Université Paris 7
U.F.R. de Mathématiques

26 mai 2002

B. Keller, M.-F. Vignéras

Maîtrise de Mathématiques : MT401S Algèbre

Un corrigé de l'examen de Septembre 2002

Exercice I

Déterminer la décomposition en groupes abéliens indécomposables et les facteurs invariants de

$$M = \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/48\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Réponse — Par le lemme chinois, nous avons les décompositions en groupes abéliens indécomposables

$$\begin{array}{rcl} \mathbb{Z}/18\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z} \\ \mathbb{Z}/48\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/2^4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ \mathbb{Z}/24\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/2^2\mathbb{Z}. \end{array}$$

Nous obtenons la décomposition en groupes abéliens indécomposables comme la somme des groupes à droite

$$M \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/2^4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z}.$$

En regroupant les facteurs et en utilisant à nouveau le lemme chinois nous obtenons la décomposition (dite de Smith)

$$M \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/144\mathbb{Z}.$$

Nous y lisons les facteurs invariants : $2, 12, 24, 144$.

Exercice II

Soit $P(X) = X^5 + 30X^2 - 6X + 18$. On considère les anneaux quotients

$$A = \mathbf{Q}[\mathbf{X}]/\mathbf{Q}[\mathbf{X}]\mathbf{P}(\mathbf{X}),\ \mathbf{B} = \mathbf{Q}[\mathbf{X}]/\mathbf{Q}[\mathbf{X}]\mathbf{P}(\mathbf{X^2}),\ \mathbf{C} = \mathbf{Q}[\mathbf{X}]/\mathbf{Q}[\mathbf{X}]\mathbf{P}(\mathbf{X}+\mathbf{1}).$$

1.a Est-ce que A est un corps ? Même question pour B et pour C.

Réponse — Le polynôme $P(X)$ est irréductible sur $\mathbb{Z}$ (Eisenstein avec $p = 2$). En outre, il est à coefficients entiers, de degré > 0 et de contenu 1. Donc il est irréductible sur $\mathbb{Q}$. Comme $\mathbb{Q}$ est un corps, $P(X)$ engendre un idéal maximal de $\mathbb{Q}[X]$ et A est un corps.

Le même argument montre que B est un corps.

Soit $f : \mathbb{Q}[X] \to \mathbb{Q}[X]$ l'unique morphisme de $\mathbb{Q}$-algèbres qui envoie X sur $X + 1$ et $g : \mathbb{Q}[X] \to \mathbb{Q}[X]$ l'unique morphisme de $\mathbb{Q}$-algèbres qui envoie X sur $X - 1$. Alors clairement f et g sont des isomorphismes inverses l'un de l'autre et ils induisent des isomorphismes entre A et C. Donc C est un corps.

1.b Est-ce que les anneaux A, B sont isomorphes ? Même question pour B, C et pour A, C.

Réponse — Si A et B étaient isomorphes en tant qu'anneaux, ils le seraient en tant que $\mathbb{Q}$-algèbres. En particulier, ils auraient la même dimension sur $\mathbb{Q}$. Or A est de dimension 5 *et B de dimension* 10. *Nous avons déjà vu que A et C étaient isomorphes.*

On considère maintenant les anneaux quotients analogues à A, B, C obtenus en remplacant $\mathbf{Q}$ par $\mathbf{Z}$

$$A' = \mathbf{Z}[\mathbf{X}]/\mathbf{Z}[\mathbf{X}]\mathbf{P}(\mathbf{X}),\ \mathbf{B}' = \mathbf{Z}[\mathbf{X}]/\mathbf{Z}[\mathbf{X}]\mathbf{P}(\mathbf{X^2}),\ \mathbf{C}' = \mathbf{Z}[\mathbf{X}]/\mathbf{Z}[\mathbf{X}]\mathbf{P}(\mathbf{X}+\mathbf{1}).$$

1.a’ Même question que 1.a pour A', B', C' au lieu de A, B, C.
Réponse — Nous avons des isomorphismes d’anneaux

$$(\mathbb{Z}[X]/(P(X)))/(\pi(2)) \xrightarrow{\sim} \mathbb{Z}[X]/(P(X), 2) \xrightarrow{\sim} ((\mathbb{Z}/2\mathbb{Z})[X]/(\pi(P(X)) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})[X]/(X^5)\ ,$$

où nous désignons par π les projections canoniques. Il s’ensuit que l’image de 2 engendre un idéal non trivial de A'. Donc A' n’est pas un corps. De même l’image de 2 engendre un idéal non trivial de B' et B' n’est pas un corps. Les anneaux A' et C' sont isomorphes (l’isomorhisme est induit par l’unique morphisme de $\mathbb{Z}[X]$-algèbres qui envoie X sur $X + 1$). Donc C' n’est pas un corps non plus.

