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

Théorie des nombres

Michel Waldschmidt

`Seul document autorisé : le polycopié du cours`

Examen partiel du mardi 24 février 2009 [1]
Durée : 2 heures

Exercice 1. Montrer que l'équation Diophantienne $y^2 = x^3 + 7$ n'a pas de solution $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

Exercice 2. Soient n un entier ≥ 3 et f, g, h trois polynômes à coefficients complexes premiers entre eux dans $\mathbf{C}[X]$. On suppose $f^n + g^n = h^n$. Montrer que les trois polynômes f, g, h sont constants.

Exercice 3. Soient a un entier positif et $(u_n)_{n\geq 0}$ une suite bornée d'entiers rationnels. Montrer que le nombre

$$\sum_{n\geq 0} u_n a^{-n^2}$$

est rationnel si et seulement si le support $\{n \geq 0\ ;\ u_n \neq 0\}$ de la suite $(u_n)_{n\geq 0}$ est fini.

Exercice 4. Soit $a \geq 2$ un entier positif.
a) Quel est le développement en fraction continue de $\sqrt{a^2 - 1}$?
b) Quelles sont les solutions en entiers positifs (x, y) de l'équation

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

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

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

Expliciter trois solutions.

[1] Deux corrections ont été apportées après le 24 février : dans l'exercice 2 on suppose les polynômes f, g, h premiers entre eux, et dans l'exercice 5 on considère les solutions dans $\mathbf{Z}_{\geq 0}$ et non dans $\mathbf{Z}$.

Exercice 5. Soient $h, a_1, \ldots, a_h$ des entiers positifs. Pour m entier ≥ 0 on désigne par $N(a_1, \ldots, a_h; m)$ le nombre de $(n_1, \ldots, n_h)$ dans $\mathbf{Z}_{\geq 0}^h$ qui vérifient

$$a_1 n_1 + \cdots + a_h n_h = m.$$

Montrer que la série

$$\sum_{m \geq 0} N(a_1, \ldots, a_h; m) z^m$$

est une fraction rationnelle de $\mathbf{Q}(z)$. Expliciter le numérateur et le dénominateur.

Exercice 6. Soient a et b deux entiers positifs et K_{ab} le corps de décomposition sur $\mathbf{Q}$ du polynôme $(X^2 - a)(X^3 - b)$. Quel est le degré de K_{ab} sur $\mathbf{Q}$? Quel est le groupe de Galois de K_{ab} sur $\mathbf{Q}$?

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

Partiel du mardi 24 février 2009
Corrigé [2]

Solution de l'exercice 1. Cet exercice a été traité en TD (feuille 1 premier exercice de la section 2.2). Le point est que les carrés modulo 4 sont 0 et 1, donc un diviseur premier impair de y^2+1 est congru à 1 modulo 4.

Solution de l'exercice 2. Cet exercice a été traité en TD (feuille 1 deuxième exercice de la section 1). On utilise simplement le théorème de Mason qui a été vu en cours (Théorème 0.4).

Solution de l'exercice 3. Si la suite $(u_n)_{n\geq 0}$ a un support fini, il est clair que le nombre

$$\theta = \sum_{n\geq 0} u_n a^{-n^2}$$

est rationnel. Supposons maintenant le nombre θ rationnel. On choisit un entier N suffisamment grand et on pose

$$q_N = a^{N^2}, \qquad p_N = \sum_{n=0}^{N} u_n a^{N^2-n^2}, \qquad R_N = q_N\theta - p_N = \sum_{n\geq N+1} u_n a^{N^2-n^2}.$$

On vérifie que p_N et q_N sont des entiers rationnels et que R_N tend vers 0 quand N tend vers l'infini. Comme θ est rationnel, il en résulte que R_N est nul pour tout N suffisamment grand. Dans le développement de R_N en série, le premier terme est $u_{N+1}a^{-(N+1)^2+N^2}$, il doit être nul, donc la suite $(u_n)_{n\geq 0}$ a un support fini.

Solution de l'exercice 4.
a) Montrons que le développement en fraction continue de $t=\sqrt{a^2-1}$ est

$$[a-1; \overline{1, 2a-2}].$$

La partie entière de t est $a-1$. On écrit

$$(a-t)(a+t) = 1, \quad \text{donc} \quad t = a - \frac{1}{a+t} = a - 1 + \frac{a+t-1}{a+t},$$

[2]La solution de l'exercice 5 a été corrigée après le partiel : le dénominateur est $(1-z^{a_1})\cdots(1-z^{a_h})$ et non $(1-z)^{a_1}\cdots(1-z)^{a_h}$.

ce qui donne

$$t = a - 1 + \cfrac{1}{1 + \cfrac{1}{a + t - 1}} \cdot$$

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

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

pour $n \geq 0$, avec les conditions initiales $t_0 = t$, $a_0 = a - 1$, alors on a, pour $k \geq 1$,

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

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

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

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

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

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

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

Ainsi les trois premières solutions dans l'ordre croissant sont

$$(x_1, y_1) = (a, 1), \quad (x_2, y_2) = (2a^2 - 1, 2a), \quad (x_3, y_3) = (4a^3 - 3a, 4a^2 - 1).$$

On les obtient aussi par les développements en fractions continues finies

$$[a - 1, 1] = \frac{x_1}{y_1}, \quad [a - 1, 1, 2a - 2, 1] = \frac{x_2}{y_2}, \quad [a - 1, 1, 2a - 2, 1, 2a - 2, 1] = \frac{x_3}{y_3} \cdot$$

Solution de l'exercice 5. Le numérateur est 1 et le dénominateur est $(1 - z^{a_1}) \cdots (1 - z^{a_h})$.

