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 le fait suivant :

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

(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 $(x_1, \dots, x_n) \notin V$.
Solution. Si $(x_1, \dots, x_n) \in V$, chaque facteur de $\prod_{i=1}^r (1 - P_i(x_1, \dots, x_n)^{q-1})$ est égal à 1, donc $Q(x_1, \dots, x_n) = 1$. Si $(x_1, \dots, x_n) \notin V$, il y a un P_i tel que $P_i(x_1, \dots, x_n) \in K^*$, donc $P_i(x_1, \dots, x_n)^{q-1}) = 1$ d'apres le theoreme de Lagrange car K^* est un groupe d'ordre $q-1$. Le facteur correspondant de $Q(x_1, \dots, x_n)$ s'annule donc, et $Q(x_1, \dots, x_n) = 0$.

2. Démontrer que le cardinal de V satisfait
$$\#V.1_K = \sum_{(x_1, \dots, x_n) \in K^n} Q(x_1, \dots, x_n).$$
Solution. Les termes non nuls de la somme $\sum_{(x_1, \dots, x_n) \in K^n} Q(x_1, \dots, x_n)$ sont ceux qui appartiennent à V, et chacun d'eux vaut $1 \in K$. Donc $\sum_{(x_1, \dots, x_n) \in K^n} Q(x_1, \dots, x_n) = \#V \pmod p$

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 $\alpha_1 + \dots + \alpha_n < n(q-1)$.
Solution. $1 - P_i^{q-1}$ est de degré $\leq d_i(q-1)$, donc Q est de degré $\leq (q-1)\sum_{i=1}^r d_i < n(q-1)$ par hypothèse.

4. En utilisant le fait admis ci-dessus, montrer que pour chaque monôme M comme ci-dessus,
$$\sum_{(x_1,\ldots,x_n)\in K^n} M(x_1,\ldots,x_n) = 0.$$

Solution. Puisque $\alpha_1 + \cdots + \alpha_n < n(q-1)$, il y a un indice i tel que $alpha_i < q-1$. Or $\sum_{(x_1,\ldots,x_n)\in K^n} M(x_1,\ldots,x_n) = (\sum_{x_1\in K} x_1^{\alpha_1})(\sum_{x_2\in K} x_2^{\alpha_2})\cdots(\sum_{x_n\in K} x_n^{\alpha_n})$. D'après la question 3, le facteur pour lequel $\alpha_i < q-1$ verifie $\sum_{x_i\in K} x_i^{\alpha_i} = 0$, donc $\sum_{(x_1,\ldots,x_n)\in K^n} M(x_1,\ldots,x_n) = 0$.

5. Démontrer que $\#V \equiv 0 \pmod p$ et conclure.
Solution. On a $\#V.1_K = \sum_{(x_1,\ldots,x_n)\in K^n} Q(x_1,\ldots,x_n) = 0$ car chacun des monômes composant Q contribue pour 0 à la somme. Donc $\#V \equiv 0 \pmod p$. Or $(0,0,\ldots,0) \in V$ puisque les polynômes P_i sont tous homogènes de de degré $d_i > 0$, V contient au moins $p-1$ autres éléments.

On veut maintenant démontrer le fait admis plus haut.

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 $\prod_{u\in U_d}(X-u)$.
Solution. $\prod_{u\in U_d}(X-u) = X^d - 1$. En effet, tous les éléments de U_d sont racines de X^d-1, donc $\prod_{u\in U_d}(X-u) | X^d-1$. Comme $d|q-1$ et que F_q^* est un groupe cyclique de cardinal $q-1$, U_d est un sous-groupe de cardinal d. Donc les deux polynômes ont même degré, et sont donc égaux puisqu'ils sont unitaires.

7. En déduire que si $d \geq 2$, $\sum_{u\in U_d} u = 0$. Que se passe-t-il si $d = 1$?
Solution. $-\sum_{u\in U_d} u$ est égal au coefficient de degré $d-1$ de $\prod_{u\in U_d}(X-u) = X^d-1$. Donc $\sum_{u\in U_d} u = 0$ si $d \geq 2$ et $\sum_{u\in U_d} u = 1$ si $d = 1$ (dans ce cas $U_d = U_1 = \{1\}$).

