UPMC Licence L3 de mathématiques 14-15

LM 371 - Théorie des groupes

Examen du 6 Janvier 2015

Durée: 2 heures

Les documents, calculatrices, portables ... ne sont pas autorisés. Les 3 énoncés sont indépendants. Les réponses devront être justifiées.
Barême approximatif (sur 75 points) : I = 21 pts, II = 33 pts, III = 21 pts.

I

1°/ Soient G un groupe fini, de centre Z. On suppose que G/Z est un groupe cyclique. Montrer que G est un groupe abélien.

2°/ Soient p un nombre premier, et G un groupe d'ordre p^2. Montrer que G est un groupe abélien. (On rappelle que tout p-groupe non trivial admet un centre non trivial.)

3°/ Soit G un groupe non abélien d'ordre p^3.
i) Montrer que le centre Z de G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et que G/Z est isomorphe à $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.
ii) Soit H un sous-groupe de G d'ordre p^2. Montrer que H contient Z.
iii) Déterminer le nombre de sous-groupes de G d'ordre p^2.

4°/ Soit G un groupe fini tel que le groupe $Aut(G)$ soit cyclique. Montrer que G est un groupe abélien.

II

Soit G un groupe non abélien d'ordre $231 = 3 \times 7 \times 11$.

1^0/ Montrer que G contient un unique sous-groupe H_7 d'ordre 7, et un unique sous-groupe H_{11} d'ordre 11.

2^0/ Montrer que $H := H_7H_{11}$ est un sous-groupe de G, distingué dans G, et cyclique.

3^0/ Soit x un élément de G d'ordre 77. Montrer que x appartient à H, et calculer le nombre d'éléments de G d'ordre 77.

4^0/ Déterminer le nombre de 3-Sylows de G. Si K est l'un d'eux, montrer que G est isomorphe à un produit semi-direct, non direct, $H \rtimes_\tau K$ de H par K.

5^o/ i) Montrer qu'il n'existe pas de morphisme non trivial de K dans le groupe $Aut(H_{11})$.
ii) Montrer que $H_{11}K$ est un sous-groupe de G isomorphe au produit direct $H_{11} \times K$.

6^o/ i) Calculer le nombre d'éléments de G d'ordre 33.
ii) Calculer le nombre d'éléments de G d'ordre 21.

T.S.V.P

III

Soit G un groupe d'ordre $5\,! = 8 \times 3 \times 5$. On suppose que G est un groupe simple, c-à-d. que $\{e\}$ et G sont les seuls sous-groupes distingués de G.

1°/ Soit $\phi : G \to \Gamma$ un morphisme de G dans un autre groupe Γ. Montrer que ϕ est ou bien trivial ($\phi(G) = \{e\}$), ou bien injectif.

2°/ i) Déterminer le nombre de 5-Sylows de G.

ii) En déduire qu'il existe un morphisme non trivial f de G dans le groupe symétrique $\mathcal{S}_6$.

3°/ Soit $G' := f(G)$ l'image de G dans $\mathcal{S}_6$.

i) Montrer que $G' \simeq G$, et que G' est contenu dans le sous-groupe $\mathcal{A}_6$ de $\mathcal{S}_6$. (On pourra considérer la restriction à G' du morphisme de signature $\epsilon : \mathcal{S}_6 \to \{\pm 1\}$.)

ii) En faisant agir G' à gauche sur l'ensemble $\mathcal{A}_6/G'$, montrer que G' est un sous-groupe distingué de $\mathcal{A}_6$.

4°/ En déduire qu'il n'existe en fait aucun groupe simple d'ordre $5\,!$.

