

Exercices - Chapitre VI

Exercice 1

Les cinq questions sont indépendantes.

- 1) Expliciter les polynômes irréductibles unitaires de degré 2 de $\mathbb{F}_3[X]$.
- 2) Posons $f = X^8 - X$ dans $\mathbb{F}_2[X]$. Déterminer la décomposition de f en produit de polynômes irréductibles de $\mathbb{F}_2[X]$.
- 3) Expliciter «les» corps \mathbb{F}_{25} et \mathbb{F}_{49} (uniques à isomorphisme près).
- 4) Montrer que 2 est un générateur de \mathbb{F}_{19}^* . Déterminer le logarithme discret de base 2 de 7 dans \mathbb{F}_{19}^* .
- 5) Soient p un nombre premier et g un générateur de \mathbb{F}_p^* . Quel est le logarithme discret de base g de -1 dans \mathbb{F}_p^* ?

Exercice 2 (Sommes de puissances)

Soient K un corps fini de cardinal q et n un entier naturel. Posons

$$S_n = \sum_{x \in K} x^n.$$

- 1) Supposons $n \geq 1$ et n divisible par $q - 1$. Montrer que l'on a $S_n = -1$.
- 2) Supposons $n = 0$, ou bien, n non divisible par $q - 1$. Montrer que l'on a $S_n = 0$.

Rappel : par convention, on a $0^0 = 1$.

Indication : utiliser le fait que K^* est un groupe cyclique (cor. 6.4 du cours).

Exercice 3 (Carrés dans K)

Soit K un corps fini de cardinal q et de caractéristique p . Notons K^2 l'ensemble des éléments de K qui sont des carrés dans K i.e. l'ensemble des x^2 où x est dans K .

- 1) Si $p = 2$, montrer que $K^2 = K$.
- 2) Si p est impair, montrer que $|K^2| = (q + 1)/2$.

Indication: utiliser le théorème 2.7, avec l'homomorphisme de groupes de K^* à valeurs dans K^* qui à x associe x^2 .

- 3) En déduire que tout élément de K est la somme de deux carrés dans K .
- 4) Supposons $p \geq 3$.

4.1) Montrer qu'un élément non nul $x \in K$ est un carré dans K si et seulement si on a $x^{\frac{q-1}{2}} = 1$.

4.2) En déduire que -1 est un carré dans K si et seulement si on a $q \equiv 1 \pmod{4}$.

Exercice 4

L'objectif de cet exercice est de déterminer l'ensemble des nombres premiers $p \geq 3$ tels que 2 soit un carré dans \mathbb{F}_p .

- 1) Supposons $p \equiv 1 \pmod{4}$. Il existe un entier k tel que $p = 4k + 1$. Montrer que l'on a $2^{2k}(2k)! \equiv (-1)^k(2k)! \pmod{p}$. En déduire la congruence

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}.$$

Indication : Remarquer que l'on a les égalités

$$2^{2k}(2k)! = \prod_{i=1}^{2k} (2i) = \prod_{i=1}^k (2i) \prod_{i=1}^k (2k+2i),$$

et pour tout $i = 1, \dots, k$, la congruence

$$2k+2i \equiv -(2k+1-2i) \pmod{p}.$$

- 2) Supposons $p \equiv 3 \pmod{4}$. Il existe un entier k tel que $p = 4k + 3$. Montrer que l'on a $2^{2k+1}(2k+1)! \equiv (-1)^{k+1}(2k+1)! \pmod{p}$. En déduire la congruence

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \pmod{p}.$$

- 3) En déduire que 2 est un carré dans \mathbb{F}_p si et seulement si on a $p \equiv \pm 1 \pmod{8}$.

Exercice 5 (Racines carrées dans \mathbb{F}_p)

Soit p un nombre premier. Considérons un élément a de \mathbb{F}_p^* qui soit un carré dans \mathbb{F}_p . Si p n'est pas congru à 1 modulo 8, on se propose d'expliciter une racine carrée de a . On utilisera la question 4.1 de l'exercice 3 et le résultat de l'exercice 4.

