Algèbre générale de base

TD

Contrôle Continu : conseils et exercices d'entrainement

1. **Le premier contrôle continu aura lieu vendredi 16 octobre.**
2. **Il portera sur les 8 premiers cours ainsi que les feuilles d'exercices nos 1-7.**
3. **Une bonne préparation serait de faire les feuilles d'exercices et éventuellement les exercices supplémentaires ci-dessous.**

Exercice 1

1. Soit $x \in \mathbb{N}$ impair. Montrez que $x^2 + 2 \equiv 3 \ (mod\ 4)$, et en déduire qu'il existe un nombre premier p tel que
$$p|(x^2 + 2) \ et \ p \equiv 3 \ (mod\ 4).$$

2. Utilisez la question précédente pour en déduire l'existence d'une infinité de nombres premiers congrus à 3 modulo 4.

3. Utilisez le fait que $\mathbb{Z}$ est factoriel pour résoudre l'équation diophantienne d'inconnue entières $(x, y) \in \mathbb{Z}^2$
$$x^2 - y^4 = 4$$

Exercice 2

Soient $P(X) = X^2 + X + 1 \in \mathbb{F}_5[X]$, $K = \mathbb{F}_5[X]/ < P(X) >$, et notons α la classe de X dans K.

1. Montrez que K est un corps. Quel est son cardinal ? Donnez une base de K comme espace vectoriel sur $\mathbb{F}_5$.

2. Déterminez les ordres de α et $\alpha+3$ dans $K^\times$, puis trouvez un générateur du groupe multiplicatif $K^\times$.

3. Déterminez le polynôme minimal de $\alpha + 3$ dans $\mathbb{F}_5[X]$.

Exercice 3

Considérons l'anneau $\mathbb{Z}[i]$.

1. Définir la norme $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$
2. Soit $\alpha \in \mathbb{Z}[i]$ tel que $N(\alpha)$ est irréductible dans $\mathbb{Z}$. Montrez que α est irréductible dans $\mathbb{Z}[i]$.
3. Calculez $N(9+2i)$. Déterminez les facteurs irréductibles de $9+2i$ dans $\mathbb{Z}[i]$.
4. Montrez que $\mathbb{Z}[i]$ est un anneau euclidien.

Exercice 4

Les trois parties de cet exercice sont indépendantes. Justifier vos réponses.

1. Déterminez les idéaux maximaux dans les anneaux suivants :
(i) $\mathbb{Q} \times \mathbb{Q}$ (ii) $\mathbb{Q}[X]/ < X^2 - 5X + 6 >$.
2. L'anneaux $R := \mathbb{Z}[X]/ < 3, X^2 + 2 >$ est-il un corps ?
3. L'idéal $I =< X^4 - 1, 2X^3 - 2X >$ est-il principal dans $\mathbb{Z}[X]$? Dans $\mathbb{Q}[X]$?

Exercice 5

Soit K un corps et supposons que $[K(\alpha) : K]$ soit impair. Montrez alors que $K(\alpha^2) = K(\alpha)$.

Exercice 6

1. 37 est-il un carré modulo 61 ?
2. 19 est-il un carré modulo $505 = 5 \times 101$?
3. Soit $p > 3$ un nombre premier. S'il existe un entier n pour lequel p divise $n^2 - n + 1$, montrez que $p \equiv 1 \ (mod\ 6)$.