# Polynômes à coefficient dans F2

## EX1 :

### 1 \

Un corps commutatif est un anneau commutatif dans lequel l'ensemble des éléments non nuls est un groupe commutatif pour la multiplication.

F2 est muni de deux opérations binaires ⊕ et ⊗ rendant possible l'addition, la soustraction, la multiplication et la division

(F2, ⊕) est un groupe Abélien dont l'élément neutre est noté 0 (tableau 1)

(F2, ⊗) est un groupe Abélien dont l'élément neutre est 1 (tableau 2)

La multiplication est distributive à gauche par rapport à l'addition

(a ⊕ b ) ⊗ c = a ⊗ c ⊕ b ⊗ c et a ⊗ (b ⊕ c) = a ⊗ b ⊕ a ⊗ c

On a F2 à un nombre fini d'élément égal à 2 (0 et 1) et d'après le théorème de Wedderburn, Tout corps qui est fini est nécessairement commutatif

* D'où (F2, ⊕, ⊗) est un corps commutatif

### 2\

⊕ est assimilable à un << XOR LOGIQUE ou OU exclusif>>

⊗ est assimilable à un << ET LOGIQUE >>

# Registre à décalage à rétroaction linéaire

## EX3

### 1\

On va représenter les LFSR sous forme d’une liste des entiers

type LFSR = int list ;;

On va représenter les Branchements sous forme d’une liste des entiers

type branchement = int list ;;

On va stocker le résultat dans une liste d’entiers

type resultat = int list ;;

### 5\

r0 = r3 = r6 = r9 = 1,  
r1 = r2 = r4 = r5 = r7 = r8 = 0,  
rn = rn−1 ⊕ rn−3 ⊕ rn−4 ⊕ rn−7 ⊕ rn−10 si n ≥ 10 ;

//  
r0 = 1,  
r1 = r2 = 0,  
rn = rn−3 si n ≥ 3 ;

Les 20 premiers branchements :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r19 | r18 | r17 | r16 | r15 | r14 | r13 | r12 | r11 | r10 | r9 | r8 | r7 | r6 | r5 | r4 | r3 | r2 | r1 | r0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |