UPMC Licence L3 de mathématiques 14-15

LM 371 - Théorie des groupes

Examen partiel du 30 Octobre 2014

Durée: 2 heures

Les documents, calculatrices, portables ... ne sont pas autorisés.
Les 3 énoncés sont indépendants.
Les réponses devront être justifiées.

Barême (sur 25 points) : I = 9 pts, II = 6 pts, III : 10 pts.

I

On considère la permutation $\sigma = (16)(1547)(2137)(136)$ du groupe symétrique $\mathcal{S}_7$.

1°/ Calculer la signature de σ.

2°/ Donner la décomposition de σ en produits de cycles disjoints.

3°/ Calculer l'ordre de σ, puis l'ordre de σ^{10}.

4°/ Donner les décompositions de σ^{27} et de σ^{26} en produits de cycles disjoints.

II

Pout tout entier $n > 1$, on note G_n le groupe $Aut(\mathbb{Z}/n\mathbb{Z})$.

1°/ Montrer que si $n = p$ est un nombre premier, l'ordre de G_p est égal à $p - 1$. On admettra pour la suite que G_p est un groupe cyclique.

2°/ [Hors barême] On suppose que $n = pq$, où p et q sont deux nombres premiers distincts. Montrer que les groupes $G_p \times G_q$ et G_{pq} sont isomorphes. Ainsi, G_{pq} est un groupe abélien, isomorphe au groupe $\big(\mathbb{Z}/(p-1)\mathbb{Z}\big) \times \big(\mathbb{Z}/(q-1)\mathbb{Z}\big)$.

3°/ On suppose désormais que $n = 247 = 13 \times 19$. Déterminer les facteurs invariants et les diviseurs élémentaires du groupe G_{247}.

4°/ Déterminer le nombre d'éléments d'ordre 3 du groupe G_{247}.

T.S.V.P

III

Soient G un groupe fini d'orde pair, et $f : G \to G$ un endomorphisme du groupe G, pour lequel on pose $f^2 = f \circ f$. On considère les deux parties

$$S = \{x \in G : f(x) = x^{-1}\} \text{ et } H = \{x \in G : f^2(x) = x\}$$

de G. Si X est une partie de G, on note $|X|$ le nombre d'éléments de X.

1°/ (Deux exemples)

i) On prend pour G le groupe $\mathbb{Z}/6\mathbb{Z}$ (dont on note la loi additivement), et on considère l'endomorphisme $f : G \to G$ défini, pour tout élément x de G, par $f(x) = 2x$. Montrer que $H \neq G$, et déterminer tous les éléments de H et de S.

ii) On prend pout G le groupe symétrique $\mathcal{S}_3$. On note τ la transposition (12), et on considère l'application $f : G \to G$ définie, pour tout élément x de G, par $f(x) = \tau x \tau^{-1}$. Montrer que f est un automorphisme de G, que $H = G$, et que S admet exactement 4 éléments, que l'on déterminera.

2°/ On se place désormais dans le cas général.

i) Montrer que H est un sous-groupe de G contenant S.

ii) On suppose ici que $|S| > \frac{|G|}{2}$. Montrer que $H = G$.

3°/ On suppose maintenant que $|S| = \frac{|G|}{2}$, mais on fait l'hypothèse supplémentaire que f est un automorphisme de G. On se propose d'en déduire qu'ici encore, $H = G$.

i) Montrer que $f(H) = H$.

ii) Montrer que si $H \neq G$, tout élément a de G n'appartenant pas à H vérifie $f(a) = ah$, où h est un élément de H. En déduire qu'alors, $f^2(a) = a$, et conclure.

Esquisse de corrigé

I. $1^o/$ $\epsilon(\sigma) = (-1) \times (-1)^{4-1} \times (-1)^{4-1} \times (-1)^{3-1} = -1$.

$2^o/$ $\sigma = \begin{pmatrix} 1 & 6 & 3 \\ 6 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 2 & 5 & 4 & 7 \\ 5 & 4 & 7 & 2 \end{pmatrix} = (163)(2547)$.

$3^o/$ $ord(\sigma) = ppcm(3,4) = 12$, donc $\sigma^{10} = \sigma^{-2}$ est d'ordre $\frac{12}{2} = 6$.

$4^o/$ $\sigma^{27} = \sigma^3 = (2547)^3 = (2547)^{-1} = (7452)$, et $\sigma^{26} = \sigma^2 = (163)^{-1}(2547)^2 = (361)(24)(57)$.

