Université Paris 7
U.F.R. de Mathématiques

26 mai 2002
B. Keller

Maîtrise de Mathématiques : MT401S Algèbre

Un corrigé de l'examen de Juin 2002

Question de cours

Soient A un anneau principal et M un A-module de type fini.

1) Qu'est-ce que le sous-module de torsion M_{tors} de M ? Montrer que M/M_{tors} est sans torsion.
Réponse — Le sous-module M_{tors} est formé des éléments $m \in M$ tels qu'il existe un élément non nul $a \in A$ tel que $am = 0$. Soit π la projection canonique de M sur M/M_{tors} et soit $\pi(m)$ un élément de torsion de M/M_{tors}. Soit a un élément non nul de A tel que $a\pi(m) = 0$. Alors am appartient à M_{tors} car $\pi(am) = a\pi(m) = 0$. Soit b un élément non nul de A tel que $b(am) = 0$. Alors ba est un élément non nul de A (car A est intègre) et $(ba)m = b(am) = 0$. Donc m appartient à M_{tors} et $\pi(m) = 0$.
2) Que peut-on dire d'un A-module de type fini sans torsion ?
Réponse — Comme A est principal, un tel module est libre.
3) Montrer que M_{tors} est un facteur direct de M qui admet un supplémentaire libre. Montrer par un exemple que ce supplémentaire n'est pas unique en général.
Réponse — Le module M/M_{tors} est libre donc la suite exacte

$$0 \to M_{tors} \to M \to M/M_{tors} \to 0$$

est scindable. Donc M_{tors} admet un supplémentaire isomorphe à M/M_{tors} et donc libre. Si $A = \mathbb{Z}$ et $M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, alors $M_{tors} = 0 \oplus \mathbb{Z}/2\mathbb{Z}$. Les sous-modules $L_1 = Z \oplus \mathbb{Z}/2\mathbb{Z}$ et $L_2 = \{(x, \pi(x) \mid x \in \mathbb{Z}\}$ sont deux supplémentaires libres de M_{tors} qui sont différents.
4) Soit $L \supset K$ une extension de corps finie. Qu'est-ce que le degré de L sur K ? Qu'est-ce que le groupe de Galois $Gal(L|K)$? Quand est-ce qu'on dit que l'extension est galoisienne ?
Réponse — Par l'inclusion $K \subset L$, le corps L devient une K-algèbre et en particulier un K-espace vectoriel. Le degré de L sur K est la dimension de cet espace. Le groupe de Galois est le groupe des automorphismes σ du corps L tels que $\sigma(x) = x$ pour tout $x \in K$. On dit que l'extension est galoisienne si son degré est égal à l'ordre de son groupe de Galois.
5) Supposons que $L \supset K$ est galoisienne de groupe de Galois cyclique d'ordre 10. Quel est le nombre d'extensions intermédiaires $L \supset E \supset K$?
Réponse — Le théorème principal de la théorie de Galois donne une bijection entre les sous-groupes du groupe de Galois et les extensions intermédiaires entre L et K. Le groupe $\mathbb{Z}/10\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ admet quatre sous-groupes (outre le sous-groupe trivial et le groupe tout entier, les seuls sous-groupes sont $\mathbb{Z}/2\mathbb{Z} \times 0$ et $0 \times \mathbb{Z}/5\mathbb{Z}$). Donc il existe quatre extensions intermédiaires $L \supset E \supset K$.

I. Décompositions

Soit M le $\mathbb{Z}$-module $\mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/135\mathbb{Z}$.

1) Quelle est la composante 3-primaire $M(3) \subset M$?
Réponse — C'est le sous-groupe $8\mathbb{Z}/24\mathbb{Z} \oplus 4\mathbb{Z}/36\mathbb{Z} \oplus 5\mathbb{Z}/135\mathbb{Z}$.
2) Quelle est la décomposition de M en $\mathbb{Z}$-modules indécomposables ?
Réponse — Nous utilisons le lemme chinois. La décomposition en indécomposables de M est

$$M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}.$$

3) Quelle est la décomposition de Smith de M et quels sont ses facteurs invariants ?
Réponse — Nous utilisons le lemme chinois. La décomposition de Smith de M est

$$M \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/1080\mathbb{Z}$$

et ses facteurs invariants sont $3, 36, 1080$.

II. Cayley-Hamilton

Soient A un anneau commutatif, $n \geq 1$ et C une matrice $n \times n$ à coefficients dans A. Rappelons qu'on a

$$\hat{C}C = C\hat{C} = \det(C) I_n$$

où $(-1)^{i+j}\hat{C}_{ij}$ est le déterminant de la sous-matrice de C obtenue en rayant la j-ième ligne et la i-ième colonne. Soit M le conoyau du morphisme $f_C : A^n \to A^n$, $x \mapsto Cx$.

1) Montrer qu'on a $(\det C)m = 0$ pour tout $m \in M$.
Réponse — Notons $\pi : M \to M/f_C(M)$ la projection canonique sur le conoyau de f_C. Soit m un élément du conoyau et $m' \in M$ un représentant. Nous avons

$$(\det C)m = (\det C)\pi(m') = \pi((\det C)m') = \pi(C\hat{C}m') = 0$$

car $C\hat{C}m'$ appartient à l'image de f_C.

2) Soient k un corps et B une matrice $n \times n$ à coefficients dans k. Soient C la matrice $X\, I_n - B$ (à coefficients dans $k[X]$) et $\chi_B(X) = \det(C)$ le polynôme caractéristique de B. Soit M_B le $k[X]$-module qui correspond à B. Montrer que $\chi_B(X)\, m = 0$ pour tout $m \in M_B$.
Réponse — Un théorème du cours affirme que M_B est isomorphe au conoyau de

$$f_C : k[X]^n \to k[X]^n\ ,\ v \mapsto Cv\ ,$$

où $C = XI_n - B$. L'affirmation résulte aussitôt du point précédent.

3) En déduire que $\chi_B(B) = 0$ (Cayley-Hamilton).
Réponse — Pour tout polynôme $P(X) \in k[X]$ et tout élément $v \in M_B$, on a $P(X)m = P(B)(v)$, par définition. En particulier, on a $\chi_B(X)v = \chi_B(B)(v)$. Or d'après le point précédent, l'élément $\chi_B(X)v$ s'annnule pour tout $v \in M_B$. Donc $\chi_B(B) = 0$.

III. Idéaux maximaux de $\mathbb{Z}[X]$

On se propose de déterminer les idéaux maximaux de l'anneau $\mathbb{Z}[X]$.

1) Montrer qu'aucun idéal principal de $\mathbb{Z}[X]$ n'est maximal.
Réponse — Soit $P(X)$ un élément de $\mathbb{Z}[X]$. Si $P(X) = c$ pour un $c \in \mathbb{Z}$, alors $\mathbb{Z}[X]/(P(X))$ est isomorphe à $(\mathbb{Z}/c\mathbb{Z})[X]$. Cet anneau n'est pas un corps : en effet, si $c = \pm 1$, c'est l'anneau nul, et sinon c'est l'anneau de polynômes sur $\mathbb{Z}/c\mathbb{Z}$, dont les seuls éléments inversibles sont les constantes inversibles. Si $P(X)$ est non constant, alors les éléments non nuls de $(P(X))$ sont de degré ≥ 1. Donc $(P(X))$ est strictement contenu dans $(P(X), p)$ pour tout nombre premier p. Choisissons p tel que le coefficient dominant de $P(X)$ n'est pas divisible par p. Alors l'idéal $(P(X), p)$ est différent de $\mathbb{Z}[X]$ (car le quotient par cet idéal est isomorphe au quotient de $(\mathbb{Z}/p\mathbb{Z})[X]$ par un idéal propre) et il contient strictement $(P(X))$. Donc $(P(X))$ n'est pas maximal.

