Feuille d'exercices n° 4

Anneaux factoriels, irréductibilité

Dans ce qui suit, si $x \in \mathbf{C}$ est racine d'un polynôme unitaire de degré 2 à coefficients dans $\mathbf{Z}$, on pose $\mathbf{Z}[x] = \{a + bx\,;\, a, b \in \mathbf{Z}\}$. Il s'agit d'un sous-anneau de $\mathbf{C}$, donc d'un anneau commutatif unitaire intègre.

Exercice 1.

(1) Rappeler pourquoi dans un anneau intègre tout élément premier (élément non nul engendrant un idéal premier) est irréductible, et pourquoi dans un anneau factoriel un élément est premier si et seulement s'il est irréductible.

(2) On considère l'anneau $A = \mathbf{Z}[i\sqrt{3}]$. À l'aide de la fonction $N : A \to \mathbf{N}$ définie par $N(z) = |z|^2$, déterminer $A^\times$.

(3) Montrer que 2 est un élément irréductible de A.

(4) L'anneau A est-il factoriel ?

Exercice 2. Soient A un anneau intègre et K son corps des fractions. Un élément $x \in K$ est dit entier sur A s'il existe un polynôme unitaire $P(X) \in A[X]$ tel que $P(x) = 0$. L'anneau A est dit intégralement clos si tout élément entier sur A appartient à A.

(1) Prouver que tout anneau factoriel est intégralement clos.

(2) Soit d un entier > 1 et sans facteur carré.

(a) Montrer que $\dfrac{1+\sqrt{d}}{2} \notin \mathbf{Z}[\sqrt{d}]$.

(b) Supposons $d \equiv 1 \bmod 4$. L'anneau $\mathbf{Z}[\sqrt{d}]$ est-il factoriel ?

Exercice 3.

(1) Soient A un anneau factoriel, $a, b, c \in A\backslash\{0\}$ et un entier $n \geqslant 2$. Montrer que si a et b sont premiers entre eux et si $ab = c^n$, alors il existe $a', b' \in A$ et $u, v \in A^\times$ tels que $a = ua'^n$ et $b = vb'^n$.

(2) Rappeler pourquoi $A = \mathbf{Z}[i]$ est factoriel.

(3) Déterminer $A^\times$.

(4) Soient $x, y \in \mathbf{Z}$ tels que $y^3 = x^2 + 1$.

(a) Montrer que x est pair et y est impair.

(b) Prouver que dans A, $x + i$ et $x - i$ sont premiers entre eux (on pourra montrer que si z est un diviseur commun de $x + i$ et $x - i$ dans A, alors $|z|^2$ divise 4 et $x^2 + 1$ dans $\mathbf{Z}$).

(5) En utilisant la question (1), déterminer tous les couples $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ vérifiant $y^3 = x^2 + 1$.

(6) En utilisant le même genre de raisonnement et un anneau A approprié, déterminer tous les couples $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ vérifiant $y^3 = x^2 + 2$.

Exercice 4.

(1) Soit p un nombre premier impair.

(a) Combien y a-t-il de carrés non nuls dans $\mathbf{Z}/p\mathbf{Z}$?

(b) En déduire que les carrés non nuls de $\mathbf{Z}/p\mathbf{Z}$ sont exactement les racines du polynôme $X^{\frac{p-1}{2}} - 1$.

(c) Montrer que -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $p \equiv 1 \bmod 4$.

(2) Soit p un nombre premier impair. Montrer que si p est somme de deux carrés dans $\mathbf{Z}$, alors $p \equiv 1 \bmod 4$.

(3) On se propose ici de démontrer la réciproque. Soit donc p premier vérifiant $p \equiv 1 \bmod 4$.

(a) Montrer qu'il existe $x \in \mathbf{Z}$ tel que $p \mid (x+i)(x-i)$ dans $\mathbf{Z}[i]$.

(b) En déduire que p n'est pas premier dans $\mathbf{Z}[i]$.

(c) Établir que p est somme de deux carrés dans $\mathbf{Z}$.

(4) Quels sont les premiers sommes de deux carrés dans $\mathbf{Z}$?

(5) Montrer qu'un entier $n \geqslant 2$ est somme de deux carrés si et seulement si les premiers congrus à -1 modulo 4 intervenant dans la décomposition en produit de facteurs premiers de n (s'il y en a) ont un exposant pair dans cette décomposition.

Exercice 5.

(1) Dresser la liste des polynômes irréductibles de degré $\leqslant 3$ de $\mathbf{Z}/2\mathbf{Z}[X]$.

(2) Le polynôme $X^6 + X + 1$ est-il irréductible dans $\mathbf{Z}/2\mathbf{Z}[X]$?

(3) Que dire du polynôme $X^6 - 2001X + 2023$ dans $\mathbf{Z}[X]$? Dans $\mathbf{Q}[X]$?

Exercice 6.

(1) Montrer que pour tout entier $n \geqslant 1$ il existe dans $\mathbf{Z}[X]$ des polynômes irréductibles dans $\mathbf{Z}[X]$ et $\mathbf{Q}[X]$ de degré n.

(2) Soit p un nombre premier. Montrer que $R(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible dans $\mathbf{Z}[X]$ et $\mathbf{Q}[X]$.

(3) Supposons $p \geqslant 4$ non premier. Montrer que $R(X)$ n'est irréductible ni dans $\mathbf{Z}[X]$ ni dans $\mathbf{Q}[X]$.

(4) Soit p un nombre premier. Pour quelles valeurs de p le polynôme $X^p + pX + p - 1$ est-il irréductible dans $\mathbf{Z}[X]$? Dans $\mathbf{Q}[X]$?

Exercice 7. Soit p un nombre premier impair.

(1) On note G l'ensemble des carrés non nuls de $\mathbf{Z}/p\mathbf{Z}$. Quel est le cardinal de G ?

(2) On note H l'ensemble des éléments non nuls de $\mathbf{Z}/p\mathbf{Z}$ qui ne sont pas des carrés. Quel est le cardinal de H ?

(3) Soit α un élément de H. Montrer que $\alpha G = H$.

(4) En déduire que si $(\alpha, \beta) \in H \times H$, alors $\alpha\beta \in G$.

(5) Soit $P(X) = X^4 - 10X^2 + 1$. Montrer que $P(X)$ est irréductible dans $\mathbf{Z}[X]$ et dans $\mathbf{Q}[X]$.

(6) Montrer que pour tout premier q, $P(X)$ est réductible dans $\mathbf{Z}/q\mathbf{Z}[X]$. Lorsque $q > 2$, on commencera par supposer que 2 est un carré modulo q, puis que 3 est un carré modulo q. Enfin, à l'aide de la question (4), on traitera le cas où ni 2 ni 3 ne sont des carrés modulo q.

(7) De même, montrer que $X^4 + 1$ est irréductible dans $\mathbf{Z}[X]$ mais réductible dans $\mathbf{Z}/q\mathbf{Z}[X]$ quel que soit q premier.

Exercice 8. Soient $A = \mathbf{Z}[i\sqrt{3}]$ et $P(X) = X^2 - X + 1 \in A[X]$.

(1) Montrer que $P(X)$ est irréductible dans $A[X]$.

(2) Soit K le corps des fractions de A. Montrer que dans $K[X]$, $P(X)$ n'est pas irréductible.

(3) Comment expliquer ce phénomène ?