

Anneaux factoriels.

Soit A un anneau commutatif (unitaire).

Exercice 1. 1 Rappeler les définitions d'élément irréductible, premier et le lien entre ces deux notions dans un anneau intègre, dans un anneau factoriel. Que se passe-t-il si A est principal ?

2 Montrer que si A est intègre $p \in A \setminus \{0\}$ est irréductible si et seulement si (p) est maximal dans l'ensemble des idéaux propres *principaux* de A .

3 Montrer que $\mathbb{Z}[X]$ n'est pas principal. Est-il factoriel ?

Exercice 2. Soit $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

1 Montrer que $\mathbb{Z}[i]$ est un anneau commutatif unitaire.

2 Pour $z = a + ib \in \mathbb{C}$ on pose $N(z) = a^2 + b^2$. Montrer que $N(z) = z \cdot \bar{z}$. En déduire que $N(z_1 z_2) = N(z_1)N(z_2)$.

3 Déterminer le groupe des unités de $\mathbb{Z}[i]$.

4 Soit $(a, b) \in \mathbb{Z}[i]^2$ avec $b \neq 0$. Montrer qu'il existe $(q, r) \in \mathbb{Z}[i]^2$ tel que $a = bq + r$ avec $N(r) < N(b)$. Un tel couple est-il unique ?

5 Montrer que $\mathbb{Z}[i]$ est principal.

6 Montrer que si $N(\pi)$ est un nombre premier alors π est irréductible. Factorisez 2 dans $\mathbb{Z}[i]$.

Exercice 3. Soient a et b deux éléments d'un anneau intègre A .

1 Si a et b admettent un pgcd δ montrer que pour tout diviseur commun d de a et b , a/d et b/d admettent un pgcd qui vaut δ/d .

2 Si a et b admettent un ppcm μ alors pour tout $c \in A$, $\text{ppcm}(ac, bc)$ existe et vaut μc .

3 Montrer que a et b admettent un ppcm μ si et seulement si $(a) \cap (b)$ est principal. Dans ce cas on a $(a) \cap (b) = (\mu)$.

4 Prouver que si a et b admettent un ppcm alors ils admettent un pgcd égal à $ab/\text{ppcm}(a, b)$.

5 On prend $A = \mathbb{Z}[i\sqrt{5}]$.

5-a Montrer que 9 et $6 + i3\sqrt{5}$ n'ont pas de pgcd.

5-b Montrer que $2 + i\sqrt{5}$ et 3 ont un pgcd mais pas de ppcm.

5-c Que peut-on dire de A ?

Exercice 4. On étudie l'équation

$$X^2 = Y^3 - 1 \tag{1}$$

dans \mathbb{Z} . Soit $(x, y) \in \mathbb{Z}^2$ solution de cette équation. On écrira $(x + i)(x - i) = y^3$.

1 Soit $d = \text{pgcd}(x - i, x + i)$. Montrez que d divise 2.

2 Décomposez 2 en produit de facteurs irréductibles dans $\mathbb{Z}[i]$.

3 Montrez que si $d \notin \mathbb{Z}[i]^\times$ alors $y \equiv 0[2]$.

4 Montrez que la congruence $u^2 \equiv -1[8]$ n'a pas de solutions dans \mathbb{Z} .

5 En déduire que $d = 1$.

6 Montrez qu'il existe $a + ib \in \mathbb{Z}[i]$ tel que $x + i = (a + bi)^3$.

7 Montrez que $3a^2b - b^3 = 1$.

8 Montrez que $(0, 1)$ est l'unique solution de (1).