

Devoir n° 3

(À remettre le 30 octobre 2006)

Soit $(G, *)$ un groupe fini d'ordre n et d'élément neutre e . Pour $p \in \mathbb{Z}$, on pose $\text{Sol}(G, p) = \{g \in G \mid g^p = e\}$ et on note $r(p)$ le cardinal de $\text{Sol}(G, p)$. On suppose désormais que p est un nombre premier fixé qui divise n . On se propose de vérifier la propriété générale suivante sur quelques exemples, puis de la démontrer :

(P) *Le nombre $r(p)$ (noté simplement r) est un multiple non nul de p .*

1) *Exemples : (Il n'est pas nécessaire d'avoir traité cette question pour faire le reste du problème).* On considère les groupes suivants :

$$G_1 = (\mathbb{Z}/3\mathbb{Z}, +), \quad G_2 = (\mathbb{Z}/12\mathbb{Z}, +), \quad G_3 = \mathfrak{S}_3 = \text{Groupe du triangle équilatéral.}$$

Préciser l'ordre $\text{card } G_i$ ($i = 1, 2$ et 3) de ces groupes. Calculer r : a) Lorsque $G = G_1$ et $p = 3$. b) Lorsque $G = G_2$ et $p = 3$. c) Lorsque $G = G_3$ et $p = 2$ ou $p = 3$. Dans chacun des cas, vérifier la propriété **(P)**.

On cherche désormais à démontrer (P).

2) On considère le sous-ensemble E de $G^p = G \times G \times \dots \times G$ (p fois), défini par $E = \{(g_1, \dots, g_p) \in G^p \mid g_1 * g_2 * \dots * g_p = e\}$. Calculer $\text{card } E$ en fonction de n et de p . Constaté que c'est un nombre divisible par p .

3) On considère le sous-ensemble

$$E = \{(g_1, \dots, g_p) \in G^p \mid g_1 * g_2 * \dots * g_p = e\} \quad \text{de} \quad G^p = G \times G \times \dots \times G \quad (p \text{ fois}).$$

Vérifier que l'application $T : E \rightarrow E$ donnée par

$$T(g_1, g_2, \dots, g_{p-1}, g_p) = (g_2, g_3, \dots, g_p, g_1)$$

est un élément de \mathfrak{S}_E , le groupe des bijections de E dans lui-même. Préciser T^{-1} .

4) On note $K = \langle T \rangle$ le sous-groupe engendré par T dans \mathfrak{S}_E et on considère l'épimorphisme canonique $p \mapsto T^p$ de \mathbb{Z} sur K . Montrer que $T^p = \text{Id}_E$ et que $T^{-1} = T^{p-1}$.

5) Soit $s = (g_1, g_2, \dots, g_p) \in E$.

a) Montrer que $T(s) = s \Leftrightarrow \exists g \in \text{Sol}(G, p)$, tel que $s = (g, g, \dots, g)$.

b) On suppose maintenant qu'il existe un entier $q \in \mathbb{Z} \setminus p\mathbb{Z}$ tel que $T^q(s) = s$. Montrer que pour tout couple (u, v) d'éléments de \mathbb{Z} , on a $T^{up+vq}(s) = s$. En utilisant le fait que p est premier, en déduire que nécessairement $T(s) = s$.

6) On note \mathcal{R} la relation définie dans E par

$$(g_1, \dots, g_p) \mathcal{R} (g'_1, \dots, g'_p) \iff \exists r \in \mathbb{Z}, \text{ tel que } (g'_1, \dots, g'_p) = T^r(g_1, \dots, g_p).$$

a) Montrer que \mathcal{R} est une relation d'équivalence.

b) À titre d'exemple, donner les éléments de E et décrire l'ensemble E/\mathcal{R} dans le cas particulier où $G = G_1$ et où $p = 3$.

c) Soit $\mathcal{C}(s)$ la classe d'équivalence modulo \mathcal{R} de $s \in E$. Montrer que $\mathcal{C}(s) = \bigcup_{0 \leq q < p} \{T^q(s)\}$. En déduire que chaque classe d'équivalence modulo \mathcal{R} possède 1 ou p éléments.

7) On note a (resp. b) le nombre de classes d'équivalence modulo \mathcal{R} ayant respectivement 1 et p éléments. Comparer a et r . Montrer que $n^{p-1} = a + bp$.

8) En déduire la propriété **(P)**.

9) Montrer que G contient au moins un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$.