1.b’ Même question que 1.b pour A', B', C' au lieu de A, B, C.
Réponse — Nous avons $A'/(2) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})[X]/(X^5)$ et $B'/(2) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})[X]/(X^{10})$. Ces deux quotients sont des espaces vectoriels sur $\mathbb{Z}/2\mathbb{Z}$ de dimensions différentes. Donc A' et B' ne sont pas isomorphes. Nous avons déjà vu que A' et C' étaient isomorphes.

Exercice III

Le but de l’exercice est de décrire les corps contenus dans le 28-ième corps cyclotomique.

1.a Quel est le nombre de sous-groupes du groupe $\mathbb{Z}/6\mathbb{Z}$?
Réponse — Il y a quatre sous-groupes, engendrés par les 4 diviseurs positifs de 6, à savoir $1, 2, 3, 6$. Les sous-groupes forment un treillis dont voici le diagramme (dit de Hasse) :

$$\begin{tikzcd}
& \mathbb{Z}/6\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}/2\mathbb{Z} \arrow[dr, dash] & & \mathbb{Z}/3\mathbb{Z} \arrow[dl, dash] \\
& 0 &
\end{tikzcd}$$

1.b Faire la liste de tous les sous-groupes H du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
Réponse — Par le lemme chinois, ce groupe est isomorphe à $(\mathbb{Z}/2 \oplus \mathbb{Z}/2) \oplus \mathbb{Z}/3$. Par cet isomorphisme, les sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ s’identifient aux produits de sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par des sous-groupes de $\mathbb{Z}/3\mathbb{Z}$ (car ils se décomposent en leurs composantes 2-primaires et 3-primaires). Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ et ses sous-groupes ne sont autres que ses sous-espaces vectoriels. Il y en a un de dimension 0, trois de dimension 1 et un de dimension 2. Il y en a donc 5 au total. Ils forment un treillis dont voici le diagramme de Hasse :

$$\begin{tikzcd}
& \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Z}/2\mathbb{Z} \arrow[dr, dash] & \mathbb{Z}/2\mathbb{Z} \arrow[d, dash] & \mathbb{Z}/2\mathbb{Z} \arrow[dl, dash] \\
& 0 &
\end{tikzcd}$$

Il y a exactement deux sous-groupes de $\mathbb{Z}/3\mathbb{Z}$. Le groupe $\mathbb{Z}/2 \times \mathbb{Z}/6\mathbb{Z}$ admet donc 10 sous-groupes. Il y a les sous-groupes produits

$$0 \times 0\ ,\ 0 \times (2)\ ,\ 0 \times (3)\ ,\ 0 \times (1)\ ,\ (1) \times 0\ ,\ (1) \times (2)\ ,\ (1) \times (3)\ ,\ (1) \times (1)\ ,$$

et les sous-groupes

$$\{(x, y) \mid x = y \mod 2 \ \ \textit{et}\ y = 0 \mod 3\} \ \textit{et}\ \{(x, y) \mid x = y \mod 2\}.$$

Le treillis des sous-groupes de $\mathbb{Z}/2 \times \mathbb{Z}/6\mathbb{Z}$ est le produit du treillis des sous-groupes de $\mathbb{Z}/2 \times \mathbb{Z}/2$ par celui des sous-groupes de $\mathbb{Z}/3\mathbb{Z}$. D'où le diagramme de Hasse

1.c Pour chaque sous-groupe H de $\mathbf{Z/2Z} \times \mathbf{Z/6Z}$, déterminer la structure du groupe quotient G/H.
Réponse — Voici la liste des quotients

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z}\ ,\ \mathbb{Z}/6\mathbb{Z}\ ,\ \mathbb{Z}/3\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z}\ ,\ 0$$

et

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ et } \mathbb{Z}/2\mathbb{Z}.$$

2 Soit $F = \mathbf{Q}(\mathbf{e^{2i\pi/7}})$ le 7-ième corps cyclotomique.

2.a Quel est le groupe de Galois $\mathrm{Gal}(F/\mathbf{Q})$?
Réponse — D'après un théorème du cours, ce groupe s'identifie au groupe des automorphismes du groupe des racines septièmes de l'unité, qu'on identifie à $\mathbb{Z}/7\mathbb{Z}$ par le choix du générateur canonique $e^{2i\pi/7}$. Le groupe de Galois s'identifie donc à $(\mathbb{Z}/7\mathbb{Z})^*$, qui est isomorphe (par le choix d'un générateur, par exemple la classe de 2) à $\mathbb{Z}/6\mathbb{Z}$.

