TD1 : Révisions sur les anneaux

Exercice 1. Anneau des décimaux

1. Montrer que $10X-1$ est irréductible dans $\mathbb{Z}[X]$.

On note $\mathbb{D}$ l'anneau des décimaux, i.e. l'ensemble des réels ayant un développement fini.

2. Montrer $\mathbb{D}$ est un anneau. Est-ce un corps ?
3. Montrer que $\mathbb{D}=\mathbb{Z}[1/10]$, i.e. est égal au plus petit sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$ et $1/10$.
4. Montrer que $\mathbb{D} \simeq \mathbb{Z}[X]/(10X-1)$.
5. L'idéal $(10X-1)$ de $\mathbb{Z}[X]$ est-il premier ? maximal ? Le cas échéant, trouver un idéal propre de $\mathbb{Z}[X]$ contenant $(10X-1)$. Indication : on pourra montrer que si un tel idéal existe, il ne peut être principal.
6. Montrer que $\mathbb{D}$ est principal.

Exercice 2. Morphismes d'anneaux et idéaux

Soit $f : A \to B$ un morphisme d'anneaux.

1. Montrer que si K est un idéal de B, alors $f^{-1}(K)$ est un idéal de A.
2. Montrer que si J est un idéal de A et f est surjective, alors $f(J)$ est un idéal de B.

Exercice 3. Idéaux d'un anneau quotient

Soit I un idéal d'un anneau commutatif A et $\pi : A \to A/I$ le morphisme quotient.

1. Montrer que l'application image réciproque $\pi^{-1} : \mathcal{P}(A/I) \to \mathcal{P}(A)$, où $\mathcal{P}(E)$ désigne l'ensemble des parties de l'ensemble E, réalise une bijection entre l'ensemble des idéaux de A/I et l'ensemble des idéaux de A contenant I.

   Par abus de notation, on notera par la suite J/I l'idéal $\pi(J)$.
2. Montrer que si J est un idéal de A contenant I, alors $(A/I)/(J/I)$ est isomorphe à A/J.
3. Montrer que A/I est un corps si et seulement si I est maximal.
4. Si A est principal, montrer que tout idéal de A/I est principal.
5. Donner la liste des idéaux de $\mathbb{Z}/n\mathbb{Z}$, où n est un entier strictement positif.

Exercice 4.

Soit A un anneau commutatif intègre. Montrer que $A[X]$ principal si et seulement si A est un corps.

Exercice 5. Anneau local

On appelle anneau (commutatif) local un anneau commutatif ayant un unique idéal maximal. On appelle corps résiduel d'un anneau local son quotient par l'unique idéal maximal.

1. Soit A un anneau local d'idéal maximal M. Montrer que M est égal à $A \setminus A^{\times}$, l'ensemble des éléments non inversibles de A. Indication : utiliser le théorème de Krull (tout idéal propre d'un anneau est contenu dans un idéal maximal).
2. Réciproquement, montrer qu'un anneau non nul A est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal, et si et seulement si la somme de deux éléments non inversibles n'est jamais inversible.

Exemple d'anneau local : soit $K[X]$ l'anneau des polynômes à une indéterminée sur un corps K et $R \in K[X]$ un polynôme irréductible. On considère

$$A = \left\{ \frac{P}{Q} : R \nmid Q \right\}.$$

3. Montrer que A est un sous-anneau du corps des fractions rationnelles à une indéterminée $K(X)$ et qu'il est local d'idéal maximal RA.
4. Montrer que son corps résiduel est isomorphe à $K[X]/(R)$.

Exercice 6. Divisibilité et éléments associés

1. Soient A un anneau intègre et $a, b \in A$ tels que $a|b$ et $b|a$. Montrer que a et b sont fortement associés, i.e. qu'il existe un élément u inversible de A tel que $a = ub$.
2. Ceci n'est pas forcément vrai dans un anneau non intègre.
   Soit K un corps, on pose $A = K[X, Y, Z]/(X - XYZ)$. On note x, y, z les classes de X, Y, Z dans A.
   (a) Montrer que A n'est pas intègre.
   (b) Montrer que $x|xy$ et $xy|x$, i.e. x et xy sont associés.
   (c) Soit $u \in A$ tel que $xy = xu$. On cherche à montrer par l'absurde que u n'est pas inversible. On suppose que v est un inverse de u et on note respectivement U et V les représentants de u et v dans $K[X, Y, Z]$. En particulier, il existe $P, Q \in K[X, Y, Z]$ tels que $UV = 1 + X(1 - YZ)P$ et $Y = U + (1 - YZ)Q$.
   Montrer que $Y \cdot V(0, Y, Z) - 1 = (1 - YZ) \cdot Q(0, Y, Z) \cdot V(0, Y, Z)$ et en déduire une contradiction en raisonnant sur le degré de $V(0, Y, Z)$ par rapport Z.

