MT 401
20/05/02

Université Paris 7
U.F.R. de Mathématiques
B. Keller

Corrigé du devoir

1) La condition i) implique iii) : soit $e_1, \ldots, e_n$ la base standard de $L = A^n$ et b_i le i-ème vecteur colonne de la matrice B. On a $b_i = f_B(e_i)$, pour $i = 1, \ldots, n$. Or, f_B est un isomorphisme $L \xrightarrow{\sim} L$ et les vecteurs images d'une base par un isomorphisme forment une base. Ainsi, les $b_i = f_B(e_i)$ forment bien une base.

La condition iii) implique i) : puisque les vecteurs b_i forment une base de L, il existe une unique application A-linéaire $g : L \to L$ telle que $g(b_i) = e_i$ pour $i = 1, \ldots, n$. On a donc $g(f_B(e_i)) = e_i$ et $f_B(g(b_i)) = b_i$ pour $i = 1, \ldots, n$. Comme (e_i) est une base et (b_i) est une base, il s'ensuit que $g \circ f_B = \mathbf{1}_L$ et $f_B \circ g = \mathbf{1}_L$. Ainsi, l'homomorphisme f_B est inversible.

La condition i) est équivalente à ii) : Soit $g : L \to L$ une application A-linéaire et C la matrice dont la i-ème colonne est le vecteur $g(e_i)$. Alors on a $g(e_i) = f_C(e_i)$, pour $i = 1, \ldots, n$. Comme f_C et g sont A-linéaires et que (e_i) est une base, cela montre qu'on a $g = f_C$ et que la matrice C est la seule avec cette propriété. On voit donc que l'application

$$M_n(A) \to \mathrm{Hom}_A(A^n, A^n)\ ,\ C \mapsto f_C$$

est bijective. En outre, elle vérifie

$$f_{C+C'} = f_C + f'_C\ ,\ f_{CC'} = f_C \circ f_{C'}\ ,\ \text{ et } f_I = \mathbf{1}.$$

C'est donc un isomorphisme d'anneaux. En particulier, on voit que l'homorphisme f_B est inversible si et seulement si la matrice B possède un inverse dans $M_n(A)$. Supposons que c'est le cas et que $BC = CB = I$. Alors nous avons $\det(BC) = \det(B)\det(C) = 1$ ce qui montre que $\det(B)$ est inversible dans A. Réciproquement, supposons que $\det(B)$ est inversible dans A. Alors la matrice $C = (\det(B))\tilde{B}$ est bien à coefficients dans A et les identités $B\tilde{B} = (\det(B))I = \tilde{B}B$ montrent que C est inverse de B.

Finalement, pour voir que $\mathrm{GL}(n, A)$ est un groupe, il suffit d'observer que c'est l'ensemble des éléments inversibles de l'anneau $M_n(A)$ muni de la loi de multiplication qui provient de l'anneau.

2) a) D'après l'exercice 1), il s'agit de trouver tous les triples $(n, x, y) \in \mathbf{Z}^3$ tels que la matrice

$$C_{n,x,y} = \begin{bmatrix} 1994\,n & x \\ 1995\,n & y \end{bmatrix}$$

soit de déterminant inversible dans $\mathbf{Z}$, c'est-à-dire que $\det(C_{n,x,y}) = \pm 1$. Cela veut dire que l'une des équations de Bezout

$$1994nx - 1995ny = 1 \text{ ou } 1994nx - 1995ny = -1$$

est satisfaite. Il faut donc que $n = \pm 1$. L'ensemble des solutions est donc $S_1 \times S_2$, où

$$\begin{aligned} S_1 &= \{\begin{bmatrix} 1995 \\ 1994 \end{bmatrix}, \begin{bmatrix} -1995 \\ -1994 \end{bmatrix}\} \\ S_2 &= \{\begin{bmatrix} 1 + 1995k \\ 1 + 1994k \end{bmatrix} \mid k \in \mathbf{Z}\} \cup \{\begin{bmatrix} -1 + 1995k \\ -1 + 1994k \end{bmatrix} \mid k \in \mathbf{Z}\}. \end{aligned}$$

b) D'après l'exercice 1), le vecteur $\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ appartient à une base de A^2 ssi il existe un vecteur $\begin{bmatrix} x \\ y \end{bmatrix}$ tel que le scalaire

$$\det \begin{bmatrix} a_1 & x \\ a_2 & y \end{bmatrix} = a_1 x - a_2 y$$

soit inversible. C'est le cas ssi l'idéal $(a_1) + (a_2)$ est égal à A. Comme A est principal, on a $(a_1) + (a_2) = A$ ssi $\mathrm{PGCD}\,(a_1, a_2)$ est inversible.

