Université P. et M. Curie (Paris VI)
Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : (12 ECTS)
code UE : MMAT4020 code Scolar : MM020

`Seul document autorisé : le polycopié du cours`

Examen du 3 juin 2009
Durée : 3 heures

Exercice 1. *Soit $a \geq 2$ un entier positif.*
a) Quel est le développement en fraction continue du nombre $t = \sqrt{a^2+a}$?
`Indication` *: on pourra remarquer que*

$$\frac{1}{t-a} = 2 + \frac{1}{t+a}\cdot$$

b) Quelles sont les solutions en entiers positifs (x, y) de l'équation

$$x^2 - (a^2+a)y^2 = -1?$$

c) Donner la liste des solutions en entiers positifs (x, y) de l'équation

$$x^2 - (a^2+a)y^2 = 1.$$

Expliciter deux solutions.

Exercice 2. *Le nombre 119 est-il un carré modulo 13 ?*

Exercice 3. *Soit n un entier ≥ 3. On pose $\zeta_n = e^{2i\pi/n}$ et $E_n = \mathbb{Q}(\zeta_n)$.*
a) Quel est l'ordre du sous–groupe de torsion de $E_n^\times$?
b) On suppose pour la suite de l'exercice que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. Montrer qu'il existe un unique sous-corps K_n de E_n tel que $[E_n : K_n] = 2$.
c) Montrer que $K_n = E_n \cap \mathbb{R}$.
d) Montrer que $K_n = \mathbb{Q}\big(\zeta_n + \zeta_n^{-1}\big)$.

Exercice 4. *On note $\omega = \sqrt[3]{2}$ et on pose $K = \mathbb{Q}(\omega)$. Dans la suite on notera $\mathcal{O}_K$ l'anneau des entiers de K et $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ la norme.*

1. *Montrez que le discriminant de $\mathbb{Z}[\omega]$ est égal à $-3^3 2^2$.*
2. *Déduisez de la question précédente que l'indice $\Big(\mathcal{O}_K : \mathbb{Z}[\omega]\Big)$ de $\mathbb{Z}[\omega]$ dans $\mathcal{O}_K$ est égal à 1 ou 3.*
3. *Montrez que $N_{K/\mathbb{Q}}(x + y\omega + z\omega^2) = x^3 + 2y^3 + 4z^3 - 6xyz$.*
4. *Montrez que $\mathcal{O}_K = \mathbb{Z}[\omega]$.*

5. *Justifiez la décomposition en produit d'idéaux premiers des idéaux suivants :*
$$2\mathcal{O}_K = \mathcal{P}_2^3, \quad 3\mathcal{O}_K = \mathcal{P}_3\mathcal{P}_3' \quad et \quad 5\mathcal{O}_K = \mathcal{P}_5\mathcal{P}_5',$$
où
$$\mathcal{P}_2 = \omega\mathcal{O}_K, \quad \mathcal{P}_3 = (3, 1+\omega), \quad \mathcal{P}_3' = (3, \omega^2 - \omega + 1),$$
$$\mathcal{P}_5 = (5, \omega + 2) \quad et \quad \mathcal{P}_5' = (5, \omega^2 - 2\omega - 1).$$
Indication : on utilisera sans justification les résultats de l'exercice 4 de l'examen de mai.
6. *Trouvez $\alpha \in \mathcal{O}_K$ (resp. $\beta \in \mathcal{O}_K$) dont la norme $N_{K/\mathbb{Q}}$ est égale à 3 (resp. à 5).*
7. *Montrez que les idéaux $\mathcal{P}_3$, $\mathcal{P}_3'$, $\mathcal{P}_5$ et $\mathcal{P}_5'$ sont principaux.*
8. *Montrez que $\mathbb{Z}[\omega]$ est principal.*
9. *Soit p un nombre premier.*
   (a) *Montrez que ou bien $p\mathcal{O}_K$ est premier ou bien il existe un idéal $\mathcal{P}$ de norme p.*
   (b) *Montrez qu'il existe un idéal de $\mathcal{O}_K$ de norme p si et seulement si 2 est un cube de $\mathbb{F}_p^\times$.*
   (c) *Montrez que si $p\mathcal{O}_K$ est premier alors $p \equiv 1 \mod 3$; en étudiant le cas $p = 31$ que pensez-vous de la réciproque ?*
10. *On considère l'équation*
$$x^3 + 2y^3 + 4z^3 - 6xyz = m$$
et on écrit $m = \pm\prod_p p^{m_p}$. Montrez que cette équation admet une solution (x, y, z) entière si et seulement si pour chaque $p \neq 2, 3$ premier tel que 2 n'est pas un cube dans $\mathbb{F}_p^\times$, l'entier m_p est divisible par 3.

