Théorie des nombres

FEUILLE DE TD N°3

1. FACTORISATION

Exercice 1

1 Montrer que les diviseurs de $7+i$ dans $\mathbf{Z}[i]$ divisent 50. Factoriser 50 dans $\mathbf{Z}[i]$. Factoriser $7+i$ dans $\mathbf{Z}[i]$.

2 Décomposer en produit d'irréductibles dans $\mathbf{Z}[j]$ les éléments $2-j, 5+j, 3, j, 7$.

Exercice 2

1 L'anneau $\mathbf{Z}[\sqrt{-3}]$ est-il factoriel ? (On pourra factoriser 4.)

2 Montrer que l'anneau des entiers de $\mathbf{Q}(\sqrt{-3})$ est euclidien (donc factoriel).

Exercice 3

Soit a un élément du corps des fractions $\mathbf{Q}(\sqrt{-3})$. Il s'écrit $a = p/q$ avec p et q dans $\mathbf{Z}[\sqrt{-3}]$, qui ont comme seuls diviseurs communs dans $\mathbf{Z}[\sqrt{-3}]$ les inversibles. On suppose qu'il est entier sur $\mathbf{Z}[\sqrt{-3}]$. Soit $P = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ un polynôme annulateur dans $\mathbf{Z}[\sqrt{-3}][X]$. On obtient $p^d = -a_{d-1}p^{d-1}q - \cdots - a_1pq^{q-1} - a_0q^d$ et donc q divise p^d dans $\mathbf{Z}[\sqrt{-3}]$. Peut-on en déduire que q est inversible dans $\mathbf{Z}[\sqrt{-3}]$ et donc que a appartient à $\mathbf{Z}[\sqrt{-3}]$? Quel est l'anneau des entiers du corps $\mathbf{Q}(\sqrt{-3})$?

Exercice 4

1 Quelle est la norme sur le corps $\mathbf{Q}(\sqrt{-3})$? Quelle est la norme sur $\mathbf{Z}[j]$ exprimée dans la base $(1, j)$?

2 Montrer qu'un nombre premier est réductible dans $\mathbf{Z}[j]$ si et seulement s'il est la norme d'un élément de $\mathbf{Z}[j]$.

3 Les nombres 3, 11 et 13 sont-ils réductibles dans $\mathbf{Z}[j]$?

4 Montrer qu'un nombre premier p est réductible dans $\mathbf{Z}[j]$ si et seulement si $\mathbf{Z}[j]/(p)$ n'est pas intègre.

5 Montrer qu'un nombre premier $p > 3$ est réductible dans $\mathbf{Z}[j]$ si et seulement si X^2+X+1 admet une racine dans $\mathbf{F}_p$ si et seulement si le groupe multiplicatif $\mathbf{F}_p^\star$ des inversibles de $\mathbf{F}_p$ a un élément d'ordre 3.

6 Montrer qu'un entier p est réductible dans $\mathbf{Z}[j]$ si et seulement si $p = 1[3]$.

2. EQUATIONS DIOPHANTIENNES

Exercice 5

1 Donner toutes les solutions dans $\mathbf{Z}^2$ des équations suivantes :

$$x^2 + 2y^2 = 6, \quad x^2 + y^2 = 11, \quad x^2 - 6y^2 = -1.$$

2 On admet que l'anneau $\mathbf{Z}[i\sqrt{2}]$ est euclidien (donc factoriel). Factoriser 6 dans l'anneau $\mathbf{Z}[i\sqrt{2}]$ en produit de facteurs irréductibles et retrouver les solutions dans $\mathbf{N}^2$ de l'équation $x^2 + 2y^2 = 6$.

3 A l'aide de l'exercice 2, déterminer deux solutions de l'équation $x^2 + 3y^2 = 16$ dans $\mathbf{N}^2$.

Exercice 6

Le but de cet exercice est de montrer que $(3,5)$ et $(3,-5)$ sont les seules solutions entières de l'équation $y^2+2=x^3$. On admet que l'anneau $\mathbf{Z}[i\sqrt{2}]$ est euclidien (donc factoriel).

1 Montrer que les inversibles de cet anneau sont des cubes.

2 Montrer que si le couple (x,y) est solution, la norme de $y+i\sqrt{2}$ est impaire et les seuls diviseurs communs à $y+i\sqrt{2}$ et $y-i\sqrt{2}$ sont les inversibles.

