TD 6 - Anneaux, partie 2

Exercice 1. Soit $\varphi : A \to B$ un morphisme d'anneaux.

1. Montrer que pour tout idéal I de B, $\varphi^{-1}(I)$ est un idéal de A.
2. On suppose que φ est surjectif. Montrer que pour tout idéal I de A, $\varphi(I)$ est un idéal de B.

Exercice 2. Soient $m, n \in \mathbb{Z}$. Déterminer les idéaux $(m) \cap (n)$ et $(m) + (n)$.

Exercice 3. Soit K un intervalle de $\mathbb{R}$. On considère $A = \mathcal{C}^0(K, \mathbb{R})$.

1. Rappeler pourquoi A est naturellement muni d'une structure d'anneau commutatif.
2. L'anneau A est-il intègre ?
3. Soit $x_0 \in K$. Montrer que l'ensemble $J = \{f \in A \mid f(x_0) = 0\}$ est un idéal de A.
4. Étudier le quotient A/J.
5. Montrer que J est un idéal maximal de A.

Exercice 4.

1. Montrer que l'application suivante est un morphisme d'anneau

$$\begin{array}{rccc} \phi : & \mathbb{R}[X] & \to & \mathbb{C} \\ & P & \mapsto & P(i). \end{array}$$

2. Déterminer le noyau de ϕ.
3. En déduire qu'il existe un isomorphisme d'anneaux entre $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{C}$.

Exercice 5. On considère l'ensemble $\mathbb{Q}[i] = \{p + iq \mid p, q \in \mathbb{Q}\}$.

1. Montrer que $\mathbb{Q}[i]$ est un corps. (*On commencera par montrer que c'est un sous-anneau de* $\mathbb{C}$.)
2. Montrer que $\mathrm{Frac}(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$.

† *Anneaux principaux*

Exercice 6. Dans $\mathbb{Z}[X]$, on considère l'idéal $I = (2, X)$.

1. Montrer que I est un idéal maximal.
2. Montrer que I n'est pas principal. En déduire que $\mathbb{Z}[X]$ n'est pas principal.

Exercice 7. Soit A un anneau principal et soit I un idéal de A.

1. Soit $a \in A$, $a \neq 0$. Montrer l'équivalence des assertions suivantes :
   (a) a est irréductible.
   (b) l'idéal (a) engendré par a est un idéal maximal.
   (c) (a) est un idéal premier.
2. Soit p un élément irréductible de A. On considère l'idéal $I = (p, X)$ de $A[X]$ engendré par le polynôme constant p et le polynôme X.
   (a) Montrer que $A[X]/I$ est isomorphe à $A/(p)$ où (p) est l'idéal de A engendré par p.
   (b) En déduire que I est un idéal maximal de $A[X]$.
   (c) Montrer que I n'est pas un idéal principal.
   (d) Montrer que 1 est le PGCD de p et de X dans $A[X]$ et qu'il n'existe pas de polynôme G, H dans $A[X]$ tels que $1 = pG + XH$.

Exercice 8 (Théorème des deux carrés). On considère l'ensemble $\mathbb{Z}[i]$ l'ensemble des nombres complexes de la forme $a+ib$ avec $a,b\in\mathbb{Z}$. On rappelle que $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme N défini par $N(a+ib)=a^2+b^2\in\mathbb{N}$. Les parties de l'exercice sont indépendantes.

Partie 1 : $\mathbb{Z}[i]$ et les sommes de deux carrés.

Soit $p\in\mathbb{N}$ un nombre premier. Montrer que les assertions suivantes sont équivalentes

(a) p est réductible dans $\mathbb{Z}[i]$.

(b) Il existe $\alpha\in\mathbb{Z}[i]$ tel que $N(\alpha)=p$ (*indication : on remarquera que* $N(zz')=N(z)N(z')$).

(c) p s'écrit comme somme de deux carrés de nombres entiers.

Partie 2 : Un isomorphisme d'anneau.

1. Soit p un nombre premier. On pose $f:\mathbb{Z}[X]\to\mathbb{Z}[i]/(p)$ le morphisme d'anneaux envoyant $P(X)$ sur la classe de $P(i)$ modulo (p).
   (a) Soit $P(X)\in\mathbb{Z}[X]$. Montrer que $P(X)$ s'écrit de manière unique sous la forme $P(X)=(X^2+1)Q(X)+aX+b$ avec $a,b\in\mathbb{Z}$.
   (b) En utilisant cette écriture, montrer que $P(X)$ appartient à l'idéal (X^2+1,p) si et seulement si p divise a et b. En déduire que (X^2+1,p) est le noyau de f.
   (c) Montrer que f induit un isomorphisme $\mathbb{Z}[X]/(X^2+1,p)\simeq\mathbb{Z}[i]/(p)$.
2. Montrer que $\mathbb{Z}[X]/(X^2+1,p)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$.
3. Montrer que p est réductible dans $\mathbb{Z}[i]$ si et seulement si X^2+1 admet une racine dans $\mathbb{Z}/p\mathbb{Z}$.

Partie 3 : Les carrés dans $\mathbb{Z}/p\mathbb{Z}$.

4. Soit $p=2$. Montrer que $-1\in\mathbb{Z}/2\mathbb{Z}$ s'écrit comme un carré dans $\mathbb{Z}/2\mathbb{Z}$.
5. Soit p un nombre premier impair. Montrer que l'application $\varphi:\mathbb{Z}/p\mathbb{Z}^*\to\mathbb{Z}/p\mathbb{Z}^*$ envoyant x sur $x^{\frac{p-1}{2}}$ est un morphisme de groupes.
6. Montrer que $\operatorname{Ker}\varphi$ est donnée par les racines non nulles du polynôme $X^{\frac{p-1}{2}}-1$. En déduire que $|\operatorname{Ker}\varphi|\leqslant\frac{p-1}{2}$.
7. Montrer que l'application $\psi:\mathbb{Z}/p\mathbb{Z}^*\to\mathbb{Z}/p\mathbb{Z}^*$ envoyant x sur x^2 est un morphisme de groupes. Montrer que son image est inclue dans $\operatorname{Ker}\varphi$.
8. Montrer que $|\operatorname{Im}\psi|=\frac{p-1}{2}$. En déduire que $\operatorname{Ker}\varphi=\operatorname{Im}\psi$.
9. Montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $(-1)^{\frac{p-1}{2}}=1$.

Partie 4 : Soit $p\in\mathbb{N}$ un nombre premier. En utilisant les parties précédentes, montrer que les deux assertions suivantes sont équivalentes :

— p s'écrit comme somme de deux carrés de nombres entiers.

— $p=2$ ou bien $p\equiv 1[4]$.