TD2-Corps finis

Thierno Mamoudou SABALY

Master 1 - Transmission des Données et Sécurité de l'Information
Option Mathématiques-Cryptographie

04 janvier 2022

Sommaire

Exercice 01

Question 1

Question 1

Montrer que $X^2 + X + 1$ est le seul polynôme unitaire irréductible de dégré 2 sur $\mathbb{F}_2$

Solution

Les autres polynômes unitaires de dégré 2 sur $\mathbb{F}_2$ sont : $X^2 + X$, $X^2 + 1$ et X^2.

Question 1

Montrer que $X^2 + X + 1$ est le seul polynôme unitaire irréductible de dégré 2 sur $\mathbb{F}_2$

Solution

Les autres polynômes unitaires de dégré 2 sur $\mathbb{F}_2$ sont : $X^2 + X$, $X^2 + 1$ et X^2.Pour chacun d'eux, nous avons bien une factorisation. En effet :

- $X^2 + X = X(X + 1)$
- $X^2 + 1 = (X + 1)(X + 1)$
- $X^2 = X \times X$

Exercice 01

Question 1

Question 1

Montrer que $X^2 + X + 1$ est le seul polynôme unitaire irréductible de dégré 2 sur $\mathbb{F}_2$

Solution

Les autres polynômes unitaires de dégré 2 sur $\mathbb{F}_2$ sont : $X^2 + X$, $X^2 + 1$ et X^2.Pour chacun d'eux, nous avons bien une factorisation. En effet :

- $X^2 + X = X(X + 1)$
- $X^2 + 1 = (X + 1)(X + 1)$
- $X^2 = X \times X$

Alors il ne reste plus qu'à vérifier que $f(X) = X^2 + X + 1$ est irreductible sur $\mathbb{F}_2$, pour cela par l'absurde, supposons que f soit réductible.

Exercice 01

Question 01

Alors $f(X) = (X+a)(X+b);\ a, b \in \mathbb{F}_2$. Donc 0 ou 1 est solution de $f(X) = 0$ or on a $f(0) = f(1) = 1$ ce qui est contradictoire. Donc f est irréductible.

Question 02

Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

Solution

Soit $P(X) = X^4 + 1$. Par l'absurbe supposons que P est réductible sur $\mathbb{Q}$ alors $P(X) = Q(X)T(X)$ avec $Q, T \in \mathbb{Q}[X]$. On a soit $deg(Q) = 1$ et $deg(T) = 3$ ou $deg(Q) = 2$ et $deg(T) = 2$.

Question 02

Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

Solution

Soit $P(X) = X^4 + 1$. Par l'absurbe supposons que P est réductible sur $\mathbb{Q}$ alors $P(X) = Q(X)T(X)$ avec $Q, T \in \mathbb{Q}[X]$. On a soit $deg(Q) = 1$ et $deg(T) = 3$ ou $deg(Q) = 2$ et $deg(T) = 2$.

1. $deg(Q) = 1 \implies \exists \frac{a}{b} \in \mathbb{Q}/P(\frac{a}{b}) = 0 \implies a^4 = -b^4 < 0$ (impossible)

Question 02

Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

Solution

Soit $P(X) = X^4 + 1$. Par l'absurbe supposons que P est réductible sur $\mathbb{Q}$ alors $P(X) = Q(X)T(X)$ avec $Q, T \in \mathbb{Q}[X]$. On a soit $deg(Q) = 1$ et $deg(T) = 3$ ou $deg(Q) = 2$ et $deg(T) = 2$.

1. $deg(Q) = 1 \implies \exists \frac{a}{b} \in \mathbb{Q}/P(\frac{a}{b}) = 0 \implies a^4 = -b^4 < 0$ (impossible)
2. $deg(Q) = 2$ alors on peut écrire $Q(X) = X^2 + \alpha X + 1$ et $T(X) = X^2 + \beta X + 1$ avec $\alpha, \beta \in \mathbb{Q}$
   $Q(X)T(X) = X^4 + (\alpha + \beta)X^3 + (2 + \alpha\beta)X^2 + (\alpha + \beta)X + 1.$
   Par identification, on a :

$\alpha + \beta = 0$ et $2 + \alpha\beta = 0 \implies 2 - \alpha^2 = 0 \implies \alpha^2 = 2$. Cette dernière équation n'a pas de solution dans $\mathbb{Q}$.

