UPMC Licence L3 de mathématiques 13-14

LM 371 - Théorie des groupes

Examen partiel du 7 Novembre 2013

Durée: 1 heure 30

Les documents, calculatrices, portables ... ne sont pas autorisés.
Les 3 énoncés sont indépendants.
Les réponses devront être justifiées.
Barême approximatif (sur 25 points) : I = 5 pts; II = 8 pts; III = 12 pts.

I

Soit G un groupe fini, *d'ordre pair*. On se propose de montrer que G *admet au moins un élément d'ordre 2.*

1°/ On considère sur G la relation $\mathfrak{R}$ définie par : $x \,\mathfrak{R}\, y$ si et seulement si $y = x$ ou $y = x^{-1}$. Montrer que $\mathfrak{R}$ est une relation d'équivalence.

2°/ Pour $x \in G$, soit $C\ell(x)$ la classe d'équivalence de x. Déterminer, suivant que x est un élément de G d'ordre 1, d'ordre 2, ou d'ordre > 2, le nombre d'éléments de $C\ell(x)$.

3°/ Conclure.

II

1°/ Soit G_1 un groupe d'ordre 31. Montrer que G_1 est un groupe cyclique.

2°/ Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre 27.

3°/ Soit G_3 un groupe abélien d'ordre 30.

i) Montrer que G_3 est cyclique.
ii) Calculer le nombre d'éléments de G_3 d'ordre 5.

4°/ i) Soient H un groupe non abélien, et K un groupe quelconque. Montrer que le groupe produit $H \times K$ n'est pas abélien.

ii) Donner un exemple d'un groupe non abélien G_4 d'ordre 30.

TSVP

III

Soit $G = GL_2(\mathbb{R})$ le groupe des matrices réelles 2×2 inversibles, muni de la loi de produit des matrices. On considère les éléments

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

de G.

1°/ i) Calculer l'ordre de s.
ii) Calculer l'ordre de r.

2°/ Montrer que $srs^{-1} = r^{-1}$.

3°/ On désigne par $\mathbb{D} =< \{s, r\} >$ le sous-groupe de G engendré par s et r, par $R =< r >$ le sous-groupe (cyclique) de $\mathbb{D}$ engendré par r, et par $S =< s >$ le sous-groupe (cyclique) de $\mathbb{D}$ engendré par s.

i) Montrer que R est distingué dans $\mathbb{D}$.
ii) Montrer que S n'est pas distingué dans $\mathbb{D}$.

4°/ On reprend les notations du **3°**/, et on note $f : \mathbb{D} \to \mathbb{R}^*$ l'application qui à tout élément g de $\mathbb{D}$, attache le déterminant $f(g) := det(g)$ de la matrice inversible g. (Ici, $\mathbb{R}^*$ désigne l'ensemble des nombres réels non nuls, qu'on munit de sa structure de groupe multiplicatif.)

i) Montrer que f est un homomorphisme de groupes.
ii) Calculer l'image $Im(f) := f(\mathbb{D})$ de f.
iii) Déterminer le noyau de f.
iv) En déduire l'ordre du groupe $\mathbb{D}/R$, et celui de $\mathbb{D}$.

Corrigé

I.1/ La relation $\mathfrak{R}$ est réflexive ($x\mathfrak{R}x$). Comme $y = x^{-1} \Rightarrow x = (x^{-1})^{-1} = y^{-1}$, elle est symétrique ($x\mathfrak{R}y \Rightarrow y = x$ ou $x^{-1} \Rightarrow x = y$ ou $y^{-1} \Rightarrow y\mathfrak{R}x$). Et elle est transitive ($x\mathfrak{R}y$ et $y\mathfrak{R}z \Rightarrow x\mathfrak{R}z$), puisque les 4 expressions $(x^{\pm 1})^{\pm 1}$ valent x ou x^{-1}.

2/ La classe d'équivalence $C\ell(x)$ de $x \in G$ est constituée des éléments x et x^{-1}. Ces éléments sont égaux si et slt si $x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow$ l'ordre $ord(x)$ de x divise 2. Donc $C\ell(x)$ a un élément si x est d'ordre 1 ou si x est d'ordre 2, tandis que $C\ell(x)$ a deux éléments si x est d'ordre > 2.

3/ Le cardinal $|G|$ de G est égal à la somme des cardinaux de ses différentes classes d'équivalence. Soient n_1, resp. n_2, resp. n_3, le nombre d'éléments de G d'ordre 1, resp. 2, resp. d'ordre > 2. On a $n_1 = 1$ car e est le seul élément d'ordre 1. De 2/, on déduit donc que $|G| = 1 + n_2 + 2n_3$. Comme $|G|$ est pair, n_2 est forcément impair, donc $n_2 \geq 1$, et il y a bien au moins un élément dans G d'ordre 2.

