Cours maths l2

Mehdi Ben Ahmed

October 5, 2025

Chapter 1

groupes et anneau $\mathbb{Z}/[\mathbb{Z}$ n]

Definition 1 (groupe) *Un groupe G est un ensemble muni d'une loi de composition si et seulement si:*

- *La loi admet un element neutre e tel que*

$$\forall a, \exists e \in G^2, a \circ e = e \circ a = a \tag{1.1}$$

- *Tout élement possède un symmetrique (noté $sym_\circ(a)$) tel que*

$$\forall a \in G \exists sym_\circ(a), a \circ sym_\circ(a) = e \tag{1.2}$$

- *la loi est associative, càd*

$$\forall a, b, c \in G^3, (a \circ b) \circ c \equiv a \circ (b \circ c) \tag{1.3}$$

si de plus, la loi est commutative, càd $a \circ b \equiv b \circ a$ alors le group est dit commutatif

Definition 2 (L'anneau $\mathbb{Z}/[\mathbb{Z}$ n) *] l'anneau $\mathbb{Z}/[\mathbb{Z}$ n] est un ensemble contenant tout les entiers de 0 à i.*

1.1 Generateurs

Definition 3 (Generateur) *un generateur est un nombre faisant partie de l'anneau $\mathbb{Z}/_n\mathbb{Z}$*

Chapter 2

Corps finis

Definition 4 (polynôme irreductible) *un polynôme est dit irréductible si il est impossible de le "réduire" en un produit de polynômes (de degré inférieur). il en découle la propriété qu'un polynôme irréductible ne possède pas de racines. on peut prouver qu'un polynome est irréductible par l'absurde. En effet, si le polynome est bel et bien irréductible, il serait impossible de décomposer le produit de polynômes en polynôme original*

(2.1)

Definition 5 (corps fini) *un corps fini est un ensemble construit a partir d'un polynôme irreductible.*

2.0.1 Polynomes

Theorème 1 *$P(x^2) = P(x)^2$ soit un polynome $P(X)$ dans le corps fini $\mathbb{F}_{2^3}$ el que:*

$$P(x) = x^3 + x^2 + x + 1 P(x)^2 = (x^3 + x^2 + x + 1)^2 \tag{2.2}$$