Exercice 01

Question 02

$\alpha + \beta = 0$ et $2 + \alpha\beta = 0 \implies 2 - \alpha^2 = 0 \implies \alpha^2 = 2$. Cette dernière équation n'a pas de solution dans $\mathbb{Q}$.
Alors aucune décomposition de $X^4 + 1$ n'est possible dans $\mathbb{Q}$, d'où $X^4 + 1$ est irréductible dans $\mathbb{Q}$.

Question 03

Montrer que le polynôme $X^4 + 1$ est réductible sur $\mathbb{F}_p$, p premier.

Solution

Trouvons une factorisation de $X^4 + 1$. On a :

(i) Soit il existe une racine $\mu \in \mathbb{F}_p$

(ii) Soit $X^4 + 1 = (X^2 + \alpha X + a)(X^2 + \beta X + a^{-1})$ avec $\alpha, a \in F_p$

.

Question 03

Montrer que le polynôme $X^4 + 1$ est réductible sur $\mathbb{F}_p$, p premier.

Solution

Trouvons une factorisation de $X^4 + 1$. On a :

(i) Soit il existe une racine $\mu \in \mathbb{F}_p$

(ii) Soit $X^4 + 1 = (X^2 + \alpha X + a)(X^2 + \beta X + a^{-1})$ avec $\alpha, a \in F_p$

.

(i) Si μ est racine alors $\mu^4 = -1 \implies \mu^8 = 1 \implies ord(\mu)|8$. Comme $\mu^4 = -1$ alors $ord(\mu) \notin \{1, 2, 4\} \implies ord(\mu) = 8 \implies 8|p - 1 \implies p = 8k + 1$.

Question 03

Montrer que le polynôme X^4+1 est réductible sur $\mathbb{F}_p$, p premier.

Solution

Trouvons une factorisation de X^4+1. On a :

(i) Soit il existe une racine $\mu \in \mathbb{F}_p$

(ii) Soit $X^4+1=(X^2+\alpha X+a)(X^2+\beta X+a^{-1})$ avec $\alpha, a \in F_p$

.

(i) Si μ est racine alors $\mu^4=-1 \implies \mu^8=1 \implies ord(\mu)|8$. Comme $\mu^4=-1$ alors $ord(\mu)\notin\{1,2,4\} \implies ord(\mu)=8 \implies 8|p-1 \implies p=8k+1$.
Si $p=8k+1$ alors $X^4+1=(X-\mu)Q(x)$

Question 03

Montrer que le polynôme $X^4 + 1$ est réductible sur $\mathbb{F}_p$, p premier.

Solution

Trouvons une factorisation de $X^4 + 1$. On a :

(i) Soit il existe une racine $\mu \in \mathbb{F}_p$

(ii) Soit $X^4 + 1 = (X^2 + \alpha X + a)(X^2 + \beta X + a^{-1})$ avec $\alpha, a \in F_p$

.

(i) Si μ est racine alors $\mu^4 = -1 \implies \mu^8 = 1 \implies ord(\mu)|8$.
Comme $\mu^4 = -1$ alors $ord(\mu) \notin \{1, 2, 4\} \implies ord(\mu) = 8 \implies 8|p - 1 \implies p = 8k + 1$.
Si $p = 8k + 1$ alors $X^4 + 1 = (X - \mu)Q(x)$
Il reste alors à évoluer les cas ou $p \in \{8k + 3, 8k + 5, 8k + 7\}$.

exercice 01

Question 03

(ii) Si $X^4+1=(X^2+\alpha X+a)(X^2+\beta X+a^{-1})$ avec $\alpha, a \in F_p$ alors on a
$X^4+1=X^4+(\alpha+\beta)X^3+(a+a^{-1}+\alpha\beta)X^2+(a^{-1}\alpha+a\beta)X+1$;

(ii) Si $X^4+1=(X^2+\alpha X+a)(X^2+\beta X+a^{-1})$ avec $\alpha, a \in F_p$ alors on a $X^4+1=X^4+(\alpha+\beta)X^3+(a+a^{-1}+\alpha\beta)X^2+(a^{-1}\alpha+a\beta)X+1$;Et donc par identification,

$$\begin{cases} \alpha + \beta = 0 \\ a + a^{-1} + \alpha\beta = 0 \\ a^{-1}\alpha + a\beta = 0 \end{cases}$$

On a alors,

$$\begin{cases} \beta & = & -\alpha \\ \alpha^2 & = & a + a^{-1} \\ \alpha(a^{-1} - a) = 0 \end{cases}$$

On a alors,

$$\begin{cases} \beta = -\alpha \\ \alpha^2 = a + a^{-1} \\ \alpha(a^{-1} - a) = 0 \end{cases}$$

$\Longrightarrow \alpha = 0$ ou $a = a^{-1}$. Traitons séparément ces 2 cas.