Exercice 7. Diviseurs de zéro et éléments non inversibles

Soit A un anneau et $x \in A$ un élément non nul. On considère l'application $f : A \to A, a \mapsto xa$.

1. Montrer que f est injective si et seulement si x n'est pas un diviseur de 0.
2. Montrer que f est surjective si et seulement si x est inversible.
3. Montrer que si A est de cardinalité finie, alors tout élément non nul de A est soit inversible soit un diviseur de 0.
4. Même question lorsque A est une K-algèbre de dimension finie.
5. Donner un exemple d'anneau admettant des éléments non inversibles et non diviseurs de zéro.

Exercice 8. Anneaux $\mathbb{Z}[\sqrt{d}]$

Soit d un entier non carré.

1. Montrer que $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ est un anneau (où par convention $\sqrt{d} = i\sqrt{|d|}$ quand d est négatif) et qu'il est isomorphe à $\mathbb{Z}[X]/(X^2 - d)$.
2. Si $w = a + b\sqrt{d}$, on note $\bar{w} = a - b\sqrt{d}$. Montrer que $w \mapsto \bar{w}$ est un automorphisme de $\mathbb{Z}[\sqrt{d}]$.
3. On pose $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}, w = a + b\sqrt{d} \mapsto w\bar{w} = a^2 - db^2$.
   (a) Montrer que N est multiplicative, i.e. $N(xy) = N(x)N(y)$.
   (b) Montrer que $x \in \mathbb{Z}[\sqrt{d}]$ est inversible si et seulement si $N(x) = \pm 1$.
   (c) Montrer que si $N(x)$ est un nombre premier, alors x est irréductible. En considérant par exemple $3 \in \mathbb{Z}[i]$, montrer que la réciproque est fausse en général.
4. Déterminer $\mathbb{Z}[\sqrt{d}]^\times$ pour $d < 0$.

Exercice 9. Pgcd et ppcm

Soient a et b deux éléments d'un anneau commutatif intègre A. On rappelle que $d \in A$ est un pgcd de a et b si pour tout élément $c \in A$ tel que $c|a$ et $c|b$ on a $c|d$.
Similairement, on dit que $m \in A$ est un ppcm de a et b si pour tout élément $c \in A$ tel que $a|c$ et $b|c$ on a $m|c$.

1. On suppose que a et b admettent un pgcd d. Montrer que l'ensemble des pgcd de a et b est exactement l'ensemble des associés de d.
   Même question pour le ppcm.
2. On suppose que A est principal.
   (a) En considérant les ensembles $(a) + (b)$ et $(a) \cap (b)$, montrer que tout couple d'éléments de A possède un pgcd et un ppcm.
   (b) Soient $a, b \in A$. Déterminer l'ensemble des éléments $c \in A$ tels que l'équation $au + bv = c$ admette des solutions (u, v).
3. On prend $A = \mathbb{R}[X, Y]$. Déterminer un pgcd de X et Y. L'équation $uX + vY = 1$ admet-elle des solutions ?
4. On prend $A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$.
   (a) Vérifier que A est un sous-anneau de $\mathbb{C}$ (donc intègre).
   (b) Montrer que le carré du module de tout élément de A est un entier positif. En déduire que 2 est irréductible dans A.
   (c) Montrer qu'aucun multiple strict de 2 (dans A) ne divise à la fois 4 et $2 + 2i\sqrt{3}$.
   (d) Montrer que $1 + i\sqrt{3}$ divise à la fois 4 et $2 + 2i\sqrt{3}$. En déduire que 4 et $2 + 2i\sqrt{3}$ n'admettent pas de pgcd.

