UPMC Licence L3 de mathématiques 15-16
D. Bertrand *3M270 - Algèbre*

Examen partiel du 30 Octobre 2015

Durée: 2 heures

Les documents, calculatrices, portables ... ne sont pas autorisés.
Les 4 *énoncés sont indépendants.* **Les réponses devront être justifiées.**
Barême approximatif (sur 25 points) : I = 5 pts; II = 8 pts; III = 6 pts; IV = 8 pts.

I

On considère la permutation $\sigma = (3546)(357)(172)$ du groupe symétrique $\mathcal{S}_7$.

1°/ [1 pt] Calculer la signature de σ.

2°/ [1 pt] Donner la décomposition de σ en produits de cycles de supports disjoints.

3°/ [2 pts] Calculer l'ordre de σ, puis l'ordre de σ^{15}.

4°/ [1 pt] Donner la décomposition de σ^{26} en produits de cycles de supports disjoints.

II

Soit G un groupe fini. Un sous-groupe H de G est dit maximal s'il est distinct de G et si le seul sous-groupe de G contenant H strictement est G lui-même.

1°/ Ici, G est le groupe cyclique $\mathbb{Z}/28\mathbb{Z}$.
i) [2 pts] Donner la liste de tous les sous-groupes de G.
ii) [1 pt] Parmi ceux-ci, lesquels sont des sous-groupes maximaux ?

2°/ Ici, G est le groupe symétrique $\mathcal{S}_n$, où n est un entier ≥ 3. On rappelle que $\mathcal{S}_n$ est engendré par les transpositions $(1\ 2), (1\ 3), ..., (1\ n)$, et on pose:

$$H = \{\sigma \in G, \sigma(n) = n\}.$$

i) [1 pt] Montrer que H est un sous-groupe de G.
ii) [2 pts] Soit τ un élément de G n'appartenant pas à H. Montrer qu'il existe une transposition $\sigma = (i\ j) \in H$ et un entier $k \in [1, n-1]$ tels que $\tau\,\sigma\,\tau^{-1} = (k\ n)$.
iii) [2 pts] Montrer que H est un sous-groupe maximal de G.

TSVP

III

Soit G un groupe abélien d'ordre fini > 1. On rappelle qu'il existe une unique famille d'entiers $d_1, ..., d_r$ strictement supérieurs à 1 (appelés facteurs invariants de G) tels que $d_i | d_{i+1}$ pour tout $i = 1, ..., r-1$ et $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times ... \times (\mathbb{Z}/d_r\mathbb{Z})$.

1°/ Ici, $G = (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/25\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$.

i) [1 pt] Déterminer les facteurs invariants de G.

ii) [2 pts] Calculer le nombre d'éléments de G d'ordre 5.

2°/ Ici, G est le groupe multiplicatif $(\mathbb{Z}/55\mathbb{Z})^*$

i) [1 pt] Calculer l'ordre de G.

ii) [2 pts] Déterminer les facteurs invariants de G.

IV

Soient G un groupe fini d'ordre $N > 1$ et H un sous-groupe distingué de G. À tout élément g de G, on attache l'application $f_g : H \to G : h \mapsto f_g(h) := ghg^{-1}$.

1°/ i) [1 pt] Montrer que pour tout $g \in G$, $\quad Im(f_g) \subset H$ et que f_g est un automorphisme du groupe H.

ii) [1 pt] Montrer que l'application $f : g \mapsto f(g) := f_g$ est un homomorphisme de groupes de G dans $Aut(H)$.

iii) [2 pts] Montrer que pour tout $g \in G$, l'ordre de l'élément f_g du groupe $Aut(H)$ divise N.

2°/ Soit p le plus petit nombre premier divisant N. On suppose ici que le sous-groupe H de G est d'ordre p.

i) [2 pts] Montrer que pour tout $g \in G$, l'ordre de l'élément f_g du groupe $Aut(H)$ divise $p - 1$.

ii) [2 pts] Montrer que pour tout $g \in G$, $f_g = id_H$, et que H est contenu dans le centre de G.

