Devoir facultatif n° 6

Dans ce problème, pour tout ensemble fini A, le cardinal de A, noté $|A|$, désigne le nombre d'éléments de A. On admet que s'il existe une bijection entre deux ensembles A et B, alors $|A| = |B|$.
Pour tout groupe, son nombre d'éléments est appelé l'*ordre* de ce groupe [1]. Enfin, pour tout groupe $(G, \times)$, on notera $a \times b$ ou ab le produit de a et b mais surtout pas $a.b$: cette notation sera réservée à un autre usage.

1) Groupes cycliques Soit $(G, \times)$ un groupe (de neutre 1_G) et $x \in G$. On pose $\langle x \rangle = \left\{ x^k \;\middle|\; k \in \mathbb{Z} \right\}$.

a) Montrer que l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & G \\ & k & \mapsto & x^k \end{array}$$

est un morphisme de groupe.

b) En déduire que $\langle x \rangle$ est un sous-groupe de G (appelé groupe cyclique engendré par x). Est-il commutatif ?

c) Montrer que si $\langle x \rangle$ est infini, alors il est isomorphe à $\mathbb{Z}$.

d) On suppose maintenant que G est fini. Montrer que $|\langle x \rangle|$ est le plus petit entier n non nul vérifiant $x^n = 1_G$. On appelle *ordre de* x cet entier.

e) Montrer que tout entier relatif n vérifiant $x^n = 1_G$ est un multiple de l'ordre de x.

f) Montrer que si $|\langle x \rangle|$ est premier, alors pour tout y différent de 1_G appartenant à $\langle x \rangle$ on a $\langle y \rangle = \langle x \rangle$.

2) Groupe opérant sur un ensemble

Soit $(G, \times)$ un groupe (de neutre 1_G) et X un ensemble, on dit que G *opère sur* X si on s'est donné une application (notée par un point)

$$\begin{array}{rccc} & G \times X & \to & X \\ & (g, x) & \mapsto & g.x \end{array}$$

vérifiant les deux propriétés suivantes :

a) $\forall (g, g') \in G^2 \; \forall x \in X \quad g.(g'.x) = (g \times g').x$

b) $\forall x \in X \quad 1_G.x = x$

1. Il n'y a donc aucun rapport avec la notion de relation d'ordre sur un ensemble.

a) Exemple : opération par translation à gauche Soit $(G, \times)$ un groupe et H un sous-groupe de G. $(H, \times)$ est donc un groupe.
Dans cette question, on s'intéresse à l'application $. : H \times G \to G$, appelée *translation à gauche* et définie par :

$$\forall h \in H,\ \forall g \in G \quad h.g = h \times g$$

Montrer que $(H, \times)$ opère sur G par translation à gauche (i.e. que les conditions données dans la définition d'opération d'un groupe sont bien vérifiées).

b) Exemple : opération par automorphismes intérieurs Soit $(G, \times)$ un groupe, on s'intéresse à l'application $. : G \times G \to G$ définie par

$$\forall g \in G,\ \forall x \in G \quad g.x = g \times x \times g^{-1}$$

Montrer que G opère sur lui-même par cette application (on dit que G opère par automorphismes intérieurs).

3) Étude des orbites

On considère un groupe $(G, \times)$ opérant sur un ensemble X par une application notée «.». On définit, pour $x \in X$, l'orbite de x, notée $\omega(x)$, comme l'ensemble des $g.x$ pour g parcourant G :

$$\forall x \in X \quad \omega(x) = \{\, g.x \mid g \in G \,\}$$

Pour x fixé appartenant à X, on note H_x et on appelle stabilisateur de x l'ensemble des éléments de g laissant x invariant :

$$H_x = \{\, g \in G \mid g.x = x \,\}$$

En outre, on dit que x est un *point fixe de X sous G* si pour tout $g \in G$, on a $g.x = x$, autrement dit, si $H_x = G$. Et enfin, on note X^G l'ensemble des points fixe de X sous G : $X^G = \{\, x \in X \mid H_x = G \,\}$.

a) Montrer que pour tout $x \in X$, H_x est un sous-groupe de G.