2.b Trouver un nombre réel non rationnel α dans F, et un élément β de F tel que $\mathbf{Q}(\beta)$ soit une extension quadratique de $\mathbf{Q}$.
Réponse — Posons $\zeta = e^{2i\pi/7}$. Considérons

$$\alpha = \zeta + \zeta^{-1}.$$

Comme $\zeta^{-1} = \overline{\zeta}$, le nombre α est réel. S'il était rationnel, alors ζ serait solution de $X^2 - 2\alpha X + 1 = 0$ et $\mathbb{Q}(\zeta)$ serait une extension de degré ≤ 2 de $\mathbb{Q}$. Contradiction car $\mathbb{Q}(\zeta)$ est de degré 6 (le cardinal du groupe de Galois) sur $\mathbb{Q}$.

Considérons $\beta = \zeta^4 + \zeta^{4^2} + \zeta^{4^3} = \zeta^4 + \zeta^2 + \zeta$. Nous avons

$$\beta^2 = \beta + 2(\zeta^3 + \zeta^5 + \zeta^6) = \beta + 2(-1 - \beta)$$

et donc

$$\beta^2 + \beta + 2 = 0 \text{ et } \beta = \frac{-1 \pm \sqrt{-7}}{2}.$$

Donc $\mathbb{Q}(\beta)$ est bien une extension quadratique de $\mathbb{Q}$.

2.c Montrer que F a 4 sous-corps distincts: $\mathbf{Q}$, $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$, F, et que $\mathbf{Q}(\alpha)$ est une extension galoisienne cubique de $\mathbf{Q}$ (de degré 3).

Réponse — Par le théorème de Galois, les sous-corps de F sont en bijection avec les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$. On a vu dans 1.a qu'il y en a quatre : $(0), (2), (3), (1)$. Ils sont engendrés respectivement par

$$\zeta \mapsto \zeta\ ,\ \zeta \mapsto \zeta^4\ ,\ \zeta \mapsto \zeta^6\ ,\ \zeta \mapsto \zeta^2.$$

Le sous-groupe (0) correspond à F et le sous-groupe (1) à $\mathbb{Q}$. Les éléments de $\mathbb{Q}(\beta)$ sont fixés par (3). Comme le degré de $\mathbb{Q}(\beta)$ est égal à l'indice de (3), le sous-corps $\mathbb{Q}(\beta)$ est le corps des points fixes par (3).

Le corps F est de degré ≤ 2 sur $\mathbb{Q}(\alpha)$. Comme F est distinct de $\mathbb{Q}(\alpha)$ (il n'est pas réel), F est de degré exactement 2 sur $\mathbb{Q}(\alpha)$. Donc $\mathbb{Q}(\alpha)$ est de degré 3 sur $\mathbb{Q}$. En outre il est fixé par (3). Comme (2) est d'indice 3 dans le groupe de Galois, le sous-corps $\mathbb{Q}(\alpha)$ doit correspondre à (2). Comme le groupe de Galois est commutatif, tous ses sous-groupes sont distingués et toutes les extensions intermédiaires sont galoisiennes.

3 Soit $L = \mathbf{Q}(\mathbf{e^{2i\pi/28}})$ le 28-ième corps cyclotomique.

3.a Quel est le groupe de Galois $\mathrm{Gal}(L/\mathbf{Q})$?

Réponse — Comme dans 2.a, ce groupe est isomorphe à

$$(\mathbb{Z}/28\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6Z.$$

3.b Trouver trois éléments x_1, x_2, x_3 de L tels que les corps $\mathbf{Q(x_1)}, \mathbf{Q(x_2)}, \mathbf{Q(x_3)}$ soient distincts deux-à-deux, et quadratiques sur $\mathbf{Q}$.