3) a) Supposons qu'il existe $v_2, \ldots, v_n$ tels que $a, v_2, \ldots, v_n$ est une base. Définissons un homomorphisme $f : L \to A$ par $f(a) = 1$, $f(v_2) = 0$, $\ldots$, $f(v_n) = 0$. Nous avons

$$1 = f(a) = f(a_1e_1 + a_2e_2 + \ldots + a_ne_n) = a_1f(e_1) + a_2f(e_2) + \ldots + a_nf(e_n).$$

Donc PGCD $(a_1, \ldots, a_n)$ divise 1. Il est donc inversible.

b) Notons $c = \text{PGCD}\,(a_1, a_2)$ et supposons que

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = c \begin{bmatrix} a'_1 \\ a'_2 \end{bmatrix}$$

où PGCD (a'_1, a'_2) est inversible. Alors, d'après l'exercice 2 b), il existe une matrice inversible B'' de la forme

$$\begin{bmatrix} x & a'_1 \\ y & a'_2 \end{bmatrix}$$

Soit B' l'inverse de B''. Par construction, on a

$$B' \begin{bmatrix} a'_1 \\ a'_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ et } B' \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 0 \\ c \end{bmatrix}.$$

Il suffit donc de prendre pour B la matrice diagonale par blocs

$$B = \begin{bmatrix} B' & 0 \\ 0 & I_{n-2} \end{bmatrix},$$

où I_{n-2} est une matrice identité de taille $n-2$.

c) résulte de d) que nous allons montrer directement.

d) Nous procédons par récurrence. D'après la partie b), il existe une matrice B_1 telle que B_1a soit de la forme ${}^t[0, b_2, \ldots, b_n]$, où $b_2 = \text{PGCD}\,(a_1, a_2)$ et $b_i = a_i$ pour $i \geq 3$. En particulier, PGCD $(a_1, \ldots, a_n) = \text{PGCD}\,(b_1, \ldots, b_n)$. Notons $c = \text{PGCD}\,(a_1, \ldots, a_n)$. D'après l'hypothèse de récurrence, il existe une matrice $B'_2 \in \text{GL}(n-1, A)$ telle que

$$B'_2\ {}^t[b_2, \ldots, b_n] = {}^t[0, \ldots, 0, c].$$

Soit B_2 la matrice diagonale par blocs

$$B_2 = \begin{bmatrix} 1 & 0 \\ 0 & B'_2 \end{bmatrix}$$

et $B = B_2B_1$. Alors B est inversible dans $M_n(A)$, car B_2 et B_1 le sont, et par construction on a $Ba = ce_n$.

e) D'après la partie a), si a appartient à une base de A^n, alors PGCD $(a_1, \ldots, a_n)$ est inversible. Réciproquement, si PGCD $(a_1, \ldots, a_n)$ est inversible, alors d'après d), il existe une matrice $B \in \text{GL}(n, A)$ telle que $Ba = e_n$. On a donc $a = B^{-1}e_n$. D'après l'exercice 1), les colonnes de B^{-1} forment une base de A^n. La dernière colonne est égale à a. Donc a appartient bien à une base de A^n.

4) a) Si A est un corps, alors M est un espace vectoriel et M' un sous-espace vectoriel. Il s'agit de montrer qu'il admet un sous-espace supplémentaire. Rappelons-en la construction : soit $(e_i)_{i \in I'}$ une base de M'. D'après le théorème de la base incomplète, il existe un ensemble I qui contient I' et une base $(e_i)_{i \in I}$ de M. Soit $I'' = I \setminus I'$ et soit M'' le sous-espace de M engendré par les e_i, $i \in I''$. Il est alors clair que $M = M' \oplus M''$.

b) Supposons que M' est un facteur direct et que $M = M' \oplus M''$. Alors tout élément m de M s'écrit de façon unique sous la forme $m = m' + m''$, où $m' \in M'$ et $m'' \in M''$. On vérifie aisément que l'application définie par $p(m) = m'$ est un homomorphisme de A-modules et que $p \circ i = \mathbf{1}_{M'}$. Réciproquement, suppposons donné un homomorphisme $p : M \to M'$ tel que $p \circ i = \mathbf{1}_{M'}$. Posons $M'' = \ker p$ et montrons que $M = M' \oplus M''$. En effet, si m appartient à la fois a M' et M'', nous avons $m = i(p(m))$ et $p(m) = p(i(p(m))) = 0$. Donc $M' \cap M'' = \{0\}$; et pour tout $m \in M$, nous avons $m = i(p(m)) + (m - i(p(m)))$, où $i(p(m)) \in M'$ et $(m - i(p(m))) \in M''$.

