1 Ensemble

(F, +, *) est un ensemble si il respecte ces 6 axiomes:

- F est fermé sur + et *.
- Association de + et *
- + et * sont inversables
- Il existe des elements neutres pour + et * **uniques et non égaux**.
- * se distribue sur +
- $\forall x \neq 0$ il existe x^{-1}

1.1 Z_n

L'ensemble Z_n est un ensemble qui contient tous les elements de Z de 0 a n.

1. $a +_F b = a + b \mod n$
2. $a *_F b = a * b \mod n$

1.2 Comment trouver rapidement le résultat

Faire le calcul normal, puis ajouter/enlever n jusqu'a tomber sur un chiffre dans l'ensemble $\{0, \ldots, n\}$.

1.3 Propriétés des scalaires

Tous les nombres d'un champs sont nommés scalaires.

- 0 et 1 sont uniques
- Pour chaque nombre il existe un seul nombre inverse et contraire
- $a * b = 0 \implies a = 0 \lor b = 0$

1.4 Demonstrations

Prouvons que $a * b = 0 \implies a = 0 \vee b = 0$: Si $a \neq 0 \wedge b \neq 0$ alors $a * b = 0 \equiv a^{-1} * a * b = a^{-1} * 0 \equiv b = 0 \equiv F$, donc a ou b doit etre égal a 0.

1.5 Chemins de solutions

Comment trouver le 0 et le 1: On a juste a resoudre b dans les equations $a + b = a$ et $a * b = a$, il doit n'y avoir qu'une seule solution de b pour tous les a.

Comment trouver l'inverse et le contraire: Il faut d'abord connaitre le 0 et le 1, puis resoudre b dans les equations $a + b = 0$ et $a * b = 1$, il ne doit ici aussi n'y avoir qu'une seule solution, (attention, b sera egal a $-a$, pas a, et les symboles +, *, 0 et 1 sont dependants du champs duquel on parle).

2 Equations linéaires

Une équation Linéaire est une équation polynomiale qui ne contient pas de multiplications d'éléments (xy) ou d'éléments seuls avec une puissance (z^3). Ainsi, elle est de ce format:

$$a_1 * x_1 + a_2 * x_2 + \ldots + a_n * x_n = b.$$

2.1 Appellations

- x - variables
- a Mekadmim
- Mekadmim hofshiim$b$
- Equation zero - Equation ou tous les mekadmim sont 0_F
- Solution privee - solutions sous forme de nombres
- Solution generale - solutions pour chaque variable sous forme de fonction avec des parametres, par exemple $(\frac{7}{2} + \frac{3}{2}t, t)$, on peut egalement la factoriser pour obtenir $(\frac{7}{2}, 0) + t(\frac{3}{2}, 1)$

2.2 Propriétés

1. Si une fonction linéaire a des paramètres provenant d'un ensemble A et une solution sur un autre ensemble B, alors elle a aussi une solution sur A.

3 Systeme d'equations lineaires

3.1 Appellations

- $(v_1, \ldots, v_n)\epsilon F^n$ est la solution de l'equation si $(x_1, \ldots, x_n) = (v_1, \ldots, v_n)$ resoud toutes les equations.
- Ordre du systeme (m, n) - m est le nombre d'equations, et n est le nombre de variables.
- Forme standard: Comme une matrice
- **עקבית**: Systeme solvable.
- Equation zero: $0 * x_1 + 0 * x_2 + 0 * x_3 = 0$, n'importe quel groupe la resoud.
- Systeme homogene: tous les mitkadmim hofshiim sont 0_F (il est forcement solvable).

3.2 Propriétés

1. Si une equation lineaire ressemble a $0 * x_1 + 0 * x_2 + 0 * x_3 = b(\neq_0)$ alors elle n'a pas de solution.
2. Un systeme homogene est forcement solvable par la solution triviale $(0, 0, \ldots, 0)$.
3. Dans un systeme homogene, si c est une solution, alors sc (s scalaire) l'est aussi, et si d est une solution, alors $c + d$ aussi

3.3 Systemes equivalents

On peut appliquer les operations suivantes sur un systeme sans le modifier:

1. Changer les equations de place
2. Additioner une equation avec une autre (ou avec une multiplication d'une autre par un scalaire)
3. Multiplier une equation entiere par un scalaire qui n'est pas 0_F

Attention: Ne pas faire d'opération R_A - R_B si R_A a des 0 sur lesquels R_B a des chiffres !

