Examen partiel - Corrigé

I - Exemples (5 points)

1. Donner un exemple de polynôme $P \in \mathbb{R}[X]$ de degré 2 tel que l'anneau quotient $\mathbb{R}[X]/(P)$ ne soit pas isomorphe à $\mathbb{C}$ (justifier rapidement, deux phrases devraient suffire).

Réponse :

$P(X) = X(X-1)$ convient, en effet l'anneau quotient $\mathbb{R}[X]/(P)$ n'est pas intègre car $\bar{X}$ est un diviseur de zéro : on a

$$\overline{X}(\overline{X-1}) = \bar{0}.$$

2. Dans l'anneau $\mathbb{Q}[X]$, donner un exemple de sous-anneau $B \subsetneq \mathbb{Q}[X]$, et un exemple (non trivial) d'idéal $I \subsetneq \mathbb{Q}[X]$.

Réponse :

$B = \mathbb{Z}[X]$ est un sous-anneau de $\mathbb{Q}[X]$, et $I = (X)$, ensemble des polynômes multiples de X, est un idéal de $\mathbb{Q}[X]$.

3. Si $P = X^3 \in \mathbb{R}[X]$, donner un représentant de degré minimal de la classe $\bar{P}$ dans l'anneau quotient $\mathbb{R}[X]/(X^2+1)$.

Réponse :

On écrit la division euclidienne $X^3 = (X^2+1)X - X$, ainsi le polynôme $-X$ convient.

4. Donner un PGCD de $1+i$ et $1-i$ dans l'anneau $\mathbb{Z}[i]$.

Réponse :

On a $1+i = i(1-i)$, ainsi $1+i$ et $1-i$ sont égaux à un inversible près, leur PGCD est donc $1+i$ (ou $1-i$, comme on veut).

5. Donner un exemple d'anneau A contenant un idéal I premier mais non maximal, que l'on explicitera.

Réponse :

Dans l'anneau $A = \mathbb{R}[X,Y]$, $I = (X)$ n'est pas maximal car $(X) \subsetneq (X,Y)$, par contre I est premier car le théorème d'isomorphisme appliqué au morphisme $P(X,Y) \in \mathbb{R}[X,Y] \mapsto P(0,Y)$ montre que $A/I \simeq \mathbb{R}[Y]$, qui est un anneau intègre.

II - Questions de cours (6 points)

1. Soit $n \geq 2$, et $k \in \mathbb{Z}$. Montrer que k et n sont premiers entre eux si et seulement si $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Réponse :

Si k et n sont premiers entre eux, on écrit une relation de Bézout $uk + vn = 1$, ce qui montre que $\bar{u}\bar{k} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$ et donc $\bar{k}$ est inversible.

Réciproquement si $\bar{k}$ est inversible d'inverse $\bar{u}$, alors il existe $v \in \mathbb{Z}$ tel que $uk + vn = 1$, ce qui montre que tout diviseur commun de k et n divise 1, ainsi k et n sont premiers entre eux.

2. Démontrer le lemme de Gauss sur $\mathbb{R}[X]$: si $A, B, C \in \mathbb{R}[X]$ sont trois polynômes tels que A, B sont premiers entre eux et A divise BC, montrer que A divise C.

Réponse :

Comme A et B sont premiers entre eux on peut écrire une relation de Bézout $AU + BV = 1$, en multipliant par C on obtient $ACU + BCV = C$. Or A divise BCV par hypothèse, et bien sûr aussi ACU, donc A divise leur somme, c'est-à-dire C.

3. Énoncer le théorème des restes chinois sur $\mathbb{Z}$, puis résoudre (rapidement) le système de congruence

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv -4 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$$

Réponse :

Théorème des restes chinois : Soit n_i, $i = 1, \ldots, r$, des entiers deux à deux premiers entre eux, et a_i des entiers. Alors le système de congruence $x \equiv a_i \mod n_i$ pour tout i admet une unique solution modulo le produit des n_i.

Pour le système de l'énoncé, 16 est une solution évidente, ainsi les solutions sont les $16 + 105k$, $k \in \mathbb{Z}$.

4. Montrer qu'il existe un isomorphisme

$$\phi \colon \mathbb{R}[X]/(X^2 + X + 1) \to \mathbb{R}[X]/(X^2 + 1),$$

et expliciter les images $\phi(\bar{1})$, $\phi(\bar{X})$ des classes $\bar{1}$, $\bar{X} \in \mathbb{R}[X]/(X^2 + X + 1)$.

Réponse :

Notons $j = e^{2i\pi/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, qui est racine cubique de l'unité et donc racine de $X^2 + X + 1$ (car $X^3 - 1 = (X - 1)(X^2 + X + 1)$).

Le théorème d'isomorphisme appliqué au morphisme d'évaluaetion $P(X) \mapsto P(j)$ donne un isomorphisme $\mathbb{R}[X]/(X^2 + X + 1) \simeq \mathbb{C}$.

De même, le morphisme d'évaluation $P(X) \mapsto P(i)$ donne un isomorphisme $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.

En composant ces deux isomorphismes on obtient l'isomorphisme ϕ attendu, et on a, en notant $\hat{P}$ une classe dans $\mathbb{R}[X]/(X^2 + 1)$:

$$\phi(\bar{1}) = \hat{1}, \quad \phi(\bar{X}) = \widehat{-\frac{1}{2} + \frac{\sqrt{3}}{2}X}.$$

III - Anneau $\mathbb{Z}/12\mathbb{Z}$ (4 points).

