Corrigé du partiel d'algèbre

Exercice 1 : Exposant d'un groupe (7 points)

a) Soit $n = \exp G$. Comme $x^n = 1$, on a par définition de l'ordre que $\omega(x)$ divise n (0.5 point).

b) Supposons le contraire. Alors, pour tout x de G l'ordre de x divise $p^{\alpha-1}m$ (puisqu'il divise $\exp G$ et n'est pas divisible par p^α), ce qui implique que $x^{p^{\alpha-1}m} = 1$. Ainsi on aurait $\exp G \leq p^{\alpha-1}m$, contradiction (1.5 point).

c) Écrivons $\exp G = p_1^{\alpha_1}...p_r^{\alpha_r}$ avec les p_i premiers deux à deux distincts et $\alpha_i \in \mathbf{N}^*$. D'après b), il existe pour tout i un élément x_i d'ordre multiple de $p_i^{\alpha_i}$, ce qui implique que le ppcm des ordres des éléments de G est divisible par $p_1^{\alpha_1}...p_r^{\alpha_r} = \exp G$ vu que les $p_i^{\alpha_i}$ sont deux à deux premiers entre eux. Comme par ailleurs ce ppcm divise $\exp G$ d'après a), il lui est égal (1.5 point).

d) Comme vu en cours, l'ordre possible d'un élément de $\mathcal{A}_5$ est 1, 2, 3, ou 5. D'après b), l'exposant de $\mathcal{A}_5$ est le ppcm de 1, 2, 3, et 5, à savoir 30 (1 point).

e) On procède par récurrence sur r. Pour $r = 1$ c'est immédiat, et le cas $r = 2$ a été vu en cours. Si maintenant on suppose le résultat vrai pour $r-1$, alors l'ordre de $(x_1...x_{r-1})$ est $\prod_{i=1}^{r-1}\omega(x_i)$, qui est premier à $\omega(x_r)$ vu que $\omega(x_r)$ est premier avec chacun des $\omega(x_i)$ pour $1 \leq i \leq r-1$. Le cas $r = 2$ donne alors que l'ordre de $(x_1...x_{r-1})x_r$ est $\prod_{i=1}^{r}\omega(x_i)$ (1 point).

f) Avec les notations de c), on a vu que G possédait pour tout i un élément d'ordre m_i multiple de $p_i^{\alpha_i}$, donc (quitte à le mettre à la puissance $p_i^{\alpha_i}/m_i$) un élément x_i d'ordre exactement $p_i^{\alpha_i}$. Alors d'après e) l'élément $\prod_{i=1}^{r} x_i$ est d'ordre $\exp G$.

Pour un groupe non abélien, le résultat est faux, prendre par exemple le groupe $\mathcal{A}_5$ comme dans la question d) (1.5 point).

Exercice 2 : 2-Sylow d'un groupe fini (3 points)

a) D'après le deuxième théorème de Sylow, ce nombre est congru à 1 modulo 2, c'est-à-dire impair (0.5 point).

b) Comme G opère par automorphismes, on a que $g.S$ est un groupe, et son cardinal est celui de S ; ainsi $g.S$ est un 2-Sylow et G opère sur l'ensemble X des 2-Sylow. Comme X est de cardinal impair d'après a), au moins une orbite doit être de cardinal impair. Mais les orbites non réduites à un élement sont de cardinal divisant celui de G, donc pair puisque G est un 2-groupe. ainsi, il y a au moins une orbite réduite à un élement, ce qui signifie qu'il existe un 2-Sylow S de A tel que $g.S = S$ pour tout g de G (1.5 point).

c) Soit T un 2-Sylow de A. Par définition du normalisateur, on a $T \lhd N$. Ainsi N/T est un groupe, qui est d'ordre impair puisque T est a fortiori un 2-Sylow de N. Le théorème de Feit-Thompson dit que N/T est résoluble et T est résoluble (il est même nilpotent car c'est un 2-groupe), ce qui implique T résoluble comme extension de N/T par T (1 point).

