Université de Poitiers, Année 2023-2024

3^{e} année de Licence de Mathématiques, Anneaux

Examen, le lundi 6 mai 2024, 9h-11h

Exercice 1 – Questions de cours (5 points)

1. Démontrer que tout anneau euclidien est principal.
2. Donner la définition d'un $PGCD$ de deux éléments d'un anneau intègre et d'un anneau à $PGCD$.
3. Soit A un anneau intègre. Montrer que, si $a \in A$ est irréductible, alors tout $b \in A$ est
   - soit premier avec a ;
   - soit divisible par a.

Exercice 2 – L'anneau $\mathbb{Z} + X\mathbb{Q}[X]$ – *Exercice issu des fiches de TD* (7 points)

Soit $A = \mathbb{Z} + X\mathbb{Q}[X]$ l'ensemble des polynômes de $\mathbb{Q}[X]$ dont le terme constant est un entier.

1. Montrer que A est un anneau. Quels sont ses éléments inversibles ?
2. (a) Justifier que les polynômes constants de la forme $P(X) = p$ pour un nombre premier p sont des éléments irréductibles de A.
   (b) Remarquer que tous les polynômes de cette forme divisent X dans A et en déduire que A n'est pas factoriel.
3. On considère $P, Q \in A$ tels que $P(0)$ et $Q(0)$ ne soient pas nuls simultanément.
   (a) Pourquoi existe-t-il $R \in \mathbb{Q}[X]$ tel que $R\mathbb{Q}[X] = P\mathbb{Q}[X] + Q\mathbb{Q}[X]$?
   (b) Vérifier que $R(0)$ est non nul.
   On pose $S = \frac{d}{R(0)}R$ où d désigne le *pgcd* des entiers relatifs $P(0)$ et $Q(0)$.
   (c) Montrer que S divise P et Q dans $\mathbb{Q}[X]$, puis dans A.
4. Soit $T \in A$ un diviseur commun de P et Q dans A.
   (a) Montrer qu'il existe $U \in \mathbb{Q}[X]$ tel que $S = UT$ et que $T(0)$ divise $P(0)$ et $Q(0)$.
   (b) En déduire que U appartient à A et que S est un $PGCD$ de P et Q dans A.

Remarque : on peut montrer que lorsque $P, Q \in A$ vérifient $P(0) = Q(0) = 0$, ils admettent aussi un $PGCD$ dans A, et ainsi démontrer que A est un anneau à $PGCD$.

Exercice 3 – Anneaux d'entiers quadratiques (12 points)

1. **Généralités**

   On fixe α un nombre complexe n'appartenant pas à $\mathbb{Q}$ et qui est racine d'un polynôme unitaire $U_\alpha = X^2 + rX + s$ de degré 2 à coefficients dans $\mathbb{Z}$.

   (a) Pour tout sous-anneau A de $\mathbb{C}$, on note $A[\alpha]$ le sous-anneau de $\mathbb{C}$ engendré par A et α. *On admet que* $A[\alpha] = \{a + b\alpha \mid a, b \in A\}$ *et que les éléments de* $\mathbb{Q}[\alpha]$ *s'écrivent de façon unique sous la forme* $a + b\alpha$ *pour* $a, b \in \mathbb{Q}$.

   i. Justifier que l'autre racine α^* de U_α vérifie $\alpha^* = -r - \alpha$ et qu'elle est différente de α.

   ii. Prouver que l'application $\omega : \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha]$ qui, à tout $z = a + b\alpha \in \mathbb{Q}[\alpha]$, associe $\omega(z) = a + b\alpha^*$, est un automorphisme de l'anneau $\mathbb{Q}[\alpha]$.

   (b) Pour tout $z \in \mathbb{Q}[\alpha]$, on note $N(z) = z\omega(z)$.

   i. Justifier que, pour tout $z \in \mathbb{Q}[\alpha]$, on a $N(z) = 0$ si et seulement si $z = 0$.

   ii. Vérifier que, pour tous $x, y \in \mathbb{Q}[\alpha]$, on a $N(xy) = N(x)N(y)$.

   iii. Montrer que $N(z) = a^2 - abr + b^2 s$ pour tout $z \in \mathbb{Q}[\alpha]$.

   iv. En déduire que, pour tout $z \in \mathbb{Z}[\alpha]$, on a $N(z) \in \mathbb{Z}$ et que l'élément z est inversible dans $\mathbb{Z}[\alpha]$ si et seulement si $N(z) \in \{+1, -1\}$.

   v. Pourquoi l'anneau $\mathbb{Q}[\alpha]$ est-il un corps ?

2. **Le nombre d'or**

   On considère le *nombre d'or* $\varphi = \frac{1+\sqrt{5}}{2}$.

   (a) Déterminer U_φ et montrer que $\mathbb{Z}[\varphi]$ a une infinité d'éléments inversibles.
   Indication : calculer $N(\varphi)$ *et considérer les puissances de* φ.

   (b) Montrer que, pour tous $x, y \in \mathbb{Z}[\varphi]$ avec y non nul, il existe $q \in \mathbb{Z}[\varphi]$ tel que $|N(\frac{x}{y} - q)| < 1$.
   Indication : est-il possible d'écrire $\frac{x}{y}$ *sous la forme* $\frac{x}{y} = a + b\varphi$ *avec* a *et* b *dans* $\mathbb{Q}$ *? Prendre alors* $q = a' + b'\varphi$ *avec* a' *et* b' *dans* $\mathbb{Z}$ *les plus proches possibles de* a *et* b.

   (c) On note $\mathbb{Z}[\varphi]^* = \mathbb{Z}[\varphi] \setminus \{0\}$. Démontrer que l'application $N^* : \mathbb{Z}[\varphi]^* \to \mathbb{N}$ définie par $N^*(z) = |N(z)|$ est un stathme euclidien sur $\mathbb{Z}[\varphi]$.

   (d) En déduire que l'anneau $\mathbb{Z}[\varphi]$ est euclidien, principal, factoriel et intégralement clos.

   (e) i. Soit $z = a + b\varphi \in \mathbb{Z}[\varphi]$. Montrer que 7 divise z dans $\mathbb{Z}[\varphi]$ si et seulement si 7 divise $N(z)$ dans $\mathbb{Z}$.
   Indication : pour la réciproque, montrer d'abord que $N(z) = a^2 + ab - b^2$, *puis que* $N(z)$ *est congru à* $(a + 4b)^2 - 3b^2$ *modulo* 7. *Calculer ensuite les carrés modulo 7, et donner les valeurs possibles de* $3b^2$ *et de* $(a + 4b)^2$ *modulo 7. En déduire que, si* $N(z)$ *est nul modulo* 7, *alors* $3b^2$ *et* $(a + 4b)^2$ *aussi.*

   ii. En déduire que 7 est un élément premier et irréductible de $\mathbb{Z}[\varphi]$.