Corrigé du partiel d'algèbre de M1 du 22/9/22

Exercice 1 : Groupes symétriques (5 points)

a) On sait que $|X|$ est congru à 1 modulo 5, et divise $2^3.3 = 24$. Les seules possibilités sont 1 et 6, mais 1 est exclu sinon le 5-Sylow (qui est de cardinal 5, donc ne contient pas $\mathcal{A}_5$) serait distingué, ce qui n'est pas le cas d'après l'énoncé rappelé au début de l'exercice (1 point).

b) On sait que l'opération de $\mathcal{S}_5$ sur X par conjugaison est transitive. Elle est de plus fidèle, car le noyau du morphisme $\Phi : \mathcal{S}_5 \to \mathcal{S}(X)$ (correspondant à cette opération) est un sous-groupe distingué de $\mathcal{S}_5$ ne contenant pas $\mathcal{A}_5$ (sinon les stabilisateurs contiendraient $\mathcal{A}_5$ et le cardinal de l'unique orbite, qui est 6, serait plus petit que $|\mathcal{S}_5|/|\mathcal{A}_5| = 2$), ainsi $\ker \Phi$ est trivial (1.5 point).

c) Il suffit d'appliquer b) et de prendre l'image H de Φ. Comme Φ est injective, le groupe H est bien de cardinal $|\mathcal{S}_5| = 5!$, donc d'indice 6 dans $\mathcal{S}(X) \simeq \mathcal{S}_6$ (qui est de cardinal 6!). De plus on a vu que H opère transitivement sur l'ensemble X, qui est de cardinal 6 (1 point).

d) Non : en effet, comme H' est le stabilisateur de 1 pour l'opération naturelle de $\mathcal{S}_6$ sur $\{1, ..., 6\}$, on voit que $gH'g^{-1}$ est le stabilisateur de $g(1)$ pour cette même opération. Or, H n'est pas le stabilisateur d'un point puisqu'il agit transitivement sur $\{1, ..., 6\}$ d'après c) (1.5 point).

Exercice 2 : Automorphismes de groupes abéliens (4 points)

a) On observe que A est un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel, et qu'un automorphisme du groupe abélien A est automatiquement aussi un automorphisme f de $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel, via la formule $f(mx) = mf(x)$, qui vaut pour tout entier m et tout $x \in A$. Ainsi $\mathtt{Aut}(A)$ est le groupe des automorphismes d'un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel de dimension n, il est donc isomorphe à $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ (1.5 point).

b) Si $n = 1$, le a) donne que $\mathtt{Aut}(A) \simeq (\mathbf{Z}/p\mathbf{Z})^*$ est abélien. Si $n \geq 2$, ce n'est plus le cas, car par exemple les deux matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

ne commutent pas (1.5 point).

c) Comme A est abélien, tout sous-groupe est distingué. Par contre, le sous-groupe composé des éléments de la forme $(x, 0, ..., 0)$ avec $x \in \mathbf{Z}/p\mathbf{Z}$ n'est pas stable par l'automorphisme qui échange les deux premières coordonnées (1 point).

Exercice 3 : Idéaux premiers (7 points)

a) Supposons par l'absurde que $\wp$ ne contienne aucun des I_j, et choisissons pour chaque j un $x_j \in I_j$ qui n'est pas dans $\wp$. Alors $x_1 ... x_r$ est dans $I_1 ... I_r$ mais pas dans $\wp$ (puisque $\wp$ est premier), ce qui contredit l'hypothèse $\wp \supset I_1 ... I_r$ (1 point).

b) Comme I n'est pas premier et est différent de A, on peut trouver $x, y \in A$ avec $xy \in I$, mais ni x ni y dans I. Soit alors I_1 l'idéal engendré par I et x, puis I_2 l'idéal engendré par I et y, ils contiennent strictement I. Par ailleurs un élément de $I_1 I_2$ est une somme d'éléments de la forme $(i_1 + ax)(i_2 + by)$, avec $i_1 \in I$, $i_2 \in I$, et a, b dans A. Un tel élément est de la forme $(i_1 i_2 + b i_1 y + a i_2 x + abxy)$, il est donc dans I puisque i_1, i_2, et xy sont dans I. Finalement $I_1 I_2 \subset I$ (1.5 point).

c) Si le résultat était faux, on pourrait choisir (vu que A est noethérien) un un idéal I maximal parmi ceux qui ne vérifient pas la propriété voulue. En particulier I n'est pas premier (sinon on prend $m = 1$, $\wp_1 = I$) et on a aussi $I \neq A$ (sinon on prend $m = 1$ et pour $\wp_1$ n'importe quel idéal maximal de A). Appliquons alors b). Les idéaux I_1 et I_2 obtenus vérifient (par maximalité de I) qu'il existe des idéaux premiers $J_1, ..., J_r$ et $J'_1, ..., J'_s$ avec :

$$I_1 \supset J_1 ... J_r; \;\; I_2 \supset J'_1 ... J'_s.$$

Alors, comme $I \supset I_1 I_2$, on a $I \supset J_1 ... J_r J'_1 ... J'_s$, ce qui contredit le fait que I ne vérifie pas la propriété voulue (2 points).

d) On applique c) à $I = 0$, ainsi $\wp_1 ... \wp_m$ est l'idéal nul. en particulier tout idéal premier de A contient $\wp_1 ... \wp_m$, donc contient l'un des $\wp_j$ d'après a) (1 point).

e) D'après d), tout idéal premier minimal contient l'un des $\wp_i$, donc lui est égal par minimalité (0.5 point).

f) Si A est intègre, l'idéal $\{0\}$ est premier et c'est clairement le seul idéal premier minimal. Si $A = \mathbf{Z}/8\mathbf{Z}$, les idéaux de A sont les $I_m := m\mathbf{Z}/8\mathbf{Z}$ avec m divisant 8. Le quotient de A par I_m est $\mathbf{Z}/m\mathbf{Z}$, donc le seul idéal premier est obtenu pour $m = 2$, et c'est a fortiori le seul idéal premier minimal (1 point).

Exercice 4 : Anneaux de polynômes (4 points)

a) Les inversibles de B sont inversibles dans A, donc ce sont des polynômes constants non nuls. Réciproquement, ceux-ci sont bien inversibles dans B, vu que B contient toutes les constantes (0.5 point).

b) On sait que A est principal, donc factoriel. La décomposition de T^2 en facteurs irréductibles dans A est $T^2 = T.T$, ainsi les diviseurs de T^2 dans A sont (à constante non nulle près) 1, T, et T^2 (1 point).

c) Les diviseurs de T^2 dans B sont aussi diviseurs de T^2 dans A, donc ce sont (à constante non nulle près) 1 et T^2, vu que T n'est pas dans B : en effet les éléments de B sont sommes de monômes de la forme $a(T^2)^m(T^3)^n$ avec $m, n \in \mathbf{N}$ et $a \in K$. Ainsi T^2 est irréductible dans B (1 point).

d) L'idéal engendré par T^2 dans B n'est pas premier car T^2 divise $T^6 = (T^3)^2$ dans B (en effet $T^6 = (T^2)^3$) mais T^2 ne divise pas T^3 dans B, vu que (T^3/T^2) (qui est dans l'anneau intègre A) n'est pas dans B. Ceci contredit une des propriétés des anneaux factoriels, puisque d'après c) on a que T^2 est irréductible dans B (1.5 point).