Théorie des nombres

Examen terminal
Durée 2h. Documents et calculatrice autorisés.
Toutes les réponses doivent être justifiées.

Exercice 1. (4 points environ)

a. 11 est-il un carré dans $\mathbb{Z}/157\mathbb{Z}$?

b. 22 est-il un carré dans $\mathbb{Z}/155\mathbb{Z}$?

c. 7 est-il un carré dans le corps fini $\mathbb{F}_{13^3}$?

d. 11 est-il un cube dans le corps fini $\mathbb{F}_{13^3}$?

Exercice 2. (5 points environ)

Soit p un nombre premier impair.

a. Montrer que $\mathbb{F}_{p^2}^{\times}$ contient un élément α d'ordre exactement 8.

b. 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 $\mathbb{F}_p(\alpha)/\mathbb{F}_p$).

c. En déduire que le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.

d. Quelle est la décomposition en produit d'irréductibles de $X^4 + 1$ dans $\mathbb{F}_2[X]$?

e. Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 3. (4 points environ)

Soit $P(X) = X^3 + X^2 + 3$, $K = \mathbb{Q}[X]/(P)$, et α l'image de X dans K.

a. Montrer que K est un corps.

b. Déterminer les traces suivantes

$$tr_{K|\mathbb{Q}}(1), tr_{K|\mathbb{Q}}(\alpha), tr_{K|\mathbb{Q}}(\alpha^2), tr_{K|\mathbb{Q}}(\alpha^3), tr_{K|\mathbb{Q}}(\alpha^4)$$

c. Déterminer le discriminant de la $\mathbb{Q}$-base $1, \alpha, \alpha^2$ de K

d. Monter que $O_K = \mathbb{Z}[\alpha]$.

Exercice 4. (8 points environ)

Soit $j = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$. On rappelle que $\mathbb{Z}[j]$ est euclidien, et que ses éléments inversibles sont $\pm 1, \pm j, \pm j^2$.

a. Déterminer la norme $N(z)$ de $z = x + yj$ pour $x, y \in \mathbb{Z}$.

b. Soit $p \in \mathbb{N}$ un nombre premier. Montrer que s'il existe $z \in \mathbb{Z}[j]$ tel que $p = N(z)$, alors $p \neq 2$ et -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

c. Déterminer les nombres premiers p tels que -3 soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.

d. Déterminer le covolume de $\mathbb{Z}[j]$ dans $\mathbb{C}$ (où $\mathbb{C}$ est muni de sa structure euclidienne standard).

e. Soit $p > 2$ un nombre premier tel que -3 est un carré modulo p.

   (i) En introduisant un sous-réseau aproprié de $\mathbb{Z}[j]$, montrer qu'il existe $z_0 \in \mathbb{Z}[j]$ tq $N(z_0) = p$.

   (ii) En déduire que p n'est pas irréductible dans $\mathbb{Z}[j]$, et donner sa décomposition en produit d'irréductibles.

f. Soit maintenant $p \in \mathbb{N}$ un nombre premier tel que p ne soit la norme d'aucun élément de $\mathbb{Z}[j]$. Montrer que p est irréductible dans $\mathbb{Z}[j]$ (si $p = z_1 z_2$, considérer la norme).

g. Déterminer l'ensemble des éléments irréductibles de $\mathbb{Z}[j]$ (on pourra montrer que tout élément irréductible z vérifie que $N(z)$ est un nombre premier, ou que z est associé à un élément de $\mathbb{Z}$).

h. Quels sont les éléments irréductibles qui sont associés à leur conjugué, mais pas associés à un élément de $\mathbb{Z}$?