UNIVERSITÉ DE RENNES 1

Théorie des nombres

Corrigé de l'examen (2e session)

Exercice 1

Soit $z \in \mathbb{C}^\times$ un entier algébrique. Soit f son polynôme minimal (sur $\mathbb{Q}$). Montrer que $\frac{1}{z}$ est un entier algébrique si et seulement si $f(0) = \pm 1$.

Notons $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. On a alors $f(0) = a_0$. Si l'on pose

$$g(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + 1 \in \mathbb{Z}[X]$$

le polynôme obtenu en renversant l'ordre des cœfficients, alors on a

$$g\left(\frac{1}{z}\right) = z^{-n} f(z) = 0,$$

donc $\frac{1}{z}$ est racine de g.

Si $f(0) = \pm 1$, alors le polynôme $a_0 g(X)$ est unitaire à cœfficients entiers et a $\frac{1}{z}$ comme racine, donc $\frac{1}{z}$ est un entier algébrique.

Réciproquement, si $\frac{1}{z}$ est un entier algébrique, alors z est inversible dans l'anneau des entiers de $\mathbb{Q}(z)$, donc sa norme $N_{\mathbb{Q}(z)/\mathbb{Q}}(z)$ est inversible dans $\mathbb{Z}$, donc $N_{\mathbb{Q}(z)/\mathbb{Q}}(z) = \pm 1$. Comme $a_0 = (-1)^n N_{\mathbb{Q}(z)/\mathbb{Q}}(z)$, on a donc $a_0 = \pm 1$, i.e. $f(0) = \pm 1$.

Montrer que c'est aussi équivalent à $\frac{1}{z} \in \mathbb{Z}[z]$.

Comme $z^{-1} f(z) = 0$, on a

$$-a_0 z^{-1} = z^{n-1} + a_{n-1} z^{n-2} + \cdots + a_1.$$

Si z est un entier algébrique, alors $a_0 = \pm 1$ d'après la question précédente, donc

$$\frac{1}{z} = -a_0 \left(z^{n-1} + a_{n-1} z^{n-2} + \cdots + a_1\right) \in \mathbb{Z}[z].$$

Réciproquement, si $\frac{1}{z} \in \mathbb{Z}[z]$, soit $h(X) \in \mathbb{Z}[X]$ tel que $\frac{1}{z} = h(z)$. On a alors $1 - zh(z) = 0$. Notons

$$h(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0 \in \mathbb{Z}[X],$$

alors comme dans la question précédente, $\frac{1}{z}$ est racine du polynôme obtenu par renversement des cœfficients de $1 - Xh(X)$, i.e.

$$X^{m+1} - b_0 X^m - b_1 X^{m-1} - \cdots - b_m \in \mathbb{Z}[X].$$

Comme c'est un polynôme unitaire à cœfficients entiers, $\frac{1}{z}$ est donc un entier algébrique.

Exercice 2

Soit K un corps fini. Montrer que tout élément de K peut s'écrire comme la somme de deux carrés d'éléments de K.

Soit $a \in K$. Notons q le nombre d'éléments de K. Si q est pair, i.e. si K est de caractéristique 2, alors l'application $x \mapsto x^2$ est un morphisme de corps (le morphisme de Frobenius). Elle est injective car c'est un morphisme de corps, donc surjective puisque K est fini, donc il existe un $x \in K$ tel que $x^2 = a$, donc $a = x^2 + 0^2$ est somme de deux carrés.

