UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen — Première session

Durée : 2h
Les notes de cours et de TD sont autorisées. Les calculatrices et les téléphones sont interdits.

Exercice 1

Soit p un nombre premier impair.

1. Montrer que $\mathbb{F}_{p^2}^\times$ contient un élément α d'ordre exactement 8.
2. Soit $Q \in \mathbb{F}_p[X]$ le polynôme minimal de α sur $\mathbb{F}_p$. Montrer que Q est de degré 1 ou 2. (Indication : on pourra considérer le degré de l'extension $\mathbb{F}_p(\alpha)/\mathbb{F}_p$).
3. En déduire que le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.
4. Quelle est la décomposition en produit d'irréductibles de $X^4 + 1$ dans $\mathbb{F}_2[X]$?
5. Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 2

Soit p un nombre premier qui s'écrit comme somme de deux carrés. Combien y a-t-il de couples $(x, y) \in \mathbb{Z}^2$ tels que $p = x^2 + y^2$? (On pourra être amené à distinguer le cas $p = 2$. Indication : chercher les diviseurs de p dans $\mathbb{Z}[\sqrt{-1}]$.)

Exercice 3

Soit $P(X) = X^3 + X + 1 \in \mathbb{Q}[X]$.

1. Montrer que P est irréductible dans $\mathbb{Q}[X]$.
2. Soit $K = \mathbb{Q}[X]/(P)$. Notons $\alpha \in K$ la classe de X. Calculer la trace $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^m)$ pour $m \in \{0, 1, 2, 3, 4\}$.
3. Déterminer une $\mathbb{Z}$-base de l'anneau $\mathcal{O}_K$ des entiers de K.
4. En déduire que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Exercice 4

Quelles sont les unités de l'anneau des entiers de $\mathbb{Q}(\sqrt{51})$? (Le détail des calculs doit être inclus dans la réponse).

Exercice 5

Soit K un corps de nombres. On note $\mathscr{O}_K$ l'anneau des entiers de K.

1. Soit $a \in \mathscr{O}_K \setminus \{0\}$. Montrer que $|\mathrm{N}_{K/\mathbb{Q}}(a)| = \mathrm{Card}(\mathscr{O}_K/(a))$.
2. Si I est un idéal non nul de $\mathscr{O}_K$, on définit $\mathrm{N}(I) \overset{\text{déf}}{=} \mathrm{Card}(\mathscr{O}_K/I)$. Montrer que $\mathrm{N}(I)$ est fini. (Indication : on pourra fixer un $a \in I \setminus \{0\}$ et comparer $\mathrm{N}(I)$ et $\mathrm{N}((a))$).
3. Montrer que $\mathrm{N}(I) \in I$.
4. Montrer que si $\mathfrak{p}$ un idéal premier non nul de $\mathscr{O}_K$, alors $\mathscr{O}_K/\mathfrak{p}$ est un corps fini.
5. On suppose désormais que $\mathscr{O}_K$ est factoriel. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathscr{O}_K$. Soit $\mathrm{N}(\mathfrak{p}) = \pi_1 \cdots \pi_m$ la factorisation de $\mathrm{N}(\mathfrak{p})$ dans $\mathscr{O}_K$, avec $\pi_1, \dots, \pi_m$ des irréductibles de $\mathscr{O}_K$ (pas forcément distincts). Montrer qu'il existe un $i \in \{1, \dots, m\}$ tel que $\pi_i \in \mathfrak{p}$.
6. Montrer que $\mathscr{O}_K/(\pi_i)$ est un corps fini.
7. Montrer que $\mathfrak{p} = (\pi_i)$. (Indication : quels sont les idéaux de $\mathscr{O}_K/(\pi_i)$?)
8. On admet que tout idéal I non nul de $\mathscr{O}_K$ s'écrit comme un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ d'idéaux premiers non nuls (pas nécessairement distincts). Montrer que l'anneau $\mathscr{O}_K$ est principal.