UPMC Master M1 de mathématiques 12-13

D. Bertrand *MM014 - Groupes finis*

Examen du 25 Avril 2013

Durée: 2 heures

L'usage du polycopié du cours et des feuilles d'exercices est autorisé.
Les 2 énoncés sont indépendants.

I

Soit G un groupe fini $\neq \{1\}$. 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. On note

$$\Phi_G = \bigcap_{H<G\ ,\ H \text{maximal}} H$$

(ou simplement Φ si le contexte est clair) l'intersection des sous-groupes maximaux de G.

1°/ i) Montrer que tout sous-groupe N de G distinct de G est contenu dans un sous-groupe maximal (éventuellement égal à N). G admet donc au moins un sous-groupe maximal.

ii) Montrer que Φ_G est un sous-groupe normal de G.

iii) On suppose que $H = \{1\}$ est un sous-groupe maximal de G. Montrer que G est cyclique d'ordre premier.

2°/ Pour chacun des groupes G suivants :

$$(a)\ G = \mathbf{Z}/6\mathbf{Z}\ ;\ (b)\ G = \mathbf{Z}/9\mathbf{Z}\ ;\ (c)\ G = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}\ ,$$

donner la liste des sous-groupes maximaux de G et déterminer le sous-groupe Φ_G correspondant.

3°/ On suppose ici que G est un p-groupe, dont on note $n = p^r$ l'ordre.

i) Rappeler brièvement pourquoi le centre $Z(G)$ de G est non trivial. En particulier, il contient un sous-groupe Z' d'ordre p.

ii) Soit $H < G$ un sous-groupe maximal ne contenant pas Z'. Montrer que $G \simeq Z' \times H$.

iii) Montrer par récurrence sur r que les sous-groupes maximaux de G sont distingués dans G, et qu'ils sont d'ordre p^{r-1}.

iv) Galculer Φ_G pour le groupe diédral (d'ordre 8) $G = D_4$.

4°/ On revient au cas d'un groupe G général, et on se propose de montrer que $\Phi = \Phi_G$ est un groupe nilpotent. On fixe un nombre premier p quelconque.

i) Soit N un sous-groupe de G tel que $\Phi.N = G$. Montrer que $N = G$.

ii) Soient F un sous-groupe normal de G, S un p-Sylow de F et $N = N_G(S)$ le normalisateur de S dans G. Montrer que pour tout $g \in G$, gSg^{-1} est un p-Sylow de F. En déduire que $g \in F.N$, donc que $G = F.N$.

iii) Soit S un p-Sylow de Φ. Montrer que $N_G(S) = G$, et conclure.

II

Soient G un groupe fini, de centre $Z(G) = Z$ et (V, ρ) une représentation complexe irréductible de G, de degré $dim(V) = n$, de caractère χ. Un théorème de Burnside affirme que n *divise* $|G|$. En admettant ce théorème, on se propose de le raffiner (Question 5^o/) sous la forme : n *divise* $[G : Z]$.

1^o/ Soient H un sous-groupe commutatif de G, $\rho_H : H \to Aut_{\mathbf{C}}(V)$ la restriction de ρ à H, et $W \subset V$ une sous-représentation irréductible de ρ_H.

i) Montrer que $dim(W) = 1$

ii) Montrer que l'orbite $\{\rho(g)(W), g \in G\}$ de W sous G est constituée d'au plus $[G : H]$ droites de V distinctes. En déduire que $n \leq [G : H]$.

2^0/ On suppose maintenant que H est un sous-groupe du centre Z de G.

i) Montrer que pour tout $h \in H$, $\rho(h)$ est une homothétie de V, et que $|\chi(h)| = n$.

ii) En déduire que $n^2 \leq [G : H]$. (On pourra considérer $(\chi|\chi)$.)

3^0/ On suppose ici que G est un groupe d'ordre p^4, où p est un nombre premier.

i) En admettant le théorème de Burnside, montrer que les représentations irréductibles de G sont de degré $n = 1$ ou $n = p$.

ii) Montrer qu'il existe au moins p^2 homomorphismes distincts de G dans $\mathbf{C}^*$.