1 Solutions

1 a) Montrons que le développement en fraction continue de $t = \sqrt{a^2+a}$ est

$$[a; \overline{2, 2a}].$$

La partie entière de t est a. Comme on écrit

$$\frac{1}{t-a} = 2 + \frac{1}{t+a},$$

on a

$$t = a + \frac{1}{2 + \dfrac{1}{a+t}}\cdot$$

Par conséquent, si on définit les deux suites $(a_n)_{n\geq 0}$ et $(t_n)_{n\geq 0}$ par les relations de récurrence

$$t_n = a_n + \frac{1}{t_{n+1}} \quad \text{et} \quad a_n = [t_n]$$

pour $n \geq 0$, avec la condition initiale $t_0 = t$, alors on a, pour $k \geq 1$,

$$t_{2k-1} = \frac{1}{t-a}, \quad a_{2k-1} = 2, \qquad t_{2k} = \frac{1}{t_{2k-1}-2} = t + a, \quad a_{2k} = 2a.$$

b) La période $(1, 2a)$ du développement en fraction continue de $\sqrt{a^2+a}$ a pour longueur 2, un nombre pair. Il en résulte que l'équation

$$x^2 - (a^2+a)y^2 = -1$$

n'a pas de solution en entiers positifs (x, y).
c) L'unité fondamentale de l'anneau $\mathbb{Z}[\sqrt{a^2+a}]$ est $2a + 1 + 2\sqrt{a^2+a}$. Les solutions en entiers positifs (x, y) de l'équation

$$x^2 - (a^2+a)y^2 = 1$$

sont donc données par la suite $(x_n, y_n)_{n\geq 1}$ avec

$$x_n + y_n\sqrt{a^2-1} = (2a + 1 + 2\sqrt{a^2+a})^n.$$

Ainsi les deux premières solutions dans l'ordre croissant sont

$$(x_1, y_1) = (2a+1, 2), \quad (x_2, y_2) = (8a^2+8a+1, 8a+4).$$

On les obtient aussi par les développements en fractions continues finies

$$[a, 2] = \frac{x_1}{y_1}, \quad [a, 2, 2a, 2] = \frac{x_2}{y_2}\cdot$$

2 On a $119 \equiv 2 \mod 13$ et comme $(13^2-1)/8 = 21 \equiv 1 \mod 2$, 2 n'est pas un carré modulo 13.

3 a) Le corps E_n est de degré $\varphi(n)$ sur $\mathbb{Q}$. Soit m l'ordre du sous-groupe de torsion $(E_n^\times)_{\text{tors}}$ de $E_n^\times$ et ζ_m un générateur du groupe cyclique $(E_n^\times)_{\text{tors}}$. Comme $\zeta_n \in (E_n^\times)_{\text{tors}}$ l'ordre n de ζ_n divise m. Comme ζ_m appartient à E_n, son degré $\varphi(m)$ sur $\mathbb{Q}$ divise $\varphi(n)$. Les couples d'entiers positifs (a, b) qui vérifient

