N° d'ordre :
N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Superieur et de la Recherche Scientifique

---

UNIVERSITÉ ECHAHID HAMMA LAKHDAR EL OUED

FACULTÉ DES SCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Thème

Matrices et Groupes de Frobenius

Présenté par: **Belarouci Maroua**
Rezzoug Hania
Zobiri Halima

Sous la supervision de :
Ameur Meziane Saide MA(A)

Année universitaire 2014 – 2015

Remerciements

Nous remercions dieu le tout puissant qui nous a guidé dans l'accomplissement de ce travail.

Ce dernier à été réalisé sous l'encadrement du professeur "SAID-AMEUR Meziane" à l'université l' EL-OUED, a qui nous reoudrons exprimer nos profondes gatitudes pour leurs disponibilités, leurs aides et leurs conseils pour réaliser ce travail.

Nous tenons également à remercier monsieurs les membres de jury pour l'honneur qu'ils nous on fait en acceptant de siéger à notre soutenance.

Ainsi qu'à tous les professeurs de l'université d'EL-OUED et surtout les professeurs "BELOUL Said, MEDEKEL Hamza, FAREH Abedlfeteh ".

Nous remercions virement nos familles surtouts mes parent pour l'aide et le soutient moral.

Nous tenons a remercié la promotion 2014/2015 de Math de l'université d'EL-OUED.

Notations générales

$\varnothing$	Ensemble vide.
$\Bbbk$	Le corps $\mathbb{R}$ ou $\mathbb{C}$.
$Z(G)$	Centre d'un groupe G.
$Hom(G,H)$	Homomorphisme de Gver H.
$M_{n,p}(\Bbbk)$	Ensemble des matrices d'ordre n × p a coefficients dans $\Bbbk$.
$\bar{A}$	Matrice hermitienne.
A^T	Transpose d'un matrice.
$tr(A)$	Trace de la matrice.
$rang(A)$	La rang d'un matrice A.
A_{ij}	Cofacteur d'un matrice.
M_{ij}	Mineur d'un matrice.
$adj(A)$	Matrice adjacente.
A^{-1}	L'inverse de la matrice A.
$Mat(f,e_i,w_j)$	Est un matrice de f relativement aux bases e_i et w_j .
$GL_n(\Bbbk)$	Groupe géneral linéaire.
$SL(n,\Bbbk)$	Le groupe dérivé de $GL(n,\Bbbk)$.
$B(n,\Bbbk)$	Le groupes des matrices trinangulaires.
$N(n,\Bbbk)$	Le groupes des matrices superieures.
$GL(n)$	Constitué des matrices de déterminants non nul.
$PGL(E)$	Le groupe projectif linéaire d'un espace vectoriel E.
$PSL(E)$	Le groupe projectif spécial linéaire.
$SL(n,\mathbb{R})$	Constitué des matrices de déterminant 1.
$\|.\|_F$	Le norme du matrice de Frobenius.
■	Fin d'une demonstration.

Table des matières

Introduction générale

Le mathematique est un science, non limite, qui a plusiers branches d'entre elle l'algébre abstract. La section des groupes (groupes générale linéaire, groupes spécial) qui a un grand interét dans l'algébre et dans l'informatique.

Note travail est précisé sur les groupes spécial(Frobenius, groupe linéaire des déterminant ± 1).

Pour ce la on a rappellé dans le prémier chapitre les principaux définitions des groupes, sous groupes, homorphismes des groupes, on plus pris les théorémes et propriétés fondamentales pour les espaces vectoriel, espaces euclidiens et algébre de lie.

Dans le deuxiéme chapitre, on a présenté les matrices, les determinants et les matrices des application linéaire avec quel que théorémes et proprietés liés aux des structures matricielles.

Dans le troixiéme chapitre, traité les structures matricials on y introduit la notation de resultant de groupe Frobenius aprés l'étude des propriéties de goupe matriciel, nous fournissons des exemples et classifier les groupes et sous groupe de Frobenius .

Chapitre 1

Les groupes

1.1 Généalites

Définition 1.1.1 *Soit G un ensemble non vide on definie l'application :*

$G \times G \longrightarrow G$

$(x, y) \longrightarrow x * y.$

$(*)$*comme loi interne satisfie :*

1. $*$ *est associative :*

   $\forall x, y, z \in G;\ x * (y * z) = (x * y) * z.$

2. *G posséde un élément neutre e pour $*$ c-à-d :*

   $\exists\ e \in G, \forall x \in G;\ x * e = e * x\ = x.$

3. *Tout $x \in G$ admet un symetrique y :*

   $\forall x \in G, \exists\ y \in G;\ x * y = y * x\ = e.$

Exemple 1.1.1

1. $(\mathbb{Z}, +)$ est un groupe.
2. $(\mathbb{R}^*, \times)$ est un groupe.
3. $(\mathbb{Z}, \times)$ n'est pas un groupe.
4. $(\mathbb{N}, +)$ n'est pas un groupe.

Définition 1.1.2 *On appelle groupe commutatif, ou groupe abélien, tout groupe G, dont la loi $*$ vérifie : $x * y = y * x$ pour tous $x, y \in G$.*

Exemple 1.1.2 *L'ensemble $\mathbb{C}$ des nombres complexes muni de l'addition est un groupe abélien.*

Notation 1.1.1 *Dans le cas génerral, on note $x * y = xy$ et ainsi aussi, on pose $e = 1$ et $(x)^{'} = x^{-1}$ (on l'appelle l'inverse de x) si $n \in \mathbb{N}^*$, on définit par récurrence $x^n = x\,(x^{n-1})$ avec $x^0 = 1$.*

Proposition 1.1.1 *Dans un groupe*

1. *L'élément neutre est unique.*

   Preuve. *Soit $e, e^{'} \in G$ deux élément neutre.*

   Puisque e est un élément neutre, on a $e = e^{'} * e = e * e^{'} = e^{'}$. ■

2. *Dans un groupe l'inverse x' d'un élément x est unique.*

   Preuve. *Soit $x^{''} \in G$ tel que $x^{'} * x = e$.*

   On a alors $x^{''} = x^{''} * e = x^{''} * \left(x * x^{'}\right) = \left(x^{''} * x\right) * x^{'} = e * x^{'} = x^{'}$.

   Dans $x^{''} = x^{'}$. ■

3. *L'inverse de l'inverse de x est x, i-e $\left(x^{'}\right)^{'} = x$.*

   Preuve. *On a $x * x^{'} = x^{'} * x = e$ donc x est l'inverse de $x^{'}$ d'aprés 2.*

   On a $x = (x')'$. ■

4. *$(x * y)^{'} = y^{'} * x^{'}$.*

   Preuve. *On a $(x * y) * (y' * x') = x * y * y' * x^{'} = x * e * x' = e$.*

   Donc $(x * y)' = y' * x'$. ■

1.2 Order d'un groupe

Un groupe est dit fini si le nombre de ses éléments est fini.

Dans ce cas, son cardinal est appele l'order du groupe G, on le note $|G| = card\ G$.

Si le groupe n'est pas fini, il est dit infini.

1.3 Sous-groupes

Définition 1.3.1 *Soient $(G,*)$ un groupe $H \in \mathcal{P}(G)$.*

On dit que H est un sous-groupe de G si et seulement si :

1. $\forall (x,y) \in H\ ^2 x * y \in H$.
2. $e \in H$.
3. $\forall x \in H, x^{-1} \in H$.

Exemple 1.3.1 $\left(\mathbb{R}_+^*, \times\right)$ *est un sous-groupe de* $(\mathbb{R}^*, \times)$ *en effet :*

1. $1 \in \mathbb{R}_+^*$.
2. *Si* $x, y \in \mathbb{R}_+^*$ *alors* $x \times y \in \mathbb{R}_+^*$.
3. *Si* $x \in \mathbb{R}_+^*$ *alors* $x^{-1} = 1/x \in \mathbb{R}_+^*$.

