

Cours maths l2

Mehdi Ben Ahmed

January 1, 1980

Chapter 1

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

- La loi admet un élément neutre e tel que

$$\forall a \in G^2, a \circ e = e \circ a = a \quad (1.1)$$

- Tout élément possède un symétrique (noté $sym_o(a)$) tel que

$$\forall a \in G \exists sym_o(a), a \circ sym_o(a) = e \quad (1.2)$$

- la loi est associative, càd

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

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 $\mathbb{Z}/[n\mathbb{Z}]$).] l'anneau $\mathbb{Z}/[n\mathbb{Z}]$ 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 $\mathbb{Z}/n\mathbb{Z}$

Definition 4 (Trouver le symétrique). il est assez facile de trouver le symétrique additive d'un élément de $\mathbb{Z}/n\mathbb{Z}$.

En effet, $sym_+(a) = n - a$, dans $\mathbb{Z}/10\mathbb{Z}$ par exemple, $sym_+(5) = 10 - 5 = 5, 5 + 5 = 0$. il est plus compliqué de trouver un symétrique multiplicative.

Chapter 2

Definition 5 (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 polynôme est irréductible par l'absurde. En effet, si le polynôme est bel et bien irréductible, il serait impossible de décomposer le produit de polynômes en polynôme original

(2.1)

Definition 6 (corps fini). un corps fini est un ensemble construit à partir d'un polynôme irréductible.

2.0.1 Polynomes

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

$$P(x) = x^3 + x^2 + x + 1 \quad P(x)^2 = (x^3 + x^2 + x + 1)^2 \quad (2.2)$$

Chapter 3

Definition 7 (\mathbb{K} -espace vectoriel). \mathbb{K} -espace vectoriel designe un espace vectoriel contenant des valeurs venant de \mathbb{K}

Un espace vectoriel consiste en un ensemble E , avec ces deux opérations $+$ et \cdot , suivant ces règles pour tout $\vec{v}, \vec{W} \in E$:

- la loi $+$ est interne, commutative et associative
 - $\vec{v} + \vec{w} \in E$
 - $\vec{v} + \vec{w} = \vec{w} + \vec{v}$
 - $\vec{a} + (\vec{b} + \vec{c}) = (\vec{a} + \vec{b}) + \vec{c}$
- il existe un vecteur nul tel que $\vec{a} + \vec{0} = \vec{0} + \vec{a} = \vec{a}$
- pour un vecteur \vec{a} quelconque dans E , il existe un symétrique tel noté $sym_e(\vec{a})$

un élément appartenant à \mathbb{K} est appelé un scalaire. il est en relation avec un vecteur grâce à l'opérateur \cdot . la loi \cdot suit ces règles pour tout $\vec{v}, \vec{w} \in E, \lambda, \delta \in \mathbb{K}$

- \cdot est dite "fermée", càd que $\lambda \cdot \vec{v} \in E$
- il existe un scalaire neutre, e tel que, $e \cdot \vec{v} = \vec{v}$
- $(\lambda + \delta) \cdot \vec{v} = \lambda \cdot \vec{v} + \delta \cdot \vec{v}$
- $\lambda \cdot (\vec{v} + \vec{w}) = \lambda \cdot \vec{v} + \lambda \cdot \vec{w}$
- $(\lambda \times \delta) \cdot \vec{v} = \lambda \cdot (\delta \cdot \vec{v})$

pour prouver qu'un ensemble est un \mathbb{K} espace vectoriel, il suffit donc juste de tester ces opérations et voir si ils correspondent à cette définition on appelle le produit d'un vecteur par un scalaire une combinaison linéaire

\mathbb{K} peut être n'importe quel ensemble, mais dans ce chapitre nous ne considérons que \mathbb{R} , $R[X]$, ou $\{f(x) = ax + b \text{ tq } \forall a, b \in \mathbb{R}\}$

testons ce qu'on a vu avec cet exercice simple. Si non, préciser quel règle cet ensemble enfreint

Exercice 1. On considère $(\mathbb{R}^2, +, \cdot)$ où \cdot est défini par $\forall \lambda \in \mathbb{R}, \forall (x, y) \in \mathbb{R}^2, \lambda \cdot (x, y) = (\lambda x, y)$. Ce magma est-il un ensemble vectoriel?

Definition 8 (famille de vecteurs). une famille de vecteurs est un tuple composé de vecteurs; on dit qu'une famille est libre si aucun des vecteurs peuvent être une combinaison linéaire d'un autre. exemple: $((1, 1, 1), (2, 2, 2))$ est une famille liée car \vec{v}_1 est le double de \vec{v}_0

formellement, une famille est dite libre si pour $\forall \lambda_1 \dots \lambda_n, \forall \vec{v}_1 \dots \vec{v}_n, \lambda_1 \cdot \vec{v}_1 + \dots + \lambda_n \cdot \vec{v}_n = 0$ il existe une unique solution où les scalaires sont tous nul et respectivement, une famille est dite liée s'il existe au moins une solution avec les scalaires non nuls.

Definition 9 (famille génératrice). soit E un \mathbb{K} -espace vectoriel et $s = (\vec{v}_1, \dots, \vec{v}_n)$ une famille de vecteur s est dite génératrice si il est possible d'obtenir n'importe quel vecteur de E grâce à une combinaison linéaire de s . autrement dit, $\forall t \in E, \forall \lambda_1, \dots, \lambda_n \in \mathbb{K}, t = \lambda_1 \cdot \vec{v}_1 + \dots + \lambda_n \cdot \vec{v}_n$

Definition 10 (Vect() ou Span()). la fonction $span()$ prend une famille de vecteurs, et renvoie l'ensemble de toutes les combinaisons linéaires possibles produites avec la famille de vecteur. $span$ d'une famille génératrice donnerait l'ensemble de vecteur. 9

Remarque 1. il est donc possible de générer des ensembles vectoriels grâce à cette fonction, et il en découle de cette propriété qu'il est donc possible de prouver qu'un ensemble est un \mathbb{K} -espace vectoriel si il est possible de trouver une famille de vecteurs $(\vec{v}_0, \dots, \vec{v}_n)$ avec $span((\vec{v}_0, \dots, \vec{v}_n))$ produisant l'ensemble.

