Feuille d'exercices n° 3

Anneaux factoriels (1)

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 $A = \mathbb{Z}[i\sqrt{3}]$. À l'aide de la fonction $N : A \to \mathbb{N}$ 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. On considère l'idéal $I = (X^2 - Y^3)$ de $\mathbb{C}[X, Y]$ et on pose $A = \mathbb{C}[X, Y]/I$.

1) Montrer que tout élément de $\mathbb{C}[X, Y]$ est congru modulo I à un unique polynôme de la forme $XP(Y) + Q(Y)$ avec $P, Q \in \mathbb{C}[Y]$.

2) Construire un morphisme d'anneaux $f : \mathbb{C}[X, Y] \to \mathbb{C}[T]$ tel que $\ker f = I$. En déduire que l'anneau A est intègre.

3) On note x et y les projections de X et Y dans A. Prouver que $y \neq 0$, que $y \notin A^\times$ et que $x \notin (y)$.

4) Établir que y est irréductible et conclure que l'anneau A n'est pas factoriel.

Exercice 3. 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 $\dfrac{1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$.

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

Exercice 4.

1) Soient A un anneau factoriel, $a, b, c \in A \setminus \{0\}$ 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 $A = \mathbb{Z}[i]$ est factoriel.

3) Déterminer $A^\times$.

4) Soient $x, y \in \mathbb{Z}$ 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 $\mathbb{Z}$).

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

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

Exercice 5.

1) Soit p un nombre premier impair.

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

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

(c) Montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ 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 $\mathbb{Z}$, 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 $x \in \mathbb{Z}$ tel que $p \mid (x + i)(x - i)$ dans $\mathbb{Z}[i]$.

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

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

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

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.