# Contrôle final - Jeudi 19 janvier 2012

**durée : 3h**

**Les documents et les calculatrices ne sont pas autorisés.**

**Une grande importance sera accordée à la concision et à la précision de la rédaction.**

**Le sujet est constitué de 5 exercices indépendants.**

**Exercice 1** Soient

$$P = X^4 + 2X^3 + 5X^2 + 4X + 4 \text{ et } Q = X^3 - 2X^2 - X - 6$$

deux polynômes de $\mathbb{Q}[X]$.

1. Calculer un PGCD de $P$ et $Q$.
2. Donner les décompositions en facteurs irréductibles dans $\mathbb{Q}[X]$ de $P$ et $Q$.

**Exercice 2** Parmi les polynômes suivants lesquels sont irréductibles ?

1. $\frac{1}{3}X^4 + \frac{15}{2}X^3 - \frac{25}{4}X^2 + \frac{10}{3}X - 45$ dans $\mathbb{Q}[X]$ ;
2. $X^3 + 5X^2 - 2X + 2$ dans $\mathbb{Q}[X]$ ;
3. $X^4 + \pi X^3 + \sqrt{\pi}X^2 + \sqrt{3}X + 7$ dans $\mathbb{R}[X]$ ;
4. $X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{Z}/5\mathbb{Z}[X]$.

**Exercice 3** On cherche à résoudre dans $\mathbb{Z}$ l'équation

$$2x^2 + y^2 = 5z^2 \qquad (E).$$

Supposons qu'il existe des entiers $a, b, c$ non tous nuls tel que $(a, b, c)$ soit solution de $(E)$.

1. Montrer qu'il existe des entiers $a', b', c'$ qui ne sont pas tous multiples de 5 tel que $(a', b', c')$ soit solution de $(E)$.
2. Montrer que $a'$ ou $b'$ n'est pas multiple de 5.
3. Soit $x \in \mathbb{Z}$. Montrer que $x^2 \equiv 0, 1$ ou $4 \bmod 5$.
4. En déduire que $(E)$ a pour unique solution $(0, 0, 0)$.

**Exercice 4**

1. Soit $G$ un groupe commutatif, $a \in G$ un élément d'ordre $n$ et $b \in G$ un élément d'ordre $m$. Montrer que $ab$ est d'ordre fini.
2. On considère le groupe $\mathrm{Gl}_2(\mathbb{R})$ et deux matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Quels sont les ordres de $A$, $B$ et $AB$ ?

**Exercice 5** Posons $\mathbb{Z}[2i] = \{a + 2ib \in \mathbb{C};\ a, b \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[2i]$ est un sous-anneau de $\mathbb{C}$.
2. Si $\alpha = a + 2ib \in \mathbb{Z}[2i]$ on pose $N(\alpha) = a^2 + 4b^2$. Montrer que pour tout $\alpha, \beta \in \mathbb{Z}[2i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.
3. Soit $\alpha \in \mathbb{Z}[2i]$. Montrer que $\alpha$ est inversible dans $\mathbb{Z}[2i]$ si et seulement si $N(\alpha) = 1$. En déduire les éléments inversibles de $\mathbb{Z}[2i]$.
4. Vérifier qu'il n'existe pas d'élément $\alpha \in \mathbb{Z}[2i]$ tel que $N(\alpha) = 2$.
5. En déduire que si $\alpha \in \mathbb{Z}[2i]$ et $N(\alpha) = 4$ alors $\alpha$ est irréductible dans $\mathbb{Z}[2i]$.
6. Vérifier que 2 et $2i$ sont deux éléments irréductibles non associés dans $\mathbb{Z}[2i]$. En déduire que 4 admet deux décompositions en facteurs irréductibles et que $Z[2i]$ n'est pas factoriel.