4^0/ On fixe désormais un entier $m \geq 1$ (on pourra prendre $m = 2$ pour la rédaction). On considère le groupe fini $G^m = G \times ... \times G$, produit de m copies de G, et l'espace vectoriel $V^{\otimes m}$, produit tensoriel de m copies de V. On admettra (ou on justifiera brièvement) l'existence d'une représentation ρ_m du groupe G^m sur l'espace $V^{\otimes m}$ vérifiant, pour tout $(g_1, ..., g_m) \in G^m$ et tout $(v_1, ..., v_m) \in V^m$:

$$\rho_m(g_1, ..., g_m)(v_1 \otimes ... \otimes v_m) = \rho(g_1)(v_1) \otimes ... \otimes \rho(g_m)(v_m).$$

Montrer que le caractère χ_m de la représentation ρ_m vérifie $\chi_m(g_1, ..., g_m) = \chi(g_1)...\chi(g_m)$. Calculer $(\chi_m|\chi_m)$, et en déduire que ρ_m est une représentation irréductible de G^m.

5^0/ i) Montrer que pour tout élement $(z_1, ..., z_m)$ de $Z \times ... \times Z = Z^m \subset G^m$, $\rho_m(z_1, ..., z_m)$ est une homothétie de $V^{\otimes m}$, dont on notera $\lambda_m(z_1, ..., z_m)$ le rapport.

ii) Calculer $\lambda_m(z_1, ..., z_m)$ en fonction de $\lambda_1(z_1 ... z_m)$. En déduire que ρ_m définit une représentation irréductible du groupe G^m/H, où $H = \{(z_1, ..., z_m) \in Z^m, z_1 ... z_m = 1\}$.

iii) En admettant le théorème de Burnside, montrer que pour tout entier $m \geq 1$, n^m divise $|G|^m/|Z|^{m-1}$. En déduire que n divise $[G : Z]$.

Corrigé

I. 1^o/ i) Si N n'est pas maximal, il existe par définition un ss-gr. N_1 strictement inclus dans G et contenant strictement N. On itère, et comme G est fini, le processus fournit au bout d'un nombre fini d'étapes un sous-groupe $N_k \supset N$ maximal. ii) L'image d'un ss-gr. maximal de G par un automorphisme de G est encore un ss-gr. maximal. Donc Φ_G est même un sous-groupe caractéristique de G. iii) Pour tout $x \neq 1 \in G$, $< x >$ contient strictement le sous-groupe maximal $\{1\}$, donc $< x >= G$, et G est cyclique, $\simeq \mathbb{Z}/N\mathbb{Z}$. Si $N = dd'$ n'était pas premier, G contiendrait le sous-groupe propre $d\mathbb{Z}/N\mathbb{Z}$, et $\{1\}$ ne serait pas maximal.

2^o/ Les sous-groupes de $\mathbb{Z}/N\mathbb{Z}$ sont en bijection avec les diviseurs d de N, et $d\mathbb{Z}/N\mathbb{Z}$ est maximal si et slt si d n'admet pas de diviseur strict, i.e. est premier. Les ss-gr. maximaux de $G_a = \mathbb{Z}/6\mathbb{Z}$ sont donc $2\mathbb{Z}/6\mathbb{Z}$ et $3\mathbb{Z}/6\mathbb{Z}$, dont l'intersection Φ_{G_a} est réduite à $\{0\}$. De même, le seul sous-groupe maximal de $G_b = \mathbb{Z}/9\mathbb{Z}$ est $3\mathbb{Z}/9\mathbb{Z}$, qui vaut donc Φ_{G_b}. Tout sous-groupe propre non nul de $G_c = \mathbb{F}_3 \oplus \mathbb{F}_3$ est une droite D de cet espace vectoriel, et il est automatiquement maximal car $D+ < x >= G_c$ pour tout $x \notin D$. Donc $\Phi_{G_c} = \{0\}$.