Remarque 1.3.1 *Un critére et plus rapide pour prouver pue H est un sous-group $H \neq \varnothing$ de G est :*

1. *H contient au moins l'élément neutre.*
2. *pour tout $x, y \in H, x * y^{-1} \in H$.*

Proposition 1.3.1 *Soit G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G; alors $\cap_{i\in I} H_i$ est un sous-groupe de G.*

Preuve. Soitent $x, y \in \cap_{i\in I} H_i$, pour tout i $\in I$ on a $x, y \in H_i$ comme H_i est un sous-groupe alors $xy^{-1} \in H_i$ pour tout i. Donc $xy^{-1} \in \cap_{i\in I} H_i$. ■

Remarque 1.3.2 *En général $\cup_{i\in I} H_i$ n'est pas un sous-group de G.*

Proposition 1.3.2 *Soitient les sous-groupes de $G = (\mathbb{Z}, +)$: $H_1 = 3\mathbb{Z}$ et $H_2 = 8\mathbb{Z}$, si ou prend $3 \in H_1$, $5 \in H_2$ on à $3 + 8 = 11 \notin H_1 \cup H_2$ alors $H_1 \cup H_2$ n' est pas un sous-groupe de $\mathbb{Z}$.*

Proposition 1.3.3 *Soient G un groupe et $\mathcal{F} = \{H_i\}_{i\in I}$ une famille de sous-groupe de G ordonnée par inchusion alors $\cup_{i\in I} H_i$ est un sous-groupe de G.*

Preuve. Soint $x, y \in \cup_{i\in I} H_i$ il existe $j, k \in I$ tels que $x \in H_j$ et $y \in H_k$ et supposons que $H_k \subset H_j$ alors $xy^{-1} \in H_j$ donc $xy^{-1} \in \cup_{i\in I} H_I$. ■

1.3.1 Centere d'un groupe

Pour tout groupe $(G,\cdot)$, on note $Z(G)$ le centre de G, ensemble des éléments de G qui commutent avec tout les éléments de G :

Centere d'un élément :

$Z(x) = \{y \in G \ / xy = yx\}$.

Centere de G :

$Z(G) = \{x \in G \ \ / xy = yx, \forall y \in G\}$.

1.3.2 Les sous-groupes distingués

Définition 1.3.2 *Soit Gun groupe et H est un sous-groupe de Gest distingué si et seulement si :* $(\forall x \in G,\ xHx^{-1} = H) \Leftrightarrow (x \in G \ / \ xH = Hx)$.

Exemple 1.3.2 *Soit* $(\mathbb{R}^*,+)$ *un groupe et* $(\mathbb{Z},+)$ *les sous-groupe distingués de groupe* $(\mathbb{R}^*,+)$

$x\mathbb{Z}\ x^{-1} = \mathbb{Z}$

$\forall x \in \mathbb{R}, x^{-1} = -x$

i-e $(x = 2\ , x^{-1} = -2)$

on a : $x\,\mathbb{Z}\ x^{-1} = x + \mathbb{Z} + (-x) = x - x + \mathbb{Z} = \mathbb{Z}$

donc $(\mathbb{Z},+)$ *les sous-groupe distingués .* ■

1.4 Morphismes de groupes

Définition 1.4.1 *Soit G et H des groupes.*

On appelle morphisme de G dans H une application $\varphi : G \to H$ telle que :

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ *pour tout* $a, b \in G$.

Définition 1.4.2 *On note $Hom(G,H)$ l'ensemble des morphismes de G dans H.*

1. *Un morphisme bijectif est applé isomorphisme.*
2. *S'il existe un isomorphisme $\varphi : G \to H$ on dit que les groupes G et H sont isomprphis et on écrit $G \cong H$.*
3. *Un isomorphisme $\varphi : G \to G$ est applé automorphisme.*

Exemple 1.4.1 $x \to 2^x$ *réalise un isomorphisme de* $(\mathbb{R},+)$ *sur* $\left(\mathbb{R}_+^*\right)$.

1.5 Type des groupes

1.5.1 Groupe des permutations

Proposition 1.5.1 *L'ensemble des bijection de* {1,2, ...,n} *dans lui-même, mumi de la loi de compositions est un groupe note* $(S_n,0)$.

Une bijection *de* {1,2,.....,n} (dans lui-même) s'appelle une permutation.

Les groupes $(S_n,0)$ s'appelle le groupe des permutation (ou le groupe symétrique) .

Les cardinal de S_n est n !, i-e : $(|S_n| = n!)$.

1.5.2 p-groupes

Définition 1.5.1 *Soit p un nombre premier.On appelle p-groupe, tout groupe d'order d'une puissance non nulle de p,* $(|G| = p^\alpha : \alpha \in \mathbb{N}^*)$.

Exemple 1.5.1 $\mathbb{Z}/8\mathbb{Z}$ *est un* $2-$*groupe* $(|\mathbb{Z}/8\mathbb{Z} = 2^3,\ p = 2|)$.

Proposition 1.5.2 *Le centre d'un p-groupe n'est pas réduit à l'élément neutre ; i-e*$(|Z(G)| > 1)$.

Corollaire 1.5.1 *Tout groupe d'ordre* p^2, (*p est un nombre prémier) est abélien.*

1.5.3 Théorèmes de sylow

Définition 1.5.2 *Un sous-groupe H d'un p-groupe fini G est un p-sous-groupe de sylow (on dira plus briévement un "p-sylow") si H est un sous-groupe d'ordre* p^n *où* p^n *est le plus grande puissance de p qui divise* $|G|$.

Théorème 1.5.1 [1] *Soit G un groupe fini et p un nombre prémier divisant* $|G|$.

Alors il existe un p-sous-groupe de sylow de G.

Théorème 1.5.2 [1] *Soit G un groupe fini d'ordre* $p^n q$ *où p et q sont de nombres entier avec* $(p, q) = 1$ *alors :*

1. *Si H est un p-sous-groupe de G, alors il existe un p-sylow K tel que* $H < K$.
2. *Tout les p-sylow sont conjugués.*
3. *Si* n_p *le nombre de p-sylow sous-groupe de G on à :* $n_p \mid |G|$ *et* $n_p \equiv 1 \,[\mathrm{mod}\, p]$.

1.5.4 groupe dérivé

Définition 1.5.3 [1] *Soit G un groupe, pour tous $x, y \in G$,on appelle commutateur de x et y élément :* $[x, y] := x^{-1}y^{-1}xy$.

Définition 1.5.4 *Le groupe dérivé et definis comme sont est groupe engendré par les mutateur.*

$G^{(\prime)} = [G : G] = \langle xyx^{-1}y^{-1} \ / x, y \in G \rangle$.

$G^{(\prime\prime)} = \left[G' : G'\right] = \left\langle aba^{-1}b^{-1} \ / a, b \ \in G' \right\rangle$.

.

.

$G^{(n)} = \left[G^{(n-1)} \ : \ G^{(n-1)}\right] = \left\langle \alpha\beta\alpha^{-1}\beta^{-1} / \alpha, \beta \in G^{(n-1)} \right\rangle$.

1.6 Structure d'espace vectoriel

Définition 1.6.1 [2] *On appelle* $\mathbb{k}-$***espace vectoriel*** *tout ensemble E mini d'une loi terne notée $+$, $\forall\,(x, y) \in E^2 / x + y \in E$ et d'une loi externe :*

$\mathbb{k} \times E \ \rightarrow E$

$(\lambda,x) \rightarrow \lambda x$ *telles que*

1. $(E,+)$ *est un groupe abélien.*
   - *a.* $\forall\,(\lambda,\, \mu) \in \mathbb{k}^2,\, \forall x \in E,\, (\lambda + \mu)\, x = \lambda x + \mu x.$
   - *b.* $\forall \lambda \in \mathbb{k},\, \forall\,(x,\, y) \in \ E^2,\, \lambda\,(x + y) = \lambda x + \lambda y.$
   - *c.* $\forall\,(\lambda,\, \mu) \in \mathbb{k}^2,\, \forall x \in E,\, \lambda\,(\mu x) = (\lambda\mu)\, x.$
   - *d.* $\forall x \in E,\, 1x = x.$

Notation 1.6.1 *Nous abrégerons* $\mathbf{E-espace\ vectoriel}$ *en* $\mathbf{E-e.v}$.

Les éléments d'un $\mathbf{E-e.v}$. Sont appelés vecteurs : les éléments de K sont appelés scalaires.

Remarque 1.6.1

1. *Les corp* $\mathbb{k}$ *est* $\mathbb{k}-$**e.v**.
2. *Soient* X *un ensemble non vide,* E *un* $\mathbb{k}-$**e.v**.

   L'ensemble E^X *des application de* X *dans* E *est un* $\mathbb{k}-$**e.v**. *Pour les lois interne et externe définies par :*

   · $\forall (f,\, g) \in \left(E^X\right)^2, \forall x \in X,\, (f+g)(x) = f(x) + g(x)$.

   · $\forall \lambda \in \mathbb{k}, \forall f \in E^X, \forall x \in X,\, (\lambda f)(x) = \lambda f(x)$.

   Par exemple, l'ensemble $\mathbb{R}^{\mathbb{N}}$ *des suites réelles est un* $\mathbb{R} - e.v.$ *pour les lois usuelles.*

Proposition 1.6.1 [2] *Soit* E *un* $\mathbf{K} - \mathbf{e.v}$. *On a, pour tous* λ, μ *de* $\mathbb{k}$ *et tous* x, y *de* E :

1. $\lambda x = 0 \Leftrightarrow (\lambda = 0 \text{ ou } x = 0)$.
2. $(\lambda - \mu)\, x = \lambda x - \mu x$.
3. $\lambda (x - y) = \lambda x$ - λy.