$$a|b \quad \text{et} \quad \varphi(b)|\varphi(a)$$

sont ceux pour lesquels

$$(a = b) \quad \text{ou} \quad (a \text{ est impair et } b = 2a).$$

On en déduit que si n est impair on a $m = 2n$, tandis que si n est pair alors $m = n$. On peut aussi rappeler que si n est impair on a $\Phi_{2n}(X) = \Phi_n(-X)$, et $-\zeta_n$ est une racine primitive de l'unité d'ordre $2n$.
b) On suppose que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. Son ordre est pair (car $\varphi(n)$ est pair pour $n \geq 3$), donc il possède un unique sous–groupe d'ordre 2. Par conséquent il existe un unique sous-corps K_n de E_n tel que $[E_n : K_n] = 2$.
c) Le corps E_n n'est pas contenu dans $\mathbb{R}$ (car $n \geq 3$ et les seules racines de l'unité réelles sont ± 1), donc la conjugaison complexe est un élément τ d'ordre 2 du groupe de Galois de E_n sur $\mathbb{Q}$. Le sous–corps de E_n fixé par τ est $K_n = E_n \cap \mathbb{R}$.
d) Noter que ζ_n^{-1} est le complexe conjugué de ζ_n, donc $\beta_n := \zeta_n + \zeta_n^{-1}$ est réel : $\beta_n = 2\cos(2\pi/n)$. Mais ζ_n est racine du polynôme quadratique $X^2 - \beta_n X + 1 \in F_n[X]$, donc si on définit $F_n := \mathbb{Q}(\beta_n)$, on a $E_n = F_n(\zeta_n)$, ce qui montre que le corps E_n est une extension quadratique de F_n. Par conséquent $F_n = K_n$.

4 (1) On applique par exemple la formule $(-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(\mu'_\theta(\theta))$ qui donne le discriminant de $\mathbb{Z}[\theta]$. Ici $\mu_\omega(X) = X^3 - 2$ et donc $\mu'_\omega(\omega) = 3\omega^2$ et le résultat découle du fait que $N_{K/\mathbb{Q}}(\omega) = 2$.

(2) L'indice $(\mathcal{O}_K : \mathbb{Z}[\omega])$ au carré doit diviser le discriminant de $\mathbb{Z}[\omega]$, ce qui donne comme possibilités $1, 2, 3, 6$. Par ailleurs on remarque que $2\mathcal{O}_K = \left(\omega\mathcal{O}_K\right)^3$ de sorte que 2 est ramifié et doit donc diviser le discriminant de K, ce qui ne laisse plus que 1 et 3 comme possibilités.

(3) La norme est donnée par exemple par le déterminant suivant :

$$\begin{vmatrix} a & b & c \\ 2c & a & b \\ 2b & 2ca & \end{vmatrix}$$

que l'on développe par exemple avec la règle de Sarrus.

(4) On cherche un élément $x \in \mathcal{O}_K$ de la forme $\frac{a+b\omega+c\omega^2}{3}$ avec $-1 \leq a, b, c \leq 1$. La trace donne $a \in \mathbb{Z}$ et ne nous apporte rien tandis que la norme nous donne $a^3 + 2b^3 + 4c^3 - 6abc \equiv 0 \mod 3^3$. En regardant modulo 3, on obtient alors $a - b + c \equiv 0 \mod 3$. Si $a = 0$ alors $b = c$ avec $2b^3 + 4c^3 = 6c^3 \equiv 0 \mod 3^3$ soit $b = c = 0$. Pour $a \neq 0$ quitte à changer x en $-x$, on suppose $a = 1$ et donc $b = 1 + c$ ce qui donne $1 + 2b^3 + 4(b-1)^3 - 6b(b-1)$ qui pour $b = 0$ (resp. $b = 1$,

resp. $b=-1$) est égal à -3 (resp. 3, resp. -21) qui ne sont donc pas divisibles par 3^3 de sorte que $\mathcal{O}_K=\mathbb{Z}[\omega]$.

(5) On factorise en irréductibles X^3-2 modulo 2 (resp. 3, resp. 5) ce qui donne X^3 (resp. $(X+1)(X^2-X+1)$, resp. $(X+2)(X^2-2X-1)$) de sorte que $2\mathcal{O}_K=\mathcal{P}_2^3$ (resp. $3\mathcal{O}_K=\mathcal{P}_3\mathcal{P}_3'$, resp. $5\mathcal{O}_K=\mathcal{P}_5\mathcal{P}_5'$) avec $\mathcal{P}_2=\omega\mathcal{O}_K$ (resp. $\mathcal{P}_3=(3,\omega+1)$, $\mathcal{P}_3'=(3,\omega^2-\omega+1)$, resp. $\mathcal{P}_5=(5,\omega+2)$, $\mathcal{P}_5'=(5,\omega^2-2\omega-1)$).

(6) On cherche donc a,b,c tels que $a^3+2b^3+4c^3-6abc=3$ (resp. égal à 5). On trouve $(1,1,0)$ (resp. $(1,0,1)$) soit l'élément $1+\omega$ (resp. $1+\omega^2$).