b) On suppose désormais que X et G sont finis. Soit $x \in X$. Montrer qu'on a $|G| = |\omega(x)| \times |H_x|$ (on pourra s'intéresser aux antécédents de chaque élément de $\omega(x)$ par l'application $g \mapsto g.x$).

c) Montrer que pour tout $(x, y) \in X^2$, $\omega(x)$ et $\omega(y)$ sont disjoints ou égaux.

d) En déduire que l'ensemble Ω des orbites est une partition de X et qu'on a

$$|X| = \sum_{\omega \in \Omega} \omega$$

e) En déduire

$$|X| = \left|X^G\right| + \sum_{\substack{\omega \in \Omega \\ |\omega| \neq 1}} |\omega|$$

4) Application : théorème de Lagrange

Soit $(G, \times)$ un groupe fini et H un sous-groupe de G. On fait opérer H sur G par translation à gauche.

a) Montrer qu'alors toutes les orbites ont même cardinal que H.

b) En déduire le théorème de Lagrange : l'ordre de tout sous-groupe d'un groupe fini divise l'ordre du groupe.

c) En déduire que dans tout groupe G fini, l'ordre de tout élément divise l'ordre du groupe.

d) Montrer que si l'ordre de G est un nombre premier, alors il s'agit d'un groupe cyclique, i.e. il existe $x \in G$ vérifiant $G = \langle x \rangle$.

5) Autre application : structure d'un groupe à pq éléments

Soit p et q deux nombres premiers distincts et $(G, \times)$ un groupe fini d'ordre pq. On fait alors opérer G sur lui-même (ainsi, $X = G$) par automorphismes intérieurs. On va montrer que G possède alors nécessairement un sous-groupe d'ordre p. Par l'absurde, on suppose que cela n'est pas le cas.

a) Montrer que X^G est un sous-groupe de G. Montrer que ce sous-groupe est commutatif.

b) Montrer que, en notant x_ω un élément quelconque de chaque $\omega \in \Omega$,

$$|X| = \left|X^G\right| + \sum_{\substack{\omega \in \Omega \\ |\omega| \neq 1}} |G|/|H_{x_\omega}|$$

et en déduire que nécessairement l'ordre de X^G est divisible par p puis que $X^G = G$.

c) On choisit dans G un élément x différent du neutre. Montrer que si l'ordre de x était pq, il existerait un sous-groupe de G d'ordre p. En déduire que x est d'ordre q. On pose $H = \langle x \rangle$.

d) On note G/H l'ensemble $\{\, Hg \mid g \in G \,\}$ (où Hg désigne $\{\, hg \mid h \in H \,\}$). Pour A et B deux éléments de G/H, on note $A\#B$ l'ensemble des produits des éléments de A et de B :

$$A\#B = \{\, xy \mid x \in A \text{ et } y \in B \,\}$$

Montrer que pour tout $(g, g') \in G^2$, on a $(Hg)\#(Hg') = H(gg')$ et que $(G/H, \#)$ est un groupe.

e) Montrer que $|G/H| = p$. En déduire qu'il existe $g \in G$ tel que $G/H = \langle Hg \rangle$.

f) En déduire que l'ordre de g est un multiple de p.

g) Montrer qu'alors G possède un sous-groupe d'ordre p.

h) Conclure.

6) Structure des groupes à 6 éléments Soit G un groupe à 6 éléments.

a) Montrer que G admet un sous-groupe H à trois éléments, de la forme $\{ 1_G, a, a^2 \}$.

b) Soit $s \in G \setminus H$. Montrer que $G = H \cup \{ s, sa, sa^2 \}$.

c) On suppose dans cette question que $s^2 \neq 1_G$. Montrer que $G = \left\{ s^k \;\middle|\; k \in [\![0, 5]\!] \right\}$. En déduire que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

d) On suppose dans cette question que $s^2 = 1_G$ et que G n'est pas cyclique. Montrer que G est isomorphe au groupe des isométries laissant invariant un triangle équilatéral, i.e. on a $s^2 = 1_G$, $sa = a^2 s$ et $sa^2 = as$. Ce groupe est appelé le groupe diédral D_3 (il est également isomorphe au groupe des permutations de trois éléments).

— **FIN** —