3^o/ i) Voir poly, preuve de la Prop. 3.2.10.(i). Tout $x \neq 1$ de $Z(G)$ est alors d'ordre p^k, avec $k > 0$, et $Z' :=< x^{p^{k-1}} >$ est un ss-gr. d'ordre p de $Z(G)$. ii) Comme $Z' \triangleleft G$, $Z'.H$ est un ss-gr. de G, qui contient strictement H puisque que $Z' \not\subset H$, donc vaut G par maximalité de H. De plus, $Z' \cap H$ est un ss-gr. strict du groupe $Z' \simeq \mathbb{Z}/p\mathbb{Z}$, donc vaut $\{1\}$. Par conséquent, $G = Z'.H \simeq Z' \rtimes H = Z' \times H$ (car Z' et H commutent). iii) Clair pour $r = 1$, admis au cran r. Soient G d'ordre p^{r+1}, $Z' < Z(G)$ comme supra, et $H < G$ maximal. Si H ne contient pas Z', alors $G = Z' \times H$ d'après (ii), et H est normal dans G, d'ordre $|G|/|Z'| = p^r$. Sinon, H/Z' est un sous-groupe de G/Z', et y est encore maximal, donc normal et d'ordre p^{r-1} par l'hypothèse de récurrence. Mais alors, H est normal dans G, et d'ordre $p^{r-1}|Z'| = p^r$. iv) Un ss-gr. normal d'indice premier est toujours maximal. Il suffit donc de lister les ss-gr. H d'ordre 4 de D_4. Hors de $< r >\subset SO_2(\mathbb{R})$, tout sous-groupe d'ordre 4 de D_4 est engendré par deux symétries de la forme $s, s' = sr^2$, donc $\Phi_{D_4} = \{1, r^2\}$

4^o/ i) Dans le cas contraire, il existerait d'après 1/(i) un ss-gr. maximal H contenant N. Alors, $G = \Phi.N \subset H.N = H$ et $H = G$, contradiction. ii) Si $|F| = p^r m$, gSg^{-1} est un ss-gr. de $F \triangleleft G$, d'ordre p^r, donc un p-Sylow de F. Il est donc conjugué à S *dans* F, i.e. $\exists f \in F, fSf^{-1} = gSg^{-1}$, et $f^{-1}g \in N_G(S)$, donc $g \in F.N$. iii) De (ii), appliqué au ss-gr. normal $F = \Phi$ de G, on déduit que $\Phi.N_G(S) = G$, et (i) entraîne alors que $N_G(S) = G$. Donc S est normal dans Φ. Pour tout nombre premier p, Φ n'a par conséquent qu'un seul p-Sylow, et on déduit du Thm. 3.2.11 du poly que Φ est nilpotent.

II. 1^o/ (cf. TD 5, Sol. 3) i) Toute repr. irréd. d'un groupe abélien est de degré 1 (poly, 4.1.7.(i) si $K = \mathbb{C}$, mais cela vaut en fait sur tout corps K alg. clos : pour tout $h, k \in H$, $khk^{-1} = h$, donc $\rho_H(h)$ est un H-morphisme de W, donc par Schur une homothétie, et toute droite de W est alors stable sous H.) ii) Pour tout g, $g.W$ ne dépend que de la classe gH de g dans G/H. L'espace vectoriel que les droites $g.W, g \in G$, engendrent dans V est donc de dimension $\leq [G : H]$. Mais il est stable sous G, donc égal à V.

2^o/ i) Même idée que supra : pour tout $h \in H \subset Z, g \in G$, $ghg^{-1} = h$, donc $\rho(h)$ est un G-morphisme de V, donc par Schur une homothétie, dont le rapport $\lambda_1(h)$ est une racine de l'unité. Donc $Tr(\rho(h)) = n\lambda_1(h)$, et $|\chi(h)| = n$. ii) $|G|.(\chi|\chi) = \Sigma_{g\in G}|\chi(g)|^2 = \Sigma_{h\in H}|\chi(h)|^2$+(des termes ≥ 0) $\geq |H|n^2$. Comme $(\chi|\chi) = 1$, $|G| \geq |H|n^2$.