II. $1^o/$ L'application $\phi : G_n \to \mathbb{Z}/n\mathbb{Z} : f \mapsto \phi(f) := f(\bar{1})$ établit une bijection entre G_n et l'ensemble X_n des générateurs de $\mathbb{Z}/n\mathbb{Z}$, donc des classes $\bar{a}$ modulo n des entiers a premiers à n. Pour $n = p$, $X_n = \{\bar{1}, ..., \overline{p-1}\}$, donc $|G_p| = p - 1$. (Et puisqu'il est cyclique, $G_p \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.)

$2^o/$ Entre 1 et $pq - 1$, il y a $q - 1$ nombres divisibles par p et $p - 1$ nombres divisibles par q, mais aucun par pq, donc X_{pq} a pour cardinal $(p-1)(q-1)$. Par ailleurs, l'application $\psi : G_p \times G_q \to Aut\big((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})\big) : (f,g) \mapsto \{\psi(f,g) : (x,y) \mapsto (f(x), g(y))\}$ est un homomorphisme de groupes injectif. D'après le lemme chinois, $Aut\big((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})\big) \simeq Aut(\mathbb{Z}/pq\mathbb{Z}) = G_{pq}$, qui est d'ordre $\sharp(X_{pq}) = (p-1)(q-1) = |G_p| \times |G_q|$. Donc ψ est un isomorphisme, et G_{pq} est bien isomorphe au produit des deux groupe cyclique indiqués.

$3^o/$ $G_{247} \simeq (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/18\mathbb{Z}) \simeq (\mathbb{Z}/4) \times (\mathbb{Z}/3) \times (\mathbb{Z}/2) \times (\mathbb{Z}/9) \simeq (\mathbb{Z}/6) \times (\mathbb{Z}/36)$. Ses facteurs invariants sont donc $\{6, 36\}$, et ses diviseurs élémentaires sont $\{(2,4); (3,9)\}$.

$4^o/$ Les éléments d'ordre 3 de $G \simeq G(2) \times G(3)$ s'identifient à ceux de $G(3) = (\mathbb{Z}/3) \times (\mathbb{Z}/9)$, donc sont de la forme (x,y), avec $x = 0, 1, 2$ (mod. 3) et $y = 0, 3, 6$ (mod. 9), mais $(x,y) \neq (0,0)$. Il y en a ainsi $9 - 1 = 8$.

III. $1^o/$ i) $H = \{x \in \mathbb{Z}/6\mathbb{Z}, 4x = x\} = \{x \in \mathbb{Z}/6\mathbb{Z}, 3x = 0\} = \{\bar{0}, \bar{2}, \bar{4}\}$ est strictement inclus dans G. Et $S = \{x \in \mathbb{Z}/6\mathbb{Z}, 2x = -x\} = \{x \in \mathbb{Z}/6\mathbb{Z}, 3x = 0\}$ coïncide avec H. - ii) Comme $f = Int(\tau)$, c'est un automorphisme de G. Comme τ est d'ordre 2, $f^2 = Int(\tau^2) = id_G$, donc $H = G$. Enfin, $\tau(i_1...i_k)\tau^{-1} = (\tau(i_1)...\tau(i_k))$, donc l'élément neutre, les deux 3-cycles de G et le 2-cycle (12) appartiennent à S, mais pas les deux autres.

$2^o/$ i) Pour $x, y \in H$, $f^2(xy^{-1}) = f^2(x)f^2(y)^{-1} = xy^{-1}$, donc H est un sous-groupe de G. Si $x \in S$, $f^2(x) = f(x^{-1}) = f(x)^{-1} = (x^{-1})^{-1} = x$, donc $S \subset H$. (Mais noter que S n'est en général pas un sous-groupe de G, cf. $1^o/$ ii.) - ii) Si $|S| > \frac{|G|}{2}$, H, qui est un sous-groupe de G d'ordre $\geq |S|$, est alors d'indice $\frac{|G|}{|H|} < 2$, donc égal à 1, et $H = G$.

$3^o/$ i) Puisque f est injectif, il suffit de montrer que $f(H) \subset H$. Or pour tout $x \in H$, $y := f(x)$ vérifie $f^2(y) = f^3(x) = f(f^2(x)) = f(x) = y$, donc $f(x) \in H$. - ii) Par hypothèse, H est un sous-groupe d'indice 2 de G, donc G est la réunion disjointe des deux classes à gauche H et aH (d'ailleurs égale à Ha, mais peu importe). Comme la bijection f vérifie $f(H) = H$, on a nécessairement $f(aH) = aH$ et $\exists h \in H, f(a) = ah$. Notons de plus que H, qui contient S, a le même cardinal, donc $H = S$. Ainsi, $f(h) = h^{-1}$, et $f^2(a) = f(f(a)) = f(ah) = f(a)f(h) = f(a)h^{-1} = ahh^{-1} = a$. Par conséquent, a appartient à H, en contradiction avec l'hypothèse de départ, donc H remplit nécessairement tout G.