Codes algébriques – Feuille de TD 3

09/02/2024

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`https://lvzl.fr/teaching/2023-24/ca.html`

($\star$) exercice fondamental ($\star\star$) pour s'entraîner ($\star\star\star$) pour aller plus loin 💻 sur machine

Exercice 1. ($\star$) Calcul de classes cyclotomiques.

Question 1.– Pour $q = 3$ et $n = 11$, déterminer la classe cyclotomique de $b = 1$ modulo n sur $\mathbb{F}_q$.

Question 2.– Déterminer toutes les classes cyclotomiques modulo 15 sur $\mathbb{F}_2$.

Question 3.– Vrai ou faux ? Fixons q et n premiers entre eux.

1. Une classe cyclotomique modulo n sur $\mathbb{F}_q$ est également une classe cyclotomique modulo n sur $\mathbb{F}_{q^2}$.
2. Une classe cyclotomique modulo n sur $\mathbb{F}_{q^2}$ est également une classe cyclotomique modulo n sur $\mathbb{F}_q$.
3. Une classe cyclotomique modulo n sur $\mathbb{F}_q$ peut être partitionnée en classes cyclotomique modulo n sur $\mathbb{F}_{q^2}$.

Question 4.– Supposons que $n = q^2 - 1$. Déterminer toutes les classes cyclotomiques modulo n sur $\mathbb{F}_q$.

Exercice 2. ($\star\star$) Divisiblité de polynômes.

Question 1.– Soient a et b deux entiers strictement positifs, et K un corps. Démontrer l'équivalence suivante :

$$x^a - 1 \text{ divise } x^b - 1 \text{ dans } K[x] \iff a \text{ divise } b \text{ dans } \mathbb{Z}.$$

Question 2.– Dans cette question on pose $K = \mathbb{F}_q$ et on fixe un entier n premier avec q. On note m l'ordre de q dans $(\mathbb{Z}/m\mathbb{Z})^\times$.

1. Déduire de la question précédente que $x^n - 1$ divise $x^{q^m} - 1$.
2. Montrer que, pour tout $1 \leq s < m$, le polynôme $x^n - 1$ ne divise pas $x^{q^s} - 1$.

Exercice 3. ($\star\star$) Factorisation de $x^n - 1$ par les classes cyclotomiques.

Dans cet exercice, on pose $q = 3$ et $n = 8$.

Question 1.– Déterminer les classes cyclotomiques modulo n sur $\mathbb{F}_q$.

Question 2.– Déterminer le corps de décomposition de $x^n - 1$, c'est-à-dire la plus petite extension de $\mathbb{F}_3$ qui contient toutes les racines de $x^n - 1$.

Question 3.–

1. Montrer que $x^2 + 1$ est irréductible sur $\mathbb{F}_3$.
2. Soit β une racine de $x^2 + 1$ dans $\mathbb{F}_9$. L'élément β est-il une racine primitive 8-ème de l'unité ?

Question 4.–

1. Montrer que $x^2 + x - 1$ est irréductible sur $\mathbb{F}_3$.
2. Soit α une racine de $x^2 + x - 1$ dans $\mathbb{F}_9$. L'élément α est-il une racine primitive n-ème de l'unité ?

Question 5.– En utilisant la question 1 et la question 4, factoriser $x^n - 1$ dans $\mathbb{F}_3$.

Exercice 4. ($\star\star$) Classification des codes cycliques pour $q = 2$ et $n = 17$.

Question 1.– Déterminer les classes cyclotomiques modulo $n = 17$ sur $\mathbb{F}_2$.

Question 2.– Sans factoriser $x^n - 1$, en déduire le nombre de codes cycliques binaires de longueur 17, ainsi que leur dimension.

Exercice 5. ($\star\star$) Liste des codes cycliques pour $q = 2$ et $n = 7$.

Question 1.– Donner la liste de tous les codes cycliques binaires de longueur 7. On décrira ces codes par leur polynôme générateur, et on donnera leur dimension.