On a alors,

$$\begin{cases} \beta & = & -\alpha \\ \alpha^2 & = & a + a^{-1} \\ \alpha(a^{-1} - a) = 0 \end{cases}$$

$\implies \alpha = 0$ ou $a = a^{-1}$. Traitons séparément ces 2 cas.

1. $\alpha = 0 \implies a^2 = -1 \implies -1$ est un résidu quadratique . Par la formule de Legendre, on a $(\frac{-1}{p}) = 1$ or

$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p = 8k + 5.$

On a alors,

$$\begin{cases} \beta & = & -\alpha \\ \alpha^2 & = & a + a^{-1} \\ \alpha(a^{-1} - a) = 0 \end{cases}$$

$\Longrightarrow \alpha = 0$ ou $a = a^{-1}$. Traitons séparément ces 2 cas.
1. $\alpha = 0 \Longrightarrow a^2 = -1 \Longrightarrow -1$ est un résidu quadratique . Par la formule de Legendre, on a $(\frac{-1}{p}) = 1$ or
$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p = 8k + 5.$
Si $p = 8k + 5, X^4 + 1 = (X^2 + a)(X^2 - a)$ avec $a^2 = -1$

2. $a = a^{-1} \implies \alpha^2 = 2a$.

2. $a = a^{-1} \implies \alpha^2 = 2a$. D'autre part
$a = a^{-1} \implies a = 1$ ou $a = p - 1 = -1$

2. $a = a^{-1} \implies \alpha^2 = 2a$. D'autre part
$a = a^{-1} \implies a = 1$ ou $a = p - 1 = -1$

- Si $p = 8k + 3$ alors par la formule de Legendre, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = -1 \implies 2$ n'est pas résidu quadratique. On choisi a tel que $2a$ soit un résidu quadratique, donc $(\frac{2a}{p}) = (\frac{2}{p})(\frac{a}{p}) = -1 \times (\frac{a}{p}) \implies (\frac{a}{p}) = -1 \implies a = -1$.

2. $a = a^{-1} \implies \alpha^2 = 2a$. D'autre part
$a = a^{-1} \implies a = 1$ ou $a = p - 1 = -1$

- Si $p = 8k + 3$ alors par la formule de Legendre, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = -1 \implies 2$ n'est pas résidu quadratique. On choisi a tel que $2a$ soit un résidu quadratique, donc $(\frac{2a}{p}) = (\frac{2}{p})(\frac{a}{p}) = -1 \times (\frac{a}{p}) \implies (\frac{a}{p}) = -1 \implies a = -1$.
  Si $p = 8k + 3, X^4 + 1 = (X^2 + \alpha X - 1)(X^2 - \alpha X - 1)$ avec $\alpha^2 = -2$.

2. $a = a^{-1} \implies \alpha^2 = 2a$. D'autre part
$a = a^{-1} \implies a = 1$ ou $a = p - 1 = -1$

- Si $p = 8k + 3$ alors par la formule de Legendre, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = -1 \implies 2$ n'est pas résidu quadratique. On choisi a tel que $2a$ soit un résidu quadratique, donc $(\frac{2a}{p}) = (\frac{2}{p})(\frac{a}{p}) = -1 \times (\frac{a}{p}) \implies (\frac{a}{p}) = -1 \implies a = -1$.
  Si $p = 8k + 3, X^4 + 1 = (X^2 + \alpha X - 1)(X^2 - \alpha X - 1)$ avec $\alpha^2 = -2$.
- Si $p = 8k + 7$ alors par la formule de Legendre, 2 est un résidu quadratique, il suffit alors de prendre $a = 1$. Et on a

2. $a = a^{-1} \implies \alpha^2 = 2a$. D'autre part
$a = a^{-1} \implies a = 1$ ou $a = p - 1 = -1$

