UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen terminal

Durée 2h. Documents et calculatrice autorisés. Téléphone interdit. Barème indicatif
On justifiera soigneusement chacune des réponses.

Exercice 1. 6 points environ

Soit K un corps fini de cardinal q, et p sa caractéristique.
On considère des polynômes $P_1, \dots, P_r \in K[X_1, \dots, X_n]$ en n variables, chaque P_i étant homogène de degré d_i (rappelons que par définition, cela signifie que P_i est une combinaison linéaires de monômes de la forme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ avec $\alpha_1 + \dots + \alpha_n = d_i$).
Soit

$$V = \{(x_1, \dots, x_n) \in K^n | P_1(x_1, \dots, x_n) = 0, \dots, P_r(x_1, \dots, x_n) = 0\}$$

le lieu des zéros communs de $P_1, \dots, P_r$. On suppose que $n > d_1 + d_2 + \dots + d_r$, et que les P_i sont non constants (i.e. $d_i > 0$), et on veut montrer que $V \neq \{(0, 0, \dots, 0)\}$.
On admet pour l'instant l'assertion suivante :

$$(*) \quad \text{pour tout entier } m < q-1, \ \sum_{x \in K} x^m = 0$$

(avec la convention usuelle $0^0 = 1$).

1. Soit
$$Q(X_1, \dots, X_n) = \prod_{i=1}^{r} (1 - P_i(X_1, \dots, X_n)^{q-1}).$$
Montrer que $Q(x_1, \dots, x_n) = 1$ si $(x_1, \dots, x_n) \in V$ et que $Q(x_1, \dots, x_n) = 0$ si $(x_1, \dots, x_n) \notin V$.
2. Démontrer que le cardinal de V satisfait
$$\#V.1_K = \sum_{(x_1, \dots, x_n) \in K^n} Q(x_1, \dots, x_n).$$
3. Montrer que $Q(X_1, \dots, X_n)$ est une combinaison linéaire de monômes de la forme
$$M(X_1, \dots, X_n) = X_1^{\alpha_1} \dots X_n^{\alpha_n}$$
avec $\alpha_1 + \dots + \alpha_n < n(q-1)$.
4. En utilisant l'assertion $(*)$, montrer que pour chaque monôme M comme ci-dessus,
$$\sum_{(x_1, \dots, x_n) \in K^n} M(x_1, \dots, x_n) = 0.$$
5. Démontrer que $\#V \equiv 0 \pmod{p}$ et conclure.

On veut maintenant démontrer l'assertion $(*)$.

6. Soit d un diviseur de $q-1$, et $U_d \subset K$ l'ensemble des racines d-ièmes de l'unité dans K. Déterminer le polynôme $\prod_{u \in U_d} (X - u)$.
7. En déduire que si $d \geq 2$, $\sum_{u \in U_d} u = 0$. Que se passe-t-il si $d = 1$?
8. Soit $m \in \mathbb{N}$. Montrer que $\sum_{x \in K^*} x^m$ vaut -1 si $(q-1) | m$, et vaut 0 sinon. Conclure soigneusement.

Exercice 2. 7 points environ

Soit α une racine complexe du polynôme $P(X) = X^3 - X - 2$. Soit $K = \mathbb{Q}(\alpha)$, et O_K l'anneau des entiers de K.

1. Montrer que le polynôme P est irréductible dans $\mathbb{Q}[X]$.
2. Est-ce que α est un entier algébrique ? Et $\frac{1}{\alpha}$? Déterminer le plus petit entier $n \geq 1$ tel que $\frac{n}{\alpha} \in O_K$.
3. Déterminer les traces de $1, \alpha, \alpha^2, \alpha^3, \alpha^4$, et α^{-1}.
4. Montrer que le discriminant de $\mathbb{Z}[\alpha]$ est égal à -104.

On cherche maintenant à déterminer une $\mathbb{Z}$-base de O_K.

5. Montrer que pour tout $n \in \mathbb{N}$, $n \geq 2$, $\frac{\alpha}{n}$ et $\frac{\alpha^2}{n}$ ne sont pas entiers algébriques.
6. Est-ce que $\frac{\alpha+\alpha^2}{2} \in O_K$?
7. Montrer que $\mathbb{Z}[\alpha] = O_K$.

Exercice 3. 8 points environ

On cherche à déterminer les nombres premiers p qui peuvent s'écrire $p = x^2 + xy - y^2$, avec $(x, y) \in \mathbb{Z}^2$.
On introduit $K = \mathbb{Q}(\sqrt{5})$, et O_K son anneau d'entiers. Pour $\alpha = x + y\sqrt{5} \in K$, on note $\bar{\alpha} = x - y\sqrt{5}$ le conjugué de α. Soit $\Phi : K \to \mathbb{R}^2$ le plongement défini par $\Phi(\alpha) = (\alpha, \bar{\alpha})$.
On notera $\omega = \frac{1+\sqrt{5}}{2}$.

1. Pour $x, y \in \mathbb{Z}$, calculer $N_{K|\mathbb{Q}}(x + y\omega)$. Existe-t-il un élément de norme -1 dans O_K ?
2. Pour quels nombres premiers p l'équation $t^2 + t - 1 = 0$ a-t-elle une solution dans $\mathbb{Z}/p\mathbb{Z}$? On donnera le résultat en termes de congruences de p modulo 5. On pourra si on veut, reconnaître le début d'un carré, et distinguer si nécessaire les cas $p = 2$, et $p = 5$.
3. On suppose qu'il existe $a \in \mathbb{Z}$ tel que $a^2 + a - 1 = 0 \pmod{p}$. Soit

$$L = \{x + y\omega \mid x, y \in \mathbb{Z},\ x - ay \equiv 0 \pmod{p}\} \subset O_K.$$

   Montrer que pour tout $\alpha \in L$, $N_{K|\mathbb{Q}}(\alpha) \equiv 0 \pmod{p}$.
4. Soit $f : \mathbb{R}^2 \to \mathbb{R}$ la fonction definie par $f(u, v) = uv$. Exprimer la norme de $\alpha \in O_K$ à l'aide de f et de Φ.
5. Donner une base du réseau $\Phi(O_K) \subset \mathbb{R}^2$
6. Montrer que le covolume du réseau $\Phi(L)$ dans $\mathbb{R}^2$ est égal à $\sqrt{5}$
7. Montrer qu'il existe $\alpha \in L \setminus \{0\}$, tel que $|N(\alpha)| < 2p$. On pourra pour cela considérer $C \subset \mathbb{R}^2$ le carré de sommets $(l, 0), (0, l), (-l, 0), (0, -l)$, et déterminer le maximum de la fonction f sur C. (Il n'est pas interdit de faire un dessin).
8. Conclure soigneusement.