# Corrigé de l'examen d'algèbre du 19 décembre 2023, M1 MF

**Exercice 1 : Indice d'un sous-groupe (6 points)**

a) Soit $x \in N$, notons $\tilde{x}$ sa classe dans $N/(N \cap H)$ et $\bar{x}$ sa classe dans $G/H$. On définit une application $u$ de $N/(N \cap H)$ dans $G/H$ en envoyant $\tilde{x}$ sur $\bar{x}$ (en effet, si $\tilde{x} = \tilde{y}$ avec $x, y$ dans $N$, alors $x^{-1}y \in (N \cap H) \subset H$ donc $\bar{x} = \bar{y}$). Cette application est injective car si $u(\tilde{x}) = u(\tilde{y})$, alors $x^{-1}y \in H$, mais on a aussi $x^{-1}y \in N$ d'où $x^{-1}y \in (N \cap H)$ et $\tilde{x} = \tilde{y}$. Le résultat en découle (1 point).

b) Comme $[G : H]$ est fini, on a égalité en a) si et seulement si l'application injective $u$ est aussi surjective. Ceci se traduit par le fait que pour tout $\bar{y} \in G/H$, il existe $x \in N$ tel que $\bar{x} = \bar{y}$, ou encore il existe $x \in N$ et $h \in H$ tel que $x = yh$. C'est donc équivalent à $G = NH$ par définition de $NH$ (1 point)

c) On définit une application $\varphi$ de $G/H$ dans $G'/H'$ en envoyant, pour tout $x \in G$, sa classe $\bar{x}$ sur la classe $\overline{f(x)}$ de $f(x)$ dans $G'/H'$. Cette application est bien définie car si $\bar{x} = \bar{y}$, alors $x^{-1}y \in H$, d'où $f(x^{-1}y) \in H'$ par définition de $H$, ce qui donne $f(x)^{-1}f(y) \in H'$, ou encore $\overline{f(x)} = \overline{f(y)}$ dans $G/H$. La surjectivité de $f$ donne immédiatement celle de $\varphi$. Enfin, $\varphi(x) = \varphi(y)$ implique $f(x)^{-1}f(y) \in H'$, soit $x^{-1}y \in f^{-1}(H') = H$, soit $\bar{x} = \bar{y}$, ce qui montre l'injectivité de $\varphi$. Finalement, $\varphi$ est bijective d'où le résultat (1 point).

d) Le résultat est clair si le cardinal de $G$ est $p$. Soit maintenant $G$ un $p$-groupe de cardinal $p^m$ avec $m > 1$, et supposons le résultat vrai pour les $p$-groupes de cardinal $< p^m$. On sait que le centre $Z$ de $G$ est non trivial, et comme $G$ n'est pas abélien le $p$-groupe $G' := G/Z$ est de cardinal strictement compris entre 1 et $p^m$, ce qui permet de lui appliquer l'hypothèse de récurrence s'il n'est pas abélien (voir e) pour le cas où $G$ est abélien). Ainsi, $G'$ contient un sous-groupe $H'$ d'indice $p$, et il suffit (via c) de prendre pour $H$ l'image réciproque de $H'$ par la surjection canonique $G \to G/Z$ pour avoir $H$ d'indice $p$ dans $G$ (2 points).

e) Oui. On raisonne encore par récurrence sur le cardinal de $G$. Si $G$ est cyclique d'ordre $p^m$ avec $m > 0$ (en particulier s'il est d'ordre $p$), on sait que $G$ a un sous-groupe d'ordre $p^{m-1}$. Sinon, $G$ possède un sous-groupe $H$ d'ordre strictement compris entre 1 et $|G|$ (le sous-groupe engendré par tout élément non trivial) et on peut appliquer l'hypothèse de récurrence à $G/H$, puis utiliser c) pour conclure (1 point).

**Exercice 2 : Dimension d'un anneau (5 points)**

a) Déjà, l'anneau non nul $A$ contient toujours un idéal maximal (qui est premier), donc la dimension de $A$ est bien $\geq 0$. Si $A$ est de dimension zéro, tout idéal premier $\wp$ est contenu dans un idéal maximal (donc premier) $I$, ce qui implique $I = \wp$, sinon on aurait une suite strictement croissante de deux idéaux premiers et la dimension de $A$ serait au moins 1. Réciproquement, si tout idéal premier est maximal, on ne peut avoir $\wp_0$ strictement inclus dans $\wp_1$ avec $\wp_0$ et $\wp_1$ premiers, par maximalité de $\wp_0$. Ainsi $\dim A = 0$ (1 point).

b) Un tel idéal premier de $A = k[X]/(X^n)$ est de la forme $I/(X^n)$, avec $I$ idéal premier de $k[X]$ contenant $X^n$. On sait que comme $k[X]$ est princpal, $I$ est engendré par un polynôme irréductible (qu'on peut prendre unitaire) $P$, avec $P$ divisant $X^n$ puisque $(P)$ contient $(X^n)$. Ainsi $P = X$ est le seul idéal premier de $A$, qui est donc de dimension zéro (1.5 point).

c) Si $A$ est principal, on a déjà l'idéal premier $\{0\}$. Comme $A$ n'est pas un corps, cet idéal n'est pas maximal, il est donc contenu strictement dans un idéal maximal (donc premier), ce qui montre que $\dim A \leq 1$. Par ailleurs, on sait que tout idéal premier non nul d'un anneau principal est maximal, donc on ne peut pas avoir

$$\wp_0 \subset \wp_1 \subset \wp_2$$

avec les $\wp_i$ premiers et les inclusions strictes, sinon cela contredirait la maximalité de $\wp_1$ (1.5 point).

d) Il suffit de prendre la châine

$$0 \subset (X_1) \subset (X_1, X_2) \subset ...(X_1, ...X_n)$$

En effet, on a que le quotient de $K[X_1, ..., X_n]$ par $(X_1, ..., X_r)$ s'identifie à $K[X_{r+1}, ..., X_n]$ (comme vu en cours pour $n = 2$, via $P \mapsto P(X_{r+1}, ..., X_n)$), qui est intègre, donc tous les idéaux de cette chaîne sont premiers (1 point). On a en fait $\dim A = n$, mais c'est beaucoup plus difficile à montrer.