- Si $p = 8k + 3$ alors par la formule de Legendre, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = -1 \implies 2$ n'est pas résidu quadratique. On choisi a tel que $2a$ soit un résidu quadratique, donc $(\frac{2a}{p}) = (\frac{2}{p})(\frac{a}{p}) = -1 \times (\frac{a}{p}) \implies (\frac{a}{p}) = -1 \implies a = -1$.
  Si $p = 8k + 3, X^4 + 1 = (X^2 + \alpha X - 1)(X^2 - \alpha X - 1)$ avec $\alpha^2 = -2$.
- Si $p = 8k + 7$ alors par la formule de Legendre, 2 est un résidu quadratique, il suffit alors de prendre $a = 1$. Et on a
  Si $p = 8k + 7, X^4 + 1 = (X^2 + \alpha X + 1)(X^2 - \alpha X + 1)$ avec $\alpha^2 = 2$.

2. $a = a^{-1} \implies \alpha^2 = 2a$. D'autre part
$a = a^{-1} \implies a = 1$ ou $a = p - 1 = -1$

- Si $p = 8k + 3$ alors par la formule de Legendre, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = -1 \implies 2$ n'est pas résidu quadratique. On choisi a tel que $2a$ soit un résidu quadratique, donc $(\frac{2a}{p}) = (\frac{2}{p})(\frac{a}{p}) = -1 \times (\frac{a}{p}) \implies (\frac{a}{p}) = -1 \implies a = -1$.
  Si $p = 8k + 3, X^4 + 1 = (X^2 + \alpha X - 1)(X^2 - \alpha X - 1)$ avec $\alpha^2 = -2$.
- Si $p = 8k + 7$ alors par la formule de Legendre, 2 est un résidu quadratique, il suffit alors de prendre $a = 1$. Et on a
  Si $p = 8k + 7, X^4 + 1 = (X^2 + \alpha X + 1)(X^2 - \alpha X + 1)$ avec $\alpha^2 = 2$.

D'où pour tout nombre premier $p, X^4 + 1$ est réductible sur $\mathbb{F}_p$.

Question 04

Déterminer tous les polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$.

Solution

Il est plus aisé de lister les réductibles et ensuite en déduire les irréductibles.
Les réductibles

Question 04

Déterminer tous les polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$.

Solution

Il est plus aisé de lister les réductibles et ensuite en déduire les irréductibles.
Les réductibles

- 0 est racine : $X^3, X(X^2+X+1) = X^3+X^2+X$

Question 04

Déterminer tous les polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$.

Solution

Il est plus aisé de lister les réductibles et ensuite en déduire les irréductibles.
Les réductibles

- 0 est racine : $X^3, X(X^2+X+1) = X^3+X^2+X$
- 0 et 1 sont racines : $X(X^2+1) = X^3+X, X(X^2+X) = X^3+X^2$

Question 04

Déterminer tous les polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$.

Solution

Il est plus aisé de lister les réductibles et ensuite en déduire les irréductibles.
Les réductibles

- 0 est racine : $X^3, X(X^2+X+1) = X^3+X^2+X$
- 0 et 1 sont racines : $X(X^2+1) = X^3+X, X(X^2+X) = X^3+X^2$
- 1 est racine : $(X+1)(X^2+1) = X^3+X^2+X+1, (X+1)(X^2+X+1) = X^3+1$

Question 04

Déterminer tous les polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$.

Solution

Il est plus aisé de lister les réductibles et ensuite en déduire les irréductibles.
Les réductibles

- 0 est racine : $X^3, X(X^2+X+1) = X^3+X^2+X$
- 0 et 1 sont racines : $X(X^2+1) = X^3+X, X(X^2+X) = X^3+X^2$
- 1 est racine : $(X+1)(X^2+1) = X^3+X^2+X+1, (X+1)(X^2+X+1) = X^3+1$

Question 04

Déterminer tous les polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$.

Solution

Il est plus aisé de lister les réductibles et ensuite en déduire les irréductibles.
Les réductibles

- 0 est racine : $X^3, X(X^2+X+1) = X^3+X^2+X$
- 0 et 1 sont racines : $X(X^2+1) = X^3+X, X(X^2+X) = X^3+X^2$
- 1 est racine : $(X+1)(X^2+1) = X^3+X^2+X+1, (X+1)(X^2+X+1) = X^3+1$

Les irréductibles sont alors : X^3+X+1 et X^3+X^2+1.