- 1) Supposons $p \equiv 3 \pmod{4}$. Montrer que $a^{\frac{p+1}{4}}$ est une racine carrée de a dans \mathbb{F}_p .
 2) Supposons $p \equiv 5 \pmod{8}$.

2.1) Montrer que l'on a $a^{\frac{p-1}{4}} = \pm 1$.

2.2) Si $a^{\frac{p-1}{4}} = 1$, montrer que $a^{\frac{p+3}{8}}$ est une racine carrée de a dans \mathbb{F}_p .

2.3) Si $a^{\frac{p-1}{4}} = -1$, montrer que $2a(4a)^{\frac{p-5}{8}}$ est une racine carrée de a dans \mathbb{F}_p .

Remarque : il y a des méthodes d'extraction de racines carrées dans \mathbb{F}_p dans le cas où $p \equiv 1 \pmod{8}$, mais a priori on ne dispose pas de formules simples.

Exercice 6

Soit K un corps fini de cardinal q . Soit $f : K \rightarrow K$ une application. Montrer qu'il existe un unique polynôme P à coefficients dans K , de degré strictement plus petit que q , tel que f soit la fonction polynôme associée à P .

Exercice 7 (Théorème de Wolstenholme)

Soit p un nombre premier ≥ 5 . Posons

$$S = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}.$$

On a $S = \frac{N}{D}$ où N et D sont des entiers premiers entre eux. L'objectif de cet exercice est de démontrer que N est divisible par p^2 , résultat établi par Wolstenholme en 1862.

- 1) Montrer que D n'est pas divisible par p .
- 2) En regroupant les termes de S deux à deux, sous la forme $\frac{1}{k} + \frac{1}{p-k}$, montrer que p divise N .
- 3) Montrer que $\frac{N}{p}$ modulo p est égal, à un facteur près, à la somme des carrés de \mathbb{F}_p^* .
- 4) En déduire le résultat.

Indication : utiliser l'exercice 2.

Exercice 8

Considérons l'anneau quotient

$$K = \mathbb{F}_2[X]/(X^4 + X + 1).$$

- 1) Montrer que K est un corps.
- 2) Quelle est sa caractéristique ? Quel est son cardinal ?

Soit α la classe de X modulo $(X^4 + X + 1)$.

On rappelle que le système $\mathcal{B} = (1, \alpha, \alpha^2, \alpha^3)$ est une base du \mathbb{F}_2 -espace vectoriel K .

- 3) Déterminer les coordonnées de $\alpha^7 + 1$ dans \mathcal{B} .
- 4) Déterminer les coordonnées de l'inverse de $\alpha^7 + 1$ dans \mathcal{B} .
- 5) Quels sont les ordres possibles des éléments du groupe K^* ?
- 6) Montrer que α est un générateur de K^* . Combien y a-t-il de générateurs dans K^* ?
- 7) Quel est l'ordre de $\alpha + \alpha^2$ dans K^* ?
- 8) Montrer que le polynôme $P = Y^3 + Y + 1$ est irréductible dans l'anneau $K[Y]$. Déterminer le cardinal de $K[Y]/(P)$.

Exercice 9

Soient ℓ et p des nombres premiers. Quel est le nombre de polynômes unitaires irréductibles de degré ℓ dans $\mathbb{F}_p[X]$?

Exercice 10

Soit K un corps fini de cardinal p^n (où p est premier). Montrer que tout élément de K^* , autre que 1, est un générateur de K^* si et seulement si l'une des deux conditions suivantes est satisfaite :

- (1) on a $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$.
- (2) On a $p = 2$ et $2^n - 1$ est un nombre premier.

