

Exercice 77 (Quotient et polynômes).

Soient A un anneau commutatif unitaire, I et J deux idéaux de A et $\phi : A \rightarrow A/I$ la surjection canonique.

- (1) Montrer que $(A/I)/\phi(J)$ est isomorphe à $A/(I+J)$.
- (2) Montrer que si p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})[X]$ est isomorphe à $(\mathbb{Z}[X])/(p)$.
- (3) Dédire des questions précédentes que

$$\mathbb{Z}[i]/(p) \text{ est isomorphe à } (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1).$$

Exercice 78. Le but de cet exercice est de montrer le résultat suivant :

Théorème (des deux carrés). *Un nombre premier $p \in \mathbb{Z}$ s'écrit comme la somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.*

Soit donc p un nombre premier

- (1) (a) Montrer que le polynôme $X^2 + 1$ est réductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.
Prenons maintenant p impair.
- (b) Montrer que $X^2 + 1$ est réductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ si et seulement si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
- (c) Montrer que si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ alors $(-1)^{\frac{p-1}{2}} = 1$.
- (d) En utilisant le fait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique montrer que si $p = 4k + 1$ alors -1 est un carré.
- (e) Dédire des questions précédentes que $X^2 + 1$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ si et seulement si $p \equiv -1 \pmod{4}$.
- (2) Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv -1 \pmod{4}$. (Penser à utiliser l'exercice précédent)
- (3) Si p est réductible dans $\mathbb{Z}[i]$ montrer qu'il existe u et v dans $\mathbb{Z}[i]$ tels que $p = uv$ avec $N(u) = N(v) = p$. (ou N est la fonction définie dans l'exercice 68)
- (4) En déduire le Théorème des deux carrés.

Extension de corps, corps finis

Exercice 79.

- (1) Donner la liste des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré ≤ 4 .
- (2) En déduire que $X^7 + X + 1$ et $X^6 + X^3 + 1$ sont irréductibles sur $\mathbb{F}_2$.

Exercice 80.

- (1) Soit P un polynôme unitaire de $\mathbb{Z}[X]$. Montrer que si P est réductible dans $\mathbb{Z}[X]$ alors il est également réductible dans $\mathbb{F}_p[X]$, pour tout p premier.
- (2) Montrer que $P = X^3 + X^2 + X + 2$ est irréductible dans $\mathbb{Z}[X]$.
- (3) Soit α une racine de ce polynôme. et $\mathbb{K} = \mathbb{Q}(\alpha)$. Donner une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{K}$.
- (4) Exprimer $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ et $(\alpha^2 - 1)^{-1}$ dans cette base.

Exercice 81. Soit $P = X^3 - X + 1 \in \mathbb{F}_3[X]$, et soit $\mathbb{K} = \mathbb{F}_3[X]/(P)$. Soit $\alpha = X \bmod (P) \in \mathbb{K}$.

- (1) Montrer que $\mathbb{K}$ est un corps. Quelle est sa caractéristique ?
- (2) Donner une base de $\mathbb{K}$ en tant qu'espace vectoriel. Quel est le cardinal de $\mathbb{K}$?
- (3) Montrer que α est d'ordre 26 dans $\mathbb{K}^\times$. En déduire que $\mathbb{K}^\times$ est cyclique.

Exercice 82. Soit $P = 1 + X + X^2 + X^3 + X^4 \in \mathbb{F}_2[X]$.

- (1) Montrer que $\mathbb{K} = \mathbb{F}_2[X]/(P)$ est un corps. Quel est son cardinal ?
- (2) Montrer que l'élément $\alpha = X \bmod (P)$ n'engendre pas $\mathbb{K}^\times$.
- (3) Trouver un générateur de $\mathbb{K}^\times$.

Exercice 83. On se place dans le corps $\mathbb{Q}$.

- (1) Donner les polynômes minimaux de $\sqrt{2}$ et $\sqrt{3}$ dans $\mathbb{Q}[X]$.
- (2) Déterminer le polynôme minimal de $\sqrt{2} \times \sqrt{3}$.
- (3) Montrer que $P = X^4 - 10X^2 + 1$ est tel que $P(\sqrt{2} + \sqrt{3}) = 0$.
- (4) Montrer que P est irréductible sur $\mathbb{Q}$.
- (5) Donner le degré de l'extension $[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}]$.
- (6) Donner une base du corps $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ en tant que $\mathbb{Q}$ -espace vectoriel.

Exercice 84 (sous-corps, extensions).

- (1) Si K et L sont des corps, montrer qu'un morphisme d'anneau unitaire de K dans L est nécessairement injectif.
- (2) Montrer que si L est de caractéristique p alors il existe un sous-corps de L qui est isomorphe au corps $\mathbb{F}_p$.
- (3) Montrer que $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$. (tout sous-corps de $\mathbb{C}$ contient $\mathbb{Q}$.)
- (4) Montrer que tout corps de caractéristique nulle est une extension de $\mathbb{Q}$.

Exercice 85. Soit $P = 8X^3 - 6X - 1$. On veut montrer que P est irréductible dans $\mathbb{Q}[X]$.

- (1) Montrer que si P est réductible alors il a une racine dans $\mathbb{Q}$. (degré)
- (2) Montrer que l'équation $8a^3 - 6ab^2 = b^3$ n'a pas de solution entière non triviale. (On pourra supposer que $a \wedge b = 1$)
- (3) En déduire que le polynôme est irréductible.

Exercice 86 (Théorème de Liouville et nombres transcendants).

- (1) Soit P un polynôme de $\mathbb{Q}[X]$ irréductible de degré $d \geq 2$. Montrer qu'il existe $k \in \mathbb{N}$ tel que pour tout rationnel $\frac{p}{q}$, on ait $\left| P\left(\frac{p}{q}\right) \right| \geq \frac{1}{kq^d}$.
- (2) Soit α un nombre algébrique de degré $d \geq 2$ et P_α son polynôme minimal. Montrer que P_α est irréductible de degré d .
- (3) En utilisant le théorème des accroissements finis (oui oui), montrer qu'il existe $A > 0$ tel que $\left| \alpha - \frac{p}{q} \right| \geq \frac{A}{q^d}$.

- (4) On considère le nombre réel suivant : $\beta = \sum_{k=0}^{+\infty} \frac{1}{10^{k!}}$

Montrer que β est transcendant. (Penser à vérifier que β est irrationnel avant d'utiliser la question précédente)