Arithmétique Des Polynômes

Plan

Cadre

Toutes les constructions présentées ci-dessous fonctionnent pour $K[X]$, où K est un corps, mais on s'intéresse principalement au cas $K = \mathbb{F}_2$.

- La définition et les propriétés élémentaires de l'anneau $\mathbb{F}_2[X]$ sont détaillées sur le support
- En résumé : $(\mathbb{F}_2[X], +, \times)$ est un anneau commutatif, **et** un $\mathbb{F}_2[X]$-espace vectoriel
- La « taille » d'un polynôme est mesurée par la fonction degré $\deg : \mathbb{F}_2[X] \setminus \{0\} \longrightarrow \mathbb{N}$ qui donne le plus grand exposant apparaissant dans l'écriture d'un polynôme
- on définit aussi $\deg(0) = -\infty$ (symbole « complétant » la relation d'ordre sur les entiers et signifiant ici *plus petit que tout entier relatif*)

Exemple

$$\begin{aligned}(1+X^2)(1+X+X^3) &= 1+X+X^3+X^2+X^3+X^5 \\ &= 1+X+X^2+X^5\end{aligned}$$

Division Euclidienne

Soit A et B des polynômes de $\mathbb{F}_2[X]$, $B \neq 0$.
Il existe deux polynômes Q et R, **uniquement déterminés**, appelés *quotient* et *reste* de la division euclidienne de A par B, tels que :

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Exemple

Division euclidienne de $X^2 + X^5$ par $(1 + X + X^3)$:

$$X^2 + X^5 = (1 + X + X^3)(1 + X^2) + 1 + X$$

Remarques.

- L'algorithme d'Euclide (étendu, coefficients de Bézout, ...) fonctionne encore dans l'anneau (euclidien) $\mathbb{F}_2[X]$
- Les polynômes à coefficients dans $\mathbb{F}_2$ se représentent de manière évidente par des mots binaires (et « réciproquement »)
- Les codes détecteurs/correcteurs d'erreurs modernes s'appuient sur cette identification (voir exemple du CRC en TD)

Plan

Congruences sur $\mathbb{F}_2[X]$

Soit $G \in \mathbb{F}_2[X]$.
On définit une relation d'équivalence sur $\mathbb{F}_2[X]$ par

$$P \equiv Q \mod G \text{ si } P - Q \text{ est un multiple de } G$$

Exemple

$$1 + X \equiv 1 + X + X^2 \equiv 1 + X + X^2 + X^4 \mod X^2$$

Proposition

1. Deux polynômes sont congrus modulo G si, et seulement si, ils ont le même reste modulo G
2. Un système de représentants des classes modulo G est donné par les restes possibles de la division euclidienne par G
3. Si $\deg(G) = n$, il y a donc 2^n classes d'équivalences

On note $\mathbb{F}_2[X]/(G)$ l'ensemble des classes d'équivalence modulo G (ou quotient de $\mathbb{F}_2[X]$ par la relation de congruence modulo G).

Exemple

$$\mathbb{F}_2[X]/(X^2) = \{\overline{0}, \overline{1}, \overline{X}, \overline{1+X}\}$$

Comme dans le cas de $\mathbb{Z}/n\mathbb{Z}$, le quotient « hérite » de $\mathbb{F}_2[X]$ une **structure d'anneau** (loi de groupe additive avec $\overline{0}$ pour neutre, loi multiplicative avec $\overline{1}$ pour neutre, distributivité).

Addition modulo X^2 :

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

Multiplication modulo X^2 :

$\times$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	0	X
$1+X$	0	$1+X$	X	1

Plan

On se place sur un anneau quotient $A = \mathbb{F}_2[X]/(G)$

Définition

Soit $f \in A$. On dit que f est un (élément) inversible de A s'il existe $g \in A$ tel que $fg = 1 \in A$.

Exemples

1. Pour $G = X^2$, $1 + X$ est inversible, mais pas X.
2. Considérons la multiplication dans $\mathbb{F}_2[X]/(1 + X + X^2)$

$\times$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

Tous les élements non nuls sont inversibles !

Définition

Soit $P \in \mathbb{F}_2[X]$. On dit que P est irréductible s'il n'a pas de diviseur « non triviaux », c'est-à-dire autre que les constantes et lui-même.

Théorème

On a équivalence entre

1. P est irréductible dans $\mathbb{F}_2[X]$
2. $\mathbb{F}_2[X]/(P)$ est un corps

Démonstration.

On peut recopier *mutatis mutandis* la démonstration de « $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier » □

Corollaire

Pour tout premier p, et tout entier n, il existe un corps de cardinal p^n.

Exemple

Le corps de Rijndael/AES :

1. $P = X^8 + X^4 + X^3 + X + 1$ est un polynôme irréductible
2. Par suite $\mathbb{F}_2[X]/(P)$ est un corps à $2^8 = 256$ élements
3. Ses éléments s'identifient à des octets ...