Corrigé

I. $1^o/$ La signature $\varepsilon : \mathcal{S}_7 \to \{\pm 1\}$ est un homomorphisme de groupes, et la signature d'un cycle de longueur ℓ est $(-1)^{\ell-1}$, donc $\varepsilon(\sigma) = (-1)^{3+2+2} = -1$.

$2^o/$ $\sigma = \begin{pmatrix} 1 & 5 & 7 & 2 \\ 5 & 7 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 6 \\ 4 & 6 & 3 \end{pmatrix} = c_1 c_2$, où $c_1 = (1572), c_2 = (346)$.

$3^o/$ Puisque $o(c_1) = 4$ et $o(c_2) = 3$ sont premiers entre eux et que c_1 et c_2 commutent, l'ordre de $\sigma = c_1 c_2$ vaut $4 \times 3 = 12$. [Ou dire que c_1 et c_2 étant des cycles disjoints, $o(\sigma) = ppcm(o(c_1), o(c_2)) = 12$.] L'ordre de σ^{15} vaut $\frac{o(\sigma)}{d}$, où $d = pgcd(o(\sigma), 15) = 3$, donc $o(\sigma^{15}) = \frac{12}{3} = 4$. [Autre méthode : comme $o(\sigma) = 12$, $\sigma^{15} = \sigma^{12}\sigma^3 = \sigma^3$, et comme $3|o(\sigma)$, $o(\sigma^3) = \frac{o(\sigma)}{3} = 4$.]

$4^o/$ $\sigma^{26} = (\sigma^{12})^2\sigma^2 = \sigma^2 = c_1^2 c_2^2 = c_1^2 c_2^{-1} = (17)(25)(364)$.

II. $1^o/$ - i) L'application qui, à un entier d divisant 28, attache le sous-groupe $G_d := d\mathbb{Z}/28\mathbb{Z}$ du groupe cyclique $G = \mathbb{Z}/28\mathbb{Z}$ établit une bijection entre l'ensemble $\{1, 2, 4, 7, 14, 28\}$ des diviseurs ≥ 1 de 28 et l'ensemble des sous-groupes de G. Donc la liste des (six) sous-groupes de G est : $G_1 = \mathbb{Z}/28\mathbb{Z} = G$ (d'ordre 28), $G_2 = 2\mathbb{Z}/28\mathbb{Z}$ (d'ordre 14), $G_4 = 4\mathbb{Z}/28\mathbb{Z}$ (d'ordre 7), $G_7 = 7\mathbb{Z}/28\mathbb{Z}$ (d'ordre 4), $G_{14} = 14\mathbb{Z}/28\mathbb{Z}$ (d'ordre 2) et $G_{28} = 28\mathbb{Z}/28\mathbb{Z} = \{0\}$ (d'ordre 1). - ii) Étant donnés deux diviseurs d, d' de 28, le groupe $G_{d'}$ contient G_d si et seulement si $d \in d'\mathbb{Z}$, c-à-d. d' divise d. Par conséquent, G_d est maximal si et slt si $d \neq 1$ et $d'|d \Rightarrow d' = d$ ou 1. Les sous-groupes maximaux de G correspondent donc aux diviseurs premiers de 28, soit : $G_2 = 2\mathbb{Z}/28\mathbb{Z}$ et $G_7 = 7\mathbb{Z}/28\mathbb{Z}$.

