Corrigé de l'examen d'algèbre de M1

Exercice 1 (4 points)

a) (**1 pt**). Soit H un sous-groupe distingué de $\mathcal{S}_n$, on a vu en cours que H est l'un des sous-groupes $\{\mathrm{Id}\}$, $\mathcal{S}_n$ ou $\mathcal{A}_n$. Le seul cas non trivial est $H = \mathcal{A}_n$, qui est caractéristique par exemple parce qu'on sait que c'est le sous-groupe dérivé de $\mathcal{S}_n$ (on peut aussi utiliser le fait que c'est le seul sous-groupe d'indice 2 de $\mathcal{S}_n$).

b) (**1.5 point**). Tout automorphisme du $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel G est un automorphisme du groupe abélien G (et réciproquement d'ailleurs). Il suffit donc de trouver un sous-groupe H de G qui n'est pas stable par tous les éléments de $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$. Soit $(e_1, ..., e_n)$ la base canonique de G, alors l'élément de $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ qui envoie e_1 sur e_2, e_2 sur e_1, et e_i sur e_i pour $i \geq 3$, ne laisse pas stable le sous-groupe H engendré par e_1.

c) (**1.5 point**). Non : si H est distingué dans G, il est l'unique p-Sylow de G car on sait que deux p-Sylow quelconques de G sont conjugués. Comme tout automorphisme de G envoie H sur un p-Sylow (par cardinalité), il laisse forcément stable H.

Exercice 2 (4 points)

a) (**1 point**). Si A est intègre, alors $\{0\}$ est un idéal premier de A. Si A est de plus de dimension 0, alors cet idéal est maximal ce qui signifie que $A = A/\{0\}$ est un corps. Réciproquement, si A est un corps, son seul idéal différent de A (et donc son seul idéal premier) est $\{0\}$, qui est bien dans ce cas maximal.

b) (**1.5 point**). On peut prendre $A = \mathbf{Z}/4\mathbf{Z}$. Ce n'est pas un anneau intègre, et comme on sait que les idéaux de A sont les $m\mathbf{Z}/4\mathbf{Z}$ avec m entier divisant 4, le seul idéal premier de A est $I = 2\mathbf{Z}/4\mathbf{Z}$, qui est clairement maximal vu que les seuls autres idéaux de A sont $\{0\}$ et A. Un autre exemple consiste à prendre un produit $k_1 \times k_2$ de deux corps, dont les seuls idéaux premiers sont l'ensemble I_2 des $(0, x_2)$ avec $x_2 \in k_2$ et l'ensemble I_1 des $(x_1, 0)$ avec $x_1 \in k_1$ (en effet un tel idéal est non nul car $k_1 \times k_2$ n'est pas intègre, et il ne peut pas contenir d'élément inversible, donc il est inclus dans I_1 ou I_2,

et on voit alors qu'il est égal à I_1 ou I_2 dès qu'il n'est pas nul, vu que tout élément non nul de k_1 ou k_2 est inversible).

c) (**1.5 point**). Soit $\wp$ un idéal premier de A/I, on sait qu'il est de la forme $\wp = J/I$, où J est un idéal de A contenant I. Comme $(A/I)/\wp$ est isomorphe à A/J, on doit avoir A/J intègre, donc J premier dans A, donc J maximal dans A puisque A est de dimension zéro. Ainsi A/J est un corps et il en va de même de $(A/I)/\wp$, ce qui signifie que $\wp$ est maximal dans A/I.

