TD2 : Théorie des anneaux

Exercice 1. Décrire le plus petit sous-anneau de $\mathbb{C}$ contenant $i \in \mathbb{C}$.

Exercice 2. Soit A un anneau et $I, J \subset A$ des idéaux.

a) Démontrer que les sous-ensembles suivants sont des idéaux de A :

$$I \cap J, \qquad I + J = \{x + y \mid x \in I,\ y \in J\}, \qquad IJ = \{x_1 y_1 + \cdots + x_n y_n \mid x_i, y_i \in I\}.$$

b) Quelles relations d'inclusions existent entre $I, J, I \cap J, I + J$ et IJ ?

c) Dans le cas où $A = \mathbb{Z}$, $I = m\mathbb{Z}$ et $J = n\mathbb{Z}$ (avec $m, n \in \mathbb{Z}$), décrire ces idéaux.

Exercice 3. Soit A un anneau et $a \in A$. Démontrer que l'unique morphisme $\mathbb{Z}[X] \to A$ tel que $X \mapsto a$ est donné par $P \mapsto P(a)$.

Exercice 4. Soit A un anneau et $I_1, \ldots, I_n \subset A$ des idéaux non-triviaux tels que si $i \neq j$ alors $I_i + I_j = A$.

a) Donner un exemple pour $A = \mathbb{Z}$ et $n = 3$.

b) Démontrer que pour tous $x_1, \ldots, x_n \in A$, il existe $x \in A$ tel que $x \equiv x_i \pmod{I_i}$ pour tout i.

c) Démontrer que $A/(I_1 \cap \ldots \cap I_n) \cong (A/I_1) \times \ldots \times (A/I_n)$.

Exercice 5. Soit A un anneau et $I \subset A$ un idéal.

a) Démontrer que les idéaux de A/I sont de la forme J/I avec $I \subset J \subset A$ un idéal, et que l'on a $(A/I)/(J/I) \cong A/J$.

b) Soit $B \subset A$ un sous-anneau de A. Démontrer que $B + I$ est un sous-anneau de A et que I est un idéal de $B + I$.

c) Démontrer que $B \cap I$ est un idéal de A et que $(B + I)/I \cong B/(B \cap I)$.

Exercice 6. Démontrer que les applications suivantes sont des morphismes d'anneaux et déterminer des générateurs de leurs noyaux respectifs :

a) $f: \mathbb{K}[X] \to \mathbb{K},\ f(P) := P(a)$, où $\mathbb{K}$ est un corps et $a \in \mathbb{K}$.

b) $g: \mathbb{R}[X] \to \mathbb{C},\ g(P) := P(i)$.

c) $h: \mathbb{Z}[X] \to (\mathbb{Z}/n\mathbb{Z})[X],\ h(P) := P$, où $n \in \mathbb{Z}$.

d) $j: \mathbb{Q}[X, Y] \to \mathbb{Q},\ j(P) := P(0, 1)$.

e) $k: \mathbb{R}[X, Y] \to \mathbb{R}[X],\ k(P) := P(X, X^2)$.

Exercice 7. Soit $\mathbb{K}$ un corps.

a) Démontrer que $\mathbb{K}[X, Y]/(X^2 + Y^2 - 1)$ est intègre lorsque $\mathrm{car}(\mathbb{K}) \neq 2$. Est-ce un corps ?

b) Démontrer que $\mathbb{Z}[X]/(2, X^4 + X + 1)$ est un corps.

c) Démontrer que $\mathbb{K}[X, Y]/(Y - X^2)$ est principal.

d) Démontrer que $\mathbb{K}[X, X^{-1}] := \mathbb{K}[X, Y]/(XY - 1)$ est principal.

Exercice 8. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non nul. Démontrer que $\mathbb{K}[X]/(P)$ est un $\mathbb{K}$-espace vectoriel de dimension $\deg(P)$.

Exercice 9. Soit $f : \mathbb{Z} \to \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ le morphisme canonique. Quel est le noyau et l'image de f ? Expliciter l'isomorphisme inverse $\mathrm{im}(f) \to \mathbb{Z}/\ker(f)$. Faire de même pour $\mathbb{Q}[X] \to \mathbb{Q}[X]/(X^3-2) \times \mathbb{Q}[X]/(X^2+1)$.

Exercice 10. Soit V un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathrm{End}(V)$, de polynôme minimal $\mu \in \mathbb{K}[X]$.

a) Décrire $\mathbb{K}[X]/(\mu)$ en termes d'endomorphismes de V.

b) Démontrer que l'anneau $\mathbb{K}[X]/(\mu)$ est principal.

Exercice 11. On pose $j \coloneqq \exp(2i\pi/3) \in \mathbb{C}$ et on note $\mathbb{Z}[j]$ (resp., $\mathbb{Q}[j]$) le sous-anneau (resp., sous-corps) de $\mathbb{C}$ contenant j.

a) Décrire les éléments de $\mathbb{Z}[j]$ et $\mathbb{Q}[j]$.

b) Démontrer que pour tout $z \in \mathbb{C}$, il existe $w \in \mathbb{Z}[j]$ tel que $|z - w| < 1$.

c) Démontrer que $\mathbb{Z}[j]$ est euclidien.