c) Si $2\mathbf{Z} \subset \mathbf{Z}$ était un facteur direct, il existerait $p : \mathbf{Z} \to 2\mathbf{Z}$ tel que $p(n) = n$ pour tout $n \in 2\mathbf{Z}$. Supposons que $p(1) = 2k$. Alors $2k = p(2k) = 2kp(1) = 4k^2$. Donc $k = 0$ ce qui est absurde car on aurait alors $2\mathbf{Z} = p(\mathbf{Z}) = \mathbf{Z}p(1) = \{0\}$.

d) Soit I un idéal de A. Si c'est un facteur direct, il existe un homomorphisme $p : A \to I$ tel que $p(x) = x$ pour tout $x \in I$. Supposons que $p(1) = e \in I$. Alors $e = p(e) = ep(1) = e^2$. Comme A est intègre, il s'ensuit que $e = 0$ ou $e = 1$. Dans le premier cas, on a $I = \{0\}$ et dans le second $I = A$.

e) Comme $a \in M$ est non nul et que A est intègre, l'homomorphisme

$$j : A \to M\ ,\ x \mapsto xa$$

est un isomorphisme sur son image Aa. Cette dernière est donc un facteur direct ssi il existe un homomorphisme $p : A^n \to A$ tel que $pj = \mathbf{1}_A$ (d'après b). L'affirmation en découle car la donnée d'un homomorphisme $p : A^n \to A$ tel que $p(a) = 1$ est équivalente à celle des éléments $x_i = p(e_i)$ et la condition $p \circ j = \mathbf{1}_A$ se traduit par l'équation

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1.$$

f) M_1 n'est pas un facteur direct car $\mathrm{PGCD}\,(7, 21) = 7$ et pour que $\mathbf{Z}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ soit un facteur direct il faut et il suffit que $\mathrm{PGCD}\,(a_1, a_2) = 1$ d'après e).

$M_2 = \{0\}$ est bien un facteur direct.

M_3 n'est pas un facteur direct : en effet, supposons qu'il existe $p : \mathbf{Z}^2 \to M_3$ tel que $p(m) = m$ pour tout $m \in M_3$. Alors nous avons $2e_1 = p(2e_1) = 2p(e_1)$. Puisque $\mathbf{Z}^2$ est sans torsion, il s'ensuit que $e_1 = p(e_1) \in M$ ce qui n'est pas le cas.

M_4 n'est pas un facteur direct. En effet, M_4 est l'image de l'endormophisme associé à la matrice

$$N = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}.$$

Un vecteur x appartient donc à M_4 ssi le vecteur

$$M^{-1}x = \frac{1}{8}\begin{bmatrix} -1 & 3 \\ 3 & -1 \end{bmatrix} x$$

est à coordonnées entières. Ainsi, $8e_1 \in M_4$ mais $e_1 \notin M$. On conclut par l'argument invoqué pour M_3.

g) Clairement, si $L = L'$, alors L' est un facteur direct de L. Réciproquement, supposons que $L' \subset L$ est un facteur direct de L et qu'on a $L = L' \oplus L''$. Comme A est principal et que L est libre de type fini, le module L'' est libre de type fini. Comme L et L' sont de même rang, il s'ensuit que L'' est de rang nul. Donc $L' = 0$ et $L = L'$.

h) Supposons que $L' \subset L$ est un facteur direct et que $L = L' \oplus L''$. Soit $q : L \to L''$ la projection sur L'' le long de L'. Alors $x \in L$ appartient à L' ssi on a $q(x) = 0$. Supposons qu'il existe $a \in A$, $a \neq 0$, tel que $am \in L'$. Alors $q(am) = aq(m) = 0$. Comme L'' est un sous-module de L et que L est sans torsion, L'' est sans torsion. Donc $q(m) = 0$ et $m \in L'$.

Réciproquement, supposons que $L' \subset L$ est pur. Alors le module L/L' est de type fini et sans torsion. Puisque A est principal, il s'ensuit que L/L' est libre. Notons $p : L \to L/L'$ la projection canonique. Soient $x_1, \ldots, x_n \in L$ tels que $p(x_1), \ldots, p(x_n)$ forment une base de L/L'. Définissons un homomorphisme $s : L/L' \to L$ par $s(p(x_i)) = x_i$, $i = 1, \ldots, n$. Alors par construction, nous avons $p \circ s = \mathbf{1}_{L/L'}$. Montrons que $L = L' \oplus s(L/L')$. En effet, si $x \in L' \cap s(L/L')$, alors $x = s(y)$ et $0 = p((x) = p(s(y)) = y$. Donc $x = 0$. De plus, si $x \in L$, nous avons $x = (x - s(p(x)) + s(p(x))$ et $x - s(p(x)) \in L'$ car $p(x - s(p(x))) = p(x) - p(s(p(x))) = 0$. Donc L' est bien un facteur direct de L.

Il est immédiat qu'une intersection de deux sous-modules purs est un sous-module pur. Il s'ensuit qu'une intersection de deux facteurs directs est un facteur direct (sur un anneau principal !).