(7) Notons tout d'abord que $\mathcal{P}_3$ contient $1+\omega$ de sorte que de l'égalité des normes on en déduit que $\mathcal{P}_3=(1+\omega)\mathcal{O}_K$ et donc $\mathcal{P}_3'$ est principal engendré par $3/(1+\omega)$. De même comme $1+\omega^2$ est de norme 5, on en déduit que $5\in(1+\omega^2)\mathcal{O}_K$; en outre $\omega+2=\omega(1+\omega^2)$ et donc $\mathcal{P}_4\subset(1+\omega^2)\mathcal{O}_K$ et l'égalité découle de l'égalité des normes. Comme précédemment $\mathcal{P}_5'$ est alors aussi principal.

(8) La constante de Minkowski est $M_K=(\frac{4}{\pi})^1\frac{3!}{3^3}$ de sorte que $M_K|D_K|^{1/2}<3$; d'après le cours toute classe d'idéaux contient un idéal entier de norme <3. Or un idéal premier de norme <3 est un idéal au dessus de 2, i.e. égal à $\mathcal{P}_2$, lequel est principal d'après la question précédente.

Remarques : pour ceux qui majorent à la main, d'après la question précédente il fallait simplement majorer strictement par 7.

(9-a) Le résultat découle directement du fait qu'un polynôme de degré 3 est soit irréductible soit admet un facteur irréductible de degré 1.

(9-b) Ainsi il existe un idéal de norme p si et seulement si X^3-2 admet une racine dans $\mathbb{F}_p$ i.e. si et seulement si 2 est un cube dans $\mathbb{F}_p^\times$.

(9-c) Si $p\not\equiv 1 \mod 3$ alors le morphisme $x\in\mathbb{F}_p^\times\mapsto x^3\in\mathbb{F}_p^\times$ est surjectif ; en effet via l'isomorphisme $\mathbb{F}_p^\times\simeq\mathbb{Z}/(p-1)\mathbb{Z}$, le morphisme précédent correspond à la multiplication par 3 qui est alors un isomorphisme car $3\wedge(p-1)=1$. Ainsi 2 est dans l'image et donc X^3-2 a une solution modulo p. Par contraposition, on en déduit donc que si $p\mathcal{O}_K$ est premier alors $p\equiv 1 \mod 3$.

Pour $p=31$, on remarque que 2 est un cube modulo 31, $4^3\equiv 2 \mod 31$ et donc bien que $p\equiv 1 \mod 3$, d'après 9-b, $31\mathcal{O}_K$ n'est pas un idéal premier.

(10) La question est de savoir si m est la norme d'un élément de $\alpha\in K$. Notons $\mathfrak{P}$ (resp. $\mathfrak{P}_1$ et $\mathfrak{P}_2$) l'ensemble des nombres premiers (resp. tels que 2 n'est pas un cube modulo p, et son complémentaire).

Montrons tout d'abord que la condition de l'énoncé est nécessaire : on décompose $\alpha\mathcal{O}_K$ en produit d'idéaux premiers en séparant ceux qui sont au dessus d'un premier p de $\mathfrak{P}_1$ des autres ; on les note respectivement $\mathfrak{I}_1$ et $\mathfrak{I}_2$:

$$\alpha\mathcal{O}_K=\prod_{\mathcal{P}\in\mathfrak{I}_1}\mathcal{P}^{m_\mathcal{P}}.\prod_{\mathcal{P}\in\mathfrak{I}_2}\mathcal{P}^{m_\mathcal{P}}.$$

En prenant les normes, on remarque que pour $p\in\mathfrak{P}_1$, $m_p\equiv 0 \mod 3$.

Réciproquement pour $p\in\mathfrak{P}_2$, on choisit un idéal $\mathcal{P}_p\in\mathfrak{I}_2$ de norme p ; pour $p\in\mathfrak{P}_1$, $p\mathcal{O}_K$ est l'unique idéal premier au dessus de p. On prend alors pour α un générateur de $\prod_{p\in\mathfrak{P}_2}\mathcal{P}_p^{m_p}\prod_{p\in\mathfrak{P}_1}(p\mathcal{O}_K)^{m_p/3}$ qui est de norme m.