Théorie des nombres
FEUILLE DE TD N○2

Exercice 1

On considère l'anneau $A = \mathbf{Z}[i]$. Montrer que $(1-i)$ est irréductible dans A. Vérifier que l'on a dans A

$$5 = (2+i)(2-i) = (1+2i)(1-2i),$$

et que ceci ne contredit pas la factorialité de A.

Exercice 2

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

Exercice 3

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

Exercice 4

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

$$x^2 + 2y^2 = 6, \qquad x^2 + y^2 = 11,$$

$$x^2 - 6y^2 = -1.$$

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

Exercice 5

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

$$y + i\sqrt{2} = (a + ib\sqrt{2})^3.$$

Conclure.

Exercice 6

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

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

Exercice 7

Dans $A = \mathbf{Z}[i\sqrt{3}]$, on considère l'idéal I engendré par 2 et $1 + i\sqrt{3}$. Montrer que I est distinct de (2) et que $I^2 = (2).I$. En déduire que les idéaux de A ne se factorisent pas de manière unique en produit d'idéaux premiers. Montrer que I est l'unique idéal premier propre contenant (2). En déduire que (2) ne s'écrit pas comme produit d'idéaux premiers.

Exercice 8

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.

Exercice 9

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

1 On suppose que P a une racine rationnelle non nulle x, avec $x = \frac{p}{q}$ et $\mathrm{pgcd}(p, q) = 1$. 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 10

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

1 Soit $P \in \mathbf{Z}[X]$ primitif. Montrer que si P est irréductible dans $\mathbf{Q}[X]$ alors il l'est dans $\mathbf{Z}[X]$.

2 Soit P de la forme $a_0 + a_1 X + a_2 X^2 + X^3 \in \mathbf{Z}[X]$. Montrer que si P est irréductible dans $\mathbf{Z}[X]$ alors il l'est dans $\mathbf{Q}[X]$.

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

4 Soit h un polynôme primitif réductible dans $\mathbf{Q}[X]$. Montrer que h est réductible dans $\mathbf{Z}[X]$.

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 11

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 12

1 Enoncer le critère d'Eisenstein.

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