8. Soit $m \in \mathbb{N}$. Montrer que $\sum_{x\in K^*} x^m$ vaut -1 si $(q-1)|m$, et vaut 0 sinon. En déduire que si $0 \leq m < q-1$, $\sum_{x\in K} x^m = 0$ (avec la convention usuelle $0^0 = 1$).
Solution. Soit $\varepsilon_m : K^* \to K^*$ definie par $x \mapsto x^m$. Son image est le sous-groupe cyclique U_d avec $d = \frac{q-1}{pgcd(m,q-1)}$, et son noyau est de cardinal $pgcd(m,q-1)$. Donc lorsque x parcours K^*, x^m parcours U_d, chaque élément de U_d etant parcouru $pgcd(m,q-1)$ fois. Donc $\sum_{x\in K^*} x^m = pgcd(m,q-1)\cdot\sum_{u\in U_d} u$. Ainsi, si $q-1|m$, $\sum_{x\in K^*} x^m = (q-1) = 1$ dans K, et si $q-1 \not| m$, $d \geq 2$, et $\sum_{x\in K^*} x^m = 0$. Finalement, si $0 < m < q-1$, $\sum_{x\in K} x^m = \sum_{x\in K^*} x^m = 0$, et pour $m = 0$, $\sum_{x\in K} x^m = 1 + \sum_{x\in K^*} x^m = 1 + -1 = 0$.

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 $\mathbb{Q}[X]$.

   Solution. Puisque P est de degré 3, il suffit de montrer qu'il n'a pas de racine dans $\mathbb{Q}$. Or toute racine de P est un entier algébrique (puisque $P \in \mathbb{Z}[X]$ et unitaire), donc toute racine de P dans $\mathbb{Q}$ est en fait dans $\mathbb{Z}$. Il s'en suit qu'une telle racine r doit être un diviseur de 2, donc $r = \pm 1, \pm 2$. Or $P(1) = -2$, $P(-1) = -2$, $P(2) = 4$, et $P(-2) = -8$, donc P est irréductible.

2. Est-ce que α est un entier algébrique ? Et $1/\alpha$? Déterminer le plus petit entier $n \geq 1$ tel que $n/\alpha \in O_K$.

   Solution. α est un entier algébrique puisque racine d'un polynôme unitaire de $\mathbb{Z}[X]$. Par contre, $1/\alpha$ est annulé par le polynome $X^3P(1/X) = -2X^3 - X^2 + 1$, donc par $Q(X) = X^3 + X^2/2 - 1/2$. Or Q est le polynome minimal de $1/\alpha$. En effet, $\mathbb{Q}(\alpha)$ est une extension de degré 3 de $\mathbb{Q}$ (puisque P est irréductible), or comme $\mathbb{Q}(1/\alpha) = \mathbb{Q}(\alpha)$ le polynôme minimal de $1/\alpha$ est de degré 3 lui aussi. Puisque le polynome minimal de $1/\alpha$ n'est pas dans $\mathbb{Z}[X]$, $1/\alpha$ n'est pas entier.

3. Déterminer les traces de $1, \alpha, \alpha^2, \alpha^3, \alpha^4$, et α^{-1}.

   Solution. $tr_{K|\mathbb{Q}}(1) = 3$ car $[K : \mathbb{Q}] = 3$. Soit M la matrice de la multiplication par α dans la $\mathbb{Q}$-base $(1, \alpha, \alpha^2)$ de K.

   $$M = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ M^2 = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix},\ M^3 = \begin{pmatrix} 2 & 0 & 2 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix},\ M^4 = \begin{pmatrix} 0 & 2 & 4 \\ 2 & 1 & 4 \\ 1 & 2 & 1 \end{pmatrix}$$

   donc $tr_{K|\mathbb{Q}}(\alpha) = 0$, $tr_{K|\mathbb{Q}}(\alpha^2) = 2$, $tr_{K|\mathbb{Q}}(\alpha^3) = 6$, $tr_{K|\mathbb{Q}}(\alpha^4) = 2$. Puisque le polynome minimal de α^{-1} est $Q(X) = X^3 + X^2/2 - 1/2$, sa trace vaut $-1/2$.

