Contrôle 2, correction

(1) Soit $F = a_{-e}X^{-e} + \cdots + a_0 + a_1X + \cdots + a_dX^d$ un élément de B. Si F est non nul, il existe $i \leq d$ tel que $a_i \neq 0$. Notons $n \leq d$ le plus petit des i tels que $a_i \neq 0$. On a donc :

$$F = a_nX^n + \cdots + a_dX^d = X^n(a_n + a_{n+1}X + \cdots + a_dX^{d-n}) = X^nP$$

où $P = a_n + a_{n+1}X + \cdots + a_dX^{d-n}$ est un élément de $A[X]$ tel que $P(0) \neq 0$, c'est-à-dire $X \nmid P$. Montrons qu'une telle écriture est unique. Supposons que $F = X^nP = X^mQ$ avec $n, m \in \mathbb{Z}$ et $P, Q \in A[X]$ non divisibles par X. Si $n > m$, on trouve $X^{n-m}P = Q$ dans $A[X]$, ce qui n'est pas possible car $X^{n-m}P$ est divisible par X alors que Q ne l'est pas. De même, on ne peut avoir $n < m$. Il s'ensuit que $n = m$ puis $P = Q$.

Commentaire : nombreux d'entre vous considèrent que l'énoncé suppose implicitement que $a_{-e} \neq 0$ et $a_d \neq 0$. Cela n'est pas le cas ; sinon comment écrirait-on alors le polynôme de Laurent nul, dont tous les coefficients sont nuls ?

Noté sur 3 points : 1 point pour introduire le plus petit i tel que $a_i \neq 0$; 1 point pour en déduire l'écriture $F = X^nP$ demandée ; 1 point pour montrer que cette écriture est unique.

(2) Comme X est inversible dans B, pour tout $(a, n) \in A^\times \times \mathbb{Z}$ l'élément aX^n est inversible dans B, donc f est bien définie. Par ailleurs $f(aa', n + n') = (aa')X^{n+n'} = (aX^n)(a'X^{n'}) = f(a, n)f(a', n')$ donc f est un morphisme de groupes. De plus, si $aX^n = 1$ alors en regardant les degrés on voit que $n = 0$, puis $a = 1$; donc f est injectif. Il ne reste qu'à montrer que f est surjectif. Considérons un élément de $B^\times$ écrit sous la forme $F = X^nP$, et notons $G = X^mQ$ son inverse, de sorte que $X^{n+m}PQ = 1$ avec $n, m \in \mathbb{Z}$ et $P, Q \in A[X]$ non divisibles par X. Si $r := n + m > 0$, alors $X^rPQ = 1$ est une égalité dans $A[X]$ entre un polynôme divisible par X et 1 ; c'est impossible. Si $-r := n + m < 0$, alors $PQ = X^r$ est une égalité dans $A[X]$ entre un polynôme divisible par X et PQ ; c'est impossible. On déduit que $n + m = 0$ puis que $PQ = 1$ dans $A[X]$, donc P est inversible dans $A[X]$, donc égal à une constante $a \in A^\times$. On a montré que $F = aX^n = f(a, n)$.

Noté sur 3 points : 1 point pour montrer que f est bien défini et est un morphisme de groupes ; 0,5 point pour montrer que f est injectif ; 1,5 point pour montrer que f est surjectif.

(3) En utilisant le fait que $\mathbb{C}[X, Y, 1/X, 1/Y] = \mathbb{C}[X, 1/X][Y, 1/Y]$ et deux fois la question (2), on trouve un isomorphisme $\mathbb{C}^\times \times \mathbb{Z} \times \mathbb{Z} \simeq (\mathbb{C}[X, 1/X])^\times \times \mathbb{Z} \simeq \mathbb{C}[X, Y, 1/X, 1/Y]^\times$ qui envoie (a, n, m) sur aX^nY^m. Un élément de cette forme est de torsion ssi il existe $r \neq 0$ dans $\mathbb{Z}$ tel que $a^rX^{nr}Y^{mr} = 1$. En regardant les degrés en X et en Y, on voit qu'on doit avoir $nr = mr = 0$ donc $n = m = 0$, et $a^r = 1$ donc a est une racine r-ième de l'unité. Finalement le sous-groupe de torsion de $\mathbb{C}[X, Y, 1/X, 1/Y]^\times$ est l'ensemble des polynômes de Laurent constants, égaux à une racine de l'unité.

Noté sur 3 points : 1 point pour montrer que $M \simeq \mathbb{C}^\times \times \mathbb{Z} \times \mathbb{Z}$; 1 point pour donner la forme concrète d'un élément de torsion ; 1 point pour donner $T(M)$.

(4) Notons $\mathbb{U} \subset \mathbb{C}^\times$ l'ensemble des racines complexes de l'unité. On a vu que $T(M) = \mathbb{U}$ de sorte que $M/T(M) \simeq (\mathbb{C}^\times/\mathbb{U}) \times \mathbb{Z}^2$. En fait, ce groupe n'est pas libre de rang 2, suite à une coquille regrettable. Néanmoins $M/T(M)$ contient un sous-module libre de rang 2 évident qui est le sous-module engendré par X et Y. Ceux qui ont calculé les facteurs invariants de l'endomorphisme déterminé par $f(X) = X^5Y$, $f(Y) = X^{-2}Y^3$ ont regardé sa matrice dans la base $\{X, Y\}$, soit :

$$U = \begin{pmatrix} 5 & 1 \\ -2 & 3 \end{pmatrix}$$

La méthode la plus rapide pour calculer les facteurs invariants est ici de dire que le premier facteur invariant d_1 est le pgcd des coefficients de U, donc 1, et que le produit $d_1 d_2$ est égal au déterminant de U, d'où $d_2 = 5 \times 3 + 2 = 17$. La méthode par opérations lignes-colonnes aboutit en trois opérations.

Commentaire : l'énoncé correct portait sur l'anneau $\mathbb{F}_p[X, Y, 1/X, 1/Y]$, au lieu de $\mathbb{C}[X, Y, 1/X, 1/Y]$. Dans ce cas, le groupe $\mathbb{F}_p^\times$ est fini donc de torsion, et $M/T(M) \simeq \mathbb{Z}^2$ libre de rang 2, avec une base composée par (les images de) X et Y.

Noté sur 1 point.