3 En déduire que si $(x,y)\in\mathbf{Z}^2$ est une solution de l'équation, il existe des entiers a et b vérifiant $y+i\sqrt{2}=(a+ib\sqrt{2})^3$.

4 Conclure.

3. Discriminants

Exercice 7

Soit P un polynôme unitaire de $\mathbf{Q}[X]$ de degré n. Soit L une extension finie de $\mathbf{Q}$ telle que le polynôme P est scindé dans $L[X]$ et s'écrit donc $P=\Pi_{i=1}^{n}(X-\alpha_i)\in L[X]$ avec les α_i dans L comptées avec multiplicités. Soit $A=L[X]/(P)$ comme L-algèbre et $x=[X]\in A$.

1 Montrer que les éléments de A

$$e_0=1\ ,\ e_1=(x-\alpha_1)\ ,\ e_2=(x-\alpha_1)(x-\alpha_2)$$

$$e_3=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots e_{n-1}=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})$$

forment une L-base $\mathcal{B}$ de A.

2 Soit $a=h(x)$ (avec $h\in L[X]$) un élément de A. La trace $Tr_{A/L}(a)$ et de la norme $N_{A/L}(a)$ de a sur L sont par définition la somme et le produit des images de a par les n morphismes de L-algèbres unitaires de A dans L. Expliciter cette définition à l'aide de h et des α_i.

3 On considère

$$\begin{array}{rccc} m_a: & A & \to & A \\ & b & \mapsto & ab \end{array}$$

Montrer que m_a est un endomorphisme L-linéaire du L-espace vectoriel A. Déterminer la matrice de m_x dans la base $\mathcal{B}$. En déduire que pour tout $a\in L$, la matrice de m_a dans la base $\mathcal{B}$ est triangulaire inférieure. Déterminer pour tout $a\in L$, la trace $Tr_{A/L}(a)$ et de la norme $N_{A/L}(a)$ de a en fonction de m_a.

4 Si z est un élément $\mathbf{Q}[X]/(P)\subset L[X]/(P)$, comparer la trace du L endomorphisme $m_z\ :\ A\to A$ et celle du $\mathbf{Q}$ endomorphisme de $m_z\ :\ \mathbf{Q}[X]/(P)\to\mathbf{Q}[X]/(P)$.

5 Soit $P\in\mathbf{Q}[X]$ un polynôme unitaire irréductible de degré n et $K=\mathbf{Q}[X]/(P)$ le corps de nombres associé. Soit k un élément de K. Montrer que $Tr_{K/\mathbf{Q}}(k)$ est la trace de l'endomorphisme de multiplication par k dans K.

Exercice 8

1 Soit A un anneau et E un A-module libre de rang n muni d'une forme bilinéaire symétrique T. Rappeler la définition du discriminant $\Delta(T,\mathcal{B})$ de T dans une base $\mathcal{B}$.

2 Soit A un anneau et B une A-algèbre qui est un A-module libre de rang n. Rappeler la définition de la trace $Tr_{B/A}(b)$ d'un élément b de B. Rappeler la définition de la forme bilinéaire symétrique "trace" $\tau_{B/A}$ sur le A-module B.

3 Soit A un anneau et B une A-algèbre qui est un A-module libre de rang n. Le discriminant $\Delta(B, \mathcal{B})$ de la base $\mathcal{B}$ est le discriminant de la forme trace dans la base $\mathcal{B}$. Si $A = \mathbf{Z}$, montrer qu'on peut définir le discriminant $\Delta(B)$ de B.
4 Soit $f \in A[X]$ et $B := A[X]/(f)$. Le discriminant Δ_f de f est par définition le discriminant de la forme trace $\tau_{B/A}$ dans la A-base $(1, [X], \cdots [X^{d-1}])$ de B. Calculer le discriminant de $X^2 + bX + c$ et celui de $X^3 + pX + q$.

