TD n°5.

1 Modules sur un anneau principal

Exercice 1. Combien y a-t-il de groupes abéliens de cardinal n=24 à isomorphisme près ? Même question pour n=48.

Exercice 2. Soient A un anneau principal et $a, b \in A$. Quels sont les facteurs invariants de $A/(a) \times A/(b)$?

Exercice 3. Soit A un anneau intègre et noetherien. Montrer que A est principal si et seulement si tous les A-modules de type fini sans torsion sont libres.

Exercice 4. Donner une base :

a) de $\mathbb{Z}^2$ adaptée à $\{(a,b) \in \mathbb{Z}^2 : 2|a+b\}$.

b) de $\mathbb{Z}^3$ adaptée au sous-module M engendrée par $(4,-2,0), (2,-2,2), (3,0,-9)$.

Exercice 5. Soit A un anneau principal, et $(a_1, a_2, a_3) \in A^3$ tels que $\text{pgcd}(a_1, a_2, a_3) = 1$. On cherche à décrire $E = \{(x_1, x_2, x_3) \in A^3, \sum_{i=1}^3 a_i x_i = 0\}$. Pour i, j, k distincts, on note $d_k = \text{pgcd}(a_i, a_j)$.

a) Montrer que E est un sous-A-module libre de A^3 de rang 2.

b) Montrer que si i, j, k sont distinct $d_i d_j | a_k$. Soit $b_k \in A$ tel que $a_k = d_i d_j b_k$.

c) Montrer que les b_i sont premiers deux à deux.

d) Soit $F = \{(y_1, y_2, y_3) \in A^3 : \sum_{i=1}^3 b_i y_i = 0\}$. Montrer que

$$\begin{array}{ccc} F & \to & E \\ (y_1, y_2, y_3) & \mapsto & (d_1 x_1, d_2 x_2, d_3 x_3) \end{array}$$

est un isomorphisme de A-modules.

e) Décrire une base de F.

f) Déterminer l'ensemble des solutions dans $\mathbb{Z}^3$ de $5x + 7y + 35z = 0$.

Exercice 6. a) Soit $f : \mathbb{Z}^n \to \mathbb{Z}^n$ un endomorphisme de groupe abélien. Montrer que $\mathbb{Z}^n / f(M)$ est fini si et seulement si $\det(f) \neq 0$, et qu'alors $\text{Card}(\mathbb{Z}^n / f(M)) = |\det(f)|$.

b) Soit $x = a + ib \in \mathbb{Z}[i]$ avec $x \neq 0$. Montrer que $\text{Card}(\mathbb{Z}[i]/(x)) = a^2 + b^2$.

2 Extensions finies de corps

Exercice 7. Montrer que pour tout corps K, il existe une infinité de polynômes unitaires irréductibles. En déduire que tout corps algébriquement clos est infini.

Exercice 8. Une extension finie de corps K/k est dite monogène s'il existe $x \in K$ tel que $K = k(x)$.

a) Montrer que toute extension de degré premier est monogène.

b) Soient K/k une extension et P un polynôme irréductible sur k. Montrer que si le degré de P est premier au degré de K/k, alors P est irréductible sur K.

c) Soient k un corps et x un élément algébrique sur k de degré impair. Montrer que $k(x^2) = k(x)$.

Exercice 9. Déterminer le degré des extensions suivantes de $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}), \qquad \mathbb{Q}(i, \sqrt[4]{2}), \qquad \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}), \qquad \mathbb{Q}(\sqrt{2+\sqrt{2}}), \qquad \mathbb{Q}(i, \sqrt{2+\sqrt{2}}).$$

Exercice 10. Soit K une extension de k de degré 2.

a) On suppose que la caractéristique de k est différente de 2. Montrer qu'il existe $a \in k$ tel que K soit isomorphe à $k[X]/(X^2 - a)$. À quelle condition deux extensions de cette forme sont-elles isomorphes ? Décrire les automorphismes de K fixant k.

b) On suppose que k est de caractéristique 2. Montrer qu'il existe $a \in k$ tel que K soit isomorphe à $k[X]/(X^2 - a)$ ou à $KkX]/(X^2 - X - a)$. À quelle condition deux extensions de cette forme sont-elles isomorphes ? Décrire les automorphismes de K fixant k.

Exercice 11. On dit qu'un nombre algébrique x est constructible à la règle et au compas si il existe une tour d'extensions de corps

$$k_0 = \mathbb{Q} \subset k_1 \subset \cdots \subset k_n$$

avec $[k_{i+1} : k_i] = 2$ et $x \in k_n$.

a) Montrer que $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.

b) Montrer que $\cos(\frac{\pi}{9})$ n'est pas constructible à la règle et au compas.

Exercice 12. Soit L/K une extension de corps de degré 3 et soient $\alpha, \beta \in L$ tels que $L = K[\alpha] = K[\beta]$. Montrer qu'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ tel que $\beta = g \cdot \alpha = \frac{a\alpha+b}{c\alpha+d}$. Discuter l'unicité de g.

Exercice 13. Montrer que tout automorphisme de corps de $\mathbb{R}$ est l'identité (on pourra montrer qu'un tel automorphisme est nécessairement croissant).