Exercice 3 (7 points)

a) (**1 point**). Posons $P = \ker u$ et montrons que $M = A.x \oplus P$. On a déjà $P \cap N = \{0\}$, car si $y = \lambda x$ est dans P avec $\lambda \in A$, alors $0 = u(y) = \lambda u(x) = \lambda$ donc $y = 0$. Si maintenant $z \in M$, alors $z = (z - u(z)x) + u(z)x$ avec $u(z)x \in A.x$ et $(z - u(z)x) \in P$ puisque $u(z - u(z)x) = u(z) - u(z)u(x) = u(z) - u(z) = 0$.

b) (**1 point**). Comme N est libre et non nul, on peut en prendre une base $(x_1, ..., x_r)$ avec $r \geq 1$, d'où une application A-linéaire $v : N \to A$ définie par $v(x_1) = 1$ et $v(x_i) = 0$ si $i > 1$. Soit P tel que $M = N \oplus P$, alors l'application A-linéaire u définie par $u_{|N} = v$ et $u_{|P} = 0$ convient.

c) (**1.5 point**). Supposons $\text{pgcd}(a_1, ..., a_n) = 1$, alors d'après Bezout il existe des éléments $\alpha_1, ..., \alpha_n$ de A tels que $\sum_{i=1}^n \alpha_i a_i = 1$. La forme linéaire $u : A^n \to A$ qui envoie tout $(x_1, ..., x_n)$ sur $\sum_{i=1}^n \alpha_i x_i$ vérifie alors $u(a) = 1$, donc N est un facteur direct de A^n d'après a). Réciproquement, si $N = A.a$ est un facteur direct de A^n, alors d'après b) il existe une application A-linéaire $u : A^n \to A$ qui prend la valeur 1 sur a (car (a) est une base de $A.a$ vu que $a \neq 0$ et A est intègre), ce qui fournit une identité de Bezout pour la famille $(a_1, ..., a_n)$.

d) (**1 point**). Si $a = (a_1, ..., a_n)$ peut être complété en une base $(a, e_2, ...e_n)$ de $M = A^n$, alors en notant encore $N = a.A$ et P le sous-module de M engendré par $(a_2, ..., a_n)$, on a $M = N \oplus P$, donc le pgcd de la famille $(a_1, ..., a_n)$ est 1 d'après c). Réciproquement, si ce pgcd est 1, alors d'après c) il existe un sous-module P de M tel que $M = N \oplus P$. Comme A est principal, on sait alors que P est libre de type fini comme sous-module de A^n, il admet donc une base $(e_2, ..., e_r)$, ce qui fait que $(a, e_2, ..., e_r)$ est une base de A^n. On a bien alors $r = n - 1$ vu que A^n est de rang n.

e) (**2.5 points**). Soit N le sous-module de M engendré par $(f_1, ..., f_r)$. S'il existe un sous-module P de N avec $M = N \oplus P$, alors comme on sait que P est libre, on peut trouver une base $(f_{r+1}, ..., f_n)$ de P telle que $(f_1, ..., f_r, ..., f_n)$ soit une base de M. Si $\mathcal{B}$ est la base canonique de A^n, la matrice B apparaît comme la matrice de l'injection $N \to M$ dans les bases $(f_1, ..., f_r)$ de N et $\mathcal{B}$ de N, et on sait que ses facteurs invariants sont $(1, ..., 1) \in A^r$ car on a

trouvé une base $(f_1, ..., f_r, ..., f_n)$ de M et une base adaptée $(f_1, ..., f_r)$ de N. Ainsi, le pgcd des mineurs d'ordre r de B est 1 d'après la formule qui relie ce pgcd aux facteurs invariants.

Réciproquement, si cette condition est vérifiée, alors le théorème de la base adaptée dit que comme les facteurs invariants de B (matrice de l'injection $N \to M$) sont $(1, ..., 1)$, il existe une base $(u_1, ..., u_n)$ de M telle que $(u_1, ..., u_r)$ soit une base de N, et il suffit de prendre pour P le sous-module engendré par $(u_{r+1}, ..., u_n)$ pour avoir $M = N \oplus P$.

