

Devoir Surveillé, 7 novembre 2012.

Durée 2h00. Documents interdits.

Dans ce qui suit, si K est un corps et si $P(X) \in K[X]$, on note $(P(X))$ l'idéal de $K[X]$ engendré par $P(X)$, i.e. l'idéal $P(X)K[X]$.

Exercice 1 –

- 1) Dresser la liste des polynômes unitaires de $\mathbb{F}_3[X]$ de degré ≤ 2 , premiers avec $X + 1$ et $X - 1$.
- 2) On considère l'anneau $A = \frac{\mathbb{F}_3[X]}{(X^3 - X^2 - X + 1)}$. Quelle est sa caractéristique ? Quel est son cardinal ? L'anneau A est-il un corps ?
- 3) Quel est le cardinal de A^\times (le groupe des éléments inversibles de A) ?
- 4) Soit α la classe de X dans A . Montrer que $\alpha \in A^\times$ et déterminer son ordre dans A^\times .
- 5) Montrer que pour tout $\beta \in A^\times$, on a $\beta^6 = 1$. Le groupe A^\times est-il cyclique ?

Exercice 2 –

- 1) Soit $P(X) = X^2 + X + 3 \in \mathbb{F}_7[X]$. Expliquer pourquoi l'anneau $B = \frac{\mathbb{F}_7[X]}{(P(X))}$ est un corps.
- 2) Quel est le nombre de polynômes unitaires irréductibles de degré 2 dans $\mathbb{F}_7[X]$? De degré 4 ?
- 3) Soit α la classe de X dans B . Quels sont les ordres possibles a priori de α dans B^\times ?
- 4) Exprimer α^2 , α^4 et α^8 comme combinaisons linéaires de 1 et α à coefficients dans \mathbb{F}_7 .
- 5) Le polynôme $P(X)$ est-il primitif ?
- 6) Quel est le nombre de polynômes unitaires irréductibles primitifs de degré 2 dans $\mathbb{F}_7[X]$? De degré 4 ?

Exercice 3 – On considère dans $\mathbb{F}_2[X]$ le polynôme $P(X) = X^6 + X + 1$ et on note C l'anneau $\mathbb{F}_2[X]/(P(X))$.

- 1) Soit α la classe de X dans C . Montrer que $\alpha \in C^\times$ et calculer l'ordre de α dans C^\times .
- 2) En déduire que C est un corps. On identifiera C à \mathbb{F}_{64} .
- 3) Montrer que $P(X)$ est irréductible et primitif.
- 4) Combien C admet-il de sous-corps stricts et quels sont leurs cardinaux respectifs ?
- 5) On pose $\beta = \alpha + \alpha^3 + \alpha^4 + \alpha^5$. Montrer que β appartient à un sous-corps strict de C à préciser.

- 6) Quels sont les éléments de ce sous-corps ?
- 7) Quel est le polynôme minimal de β sur \mathbb{F}_2 ? Que vaut $\text{Tr}(\beta)$?
- 8) On pose $\gamma = \alpha + \alpha^2 + \alpha^3$. Combien le corps $\mathbb{F}_2(\gamma)$ compte-t-il d'éléments ?
- 9) Quel est le polynôme minimal de γ sur \mathbb{F}_2 ? Que vaut $\text{Tr}(\gamma)$?
- 10) Déterminer $\mathbb{F}_2(\beta) \cap \mathbb{F}_2(\gamma)$.

Exercice 4 –

- 1) Décomposer $X^4 - 1$ en produit d'irréductibles unitaires dans $\mathbb{F}_5[X]$.
- 2) Quel est le nombre de facteurs irréductibles unitaires intervenant dans la décomposition de $X^8 - 1$ dans $\mathbb{F}_5[X]$. Préciser leurs degrés.
- 3) En déduire la décomposition de $X^4 + 1$ dans $\mathbb{F}_5[X]$.
- 4) Quel est le nombre de facteurs irréductibles unitaires intervenant dans la décomposition de $X^8 + 1$ dans $\mathbb{F}_5[X]$. Préciser leurs degrés.
- 5) Quel est le nombre de facteurs irréductibles unitaires intervenant dans la décomposition de $X^{200} + 1$ dans $\mathbb{F}_5[X]$. Préciser leurs degrés.