1.7 Sous-espace vectoriel

Définition 1.7.1 *Soient* E *un* $\mathbb{k}-$**e.v**.$\mathbf{F}$ $\in \mathcal{P}(E)$.*On dit que* F *est un Sous-espace vectoriel de* E *si et seulenent si :*

1. $F \neq \varnothing$.
2. $\forall (x,\, y) \in F^2 : x + y^{'} \in F; i - e : (x - y \in F)$.
3. $\forall \lambda \in \mathbb{k}, \forall x \in F : \lambda x \in F$.

Remarque 1.7.1 *Nous abrégerons* ***sous-espace vectoriel*** *en* $\mathbf{S} - \mathbf{e.v}$.

Pour rappeler le corps $\mathbb{k}$ *utilisé, on dit quelque fois* ***sous*** $\mathbb{k}-$**e.v**. *Au lieu de* $\mathbf{S} - \mathbf{e.v}$.

Exemple 1.7.1 $\mathbb{R}^2-$*espace vactoriel sur* $\mathbb{R}$.*Sous-ensemble* $\mathbb{R} \times \{0\}$ *est un sous-espace vectoriel de* $\mathbb{R}^2$ *sur* $\mathbb{R}$.

1.8 Les applications linéaires

Définition 1.8.1 [5] *Soient E et E' deux $\mathbb{k}$-espaces vectoriels.*

Une application $U : E \to E'$ est dite linéaire si, pour tous vecteurs $x, y \in E$ et scalaires $\lambda, \mu \in \mathbb{k}, U(\lambda x + \mu y) = \lambda U(x) + \mu U(y)$. Il découle de cette définition que $U(0) = 0$.

1.8.1 Espace vectoriel des applications linéaires

Soient U et V sont deux applications linéaires de E dans E' et $\lambda \in \mathbb{k}$ un scalaire, alors les applications $U + V$ et λU définies, pour tout $x \in E$, par :

$$\begin{aligned} (U+V)(x) &= U(x) + V(x). \\ (\lambda U)(x) &= \lambda U(x). \end{aligned}$$

Sont des applications linéaires.

1.9 Formes bilinéaires

Soient E, F deux $\mathbb{k}-$espaces vectoriels. On dit qu'une application $B : E \times F \to \mathbb{k}$ est une forme bilinéaire si :

$$\forall x, x' \in E, \forall t, t' \in \mathbb{k}, B(tx + t'x', y) = tB(x, y) + t'Bx', y).$$

$$B(x, ty + t'y') = tB(x, y) + t'B(x, y').$$

1.10 Espaces Euclidiens

1.10.1 Produit Scalaire

Définition 1.10.1 [2] *Soit X un espace linéaire sur le corps $\mathbb{k}$.*

Un produit scalaire sur X est une application $\Phi : X \times X \to \mathbb{k}$ telle que

pour tout $x, x_1, x_2, y \in X$ et $\lambda \in \mathbb{k}$, on a :

1. *$\Phi(x,x)$ est un réel non négatif $(\Phi(x,x) \geq 0)$ et $\Phi(x,x) = 0$ si et seulement si $x = 0$.*
2. *$\Phi(x,y) = \Phi(y,x)$.*
3. *$\Phi(x_1 + x_2, y) = \Phi(x_1, y) + \Phi(x_2, y)$.*
4. *$\Phi(\lambda x, y) = \lambda\Phi(x,y)$.*

Pour désigner un produit scalaire on emploie d'habitude les notations $(x \mid y)$ où (x,y) où $\langle x, y\rangle$.

On utilisera la notation $(x \mid y)$.

Définition 1.10.2 *Un espace linéaire X sur le croups $\mathbb{k}$ muni d'un produit scalaire est appelé un espace euclidien.*

On rencontre aussi le nom d'espace unitaire, quand $\mathbb{k} = \mathbb{C}$.

On notera les espaces euclidiens par $E, E_1, \cdots\cdots, E_n$.

1.11 Forme quadratique

Définition 1.11.1 [2] $\mathbb{k}$ *corps car*$(\mathbb{k}) \neq 2$ $(\mathbb{k} = \mathbb{R}, \mathbb{Q}, \mathbb{C})$ *.Soit b une forme bilinéaire symétrique sur E.*

L'application $Q : E \to \mathbb{k}$

$$X \to b(x,x)$$

et appelée forme quadratique associée.

Remarque 1.11.1 .

1. *$Q(\lambda x) = \lambda^2 Q(x)\,; \forall \lambda \in \mathbb{k}$.*
2. *$Q(x)$ l'ensemble des formes quadratiques sur E est un espace vectoriel sur $\mathbb{k}$.*

1.12 Algèbre de Lie

Définition 1.12.1 *Une algébre de lie est une couple (G, μ) où G est un espace vectoriel complexe et μ une application bilinéaire $\mu : G \times G \to G$ satisfaisant :*

$$\mu(X, Y) = -\mu(Y, X) \,; \forall X, Y \in G.$$

$$\mu(X, \mu(Y, Z)) + \mu(Y, \mu(Z, X)) + \mu(Z, \mu(X, Y)) = 0 \ ; \ \forall X, Y, Z \in G.$$

Remarque 1.12.1 *Contrairement aux algèbres tensorielles (et aux algèbres ni Clifford, dont les algèbres extérieures), les algèbres de Lie ne sont pas unitaires, ni associatives.*

Chapitre 2

Matrice

Définition 2.0.2 *Soit un corps commutatif* $\mathbb{k}$ *et deux entiers* n, $p \geq 1$ *appelle matrice* $n \times p$ *à cofficients dans* $\mathbb{k}$, *une application*

$$A : [1, n] \times [1, p] \to \mathbb{k}$$
$$(i, j) \to a_{ij}$$

que l'on note : $A = \left(a_{i_j}\right) = \begin{bmatrix} a_{11} & a_{12} & \cdot & \cdot & \cdot & \cdot & a_{1p} \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & \cdot & a_{2p} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdot & \cdot & \cdot & \cdot & \cdot & a_{np} \end{bmatrix}$; *ou* $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$.

Le cofficient a_{ij} *se trouve à l'intersection de la* i*-éme ligne et de la* j*-éme colonne.*

On note $M_{n,p}(\mathbb{k})$*l'ensemble des matrice* $n \times p$ *à coefficients dans la corps* $\mathbb{k}$.

Si $n = p$ *on utilisera les natations* M_n *ou* $M_n(\mathbb{k})$. *Si* $n = p = 1$*une dermiére remarque : on peut envisager des matrices sans ligne ou colonnes* (*cas* $n = 0$ *ou* $p = 0$) *pour certains cas particuliers.*

Exemple 2.0.1 *Soit* A *matrice* (3×4)*définie par :* $A = \begin{bmatrix} 1 & 2 & 0 & -5 \\ 4 & 3 & -1 & 3 \\ 2 & 5 & -2 & 0 \end{bmatrix}$.

On a par exemple les coefficients $a_{21} = 4$ *et* $a_{13} = 0$.

2.1 Opérations élémentaires sur les matrices

2.1.1 Egalité

Définition 2.1.1 [5] *Les matrice A et B sont égales si et seulement si elles ont les méme dimensions et si $a_{ij} = b_{ij}, \forall i, j$ (tous les éléments sont égaux un à un).*

Les deux matrices suivantes sont égales :

$$A = \begin{bmatrix} 2 & 4 & 8 \\ 4 & 5 & 10 \\ 6 & 6 & 12 \end{bmatrix}, B = \begin{bmatrix} 2 & 4 & 8 \\ 4 & 5 & 10 \\ 6 & 6 & 12 \end{bmatrix}.$$

2.1.2 Somme des matrices

Définition 2.1.2 [6] *Pour $A, B \in M_{n,p}(\mathbb{k})$ (deux matrice ayant le méme nombre de lignes et colonnes), notées $A = (a_{ij})$ et $B = (b_{ij})$ .On définit la matrice somme $A + B$ commé étant la matrice à n lignes et p colonnes de terme général $a_{ij} + b_{ij}$.*

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdot & \cdot & a_{1p} + b_{1p} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdot & \cdot & a_{2p} + b_{2p} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdot & \cdot & a_{np} + b_{np} \end{bmatrix}.$$

Exemple 2.1.1 $$\begin{bmatrix} 1 & 2 & 0 \\ 4 & 3 & -1 \end{bmatrix} + \begin{bmatrix} 5 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 1+5 & 2+2 & 0+3 \\ 4+1 & 3+3 & -1+4 \end{bmatrix} = \begin{bmatrix} 6 & 4 & 3 \\ 5 & 6 & 3 \end{bmatrix}.$$

Proposition 2.1.1 *L'addition des matrice satisfait les propriétés suivantes, pour A, B et C des matrices de type (n, p) on a :*

1. $A + B = B + A$.
2. $(A + B) + C = A + (B + C)$.
3. $A + 0 = 0 + A = A$ ou 0 est matrice nulle.
4. $A + (-A) = 0$ ou $-A = (-a_{ij})$.