4. Montrer que le discriminant de $\mathbb{Z}[\alpha]$ est égal à -104.

   Solution. Le discriminant de $\mathbb{Z}[\alpha]$ est le déterminant de la matrice donnée par les traces des puissances de α : $\det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 6 \\ 2 & 6 & 2 \end{pmatrix} = -104$.

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

5. Montrer que pour tout $n \in \mathbb{N}$, $n \geq 2$, α/n et α^2/n ne sont pas entiers algébriques.

   Solution. Le polynome minimal de α/n est de même degré que celui de α, or $X^3 - \frac{1}{n^2}X - \frac{2}{n^3}$ annule α, c'est donc son polynôme minimal, et comme il n'est pas à coefficients entiers dès que $n \geq 2$, $\alpha/n \notin O_K$. Le determinant de la matrice de a^2 étant egal a 4, $N(a^2/n) = 4/n^3$, et a^2/n n'est donc pas entier pour $n \geq 2$.

6. Est-ce que $\frac{\alpha+\alpha^2}{2} \in O_K$?

   Solution. La matrice de $\frac{\alpha+\alpha^2}{2}$ est

   $$M = \begin{pmatrix} 0 & 1 & 1 \\ \frac{1}{2} & \frac{1}{2} & \frac{3}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

   Son déterminant vaut $1/2 = N(\frac{\alpha+\alpha^2}{2})$, donc $\frac{\alpha+\alpha^2}{2} \notin O_K$.

7. Montrer que $\mathbb{Z}[\alpha] = O_K$.

Solution. Considérons la base $1, \alpha, \alpha^2$ de $\mathbb{Z}[\alpha]$. Puisque son dicriminant est $-104 = 8 * 13$, le seul nombre premier dont le carré divise 104 est $p = 2$. On sait alors que si $\mathbb{Z}[\alpha] \neq O_K$, il existe $n_1, n_2, n_3 \in \{0, 1\}$ tel que l'element $u = \frac{n_1+n_2\alpha+n_3\alpha^2}{2}$ appartienne a $O_K \setminus \mathbb{Z}[\alpha]$. Or $tru = 3/2n_1 + n_3$ doit etre entière donc $n_1 = 0$. Si n_2 ou n_3 est nul, alors $u = \alpha/2$ ou $\alpha^2/2$ dont on a vu qu'il n'étaient pas entiers. La seule possibilité restante est $u = \frac{\alpha+\alpha^2}{2}$, mais on a vu qu'il n'est pas entier. Il n'y a donc pas de u de cette forme qui appartienne a $O_K \setminus \mathbb{Z}[\alpha]$, donc $O_K = \mathbb{Z}[\alpha]$.

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 ?
   Solution. $N(x + y\omega) = (x + y\omega)(x + y\bar{\omega}) = x^2 + (\omega + \bar{\omega})xy + \omega\bar{\omega}y^2 = x^2 + xy - y^2$. ω est un élément de norme -1.

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 $p = 5$.
   Solution. Si $p = 2$, on voit que ni 0 ni 1 n'est solution de l'équation. Si $p \neq 2$, 2 est inversible dans $\mathbb{Z}/p\mathbb{Z}$, et on peut écrire $t^2 + t - 1 = (t + 1/2)^2 - 1/4 - 1 = (t + 1/2)^2 - 5/4$. L'equation a donc des solutions si et seulement si $5/4$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Puisque 4 est un carré, c'est le cas si et seulement si 5 est un carré modulo p. C'est bien sur le cas si $p = 5$. Sinon, la loi de reciprocité quadratique donne $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, donc cette équation a des solutions si et seulement si $p = 5$ ou $p \equiv \pm 1 \pmod 5$.

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 $\alpha \in L$, $N_{K|\mathbb{Q}}(\alpha) \equiv 0 \pmod p$.
   Solution. Pour $\alpha = x + y\omega \in L$, $N(\alpha) = x^2 + xy - y^2 \equiv a^2y^2 + ay^2 - y^2 = y^2(a^2 + a - 1) = 0 \pmod p$.

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.
   Solution. Puisque $N(\alpha) = \alpha\bar{\alpha}$, et que $\Phi(\alpha) = (\alpha, \bar{\alpha})$, $f(\Phi(\alpha)) = N(\alpha)$.