Corrigé

I. $1^o/$ (Comme $Z \lhd G$, G/Z est bien un groupe.) Soient $\overline{x}$ un générateur de ce groupe cyclique, n son ordre, et x un relevé de $\overline{x}$ à G. Alors, $\{x^i, i = 0, ..., n-1\}$ forme un système de représentants des classes à gauche modulo Z, et G est la réunion (disjointe) des $x^i Z$. Soient alors $y = x^i z$, $y' = x^{i'} z'$ $(z, z' \in Z)$ deux éléments quelconques de G. Comme z et z' sont centraux, $yy' = x^i x^{i'} zz' = x^{i'+i} z' z = y'y$, et G est bien abélien.
$2^o/$ Le centre Z de G est non trivial, donc d'ordre p^2 (auquel cas $G = Z$ est abélien), ou d'ordre p, auquel cas G/Z est un groupe d'ordre p, donc cyclique, et par $1/$, G est abélien (finalement, Z est toujours d'ordre p^2).
$3^o/$ i) Ce centre Z ne peut être d'ordre p^2, sans quoi G/Z, d'ordre p, serait cyclique, et G serait abélien. Donc Z, non trivial, est d'ordre p (et donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$). Par conséquent G/Z est d'ordre p^2, donc isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$. Le premier cas, cyclique, donne un groupe G abélien, donc on est forcément dans le 2e cas. - ii) Comme Z est d'ordre premier, $H \cap Z = \{e\}$ ou Z. Dans le premier cas, ZH aurait $p \times p^2$ éléments, donc coïnciderait avec G; mais Z est central et H, d'ordre p^2, est abélien, donc $G = ZH$ serait abélien. Ainsi, $H \cap Z = Z$, et $Z < H$. - iii) Les sous-groupes d'ordre p^2 contiennent Z, et sont donc en bijection avec les sous-groupes de $G/Z = (\mathbb{Z}/p) \times (\mathbb{Z}/p)$ d'ordre $p^2/|Z| = p$. Deux tels sous-groupes distincts ne se rencontrent qu'en $(0, 0)$. Or les éléments $\neq (0, 0)$ de $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$, qui sont au nombre de $p^2 - 1$, sont tous d'ordre p; chacun engendre donc un tel sous-groupe. Comme un groupe d'ordre p admet $p - 1$ générateurs, il y a $(p^2 - 1)/(p - 1) = p + 1$ sous-groupes d'ordre p de $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$, donc $p + 1$ sous-groupes d'ordre p^2 de G.
$4^o/$ Pour tout $g \in G$, soit $\sigma_g : x \mapsto gxg^{-1}$ l'automorphise de conjugaison par g du groupe G, et soit $\sigma : G \to Aut(G)$ l'application $g \mapsto \sigma(g) := \sigma_g$. Alors, σ est un morphisme de groupes $(\sigma_{gg'} = \sigma_g \circ \sigma_{g'})$. L'image $\sigma(G) := Int(G)$ de σ est donc un sous-groupe de $Aut(G)$. Comme ce dernier est cyclique, $Int(G)$ est aussi un groupe cyclique. Par ailleurs, $Ker(\sigma) = \{g \in G, \forall x \in G, gx = xg\}$ est le centre Z de G. Ainsi, $G/Z = G/Ker(\sigma) \simeq Im(\sigma) = Int(G)$ est un groupe cyclique, donc G est abélien par $1/$.

II. $1^o/$ (Dans ce qui suit, on note n_p le nb de p-Sylows de G, et ν_ℓ le nb d'élts de G d'ordre ℓ.) Comme $(7, |G|/7) = 1$, les ss-groupes d'ordre 7 de G sont ses 7-Sylows. De $n_7 | 33$ et $n_7 \equiv 1$ mod. 7, on tire $n_7 = 1$, donc G n'a qu'un ss-groupe d'ordre 7. De même, $n_{11} = 1$.
$2^o/$ Comme il n'y a qu'un 7-, resp. 11-Sylow H_7, resp. H_{11}, ils sont distingués dans G. De $H_7 \lhd G$, on déduit que $H := H_7 H_{11}$ est un sous-groupe de G, et comme H_{11} est aussi distingué dans G, $H_7 H_{11}$ est isomorphe au produit direct $H_7 \times H_{11}$, donc à $(\mathbb{Z}/7) \times (\mathbb{Z}/11)$, donc à $\mathbb{Z}/77\mathbb{Z}$ (lemme chinois). Ainsi, H est bien un groupe cyclique, d'ordre 77. Enfin, pour tout $g \in G$, on a $gHg^{-1} = gH_7 g^{-1} gH_{11} g^{-1} = H_7 H_{11}$, et $H \lhd G$.
$3^o/$ Comme x est d'ordre 7×11, x^{11} est d'ordre 7 et engendre l'unique sous-groupe H_7 d'ordre 7 de G, donc $x^{11} \in H_7$. De même, $x^7 \in H_{11}$. Par Bezout, il existe des entiers rationnels a, b tels que $11a + 7b = 1$. Donc $x = (x^{11})^a.(x^7)^b \in H_7 H_{11} = H$. Par conséquent, les éléments d'ordre 77 de G sont les générateurs du groupe cyclique H, d'ordre 7×11; ils s'identifient aux entiers $x \in [0, 76]$ premiers à 77, c-à-d. non multiples de 7 ou de 11. Il y en a $\nu_{77} = 77 - 11 - 7 + 1 = (7 - 1) \times (11 - 1) = 60$.