3^o/ i) D'après Burnside, une telle représentation V est de degré $n = p^a$, avec $0 \leq a \leq 4$. Par ailleurs, le centre Z d'un p-groupe est non trivial (cours, cf. I.3), donc $[G : Z] = p^b$, avec $0 \leq b \leq 3$. D'après 2/ii, $n^2 \leq [G : Z]$, donc $2a \leq b$, et $a = 0$ ou 1. ii) Avec les notations du Cor. 4.2.8.(iii) du poly, $\Sigma_W\ dim(W)^2 = p^4$, et les nombres N_1, resp. N_p, de classes d'iso. de représentations irréductibles de degré 1, resp. p, vérifient : $N_1 + N_p p^2 = p^4$. Donc p^2 divise N_1, et puisque $N_1 \neq 0$ (repr. triviale), on a bien $p^2 \leq N_1$. Pour conclure, noter que deux repr. de degré 1 sont isomorphes si et slt les morphismes de G dans $\mathbb{C}^*$ qui leur correspondent sont égaux.

4^o/ (cf. TD 6, Sol. 7, qui couvre le cas $m = 2$. - L'existence de ρ_m provient du caractère m-linéaire de l'application $(v_1, ..., v_m) \mapsto \rho(g_1)(v_1)\otimes...\otimes\rho(g_m)(v_m)$.) Soient $\lambda_j(g_i), j = 1, ...n$, les valeurs propres avec multiplicités des $\rho(g_i), i = 1, ..., m$. En diagonalisant chacun des automorphismes $\rho(g_i)$ de V (dans des bases de V dépendant de chaque g_i), on voit que $\rho_m(g_1, ..., g_m)$ est une matrice diagonale, dont les n^m coeff. diagonaux sont les produits $\Pi_{i=1,...,m}\lambda_{j(i)}(g_i)$, où $\{i \mapsto j(i)\}$ parcourt l'ensemble J des applications de $[1, ..., m]$ dans $[1, ..., n]$. Donc $\chi_m(g_1, ..., g_m) = \Sigma_J\ \Pi_{i=1,...,m}\lambda_{j(i)}(g_i) = \chi(g_1)...\chi(g_m)$. Par conséquent, $(\chi_m|\chi_m) = |G|^{-m}\ \Pi_{i=1,...,m}\ (\Sigma_{g_i\in G}|\chi(g_i)|^2) = 1^m = 1$, et ρ_m est bien une repr. irréd. du groupe G^m.

5^o/ i) Le centre de G^m est Z^m. Le résultat découle donc de 2/(i), appliqué au groupe G^m. ii) Pour $z_i \in Z$, $\rho(z_i) = \lambda_1(z_i)id_V$, où $\lambda_1 : Z \to \mathbb{C}^*$ est un caractère du groupe Z, donc $\rho_m(z_1, ..., z_m) = \otimes_{i=1,...,m}\lambda_1(z_i)id_V = (\Pi_{i=1,...,m}\lambda_1(z_i))id_{V^{\otimes m}}$ et $\lambda_m(z_1, ..., z_m) = \lambda_1(z_1...z_m)$. Comme $\lambda_1(1) = 1$, le sous-groupe H de Z^m est contenu dans le noyau du morphisme $\rho_m : G^m \to Aut(V^{\otimes m})$, et ρ_m définit par passage au quotient une représentation $\overline{\rho}_m$ de G^m/H sur $V^{\otimes m}$. Un ss-espace W de $V^{\otimes m}$ stable sous G^m/H l'est aussi sous G^m, donc $\overline{\rho}_m$ est une représentation irréductible de G^m/H. iii) D'après Burnside, le degré n^m de la repr. irréd. $\overline{\rho}_m$ divise l'ordre du groupe G^m/H. Comme H est le noyau de la surjection $Z^m \to Z : (z_1, ..., z_m) \mapsto z_1...z_m$, on a $|H| = |Z|^{m-1}$, donc $|G^m/H| = |G|^m/|Z|^{m-1}$. Ainsi, pour tout m, le dénominateur du nombre rationnel $(|G|/n|Z|)^m$ divise $|Z|$. Donc $|G|/n|Z|$ est un entier, et n divise $|G|/|Z|$.