Exercice 9

Soit $K = \mathbf{Q}[X]/(P)$ un corps de nombres (avec P unitaire irréductible de degré n dans $\mathbf{Q}[X]$). On note $x = [X]$ et $\theta_k = \sigma_k(x)$ les différentes images complexes de x.
1 Rappeler la définition du discriminant Δ_K de K. A-t-on $\Delta_P = \Delta_K$? A-t-on une relation de divisibilité entre ces deux quantités ?
2 Calculer $\sum_k \sigma_k(x^i)\sigma_k(x^j)$ et montrer que $\Delta_P = \det\left((\theta_k^i)_{\substack{1\le k\le n\\ 0\le i\le n-1}}\right)^2$ puis que

$$\Delta_P = \Pi_{\substack{1\le k,k\le n\\ k<l}}(\theta_k - \theta_l)^2 = (-1)^{\frac{n(n-1)}{2}}\Pi_1^n P'(\theta_k) = (-1)^{\frac{n(n-1)}{2}} N(P'(\theta)).$$

3 Montrer que si p est un entier qui divise Δ_P, alors P a une racine multiple dans $\mathbf{F}_p$.

Exercice 10

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

4. Anneaux d'entiers

Exercice 11

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

Exercice 12

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

Exercice 13

1 Calculer le discriminant de $\mathbf{Q}(\sqrt{3})$ et celui de $\mathbf{Q}(\sqrt{5})$.
2 Montrer que $\zeta = \sqrt{3} + \frac{1+\sqrt{5}}{2}$ est un élément primitif de $\mathbf{Q}(\sqrt{3}, \sqrt{5})$.
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 $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ puis le polynôme minimal μ_ζ de ζ sur $\mathbf{Z}$.
4 Calculer le discriminant de la base $\mathcal{B}$.

Exercice 14

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

1 Montrer que A est, comme $\mathbf{Z}$-module, libre de base $(1, \sqrt[3]{2}, \sqrt[3]{4})$.

2 Montrer que K est un corps. Préciser une base de K comme $\mathbf{Q}$-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.

5. Factorisation des polynômes (rappels)

Exercice 15

Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{Z}[X]$.

1 On suppose que P a une racine rationnelle non nulle x, avec $x = \frac{p}{q}$ et $\text{pgcd}(p,q) = 1$. 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 $n \in \mathbf{N}^*$. Montrer que $\sqrt{n}$ est soit un entier, soit un irrationnel.

Exercice 16

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

1 Montrer qu'un polynôme constant a est irréductible dans $\mathbf{Z}[X]$ si et seulement si la constante a est irréductible dans $\mathbf{Z}$.

2 Le polynôme $4X$ est-il irréductible dans $\mathbf{Z}[X]$? et dans $\mathbf{Q}[X]$? Montrer qu'un polynôme P de $\mathbf{Z}[X]$ primitif irréductible dans $\mathbf{Q}[X]$ l'est aussi dans $\mathbf{Z}[X]$.

3 Réciproquement, soit P de la forme $a_0 + a_1X + a_2X^2 + X^3 \in \mathbf{Z}[X]$. Montrer que si P est irréductible dans $\mathbf{Z}[X]$ alors il l'est dans $\mathbf{Q}[X]$.

4 Soit f et g deux polynômes primitifs de $\mathbf{Z}[X]$. Montrer que leur produit fg est primitif.

5 Montrer qu'un polynôme de $\mathbf{Z}[X]$ de degré strictement positif irréductible dans $\mathbf{Z}[X]$ (donc primitif) est irréductible dans $\mathbf{Q}[X]$.

Plus généralement, on peut montrer que si A est un anneau factoriel et K son corps des fractions, les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes primitifs de A[X] qui sont irréductibles en tant que polynômes de $K[X]$.

Exercice 17

Soient p un nombre premier et $P \in \mathbf{Z}[X]$. On note $\bar{P}$ la réduction modulo p de P, c'est à dire l'élément de $\mathbf{Z}/p\mathbf{Z}[X]$ dont les coefficients sont les coefficients de P réduits modulo p.

1 Soit $P \in \mathbf{Z}[X]$ un polynôme unitaire. Montrer que si $\bar{P}$ est irréductible dans $\mathbf{Z}/p\mathbf{Z}[X]$, alors P est irréductible dans $\mathbf{Z}[X]$.

2 Le polynôme $X^3 - X - 1$ est-il irréductible dans $\mathbf{Q}[X]$?

3 Montrer que $X^2 + 4$ est irréductible dans $\mathbf{Z}[X]$ mais réductible dans $\mathbf{Z}/2\mathbf{Z}[X]$.

Exercice 18

1 Enoncer le critère d'Eisenstein.

2 L'équation $X^5 + 6X^4 - 12$ a-t-elle des solutions dans $\mathbf{Z}$, dans $\mathbf{Q}$?