# Corrigé de l'examen d'algèbre de M1

**Exercice 1 : Groupes (4 points)**

a) Si $A$ est un groupe abélien, on a $D(A) = \{1\}$ par définition du sous-groupe dérivé, donc seul le groupe trivial est abélien et parfait (0.5 point).

b) Si $G$ est simple, alors comme $D(G)$ est distingué dans $G$, le seul cas où $D(G) \neq G$ est quand $D(G)$ est trivial, c'est-à-dire quand $G$ est abelien. On sait qu'alors $G$ est isomorphe à $\mathbf{Z}/p\mathbf{Z}$ avec $p$ premier, qui est effectivement simple et non parfait (1 point).

c) Soit $(g, h)$ dans $G \times H$ avec $g \in G$ et $h \in H$. On observe que $(g, h) = (g, 1).(1, h)$, et il suffit donc de prouver que $(g, 1)$ et $(1, h)$ sont des produits de commutateurs. Comme $G$ est parfait, tout $g \in G$ est produit de commutateurs. Or, si $g = c_1...c_r$ (où chaque $c_i$ est un commutateur), $(g, 1)$ est le produit des $(c_i, 1)$, et si $c_i = [x_i, y_i]$, alors $(c_i, 1) = [(x_i, 1), (y_i, 1)]$ est encore un commutateur. La preuve pour $(1, h)$ est analogue (1.5 point).

d) Soit $f : G \to A$ un morphisme. Alors l'image d'un commutateur $[x, y]$ de $G$ est le commutateur $[f(x), f(y)]$, qui est trivial vu que $A$ est abélien. Comme $G$ est parfait, il est engendré par les commutateurs, donc comme $\ker f$ contient tous les commutateurs, c'est $G$ tout entier (1 point).

**Exercice 2 : Anneaux (6 points)**

a) Supposons $I$ premier. Alors $I \neq A$ par définition. Si $xy \in I$ et $y \notin I$, alors $x \in I$ donc a fortiori $x \in \sqrt{I}$ (en prenant $n = 1$ dans la définition de $\sqrt{I}$) (1 point).

b) Prenons $I = 4\mathbf{Z}$. Alors $I$ n'est pas premier car il contient 2.2, mais pas 2. Si maintenant $xy \in I$ et $y \notin I$, alors comme 4 ne divise pas $y$ on a forcément $x$ pair, et alors $x^2 \in I$, donc $x \in \sqrt{I}$. ainsi, $I$ est primaire (1 point).

c) Soit $Q$ un idéal maximal de $A$ contenant $I$. Alors il contient $\sqrt{I}$ cat si $x^n \in I$, alors $x^n \in Q$, d'où $x \in Q$ vu que $Q$ est premier (car maximal). Comme $\sqrt{I}$ est maximal et $Q \neq A$, cela impose $Q = \sqrt{I}$ (1.5 point).

d) Supposons le contraire. Alors il existerait un idéal maximal $Q$ contenant $I$ et $x$. D'après c), on aurait $Q = \sqrt{I}$, ce qui est impossible vu que $x \notin \sqrt{I}$ (1 point).

e) Déjà $I \neq A$, sinon $\sqrt{I} = A$ ne serait pas maximal. Soient $x, y$ dans $A$ avec $xy \in I$ et $y \notin I$. Si on avait $x \notin \sqrt{I}$, on pourrait d'après d) écrire $1 = ax + i$ avec $a \in A$ et $i \in I$. Alors $y = axy + iy$ serait dans $I$, puisque $xy$ et $i$ sont dans $I$, contradiction. Ainsi, $I$ est primaire (1.5 point).

**Exercice 3 : Modules (6 points+1 point pour la question bonus)**

a) On applique la définition d'un module injectif au morphisme identité $Q \to Q$ : il existe un morphisme $r : M \to Q$ qui prolonge l'identité, i.e. $r \circ i = \mathrm{Id}_Q$ (1 point).

b) On pose $P = \ker r$. Alors, si $x \in P \cap Q$, on a $r(x) = 0$ et aussi $x = r(x) = 0$ donc $P$ et $Q$ sont en somme directe. Si maintenant $y \in M$, alors on écrit $y = (y - r(y)) + r(y)$, avec $r(y) \in Q$ et $(y - r(y)) \in \ker r$, vu que comme $r(y) \in Q$, il est fixé par $r$ (1 point).

c) Si $x \in aA$, il existe $y \in A$ tel que $x = ay$, et ce $y$ est unique parce que $A$ est intègre et $a \neq 0$, d'où un morphisme de $aA$ dans $A$ défini par $x \mapsto x/a := y$. On définit alors bien un morphisme $u$ de $aA$ dans $M$ en envoyant $x = ay$ sur $ym = (x/a)m$ et ce morphisme envoie $a$ sur $m$ (1.5 point).

d) Soit $m \in Q$ et $a$ non nul dans $A$. D'après c), on a un morphisme $u : aA \to Q$ qui envoie $a$ sur $m$. Comme $Q$ est injectif, on le prolonge en un morphisme $f : A \to Q$. Alors $f(a) = af(1) = m$, ce qui montre qu'on a bien un élément $z$ de $Q$ (à savoir $f(1)$) tel que $az = m$ (1 point).

