UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°5 : Anneaux d'entiers, équation de Pell-Fermat

Anneaux d'entiers de corps de nombres

Exercice 1

1. Quelle est la norme sur le corps $\mathbb{Q}(\sqrt{-3})$? Notons $j = \frac{-1+\sqrt{-3}}{2}$. Quelle est la norme sur $\mathbb{Z}[j]$ exprimée dans la base $(1, j)$?
2. Montrer qu'un nombre premier est réductible dans $\mathbb{Z}[j]$ si et seulement s'il est la norme d'un élément de $\mathbb{Z}[j]$.
3. Les nombres 3, 11 et 13 sont-ils réductibles dans $\mathbb{Z}[j]$?
4. Montrer qu'un nombre premier p est réductible dans $\mathbb{Z}[j]$ si et seulement si $\mathbb{Z}[j]/(p)$ n'est pas intègre.
5. Montrer qu'un nombre premier $p > 3$ est réductible dans $\mathbb{Z}[j]$ si et seulement si $X^2 + X + 1$ admet une racine dans $\mathbb{F}_p$ si et seulement si le groupe multiplicatif $\mathbb{F}_p^\times$ des inversibles de $\mathbb{F}_p$ a un élément d'ordre 3.
6. Montrer qu'un nombre premier p est réductible dans $\mathbb{Z}[j]$ si et seulement si $p \equiv 1 \pmod 3$ ou $p = 3$.
7. Montrer qu'un nombre premier p s'écrit sous la forme $p = a^2 - ab + b^2$, avec $a, b \in \mathbb{Z}$, si et seulement si $p \equiv 1 \pmod 3$ ou $p = 3$.

Exercice 2

1. Expliciter les deux plongements complexes du corps quadratique $\mathbb{Q}(\sqrt{13})$.
2. Calculer la norme et la trace de l'élément $a + b\sqrt{13}$ de $\mathbb{Q}(\sqrt{13})$.
3. Calculer le discriminant de la $\mathbb{Q}$-base $(1, \sqrt{13})$ de $\mathbb{Q}(\sqrt{13})$.
4. Déterminer une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{13})$ formée d'entiers algébriques et de discriminant strictement plus petit que l'entier obtenu dans la question précédente.

Exercice 3

Montrer que le polynôme $X^3 - X - 1$ de $\mathbb{Q}[X]$ est irréductible. Calculer son discriminant. Déterminer l'anneau des entiers du corps $\mathbb{Q}[X]/(X^3 - X - 1)$.

Exercice 4

1. Rappeler l'anneau des entiers de l'extension quadratique $\mathbb{Q}(\sqrt{6})$ et celui de $\mathbb{Q}(\sqrt{14})$.
2. Montrer que $\alpha = \frac{\sqrt{6}+\sqrt{14}}{2}$ est un entier de l'extension biquadratique $\mathbb{Q}(\sqrt{6}, \sqrt{14})$.

Exercice 5

Quels sont les entiers n tels que l'anneau des entiers du corps quadratique $\mathbb{Q}(\sqrt{n})$ admet un plongement complexe dont l'image est un réseau de $\mathbb{C}$? Calculer le volume de ce réseau quand n est sans facteur carré.

Exercice 6

Montrer que si $d \neq d'$ sont deux entiers positifs sans facteur carré, les corps $\mathbb{Q}[\sqrt{d}]$, $\mathbb{Q}[\sqrt{d'}]$, $\mathbb{Q}[i\sqrt{d}]$ et $\mathbb{Q}[i\sqrt{d'}]$ sont deux à deux non isomorphes.

Exercice 7

1. Quels sont les inversibles de $\mathbb{Z}[\sqrt{-1}]$?
2. Soit $a \in \mathbb{Z}[\sqrt{-1}]$. Montrer que si $\mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a)$ est un nombre premier, alors a est irréductible.
3. Montrer que $\mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a) = \mathrm{Card}\left(\mathbb{Z}[\sqrt{-1}]/(a)\right)$.
4. Montrer que $a \mid \mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a)$ dans l'anneau $\mathbb{Z}[\sqrt{-1}]$.
5. L'anneau $\mathbb{Z}[\sqrt{-1}]$ est-il factoriel ? (Aucune démonstration n'est demandée).
6. Soit a un irréductible de $\mathbb{Z}[\sqrt{-1}]$. Montrer que $\mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a)$ est une puissance d'un nombre premier. (On pourra étudier l'anneau $\mathbb{Z}[\sqrt{-1}]/(a)$).
7. Soit p un nombre premier. Montrer que les anneaux $\mathbb{Z}[\sqrt{-1}]/(p))$ et $\mathbb{F}_p[X]/(X^2+1)$ sont isomorphes.
8. Montrer que p est irréductible si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$.
9. Soit a un diviseur irréductible de p dans $\mathbb{Z}[\sqrt{-1}]$. Montrer que $\mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a) \in \{p, p^2\}$. Pour quels nombres premiers p trouve-t-on p, et pour lesquels trouve-t-on p^2 ?
10. Soit a un irréductible de $\mathbb{Z}[\sqrt{-1}]$. Montrer que l'on est dans un des trois cas suivants :
    (i) $a = u(1+\sqrt{-1})$, avec u une unité ;
    (ii) $a = up$, avec u une unité et p un nombre premier vérifiant $p \equiv 3 \pmod 4$;
    (iii) $a = u(x+y\sqrt{-1})$, avec u une unité et $x, y \in \mathbb{Z}$ tels que x^2+y^2 soit un nombre premier impair.

11. Soit $N \in \mathbb{N} \setminus \{0\}$. On suppose qu'il existe $x, y \in \mathbb{Z}$ tels que $N = x^2 + y^2$. Soit $x + y\sqrt{-1} = u\pi_1^{\alpha_1} \dots \pi_m^{\alpha_m}$, avec $u \in \mathbb{Z}[\sqrt{-1}]^\times$, $\alpha_1, \dots, \alpha_m \in \mathbb{N} \setminus \{0\}$ et $\pi_1, \dots, \pi_m$ des irréductibles de $\mathbb{Z}[\sqrt{-1}]$, la décomposition de $x + y\sqrt{-1}$ en produit d'irréductibles. Montrer que $N = \prod_{i=1}^{m} \mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\pi_i)^{\alpha_i}$.
12. En déduire que si p est un diviseur premier de N, alors $p \equiv 3 \pmod 4 \implies 2 \mid v_p(N)$.
13. Réciproquement, montrer que si $N \in \mathbb{N} \setminus \{0\}$ vérifie la propriété de la question précédente, alors N est somme de deux carrés.

Exercice 8

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

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 $\mathrm{N}_{K/\mathbb{Q}}$.
2. Calculer le discriminant de la $\mathbb{Q}$-base $\left(1, 2^{1/3}, 2^{2/3}\right)$ de K.
3. En déduire que $\mathscr{O}_K = \mathbb{Z}\left[2^{1/3}\right]$.
4. Montrer que l'équation diophantienne $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ a une infinité de solutions $(x, y, z) \in \mathbb{Z}^3$.

Équation de Pell-Fermat

Exercice 9

Soit θ un réel.

On considère les deux suites (a_n) et (θ_n) définies par récurrence de la façon suivante : $\theta_0 = \theta$, et pour tout $i \geq 0$, $a_i = \lfloor \theta_i \rfloor$, $\theta'_{i+1} = \theta_i - a_i$, de sorte que (a_n) est une suite d'entiers et (θ_n) une suite de réels. De plus, on définit, tant que θ'_{n+1} est non nul (ou de manière équivalente tant que θ_n n'est pas entier), $\theta_{n+1} = \frac{1}{\theta'_{n+1}}$. Par exemple si θ est un entier, $\theta_0 = \theta$ et θ_1 n'est pas défini. Remarquer que pour $i \geq 1$, $\theta_i > 1$ donc $a_i \geq 1$.

Si le processus s'arrête, c'est à dire si θ_n est entier pour un certain n, vérifier que

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}},$$

sinon, pour tout n on a

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{\theta_n}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

Cette écriture est appelée développement de θ en fractions continues. On la note aussi $\theta = [a_0, a_1, \dots, a_{n-1}, a_n]$, respectivement $\theta = [a_0, \dots, a_n, \dots]$.

1. Montrer que le développement est fini si et seulement si θ est un nombre rationnel.
2. Donner le développement en fractions continues de $\frac{116}{27}$.
3. Quel est le nombre dont le développement en fractions continues est

$$5 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}?$$

4. Supposons θ irrationnel. On appelle réduite d'ordre n la fraction $[a_0, \dots, a_n]$. Elle s'écrit de manière unique $\frac{p_n}{q_n}$, avec p_n et q_n entiers, calculés sans simplification. Vérifier que $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1 + 1$ et $q_1 = a_1$ et que p_n comme q_n sont des polynômes en les $(a_i)_{0 \le i \le n}$.
5. Pour $n \geq 2$, montrer que

$$p_n = a_n p_{n-1} + p_{n-2} \tag{1}$$
$$q_n = a_n q_{n-1} + q_{n-2}. \tag{2}$$

6. En déduire $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$ et $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$.
7. Montrer que pour tout n,

$$\theta = \frac{\theta_{n+1} p_n + p_{n-1}}{\theta_{n+1} q_n + q_{n-1}}. \tag{3}$$

Exercice 10

1. Soit $\theta = \frac{1}{2}(\sqrt{5} - 1)$. Montrer que θ est un entier algébrique et trouver le polynôme minimal de $\frac{1}{\theta}$. En déduire le développement en fractions continues de θ.
2. Écrire le développement en fraction continue de $3 + \sqrt{2}$, $2 + \sqrt{6}$ et $2 + \frac{\sqrt{15}}{5}$.

