M1 MPA : Algèbre et Arithmétique 2016–2017
Devoir maison n° 2

Justifier toutes vos réponses.

I. Donner une liste de toutes les classes d'isomorphisme de groupes abéliens d'ordre 144. Combien y en a-t-il ?

II. (a) Soit $L \subset \mathbf{Z}^m$ un $\mathbf{Z}$-sous-module engendré par $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{Z}^m$, et soit A la matrice $m \times n$ dont les colonnes sont $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Soit $P \in GL_m(\mathbf{Z})$ et $Q \in GL_n(\mathbf{Z})$ des matrices (avec coefficients dans $\mathbf{Z}$ et inverses à coefficients dans $\mathbf{Z}$) telles qu'on ait

$$P^{-1}AQ = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

avec $D = \mathrm{diag}(d_1, \ldots, d_r)$ avec tous les d_i non nuls et d_i divisant d_{i+1} pour $i = 1, \ldots, r-1$.

Montrer qu'il existe une base $\mathbf{w}_1, \ldots, \mathbf{w}_m$ de $\mathbf{Z}^m$ telle que $d_1\mathbf{w}_1, \ldots, d_r\mathbf{w}_r$ soit une base du sous-module L. (Interpreter des morceaux de l'équation $AQ = P\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$). Une telle base est dite *adaptée à* L.

(b) Soit $\mathbf{u} \in \mathbf{Z}^m$ un élément qui est *primitif* dans le sens que le pgcd de ses coefficients est 1. Montrer que $\mathbf{u}$ fait partie d'une base de $\mathbf{Z}^n$.

(c) Un élément non primitif $\mathbf{x} \in \mathbf{Z}^m$ peut-il faire partie d'une base de $\mathbf{Z}^m$?

(d) Trouver une base de $\mathbf{Z}^3$ contenant $(6, 14, 21)$.

III. (a) Donner un isomorphisme de groupes abéliens explicite de la forme

$$\varphi\colon \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z} \xrightarrow{\cong} \frac{\mathbf{Z}[i]}{(4+8i)\mathbf{Z}[i]}.$$

(b) Sous quelles conditions sur a et b le groupe abélien $\left(\dfrac{\mathbf{Z}[i]}{(a+bi)\mathbf{Z}[i]}, +, 0\right)$ est-il un groupe cyclique ?

IV. Soit E un espace vectoriel de dimension 3. Montrer que deux endomorphismes de E avec le même polynôme minimal et le même polynôme caractéristique sont semblables.

V. (a) Soit $K \subset L \subset F$ des extensions de corps et $\gamma \in F$. Peut-on trouver une relation entre $[K(\gamma) : K]$ et $[L(\gamma) : L]$? (égalité ? divisibilité ? majoration ? ...)

(b) Considérons une extension de corps $K \subset K(\alpha, \beta)$ avec $[K(\alpha) : K] = d$ et $[K(\beta) : K] = e$ et avec $\underline{\text{pgcd}(d, e) = 1}$. Quel est $[K(\alpha, \beta) : K]$?

VI. (a) Lesquels des polynômes suivants sont irréductibles sur $\mathbf{Q}$?

$$X^4 + 4, \qquad X^6 + X^3 + 1, \qquad X^5 - 2$$

Si un des polynômes est réductible dans $\mathbf{Q}[X]$, donner sa factorisation en irréductibles de $\mathbf{Q}[X]$.

(b) Quel sont les corps de rupture des facteurs irréductibles de chaque polynôme ? Combien d'automorphismes ont-ils ?

(c) Quel est le degré sur $\mathbf{Q}$ du corps de décomposition de chaque polynôme ?

VII. (a) Donner une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{3}, \sqrt{5})$.

(b) Quel est le polynôme minimal P sur $\mathbf{Q}$ de $\sqrt{3} + \sqrt{5}$?

(c) Quel est le corps de décomposition de P ?