Exercice 1

$n = 2 \Rightarrow \mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{F}_2 = \{0; 1\}$

$\mathbb{Z}/p\mathbb{Z}$ est un corps si p est premier

$\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps :

$\{0, 1, 2, 3\}$

$2 \times 2 = 4 \equiv 0$ dans $\mathbb{Z}/4\mathbb{Z}$

donc : 2 n'est pas inversible

Il existe des corps finis à

$\{2, 3, 4, 5, 7, 8, 9\}$

Dans $\mathbb{F}_4 = \{0, 1, a, b\}$

$0+0 = 0$
$1+1 = 0$ dans $\mathbb{F}_4$
$a+a = 0$
$b+b = 0$

Dans les corps $\mathbb{F}_{p^k}$: si $a \in \mathbb{F}_{p^k}$

alors $\overbrace{a + a + \dots + a}^{p \text{ fois}} = 0$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

x	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

Section 12-1 du livre

14.3 ⇒ exemple du corps F_{256}

F_4

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Exercice 1 :

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$

$\mathbb{Z}/8\mathbb{Z} = \{[0]_8, [1]_8, [2]_8 \dots, [7]_8\}$

exemple : $[2]_8 \times [4]_8 = [8]_8 = [0]_8$

$[3]_8 \times [5]_8 = [15]_8 = [7]_8$

(1) a) Un élément de $\mathbb{Z}/8\mathbb{Z}$ est inversible si il existe $y \in \mathbb{Z}/8\mathbb{Z}$ tel que $x\,y = [1]_8$

$0 \times x = 0 \Rightarrow 0$ n'est pas inversible

$[x]_8$ est inversible ssi x est premier avec 8.

ssi x n'est pas pair.

Autrement dit : $\{1, 3, 5, 7\}$ sont inversibles dans $(\mathbb{Z}/8\mathbb{Z})$.

$3 \times 3 = 9 = 1 \bmod 8$

$5 \times 5 = 25 = 1 \bmod 8$

$7 \times 7 = 49 = 1 \bmod 8$

$[3]_8^{-1} = [3]_8^{-1}$

$[1]_8^{-1} = [1]_8^{-1}$

b) * $\mathbb{Z}/8\mathbb{Z}$ n'est pas un corps car $[2]_8$ n'est pas inversible.

* $\mathbb{Z}/8\mathbb{Z}$ n'est pas un corps car 8 n'est pas premier.

(2) 97 est un nombre premier donc tout nombre $x \in \{1, 2, \dots, 96\}$ est premier avec 97 donc $\mathbb{Z}/97\mathbb{Z}$ est un corps et tous les éléments non nuls de $\mathbb{Z}/97\mathbb{Z}$ sont inversible.

a) $97 = 8 \times \underset{\text{quotient}}{\uparrow 12} + \underset{\text{reste}}{\uparrow 1}$

$= 8 \times 12 + 1$

$8 \times 12 + 1 = 0$ modulo 97

$[8]_{97}[12]_{97} = [-1]_{97}$

$[8]_{97}(-[12]_{97}) = [1]_{97}$

donc l'inverse de 8 est $-[12]_{97} = [85]_{97}$

$8 \times 85 = 680 \quad = 1 \bmod 97$

Exercice 2.

1. Est-ce que 10^k est inversible dans $\mathbb{Z}/97\mathbb{Z}$?

car 10^k est premier avec 97

car 10 est premier avec 97

2.

$x = x_{n-1}\, x_{n-2} \dots x_k \dots x_0$ ← mot valide

$x' = x_{n-1}\, x_{n-2} \dots x_k' \dots x_0$ ← mot valide avec 1 chiffre changé

donc : $x - x' = 10^k (x_k - x_k')$

3. x' est un mot de code mod 97-10 valide si $[x']_{97} = [1]_{97}$

or $[x']_{97} = [x]_{97} + [x' - x]_{97}$ (*)

$= 1 + 10^k (x_k - x_k') \bmod 97$

car $\hat{x}$ est un mot de mod 97-10 valide.

$[x']_{97}$ est valide ssi $10^k(x_k - x_k') = 0 \mod 97$

10^k est inversible dans $\mathbb{Z}/97\mathbb{Z}$.

soit y son inverse.

si (*) est vraie, alors

$y\,10^k(x_k - x_k') = y \cdot 0 = 0$

donc : $x_k - x_k' = 0 \mod 97$

donc : $x_k = x_k'$

Exercice 3

③. $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps car 2 n'est pas inversible

$2 \times 2 = 0 \mod 4$

② $x = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ $\quad x \times x = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

donc x n'est pas inversible

si x était inversible, alors $\exists y \in M_2$ tel que $xy = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

or $xx = 0$

$x = xxy = 0 \cdot y = 0$

---

3 vecteurs $(1,0,0) = w_1$

$(1,1,1) = w_2$

$(0,1,1) = w_3$

W = espace engendré par w_1, w_2 et w_3

$= \{ a w_1 + b w_2 + c w_3 \ / \ a, b, c \in \mathbb{Z}/2\mathbb{Z} \}$

$= \{ 0, w_1, w_2, w_3, w_1+w_2, w_1+w_3, w_2+w_3, w_1+w_2+w_3 \}$

$= \{ (0,0,0), (100), (111), (011), (0,11), (111), (100), (0,0,0) \}$

$= \{ (000), (100), (111), (011) \}$

$(0,11) = w_3$

Dans $\mathbb{Z}/2\mathbb{Z}$: $1 = -1$

$$w_2 - w_1 = w_2 + w_1 = w_3$$

W est engendré par (w_1, w_2)

car $w_3 = w_1 + w_2$

les vecteurs de w_1 et w_2 sont linéairement indépendants c'est à dire

$$a w_1 + b w_2 = 0 \Rightarrow a = b = 0$$

$$a w_1 + b w_2 = (a+b, b, b) = 0$$

Donc W est de dimension 2.