3. Le but de cette question est de calculer les trois premières réduites du développement en fractions continues de $\sqrt[3]{2}$. Montrer que $1,2 < \sqrt[3]{2} < 1,3$ et $1,5 < \sqrt[3]{4} < 1,6$. Dans l'anneau $\mathbb{Q}[X]/(X^3-2)$, déterminer l'inverse de $X-1$ et celui de X^2+X-2, exprimés dans la base $(1, X, X^2)$. Conclure.

Exercice 11

Montrer que pour $a, b \in \mathbb{N}$, $a \neq 0$, $b < 2a+1$, on a

$$\sqrt{a^2+b} = a + \cfrac{b}{2a + \cfrac{b}{2a + \cfrac{b}{\ddots}}}.$$

En déduire le développement en fraction continue de $\sqrt{5}$, $\sqrt{10}$, $\sqrt{17}$, $\sqrt{26}$, $\sqrt{37}$.

Exercice 12

1. Quel est le nombre dont le développement en fractions continues est $[\bar{1}]$?
2. Quel est le nombre dont le développement en fractions continues est $[\overline{4,5}]$?
3. Montrer que le nombre dont le développement en fractions continues est $[\bar{a}]$ est $\frac{a+\sqrt{a^2+4}}{2}$.

Exercice 13

1. Soit d un entier sans facteur carré. Considérons l'équation de Pell-Fermat :

   $$x^2 - dy^2 = 1.$$

   Soit (x_1, y_1) une solution de l'équation. Dans $\mathbb{Q}(\sqrt{d})$ considérons l'écriture $x_n + y_n\sqrt{d}$ de $(x_1+y_1\sqrt{d})^n$ dans la $\mathbb{Q}$-base $(1, \sqrt{d})$. Montrer que (x_n, y_n) est une solution de l'équation de Pell-Fermat pour tout n.
   D'après le cours, il existe une solution (x_1, y_1) « minimale » et toutes les autres solutions s'en déduisent à l'aide de l'expression ci-dessus.
2. Cherchons maintenant une solution minimale (x_1, y_1) de l'équation.
   Montrer que si (p, q), avec p et q de même signe, est solution de l'équation, alors $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$.
   La fraction $\frac{p}{q}$ est donc une bonne approximation de $\sqrt{d}$. On peut déduire de cela que $\frac{p}{q}$ est nécessairement une réduite du développement de $\sqrt{d}$.

3. Soit T la période du développement de $\sqrt{d}$. Si T est impaire, on pose $n := 2T - 1$. Si Test pair, on pose $n = T - 1$. Dans tous les cas, $n + 1$ est le plus petit multiple pair de T. Nous allons montrer que la réduite $\frac{p_n}{q_n}$ de $\sqrt{d}$ fournit une solution (p_n, q_n) de l'équation de Pell-Fermat.
   On peut montrer que la solution obtenue est minimale.
4. On pose $\alpha = \sqrt{d}$ et on reprend les notations de l'exercice 9.
   Remarquer que $\frac{1}{\alpha_{n+2}} = \frac{1}{\alpha_1} = \alpha - a_0$.
5. En utilisant (3), montrer que $(q_{n+1} - a_0 q_n)\sqrt{d} + dq_n = p_n\sqrt{d} + (p_{n+1} - a_0 p_n)$.
6. En déduire que $p_n^2 - dq_n^2 = (-1)^{n+1}$ et conclure.

Pour trouver les solutions de l'équation de Pell-Fermat $x^2 - dy^2 = 1$, on commence donc par chercher le développement en fraction continue de $\sqrt{d}$: $\sqrt{d} = [a_0, \overline{a_1, \dots, a_T}]$. La solution non neutre minimale est obtenue avec le numérateur et le dénominateur de la réduite d'indice n où $n + 1$ est le plus petit multiple pair de la plus petite période T. Toutes les autres solutions s'en déduisent.

Pour trouver les solutions de l'équation $x^2 - dy^2 = -1$, on commence par chercher le développement en fraction continue de $\sqrt{d}$: $\sqrt{d} = [a_0, \overline{a_1, \dots, a_T}]$. Les solutions sont obtenues avec le numérateur et le dénominateur des réduites d'indice n où $n + 1$ est un multiple impair de la plus petite période T. En particulier, si la période est paire, l'équation n'a pas de solution.

Application : solutions de l'équation de Pell-Fermat pour $d = 3, 5, 34, 37, 53$. (Indication : $\sqrt{34} = [5, \overline{1, 4, 1, 10}]$, $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$.)

Exercice 14

Déterminer les unités de l'anneau $\mathbb{Z}[\sqrt{41}]$. Montrer que les unités de l'anneau des entiers de $\mathbb{Q}(\sqrt{41})$ sont en fait les unités de l'anneau $\mathbb{Z}[\sqrt{41}]$.