2) Soit p un nombre premier et $P \in \mathbb{Z}[X]$ un polynôme dont l'image dans $\mathbb{F}_p[X]$ est irréductible. Montrer que l'idéal (p, P) est maximal dans $\mathbb{Z}[X]$. Nous allons montrer dans la suite qu'on obtient ainsi tous les idéaux maximaux.
Réponse — En utilisant des isomorphismes canoniques démontrés en cours nous obtenons

$$\mathbb{Z}[X]/(p, P(X)) \xrightarrow{\sim} (\mathbb{Z}[X]/(p))/(\pi(P(X)) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P(X))\ ,$$

où π est la projection canonique sur le quotient $\mathbb{Z}[X]/(p)$. Par hypothèse, le dernier anneau est un corps. Donc $(p, P(X))$ est maximal.

3) Soit I un idéal maximal de $\mathbb{Z}[X]$. Montrer que $I \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.
Réponse — L'idéal $I \cap \mathbb{Z}$ est l'image réciproque de I par l'inclusion $\mathbb{Z} \subset \mathbb{Z}[X]$. Comme I est premier dans $\mathbb{Z}[X]$, $I \cap \mathbb{Z}$ est premier dans $\mathbb{Z}$.

4) Supposons que $I \cap \mathbb{Z}$ est un idéal non nul de $\mathbb{Z}$. Montrer que $I = (p, P)$ pour un nombre premier p et un polynôme $P \in \mathbb{Z}[X]$ dont l'image dans $\mathbb{F}_p[X]$ est irréductible.
Réponse — Comme $I \cap \mathbb{Z}$ est premier et non nul, il est de la forme (p) pour un nombre premier p. Nous avons donc $p\mathbb{Z}[X] \subset I$ et $\mathbb{Z}[X]/I$ est un quotient de

$$\mathbb{Z}[X]/(p) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X].$$

Le morphisme induit $(\mathbb{Z}/p\mathbb{Z})[X] \to \mathbb{Z}[X]/I$ est clairement surjectif et son noyau est donc un idéal maximal. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il est engendré par un polynôme $Q(X)$ irréductible à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Si nous choisissons $P(X) \in \mathbb{Z}[X]$ tel que l'image de $P(X)$ soit $Q(X)$, nous obtenons l'affirmation.

Dans la suite, nous supposons que $I \cap \mathbb{Z}$ est nul. Nous allons aboutir à une contradiction.

5) Montrer que le morphisme canonique $\mathbb{Z} \to \mathbb{Z}[X]$ se prolonge en un morphisme $\mathbb{Q} \to \mathbb{Z}[X]/I$ et que ce dernier se prolonge en un morphisme surjectif $\phi : \mathbb{Q}[X] \to \mathbb{Z}[X]/I$.
Réponse — Le noyau de la composition $\mathbb{Z} \to \mathbb{Z}[X] \to \mathbb{Z}[X]/I$ est l'idéal $I \cap \mathbb{Z}$. Par hypothèse, il s'annule. Donc les images dans $\mathbb{Z}[X]/I$ des éléments non nuls de $\mathbb{Z}$ sont non nuls, et, par conséquent, inversibles. Par la propriété universelle de l'anneau des fractions, le morphisme $\mathbb{Z} \to \mathbb{Z}[X]/I$ induit un morphisme $f : \mathbb{Q} \to \mathbb{Z}[X]/I$. Alors, par la propriété universelle de l'anneau des polynômes, il existe un unique morphisme $\phi : \mathbb{Q}[X] \to \mathbb{Z}[X]/I$ qui prolonge f et envoie $X \in \mathbb{Q}[X]$ sur l'image de $X \in \mathbb{Z}[X]$ dans $\mathbb{Z}[X]/I$. L'image de ϕ contient clairement l'image de $\mathbb{Z}[X]$ dans $\mathbb{Z}[X]/I$. Donc ϕ est surjectif.

6) Montrer que $\ker(\phi)$ est engendré par un polynôme irréductible $Q(X) \in \mathbb{Q}[X]$.
Réponse — Nous avons un isomorphisme de $\mathbb{Q}[X]/\ker\phi$ sur le corps $\mathbb{Z}[X]/I$. Donc $\ker\phi$ est un idéal maximal de $\mathbb{Q}[X]$. Comme $\mathbb{Q}$ est un corps, il est engendré par un polynôme irréductible Q.