   On déduite que $(M_{n,p}(\mathbb{k}), +)$ un groupe abelien.

2.1.3 Produit des matrices

Soit $A \in M_{n,p}(\mathbb{k})$ et $B \in M_{r,q}(\mathbb{k}), A = (a_{ij}), B = (b_{ij})$.

On définit une matrice notée AB si $p = r$ à n lignes et q colonnes comme la matrice de terme général c_{ij} telle que $AB = C, C = (c_{ij})_{\substack{1\leq i \leq n \\ 1\leq j \leq p}}$

$$c_{ij} = \sum_{k=1}^{p} a_{ik}b_{kj}, \forall i \in \{1, \cdots\cdots, n\}, \forall j = \{1, \cdots\cdots, p\}.$$

Exemple 2.1.2 $A = \begin{bmatrix} 1 & 2 & 0 \\ 4 & 3 & -1 \end{bmatrix}, B = \begin{bmatrix} 5 & 1 \\ 2 & 3 \\ 3 & 5 \end{bmatrix}$

$$A \times B = \begin{bmatrix} 1 & 2 & 0 \\ 4 & 3 & -1 \end{bmatrix} \times \begin{bmatrix} 5 & 1 \\ 2 & 3 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 1\times 5 + 2\times 2 + 0\times 3 & 1\times 1 + 2\times 3 + 0\times 5 \\ 4\times 5 + 3\times 2 - 1\times 3 & 4\times 1 + 3\times 3 - 1\times 5 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 7 \\ 23 & 8 \end{bmatrix}.$$

Proposition 2.1.2

1. Soient $A = (a_{ij})$ une matrice de $M_{n,p}(\mathbb{k})$ et λ un scalire on défini la matrice λA par $\lambda A = (\lambda a_{ij})$, c'est la matrice A dont tout les coefficients on élé multiplies par λ.
2. Produit des matrice est associatuve : $A(BC) = A(CB)$.
3. L'élément neutre de multiplication est la matrice unite I_n.
4. Produit des matrice non abélien : $AB \neq BA$.

2.2 Matrices particuliées

2.2.1 Matrice nulle

Définition 2.2.1 *Une matrice nulle est une matrice dont tous les éléments sant nulle.*

Exemple 2.2.1 $A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$, *A matrice nulle.*

2.2.2 Matrice ligne

Définition 2.2.2 *Une matrice ligne est une matrice ayant un seule ligne :*

$[a_{11} \quad a_{12} \quad a_{13} \cdot \cdot \cdot \cdot \cdot \cdot a_{1p}]$.

Exemple 2.2.2 $A = [1 \quad 0 \quad 3 \quad 4 \quad 10]$, *est une matrice ligne d'ordre* (1×5).

2.2.3 Matrice colonne

Définition 2.2.3 *Une matrice colonne est matrice ayant une seule colomme* $\begin{bmatrix} a_{11} \\ a_{12} \\ . \\ . \\ a_{n1} \end{bmatrix}$.

Exemple 2.2.3 $A = \begin{bmatrix} 0 \\ 2 \\ 3 \\ 7 \end{bmatrix}$, *est une matrice colonne d'order* (4×1).

2.2.4 Matrice carrée

Définition 2.2.4 *Si* $n = p$ *(méme nombre de lignes que colonnes); la matrice est dite matrice carrée.*

On note $M_n(\mathbb{k})$*ou lieu de* $M_{n,n}(\mathbb{k}) = \begin{bmatrix} a_{11} & a_{12} & . & . & . & . & a_{1n} \\ a_{12} & a_{22} & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ a_{n1} & . & . & . & . & . & a_{nn} \end{bmatrix}$.

Exemple 2.2.4 $A = \begin{bmatrix} 2 & -1 & 6 & 5 \\ 4 & 5 & -2 & 3 \\ 3 & 7 & 4 & 9 \\ 1 & 2 & 1 & 8 \end{bmatrix}$.

1. **Matrice symétrique :**

   Une matrice carré est symétrique si et seulement si $a_{ij} = a_{ji}, \forall i \neq j$.

   Exemple 2.2.5 $A = \begin{bmatrix} 2 & -1 & 2 \\ -1 & 0 & 3 \\ 2 & 3 & 4 \end{bmatrix}$.

2. **Matrice unité :** On définit la matrice unité I_n d'ordre n que posséde que des "1" sur sa digonale est des "0" ailleurs.

   Pour tous $i, j \leq n, \delta_{ij} = \begin{cases} 1 & si \quad i = j \\ 0 & si \quad i \neq j \end{cases}$ ou $I_n = \begin{bmatrix} 1 & 0 & \cdot & \cdot & 0 \\ 0 & 1 & \cdot & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & 0 & 1 \end{bmatrix}$.

   Exemple 2.2.6 $I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, *matrice unité d'ordre* 4.

3. **Matrice diagonale :**

   Une matrice diagonale est une matrice d'ordre n telle que $a_{ij} = 0$, pour $i \neq j$ et $a_{ij} \neq 0$ pour $i = j$

   $\begin{bmatrix} a_{11} & 0 & \cdot & \cdot & 0 \\ 0 & a_{22} & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & 0 & a_{nn} \end{bmatrix}$.

Exemple 2.2.7 $A = \begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$, *est une matrice diagonale d'ordre* 4.

4. **Matrice triangulaires :**

   (a) **Matrice triangulaire supérieure :**

   On déffinit une matrice triangulaire supérieure d'ordre n que posséde un triangle composé uniquement de "0"; $\begin{cases} a_{ij} \neq 0 & si \quad i \leq j \\ a_{ij} = 0 & si \quad i > j \end{cases}$

$$A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} = \begin{bmatrix} a_{11} & a_{12} & \cdot & \cdot & a_{1n} \\ 0 & a_{22} & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & a_{nn} \end{bmatrix}.$$

Exemple 2.2.8 $A = \begin{bmatrix} 1 & 4 & -1 & 3 \\ 0 & 2 & 5 & -2 \\ 0 & 0 & 6 & 4 \\ 0 & 0 & 0 & 7 \end{bmatrix}$.

Si la digonale est composée de "0", on dit alors que la matrice est strictement triangulaire supérieure. $\begin{bmatrix} 0 & a_{12} & \cdot & \cdot & a_{1n} \\ 0 & 0 & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 \end{bmatrix}$.

Exemple 2.2.9 $A = \begin{bmatrix} 0 & 4 & 5 & 1 \\ 0 & 0 & 7 & 3 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(b) **Matrice triangulaire inférieure :**

Une matrice triangulaire inférieure si : $\begin{cases} a_{ij} \neq 0 & si \quad i \geq j \\ a_{ij} = 0 & si \quad i < j \end{cases}$

$$A = (a_{ij})_{\substack{1\leq i \leq n \\ 1\leq j \leq n}} = \begin{bmatrix} a_{11} & 0 & \cdot & \cdot & 0 \\ a_{21} & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \\ a_{n1} & a_{n2} & \cdot & \cdot & a_{nn} \end{bmatrix}.$$

Exemple 2.2.10 $A = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 \\ 1 & 4 & 5 & 0 \\ 5 & 2 & 7 & 1 \end{bmatrix}$.

2.2.5 Matrice Réguliére

On appelle A est une matrice réguliére si : $\det(A) \neq 0$.

2.2.6 Matrice Inverse

Une matrice carrée A est dites inversible (ou réguliére) si et seulement si, il existe une matrice carrée, appelée matrice inverse et notée A^{-1} telle que : $A \times A^{-1} = A^{-1} \times A = I_n$.

Si A^{-1} n'existe pas, on dit que la matrice A est simguliére, $(\det A = 0)$.

2.2.7 Matrice Hermitienne

C'est une matrice A de $\mathrm{M}_n(\mathbb{C})$ telle que : $a_{ij} = \bar{a}_{ji}, (\forall i, j)$.

Exemple 2.2.11 $A = \begin{bmatrix} 5 & -1+i & \sqrt{2}-i \\ -1-i & 6 & 1+3i \\ \sqrt{2}-i & 1-3i & 7i \end{bmatrix}$.