Exercice 10. Les entiers de Gauss. Application au théorème des deux carrés

Soit $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

1. Montrer que c'est un sous-anneau de $\mathbb{C}$ appelé l'anneau des entiers de Gauss.
2. On définit l'application norme $N : \mathbb{Z}[i] \to \mathbb{N}, z \mapsto z\bar{z}$.
   Montrer que N est une fonction multiplicative, puis déterminer les inversibles de l'anneau $\mathbb{Z}[i]$.
3. Montrer que $z \in \mathbb{C}$, il existe $w \in \mathbb{Z}[i]$ tel que $|z - w| < 1$.

4. Montrer que $\mathbb{Z}[i]$ est euclidien, i.e. qu'il existe une division euclidienne pour la norme N. Plus précisément, montrer que pour tout couple $a, b \in \mathbb{Z}[i], b \neq 0$, il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $N(r) < N(b)$.
5. En déduire que $\mathbb{Z}[i]$ est un anneau principal.

Classification des irréductibles de $\mathbb{Z}[i]$:

6. Soit p un entier premier. Montrer que les anneaux $\mathbb{Z}[i]/(p)$ et $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ sont isomorphes. En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, et donc si et seulement si $p = 3 \bmod 4$.
7. Soit p un entier premier non congru à 3 mod 4. En considérant la norme, montrer qu'il existe un élément irréductible π tel que $p = \pi\bar{\pi}$.
8. Soit π un élément irréductible de $\mathbb{Z}[i]$. Montrer que $(\pi) \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.
   En déduire que les irréductibles de $\mathbb{Z}[i]$ sont :
   — les nombres entiers premiers congrus à 3 mod 4 et leurs associés
   — les éléments dont la norme est un entier premier, non congru à 3 mod 4.

Théorème des deux carrés :

9. Soit p un entier premier. Déduire de ce qui précède que p est une somme de deux carrés si et seulement si $p = 1$ ou $2 \bmod 4$.
10. Montrer que si m et n sont tous deux sommes de deux carrés d'entiers, alors mn est somme de deux carrés également.
11. Démontrer le théorème des deux carrés : soit n un entier naturel et $n = \prod_p p^{v_p(n)}$ sa décomposition en facteurs premiers. Alors n est une somme de deux carrés d'entiers si et seulement si $v_p(n)$ est pair pour tout entier premier p tel que $p = 3 \bmod 4$.

Exercice 11. Fibonacci et $\mathbb{Z}[\varphi]$

On considère le sous-anneau A de $\mathbb{C}$ engendré par $\varphi = \dfrac{1+\sqrt{5}}{2}$:

$$A = \mathbb{Z}[\varphi] = \{P(\varphi) : P \in \mathbb{Z}[X]\}.$$

1. Vérifier que $\varphi^2 - \varphi + 1 = 0$. En déduire que $A = \{a + b\varphi : a, b \in \mathbb{Z}\}$.
2. On note $\bar{\varphi} = \dfrac{1-\sqrt{5}}{2} = 1 - \varphi$ et si $w = a + b\varphi \in A$, on note $\bar{w} = a + b\bar{\varphi}$. Montrer que $w \mapsto \bar{w}$ est un automorphisme de A.
3. On pose $N : A \to \mathbb{Z}, w = a + b\varphi \mapsto w\bar{w} = (a + b\varphi)(a - b\varphi)$.
   (a) Montrer que $x \in A$ est inversible si et seulement si $N(x) = \pm 1$.
   (b) Montrer que φ est inversible dans A d'inverse $-\bar{\varphi} = \varphi - 1$.
4. Soit (F_n) la suite de Fibonacci. On rappelle que cette suite est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$.
   (a) Montrer que pour tout $n \in \mathbb{N}^*$, $\varphi^n = F_{n-1} + F_n\varphi$.
   (b) En déduire que l'ensemble des inversibles de A est de cardinalité infinie.
   (c) En déduire que $\mathbb{Z}[\sqrt{5}]^\times$ est infini.

Exercice 12. Une équation diophantienne

Résoudre l'équation $y^3 - x^2 = 2$ dans $\mathbb{Z}$. Indication : utiliser le fait que $\mathbb{Z}[i\sqrt{2}]$ est euclidien et montrer que $x + i\sqrt{2}$ est nécessairement un cube dans $\mathbb{Z}[i\sqrt{2}]$.