Exercice 12. Soit $\mathbb{K}$ un corps et $A = \mathbb{K}[X,Y]/(X^2, Y^2, XY)$.

a) Déterminer les éléments inversibles de A.

b) Déterminer les idéaux principaux de A.

c) Déterminer tous les idéaux de A.

Exercice 13. On considère la courbe $\mathcal{C} = \{\, (x,y) \in \mathbb{C}^2 \mid y^2 = x^3 \,\}$. On dit qu'une fonction $f : \mathcal{C} \to \mathbb{C}$ est polynômiale si c'est la restriction à $\mathcal{C}$ d'une fonction polynômiale $\mathbb{C}^2 \to \mathbb{C}$.

a) Démontrer que l'ensemble A des fonctions polynômiales sur $\mathcal{C}$ forme un anneau.

b) Démontrer que A est isomorphe à l'anneau :

$$\mathbb{C}[T^2, T^3] \coloneqq \{\, P(T^2, T^3) \mid P \in \mathbb{C}[X,Y] \,\} \subset \mathbb{C}[T].$$

On pourra utiliser la paramétrisation $\mathcal{C} = \{\, (t^2, t^3) \mid t \in \mathbb{C} \,\}$. Décrire les éléments de $\mathbb{C}[T^2, T^3]$.

c) Démontrer que A est intègre.

d) Démontrer que les fonctions $\alpha, \beta \in A$ sont des éléments irréductibles de A :

$$\alpha(x,y) \coloneqq x, \qquad \beta(x,y) \coloneqq y.$$

e) Soit $J = \{\, f \in A \mid f(0,0) = 0 \,\}$. Démontrer que J est un idéal de A et déterminer une famille génératrice. Démontrer que A n'est pas principal.

f) Démontrer que $A/J \cong \mathbb{C}$.

g) Démontrer que $A \cong \mathbb{C}[X,Y]/(Y^2 - X^3)$. Est-ce que cet anneau quotient est principal, euclidien ?

h) Est-ce que A est factoriel ?

Exercice 14. Soit $A = \{\, x + iy\sqrt{5} \mid x, y \in \mathbb{Z} \,\}$. Étant donné $z \in A$, on note sa norme $N(z) \coloneqq z\bar{z}$.

a) Démontrer que les éléments inversibles de A sont exactement les éléments de norme 1.

b) Démontrer que tous les éléments de norme 9 sont irréductibles.

c) Démontrer que A n'est pas factoriel. Indication : considérer des produits d'éléments de norme 9 bien choisis.

Exercice 15. On note $\xi = (1 + i\sqrt{19})/2$ et on note $\mathbb{Z}[\xi]$ le sous-anneau de $\mathbb{C}$ engendré par ξ.

a) Démontrer que tout élément de $\mathbb{Z}[\xi]$ s'écrit de manière unique sous la forme $x + y\xi$ avec $x, y \in \mathbb{Z}$.

b) Démontrer que pour tout $z \in \mathbb{Z}[\xi]$, le conjugué $\bar{z}$ appartient à $\mathbb{Z}[X]$ et que la norme $z\bar{z}$ est un entier.

c) Démontrer que $\mathbb{Z}[\xi]$ est intègre.

d) Démontrer que $z \in \mathbb{Z}[\xi]$ est inversible si et seulement si $z\bar{z} = 1$.

e) Étant donnés $x, y \in \mathbb{Z}$, démontrer que $x^2 + xy + 5y^2 \geq 4y^2$. En déduire que $\mathbb{Z}[\xi]^\times = \{\pm 1\}$.

f) Démontrer que $\mathbb{Z}[\xi]$ est isomorphe à $\mathbb{Z}[X]/(X^2 - X + 5)$.

Exercice 16. Soit $d \in \mathbb{Z}$ un entier sans facteur carré.

a) Démontrer que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $\mathbb{C}$. À quelle condition est-ce un réseau de $\mathbb{C}$?

b) On suppose désormais que $d < 0$. Démontrer que $\nu(z) \coloneqq z\bar{z}$ est multiplicative et à valeurs dans $\mathbb{N}$.

c) Démontrer que ν est un stathme euclidien si et seulement si pour tout $z \in \mathbb{Q}[\sqrt{d}]$, la boule unité centrée en z rencontre un point de $\mathbb{Z}[\sqrt{d}]$.

d) Démontrer que cela n'est le cas que si $d = -1$ ou $d = -2$.

