Théorie des nombres

Feuille n°5 : Anneaux d'entiers 2

1 Factorisation

Exercice 1

1. L'anneau $(\mathbb{Z}/6\mathbb{Z})[X]$ est-il factoriel ?
2. Déterminer tous les éléments de norme 2 de $\mathbb{Z}[\sqrt{-3}]$. L'anneau $\mathbb{Z}[\sqrt{-3}]$ est-il factoriel ? (factoriser 4).
3. Quelles sont les normes possibles d'un diviseur de $1+\sqrt{-3}$ dans $A=\mathbb{Z}[\sqrt{-3}]$? Donner un idéal non principal de $A=\mathbb{Z}[\sqrt{-3}]$.
4. Montrer que le sous-anneau A de $\mathbb{R}[X]$ engendré par X^2 et X^3 n'est pas factoriel.
5. Vérifier l'égalité $17=(5+2\sqrt{2})(5-2\sqrt{2})=(7+4\sqrt{2})(7-4\sqrt{2})$. Peut-on en déduire que $A=\mathbb{Z}[\sqrt{2}]$ n'est pas factoriel ?

Exercice 2

Soit $d\geqslant 3$ un entier, montrer que que dans l'anneau $\mathbb{Z}[i\sqrt{d}]$, 2 est irreductible et que l'idéal engendré par 2 n'est pas premier. L'anneau $\mathbb{Z}[i\sqrt{d}]$ est-il factoriel ?

Dans $\mathbb{Z}[i\sqrt{5}]$, 11 est-il irréductible ? L'idéal engendré par 11 est-il premier ?

Exercice 3

Montrer que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien (donc factoriel).

Exercice 4

1. Quelle est la norme sur le corps $\mathbb{Q}(\sqrt{-3})$? 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 $\mathbb{F}_p^\star$ des inversibles de $\mathbb{F}_p$ a un élément d'ordre 3.
6. Montrer qu'un entier p est réductible dans $\mathbb{Z}[j]$ si et seulement si $p = 1[3]$.

2 Sur les polynômes

Exercice 5

Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$.

1. On suppose que P a une racine rationnelle non nulle x, avec $x = \frac{p}{q}$ et $pgcd(p, q) = 1$. Montrer que p divise a_0 et q divise a_n.
2. Le polynôme $7X^3 - 5X^2 - 9X + 4$ a-t-il des racines rationnelles ? et $X^4 - 2X^2 - 3$?
3. Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que $\sqrt{n}$ est soit un entier, soit un irrationnel.

Exercice 6

Un polynôme de $\mathbb{Z}[X]$ est dit primitif si ses coefficients sont premiers entre eux dans leur ensemble.

1. Soit $P \in \mathbb{Z}[X]$ primitif. Montrer que si P est irréductible dans $\mathbb{Q}[X]$ alors il l'est dans $\mathbb{Z}[X]$.
2. Soit P de la forme $a_0 + a_1 X + a_2 X^2 + X^3 \in \mathbb{Z}[X]$. Montrer que si P est irréductible dans $\mathbb{Z}[X]$ alors il l'est dans $\mathbb{Q}[X]$.
3. Soit f et g deux polynômes primitifs de $\mathbb{Z}[X]$. Montrer que leur produit fg est primitif.
4. Soit h un polynôme primitif réductible dans $\mathbb{Q}[X]$. Montrer que h est réductible dans $\mathbb{Z}[X]$.

Exercice 7

Les polynômes symétriques élémentaires en n indéterminées sont par définition

$$\begin{aligned}
s_1(t_1, t_2, \cdots, t_n) &:= t_1 + t_2 + \cdots + t_n \\
s_2(t_1, t_2, \cdots, t_n) &:= t_1 t_2 + t_1 t_3 + \cdots + t_2 t_3 + t_2 t_4 + \cdots + \cdots t_{n-1} t_n \\
&\vdots \\
s_n(t_1, t_2, \cdots, t_n) &:= t_1 t_2 \cdots t_n.
\end{aligned}$$

1. Soit $F(X) = a(X - t_1)(X - t_2) \cdots (X - t_n)$. Développer $F(X)$ en puissances de X.
2. Ecrire $t_1^3 + t_2^3 + t_3^3$ comme polynôme à coefficients entiers de s_1, s_2, s_3.