Si q est impair, considérons les ensembles

$$\begin{aligned} A &= \left\{ x^2 \,;\, x \in K \right\} \\ B &= \{ a - y \,;\, y \in A \} \,. \end{aligned}$$

Comme l'application $y \mapsto a - y$ est une bijection de K sur lui-même (qui est son propre inverse), on a $\operatorname{Card} A = \operatorname{Card} B$. D'autre part, on a $\operatorname{Card} A = \frac{q+1}{2}$. En effet, si l'on considère le morphisme de groupes

$$\left\{ \begin{array}{ccc} K^\times & \longrightarrow & K^\times \\ x & \longmapsto & x^2, \end{array} \right.$$

son image est $A \cap K^\times = A \setminus \{0\}$, et son noyau est l'ensemble des racines du polynôme $X^2 - 1 = (X-1)(X+1)$, c'est-à-dire $\{\pm 1\}$. On en déduit donc un isomorphisme de groupes $K^\times/\{\pm 1\} \simeq A \setminus \{0\}$, donc $\operatorname{Card}(A \setminus \{0\}) = \frac{q-1}{2}$. Enfin, comme $0 = 0^2 \in A$, on a $\operatorname{Card} A = \frac{q+1}{2}$.

On a donc $\operatorname{Card} A = \operatorname{Card} B = \frac{q+1}{2}$, or

$$\operatorname{Card}(A \cup B) + \operatorname{Card}(A \cap B) = \operatorname{Card} A + \operatorname{Card} B = q + 1$$

et

$$\operatorname{Card}(A \cup B) \leqslant \operatorname{Card} K = q \qquad (\text{puisque } A \cup B \subseteq K)$$

donc $\operatorname{Card}(A \cap B) \geqslant q + 1 - q = 1$. Il existe donc un $y \in A \cap B$. Comme $y \in A$, il existe un $x \in K$ tel que $x^2 = y$. Comme $y \in B$, on a $a - y \in A$, donc il existe un $z \in K$ tel que $z^2 = a - y$. On a alors $a = x^2 + z^2$, donc a est somme de deux carrés.

Donc pour tout corps fini K et tout $a \in K$, a peut s'écrire comme somme de deux carrés dans K.

Exercice 3

Calculer le symbole de Jacobi $\left(\frac{6547}{8731}\right)$.

On a :

$$\begin{aligned}
\left(\frac{6547}{8731}\right) &= -\left(\frac{8731}{6547}\right) && \text{car } 6547 \equiv 8731 \equiv -1 \pmod 4\\
&= -\left(\frac{2184}{6547}\right) && \text{car } 8731 \equiv 2184 \pmod{6547}\\
&= -\left(\frac{2^3 \cdot 273}{6547}\right) &&\\
&= -\left(\frac{2}{6547}\right)\left(\frac{273}{6547}\right) &&\\
&= \left(\frac{273}{6547}\right) && \text{car } 6547 \equiv 3 \pmod 8\\
&= \left(\frac{6547}{273}\right) && \text{car } 273 \equiv 1 \pmod 4\\
&= \left(\frac{-5}{273}\right) && \text{car } 6547 \equiv -5 \pmod{273}\\
&= \left(\frac{-1}{273}\right)\left(\frac{5}{273}\right) &&\\
&= \left(\frac{5}{273}\right) && \text{car } 273 \equiv 1 \pmod 4\\
&= \left(\frac{273}{5}\right) && \text{car } 273 \equiv 1 \pmod 4\\
&= \left(\frac{-2}{5}\right) && \text{car } 273 \equiv -2 \pmod 5\\
&= \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) &&\\
&= -1 && \text{car } 5 \equiv 1 \pmod 4 \text{ et } 5 \equiv -3 \pmod 8.
\end{aligned}$$

Exercice 4

Soit $K = \mathbb{Q}(2^{1/3})$. Notons $\mathcal{O}_K$ l'anneau des entiers de K.

Question 1

Calculer l'image de $x + y2^{1/3} + z2^{2/3} \in K$ par l'application trace $\mathrm{Tr}_{K/\mathbb{Q}}$ et par l'application norme $\mathrm{N}_{K/\mathbb{Q}}$.