**Exercice 3 : Modules de type fini (6 points)**

a) Tout élément de $(1+x)M$ s'écrit $(1+x)m$ avec $m \in M$. Mais $M = IM$, donc $m$ est somme finie d'éléments de la forme $am'$ avec $a \in I$ et $m' \in M$.

Ainsi, $(1+x)m$ est somme finie d'éléments de la forme $a(1+x)m'$ avec $a \in I$ et $m' \in M$. Mais l'hypothèse $(1+x)M' = 0$ implique $(1+x)M \subset A.w$, donc chaque $a(1+x)m'$ s'écrit $abw$ avec $b \in A$, soit $i.w$ avec $i \in I$, il est donc dans $I.w$. Finalement, tout élément de $(1+x)M$ est bien dans $I.w$ (1.5 point).

b) Tout élément $t$ de $(1+x)M$ s'écrit $t = aw$ avec $a \in A$. Alors $(1+x-y)t = a(1+x-y)w$, mais $(1+x-y)w = 0$ via a) (0.5 point).

c) Posons $z = (1+x-y)(1+x) - 1$, alors $(1+z)M = 0$ via b). Par ailleurs, $z = x + (x-y) + x(x-y)$ est bien dans l'idéal $I$, vu que $x$ et $y$ y sont (1 point).

d) Supposons $P$ engendré par $s$ éléments $w_1, ...., w_s$, on procède par récurrence sur $s$. Si $s = 0$, il n'y a rien à démontrer. Supposons le résultat vrai quand $P$ est engendré par au plus $s-1$ éléments. On peut alors appliquer l'hypothèse de récurrence à $M' = P/A.w_s$, qui vérifie clairement encore $IM' = M'$, et est engendré par les classes de $w_1, ..., w_{s-1}$. Ainsi il existe $x \in I$ tel que $(1+x)M' = 0$. D'après c), on a alors un $z \in I$ tel que $(1+z)P = 0$, et il suffit de poser $a = 1+z$ (2 points).

e) On applique d). Ici, $a$ ne peut être dans aucun idéal maximal $J$ de $A$, sinon comme $(a-1) \in I$, on aurait $(a-1) \in J$, puis $1 \in J$. Ainsi, $a$ est inversible et $aP = 0$ donne alors $P = 0$ en multipliant par $a^{-1}$ (1 point). C'est une des formes du lemme de Nakayama.

**Exercice 4 : Théorie de Galois (4 points)**

a) On a vu en cours que $\mathbf{Q}(j, \sqrt[3]{2})$ est galoisienne, mais son groupe de Galois $\mathcal{S}_3$ n'est pas abélien (0.5 point).

b) On sait que l'extension $L/F$ est galoisienne, avec $\mathrm{Gal}\,(L/F)$ sous-groupe de $\mathrm{Gal}\,(L/K)$. Comme on sait qu'un sous-groupe d'un groupe abélien (resp. cyclique) est cyclique (resp. cyclique), on a $L/F$ abélienne (resp. cyclique) dès que $L/K$ est abélienne (resp. cyclique).

Par ailleurs, si $\mathrm{Gal}\,(L/K)$ est abélien, le sous-groupe $\mathrm{Gal}\,(L/F)$ en est un sous-groupe distingué, et on sait qu'alors $\mathrm{Gal}\,(F/K)$ est un quotient de $\mathrm{Gal}\,(L/K)$. C'est donc aussi un groupe abélien et $F/K$ est abélienne. Si de plus $\mathrm{Gal}\,(L/K)$ est cyclique, alors tout quotient de ce groupe est aussi cyclique (il est engendré par l'image dans le quotient d'un générateur de $\mathrm{Gal}\,(L/K)$), et donc $F/K$) est cyclique (1.5 point).

c) On sait que $\mathbf{Q}(\zeta)/Q$ est une extension galoisienne de groupe de Galois $(\mathbf{Z}/n\mathbf{Z})^*$. choisissons $n = p^{m+1}$, alors si $p > 2$ on a vu que ce groupe $G$ est cyclique d'ordre $p^m(p-1)$. On sait qu'un tel groupe a un sous-groupe $H$ d'ordre $p-1$, donc d'indice $p^m$. Par la correspondance de Galois, ce sous-groupe correspond à une extension $L$ de $\mathbf{Q}$ avec $\mathrm{Gal}\,(L/\mathbf{Q}) = G/H$, i.e. ce groupe de Galois est cyclique d'ordre $p^m$ comme on voulait (2 points). Si

$p = 2$, le groupe $G$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2^{m-1}\mathbf{Z})$, qui a de manière évidente un sous-groupe isomorphe à $(\mathbf{Z}/2^{m-1}\mathbf{Z})$ ; il suffit alors de remplacer $m$ par $m + 1$.