II.1/ Soit $x \neq e$ un élément de G_1. Son ordre est > 1, et divise $|G_1| = 31$. Or 31 est un nombre premier. Donc $ord(x) = 31$, et $G =< x >$ est engendré par x, donc est cyclique.

2/ Les diviseurs élémentaires d'un 3-groupe d'ordre 3^3 sont de la forme $\{3^{\alpha_1}, ..., 3^{\alpha_k}\}$, avec des entiers $0 < \alpha_1 \leq ... \leq \alpha_k$ de somme égale à 3. À isomorphisme près, il y a donc trois groupes d'ordre 27 : $G_2 = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, $G_2' = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$ et $G_2'' = \mathbb{Z}/27\mathbb{Z}$.

3/ i) Les nombres premiers divisant 30 sont 2, 3, 5 et $|G_3| = 2.3.5$. La décomposition primaire de $G = G_3$ s'écrit donc $G(2) \times G(3) \times G(5)$, avec $|G(p)| = p$ pour $p = 2, 3, 5$. Pour tout nombre premier p, le seul groupe d'ordre p est, à isomorphisme près, le groupe $\mathbb{Z}/p\mathbb{Z}$. Donc $G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$. Du lemme chinois, on déduit que $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/6\mathbb{Z})$, et que $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \simeq (\mathbb{Z}/30\mathbb{Z})$. Donc G_3, isomorphe à $\mathbb{Z}/30\mathbb{Z}$, est cyclique. ii) $\overline{x} \in \mathbb{Z}/30\mathbb{Z}$, représenté par $x \in \mathbb{Z}$, est d'ordre 5 si et slt si $\overline{x} \neq \overline{0}$ et $5\overline{x} = \overline{0}$, c-à-d. $30|5x, 30 \not| x$, soit $x \equiv 6, 12, 18, 24 \mod 30$. Donc G_3 admet 4 éléments d'ordre 5.

4/ i) Soient h_1, h_2 deux éléments de H tels que $h_1h_2 \neq h_2h_1$, et k_1, k_2 deux éléments quelconques de K. Alors, les éléments $g_1 = (h_1, k_1), g_2 = (h_2, k_2)$ de $H \times K$ ne commutent pas, puisque $g_1g_2 = (h_1h_2, k_1k_2)$ a une première composante h_1h_2 différente de la première composante h_2h_1 de g_2g_1. ii) Le groupe symétrique S_3 est un groupe non abélien d'ordre 6. Le groupe $G_4 = S_3 \times (\mathbb{Z}/5\mathbb{Z})$ n'est donc pas abélien, et son ordre vaut $6 \times 5 = 30$.

III.1/ i) L'élément neutre de G est $e = \mathbf{I}_2$. Comme $s \neq e$ et $s^2 = e$, s est d'ordre 2. ii) $r^2 = -\mathbf{I}_2, r^4 = e$, donc $2 < ord(r)$, qui divise 4, donc r est d'ordre 4.

2/ s, d'ordre 2, est égal à s^{-1}, tandis que r^{-1}, d'ordre 4, est égal à $r^3 = -\mathbf{I}_2.r = -r$. La vérification est alors immédiate.

3/ i) De $s^{-1} = s$ et $r^{-1} = r^3$, on déduit que tout élément de $\mathbb{D} =< \{r, s\} >$ est un produit de copies de s et de r. Il suffit donc de montrer que rRr^{-1} et sRs^{-1} sont inclus (donc égaux) à R. C'est évident pour r, et cela découle de 2/ pour s. ii) En revanche $rsr^{-1} = rs.srs^{-1} = r^2s = -s$ n'appartient pas à $S = \{e, s\}$, donc S n'est pas distingué dans $\mathbb{D}$.

4/ i) Pour $x, y \in G, det(xy) = det(x).det(y)$, donc pour tout $x, y \in \mathbb{D}, f(xy) = f(x)f(y)$, et f est bien un homomorphisme du groupe $\mathbb{D}$ dans le groupe multiplicatif $\mathbb{R}^*$. ii) Le sous-groupe $f(\mathbb{D})$ de $\mathbb{R}^*$ est engendré par $f(s) = -1$ et $f(r) = 1$. C'est donc le sous-groupe $\{1, -1\}$, d'ordre 2, du groupe multiplicatif $\mathbb{R}^*$. iii) On a $f(R) = \{1\}$, donc $R \subset Ker(f)$. Si l'écriture de $x \in \mathbb{D} =< \{r, s\} >$ fait intervenir N fois l'élément s, on aura donc $f(x) = (f(s))^N = (-1)^N$, et $x \in Ker(f)$ si et slt si N est pair. De $s^2 = e$ et $sRs = R$, on déduit alors que $x \in R$, et $Ker(f) = R$. iii) D'après le théorème de décomposition des homomorphismes, f induit donc un isomorphisme de $\mathbb{D}/R$ vers $Im(f)$, et $|(\mathbb{D}/R)| = |Im(f)| = 2$, de sorte que $|\mathbb{D}| = 2.|R| = 8$.