4^o/ S'il n'y avait qu'un 3-Sylow H_3, il serait distingué dans G, tout comme les autres p-Sylows H_7 et H_{11}, et G serait isomorphe au produit direct $H_3 \times H_7 \times H_{11}$ (cf. §8.4 du poly), donc ici abélien ($H_3 \simeq \mathbb{Z}/3\mathbb{Z}$), en contradiction avec l'hypothèse. Par conséquent, $n_3 \neq 1$. Les relations $n_3|77$ et $n_3 \equiv 1$ mod. 3 imposent alors que $n_3 = 7$. Pour tout 3-Sylow K de G, $H \cap K = \{e\}$ (car $|K| = 3$ est premier à 77), et $|H|.|K| = |G|$, donc $G = HK$. Mais $H \triangleleft G$, et K n'est pas distingué dans G, donc $G = H \rtimes_\tau K$ est un produit semi-direct, non direct, de H par K (τ est l'action de K sur H par conjugaison).
5^o/ i) Le groupe $Aut(H_{11}) \simeq Aut(\mathbb{Z}/11\mathbb{Z})$ est d'ordre 10, donc l'image de tout élément de K est d'ordre $1 = pgcd(3, 10)$, c-à-d. est l'élément neutre $id_{H_{11}}$ de $Aut(H_{11})$, et le morphisme est trivial. - ii) Puisque $H_{11} \triangleleft G$ et $H_{11} \cap K = \{e\}$, on sait déja que $H_{11}K$ est un sous-groupe de G, isomorphe à un produit semi-direct $H_{11} \rtimes_\tau K$. Il s'agit de montrer que le produit est direct, autrement dit que tout élément k de K commute avec tout élément h de H_{11}. Pour tout $k \in K$, soit $\sigma_k : x \mapsto kxk^{-1}$ l'automorphisme de G de conjugaison par k. Comme $H_{11} \triangleleft G$, $\sigma_k(H_{11}) = H_{11}$, et la restriction σ'_k à H_{11} de σ_k est un automorphisme de H_{11}. Mais l'application $\sigma' : k \mapsto \sigma'_k$ de K dans $Aut(H_{11})$ est un morphisme de groupes, donc est triviale par (i). Ainsi, pour tout $k \in K, h \in H_{11}$, on a : $khk^{-1} = \sigma'_k(h) = id_{H_{11}}(h) = h$, et $kh = hk$, comme souhaité.
6^o/ i) Soient $K_1, ..., K_7$ les 3-Sylows de G. Par 5/, chacun des groupes $H_{11}K_i$ est cyclique d'ordre 33. De plus, pour tout $i \neq j$, $H_{11}K_i \cap H_{11}K_j = H_{11}$, car ces groupes étant abéliens, toute relation $hk_i = h'k_j$ entraîne $h^{11}k_i^{11} = h'^{11}k_j^{11}$, d'où $k_i^{-1} = k_j^{-1} = e$. Par le même raisonnement qu'en 3/, on voit que les éléments d'ordre 33 de G s'identifient aux générateurs de ces sous-groupes. Chacun en a $(11-1) \times (3-1) = 20$, et ils sont distincts, puisqu'ils n'appartiennent pas à H_{11}. Finalement, $\nu_{33} = 7 \times 20 = 140$. - ii) En reprenant ce qu'on a dit au début du 5/(ii), on voit que H_7K est un sous-groupe de G isomorphe à un produit semi-direct $H_7 \rtimes_\tau K$, mais cette fois-ci non direct, sans quoi G serait un groupe abélien. Le raisonnement de 3/ montre qu'un élément d'ordre 21 de G appartient à l'un des H_7K_i. Mais aucun de ces produits semi-directs n'a d'élément d'ordre 21. Donc $\nu_{21} = 0$. Autre méthode : $\nu_1 = 1, \nu_3 = 7 \times (3-1) = 14, \nu_7 = 6, \nu_{11} = 10, \nu_{33} = 140, \nu_{77} = 60$ (et $\nu_{231} = 0$), donc $\nu_{21} = |G| - 1 - 14 - 6 - 10 - 140 - 60 = 0$.
III. 1^o/ $Ker(\phi) \triangleleft G$, donc est égal à G ($\Leftrightarrow \phi(G) = \{e\}$) ou à $\{e\}$ ($\Leftrightarrow \phi$ est injectif).
2^o/ i) Comme G est simple, il ne peut avoir un seul 5-Sylow, et les relations $n_5|24, n_5 \equiv 1$ mod. 5 entraînent que l'ensemble X des 5-Sylows de G a $n_5 = 6$ éléments. - ii) Le groupe G agit par conjugaison sur X, d'où un morphisme f de G dans le groupe $\mathcal{S}_X \simeq \mathcal{S}_6$ des permutations de X. Comme G agit transitivement sur X, f ne peut être trivial.
3^o/ i) Comme f n'est pas trivial, il est injectif et $G' \simeq G$ est encore un groupe simple d'ordre $5\,!$. La restriction ϵ' de ϵ à G' est un morphisme de G' vers un groupe à 2 éléments. Comme $5\,! > 2$, il ne peut être injectif, donc il est trivial et $G' = Ker(\epsilon') < Ker(\epsilon) = \mathcal{A}_6$. - ii) L'action de G' sur l'ensemble $\mathcal{A}_6/G'$, qui a $6!/2.5! = 3$ éléments, est donnée par $(g', aG') \mapsto g'aG'$ et fournit un morphisme ϕ de G' dans $\mathcal{S}_3$. Comme $5! > 3!$, ce morphisme est trivial. Ainsi, pour tout $g' \in G', a \in \mathcal{A}_6$, on a $g'aG' = aG'$, d'où $a^{-1}g'a \in G'$ et $G' \triangleleft \mathcal{A}_6$.
4^o/ Le groupe $\mathcal{A}_6$ est simple (cf. §8.5 du poly). Il ne peut donc admettre de sous-groupe distingué G' d'ordre $5! < 6!/2$ (et > 1), et l'hypothèse de l'énoncé n'est jamais satisfaite.