Exercice 11

Dans $\mathbb{F}_5[X]$, posons $f = X^3 + X + 1$. Considérons l'anneau quotient

$$K = \mathbb{F}_5[X]/(f).$$

- 1) Montrer que K est un corps.
- 2) Quelle est sa caractéristique ? Quel est son cardinal ?
- 3) Quels sont les ordres possibles des éléments de K^* ?

Soit α la classe de X modulo (f) . On rappelle que le système $\mathcal{B} = (1, \alpha, \alpha^2)$ est une base du \mathbb{F}_5 -espace vectoriel K .

- 4) Expliciter les développements de α^3 , α^{15} et α^{30} dans \mathcal{B} .
- 5) En déduire l'ordre de α , et celui de 2α , dans K^* .
- 6) Déterminer les coordonnées de l'inverse de $\alpha + 1$ dans \mathcal{B} .
- 7) Que vaut $f(\alpha^5)$? En déduire les racines de f dans K . On écrira leurs développements dans la base \mathcal{B} .

Exercice 12

Soient p un nombre premier et u un élément non nul de \mathbb{F}_p . Posons

$$f = X^p - X + u \in \mathbb{F}_p[X].$$

On se propose de montrer que f irréductible sur \mathbb{F}_p . Rappelons qu'il existe un corps fini K contenant \mathbb{F}_p dans lequel f possède une racine α (cf. le th. 5.11, utilisé avec un facteur irréductible de f).

- 1) Montrer que pour tout $a \in \mathbb{F}_p$, on a $f(a + \alpha) = 0$.
- 2) En déduire que les racines de f sont les $a + \alpha$ où $a \in \mathbb{F}_p$.
- 3) Supposons f réductible sur \mathbb{F}_p . Soit $g \in \mathbb{F}_p[X]$ un diviseur de f , non constant et de degré strictement plus petit que p .
 - 3.1) Montrer que la somme des racines de g appartient à \mathbb{F}_p .

3.2) En déduire une contradiction et le résultat.

Exercice 13

Considérons l'anneau

$$K = \mathbb{F}_2[X]/(X^6 + X + 1).$$

Soit α la classe de X modulo l'idéal $(X^6 + X + 1)$.

- 1) Montrer que K est un corps. Quel est son cardinal ?
- 2) Montrer que α est un générateur de K^* .
- 3) L'élément α est-il un carré dans K ?
- 4) Résoudre dans K l'équation $x^2 + x + 1 = 0$.

Indication : remarquer que pour tout $x \in K$, on a $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

Exercice 14 (Protocole de Diffie-Hellman)

Considérons l'anneau

$$K = \mathbb{F}_3[X]/(X^2 + 1).$$

Soit α la classe de X modulo l'idéal $(X^2 + 1)$.

- 1) Montrer que K est un corps et que $1 + \alpha$ est un générateur de K^* .
- 2) Deux personnes, Alice et Bob, souhaitent se construire une clé commune de chiffrement, en utilisant le protocole de Diffie-Hellman avec le couple public

$$(K, 1 + \alpha).$$

Alice transmet à Bob l'élément α , et Bob transmet à Alice l'élément $2 + \alpha$. Quelle est leur clé de chiffrement ? On déterminera ses coordonnées dans la base $(1, \alpha)$ du \mathbb{F}_3 -espace vectoriel K .

Exercice 15 (Algorithme de El Gamal)

Alice souhaite se faire envoyer des messages confidentiellement en utilisant l'algorithme de El Gamal. Pour cela, elle utilise le corps

$$K = \mathbb{F}_2[X]/(X^4 + X + 1)$$

étudié dans l'exercice 8 et l'élément $\alpha = X + (X^4 + X + 1)$, qui rappelons-le est un générateur de K^* . Elle choisit par ailleurs un entier a compris entre 1 et 14 pour lequel on a l'égalité

$$\alpha^a = 1 + \alpha^2.$$

Bob envoie publiquement à Alice le message $(\alpha^3, \alpha + \alpha^2 + \alpha^3)$. Quel est le message secret que Bob souhaite lui transmettre ?