Solution de l'exercice 6.
a) Notons j une racine du polynôme $X^2 + X + 1$. Montrons que le corps $K_{ab} = \mathbf{Q}(\sqrt{a}, j, \sqrt[3]{b})$ a pour degré $[K_{ab} : \mathbf{Q}] = pq$, avec $p = 2$ si a n'est pas un carré dans $\mathbf{Q}$ et $p = 1$ si a est un carré dans $\mathbf{Z}$, et avec $q = 6$ si b n'est pas un cube dans $\mathbf{Z}$ et $q = 2$ si b est un cube dans $\mathbf{Z}$. Pour le démontrer on procède de la façon suivante.

On rappelle d'abord que si a n'est pas un carré dans $\mathbf{Z}$, alors a n'est pas un carré dans $\mathbf{Q}$ et le polynôme $X^2 - a$ est irréductible sur $\mathbf{Q}$ (la démonstration a été faite en cours et en TD).

Le corps de décomposition sur $\mathbf{Q}$ de $X^2 - a$ est $\mathbf{Q}(\sqrt{a}$, qui est égal à $\mathbf{Q}$ si a est un carré dans $\mathbf{Z}$, et qui est une extension quadratique réelle de $\mathbf{Q}$ sinon.

De même si b n'est pas un cube dans $\mathbf{Z}$, alors b n'est pas un cube dans $\mathbf{Q}$ et le polynôme X^3-b est irréductible sur $\mathbf{Q}$; alors un corps de rupture de X^3-2 sur $\mathbf{Q}$ est l'extension cubique $\mathbf{Q}(\sqrt[3]{b})$ de $\mathbf{Q}$.

Le corps de décomposition de X^3-b sur $\mathbf{Q}$ est l'extension quadratique $\mathbf{Q}(j, \sqrt[3]{b})$ de $\mathbf{Q}(\sqrt[3]{b})$. Par conséquent le corps de décomposition sur $\mathbf{Q}$ de X^3-b, qui est $\mathbf{Q}(j, \sqrt[3]{b})$, est égal à $\mathbf{Q}(j)$ si b est un cube dans $\mathbf{Z}$, c'est une extension de degré 6 de $\mathbf{Q}$ sinon.

Pour terminer la démonstration il reste à préciser le cas où a n'est pas un carré dans $\mathbf{Z}$ et b n'est pas un cube dans $\mathbf{Z}$. Comme les degrés des extensions $\mathbf{Q}(\sqrt{a})/\mathbf{Q}$ et $\mathbf{Q}(\sqrt[3]{b})/\mathbf{Q}$ sont premiers entre eux (ce sont 2 et 3), il en résulte que le compositum $\mathbf{Q}(\sqrt{a}, \sqrt[3]{b})$ a pour degré sur $\mathbf{Q}$ le produit de ces degrés, soit 6. Comme j n'est pas réel il n'appartient pas à $\mathbf{Q}(\sqrt{a}, \sqrt[3]{b})$, donc K_{ab} a pour degré 12 sur $\mathbf{Q}$.

b) Si a est un carré et b un cube, le groupe de Galois de $K_{ab} = \mathbf{Q}(j)$ sur $\mathbf{Q}$ est le groupe cyclique à deux éléments.

Si a n'est pas un carré et que b est un cube, le groupe de Galois de $K_{ab} = \mathbf{Q}\sqrt{a}, j)$ sur $\mathbf{Q}$ est le groupe abélien non cyclique à quatre éléments $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Si a est un carré et que b n'est pas un cube, le groupe de Galois de $K_{ab} = \mathbf{Q}(j, \sqrt[3]{b})$ sur $\mathbf{Q}$ est le groupe non commutatif $\mathfrak{S}_3$ à 6 éléments.

Enfin si a n'est pas un carré et que b n'est pas un cube, le corps $K_{ab} = \mathbf{Q}(j, \sqrt[3]{b}, \sqrt{a})$ est le compositum du corps quadratique $\mathbf{Q}\sqrt{a})$ avec le corps $\mathbf{Q}(j, \sqrt[3]{b})$ qui est aussi Galoisien sur $\mathbf{Q}$ de groupe de Galois $\mathfrak{S}_3$. C'est pourquoi dans ce cas le groupe de Galois G de K_{ab} sur $\mathbf{Q}$ est le produit direct de $\mathbf{Z}/2\mathbf{Z}$ par $\mathfrak{S}_3$.

Le tableau est le suivant

a carré	b cube	K_{ab}	$[K_{ab} : \mathbf{Q}]$	$\mathrm{Gal}(K_{ab}/\mathbf{Q})$
oui	oui	$\mathbf{Q}(j)$	2	$\mathbf{Z}/2\mathbf{Z}$
non	oui	$\mathbf{Q}(\sqrt{a}, j)$	4	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$
oui	non	$\mathbf{Q}(j, \sqrt[3]{b})$	6	$\mathfrak{S}_3$
non	non	$\mathbf{Q}(\sqrt{a}, j, \sqrt[3]{b})$	12	$\mathbf{Z}/2\mathbf{Z} \times \mathfrak{S}_3$