Réponse — Le corps L contient les nombres $x_1 = i$ (car il contient les racines quatrièmes de l'unité) et $x_2 = i\sqrt{7}$ (d'après 2 b puisqu'il contient les racines 7-ièmes de l'unité). Donc il contient aussi $x_3 = \sqrt{7}$. Le nombre 7 n'est pas un carré dans $\mathbb{Z}[i]$ (il y est irréductible). Comme $\mathbb{Z}[i]$ est factoriel, le nombre 7 n'est pas non plus un carré dans son corps des fractions $\mathbb{Q}[i]$. Donc $\mathbb{Q}[i]$ et $\mathbb{Q}[i\sqrt{7}]$ sont différents. Ces corps sont clairment différents de $\mathbb{Q}[\sqrt{7}]$, qui est réel. Clairement les trois corps sont quadratiques sur $\mathbb{Q}$.

3.c Décrire tous les corps L' contenus dans L, ainsi que les groupes de Galois $\mathrm{Gal}(L/L')$ et $\mathrm{Gal}(L'/\mathbf{Q})$.

Réponse — Dans 3b, nous avons construit trois extensions quadratiques distinctes contenues dans L. Ils correspondent aux trois sous-groupes d'indice 2 de $Gal(L/\mathbb{Q})$. Appelons H_1, H_2, H_3 ces trois sous-groupes. D'après 2b, nous avons également l'extension cubique $\mathbb{Q}(\alpha)$ contenue dans L. Elle correspond à l'unique sous-groupe d'indice 3 de $Gal(L/\mathbb{Q})$. Appelons H_0 ce sous-groupe et posons $x_0 = \alpha$. Comme le montre le diagramme de Hasse obtenu dans 1 b, tout sous-groupe de $Gal(L/\mathbb{Q})$ est obtenu comme intersection de certains groupes H_p, $0 \leq p \leq 3$. Il s'ensuit que l'extension intermédiare correspondante est obtenue comme engendrement de certains des 4 extensions intermédiaires $\mathbb{Q}(x_p)$. Nous obtenons la liste suivante

sous-groupe	*extension*	*groupe de Galois*
G	$\mathbb{Q}$	e
H_0	$\mathbb{Q}(x_0)$	$\mathbb{Z}/3\mathbb{Z}$
H_p, $1 \leq p \leq 3$	$\mathbb{Q}(x_p)$	$\mathbb{Z}/2\mathbb{Z}$
$H_0 \cap H_p$, $1 \leq p \leq 3$	$\mathbb{Q}(x_0, x_p)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$H_0 \cap H_2$	$\mathbb{Q}(x_1, x_2)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
e	L	G

Exercice IV

Soit k un corps. Pour deux $k[X]$-modules L et M, on note $Hom(L, M)$ l'ensemble des applications $k[X]$-linéaires $f : L \to M$.

1.a Définir une structure d'espace vectoriel sur $Hom(L, M)$. Supposons que k est le corps des nombres complexes. Rappeler la forme des $k[X]$-modules indécomposables de type fini. Déterminer la dimension de $Hom(L, M)$ lorsque L et M sont indécomposables de type fini.

Réponse — Une application k-linéaire $f : L \to M$ appartient à $Hom(L, M)$ ssi elle vérifie

$$f(Xx) = Xf(x)$$

pour tous les $x \in L$. Ces conditions sont linéaires en f de façon que $Hom(L, M)$ est un sous-espace vectoriel de l'espace vectoriel des applications k-linéaires de L dans M.

Les $\mathbb{C}[X]$-modules indécomposables de type fini sont $\mathbb{C}[X]$ et les modules $\mathbb{C}[X]/(X-\alpha)^n$, où $\alpha \in \mathbb{C}$ et $n \geq 1$.

Fixons $\alpha \in \mathbb{C}$ et $n \geq 1$ et considérons les applications $k[X]$-linéaires de source $\mathbb{C}[X]/(X-\alpha)^n$. Soit M un $\mathbb{C}[X]$-module et $f : \mathbb{C}[X]/(X-\alpha)^n \to M$ une application $k[X]$-linéaire. Comme $\mathbb{C}[X]/(X-\alpha)^n$ est un module $(X-\alpha)$-primaire, l'image de f est $(X-\alpha)$-primaire. En particulier, f s'annule si la composante $(X-\alpha)$-primaire de M s'annule. C'est le cas si $M = \mathbb{C}[X]$ ou $M = \mathbb{C}[X]/(X-\beta)^m$ pour $\beta \neq \alpha$. Il reste à étudier le cas ou $M = \mathbb{C}[X]/(X-\alpha)^m$. Clairement on peut supposer $\alpha = 0$. Alors les applications $\mathbb{C}[X]/(X^n) \to C[X]/(X^m)$ correspondent aux éléments de $\mathbb{C}[X]/(X^m)$ annulés par X^n (en effet, la donnée de f équivaut à celle de l'image de la classe de 1). Si $n \geq m$, ce sont tous les éléments de $\mathbb{C}[X]/(X^m)$, si $n < m$, ce sont les éléments de $X^{(n-m)}\mathbb{C}[X]/(X^m)$. L'espace des applications $k[X]$-linéaires est donc de dimension égale au minimum entre m et n.