1. Donner la liste des éléments inversibles dans l'anneau $\mathbb{Z}/12\mathbb{Z}$.

Réponse :

Les inversibles sont les classes $\bar{k}$ avec k premier avec 12, on trouve donc les quatre éléments : $\bar{1}, \bar{5}, \bar{7}, \bar{11}$.

2. Donner les diviseurs de zéro dans $\mathbb{Z}/12\mathbb{Z}$.

Réponse :

Les diviseurs de zéro sont $\bar{0}, \bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8} = -\bar{4}, \bar{9} = -\bar{3}, \bar{10} = -\bar{2}$ car par exemple

$$\bar{2} \cdot \bar{6} = \bar{12} = \bar{0}$$
$$\bar{3} \cdot \bar{4} = \bar{12} = \bar{0}$$

3. Montrer que les idéaux de $\mathbb{Z}/12\mathbb{Z}$ sont principaux (*on pourra utiliser le morphisme naturel de* $\mathbb{Z}$ *vers* $\mathbb{Z}/12\mathbb{Z}$).

Réponse :

Soit ϕ le morphisme de $\mathbb{Z}$ vers $\mathbb{Z}/12\mathbb{Z}$. Soit I un idéal de $\mathbb{Z}/12\mathbb{Z}$, alors $\phi^{-1}(I)$ est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. On en déduit que $I = \phi(\phi^{-1}(I))$ est égal à $(\bar{n})$, et en particulier est principal.

4. Donner la liste des idéaux de $\mathbb{Z}/12\mathbb{Z}$, indiquer lesquels sont des idéaux maximaux, et à quels corps bien connus sont isomorphes les quotients de $\mathbb{Z}/12\mathbb{Z}$ par ces idéaux maximaux.

Réponse :

Les idéaux de $\mathbb{Z}/12\mathbb{Z}$ sont $(\bar{0})$, $(\bar{1}) = \mathbb{Z}/12\mathbb{Z}$, $(\bar{2})$, $(\bar{3})$, $(\bar{4})$, $(\bar{6})$.

On a $(\bar{0}) \subsetneq (\bar{4}) \subsetneq (\bar{2})$, et $(\bar{6}) \subsetneq (\bar{2}) \cap (\bar{3})$.

Les idéaux maximaux sont donc $(\bar{2})$ et $(\bar{3})$, les quotients ont respectivement 2 et 3 éléments, et sont donc isomorphes aux corps $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

NB: on a $(\bar{8}) = (\bar{4})$, $(\bar{9}) = (\bar{3})$...

IV - Anneaux factoriels et de Bézout. (5 points)

Soit A un anneau commutatif intègre, et (p_i) un système de représentants des irréductibles de A à inversibles près.
On suppose que A est *factoriel*, c'est-à-dire que tout élément $a \in A \setminus \{0\}$ admet une unique factorisation de la forme

$$a = x p_{i_1}^{\alpha_1} \dots p_{i_s}^{\alpha_s}, \qquad (\dagger)$$

avec $\alpha_i \geq 1$, et x inversible.
On suppose également que A est un anneau de *Bézout*, c'est-à-dire que tout couple a, b d'éléments de A admet un PGCD, et qu'on peut écrire une relation de Bézout pour a et b.
Le but de cet exercice est de montrer que A est un anneau *principal*.

1. Rappeler la définition générale d'un anneau principal.

Réponse :

Un anneau principal est un anneau commutatif **intègre** dont chaque idéal est principal, c'est-à-dire engendré par un seul élément.

NB: il est crucial de ne pas oublier "intègre" dans la définition. Par exemple, l'anneau $\mathbb{Z}/12\mathbb{Z}$ de l'exercice III a tous ses idéaux principaux, mais ce n'est pas un anneau principal car il n'est pas intègre.

2. Soit I un idéal, qui est non nul et non égal à A. Justifier qu'il existe $a \in I \setminus \{0\}$ qui minimise, parmi tous les élements de $I \setminus \{0\}$, la somme des exposants $\sum_j \alpha_j$ dans l'écriture (†).

Réponse :

La somme $\sum_j \alpha_j$ est à valeur dans $\mathbb{N} \setminus \{0\}$, et tout sous-ensemble de $\mathbb{N}$ contient sa borne inférieure.

3. Soit $b, c \in I \setminus \{0\}$. Montrer que le PGCD de b et c appartient aussi à l'idéal I.

Réponse :

Comme on suppose l'anneau de Bézout, il existe une relation de Bézout $bu+cv = d$, où $u, v \in A$, et d est un PGCD de a et b. Ainsi bu et cv sont dans I, et leur somme, égale à d, également.

4. Conclure.

Réponse :

Comme A est commutatif intègre par hypothèse, il s'agit de montrer que tout idéal I de A est principal. Si $I = (0)$ ou $I = (1)$ il n'y a rien à montrer. Sinon soit $a \in I \setminus \{0\}$ donné par la question 2, et montrons que $I = (a)$. Soit $b \in I$, et d PGCD de a et b, qui est dans I par la question 3. Ecrivons $d = y p_{i_1}^{\beta_1} \dots p_{i_s}^{\beta_s}$, on a $\beta_i \leq \alpha_i$ pour tout i car d divise a, et donc $\beta_i = \alpha_i$ par minimalité de a. On en déduit que a est un PGCD de a et b, autrement dit a divise b, comme attendu.