$2^o/$ - i) H est non vide et pour tout $\tau \in G, n = \tau(n) \Rightarrow \tau^{-1}(n) = \tau^{-1}\tau(n) = n$. Ainsi, pour tout σ, τ dans H, $\sigma\tau^{-1}(n) = \sigma(n) = n$, et $\sigma\tau^{-1} \in H$, qui est donc bien un sous-groupe de G. - ii) Posons $j := \tau^{-1}(n)$. Comme $\tau \notin H$, $j \neq n$ (sans quoi $\tau(n) = n$), donc $j \in [1, ..., n-1]$. Puisque $n \geq 3$, il existe un indice $i \in [1, ..., n-1]$ distinct de j. Alors, l'indice $k := \tau(i)$ est distinct de n (car $i \neq j \Rightarrow \tau(i) \neq \tau(j)$), donc $k \in [1, ..., n-1]$. Dans ces conditions, $\tau(i\ j)\tau^{-1} = (\tau(i)\ \tau(j)) = (k\ n)$, et $(i\ j)$, de support disjoint de n, appartient à H. Ainsi, $\sigma := (i\ j)$ et k vérifient toutes les conditions demandées. - iii) Soient H' un sous-groupe de G contenant strictement H et $\tau \notin H$ un élément de H', pour lequel nous reprenons les notations $\sigma \in H$ et $k \in [1, ..., n-1]$ du (ii). Comme σ et $\tau \in H' < G$, $\tau\sigma\tau^{-1} \in H'$, qui contient donc la transposition $(k\ n)$. Par ailleurs, les transpositions $(k\ \ell)$, où $\ell \in [1, ..., n-1], \ell \neq k$, appartiennent toutes à H, donc à H'. Ainsi, H' contient les $n-1$ transpositions $(k\ \ell), \ell = 1, ..., n, \ell \neq k$. Or d'après le rappel (où l'on peut inverser le rôle de k et de 1), ces $n-1$ transpositions engendrent le groupe $\mathcal{S}_n = G$. Donc $H' = G$, et H est bien un sous-groupe maximal de G. [NB : "inverser le rôle de k et de 1" revient, pour $k \neq 1$, à considérer les conjuguées $(1\ k)(1\ m)(k\ 1) = (k\ m)(m \neq 1, k)$ et $(1\ k)(1\ k)(k\ 1) = (k\ 1)$ du système générateur du rappel; ces conjugués $(k\ m), m = 1, ..., n, m \neq k$, engendrent le conjugué $(1\ k)G(k\ 1) = G$ de G, donc forment aussi un système générateur.]

III. $1^o/$ - i) D'après le lemme chinois (et en écrivant $\mathbb{Z}/N$ pour $\mathbb{Z}/N\mathbb{Z}$), $G \simeq (\mathbb{Z}/3) \times (\mathbb{Z}/2^2) \times (\mathbb{Z}/5^2) \times (\mathbb{Z}/5) \times (\mathbb{Z}/3^2)$, et une nouvelle application du lemme chinois donne $G \simeq (\mathbb{Z}/3.5) \times (\mathbb{Z}/2^2.3^2.5^2)$. Les facteurs invariants de G sont donc $\{15, 900\}$. - ii) Si $G = G_1 \times G_2$ est un produit de groupes (disons abéliens pour avoir des notations additives),

les éléments d'ordre 5 de G sont de la forme (x_1, x_2), où $5x_1 = 0, 5x_2 = 0$ (c-à-d. x_1 et x_2 sont d'ordre divisant 5), *et* $\text{ppcm}(o(x_1), o(x_2)) = 5$. Puisque 5 est un nombre premier, cette dernière condition, sous les précédentes, revient à demander que $(x_1, x_2) \neq (0, 0)$. Les éléments d'ordre divisant 5 d'un groupe cyclique $\mathbb{Z}/N$ sont réduits à $\{0\}$ si 5 ne divise pas N, et forment dans le cas contraire l'unique sous-groupe $d\,\mathbb{Z}/N$ d'ordre 5 de $\mathbb{Z}/N$ (avec $d = \frac{N}{5}$). Il y en a donc 5 . Dans notre cas, G_1 et G_2 sont cycliques d'ordres divisibles par 5, donc G a $5 \times 5 = 25$ éléments d'ordre divisant 5, et $25 - 1 = 24$ éléments d'ordre 5.