7) Montrer que I est engendré par le polynôme primitif $P \in \mathbb{Z}[X]$ associé à Q. Conclure.
Réponse — Ecrivons $Q(X) = cP(X)$ où $P(X)$ est à coefficients dans $\mathbb{Z}$ et primitif et c est le contenu de $Q(X)$. Soit $U(X)$ un polynôme à coefficients entiers qui appartient à I. Alors dans $\mathbb{Q}[X]$, $U(X)$ appartient à l'idéal engendré par $Q(X)$. Donc

$$U(X) = V(X)Q(X)$$

pour un polynôme $V(X) \in \mathbb{Q}[X]$. Ecrivons $U(X) = uU_1(X)$ et $V(X) = vV_1(X)$, où $U_1(X)$ et $V_1(X)$ sont à coefficients entiers et primitifs et u et v sont les contenus de $U(X)$ et $V(X)$. Par la propriété de multiplicativité des contenus et des parties primitives, nous avons

$$U_1(X) = \pm V_1(X)P(X)$$

et

$$U(X) = uU_1(X) = \pm uV_1(X)P(X).$$

Comme $U(X)$ est á coefficients entiers, u est entier et $\pm uV_1(X)$ est à coefficients entiers. Donc $U(X)$ appartient bien à l'idéal de $\mathbb{Z}[X]$ engendré par $P(X)$. Ceci est une contradiction avec le point 1).

IV. Modules semisimples sur un anneau principal

Soit A un anneau principal. Un A-module M est *semi-simple* si pour tout sous-module $M' \subset M$, il existe un sous-module $M'' \subset M$ tel que $M = M' \oplus M''$.

1) Soit k un corps. Montrer que tout k-module de type fini est semi-simple.
Réponse — Soit M un k-module de type fini, c'est-à-dire un k-espace vectoriel de dimension finie. On sait que tout sous-espace vectoriel $M' \subset M$ admet un sous-espace supplémentaire (si on complète une base $v_1, \ldots, v_p$ de M' et une base $v_1, \ldots, v_n$ de M', alors $v_{p+1}, \ldots, v_n$ engendrent un supplémentaire). Donc M est semi-simple.

2) Soient p un irréductible de A et $m \in \mathbb{N}$. Montrer que $(A/(p))^m$ est semi-simple.
Réponse — L'anneau $k = A/(p)$ est un corps. Le A-module $(A/(p))^m$ est aussi un module sur le corps k et ses sous-A-modules sont exactement ses sous-k-espaces vectoriels. Par le point précédent, le module $(A/(p))^m$ est semi-simple.

3) Soient p un irréductible de A et $n \in \mathbb{N}$. Montrer que le module $A/(p^m)$ est semi-simple si et seulement si $m = 1$.
Réponse — Si $m = 1$, la semi-simplicité résulte du point précédent. Réciproquement, supposons que $A/(p^m)$ est semi-simple. Alors la suite exacte

$$0 \to pA/(p^m) \to A/(p^m) \to A/(p) \to 0$$

est scindable. Donc $A/(p^m)$ est isomorphe à la somme directe de $A/(p)$ et $pA/(p^m)$. Comme $A/(p^m)$ est indécomposable, il s'ensuit que $pA/(p^m) = 0$, donc $m = 1$.

4) Soit M un module semi-simple. Montrer que tout sous-module $N \subset M$ est semi-simple.
Réponse — Soit N' un sous-module de N. Alors il existe un supplémentaire M'' de N' dans M. Soit $N'' = N \cap M''$. Il est clair que $N' \cap N'' = 0$. Montrons que $N' + N'' = N$. L'inclusion $\subset$ est claire. Soit $n \in N$. Alors $n = n' + m''$ pour un $n' \in \mathbb{N}$ et un $m'' \in M''$. Nous avons $m'' = n - n''$. Donc $m'' \in N''$.