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit
$(X+a)(X+b) = X^2 + (a+b)X + ab;\ a, b \in \mathbb{F}_3$ Ce sont alors :

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$

Exercice 01

Question 05

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$
- $a = 0, b = 2$ ou $a = 2, b = 0 \implies X^2 + 2X$

Exercice 01

Question 05

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$
- $a = 0, b = 2$ ou $a = 2, b = 0 \implies X^2 + 2X$
- $a = 1, b = 1 \implies X^2 + 2X + 1$

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit
$(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$
- $a = 0, b = 2$ ou $a = 2, b = 0 \implies X^2 + 2X$
- $a = 1, b = 1 \implies X^2 + 2X + 1$
- $a = 1, b = 2$ ou $a = 2, b = 1 \implies X^2 + 2$

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$
- $a = 0, b = 2$ ou $a = 2, b = 0 \implies X^2 + 2X$
- $a = 1, b = 1 \implies X^2 + 2X + 1$
- $a = 1, b = 2$ ou $a = 2, b = 1 \implies X^2 + 2$
- $a = 2, b = 2 \implies X^2 + X + 1$

Exercice 01

Question 05

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab$; $a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$
- $a = 0, b = 2$ ou $a = 2, b = 0 \implies X^2 + 2X$
- $a = 1, b = 1 \implies X^2 + 2X + 1$
- $a = 1, b = 2$ ou $a = 2, b = 1 \implies X^2 + 2$
- $a = 2, b = 2 \implies X^2 + X + 1$

Question 05

Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

Solution

Un polynôme réductible de degré 2 et unitaire s'écrit $(X+a)(X+b) = X^2 + (a+b)X + ab;\ a, b \in \mathbb{F}_3$ Ce sont alors :

- $a = 0, b = 0 \implies X^2$
- $a = 0, b = 1$ ou $a = 1, b = 0 \implies X^2 + X$
- $a = 0, b = 2$ ou $a = 2, b = 0 \implies X^2 + 2X$
- $a = 1, b = 1 \implies X^2 + 2X + 1$
- $a = 1, b = 2$ ou $a = 2, b = 1 \implies X^2 + 2$
- $a = 2, b = 2 \implies X^2 + X + 1$

Ainsi les irréductibles sont : $X^2 + 1$, $X^2 + X + 2$ et $X^2 + 2X + 2$.

Question 06

Les polynômes $A(X) = X^3 + X + 1$ et $B(X) = X^3 + X^2 + 1$, sont-ils irréductibles sur $\mathbb{F}_2$.

Solution

$A(X)$ et $B(X)$ sont irréductibles sur $\mathbb{F}_2$. cf. Question 04.

Exercice 01

Question 07

Question 07

Lister les éléments de $\mathbb{F}_2[X]/(A)$. En déduire ses tables d'addition et de multiplication correspondantes.

Solution

Soit $\alpha = Xmod(A(x))$, on a : $\alpha^3 + \alpha + 1 = 0 \implies \alpha^3 = \alpha + 1$;

On a :

Exercice 01

Question 07

Question 07

Lister les éléments de $\mathbb{F}_2[X]/(A)$. En déduire ses tables d'addition et de multiplication correspondantes.

Solution

Soit $\alpha = Xmod(A(x))$, on a : $\alpha^3 + \alpha + 1 = 0 \implies \alpha^3 = \alpha + 1$;

On a :

Exponentielle	polynomiale	binaire	décimal
α	α	010	2
α^2	α^2	100	4
α^3	$\alpha + 1$	011	3
α^4	$\alpha^2 + \alpha$	110	6
α^5	$\alpha^2 + \alpha + 1$	111	7
α^6	$\alpha^2 + 1$	101	5
α^7	1	001	1

Sommaire

Sommaire

Sommaire

Sommaire

Sommaire

Sommaire

Exercice 07

Question 02

Question 02

Déterminer le cardinale de $\mathbb{F}$.