2.3 Transposition d'une matrice

Pour $A = \begin{bmatrix} a_{11} & a_{12} & \cdot & \cdot & a_{1p} \\ a_{21} & \cdot & \cdot & \cdot & a_{2p} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdot & \cdot & \cdot & a_{np} \end{bmatrix}$ $deM_{n,p}(\mathbb{k})$.

On appelle matrice transposée de A la matrice A^T de taille $p \times n$ définie par :

$A^T = \begin{bmatrix} a_{11} & a_{21} & \cdot & \cdot & a_{n1} \\ a_{12} & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{1p} & \cdot & \cdot & \cdot & a_{np} \end{bmatrix}$ de $M_{n,p}(\mathbb{k})$.

En particulier, la transposée d'une matrice-ligne est une matrice-colonne

et réciproquement :

$$\begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix}^T = \begin{bmatrix} x_1 & \cdot & \cdot & \cdot & x_n \end{bmatrix}.$$

$$\begin{bmatrix} x_1 & \cdot & \cdot & \cdot & x_n \end{bmatrix}^T = \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix}.$$

On peut aussi écrire transposition de A : $A^t = A^T$.

Exemple 2.3.1 $A_{4,3} = \begin{bmatrix} 0 & 3 & -1 \\ 2 & 1 & 4 \\ 3 & 7 & 6 \\ 1 & 2 & 8 \end{bmatrix}$ *alors* $A^T_{3,4} = \begin{bmatrix} 0 & 2 & 3 & 0 \\ 3 & 1 & 7 & 2 \\ -1 & 4 & 6 & 8 \end{bmatrix}$.

$A_{1,3} = \begin{bmatrix} 1 & -2 & 5 \end{bmatrix}$ *alors* $A_{3,1}^T = \begin{bmatrix} 1 \\ -2 \\ 5 \end{bmatrix}$.

Proposition 2.3.1 .

1. *Si A est une matrice carrée symetrique, alors :* $A^T = A$.
2. *Si A est une matrice antisymetique, alors :* $A^T = -A$.
3. *Si A est inversible alors A^T l'est aussi et on a* $\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$.
4. $\left(A^T\right)^T = A$.
5. $T : A \to A^T$ *est un isomorphisme de* $M_{n,p}(\mathbb{k})$ *sur* $M_{p,n}(\mathbb{k})$ *lorsque* $n = p, T$ *est un automorphisme involutif de* $M_n(\mathbb{k})$.

2.4 Matrice orthogonale

Une matrice carrée A (n lignes, n colonnes) orthogonale est une matrice diagonale (unité)à coefficients réels.

Elle vérifie donc $A^tA = I_n$, où A^t est la matrice transposée de A et I_n est la matrice identité.

Comme la matrice de rotation plane d'angle θ : $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$; ou

Les matrices de permutation, comme : $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$.

2.5 Tarce D'une Matrice

On appelle trace d'une matrice carrée $A \in M_n(\mathbb{k})$ la somme des éléments de la diagonal principale et on la note $tr(A)$, c'est à dire que $tr(A) = \sum_{i=1}^{n} a_{ii}$.

Exemple 2.5.1 *Soit* $A = \begin{bmatrix} 1 & 7 & 3 \\ -3 & 5 & 2 \\ 5 & 3 & -12 \end{bmatrix}$ *alors* $tr(A) = 1 + 5 + (-12) = -6$.

Proposition 2.5.1 *Si* $A, B \in M_n(\Bbbk)$ *alors* :

1. $tr(A+B) = tr(A) + tr(B)$.
2. $tr(\alpha A) = \alpha tr(A)$, *pour tout* $\alpha \in \Bbbk$.
3. $tr\left(A^T\right) = tr(A)$.
4. $tr(AB) = tr(BA)$.

2.6 Le rang d'une matrice

Le rang d'une matrice correspond au nombre maximum de colonnes ou de lignes linéairement indépendantes.

C'est aussi l'ordre du plus grand déterminant non nul.

Si r est cet ordre, on dit que la matrice $A, A \in M_{n,p}(\Bbbk)$ est dite de $rang(A) = \min(n,p)$.

Proposition 2.6.1 *Quelle que soit une matrice* $A, A \in M_{n,p}(\Bbbk)$

$rang(A) = rang\left(A^T\right) = rang\left(AA^T\right) = rang\left(A^TA\right)$.

2.7 Les Déterminants

2.7.1 Déterminant des matrices carrées

Définition 2.7.1 [8] *On défnit tout d'abord le déterminant d'une matrice d'ordre deux*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\Bbbk) \text{ par : } \det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ab - bc.$$

Une matrice d'ordre 1 étant tout simplement un scalaire, son déterminant est lui même.

Le déterminant d'une matrice $A = (a_{ij})_{1 \le i\,,\, j \le n} \in M_n(\Bbbk)$ d'ordre $n \geq 3$ peut se défnir par récurrence comme suit : $\det(A) = \sum_{i=1}^{n} (-1)\, a_{i,1} \det(A_{i,1})$.

Où $A_{i,n}$ est, pour i compris entre 1 et n, la matrice d'ordre $n-1$ déduite de A en supprimant, la première colonne et la ligne numéro i.

Dans cette expression,on dit qu'on développe le déterminant suivant la première colonne.

$$\text{On note : } \det(A) = \begin{vmatrix} a_{11} & \cdot & \cdot & \cdot & a_{1n} \\ a_{21} & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdot & \cdot & \cdot & a_{nn} \end{vmatrix}.$$

2.7.2 Le mineur et cofacteur

Les déterminant est égal à la somme des produits obtenus en multipliant les éléments d'une ligne quelconque (ou d'une colonne) par leur cofacteurs respectifs cofacteur :

$A_{ij} = (-1)^{i+j} M_{ij}$ ou M_{ij} (mineur) est la sous-matrice carrée $(n-1) \times (n-1)$ obtenue en supprimant la $i^{émé}$(ligne la $j^{éme}$) colonne de n ainsi $|A| = \sum_{i=1}^{n} a_{ii} |A_{ij}|$.

2.7.3 Calcul d'un déterminant

Le déterminant peut s'obtenir par l'intermédiaire des cofacteurs :
$\det(A) = \sum_{j=1}^{n} a_{ij} |A_{ij}|$ (Suivante la ligne) ou : $\det(A) = \sum_{i=1}^{n} a_{ij} |A_{ij}|$
(suivante la colonne j) A_{ij} étant le cofacteur de l'élément a_{ij}.

Exemple 2.7.1 $A = \begin{bmatrix} 1 & 4 & -1 \\ 2 & 0 & 2 \\ 3 & 1 & 3 \end{bmatrix}$, $\begin{vmatrix} 1 & 4 & -1 \\ 2 & 0 & 2 \\ 3 & 1 & 3 \end{vmatrix} = (1)\begin{vmatrix} 0 & 2 \\ 1 & 3 \end{vmatrix} - (4)\begin{vmatrix} 2 & 2 \\ 3 & 3 \end{vmatrix} + (-1)\begin{vmatrix} 2 & 0 \\ 3 & 1 \end{vmatrix} = -4.$

2.7.4 Properties des déterminants

Soit $A \in M_n(\mathbb{k})$ une matrice carrée d'ordre n.

1. On ne modifie pas déterminant de A si en ajoutant à une colonne de A une combinaison linéaire des autres colonnes.
2. Si on multiple l'une des colonnés de A par un scalaire λ, alors le déterminant de A est multiplie par λ :

   $\det(c_1, \cdots, c_{i-1}, \lambda c_i, c_{i+1}, \cdots \cdot c_n) = \lambda \det(c_1, \cdots \cdot \cdot \cdot \cdot, c_n)$.
3. Si A a deux colonnes identique (ou ligne), alors $\det(A) = 0$.

4. Si on échanage deux colonnes de A, alors son déterminant est changé en son opposé.
5. Si $A \in M_n(\Bbbk)$, alors : $\det(A^t) = \det(A)$ .Il en résult que les régles de calculs concernant les colonnes de A, s'appliquent aussi aux lignes.
6. Déterminant d'une matrice triangulaire :

   soit $M = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$ une matrice triangu-laire par bloce, ou A et C sont des matrice carrées d'ordre respectif p et q.

   On alors $\det(M) = \det(A) \times \det(C)$.

   Il en résulte que le déterminant d'une matrice triangulaire est égale au produit de ses élements diagonaux.

2.8 Matrice Adjacente

Définition 2.8.1 [2] *Soit $A \in M_n(\Bbbk)$ matrice carrée d'ordre n. La matrice adjacente de A (notée $adj(A)$) est définie comme la transposée de la matrice des cofacteurs de A.*

Théorème 2.8.1 *Soit $A \in M_n(\Bbbk)$ alors A est inversible $\Longleftrightarrow \det(A) \neq 0$ et on a* $A^{-1} = \frac{adj(A)^t}{\det(A)}$.

2.9 Matrice d'une application linéaire

Pour étudier les matrices, il est commode de les associer aux application lineaires.

Définition 2.9.1 *Soient E un $\Bbbk$ espace vectoriel de dimension finie p, F un $\Bbbk$ espace vectoriel de dimension finie n et $f : E \to F$ une application lineare.*

On appelle matrice de l'application f par napport bases $\{e_i\}_i$ de E et $\{w_j\}_j$ de F le tableau rectangulaire (ou carré) des coefficients a_{ij} des images

$f(e_i) = a_{1i}w_1 + a_{2i}w_2 + \cdots\cdots + a_{ni}w_n$ *écrits en colonnes :*

$$f(e_1) \cdots f(e_i) \cdots f(e_p).$$

$$M = Mat\,(f, e_i, w_j) = \begin{bmatrix} a_{11} & \cdot & a_{1i} & \cdot & a_{1P} \\ a_{21} & \cdot & a_{2i} & \cdot & a_{2p} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdot & a_{ni} & \cdot & a_{np} \end{bmatrix}.$$

Il en résulte que la matrice de f posséde $\dim(E) = p$ colonnes et $\dim(F) = n$ lignes.

Si on change de bases, les éléments de la matrice changent aussi.

Exemple 2.9.1 *Soient l'espace vectoriel réel : $E = \{p \ \in \mathbb{R}_3[X], degp \leq 2\}$*

et l'endomorphisme f de E de valeurs $f(p) = 3p + (X-3)p' + (2X^2 - X - 4)p''$

la base $\{1, X, X^2\}$.

$f(1) = 3.$

$f(X) = 4X - 3.$

$f(X^2) = 9X^2 - 8X - 8.$

On en déduit la matrice de f : $Mat\,(f, e_i) = \begin{bmatrix} 3 & -3 & -8 \\ 0 & 4 & -8 \\ 0 & 0 & 9 \end{bmatrix}$.

2.10 Matrice bassage

Soit $B = (e_{1,\cdots,}e_n)$ un base de E. Considérons p vecteurs $x_1, \cdots, x_p \in E$, la matrice représentant la famille $x_1, \cdots, x_p$ dans B est la matrice (n, p) dont la K-éme colonne est la matrice coordonnée de x_K dans B. Elle est notée $Mat\,(x_1, \cdots, x_p)$.

Soit $B' = (e'_1, \cdots\cdots, e'_n)$ une autre base de E. La matrice de passage entre B et B' est la matrice représentant $(e'_1, \cdots, e'_n)$ dans B. Elle est notée $p = M_{n,p}(B, B')$.

$$M_{n,p}(B, B') = Mat\,(e'_1, \cdots, e'_n) = \begin{bmatrix} p_{11} & \cdot & \cdot & \cdot & p_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{n1} & \cdot & \cdot & \cdot & p_{nn} \end{bmatrix}.$$

Exemple 2.10.1 $B = \{e_1 = (0,0,1), e_2 = (0,-1,0), e_3 = (1,-1,0)\}$.

$C = \{e'_1 = (2,0,1), e'_2 = (0,1,1), e'_3 = (1,1,-1)\}$.

$$p = \begin{bmatrix} 1 & 1 & -1 \\ -2 & -1 & -2 \\ 2 & 0 & 1 \end{bmatrix}.$$

2.11 Matrice Semblable

Définition 2.11.1 [6] *Deux matrice A et B de $M_n(\mathbb{k})$ sont dites semblable s'il existe*

$P \in M_n(\mathbb{k})$ tell que : $B = P^{-1}AP$.

Exemple 2.11.1 *La matrice suivintes sont semblables* :

$$A = \begin{bmatrix} 2 & 1 \\ -2 & 0 \end{bmatrix}, B = \begin{bmatrix} -2 & -2 \\ 5 & 4 \end{bmatrix}.$$

En effet en posant :

$$P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, P^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}.$$

On obtient : et on vérifie aisément que : $P^{-1}AP = \begin{bmatrix} -2 & -2 \\ 5 & 4 \end{bmatrix} = B$.

2.12 Matrice équivalentes

Définition 2.12.1 [6] *Des matrices A et B de $M_n(\mathbb{k})$ sont dites équivalentes s'il existe de matrices inversibles P et Q tell que.*

$A = Q^{-1}BP$ où $QAP^{-1} = B$.

Proposition 2.12.1 .

1. *Les matrice A et B de $M_{n,p}(\mathbb{k})$ sont equivalentes si et seulement si, étant donné E et F des $\mathbb{k}-$espaces vectoriels de dimensions p et n.*

   Par rapportés à des base respectives U et V et $f \in L(E,F)$,telle que $A = mat_{u,v}(f)$, il existe U' et V' bases de E et F, telle que : $B = mat_{u'v'}(f)$.

2. *L'équivalences des matrices est une relation d'équivalence dans $M_{n,p}(\mathbb{k})$.*

Chapitre 3

Matrices de Frobenius et les groupes

3.1 Groupe général linéaire

Définition 3.1.1 [3] *En mathématiques, le groupe général linéaire ou groupe linéaire de degré n d'un corps commutatif $\mathbb{k}$ (ou plus généralement : d'un anneau commutatif unitère) est les groupes des matrices $n \times n$ inversibles à coefficients dans $\mathbb{k}$, muni de la multiplication matricielle.On le note $GL_n(\mathbb{k})$, ou $GL_n(ici\ GL(n,\mathbb{k}))$.*

i.e : $GL(n,\mathbb{R}) = \{matrice\ A, n \times n\ inversible \quad (\det(A) \neq 0)\}$.

Ces groupes sont importants dans la théorie des représentations de groupes et apparaissent lors de l'étude des symétries et des polynômes.

$GL(n,\mathbb{k})$ et ses sous-groupes sont souvent appelés « groupes linéaires » ou « groupes matriciels », (muni de loi conposition interne maltplication).

Le groupe spécial linéaire, noté $SL(n,\mathbb{k})$ et constitué des matrices de déterminant 1, est un sous-groupe normal de $GL(n,\mathbb{k})$. Pour tout anneau commutatif unitère $\mathbb{R}, GL(n,\mathbb{R})$ est un groupe pour la multiplication des matrices : c'est le groupe des unités de l'anneau des matrices $n \times n$ à coefficients dans $\mathbb{R}$.

Si $n \geq 2, GL(n,\mathbb{R})$ n'est pas abélien.

Pour tout corps commutatif $\mathbb{k}, GL(n,\mathbb{k})$ est engendré par les matrices élémentaires de transvections et de dilatations (car les transvections engendrent le groupe spécial linéaire).

3.2 Groupes linéaire

Définition 3.2.1 [4] *On appelle groupe linéaire un sous-groupe d'un groupe général linéaire* $GL(n, \mathbb{R})$.

Remarque 3.2.1 *Tout sous-groupe d'un groupe linéaire est linéaire.*

Le groupe $GL(n, \mathbb{C})$ *est linéaire ; puisqu'on peut le plonger naturellement dans* $GL(2n, \mathbb{R})$.

Exemple 3.2.1 *Le groupe* $SL(n, \Bbbk) = \{M : M \lhd GL(n, \Bbbk)\}$.

Le groupe $B(n, \Bbbk)$ $\{B(n, \Bbbk)$ *des matrices triangulaires*$\}$.

Les groupe $N(n, \Bbbk)$*des matrices triangulaires superieures avec*1 *sur la diagonale.*

3.2.1 Groupe général linéaire d'un espace vectoriel

Si E est un espace vectoriel sur le corps $\Bbbk$, on appelle groupe général linéaire de E et on note $GL(E)$ où ($Aut(E)$, le groupe des automorphismes de E) muni de la composition des applications.

Si E est de dimension n, alors $GL(E)$ et $GL(n, \Bbbk)$ sont isomorphes.

Cet isomorphisme n'est pas canonique et dépend du choix d'une base de E.

Une fois cette base choisie, tout automorphisme de E peut être représenté par une matrice $n \times n$ inversible qui détermine l'isomorphisme.

1. Sur les réels et les complexes

Si le corps $\Bbbk$ est $\mathbb{R}$ (les nombres réels) où $\mathbb{C}$ (les nombres complexes), alors $GL(n, \Bbbk)$ est un groupe de Lie réel où complexe de dimension n^2.

En effet, $GL(n)$ est constitué des matrices de déterminant non nul.

Le déterminant étant une application continue (et même polynomiale).