Comme $\left(1, 2^{1/3}, 2^{2/3}\right)$ est une $\mathbb{Q}$-base de K, en écrivant la matrice de la multiplication par $x + y2^{1/3} + z2^{2/3}$, on trouve :

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}\left(x + y2^{1/3} + z2^{2/3}\right) &= \mathrm{tr}\left(\begin{pmatrix} x & 2z & 2y \\ y & x & 2z \\ z & y & x \end{pmatrix}\right) \\ &= 3x\end{aligned}$$

et

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}\left(x + y2^{1/3} + z2^{2/3}\right) &= \begin{vmatrix} x & 2z & 2y \\ y & x & 2z \\ z & y & x \end{vmatrix} \\ &= x^3 + 2y^3 + 4z^3 - 6xyz.\end{aligned}$$

Question 2

Calculer le discriminant de la $\mathbb{Q}$-base $\left(1, 2^{1/3}, 2^{2/3}\right)$ de K.

On a :

$$\begin{aligned}\mathrm{disc}_{K/\mathbb{Q}}\left(1, 2^{1/3}, 2^{2/3}\right) &= \begin{vmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1) & \mathrm{Tr}_{K/\mathbb{Q}}\left(2^{1/3}\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(2^{2/3}\right) \\ \mathrm{Tr}_{K/\mathbb{Q}}\left(2^{1/3}\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(2^{2/3}\right) & \mathrm{Tr}_{K/\mathbb{Q}}(2) \\ \mathrm{Tr}_{K/\mathbb{Q}}\left(2^{2/3}\right) & \mathrm{Tr}_{K/\mathbb{Q}}(2) & \mathrm{Tr}_{K/\mathbb{Q}}\left(2 \cdot 2^{1/3}\right) \end{vmatrix} \\ &= \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{vmatrix} \qquad \text{d'après la question précédente} \\ &= -3 \cdot 6 \cdot 6 \\ &= -2^2 \cdot 3^3 \\ &= -108\end{aligned}$$

Question 3

En déduire que $\mathcal{O}_K = \mathbb{Z}\left[2^{1/3}\right]$.

Montrons d'abord que $\left(1, 2^{1/3}, 2^{2/3}\right)$ est une base du $\mathbb{Z}$-module $\mathcal{O}_K$. D'après la question précédente, on a $\operatorname{disc}_{K/\mathbb{Q}}\left(1, 2^{1/3}, 2^{2/3}\right) = -2^2 \cdot 3^3$. Il suffit donc de montrer qu'il n'y a pas d'élément de $\mathcal{O}_K \setminus \{0\}$ de la forme $\frac{1}{2}\left(x + y2^{1/3} + z2^{2/3}\right)$ avec $x, y, z \in \{0, 1\}$ ou de la forme $\frac{1}{3}\left(x + y2^{1/3} + z2^{2/3}\right)$ avec $x, y, z \in \{-1, 0, 1\}$.

Montrons qu'il n'y a pas d'élément de $\mathcal{O}_K \setminus \{0\}$ de la forme $\frac{1}{2}\left(x + y2^{1/3} + z2^{2/3}\right)$ avec $x, y, z \in \{0, 1\}$. D'après la première question, la trace d'un tel élément serait $\frac{3}{2}x \in \mathbb{Z}$, donc $x = 0$. Sa norme serait $\frac{1}{8}\left(2y^3 + 4z^3\right) \in \mathbb{Z}$, donc $y^3 + 2z^3 \equiv 0 \pmod 4$. Comme y est donc pair, on a $y = 0$, donc z est pair, donc $z = 0$, ce qui contredit la non nullité de l'élément.