5. Donner une base du réseau $\Phi(O_K) \subset \mathbb{R}^2$
   Solution. Puisque O_K a pour base $1, \omega$, $\Phi(1), \Phi(\omega)$ est une base de $\Phi(O_K)$. On obtient que $\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}\omega\\\bar{\omega}\end{pmatrix}$ est une base de $\Phi(O_K)$.

6. Montrer que le covolume du réseau $\Phi(L)$ dans $\mathbb{R}^2$ est égal à $\sqrt{5}$
   Solution. Le covolume de $\Phi(O_K)$ est $|\det \begin{pmatrix}1 & \omega\\1 & \bar{\omega}\end{pmatrix}| = |\bar{\omega} - \omega| = \sqrt{5}$. Puisque $[O_K : L] = p$ et que Φ est injective, $[\Phi(O_K) : \Phi(L)] = p$ et $\Phi(L)$ est de covolume $p\sqrt{5}$.

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).

Solution. C est un convexe symétrique. C'est un carré de côté $l\sqrt{2}$. Son aire est égale à $(l\sqrt{2})^2 = 2l^2$. Si $2l^2 > 4Vol(\Phi(L) = 4p\sqrt{5}$, le theoreme de Minkowski assure que C contient un vecteur non nul $\Phi(\alpha) \in \Phi(L)$. Puisque $N(\alpha) = f(\Phi(\alpha))$, pour majorer $|N(\alpha)|$ il faut majorer $|f|$ sur C. Par symétrie de la fonction, il suffit de majorer $f(u,v)$ sur le triangle défini par $u,v \geq 0$, $u+v \leq l$. Montrons que le maximum est atteint en $(l/2, l/2)$: en effet l'inegalité arithmético-géométrique donne $\sqrt{uv} \leq \frac{u+v}{2} \leq l/2$ donc $f(u,v) = uv \leq l^2/4 = f(1/2,1/2)$ (on peut aussi dire que f n'a pas de point critique dans le triangle, et s'annule sur les deux axes de coordonnees, donc atteint son maximum sur l'hypothenuse, et on trouve le maximum en disant que la derivee de $t \mapsto f(t, l-t)$ s'annule). Ceci montre que $N(\alpha) \leq l^2/4$.

Pour que $l^2/4 < 2p$, il suffit de prendre $l^2 < 8p$. On veut simultanément que $2l^2 > 4p\sqrt{5}$ i.e. $l^2 > 2p\sqrt{5}$, ce qui est possible puisque $2\sqrt{5} < 8$.

8. Conclure soigneusement.

Solution. Montrons s'abord que si p s'ecrit sous la forme $p = x^2 + xy - y^2$, alors $p = 5$ ou $p \equiv \pm 1 \pmod 5$. Si $p|y$, alors $x^2 = 0 \pmod p$ donc $p|x$, donc $p^2|x^2 + xy - y^2$ ce qui contredit $p = x^2 + xy - y^2$. Donc y est inversible dans $\mathbb{Z}/p\mathbb{Z}$, et l'equation $x^2 + xy - y^2 = 0$ dans $\mathbb{Z}/p\mathbb{Z}$ dit que le quotient $xy^{-1} \in \mathbb{Z}/p\mathbb{Z}$ est solution de l'equation $t^2 + t - 1 = 0 \pmod p$. D'apres la question 2, $p = 5$ ou $p \equiv \pm 1 \pmod 5$.

Supposons reciproquement que $p = 5$ ou $p \equiv \pm 1 \pmod 5$, et donc que l'equation $t^2 + t - 1 = 0 \pmod p$ a une solution $a \in \mathbb{Z}$. D'apres la question precedente, il existe $\alpha \in L \setminus \{0\}$ tel que $|N(\alpha)| < 2p$. Or $N(\alpha) = 0 \pmod p$ d'apres la question 3, donc $N(\alpha) \in \{0, p, -p\}$. On ne peut pas avoir $N(\alpha) = 0$ car $\alpha \neq 0$. Si on avait $N(\alpha) = -p$, comme il existe un element $\varepsilon \in O_K$ de norme -1 d'apres la question 1, l'element $\alpha' = \varepsilon\alpha$ verifie $N(\alpha') = N(\varepsilon)N(\alpha) = p$. Ceci montre dans tous les cas que p peut s'ecrire sous la forme $p = N(\alpha)$ pour un certain $\alpha \in O_K$. Ceci conclut d'apres la question 1.