L'algèbre de Lie associée à $GL(n)$ est $M(n)$; son groupe fondamental est monogène infini.

2. les matrices de déterminant positif et celles de déterminant négatif

Les matrices $n \times n$ réelles de déterminant positif forment un sous-groupe de $GL(n, \mathbb{R})$, noté $GL^+(n, \mathbb{R})$.

Ce dernier est également un groupe de Lie de dimension n^2et possède la même algèbre de Lie que $GL(n, \mathbb{R})$.

Son groupe fondamental est monogène :

trivial pour $n = 1$, infini pour $n = 2$ et d'ordre 2 pour $n > 2$.

3. Sur les corps finis

Si $\Bbbk$ est un corps fini à q éléments, alors on écrit parfois $GL(n, q)$ à la place de $GL(n, \Bbbk)$.

C'est un groupe fini d'ordre $(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$, ce qui peut être prouvé, en comptant les bases d'un espace vectoriel fini.

Exemple 3.2.2 *$GL(3, \mathbb{R}^2)$, c'est un groupe fini d'ordre*

$(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 7 \times 6 \times 5 = 210$.

3.2.2 Groupe projectif linéaire

Le groupe projectif linéaire (en) $PGL(E)$ d'un espace vectoriel E sur un corps commutatif $\Bbbk$ est le groupe quotient $GL(E)/Z(E)$, où $Z(E)$ est le centre de $GL(E)$, c'est-à-dire le sous-groupe formé des homothéties non nulles.

Le groupe projectif spécial linéaire $PSL(E)$ d'un espace E de dimension finie est le groupe quotient de $SL(E)$ par son centre $SZ(E)$, c'est-à-dire par le sous-groupe formé des homothéties de déterminant 1^2.

Si $E = K^n$, ils sont notés respectivement $PGL(n, \Bbbk)$ et $PSL(n, \Bbbk)$.

Le groupe projectif spécial linéaire $PSL(n, F_q)$ d'un corps fini F_q est parfois noté $L_n(q)$.

Cette dénomination de « groupe projectif » vient de la géométrie projective, où le groupe projectif agissant sur les coordonnées homogènes $(x_0 : x_1 : \dots : x_n)$ est le groupe sous-jacent de cette géométrie (en conséquence, le groupe $PGL(n + 1, \Bbbk)$ agit sur l'espace projectif de dimension n).

Exemple 3.2.3 .

1. *Le groupe projectif linéaire généralise donc le groupe $PGL(2)$ des transformations de Mobius, parfois appelé le groupe de Mobius.*

$PGL(2) = \{M_f$ transformations de Mobius$\}$, $PGL(2)$ sont appele le groupe de Mobius

($f(z) = \frac{az+b}{cz+d}$ $/ z \in \mathbb{C}, z \neq \frac{-d}{c}$, transformation de Mobius).

2. *Tous les groupes $PSL(n, \Bbbk)$ pour $n \geq 2$ sont simples, sauf $PSL(2, F_2)$ et $PSL(2, F_3)$*[3].

Sur les entiers relatifs

Une matrice carrée à coefficients dans un anneau commutatif $\Bbbk$ est inversible (i.e. possède une matrice inverse également à coefficients dans $\Bbbk$) si et seulement si son déterminant est inversible dans $\Bbbk$ (si $\Bbbk$ n'est pas un corps, il ne suffit donc pas que le déterminant soit non nul).

Les éléments de $GL(n, \Bbbk)$ sont donc les matrices $n \times n$ à coefficients entiers

de déterminant égal à 1 ou -1.

Sous-groupes Diagonaux

L'ensemble des matrices diagonales de déterminant non nul forme un sous-groupe

de $GL(n, \Bbbk)$ isomorphe à $(\Bbbk^\times)^n$.

Il est engendré par les dilatations.

Une matrice scalaire est une matrice d'homothétie, c'est-à-dire une matrice diagonale qui est le produit de la matrice identité par une constante.

Ce groupe est le centre de $GL(n, \Bbbk)$.

Il est donc normal dans $GL(n, \Bbbk)$ et abélien.

Le centre de $SL(n, \Bbbk)$, noté $SZ(n, \Bbbk)$, est simplement l'ensemble des matrices scalaires de

déterminant 1. Il est isomorphe au groupe des racines n-ièmes de 1.

3.2.3 Groupes Classiques

Les groupes classiques sont les sous-groupes de $GL(E)$ qui préservent une partie du produit interne sur E. Par exemple :

- Le groupe orthogonal, $O(E)$.

- Le groupe symplectique, $Sp(E)$.

- Le groupe unitaire, $U(E)$.

3.3 Groupe frobenius

d'apres notre étude des groupes lineaire on générale on selexion les frobenius groupes par : le caracteristique qui est leurs determiant si 1 òu -1; $ie : Fr\,(n,\mathbb{R}) = \{Matrice\ \mathrm{A}\,;\ \det A = \pm 1\}$.

3.4 Divers groupes de forbenius

3.4.1 Groupe spécial linéaire

Le groupe spécial linéaire d'ordre n sur l'anneau commutatif $\mathbb{R}$, noté $SL(n,\mathbb{R})$, est constitué des matrices de déterminant 1.

i.e : $SL\,(n,\mathbb{R}) = \{A \in GL\,(n,\mathbb{R})\,, \det(A) = 1\}$.

C'est un sous-groupe normal de $GL(n,\mathbb{R})$, puisque c'est le noyau du morphisme de groupes « déterminant », de $GL(n,\mathbb{R})$ dans le groupe multiplicatif $R^{\times}$des éléments inversibles de $\mathbb{R}$.

D'après le premier théorème d'isomorphisme, le groupe quotient $GL(n,\mathbb{R})/SL(n,\mathbb{R})$ est isomorphe à $R^{\times}$.

En fait, $GL(n,\mathbb{R})$ est un produit semi-direct de $SL(n,\mathbb{R})$ par $\mathbb{R}^{\times}$:

$GL(n,\mathbb{R}) = SL(n,\mathbb{R}) \times R^{\times}$.

Pour un corps $\Bbbk$, $SL(n,\Bbbk)$ est engendré par les matrices élémentaires de transvections 1.

$SL(n,\Bbbk)$ est le groupe dérivé de $GL(n,\Bbbk)$, sauf si $n = 2$ et $\Bbbk = F_2$.

i.e : $SL\,(n,\Bbbk) = [GL\,(n,\Bbbk) :\ \mathrm{GL}\,(n,\Bbbk)] = (GL\,(n,\Bbbk))'$.

Exemple 3.4.1 $SL\,(2,\mathbb{R}) = (GL\,(2,\mathbb{R}))' = [GL\,(2,\mathbb{R}) : GL\,(2,\mathbb{R})]$.

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \times \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \times \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^{-1} = M \in SL$$

tel que : $a, b, c, d, \alpha, \beta, \gamma, \delta \in \mathbb{R}$

et $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0, \det \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \neq 0.$

Démonstration Lorsque $\mathbb{k}$ est $\mathbb{R}$ ou $\mathbb{C}$.

$SL(n)$ est un sous-groupe de Lie de $GL(n)$ de dimension $n^2 - 1$.

L'algèbre de Lie de $SL(n)$ est formée des matrices $n \times n$ coefficicients réels ou complexes de trace nulle.

Le groupe spécial linéaire $SL(n, \mathbb{R})$ peut être vu comme le groupe des transformations linéaires de $\mathbb{R}_n$ préservant le volume et l'orientation.

3.4.2 Groupe orthogonal

Définition 3.4.1 [8] *L'ensemble des éléments f du groupe linéaire $GL(E)$ tels que $q(f(x)) = q(x)$ pour tout vecteur x de E est un groupe pour la composition des applications.*

On l'appelle groupe orthogonal de q et on le note $O(q)$ ou $O(E, q)$.

Exemple 3.4.2 .

1. *Un cas important est celui de la forme quadratique suivante (en supposant que la caractéristique de $\mathbb{k}$ est différente de 2 (car $\mathbb{k} \neq 2$) : $E = K^n$, et q est la forme quadratique canonique : $q(x_1, ..., x_n) = \sum_{k=1}^{n} x_k^2$.*
2. *Les matrices carrées réelles d'ordre 2 du type :* $\begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix}$ *sont orthogonales.*
3. *Les matrices diagonales avec seulement des 1 ou des -1 sur la diagonale sont orthogonales.*

Définition 3.4.2 *Le groupe orthogonal correspondant est noté $O(n, \mathbb{k})$, ou $O_n(\mathbb{k})$.*

Il est appelé groupe orthogonal standard de degré n sur $\mathbb{k}$.

Il s'identifie canoniquement au groupe des matrices orthogonales.

