une puissance de n. Mais $a \wedge n = 1$, donc $a \wedge \mathbf{Card}(\mathcal{G}_x) = 1$. En outre $a \mid \mathbf{Card}(G) = \mathbf{Card}\left(\dfrac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}\right)\mathbf{Card}(\mathcal{G}_x)$, alors par Gauss $a \mid \mathbf{Card}(G) = \mathbf{Card}\left(\dfrac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}\right)$. Ceci montre que a divise $\displaystyle\sum_{\substack{x \in \mathcal{S} \\ x \notin Z(G)}} \dfrac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$.
     D'après l'équation aux classes on en déduit que $a \mid \mathbf{Card}(Z(G))$. Or, comme $Z(G)$ est abélien, alors $\mathbf{Card}(Z(G))$, et donc a, divise une puissance de n, ce qui est impossible car $a \wedge n = 1$ sauf si $a = 1$

   Récurrence achevée

2. **Application 2:** Soit $(G, .)$ un groupe abélien d'ordre mp^r, avec p premier et $m \wedge p = 1$

   (a) Soit l'application $\varphi : \left\{\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{p^r} \end{array}\right.$. φ est un endomorphisme de groupes car G est abélien. On sait que $\mathrm{Ker}(\varphi)$ est un sous-groupe de G, et de plus on a pour tout $x \in \mathrm{Ker}\varphi$: $x^{p^r} = e$. On en déduit, d'après l'application 1, que $\mathbf{Card}(\mathrm{Ker}(\varphi))$ divise une puissance de p^r. De même, pour tout $x \in \mathrm{Im}(\varphi)$: $x^m = e$, donc $\mathbf{Card}(\mathrm{Im}(\varphi))$ divise une puissance de m. Mais $mp^r = \mathbf{Card}(\mathrm{Ker}(\varphi))/times\mathbf{Card}(\mathrm{Im}(\varphi))$ avec $m \wedge p^r = 1$, on en déduit forcément que: $\mathbf{Card}(\mathrm{Ker}(\varphi)) = p^r$ et $\mathbf{Card}(\mathrm{Im}(\varphi)) = m$. En conclusion $\mathrm{Ker}(\varphi)$ est un sous-groupe de G d'ordre p^r

   (b) On fait un raisonnement par récurrence sur l'ordre de G. Soit

   $\mathcal{P}(m)$: Tout groupe d'ordre kp^s avec p premier, $p \wedge k = 1$ et $kp^s \leqslant m$, admet un sous-groupe d'ordre p^s

   - Pour $m = 1$ le résultat est vrai.
   - Soit $m \in \mathbb{N}$ et soit G un groupe d'ordre $m+1 = hp^r$ avec p premier et $p \wedge h = 1$. On sait que
     $$\mathbf{Card}(G) = \mathbf{Card}(G/\mathrm{gr}(x)) \times \mathbf{Card}(\mathrm{gr}(x))$$
     - S'il existe un élément $x \in S \setminus Z(G)$ tel que $p^r \mid \mathbf{Card}(\mathcal{G}_x)$, on applique l'hypothèse de récurrence $\mathcal{G}_x$
     - Sinon, pour tout $x \in \mathcal{S} \setminus Z(G)$, $p \mid \mathbf{Card}(Z(G))$. On distingue alors deux cas
       * G est abélien, le problème est réglé
       * G n'est pas abélien, alors on applique le résultat à $Z(G)$ qui est un groupe abélien de G. D'où, $Z(G)$ admet un sous-groupe H d'ordre p^s, avec $s \in [\![1, r]\!]$. De plus H est distingué dans G car $Z(G)$ l'est et $\mathbf{Card}(G/H) = hp^{r-s}$, donc $\mathbf{Card}(G/H) < \mathbf{Card}(G)$, et par hypothèse de récurrence G/H admet un sous-groupe K d'ordre p^{r-s}. Finalement, soit $\pi : G \longrightarrow G/H$ la surjection canonique, alors $\pi^{-1}(K)$ est un sous-groupe de G de cardinal p^r

3. **APPLICATION 3:** Soit $(G, .)$ un groupe d'ordre p^r, avec p premier et $r \geqslant 2$