e) Notons au passage que $z$ existe bien via l'hypothèse que $D$ est divisible (même si $d = 0$ car alors $y = 0$). Montrons qu'on peut définir $g$ par la formule $g(n + ax_0) = f(n) + az$ pour tous $n \in N, a \in A$. L'écriture d'un élément $y$ de $(N + Ax_0)$ sous la forme $y = n + ax_0$ n'est en général pas unique ; toutefois, si $n + ax_0 = n' + a'x_0$, alors $(a' - a)x_0 = n - n'$ est dans $N$, ce qui montre que $(a' - a) \in I$, donc par définition de $d$ on peut écrire $(a' - a) = db$ avec $b \in A$. Alors $n' - n = -dbx_0$, ce qui donne

$$f(n') + a'z = f(n) + az - f(bdx_0) + dbz = f(n) + az - f(bn_0) + by = f(n) + az,$$

vu que $f(n_0) = y$. Ainsi $g$ est bien défini, et il est alors immédiat que c'est un morphisme (1.5 point).

f) Soit $N$ un sous-module d'un $A$-module $M$ et soit $f : N \to A$ un morphisme. Considérons l'ensemble $E$ des paires $(P, g)$, où $P$ est un sous-module de $M$ contenant $N$ et $g$ prolonge $f$. L'ensemble $E$ est partiellement ordonné

par la relation $(P, g) \leq (P', g')$ ssi $P' \supset P$ et $g'$ prolonge $g$. L'ensemble $E$ est inductif pour cet ordre, car si $((P_i, g_i))_{i \in I}$ est une famille totalement ordonnée d'éléments de $E$, on en obtient un majorant $(R, h)$ en prenant pour $R$ la réunion des $P_i$ (qui reste un sous-module parce que la famille est totalement ordonnée) et pour $h$ le morphisme dont la restriction à chaque $P_i$ est $g_i$ (il est bien défini, toujours parce que la famille est totalement ordonnée). Le lemme de Zorn dit alors que $E$ admet un élément maximal $(P_0, g_0)$. Mais alors, $P_0 = M$, sinon le e) permettrait de prolonger $g_0$ à un sous-module $P_0 + Ax$ contenant strictement $P_0$, ce qui contredirait la maximalité de $(P_0, g_0)$ (1 point de bonus).

**Exercice 4 : Corps, théorie de Galois (5 points +1 pour le bonus)**

a) Supposons $P$ non scindé sur $K$, il admet alors une racine $\alpha$ dans $L$ (vu que $P$ est scindé sur $L$) qui n'est pas dans $K$. Le corps $K(\alpha)$ est alors inclus dans $L$, donc le degré $[K(\alpha) : K]$ (qui est $> 1$ vu que $\alpha \notin K$) doit diviser $n = [L : K]$, donc ce degré est $n$ vu que $n$ est premier. Mais ceci est impossible car comme $P$ est divisible par $X - 1$, ses facteurs irréductibles sont de degré au plus $n - 1$ donc le polynôme minimal de $\alpha$ est de degré au plus $n - 1$ (1.5 point).

b) Prenons $K = \mathbf{Q}$ et $L = \mathbf{Q}(i, \sqrt{2})$, alors $L$ est de degré 4 sur $\mathbf{Q}$ et $X^4 - 1$ est scindé sur $L$, pourtant il n'est pas scindé sur $\mathbf{Q}$ car $i \notin \mathbf{Q}$ (1 point).

c) Considérons le sous-groupe dérivé $D(G)$ de $G$. Soit $M = L^{D(G)}$ le corps fixe par $D(G)$. La correspondance de Galois dit alors que comme $D(G)$ est distingué dans $G$, l'extension $M/K$ est galoisienne de groupe $G/D(G)$, lequel est abélien. Si $M'$ a cette propriété, alors le groupe de Galois $H := \mathrm{Gal}\,(L/M')$ doit être distingué et le quotient $G/H = \mathrm{Gal}\,(M'/K)$ doit être abélien, ce qui signifie $H \supset D(G)$, ou encore par la correspondance de Galois que $M' \subset M$ (1.5 point).

d) On a vu en cours que $\mathrm{Gal}\,(L/K)$ est isomorphe à $\mathcal{S}_3$ qui n'est pas abélien. Comme le seul sous-groupe distingué non trivial de $\mathcal{S}_3$ est $\mathcal{A}_3$ (qui est d'indice 2 dans $\mathcal{S}_3$), l'extension $M$ est l'unique extension de degré 2 de $\mathbf{Q}$ incluse dans $L$, soit $M = \mathbf{Q}(j)$ (1 point).

e) Soit $L'$ la clôture galoisienne de $L$ sur $K$, posons $G' = \mathrm{Gal}\,(L'/K)$ et $U = \mathrm{Gal}\,(L'/L)$. On s'intéresse aux extensions $M$ intermédiaires entre $K$ et $L'$, qui vérifient $M/K$ galoisienne, $M \subset L$, et $\mathrm{Gal}\,(M/K)$ abélien. Posons $H = \mathrm{Gal}\,(L'/M)$, les conditions se traduisent par $H$ distingué dans $G'$ avec $G'/H$ abélien et $H \supset U$. Il existe un plus petit sous-groupe vérifiant ces conditions, c'est le sous-groupe $V$ engendré par $D(G')$ et $U$. L'extension $M = (L')^V$ associée à $V$ par la correspondance de Galois répond alors à la question (1 point de bonus).