Solution

$\mathbb{F} = \{a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1}, a_i \in \mathbb{F}\} \backsimeq \{(a_i)_{0\leq i\leq m-1}, a_i \in \mathbb{F}_p\}$.
On peut voir cet ensemble comme l'ensemble des m-uplets de $\mathbb{F}_p$.
Donc son cardinale c'est le nombre d'uplets possibles, c'est-à-dire p^m.
$card(\mathbb{F}) = p^m$.

Question 03

Montrer que $\mathbb{F}$, muni de l'addition $+$ des polynômes et de $\cdot$ multiplication de polynômes modulo g, est un corps.

Solution

- La somme de deux polynômes de degré inférieur ou égale à m-1 à coefficients dans $\mathbb{F}_p$ est un polynôme de degré inférieur ou égale à m-1 et à coefficients dans $\mathbb{F}_p$ (car $\mathbb{F}_p$ est un corps). Stabilité par somme

Question 03

Montrer que $\mathbb{F}$, muni de l'addition $+$ des polynômes et de $\cdot$ multiplication de polynômes modulo g, est un corps.

Solution

- La somme de deux polynômes de degré inférieur ou égale à m-1 à coefficients dans $\mathbb{F}_p$ est un polynôme de degré inférieur ou égale à m-1 et à coefficients dans $\mathbb{F}_p$ (car $\mathbb{F}_p$ est un corps). Stabilité par somme
- Le produit module g de deux polynômes de degré inférieur ou égale à m-1 est aussi un polynôme de degré inférieur ou égale à m-1 et à coefficients dans $\mathbb{F}_p$. Stabilité par produit

Question 03

Montrer que $\mathbb{F}$, muni de l'addition $+$ des polynômes et de $\cdot$ multiplication de polynômes modulo g, est un corps.

Solution

- La somme de deux polynômes de degré inférieur ou égale à m-1 à coefficients dans $\mathbb{F}_p$ est un polynôme de degré inférieur ou égale à m-1 et à coefficients dans $\mathbb{F}_p$ (car $\mathbb{F}_p$ est un corps). Stabilité par somme
- Le produit module g de deux polynômes de degré inférieur ou égale à m-1 est aussi un polynôme de degré inférieur ou égale à m-1 et à coefficients dans $\mathbb{F}_p$. Stabilité par produit
- Soit $P \in \mathbb{F}_p[X]$, alors comme g irréductible alors soit $pgcd(P,g) = g$ ou $pgcd(P,g) = 1 \implies P = 0$ ou P inversible. Or tout élement P non nul de $\mathbb{F}$ est de degré inférieur ou égale à $deg(g) \implies pgcd(P,g) = 1 \implies P$ inversible.

Exercice 07

Question 03

Example

Donc $(\mathbb{F}, +, \cdot)$ est un corps.

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k\alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_kX^k \in \mathbb{F}_p[X]$.

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k \alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_k X^k \in \mathbb{F}_p[X]$.
- $ker\phi = \{P \in \mathbb{F}_p[X] / P(\alpha) = 0\} = (g)$.

Exercice 07

Question 04

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k\alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_k X^k \in \mathbb{F}_p[X]$.
- $ker\phi = \{P \in \mathbb{F}_p[X]/P(\alpha) = 0\} = (g)$.En effet, $\forall P \in (g), P(X) = g(X)Q(x) \implies P(\alpha) = g(\alpha)Q(\alpha) = 0$

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k \alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_k X^k \in \mathbb{F}_p[X]$.
- $ker\phi = \{P \in \mathbb{F}_p[X]/P(\alpha) = 0\} = (g)$.En effet, $\forall P \in (g), P(X) = g(X)Q(x) \implies P(\alpha) = g(\alpha)Q(\alpha) = 0$ Et $\forall P \in \mathbb{F}_p[X], P(\alpha) = 0$ alors $deg(P) > deg(g)$, on a $P(X) = g(X)Q(X) + R(X), deg(R) = 0$ ou $deg(R) < deg(g)$.

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k\alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_k X^k \in \mathbb{F}_p[X]$.
- $ker\phi = \{P \in \mathbb{F}_p[X]/P(\alpha) = 0\} = (g)$.En effet, $\forall P \in (g), P(X) = g(X)Q(x) \implies P(\alpha) = g(\alpha)Q(\alpha) = 0$ Et $\forall P \in \mathbb{F}_p[X], P(\alpha) = 0$ alors $deg(P) > deg(g)$, on a $P(X) = g(X)Q(X) + R(X), deg(R) = 0$ ou $deg(R) < deg(g)$.Alors $P(\alpha) = R(\alpha) = 0 \implies deg(R) = 0$ par minimalité de g.