Considérons maintenant les applications $\mathbb{C}[X]$-linéaires de source $\mathbb{C}[X]$. La donnée d'une telle application $f : \mathbb{C}[X] \to M$ est équivalente à la donnée d'un élément de M (à savoir $f(1)$). Donc la dimension de l'espace des applications $\mathbb{C}[X]$-linéaires de $\mathbb{C}[X]$ dans M est égale à la dimension du k-espace vectoriel sous-jacent à M.

En résumé, nous trouvons

$$\begin{aligned}
\dim Hom(\mathbb{C}[X], \mathbb{C}[X]) &= \infty \\
\dim Hom(\mathbb{C}[X], \mathbb{C}[X]/(X-\alpha)^n) &= n \\
\dim Hom(\mathbb{C}[X]/(X-\alpha)^n, \mathbb{C}[X]) &= 0 \\
\dim Hom(\mathbb{C}[X]/(X-\alpha)^n, \mathbb{C}[X]/(X-\beta)^m) &= \begin{cases} 0 & si\ \alpha \neq \beta \\ min(n,m) & si\ \alpha = \beta \end{cases}
\end{aligned}$$

1.b Montrer que si L et M sont de torsion et de type fini, l'espace $Hom(L, M)$ est de dimension finie. Pour toute application $k[X]$-linéaire $g : M_1 \to M_2$, définir une application linéaire naturelle

$$g_* : Hom(L, M_1) \to Hom(L, M_2).$$

Montrer que si $M = M_1 \oplus M_2$, on a un isomorphisme d'espaces vectoriels

$$Hom(L, M_1 \oplus M_2) \to Hom(L, M_1) \oplus Hom(L, M_2).$$

Réponse — Si L et M sont de torsion et de type fini, alors leurs k-espaces vectoriels sous-jacents sont de dimension finie. Donc $Hom(L, M)$ est de dimension finie en tant que sous-espace de l'espace des applications k-linéaires de L dans M.

L'application g_* envoie f sur $g \circ f$.

Soient $i_p : M_p \to M_1 \oplus M_2$ les injections canoniques. Par la propriété universelle de la somme $M_1 \oplus M_2$, la donnée d'une application $k[X]$-linéaire $f : L \to M_1 \oplus M_2$ équivaut à celle de $f \circ i_1$ et $f \circ i_2$, qui sont des applications $k[X]$-linéaires quelconques de L dans M_1 resp. M_2. L'isomorphisme recherché envoie f sur le couple $(f \circ i_1, f \circ i_2)$.

Soit *une suite* exacte de $k[X]$-modules

$$0 \to L \xrightarrow{i} M \xrightarrow{p} N \to 0,$$

c'est-à-dire que i est injectif, p est surjectif et que le noyau de p est l'image de i.

2.a Montrer que la suite

$$0 \to Hom(N, L) \xrightarrow{i_*} Hom(N, M) \xrightarrow{p_*} Hom(N, N)$$

est exacte, c'est-à-dire que i_* est injectif et que son image est le noyau de p_*.

Supposons que L, M et N sont de torsion et de type fini et qu'il existe un isomorphisme $\phi : L \oplus N \to M$. On se propose de montrer qu'on peut choisir ϕ tel que $p \circ \phi$ soit la projection canonique et $\phi^{-1} \circ i$ l'injection canonique (c'est-à-dire que la suite est *scindable*).
Réponse — Soit $f : N \to L$ une application $k[X]$-linéaire. Supposons que $i_*(f) = 0$. Cela veut dire que $i \circ f = 0$. Comme i est injectif, il s'ensuit que $f = 0$. Donc i_* est bien injective.