3. Soit $m_1, m_2, \cdots, m_n$, n entiers naturels. Quel est le terme dominant de $s_1^{m_1} s_2^{m_2} \cdots s_n^{m_n}$?
4. Ranger dans l'ordre lexicographique décroissant les monômes du polynôme symétrique
$$f(t_1, t_2, t_3) = t_1^2 t_2^3 + t_1^2 t_3^3 + t_2^2 t_1^3 + t_2^2 t_3^3 + t_3^2 t_1^3 + t_3^2 t_2^3.$$
5. Ecrire f comme polynôme à coefficients entiers en les polynômes symétriques élémentaires.
6. Soit θ en entier algébrique de degré 3 et θ_2 et θ_3 ses conjugués. Montrer que $f(\theta, \theta_2, \theta_3)$ est un entier naturel.

Plus généralement, tout polynôme symétrique s'écrit comme polynôme à coeficients entiers dans les polynômes symétriques élémentaires.

3 Corps de nombres

Exercice 8

Soit $K = [X]/(P)$ un corps de nombre de degré n. Soit x la classe de X dans K. Soient $\sigma_1, \ldots, \sigma_n$ les n plongements complexes de K. Etant donné une base $\mathcal{B} = (\alpha_1, \ldots, \alpha_n)$ de K sur $\mathbb{Q}$, on définit le discriminant de $\mathcal{B}$ par $\Delta(\mathcal{B}) = \Delta[\alpha_1, \ldots, \alpha_n] = \{\det(\sigma_i(\alpha_j))\}^2$.

1. Montrer que pour toute base $\mathcal{B}$ de K sur $\mathbb{Q}$, $\Delta(\mathcal{B})$ est un élément non nul de $\mathbb{Q}$.
2. Si de plus, les éléments de la base $\mathcal{B}$ sont des entiers algébriques, montrer que $\Delta(\mathcal{B})$ est un entier.
3. Soit $\mathcal{B}$ une base de K sur $\mathbb{Q}$ constituée d'entiers algébriques et telle que $\Delta(\mathcal{B})$ est sans facteur carré. Vérifier que $\Delta(\mathcal{B})$ est minimal.
4. Montrer que sous les hypothèses de la question précédente, la base $\mathcal{B}$ est une base de l'anneau des entiers de K.

Exercice 9

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 10

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 11

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 12

1. Calculer le discriminant de $\mathbb{Q}(\sqrt{3})$ et celui de $\mathbb{Q}(\sqrt{5})$.
2. Montrer que $\zeta = \sqrt{3} + \frac{1+\sqrt{5}}{2}$ est un élément primitif de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. On vérifiera que ses quatre conjugués sont deux à deux distincts, que son polynôme minimal sur $\mathbb{Z}$ est invariant par tout $\mathbb{Q}$-automorphisme de tout corps de nombres et que son degré est donc 4.
3. Déterminer la matrice de la multiplication par ζ dans la base $\mathcal{B} = (1, \sqrt{3}, \frac{1+\sqrt{5}}{2}, \sqrt{3}\frac{1+\sqrt{5}}{2})$ de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ puis le polynôme minimal μ_ζ de ζ sur $\mathbb{Z}$.
4. Calculer le discriminant de la base $\mathcal{B}$.

Exercice 13

On note $K := \mathbb{Q}[X]/(X^3 - 2)$ et $A = \mathbb{Z}[\sqrt[3]{2}]$ le sous-anneau de $\mathbb{C}$ engendré par la racine cubique réelle de 2.

1. Montrer que A est, comme $\mathbb{Z}$-module, libre de base $(1, \sqrt[3]{2}, \sqrt[3]{4})$.
2. Montrer que K est un corps. Préciser une base de K comme $\mathbb{Q}$-espace vectoriel.
3. Décrire tous les plongements complexes de K.
4. Décrire la trace, la norme et la fonction symétrique des sommes de produits deux à deux des conjugués des éléments de K.
5. Calculer le discriminant d'une base $\mathcal{B}$ de K formée d'entiers algébriques.
6. Déterminer l'anneau des entiers de K.

Exercice 14

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 $\mathbb{R}^2$? Calculer alors le volume de ce réseau.

Exercice 15

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.