

Propriétés arithmétiques des anneaux

- Exercice 1 [Quelques exemples].**
1. Déterminer tous les idéaux propres de l'anneau $A = \mathbb{Z}/180\mathbb{Z}$ et donner les inclusions les uns par rapport aux autres. Déterminer les idéaux premiers, les idéaux maximaux.
 2. Soit $A = \mathcal{C}([0, 1], \mathbb{R})$ l'anneau des fonctions continues de $[0, 1]$ dans $\mathbb{R}$ et soit I le sous-ensemble de A de fonctions qui s'annulent en $1/2$. Montrer que I est idéal premier de A . Est-il maximal ?
 3. Soient E un espace vectoriel et F un sous-espace vectoriel de E . On considère

$$I = \{f \in \text{End}(E) \text{ tel que } \text{Im}(f) \subset F\} \quad \text{et} \quad J = \{f \in \text{End}(E) \text{ tel que } F \subset \text{Ker}(f)\}.$$

Montrer que I est un idéal à droite principal et J est un idéal à gauche principal de $\text{End}(E)$.

- Exercice 2 [Idéaux premiers, idéaux maximaux].**
1. Parmi les idéaux $(2X)$, (X, Y) et $(2, X, Y)$ de $\mathbb{Z}[X, Y]$, lesquels sont premiers ? maximaux ?
 2. Soit A un anneau intègre. Montrer que si A contient un nombre fini d'idéaux alors A est un corps (on pourra considérer les idéaux de la forme (a^n)).
 3. Soit A un anneau commutatif. Montrer que si A contient un nombre fini d'idéaux alors tout idéal premier est maximal.
 4. Soit A un anneau intègre tel que tout idéal est premier. Montrer que A est un corps (on pourra considérer les idéaux de la forme (x^2)).

- Exercice 3 [Quelques idéaux non principaux].**
1. Montrer que $(2, X)$ n'est pas un idéal principal de $\mathbb{Z}[X]$.
A quoi est isomorphe $\mathbb{Z}[X]/(2, X)$?
 2. Montrer que (X, Y) n'est pas un idéal principal de $A[X, Y]$.
 3. Soit $a \in A$. Montrer que $A[X]/(X - a)$ est isomorphe à A .

Exercice 4 [Lemme chinois]. Soit A un anneau, I et J deux idéaux de A .

1. Soit I et J deux idéaux de A premiers entre eux (c'est à dire $I + J = A$). Montrer qu'alors $IJ = I \cap J$. Montrer que cette égalité n'est pas forcément vraie si on ne suppose plus les idéaux premiers entre eux.
2. Montrer que A/IJ est isomorphe à $A/I \times A/J$.
3. Soit $I_1, \dots, I_n$ des idéaux de A premiers entre eux deux à deux. Montrer que $A/(I_1 \dots I_n)$ est isomorphe à $A/I_1 \times \dots \times A/I_n$ (commencer par $n = 2$).

Exercice 5. Soit A un anneau, I un idéal de A . Montrer :

- I est premier si et seulement si A/I est intègre ;
- I est maximal si et seulement si A/I est un corps.

- Exercice 6 [Premier vs irréductible].**
1. Soit A un anneau intègre. Un élément $a \in A$ est premier si l'idéal (a) est premier. Montrer qu'un élément premier de A est nécessairement irréductible.
 2. Soit A un anneau factoriel. Montrer que tout élément irréductible est premier.
 3. Soit A l'anneau $\mathbb{Z}[i\sqrt{5}]$.
 - (a) Vérifier que chacun des éléments $2, 3, 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ est irréductible.
 - (b) Montrer qu'aucun de ces éléments n'est premier (Vérifier l'égalité $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$).

Exercice 7 [Entiers de Gauss]. Soit $\mathbb{Z}[i]$ le sous-ensemble de $\mathbb{C}$ constitué des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbb{Z}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ appelé l'anneau des entiers de Gauss.
2. Montrer que la norme $N : \mathbb{Z}[i] \rightarrow \mathbb{N}$ définie par $N(a + ib) = a^2 + b^2$ est multiplicative.
3. Quelle est la structure de groupe de $(\mathbb{Z}[i])^\times$?
4. Montrer que $\mathbb{Z}[i]$ est un anneau euclidien munit de la norme N .
5. Déterminer le pgcd dans $\mathbb{Z}[i]$ de $19 + 4i$ et $13 - i$.
6. Soit α un élément non inversible de $\mathbb{Z}[i]$, montrer que si $N(\alpha)$ est premier dans $\mathbb{Z}$ alors α est irréductible dans $\mathbb{Z}[i]$.
7. Montrer si m et n sont tous deux sommes de deux carrés d'entiers, alors mn est somme de deux carrés également.
8. Soit p un entier premier. Montrer que p est une somme de deux carrés si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.
9. Soit p un entier premier. Montrer que les anneaux $\mathbb{Z}[i]/(p)$ et $\mathbb{F}_p[X]/(X^2 + 1)$ sont isomorphes. En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.
10. Soit p un entier premier. Déduire de ce qui précède que p est une somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.
11. Démontrer le théorème des deux carrés : soit n un entier naturel et $n = p_1^{v_{p_1}(n)} \dots p_k^{v_{p_k}(n)}$ sa décomposition en facteurs premiers. Alors n est somme de deux carrés d'entiers si et seulement si $v_p(n)$ est pair pour tout entier premier p tel que $p \equiv 3 \pmod{4}$.

Exercice 8 [Anneau principal non euclidien]. Soit $\alpha = \frac{1+i\sqrt{19}}{2}$. On note $A = \mathbb{Z}[\alpha]$. On se propose de montrer que A est principal, mais pas euclidien.

1. Si $a \in A$, on note $N(a) = |a|^2$. Vérifier que N est une application multiplicative. Vérifier que si $a = u + v\alpha$, $u, v \in \mathbb{Z}$, alors $N(a) = u^2 + uv + 5v^2$. Quelles sont les unités de A ?
2. Montrer que α vérifie $\alpha^2 - \alpha + 5 = 0$. En déduire que A est isomorphe à $\mathbb{Z}[X]/(X^2 - X + 5)$. Soit B un anneau, montrer qu'il existe un morphisme de A dans B si et seulement si il existe $b \in B$ vérifiant $b^2 - b + 5 = 0$. En déduire qu'il n'existe pas de morphisme de A dans $\mathbb{Z}/2\mathbb{Z}$ ni dans $\mathbb{Z}/3\mathbb{Z}$.
3. Montrer que si un anneau B est euclidien alors il existe $x \in B \setminus B^\times$ tel que la restriction à $B^\times \cup \{0\}$ de la projection canonique de B sur $B/(x)$ soit surjective.
4. En déduire que A n'est pas euclidien.
5. Soit a et b dans A . Montrer que l'une des situations suivantes est réalisée :
 - (a) il existe q et r dans A , avec $r = 0$ ou $N(r) < N(b)$, et $a = bq + r$;
 - (b) il existe q et r dans A , avec $r = 0$ ou $N(r) < N(b)$, et $2a = bq + r$.
 On a donc une pseudo-division euclidienne sur A .
6. Montrer que (2) est un idéal maximal de A .
7. Soit I un idéal non nul de A , montrer que I est principal.