Exercice 4 (6 points+2 pour le bonus)

a) (**1 point**). Soit H le sous-groupe de G engendré par $G_1 \cup G_2$. Le corps fixe L^H est en particulier fixe par G_1 et G_2, donc il est inclus dans F_1 et F_2 (les extensions L/F_1 et L/F_2 sont galoisiennes de groupes de Galois respectifs G_1 et G_2, donc $L^{G_1} = F_1$ et $L^{G_2} = F_2$). ainsi $L^H = K$ puisque $F_1 \cap F_2 = K$, ce qui implique $H = G$ via la correspondance de Galois.

b) (**1 point**). Le corps $F_1 \cap F_2$ est fixe par $G_1 \cup G_2$, donc par G tout entier si $G_1 \cup G_2$ engendre G. Ainsi $F_1 \cap F_2 = K$ puisque l'extension L/K est galoisienne.

c) (**1 point**). Le groupe $G_1 \cap G_2$ fixe F_1 et F_2, donc fixe le corps F engendré par $F_1 \cup F_2$. Si $F = L$, on a donc que $G_1 \cap G_2$ est le groupe trivial. Réciproquement, si $G_1 \cap G_2$ est le groupe trivial, alors comme $\mathrm{Gal}\,(L/F)$ est un sous-groupe de G_1 et de G_2, on obtient que $\mathrm{Gal}\,(L/F)$ est le groupe trivial, et donc $L = F$ via la correspondance de Galois.

d) (**2 points**). D'après ce qu'on vient de voir, on a $G_1 \cap G_2 = \{1\}$ et G est engendré par G_1 et G_2. De plus, les sous-groupes G_1 et G_2 sont distingués dans G vu que F_1 et F_2 sont supposées galoisiennes sur K. Ceci implique (voir cours sur les groupes) que l'ensemble G_1G_2 des produits g_1g_2 avec $g_1 \in G_1$ et $g_2 \in G_2$ est un sous-groupe de G, qui est donc égal à G puisque G est engendré par G_1 et G_2. On sait alors que G est isomorphe à un produit semi-direct de G_1 et G_2, mais comme ces deux sous-groupes sont distingués dans G, il est en fait isomorphe à leur produit direct. Le même argument montrerait que si on suppose seulement G_1 distingué dans G, alors G serait isomorphe à un produit semi-direct $G_1 \rtimes G_2$.

e) (**1 point**). On prend $K = \mathbf{Q}$, $L = \mathbf{Q}(j, \sqrt[3]{2})$, $F_1 = \mathbf{Q}(\sqrt[3]{2})$ et $F_2 = \mathbf{Q}(j.\sqrt[3]{2})$. Alors $G \simeq \mathcal{S}_3$, tandis que G_1 et G_2 sont tous deux isomorphes à $\mathbf{Z}/2\mathbf{Z}$, donc $G_1 \times G_2$ n'est pas isomorphe à G (qui n'est pas abélien).

f) (**2 points**). La propriété universelle du produit tensoriel de deux K-algèbres donne un K-morphisme $f : F_1 \otimes_K F_2 \to F$ tel que

$$f(x_1 \otimes x_2) = x_1x_2$$

pour tous $x_1 \in F_1, x_2 \in F_2$. L'image de f est une K-algèbre F' de dimension finie sur K (comme sous-algèbre de L), c'est donc un corps (le K-morphisme $F' \to F'$ qui envoie y sur xy est injectif, donc bijectif, pour tout x non nul de F'). Comme F' contient clairement F_1 et F_2, elle contient le sous-corps engendré par $F_1 \cup F_2$, c'est-à-dire F. Ainsi f est surjectif.

Il se peut pourtant que $F_1 \otimes_K F_2$ ne soit pas un corps : par exemple dans l'exemple e), comme $F_1 \simeq \mathbf{Q}[T]/(T^3 - 2)$, on a

$$F_1 \otimes_K F_2 \simeq F_2[T]/(T^3 - 2),$$

qui n'est pas un corps vu que le polynôme $T^3 - 2$ ne reste pas irréductible sur F_2.