Soit $f : N \to L$ une application $k[X]$-linéaire. Nous avons $p_*(i_*(f)) = p \circ i \circ f = 0$. Il s'ensuit que l'image de i_* est contenue dans le noyau de p_*.

Soit $f : N \to M$ une application $k[X]$-linéaire. Supposons que $p_*(f) = 0$. Cela veut dire que $p \circ f = 0$. Mais alors l'image de f est contenu dans le noyau de p, qui n'est autre que l'image de i. Si nous définissons $g : N \to L$ telle que $i(g(x)) = f(x)$ pour tous $x \in N$, alors g est $k[X]$-linéaire et $i_*(g) = f$. Donc le noyau de p_* est bien contenu dans l'image de i_*.

Supposons que L, M et N sont de torsion et de type fini et qu'il existe un isomorphisme $\phi : L \oplus N \to M$. On se propose de montrer qu'on peut choisir ϕ tel que $p \circ \phi$ soit la projection canonique et $\phi^{-1} \circ i$ l'injection canonique (c'est-à-dire que la suite est *scindable*).

2.b Montrer que l'application p_* est surjective. Indication : on pourra montrer que son image a même dimension que $Hom(N, N)$. Déduire que la suite est scindable.
Réponse — On sait que

$$\dim Im(p_*) = \dim Hom(N, M) - \dim Kerp_*$$

Par le point précédent, nous avons $Kerp_* = Imi_*$. Comme i_* est injective, elle induit un isomorphisme de $Hom(N, L)$ sur Imi_*. Nous avons donc

$$\dim Im(p_*) = \dim Hom(N, M) - \dim Hom(N, L).$$

De l'autre côté, comme M est isomorphe à $L \oplus N$, nous avons

$$Hom(N, M) \xrightarrow{\sim} Hom(N, L \oplus N) \xrightarrow{\sim} Hom(N, L) \oplus Hom(N, N).$$

Donc

$$\dim Hom(N, M) = \dim Hom(N, L) + \dim Hom(N, N).$$

Il s'ensuit que

$$\dim Imp_* = \dim Hom(N, M) - \dim Hom(N, L) = \dim Hom(N, N).$$

Donc p_* est bien surjective. En particulier, il existe une application $k[X]$-linéaire $s : N \to M$ telle que $p \circ s = Id_M$. Par un théorème du cours, il s'ensuit que la suite est scindable.

3. Soit une matrice trigonale par blocs

$$T = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$$

où A est carrée $p \times p$ et B est carrée $q \times q$. Montrer, à l'aide de **2**, que les conditions suivantes sont équivalentes

(i) Il existe une matrice inversible P telle que

$$PTP^{-1} = \begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}.$$

(ii) Il existe une matrice inversible

$$Q = \begin{bmatrix} I_p & X \\ 0 & I_q \end{bmatrix}$$

telle que

$$QTQ^{-1} = \begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}.$$

(iii) Il existe une matrice X de format $p \times q$ telle que $B = AX - XC$.

Réponse — Soient L, M et N les $k[X]$-modules associés respectivement aux matrices

$$A\,,\ \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \text{ et } C.$$

Alors $L \oplus N$ est le module associé à la matrice

$$\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}.$$

La condition (i) signifie qu'on a un isomorphisme

$$\phi : L \oplus N \to M.$$

La condition (ii) signifie qu'on peut choisir ϕ tel que $p \circ \phi$ soit la projection canonique et que $\phi^{-1} \circ i$ soit l'injection canonique. Donc la condition (ii) veut dire que la suite

$$0 \to L \to M \to N \to 0$$

est scindable. La condition (i) implique (ii) car si une suite exacte est scindable, le terme du milieu est isomorphe à la somme des deux termes aux extrémités. La condition (ii) implique (i) d'après 2 b.

Montrons que les conditions (ii) et (iii) sont équivalentes. Soit X une matrice de format $p \times q$ et

$$Q = \begin{bmatrix} I_p & X \\ 0 & I_q \end{bmatrix}.$$

Alors nous avons

$$QTQ^{-1} = \begin{bmatrix} I_p & X \\ 0 & I_q \end{bmatrix} \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \begin{bmatrix} I_p & -X \\ 0 & I_q \end{bmatrix} = \begin{bmatrix} A & B - AX + XC \\ 0 & C \end{bmatrix}.$$

Dire que $B = AX - XC$, c'est dire que la dernière matrice est égale à

$$\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}.$$

D'où l'équivalence de (ii) et (iii).