Arithmétique et applications, combinatoire et graphes

Contrôle No. 1, 13 fevrier 2019, corps finis

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

1. Factoriser le polynôme $x^4 + x^3 + x + 1$ en polynômes irréductibles sur $\mathbb{F}_2 = \mathbf{Z}/2\mathbf{Z}$.

2. Montrer que le polynôme $x^4 + x + 1$ est irréductible sur $\mathbb{F}_2$.

Soit $\mathbb{K}$ le corps $\mathbb{K} = \dfrac{\mathbb{F}_2[x]}{(x^4 + x + 1)}$.

3. Combien d'éléments y a-t-il dans $\mathbb{K}$?

4. Calculer l'inverse multiplicative de $x^2 + 1$ dans $\mathbb{K}$.

5. Est-ce-que le polynôme $x^4 + x + 1$ est primitif, vu comme un polynôme sur $\mathbb{F}_2$?

6. Soit $a = \overline{x} = x + (x^4 + x + 1) \in \mathbb{K}$ et soit $f(x) = x^6 + x^4 + x^2 + 1$. Calculer $f(a^4)$.

7. Quel est le polynôme minimal de a, de a^2, de a^4 ?

1. Soit $f(x) = x^4 + x^3 + x + 1$: $f(0) = 1$, $f(1) = 0$ (mod 2)
d'où $x+1$ est facteur:

$$x^4 + x^3 + x + 1 = (x+1)(x^3+1) \quad \text{(inspection)}$$

x^3+1 a aussi $x+1$ comme facteur: $x^3+1 = (x+1)(x^2+x+1)$

Enfin x^2+x+1 est irréductible car il ne s'annulle pas lorsque $x=0$ ou $x=1$:

$$x^4 + x^3 + x + 1 = (x+1)^2(x^2+x+1)$$

2. Soit $f(x) = x^4 + x + 1$, $f(0) = f(1) = 1$ (mod 2) $\Rightarrow$ pas de facteur linéaire.

Supposons $x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ (seule possibilité)

On compare coefficients:
$0 = a+b$ (coefft de x^3)
$0 = ab$ (coefft. de x^2)
$1 = a+b$ (coefft. de x)

Ce système est incompatible, d'où x^4+x+1 est irréductible

3. $\mathbb{K}$ contient 2^4 éléments : le nombre de polynômes de degré ≤ 3.

4. $x^4 + x + 1 = (x^2+1)(x^2+1) + x$
$x^2+1 = x \cdot x + 1$

$1 = x^2+1 + x \cdot x$
$= x^2+1 + x\left(x^4+x+1 + (x^2+1)(x^2+1)\right)$
$= \underbrace{x(x^4+x+1)}_{0} + \left(1 + x(x^2+1)\right)(x^2+1)$

Inverse multiplicatif: $1 + x(x^2+1) = x^3+x+1$

vérification $(x^3+x+1)(x^2+1) \stackrel{?}{=} x^5 + x^2 + x + 1 = x(x+1) + x^2+x+1 = 1$
(car $x^4 = x+1$ dans $\mathbb{K}$)

5. ~~Oui, car $2^4 - 1$ $|\mathbb{K}^*| = 2^4 - 1$~~

... SUITE

5. x^4+x+1 est primitif ?

Soit $a = \bar{x} = x + (x^4+x+1) \in \mathbb{K}$.

Alors $a^4 = a+1$. D'autre part $|\mathbb{K}^*| = 2^4-1=15$

donc chaque élément de $\mathbb{K}^*$ a ordre 1, 3, 5 ou 15. (les facteurs de 15)

1	1
a	a
a^2	a^2
a^3	a^3
a^4	$a+1$
a^5	a^2+a
a^6	a^3+a^2

Puisque ordre a est > 5, il est nécessairement d'ordre 15 d'où il ~~engen~~ engendre $\mathbb{K}^*$ et x^4+x+1 est primitif.

6. $f(a) = a^6+a^4+a^2+1 = a^3+a^2+a+1+a^2+1 = \cancel{a^3+a^2}\ a^3+a$ (tableau)

On continue le tableau

a^7	$a^4+a^3 = a^3+a+1$
a^8	$a^4+a^2+a = a^2+1$
a^9	a^3+a

a^7	$a^4+a^3 = a^3+a+1$
a^8	a^4+a^2+a
a^9	$a^4+a^3+a^2 = a^3+a^2+a+1$
a^{10}	$a^4+a^3+a^2+a = a^3+a^2+1$
a^{11}	$a^4+a^3+a = a^3+1$
a^{12}	$a^4+a =$

d'où $f(a) = a^3+a = a^9$.

Fröbenius : $f(a^4) = f(a^2)^2 = f(a)^4 = a^{4\times 9} = a^{36} = a^6$ (car $a^{15}=1$)

d'où $f(a^4) = a^6 = a^3+a^2$

7. Le poly minimal de a est ~~$f(x)$~~ $m(x) = x^4+x+1$

Fröbenius: ~~$f(a^2) = f(a)^2$~~ $m(a^2) = m(a)^2 = 0 \Rightarrow m(x)$ poly mini de a^2

Fröbenius: ~~$f(a^4)$~~ $m(a^4) = m(a^2)^2 = 0 \Rightarrow m(x)$ poly mini de a^4.