$2^o/$ - i) L'ordre de G est donné par la fonction indicatrice d'Euler ϕ. Puisque 5 et 11 sont premiers entre eux, $|G| = \phi(55) = \phi(5)\phi(11)$, et puisque ce sont des nombres premiers, $|G| = (5-1)(11-1) = 40$. - ii) D'après le lemme chinois (version multiplicative), $G \simeq (\mathbb{Z}/5)^* \times (\mathbb{Z}/11)^* = \mathbb{F}_5^* \times \mathbb{F}_{11}^*$. Pour p premier, le groupe multiplicatif du corps fini $\mathbb{F}_p$ est cyclique d'ordre $p-1$, donc $G \simeq (\mathbb{Z}/4) \times (\mathbb{Z}/10)$. Le lemme chinois (version additive) entraîne alors que $G \simeq (\mathbb{Z}/2^2) \times (\mathbb{Z}/2) \times (\mathbb{Z}/5) \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/2^2.5)$. Les facteurs invariants de G sont donc $\{2, 20\}$.

IV. $1^o/$ - i) Soient $h \in H, g \in G$. Puisque $H \lhd G$, $f_g(h) := ghg^{-1} \in H$, donc $Im(f_g) \subset H$. Comme $f_g : H \to H$ est injective ($ghg^{-1} = gh'g^{-1} \Rightarrow h = h'$), et qu'elle est surjective ($\forall h' \in H, \exists h := g^{-1}h'g \in H, f_g(h) = h'$ [ou invoquer ici la finitude de l'ensemble H]), c'est une bijection de H sur H. Enfin, $f_g(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = f_g(h)f_g(h')$ pour tout $h, h' \in H$, donc f_g est un automorphisme du groupe H. - ii) Pour tout $g, g' \in G$ et $h \in H$, $f_{gg'}(h) = gg'hg'^{-1}g^{-1} = g(f_{g'}(h))g^{-1} = f_g(f_{g'}(h))$, donc $f_{gg'} = f_g \circ f_{g'}$, et $f : G \to Aut(H)$ est bien un homomorphisme de groupes. - iii) L'ordre de l'image $f_g = f(g) \in Aut(H)$ de g par l'homomorphisme f divise l'ordre de g, qui par Lagrange divise l'ordre N de G. Donc $o(f_g)$ divise N. [Ou écrire : $(f_g)^N = (f(g))^N = f(g^N) = f(e_G) = e_{Aut(H)}$. Ou encore : pour tout $h \in H$, $(f_g)^N(h) = f_g(f_g...(f_g(h))...) = g(g...(ghg^{-1})...g^{-1})g^{-1} = g^N hg^{-N} = h$, donc $(f_g)^N = id_H$.]

$2^o/$ - i) Comme $|H| = p$ est un nombre premier, tout élément $\neq e_H$ de H est d'ordre p. Donc H est un groupe cyclique, isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Par conséquent, $Aut(H) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $p-1$. D'après Lagrange, l'ordre de tout élément du groupe $Aut(H)$ divise $|Aut(H)|$. Donc $o(f_g)$ divise $p-1$. - ii) Puisque p est le plus petit diviseur premier de N, aucun des diviseurs premiers de $p-1$ ne divise N, de sorte que N et $p-1$ sont premiers entre eux, et leur pgcd vaut 1. Or pour tout $g \in G$, l'ordre de f_g divise à la fois N (cf. 1/iii) et $p-1$ (cf. 2/i)). Donc $o(f_g) = 1, f_g = e_{Aut(H)} = id_H$, et pour tout $h \in H, f_g(h) = h$. Autrement dit, pour tout $h \in H$, on a pour tout $g \in G$: $ghg^{-1} = h$, c-à-d. $gh = hg$, et H est inclus dans le centre $Z(G) = \{k \in G, \forall g \in G, kg = gk\}$ de G.