
Approfondissement

Énoncés

Exercice 1.

1. Quels sont les ordres multiplicatifs de 2 mod 3, mod 7, mod 9 et mod 19 ?
2. Montrer que si n est un entier impair, alors 7 divise $2^{2^n} + 3$.
3. Montrer que si $n \equiv 2 \pmod{6}$, alors 19 divise $2^{2^n} + 3$.

Exercice 2.

1. Déterminer le nombre d'éléments de l'anneau $\mathbb{A} = \mathbb{F}_5[X]/(X^2 + 4)$.
2. Justifier si la classe du polynôme $X^3 + 2X^2 - X + 2$ est inversible dans $\mathbb{A}$. Dans le cas échéant, calculer son inverse.
3. L'anneau $\mathbb{A}$ est-il un corps ? Pourquoi ?

Exercice 3. On considère le polynôme $P(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$ et soit $K = \mathbb{F}_2[X]/(P)$. On note $\alpha \in K$ la classe de X .

1. Montrer que K est un corps. Quel est son cardinal ?
2. Montrer que $P(X)^2 = P(X^2)$. En déduire que P a 4 racines distinctes dans K dont on donnera les valeurs.
3. Donner une base du $\mathbb{F}_2$ -espace vectoriel K .
4. Déterminer l'ordre de α dans le groupe K^* .
5. Trouver l'inverse de $1 + \alpha + \alpha^2$ dans K^* .

Exercice 4. Soit $\mathbb{F}_5$ le corps à 5 éléments. On considère $a, b \in \mathbb{F}_5$ et deux polynômes $P = X^2 + aX + b$ et $Q = (X + 3a)^2$ dans $\mathbb{F}_5[X]$.

1. Donner la liste des carrés dans $\mathbb{F}_5$.
2. Calculer $P - Q$ et montrer que P a une racine dans $\mathbb{F}_5$ si et seulement si $4a^2 - b$ est un carré dans $\mathbb{F}_5$.
3. Soit $P = X^2 + 2X + b \in \mathbb{F}_5[X]$. Pour quelles valeurs de $b \in \mathbb{F}_5$, P est-il irréductible ?

On pose désormais $a = 2, b = 3$ et $K = \mathbb{F}_5[X]/(P)$ et on note x la classe de X dans K .

4. Déterminer le nombre d'éléments de K .
5. Quel est l'inverse de x dans K^* .
6. Trouver l'ordre de x dans K^* .
7. Montrer que P a 2 racines distinctes dans K dont on donnera les valeurs.

Exercice 5. On considère l'ensemble $\mathbb{Z}[\sqrt{2}i] = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$

1. Montrer que $\mathbb{Z}[\sqrt{2}i]$ est un anneau commutatif intègre.
2. Pour tout nombre complexe $\alpha = x + yi$, on considère sa norme $N(\alpha) = x^2 + y^2$.
Montrer que si $z_1, z_2 \in \mathbb{C}$, alors $N(z_1 z_2) = N(z_1)N(z_2)$.
3. Montrer que tout idéal de $\mathbb{Z}[\sqrt{2}i]$ est principal.