Exercice 3 : Éléments premiers d'un anneau intègre (11 points)

a) Si $p = ab$ avec a et b dans A non inversibles, alors p divise ab, donc comme (p) est premier cela implique que p divise a ou b par exemple a. Comme a divise p, on obtient que a et p sont associés et b est inversible. Ainsi, p est irréductible (1 point).

b) Si A est factoriel, on sait que tout x est inversible ou s'écrit $x = up_1p_2...p_r$ avec $u \in A^*$ et les p_i irréductibles, donc premiers puisque l'anneau est factoriel. Ainsi $T = A - \{0\}$. En sens inverse, supposons $T = A - \{0\}$. Alors tout élement non nul de A admet une décomposition en irréductibles via a). Par ailleurs, si p est irréductible, alors comme $p \in T$ on peut écrire $p = up_1...p_r$ avec les p_i premiers et $u \in A^*$. Le fait que p soit irréductible impose alors que l'un des p_i soit associé à p, et $(p) = (p_i)$ est alors un idéal premier. On a donc bien vérifié un des critères pour que A soit factoriel (1.5 point).

c) On procède par récurrence sur m. Pour $m = 0$, il suffit de prendre $r = s = 0$. Supposons $m \leq 1$ et le résultat vrai pour $m-1$. Alors p divise ab, donc comme p est premier il divise a ou b, par exemple a. Posons $a = pa'$, alord p^{m-1} divise $a'b$ et par hypothèse de récurrence on trouve n', s dans $\mathbf{N}$ avec $n'+s = m-1$, $p^{n'}$ divise a' et p^s divise b. Il suffit alors de poser $n = n'+1$ (1.5 point).

d) Écrivons

$$ab = up_1^{\alpha_1}...p_r^{\alpha_r},$$

avec les p_i premiers deux à deux non associés. On raisonne par récurrence sur $r \in \mathbf{N}$. Le cas $r = 0$ correspond à ab inversible, auquel cas a et b sont inversibles donc dans T. Supposons le résultat vrai pour $r-1$. D'après c), on

peut trouver n et s tels que $n+s=\alpha_r$ et a, b soient respectivement divisibles par p_r^n et p_r^s. Posons alors $a'=a/p_r^n$ et $b'=b/p_r^s$. Comme

$$a'b' = up_1^{\alpha_1}...p_{r-1}^{\alpha_{r-1}},$$

l'hypothèse de récurrence donne que a' et b' sont dans T, donc aussi a et b vu que p_r est premier (2 points).

e) Il est immédiat que B contient $0=0/1$ et $1=1/1$, et que si $z \in B$, alors $-z \in B$. Si maintenant $z=x/y$ et $z'=x'/y'$ sont dans B, alors $zz'=(xx')/(yy')$ et $z+z'=(xy'+x'y)/yy'$ sont encore dans B, vu que A est un sous-anneau de K et le produit de deux éléments de T reste dans T par définition de T.

Si maintenant I est un idéal premier de B, alors $\wp$ est un idéal de A (comme image réciproque de I par l'inclusion $i : A \to B$), qui reste premier vu que $1 \notin \wp$ (sinon on aurait $1 \in I$ et $I = B$ ne serait pas premier) et si $xy \in \wp$ avec $x, y \in A$, alors par exemple $x \in I$ vu que I est un idéal premier de B, donc $x \in \wp = A \cap I$. Enfin, si on avait un élément t dans $\wp \cap T$, on aurait $1 = (1/t).t$ dans I, donc $I = B$ ne serait pas un idéal premier (1.5 point).

f) On a $aB \neq B$, sinon on pourrait écrire $1 = ax/t$ avec $x \in A$ et $t \in T$, soit $ax = t$, ce qui impliquerait $x \in T$ d'après d). D'après le théorème de Krull, l'idéal aB de B est contenu dans un idéal maximal (donc premier) I de B. D'après e), l'idéal $\wp = I \cap A$ de A est premier et ne rencontre pas T, et de plus il contient a puisque I et A contiennent a (2 points).

g) Si A est factoriel, alors un idéal premier non nul $\wp$ de A contient un élément non nul et non inversible x. On écrit alors $x = up_1...p_r$ avec $u \in A^*$, $r \geq 1$, et les p_i irréductibles. Comme $\prod_{i=1}^r p_i \in \wp$, l'un des p_i est dans $\wp$ et c'est bien un élément premier puisqu'il est irréductible et A est factoriel.

En sens inverse, si tout idéal premier non nul de A contient un élement premier, alors $T = A - \{0\}$ d'après f), ce qui implique A factoriel d'après b) (1.5 point).