4 Matrices de coefficients

Avec cette matrice, on peut resoudre l'equation, en essayant d'avoir des parametres que sur une sur ligne.

4.1 Exemple

$$\begin{aligned}
a_{1_1}x_1 + a_{1_2}x_2 + \ldots + a_{1_n}x_n &= b_1 \\
a_{2_1}x_1 + a_{2_2}x_2 + \ldots + a_{2_n}x_n &= b_2 \\
&\dots \\
a_{3_n}x_1 + a_{3_n}x_2 + \ldots + a_{n_n}x_n &= b_n
\end{aligned}$$

Donne:

$$\left[\begin{array}{cccc|c}
a_{1_1} & a_{1_2} & \ldots & a_{1_n} & b_1 \\
a_{n_1} & a_{2_2} & \ldots & a_{2_n} & b_2 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
a_{m_1} & a_{m_2} & \ldots & a_{m_n} & b_m
\end{array}\right]$$

4.2 Appellations

- Element ouvreur (איבר הפתוח): Premier element de chaque ligne.
- Variables liées et variables libres: une variable liée est une variable qui est attachée a un element ouvreur au moins une fois dans la matrice (on parle ici du x). Une fois que la matrice est en escalier, on peut exprimer chaque variable liée a l'aide des variables libres.
- Matrice escalier (מטריצה מדרגות): Toutes les lignes zero sont en bas, et chaque element ouvreur et a droite de celui de la ligne d'au dessus. Le systeme est donc appelé système escalier (מערכת מדורג).
- Matrice canonique: Tous les elements ouvreurs sont des 1 et ils sont seuls dans leur colonne. Il n'y a qu'une et unique matrice canonique pour un système linéaire. On peut donc s'en servir pour regarder si deux matrices sont équivalentes.
- Matrice identité (יחידה) d'ordre n: Matrice de forme $n * n$ avec que des 0 sauf des 1 dans la diagonale principale (אלכסון הראשי).
- Système homogène: Tous les mekadmim hofshiim (b) sont 0, ces systèmes ont au moins une solution (la solution **triviale** $(0, \ldots, 0)$), si le nombre de variables est plus grand que le nombre d'équations alors le systeme a aussi une solution non triviale. Un système homogène peut être représenté par une matrice réduite (une matrice qui ne contient pas les mekadmim hofshiim (b)).

4.3 Mettre une matrice en escalier

1. Mettre tout en haut la ligne avec l'ouvreur le plus a gauche
2. Utiliser cette ligne du haut pour tondre cette colonne, de sorte a ce que la ligne du haut soit la seule a avoir un ouvreur sur cette colonne
3. Recommencer en ignorant la premiere ligne

4.4 Mettre une matrice en canonique

1. La mettre en escalier

2. Transformer l'ouvreur de la dernière ligne en 1 en multipliant la ligne par son inverse

3. Tondre toute la colonne grace a lui

4.5 Chemins de solution

- Regarder si deux matrices sont équivalentes: les réduire a leur forme canonique et regarder si elles sont pareilles.

5 Nombre de solutions d'un système linéaire

Un système linéaire peut soit ne pas avoir de solutions, soit n'en avoir qu'une seule et unique, soit en avoir une infinité (si l'ensemble de definition est fini).

1. Pas de solution: On peut le determiner si une matrice a une ligne de contradiction, si une matrice escalier n'a pas de ligne contradictoire, normalement elle a au moins une solution (**עקבית**)

2. Une solution: Toutes les variables sont des variables liées donc la matrice canonique reduite (**מצומצמת**) est une matrice identité. D'ailleurs, **si une matrice canonique réduite est une matrice identité, alors tous les systèmes dont elle peut être la matrice (peu importe les b) ont une solution unique.** On en déduit que pour un système homogène la matrice réduite a soit des lignes de 0 (une solution ou plus) ou alors est une matrice identité (donc solution unique triviale[1.14.4]).

3. Si elle a des variables libres, alors elle a un nombre infini de solutions sur un ensemble infini, et $|F|^{libres}$ solutions sur un ensemble F fini.