Algèbre 1, M1 Examen final

Aucun document autorisé. Calculatrices et téléphones portables interdits.

Exercice 1. Étudier l'irréductibilité des polynômes suivants dans $A[X]$:

(a) $A = \mathbb{R}$, $f = X^4 + 2X + 2$.

(b) $A = \mathbb{F}_3$, $f = X^5 + X^2 + 1$.

(c) $A = \mathbb{F}_2$, $f = X^8 + X + 1$.

Indication. On pourra d'abord démontrer le résultat suivant : soit F un corps, et soient $P, Q \in F[X]$. Si $\alpha \in F_{alg}$ vérifie $P(\alpha) = Q(\alpha) = 0$, alors $D(\alpha) = 0$, où $D = pgcd(P, Q)$.

(d) $A = \mathbb{Q}$, $f = X^8 + X + 1$.

(e) $A = \mathbb{Q}$, $f = X^{p^m} + p - 1, p$ premier, $m \geq 1$.

Exercice 2. Soit p un nombre premier.

1. Pour tous $d, n \geq 1$, montrer que $p^d - 1 \mid p^n - 1 \iff d \mid n$.

Indications. On pourra calculer dans $\mathbb{Z}/(p^d - 1)\mathbb{Z}$.

2. Soit $n \geq 1$ un entier. Soit $f \in \mathbb{F}_p[X]$ un polynôme irréductible unitaire de degré $d, d \mid n$. En considérant l'extension de $\mathbb{F}_p$ engendrée par une racine de f dans une clôture algébrique de $\mathbb{F}_p$, montrer que $f \mid X^{p^d} - X$, puis que $f \mid X^{p^n} - X$.

3. Soit $f \in \mathbb{F}_p[X]$ un diviseur unitaire irréductible de degré d de $X^{p^n} - X$. Soit α une racine de f dans une clôture algébrique de $\mathbb{F}_p$. Montrer que $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$. En déduire soigneusement que $p^d - 1 \mid p^n - 1$, puis que $d \mid n$.

4. En déduire que $X^{p^n} - X$ est le produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré divisant n. On admettra que $X^{p^n} - X$ est sans facteurs carrés.

Exercice 3. Soit A un anneau euclidien.

1. Énoncer le théorème de la base adaptée.

Soit $C \in \mathrm{M}_{m \times n}(A)$ de rang r (vue comme matrice de $\mathrm{M}_{m \times n}(K_A)$). On pose

$$\mathcal{N}(C) = \{v \in A^n \mid Cv = 0\}.$$

C'est un sous-module de A^n.

2. Montrer que $\mathcal{N}(C)$ contient une famille de $n - r$ éléments K_A-linéairement indépendants. Donner un exemple simple de matrice C où une telle famille n'est pas une base de $\mathcal{N}(C)$.

3. Montrer qu'une A-base de $\mathcal{N}(C)$ est donnée par les $n - r$ premiers éléments d'une base de A^n adaptée au sous-module N engendré par une famille de $n - r$ éléments de $\mathcal{N}(C)$ K_A-linéairement indépendants.

Indications : On pourra que montrer si $a{\cdot}x \in N$, alors $x \in \mathcal{N}(C)$. De plus, si $(e_1, \dots, e_n)$ est une base adaptée à N, on pourra montrer par l'absurde que
$$\mathcal{N}(C) \cap \langle e_{n-r+1}, \dots, e_n \rangle = 0.$$

4. Application : trouver une base de solutions du système d'équations
$$\left\{ \begin{array}{rcl} 2x + 3y + 5z + 7t & = & 0 \\ -2x - y - z + t & = & 0 \end{array} \right. \quad x, y, z, \in \mathbb{Z}.$$

Exercice 4. Soit A un anneau. On dit qu'un A-module M est **indécomposable** s'il est non nul et si pour tous sous-modules P et Q de M, on a
$$M = P \oplus Q \Rightarrow P = 0 \ \text{ ou } Q = 0.$$

Si B est un anneau, on rappelle que $e \in B$ est un **idempotent** si $e^2 = e$.

On suppose A commutatif.

1. Montrer que M est indécomposable si et seulement si le morphisme nul et Id_M sont les seuls idempotents de l'anneau $\mathrm{End}_A(M)$.

On pourra d'abord vérifier rapidement que si $f \circ f = f$, alors
$$M = \ker(f) \oplus \mathrm{Im}(f).$$

2. Vérifier que l'on a un isomorphisme d'anneaux $\mathrm{End}_A(A) \simeq A$. En déduire que A est un A-module indécomposable si et seulement les seuls idempotents de A sont 0 et 1.

3. Soit $\pi \in A$ un élément irréductible, et soit $n \geq 1$. Montrer que tout élément de $\mathrm{End}_A(A/(\pi^n))$ est de la forme
$$\ell_a : A/(\pi^n) \longrightarrow A/(\pi^n), \overline{x} \longmapsto \overline{ax},$$
puis que l'on a un isomorphisme d'anneaux $\mathrm{End}_A(A/(\pi^n)) \simeq A/(\pi^n)$.

4. En déduire que si A est factoriel, $A/(\pi^n)$ est indécomposable.

5. Soit A un anneau euclidien. Montrer que les A-modules indécomposables de type fini sont, à isomorphisme près, A et les A-modules $A/(\pi^n)$, où π est irréductible et $n \geq 1$.

6. Soit $A = \mathbb{Z}[i\sqrt{6}]$. Montrer que $\pi = i\sqrt{6}$ est irréductible dans A, mais que $A/(\pi)$ n'est pas indécomposable (on pourra considérer $\overline{3}$).