Definition 11 (base). une famille de vecteur est dite une base si elle est liée et génératrice. (base car elle est capable de générer tout un ensemble).

Exercice 2. Dans \mathbb{R}^3 , donnez:

1. un exemple de famille génératrice qui n'est pas libre
2. un exemple de famille libre non génératrice
3. une famille ni libre ni génératrice
4. donnez un exemple de base autre que la famille $((1, 0, 0), (0, 1, 0), (0, 0, 1))$

pour numéro 1, il suffit d'ajouter un vecteur qui est une combinaison linéaire d'un autre. soit la base $((1, 0, 0), (0, 1, 0), (0, 0, 1))$, il suffit qu'elle devienne $((1, 0, 0), (0, 1, 0), (0, 0, 1), (2, 0, 0))$ pour qu'elle reste génératrice mais non linéaire $((1, 0, 0), (0, 1, 0), (0, 0, 1))$,

pour numéro 2, il suffit d'en enlever un. $((1, 0, 0), (0, 1, 0))$ est linéaire mais non génératrice dans \mathbb{R}^3

numéro 3, $((0, 3, 0), (0, 1, 0))$. cette famille est ni libre, car un vecteur est le triple d'un autre, ni génératrice, car il est impossible d'obtenir les autres composantes à partir de cette famille.

numéro 4, j'ai choisi de remplacer une des composantes par -1, $((-1, 0, 0), (0, 1, 0), (0, 0, 1))$. elle reste génératrice car on est dans \mathbb{R} , et $-1 \cdot (-1, 0, 0) \equiv 1 \cdot (1, 0, 0)$

Definition 12 (Sous Espace Vectoriel).

Chapter 4

4.1 regles de notation

Definition 13 (Matrice).

Definition 14 (matrice identite). la matrice identite est une matrice carre contenant seulement des 1 dans sa diagonale, et des 0 dans tout les autres cases.

4.2 definitions

Definition 15 (transpose). la transposition est une operation qui change les lignes en colonnes, et les colonnes en ligne. elle est obtenue en faisant "pivoter" les elements de la matrice autour de la diagonale.

Definition 16 (matrice inverse). comme dans les autres espaces, "inverse" signifie que c'est la matrice symmetrique a une autre matrice par rapport a une operation, ici la multiplication. formellement, pour une matrice $M, \exists M^{-1} t.q M \cdot M^{-1} \equiv M_{Id}$. remarquez le $\exists M$. En effet, pas toute les matrices possedent un inverse, et ceux qui en possedent un sont appelees **matrices inversibles**.

Definition 17. determinant le determinant d'une matrice A est donne par la formule

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det(A_{ij})$$

ou A_{ij} est la matrice obtenue en enlevant la ligne i et la colonne j de A. Cette formule est valable quelle que soit la ligne i choisie. Elle fait intervenir tous les coefficients a_{ij} de cette ligne. Chacun de ces coefficients étant multiplié par le déterminant d'une matrice $(n1) \times (n1)$, il s'agit donc d'une définition récursive. Etant donné que cette formule donne le même résultat quelle que soit la ligne i choisie, on a intérêt à chercher dans A

la ligne possédant le plus de coefficients nuls pour réduire le nombre de calculs. Si la matrice ne contient que des coefficients non nuls, il n'y a pas à priori de stratégie particulière à adopter.

Une formule équivalente existe en choisissant cette fois-ci une colonne j quelconque dans la matrice A :

$$\det(A) = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det(A_{ij})$$

Definition 18 (calcul inverse de matrice). Afin de calculer efficacement l'inverse d'une matrice A , on peut appliquer l'algorithme de Gauss de la façon suivante :

- Appliquer l'algorithme de Gauss à la matrice A afin d'obtenir une matrice triangulaire supérieure T_A . Pour chaque transformation effectuée au cours de l'algorithme, effectuer exactement la même transformation sur la matrice identité. A la fin de ce procédé vous avez obtenu 2 matrices :
 - T_A qui est la matrice A modifiée par l'algorithme de Gauss
 - I_A qui est la matrice identité sur laquelle on a appliqué l'ensemble des transformations effectuées sur A . En particulier on a $I_A \times A = T_A$.
- En partant de la dernière colonne de T_A et en remontant jusqu'à la deuxième colonne, appliquer le principe de Gauss afin de placer des 0 dans chaque colonne, au-dessus de l'élément diagonal. Remarque : tous les éléments diagonaux de T_A étant non nuls, il n'y aura dans ce cas, aucune permutation de lignes à effectuer. Pour chaque transformation effectuée au cours de ce deuxième passage, effectuer exactement la même transformation sur la matrice I_A .
- A l'issu de ce procédé on obtient donc 2 matrices :
 - D_A qui est la matrice T_A modifiée par l'algorithme de Gauss et qui est donc à présent une matrice diagonale.
 - S_A qui est la matrice I_A sur laquelle on a appliqué l'ensemble des transformations effectuées sur T_A . En particulier on a $S_A \times A = D_A$

L'inverse de A est obtenu en divisant pour chaque ligne i de S_A les coefficients de la ligne par l'élément diagonal situé sur la ligne i de la matrice D_A .