   (a) Soit $x \in G$, le stabilisteur $\mathcal{G}_x$ de x est un sous-groupe de G, donc son cardinal est une spuissance de p. De plus, si $x \notin Z(G)$ alors $\mathbf{Card}\,(\mathcal{G}_x) < \mathbf{Card}(G)$ car $\mathcal{G}_x \neq G$. Or, $\mathbf{Card}\,(\mathcal{O}_x) = \dfrac{\mathbf{Card}(G)}{\mathbf{Card}\,(\mathcal{G}_x)}$, donc $\mathbf{Card}(\mathcal{O}_x) > 1$ pour tout $x \notin Z(G)$. D'où, $\mathbf{Card}\,(\mathcal{O}_x) = p^k$ avec $k \geqslant 1$ pour tout $x \notin Z(G)$. Par conséquent, p divise $\displaystyle\sum_{\substack{x\in\mathcal{S}\\ x\notin Z(G)}} \mathbf{Card}\,(\mathcal{O}_x)$. Comme $p \mid \mathbf{Card}(G)$, alors, d'après l'équation aux classes p divise $\mathbf{Card}(Z(G))$, donc $Z\,(G) \neq \{e\}$

   (b) D'après la question ci-dessus on sait que $\mathbf{Card}(Z(G)) > 1$ et p divise $\mathbf{Card}(Z(G))$. D'où, puisque $\mathbf{Card}(G) = p^2$, on a $\mathbf{Card}(Z(G)) = p$ ou $\mathbf{Card}(Z(G)) = p^2$. Par absurde si G n'est pas abélien, alors $Z(G) \subsetneq G$, donc $\mathbf{Card}(Z(G)) = p$. Mais s'il existe $x \in G$ tel que $x \notin Z(G)$, alors $x \cup Z(G) \subset \mathcal{G}_x$, et par suite $\mathcal{G}_x$ est de cardinal $> p+1$ et il divise p^2, alors $\mathcal{G}_x$ est forcément vaut p^2, puis $\mathcal{G}_x = G$, ceci entraîne $\mathcal{O}_x$ est de cardinal 1, c'est-à-dire $x \in Z(G)$. Ce qui absurde

4. **APPLICATION 4:** Soit $(G, .)$ un groupe non abélien d'ordre pq, avec p et q premiers et $r \geqslant 2$

   (a) On sait que $\mathbf{Card}\,(Z(G))$ divise pq, par suite si $Z(G) \neq \{e\}$ alors $Z(G)$ est de cardinal soit p, soit q car G n'est pas abélien et p et$q$ sont premiers entre eux. Puisque p et q jouent un rôle symétrique, on peut supposer par exemple que $\mathbf{Card}(Z(G)) = p$, alors $H = G/Z(G)$ est un groupe de cardinal q premier. Par suite, H est monogène engendré par $\overline{x}$ avec $x \in G$. Soit $a, b \in G$, alors il existe $m, n \in \mathbb{N}$ tel que $\overline{a} = \overline{x}^m$ et $\overline{b} = \overline{x}^n$, c'est-à-dire $a(x^{-1})^m \in Z(G)$ et $b(x^{-1})^n \in Z(G)$, donc on peut trouver deux éléments k et ℓ dans $Z(G)$ tels que $a(x^{-1})^m = k$ et $b(x^{-1})^n = \ell$, alors on a:

$$\begin{aligned} ab &= x^m k x^n \ell = x^m x^n k\ell \quad (\text{ car } k \in Z(G)\ ) \\ &= x^n x^m \ell k \quad (\text{ car } x^m x^n = x^n x^m\ ) \\ &= x^n \ell x^m k \quad (\text{ car } \ell \in Z(G)\ ) \\ &= ba \end{aligned}$$

   On a donc montré que G est abélien. Absurde

   (b) D'après l'équation aux classes on a:

$$pq = 1 + \sum_{\substack{x\in\mathcal{S}\\ x\notin Z(G)}} \frac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$$

   Si G n'admet aucun sous-groupe d'ordre p, alors pour tout $x \in G \setminus Z(G)$ on a $\mathbf{Card}(\mathcal{G}_x) < \mathbf{Card}(G)$, donc $\mathbf{Card}\,(\mathcal{G}_x) = 1$ ou q. Alors, on aurait p divise $\displaystyle\sum_{\substack{x\in\mathcal{S}\\ x\notin Z(G)}} \frac{\mathbf{Card}(G)}{\mathbf{Card}(\mathcal{G}_x)}$ et donc $p \mid 1$. Contradiction