Exercice 07

Question 04

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k \alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_k X^k \in \mathbb{F}_p[X]$.
- $ker\phi = \{P \in \mathbb{F}_p[X] / P(\alpha) = 0\} = (g)$.En effet, $\forall P \in (g), P(X) = g(X)Q(x) \implies P(\alpha) = g(\alpha)Q(\alpha) = 0$
  Et $\forall P \in \mathbb{F}_p[X], P(\alpha) = 0$ alors $deg(P) > deg(g)$, on a $P(X) = g(X)Q(X) + R(X), deg(R) = 0$ ou $deg(R) < deg(g)$.Alors $P(\alpha) = R(\alpha) = 0 \implies deg(R) = 0$ par minimalité de g. D'où
  $R(X) = 0 \implies P(X) = g(X)Q(X) \in (g)$.

Exercice 07

Question 04

Question 04

Montrer que $\mathbb{F}$ est isomorphe à $\mathbb{F}_p[X]/(g)$.

Solution

Soit l'application : $\phi : \mathbb{F}_p[X] \to \mathbb{F}; P \mapsto P(\alpha)$.

- Surjection : soit $Y \in \mathbb{F} \implies Y = \sum_{k=0}^{m-1} a_k \alpha^k = P(\alpha)$ avec $P(X) = \sum_{k=0}^{m-1} a_k X^k \in \mathbb{F}_p[X]$.
- $ker\phi = \{P \in \mathbb{F}_p[X] / P(\alpha) = 0\} = (g)$.En effet, $\forall P \in (g), P(X) = g(X)Q(x) \implies P(\alpha) = g(\alpha)Q(\alpha) = 0$
  Et $\forall P \in \mathbb{F}_p[X], P(\alpha) = 0$ alors $deg(P) > deg(g)$, on a $P(X) = g(X)Q(X) + R(X), deg(R) = 0$ ou $deg(R) < deg(g)$.Alors $P(\alpha) = R(\alpha) = 0 \implies deg(R) = 0$ par minimalité de g. D'où $R(X) = 0 \implies P(X) = g(X)Q(X) \in (g)$.

D'après le premier théorème d'isomorphisme, on a : $\mathbb{F}_p[X]/(g) \simeq \mathbb{F}$.

Exercice 07

Question 05

Question 05

Donner de manière explicite $\mathbb{F}_{256}$.

Solution

De ce qui précède, $\mathbb{F}_{256} = \mathbb{F}_{2^8}$ c'est l'ensemble des polynômes de degré inférieur ou égale à 7 et à coefficients dans $\mathbb{F}_2$.

Exercice 07

Question 05

Question 05

Donner de manière explicite $\mathbb{F}_{256}$.

Solution

De ce qui précède, $\mathbb{F}_{256} = \mathbb{F}_{2^8}$ c'est l'ensemble des polynômes de degré inférieur ou égale à 7 et à coefficients dans $\mathbb{F}_2$.
D'où $\mathbb{F}_{256} = \{\sum_{k=0}^{7} a_k x^k ; a_k \in \{0,1\}\}$.

Question 06

Expliciter un isomorphisme entre $\mathbb{F}_{81}$ et $\mathbb{F}_9[X]/(P)$, avec P à déterminer.

Solution ! ! !

Le polynôme $g(X) = X^4 + 1$ est unitaire et irréductible sur $\mathbb{F}_9$. De ce qui précède, $\mathbb{F}_{81} \backsimeq \mathbb{F}_3[X]/(g)$.

Question 06

Expliciter un isomorphisme entre $\mathbb{F}_{81}$ et $\mathbb{F}_9[X]/(P)$, avec P à déterminer.

Solution ! ! !

Le polynôme $g(X) = X^4 + 1$ est unitaire et irréductible sur $\mathbb{F}_9$. De ce qui précède, $\mathbb{F}_{81} \backsimeq \mathbb{F}_3[X]/(g)$.Et on a
$\tilde{\phi} : \mathbb{F}_3[X]/(g) \to \mathbb{F}_{81}; \tilde{f} \mapsto \tilde{f}(\alpha)$.

Question 06

Expliciter un isomorphisme entre $\mathbb{F}_{81}$ et $\mathbb{F}_9[X]/(P)$, avec P à déterminer.

Solution ! ! !

Le polynôme $g(X) = X^4 + 1$ est unitaire et irréductible sur $\mathbb{F}_9$. De ce qui précède, $\mathbb{F}_{81} \backsimeq \mathbb{F}_3[X]/(g)$.Et on a
$\tilde{\phi} : \mathbb{F}_3[X]/(g) \to \mathbb{F}_{81}; \tilde{f} \mapsto \tilde{f}(\alpha)$.
avec $\alpha = X mod(g(X)) \implies g(\alpha) = 0 \implies \alpha^4 = -1$.

Exercice 07

question 06

Question 06

Expliciter un isomorphisme entre $\mathbb{F}_{81}$ et $\mathbb{F}_9[X]/(P)$, avec P à déterminer.

Solution ! ! !

Le polynôme $g(X) = X^4 + 1$ est unitaire et irréductible sur $\mathbb{F}_9$. De ce qui précède, $\mathbb{F}_{81} \backsimeq \mathbb{F}_3[X]/(g)$.Et on a
$\tilde{\phi} : \mathbb{F}_3[X]/(g) \to \mathbb{F}_{81}; \tilde{f} \mapsto \tilde{f}(\alpha)$.
avec $\alpha = Xmod(g(X)) \implies g(\alpha) = 0 \implies \alpha^4 = -1$.
Soit $P(X) = X^2 + X + 1$, P est irréductible sur $\mathbb{F}_9$ donc $\mathbb{F}_9[X]/(P)$ est un corps.

Exercice 07

question 06

Question 06

Expliciter un isomorphisme entre $\mathbb{F}_{81}$ et $\mathbb{F}_9[X]/(P)$, avec P à déterminer.

Solution ! ! !

Le polynôme $g(X) = X^4 + 1$ est unitaire et irréductible sur $\mathbb{F}_9$. De ce qui précède, $\mathbb{F}_{81} \backsimeq \mathbb{F}_3[X]/(g)$.Et on a
$\tilde{\phi} : \mathbb{F}_3[X]/(g) \to \mathbb{F}_{81}; \tilde{f} \mapsto \tilde{f}(\alpha)$.
avec $\alpha = Xmod(g(X)) \implies g(\alpha) = 0 \implies \alpha^4 = -1$.
Soit $P(X) = X^2 + X + 1$, P est irréductible sur $\mathbb{F}_9$ donc $\mathbb{F}_9[X]/(P)$ est un corps.
Les éléments de $\mathbb{F}_9[X]/(P)$ sont des polynômes de la forme $aX + b$ avec $a, b \in \mathbb{F}_9$. Cherchons une racine de g dans $\mathbb{F}_9[X]/(P)$

Exercice 07

question 06

Question 06

Expliciter un isomorphisme entre $\mathbb{F}_{81}$ et $\mathbb{F}_9[X]/(P)$, avec P à déterminer.

Solution ! ! !

Le polynôme $g(X) = X^4 + 1$ est unitaire et irréductible sur $\mathbb{F}_9$. De ce qui précède, $\mathbb{F}_{81} \backsimeq \mathbb{F}_3[X]/(g)$.Et on a
$\tilde{\phi} : \mathbb{F}_3[X]/(g) \to \mathbb{F}_{81}; \tilde{f} \mapsto \tilde{f}(\alpha)$.
avec $\alpha = Xmod(g(X)) \implies g(\alpha) = 0 \implies \alpha^4 = -1$.
Soit $P(X) = X^2 + X + 1$, P est irréductible sur $\mathbb{F}_9$ donc $\mathbb{F}_9[X]/(P)$ est un corps.
Les éléments de $\mathbb{F}_9[X]/(P)$ sont des polynômes de la forme $aX + b$ avec $a, b \in \mathbb{F}_9$. Cherchons une racine de g dans $\mathbb{F}_9[X]/(P)$
$g(aX + b) = (aX + b)^4 + 1 =$
$2a^3bX^3 + 6a^2b^2X^2 + 4ab^3X + b^4 - a^4 + 1 = 0 \implies b = 0$ et $a^4 = 1$.
On peut alors prendre $a = 1 \implies aX + b = Xmod(P(X)) = \beta$.

Sommaire

Exercice 08

Question 01