Arithmétique et applications, combinatoire et graphes

Contrôle No. 1, 12 fevrier 2020, 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 $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

2. Montrer que le polynôme $x^4 + x^3 + x^2 + x + 1$ est irréductible sur $\mathbb{F}_2$.

Soit $\mathbb{K}$ le corps $\mathbb{K} = \dfrac{\mathbb{F}_2[x]}{(x^4 + x^3 + x^2 + x + 1)}$.

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 $x^4 + x^3 + x^2 + x + 1$ est primitif, vu comme un polynôme sur $\mathbb{F}_2$?

6. Soit $a = \overline{x} = x + (x^4 + x^3 + x^2 + x + 1) \in \mathbb{K}$ et soit $f(x) = x^6 + x^4 + x^2 + 1$. Calculer $f(a^4)$ comme une puissance de a.

7. Quels sont les polynômes minimaux de a, de a^2, de a^4 ?

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

Ensuite $x+1$ est facteur de x^3+1 : $x^3 + 1 = (x^2+x+1)(x+1)$

Enfin x^2+x+1 est irréductible étant non-nul sur $\mathbb{F}_2 = \{0, 1\}$.

$$\boxed{x^4 + x^3 + x + 1 = (x+1)^2(x^2 + x + 1)}$$

2. Soit $f(x) = x^4 + x^3 + x^2 + x + 1$, alors $f(0) \neq 0$ et $f(1) \neq 0$ donc aucun facteur de degré 1. Supposons

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

En comparant les coefficients
x^3: $1 = a + c$
x^2: $1 = b + d + ac$
x: $1 = bc + ad$
x^0: $1 = bd$

d'où $b = d = 1$ et $\begin{cases} 1 = a + c \\ 1 = ac \end{cases}$. Mais $1 = ac \Rightarrow a = c = 1$ qui est incompatible avec $1 = a + c$

donc irréductible.

3. $\mathbb{K}$ contient 2^4 éléments

4. On effectue une division euclidienne :

$$x^4+x^3+x^2+x+1 = (x^2+x+0)(x^2+1) + 1$$

Dans le corps $\quad \overline{0} = \overline{(x^2+x)}\,\overline{(x^2+1)} + \overline{1}$

C'est à dire l'inverse multiplicatif est $\boxed{x^2+x}$

On vérifie : $\quad (x^2+x)(x^2+1) = x^4+x^3+x^2+x$
$\quad = (x^3+x^2+x+1)+x^3+x^2+x = 1.$

5. Soit $a=\bar{x}\in\mathbb{K}$. On calcule ses puissances
On note que $a^4 = a^3+a^2+a+1$

D'abord, par la partie 3, le polynôme est irréductible

a^0	1
a	a
a^2	a^2
a^3	a^3
a^4	a^3+a^2+a+1
a^5	$a^4+a^3+a^2+a = a^3+a^2+a+1+a^3+a^2+a = 1$

Donc a est d'ordre 5, et ne peut pas engendrer le groupe multiplicatif $\mathbb{K}^*$ qui est d'ordre $2^4-1=15$

<u>Le polynôme n'est pas primitif</u>

6. D'abord, on calcule $f(a)$ et puis on applique le morphisme de Fröbenius :

$$f(a) = a^6+a^4+a^2+1 = a+a^4+a^2+1$$
$$= a+(a^3+a^2+a+1)+a^2+1$$
$$= a^3$$

Par le morphisme de Fröbenius : $\phi(x)=x^2$
$f(a^2)=f(a)^2$ et $f(a^4)=f(a^2)^2 = f(a)^4$
Donc $f(a^4)=f(a)^4 = a^{12} = a^2$

7. Étant irréductible, le polynôme minimal de a est $p(x)=x^4+x^3+x^2+x+1$, car $p(a)=0$ dans $\mathbb{K}$.
Par le morphisme de Fröbenius $p(a^2)=p(a)^2=0$
donc $p(x)$ annulle a^2 ; il est donc le polynôme minimal de a^2.
Aussi $p(a^4)=p(a^2)^2=0$; il est aussi le polynôme minimal de a^4.