TD n°4 : Anneaux de polynômes, anneaux factoriels

Dans ce TD, sauf mentionné, tous les anneaux et corps sont supposés commutatifs.

Exercice 1. [Questions diverses]

1. Un sous-anneau (respectivement quotient par un idéal premier) d'un anneau factoriel est-il aussi factoriel ?
2. Montrer que pour tout entier $n \geq 3$, l'anneau $\mathbb{Z}[i\sqrt{n}]$ n'est pas factoriel.
3. Trouver tous les éléments inversibles dans l'anneau $\mathbb{Z}[\sqrt{2}]$.

Exercice 2. Soit A un anneau commutatif unitaire.

1. Si $a, b \in A$, montrer que l'application $A[X,Y] \to A$ donnée par $P(X,Y) \mapsto P(a,b)$ est un morphisme d'anneaux.
2. Montrer que si $A = \mathbf{Q}$, alors tout morphisme $\mathbf{Q}[X,Y] \to \mathbf{Q}$ est de cette forme.
3. Montrer que si $A = \mathbf{C}$, alors il existe un morphisme $\mathbf{C}[X,Y] \to \mathbf{C}$ qui n'est pas de cette forme.
4. Décrire tous les morphismes d'anneaux $A[X,Y] \to A$.

Exercice 3. Pour tout entier $n \geqslant 1$, on note $U_n = \{e^{2ik\pi/n} \mid k \wedge n = 1\}$ l'ensemble des racines de l'unité n-ièmes primitives, et on définit le n-ième polynôme cyclotomique

$$\Phi_n(X) = \prod_{\zeta \in U_n} (X - \zeta) \in \mathbb{C}[X].$$

1. Montrer que le degré de $\Phi_n(X)$ est $\phi(n)$, l'indicatrice d'Euler de n.
2. Montrer que pour tout n on a
$$X^n - 1 = \prod_{d|n} \Phi_d(X),$$
et en déduire la formule $n = \sum_{d|n} \phi(d)$.
3. En déduire que $\Phi_n(X) \in \mathbb{Z}[X]$.
4. Pour $n = p$ un nombre premier, calculer explicitement $\Phi_p(X)$ et montrer que celui-ci est irréductible.

Exercice 4. [Équation de Mordell] Le but de cet exercice est de résoudre dans $\mathbb{Z}$ l'équation de Mordell $y^2 = x^3 - 2$.

1. Si A est un anneau factoriel et si a, b sont deux éléments de A premiers entre eux tels que $ab = c^n$ pour un certain $c \in A$ et $n \in \mathbb{N}$, montrer qu'il existe alors $u, v \in A^\times$ et $\alpha, \beta \in A$ tels que $a = u\alpha^n$ et $b = v\beta^n$.
2. Soit $(x,y) \in \mathbb{Z}^2$ une solution de l'équation de Mordell. Montrer que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$.
3. En déduire toutes les solutions dans $\mathbb{Z}^2$ de l'équation de Mordell.

Exercice 5. Soit K un corps infini. Montrer que si $P \in K[X,Y]$ est tel que $\forall x, y \in K, P(x,y) = 0$ alors $P = 0$.

Exercice 6. Le but de cet exercice est de déterminer la forme des idéaux premiers et maximaux de $\mathbb{Z}[X]$. Soit I un idéal premier.

1. Montrer que $I \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.
2. On suppose que $I \cap \mathbb{Z} = 0$ et on note $\tilde{I} = I\mathbb{Q}[X]$ l'idéal engendré par I dans $\mathbb{Q}[X]$. Montrer que $\tilde{I} \cap \mathbb{Z}[X] = I$. En déduire que I est principal engendré par un polynôme non constant irréductible et primitif.
3. On suppose que $I \cap \mathbb{Z} = p\mathbb{Z}$. Montrer que I/pI est un idéal premier de $\mathbb{F}_p[X]$. En déduire que I est engendré soit par p, soit par p et un polynôme unitaire dont la réduction modulo p est irréductible.
4. Parmi les idéaux trouvés, lesquels sont maximaux ?
5. En s'inspirant de cette méthode, montrer que les idéaux premiers de $\mathbb{C}[X, Y]$ sont soit principaux, soit de la forme $(X - a, Y - b)$. Quels sont les idéaux maximaux ?