V est engendré par (v_1, v_2, v_3, v_4)

donc : V est de dimension 1, 2, 3 ou 4.

La dimension de V est ≥ 3 car v_1, v_2, v_3 sont linéairement indépendants.

$$a\begin{pmatrix}0\\0\\1\\\vdots\end{pmatrix} + b\begin{pmatrix}0\\1\\1\\\vdots\end{pmatrix} + c\begin{pmatrix}1\\1\\1\\\vdots\end{pmatrix}$$

$$\begin{pmatrix} c \\ \uparrow \\ =0 \end{pmatrix}, \begin{pmatrix} b+c \\ \uparrow \\ =0 \end{pmatrix}, \begin{pmatrix} a+b+c \\ \uparrow \\ =0 \end{pmatrix}, \dots$$

si $a v_1 + b v_2 + c v_3 = 0$

alors : $c = 0$
$b = 0$
$a = 0$

$v_4 = v_2 + v_3$

donc : V est engendré par v_1, v_2, v_3
et est donc de dimension 3.

(2) Quels sont les éléments de V ?

Les éléments de V sont tous les vecteurs de la forme $a v_1 + b v_2 + c v_3$ avec $a, b, c \in \mathbb{Z}/2\mathbb{Z}$.

$2 \times 2 \times 2 = 8$

$\vec{0}$
v_1
v_2
v_3
$v_1 + v_2 = (0,1,0,0,1,1,1)$
$v_1 + v_3 = (1,1,0,1,0,0,0)$
$v_2 + v_3$:
$v_1 + v_2 + v_3$

(3) Une base de V est $\{v_1, v_2, v_3\}$

Code de parité $(n, n-1)$

$\vec{x}$ = mot du code si $\vec{x}$ est une suite de n "0" ou "1" qui a un nombre pair de "1".

(1). Un code C est linéaire si C est un espace vectoriel.

c'est à dire que :

* si $x, y \in C$ sont deux mots de code et $a \in \mathbb{Z}/2\mathbb{Z}$

alors : $x + y \in C$

$a x \in C$ ←

un vecteur x a un nombre pair de "1"

ssi $\underbrace{x_1 + x_2 + \cdots + x_n = 0 \mod 2}$.

équation linéaire (**)

C est l'ensemble des vecteurs de longueur n qui vérifient l'équation linéaire (**)

donc C est un espace vectoriel,
donc C est un code linéaire.

si x et y sont deux mots de code
$x+y$ est aussi un mot de code.

exemple : $x = (1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1) \to 6$

$y = (0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0) \to 2$

$x+y = (1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1) \to 6$

Exemples de base de C : (avec $n = 6$)

Base 1 :
(110000)
(011000)
(001100)
(000110)
(000011)

Base 2
(100001)
(010001)
(001001)
(000101)
(000011)

Q3 La distance minimale d'un code C est

$$\min_{\substack{x,y \in C \\ x \neq y}} d(x,y).$$

- La distance minimale est au plus 2 car
$$d((110000),(011000)) = 2$$

- Comme C est linéaire la distance minimale de C est le poids minimal d'un mot de code.

= nombre de bits non nuls.

→ est-ce qu'il existe un mot de code de

poids 1 ? → non

2 ? → oui → la distance minimale est 2.

(4) • Une matrice génératrice d'un code linéaire C de dimension k et de longueur n est une matrice G de taille $n \times k$ telle que

$$C = \left\{ \vec{u} \cdot G \text{ où } \vec{u} \in \{0;1\}^k \right\}$$

• Une matrice de contrôle pour ce même code est une matrice H de taille $n \times (n-k)$ telle que $x \in C$ ssi $x \cdot H^T = 0$

exemple : $G = \begin{bmatrix} 1&1&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&1&1&0 \\ 0&0&0&0&1&1 \end{bmatrix}$ est une matrice génératrice

Base : $\begin{pmatrix} 1&1&0&0&0&0 \\ 0&1&1&1&0&\cdots \end{pmatrix}$

$G' = \begin{bmatrix} 1&0&\cdots&0&1 \\ 0&1&0&0&0&1 \\ 0&0&1&0&0&1 \\ 0&0&0&1&0&1 \\ 0&0&0&0&1&1 \end{bmatrix}$ est aussi une matrice génératrice.

$H = \begin{bmatrix} 1 & \cdots & 1 \end{bmatrix}$ est une matrice de contrôle.

Exercice 7

(1) Une matrice génératrice est par exemple $\begin{bmatrix} v_1 \\ v_2 \\ v_4 \end{bmatrix}$

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} \leftarrow v_1 \\ \leftarrow v_2 \\ \leftarrow v_4 \end{matrix}$$

une autre matrice est :

$$G' = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} \in v_1 \\ \in v_1 + v_2 \\ \in v_4 \end{matrix}$$

(2) La matrice G' étant sous forme systématique, une matrice de contrôle H est

$$H = \begin{bmatrix} -P^T & I_4 \end{bmatrix} \quad \text{où} \quad P = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

(note : dans $\mathbb{F}_2$, $-P^T = P^T$)

On peut vérifier en calculant

$$G' H = O_{3\times 4}$$

où $O_{3\times 4}$ est une matrice de taille 3×4 remplie de 0.

3. On calcule $\sim$. $H^T = (a, b, c, d)$ où

$a = (1011000)(1010101) = 0$
$b = (1110100)(1010101) = 1$
$c = (1100010)(1010101) = 1$
$d = (1100010)(1010101) = 1$

le syndrome est donc $(0,1,1,1) \neq \vec{0}$

le mot (1010101) n'est donc pas valide.