5) Soient p un irréductible et M un A-module p-primaire de type fini. Montrer que M est semi-simple si et seulement si M est isomorphe à $(A/(p))^n$ pour un $n \in \mathbb{N}$.
Réponse — Nous avons vu au point 2) que la condition est suffisante. Réciproquement, supposons que M est semi-simple. Comme M est p-primaire, M est somme directe de sous-modules isomorphes à des modules $A/(p^m)$ pour des $m \in \mathbb{N}$. D'après 4), ces $A/(p^m)$ sont semi-simples. D'après 3), on doit avoir $m = 1$. Donc M est bien isomorphe à une somme $(A/(p))^n$ pour un $n \in \mathbb{N}$.

6) Soit M un A-module de torsion et de type fini. Montrer que M est semi-simple si et seulement si pour tout irréductible p de A, la composante p-primaire $M(p)$ est semi-simple. Déduire que M est semi-simple si et seulement si M est isomorphe à une somme directe finie de modules de la forme $A/(p)$, où p est irréductible.
Réponse — Supposons que M est semi-simple. Les composantes p-primaires de M sont en particulier des sous-modules. Donc elles sont semi-simples d'après 4). Réciproquement, supposons que les composantes p-primaires de M sont semi-simples. Soit $N \subset M$ un sous-module. Alors $N(p) \subset M(p)$ est un sous-modules pour chaque irréductible p. On choisit un supplémentaire N'_p de $N(p)$ dans $M(p)$. Alors la somme des N'_p est un supplémentaire de N dans M. La deuxième affirmation en résulte d'après 5).

7) Soient $n \geq 1$ et B une matrice carrée $n \times n$ à coefficients réels. Soit $f_B : \mathbb{R}^n \to \mathbb{R}^n$ l'application $x \mapsto Bx$. Montrer qu'on a équivalence entre
(i) Tout sous-espace $U \subset \mathbb{R}^n$ stable par f_B admet un supplémentaire stable par f_B.
(ii) B est semblable à une matrice diagonale par blocs dont les blocs diagonaux sont de la forme

$$[a]\ ,\ a \in \mathbb{R}, \quad \text{ou} \quad \begin{bmatrix} \rho\cos\theta & -\rho\sin\theta \\ \rho\sin\theta & \rho\cos\theta \end{bmatrix}\ ,\ \rho > 0\ ,\ \theta \in \mathbb{R}.$$

Réponse — Supposons que (i) est vérifié. Soit M le $\mathbb{R}[X]$-module associé à B. Alors il résulte de (i) que M est semi-simple. Donc M est isomorphe à une somme de modules $\mathbb{R}[X]/(P(X))$ où $P(X)$ est irréductible dans $\mathbb{R}[X]$. On sait que les irréductibles de $\mathbb{R}[X]$ sont de la forme $X - a$, $a \in \mathbb{R}$, et $X^2 + bX + c$ où $b^2 - 4c < 0$. On sait qu'un module $\mathbb{R}[X]/(X - a)$ correspond à un bloc $[a]$. Il reste à montrer qu'un module $\mathbb{R}[X]/(X^2 + bX + c)$ correspond à un bloc du deuxième type. En effet, écrivons les deux racines complexes conjuguées de $X^2 + bX + c$ sous la forme $\rho e^{i\theta}$. Alors $b = 2\cos\theta$ et $c = \rho^2$. Alors la matrice compagnon de $X^2 + bX + c$ et la matrice

$$\begin{bmatrix} \rho\cos\theta & -\rho\sin\theta \\ \rho\sin\theta & \rho\cos\theta \end{bmatrix}\ ,\ \rho > 0\ ,\ \theta \in \mathbb{R}.$$

sont toutes deux diagonalisables sur $\mathbb{C}$ avec les mêmes valeurs propres. Donc elles sont semblables sur $\mathbb{C}$ et donc sur $\mathbb{R}$. Ainsi elles correspondent à des $\mathbb{R}[X]$-modules isomorphes.
Réciproquement, si (ii) est vérifié, alors le $\mathbb{R}[X]$-module correspondant est isomorphe à une somme de modules $\mathbb{R}[X]/(P(X))$ où $P(X)$ est irréductible dans $\mathbb{R}[X]$. Donc ce module est semi-simple et (i) est vérifié.