Montrons qu'il n'y a pas d'élément de $\mathcal{O}_K \setminus \{0\}$ de la forme $\frac{1}{3}\left(x + y2^{1/3} + z2^{2/3}\right)$ avec $x, y, z \in \{-1, 0, 1\}$. La norme d'un tel élément est

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}}\left(\frac{1}{3}\left(x + y2^{1/3} + z2^{2/3}\right)\right) &= \frac{1}{27}\left(x^3 + 2y^3 + 4z^3 - 6xyz\right) \\
&= \frac{1}{27}\left(x + 2y + 4z - 6xyz\right) \qquad \text{car } x, y, z \in \{-1, 0, 1\} \\
&\in \mathbb{Z}.
\end{aligned}$$

donc $x + 2y + 4z - 6xyz \equiv 0 \pmod{27}$. Comme

$$\begin{aligned}
|x + 2y + 4z - 6xyz| &\leqslant |x| + 2|y| + 4|z| + 6|xyz| \\
&\leqslant 1 + 2 + 4 + 6 \\
&\leqslant 13,
\end{aligned}$$

on a $x + 2y + 4z - 6xyz = 0$, donc $\mathrm{N}_{K/\mathbb{Q}}\left(\frac{1}{3}\left(x + y2^{1/3} + z2^{2/3}\right)\right) = 0$. Le seul élément de K de norme nulle (donc tel que la multiplication par cet élément soit non inversible) étant 0, on trouve $\frac{1}{3}\left(x + y2^{1/3} + z2^{2/3}\right) = 0$, ce qui contredit à nouveau l'hypothèse de non nullité.

Donc $\left(1, 2^{1/3}, 2^{2/3}\right)$ est une base du $\mathbb{Z}$-module $\mathcal{O}_K$. Montrons maintenant que l'on a bien $\mathcal{O}_K = \mathbb{Z}\left[2^{1/3}\right]$. Comme $1, 2^{1/3}, 2^{2/3} \in \mathbb{Z}\left[2^{1/3}\right]$, on a $\mathcal{O}_K \subseteq \mathbb{Z}\left[2^{1/3}\right]$. D'autre part, $2^{1/3} \in \mathcal{O}_K$ et $\mathcal{O}_K$ est une $\mathbb{Z}$-algèbre, donc $\mathbb{Z}\left[2^{1/3}\right] \subseteq \mathcal{O}_K$, d'où l'égalité voulue.

Question 4

Montrer que l'équation diophantienne $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ a une infinité de solutions $(x, y, z) \in \mathbb{Z}^3$.

D'après les questions 1 et 3, cela revient à montrer que l'ensemble

$$\left\{\alpha \in \mathcal{O}_K \middle/ \mathrm{N}_{K/\mathbb{Q}}(\alpha) = 1\right\}$$

est infini. Comme les entiers de norme 1 sont inversibles, cela revient à montrer que le noyau du morphisme de groupes

$$\mathrm{N}_{K/\mathbb{Q}} \colon \mathcal{O}_K^\times \longrightarrow \{\pm 1\}$$

est infini. Comme l'image du morphisme est finie (puisque contenue dans $\{\pm 1\}$), son noyau est d'indice fini dans $\mathcal{O}_K^\times$, donc il suffit de montrer que $\mathcal{O}_K^\times$ est infini. Or, d'après le théorème des unités de Dirichlet, le groupe $\mathcal{O}_K^\times$ est isomorphe à $\mu(K) \times \mathbb{Z}^{r+s-1}$, où

- $\mu(K)$ est le groupe (fini) des racines de l'unité dans le corps K ;
- r est le nombre de plongements de K dans $\mathbb{R}$;
- s est la moitié du nombre de plongements non réels de K dans $\mathbb{C}$.

Cela revient donc à montrer que $r + s - 1 > 0$.

Le polynôme minimal sur $\mathbb{Q}$ de $2^{1/3}$ est $X^3 - 2$, dont les racines dans $\mathbb{C}$ sont $2^{1/3} \in \mathbb{R}$, $2^{1/3} e^{\frac{2\pi i}{3}} \notin \mathbb{R}$ et $2^{1/3} e^{-\frac{2\pi i}{3}} \notin \mathbb{R}$. On trouve donc $r = 1$ et $s = 1$, donc $r + s - 1 = 1 > 0$. L'équation diophantienne $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ a donc une infinité de solutions $(x, y, z) \in \mathbb{Z}^3$.