Exercice 17. Soit p un nombre premier impair. On rappelle que $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ est un anneau euclidien.

a) Démontrer que s'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$, alors $p \equiv 1 \pmod 4$.

b) On suppose désormais que $p \equiv 1 \pmod 4$. Démontrer qu'il existe $\alpha \in \mathbb{Z}$ tel que $\alpha^2 \equiv -1 \pmod p$.

c) Démontrer que la fonction suivante définit un morphisme d'anneaux :

$$\mathbb{Z}[i] \to (\mathbb{Z}/p\mathbb{Z})^2, \qquad a + bi \mapsto (a + \alpha b, a - \alpha b).$$

Déterminer son noyau et son image.

d) En déduire que p est réductible dans $\mathbb{Z}[i]$ et qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

Exercice 18. (Anneau des entiers de Gauss.)

a) Démontrer que $1 + i$ est irréductible dans $\mathbb{Z}[i]$. Factoriser $2 \in \mathbb{Z}[i]$. Est-ce que les irréductibles qui apparaissent sont associés ?

b) Soit $p \equiv 3 \pmod 4$ un nombre premier. Démontrer que p est irréductible dans $\mathbb{Z}[i]$.

c) Soit $p \equiv 1 \pmod 1$ un nombre premier. Démontrer que $p = \alpha\bar{\alpha}$ avec $\alpha \in \mathbb{Z}[i]$ irréductible et que α et $\bar{\alpha}$ ne sont pas associés.

d) Soit $\alpha \in \mathbb{Z}[i]$ irréductible et $(\alpha) \subset \mathbb{Z}[i]$ l'idéal engendré par α. Démontrer que $\mathbb{Z} \cap (\alpha) = p\mathbb{Z}$ pour un nombre premier p, et que p est le seul nombre premier divisible par α dans $\mathbb{Z}[i]$.

e) En déduire que les irréductibles de $\mathbb{Z}[i]$ sont les nombres premiers p congrus à 3 mod 4 et les entiers de Gauss de la forme $\alpha = x + iy$ avec $x^2 + y^2$ premier.

f) Factoriser $-3 + 15i$ dans $\mathbb{Z}[i]$.

Exercice 19. Soit $p \in \mathbb{Z}$ un nombre premier. Combien existe-t-il de couples $(a, b) \in \mathbb{Z}^2$ tels que $p = a^2 + b^2$?

Exercice 20. (Évaluation 2020) Soit $A = \mathbb{Z}[i]$ l'anneau des entiers de Gauss.

a) Faire la division euclidienne de $6 + 8i$ par $1 + 5i$.

b) En déduire le PGCD de $6 + 8i$ et $1 + 5i$.

c) Proposer une autre méthode pour calculer ce PGCD.

Exercice 21. (Évaluation 2020) Soit $A = \{ P \in \mathbb{R}[X] \mid P'(0) = 0 \}$.

a) Démontrer que A est un anneau intègre.

b) Quels sont les éléments inversibles de A ?

c) Démontrer que X^2 et X^3 appartiennent à A. Est-ce que X^2 divise X^3 dans A ?

d) Démontrer que X^2 et X^3 sont irréductibles dans A.

e) Démontrer que A n'est pas factoriel.

f) L'idéal de A engendré par X^2 est-il premier ?

Exercice 22. (Évaluation 2021) Soit A un anneau commutatif. Le nilradical de A, noté $\mathrm{Nil}(A)$, est l'ensemble des éléments nilpotents $\{ a \in A \mid \exists m \in \mathbb{N},\ a^m = 0 \}$.

a) Que vaut $\mathrm{Nil}(A)$ lorsque A est intègre ?

b) Démontrer que $\mathrm{Nil}(A)$ est un idéal de A.

c) Démontrer que pour tout $a \in A, k \in \mathbb{N}$, $1 - a$ divise $1 - a^k$.

d) Soit $a \in \mathrm{Nil}(A)$. Démontrer que $1 - a \in A^\times$ et en déduire que pour tout $u \in A^\times$, $u + a \in A^\times$.

e) Démontrer que $\mathrm{Nil}(A) \subset \mathrm{Nil}(A[X])$.

f) Soit $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polynôme. Démontrer que $P \in \mathrm{Nil}(A[X])$ si et seulement si $a_0, a_1, \dots, a_n \in \mathrm{Nil}(A)$.

g) Soit $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polynôme. Démontrer que $P \in A[X]^\times$ si et seulement si $a_0 \in A^\times$ et $a_1, \dots, a_n \in \mathrm{Nil}(A)$.

Exercice 23. Soit A un anneau, que l'on ne suppose pas nécessairement commutatif. On dit que $a \in A$ est idempotent si $a^2 = a$. On suppose que tous les éléments de A sont idempotents.

a) Démontrer que A est commutatif et que sa caractéristique vaut 2.

b) Donner un exemple d'un tel anneau A.

c) Dans quel cas A est-il intègre ?

d) Démontrer qu'on peut munir A d'une structure d'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$. En déduire que si A est fini, alors il existe $n \in \mathbb{N}$ tel que $|A| = 2^n$.

e) On suppose maintenant que A est un anneau commutatif quelconque, et que $A = A_1 \times A_2$ pour des anneaux $A_1, A_2 \neq \{0\}$. Démontrer que A possède au moins quatre éléments idempotents.