Une matrice M est donc orthogonale si et seulement si $M^t M = I_n$, où M^t est la matrice transposée de M et I_n est la matrice identité.

Sa multiplication est la multiplication matricielle.

C'est un sous-groupe du groupe général linéaire $GL(n, \mathbb{k})$.

i.e : $O(n, \mathbb{k}) = \{A \in GL(n, \mathbb{k}) \mid A^t A = I\}$.

Le déterminant de tout élément de $O(q)$ est égal à 1 ou à -1.

3.4.3 Groupe Spécial Orthogonal

Définition 3.4.3 *Si la caractéristique de* $\mathbb{k}$ *est différente de* 2, *l'ensemble* $O(q) \cap SL(E)$ *des éléments de* $O(q)$ *dont le déterminant est* 1 *est un sous-groupe de* $O(q)$, *que l'on l'appelle groupe spécial orthogonal de* q *et on le note* $SO(q)$ *ou* $SO(E, q)$.

Dans le cas de l'exemple vu plus haut, on le note aussi $SO(n, \mathbb{k})$ *ou* $SO_n(\mathbb{k})$.

Donc $SO(n, \mathbb{k})$ *est le groupe des matrices orthogonales d'ordre* n *dont le déterminant est* 1.

$SO(q)$ *est un sous-groupe d'indice* 2 *de* $O(q)$, *et donc* $SO(n, \mathbb{k})$ *est un sous-groupe d'indice* 2 *de* $O(n, \mathbb{k})$.$i.e : SO(n, \mathbb{k}) = \{A \in O(n, \mathbb{k}) \mid \det(A) = 1\}$.

Remarque 3.4.1 .

1. En caractéristique 2, le déterminant de tout élément de $O(q)$ est 1, et la définition du groupe spécial orthogonal est alors tout autre.
2. Les $O(q)$ et, si la caractéristique de $\mathbb{k}$ est différente de 2, les $SO(q)$ sont des groupes algébriques : si $\mathbb{k}$ est un corps infini, il est un fermé de $GL(E)$ pour la topologie de Zariski.

   Dans le cas du groupe $O(n, \mathbb{k})$, il suffit d'observer que c'est l'ensemble des zéros de l'application polynomiale $M \to M^t M - I_n$ de $M_n(\mathbb{k})$ (espace des matrices carrées) dans lui-même.

Groupes orthogonaux réels et complexes

Groupes orthogonaux réels Dans cette section on suppose que $\mathbb{k}$ est le corps $\mathbb{R}$ des nombres réels.

Si q est définie positive, alors $O(q)$ et $SO(q)$ sont isomorphes à $O(n, \mathbb{R})$ et $SO(n, \mathbb{R})$.

On les note $O(n)$ et $SO(n)$.

Géométriquement, $O(n)$ est le groupe des isométries euclidiennes de R^n qui préservent l'origine (ou, ce qui est équivalent, appartiennent à $GL(n, \mathbb{R})$), $SO(n)$ son sous-groupe des éléments qui préservent l'orientation (isométries directes).

$SO(2)$ est isomorphe (en tant que groupe de Lie, voir plus loin) au cercle S^1, formé des nombres complexes de module 1, muni de la multiplication.

Cet isomorphisme lie le nombre complexe $\exp(it) = \cos t + i \sin t$ à la matrice orthogonale

$$S^1 = \left\{ M : M_t = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix} \right\}.$$

Le groupe $SO(3)$ est souvent appelé groupe des rotations (vectorielles) dans l'espace (tridimensionnel).

Définition 3.4.4 *Les groupes $O(n)$ et $SO(n)$ sont des sous-groupes fermés du groupe de Lie $GL(n,\mathbb{R})$ (par exemple : $O(n)$ est fermé dans $GL(n,\mathbb{R})$ — et même dans $M_n(R) \cong R^{n^2}$ - car c'est l'image réciproque du singleton $\{I_n\}$ par l'application continue $M \to M^t M$).*

Ce sont donc des groupes de Lie réels. Leurs dimensions sont égales à $n(n-1)/2$.

Exemple 3.4.3 *Sont f application $f : E \to E$, f continue,*

$$O(3) = \{M_f \ ; M_f = M\,{}^tM\}, \text{soit } A = \begin{bmatrix} 1 & 0 & -2 \\ 2 & -1 & 0 \\ 0 & 3 & 4 \end{bmatrix}, A^t = \begin{bmatrix} 1 & 2 & 0 \\ 0 & -1 & 3 \\ 0 & 0 & 4 \end{bmatrix}.$$

$$M_f = \begin{bmatrix} 1 & 0 & -2 \\ 2 & -1 & 0 \\ 0 & 3 & 4 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 0 \\ 0 & -1 & 3 \\ 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & -8 \\ 0 & 1 & -3 \\ 2 & 1 & 24 \end{bmatrix}.$$

L'algèbre de Lie associée aux groupes de Lie $O(n)$ et $SO(n)$ est formée des matrices carrées d'ordre n qui sont antisymétriques.

Elle est généralement notée $O(n)$ ou $SO(n)$.

En termes de topologie algébrique, pour $n > 2$, le groupe fondamental de $SO(n)$ est d'ordre 2 et son revêtement universel est $Spin(n)$.

Pour $n = 2$, le groupe fondamental est $\mathbb{Z}$ et le revêtement universel est $\mathbb{R}$.

Groupes orthogonaux complexes Si $\mathbb{k}$ est le corps $\mathbb{C}$ des nombres complexes, alors $O(q)$ et $SO(q)$ sont isomorphes à $O(n,\mathbb{C})$ et $SO(n,\mathbb{C})$.

De manière analogue aux groupes orthogonaux euclidiens (en remplaçant $\mathbb{R}$ par $\mathbb{C}$), $O(n,\mathbb{C})$ et $SO(n,\mathbb{C})$ sont des sous-groupes fermés du groupe de Lie $GL(n,\mathbb{C})$ et sont donc des groupes de Lie complexes. Leurs dimensions (sur $\mathbb{C}$) sont égales à $n(n-1)/2$.

Si $n \geq 2$, les groupes topologiques $O(n,\mathbb{C})$ et $SO(n,\mathbb{C})$ ne sont pas compacts, mais $O(n)$ et $SO(n)$ sont des sous-groupes compacts maximaux de ces groupes.

La composante neutre de $O(n,\mathbb{C})$ est $SO(n,\mathbb{C})$ L'algèbre de Lie associée aux groupes de Lie $O(n,\mathbb{C})$ et $SO(n,\mathbb{C})$ est formée des matrices complexes carrées d'ordre n qui sont antisymétriques.

Elle est généralement notée $O(n,\mathbb{C})$ ou $SO(n,\mathbb{C})$.

Pour $n>2$, le groupe fondamental de $SO(n,\mathbb{C})$ est d'ordre 2 et son revêtement universel est le groupe spinoriel complexe $Spin(n,\mathbb{C})$.

Pour $n=2$, le groupe fondamental est $\mathbb{Z}$ et le revêtement universel est $\mathbb{C}$.

3.4.4 Groupe unitaire

Définition 3.4.5 [7] *Une matrice A de $M_n(\mathbb{C})$ est dite unitaire si et seulement si l'endomorphisme de $\mathbb{C}^n$ représenté par A dans la base cononique de $\mathbb{C}^n$, est un endomorphisme unitaire de $\mathbb{C}^n$ muni de produit scalaire hermitien usual.*

On note $U(n)$ l'ensemble des matrices unitaires de $M_n(\mathbb{C})$.

i.e : $U(n)=\left\{A\in GL(n,\mathbb{C}) \mid A^t\bar{A}=I\right\}$.

3.4.5 Groupe spécial unitaire

L'ensemble de matrices unitaires d'ordre n de déterminant à 1 est un sous-groupe de $U(n)$, *appelé groupe* spécial unitaire (*d'ordre*) ; et noté $SU(n)$.

i.e : $SU(n)=\{A\in U(n)\,;\det(A)=1\}$.

3.4.6 Groupe symplectique

Définition 3.4.6 *Un groupe symplectique est un sous-groupe du groupe général linéaire laissant invariante une forme bilinéaire alternée* 1.

Définition 3.4.7 *De façon plus abstraite, sur un corps commutatif $\Bbbk$ de caractéristique différente de 2, le groupe symplectique de degré $2n$, noté $Sp(2n,\Bbbk)$,*

i.e : $Sp(2n,\mathbb{R})=\{A\in GL(n,\mathbb{R})\ ;\ -JA^tJ=A^{-1}\}$.

Peut être défini comme l'ensemble des automorphismes d'un $\Bbbk$-espace vectoriel symplectique E de dimension $2n$, c'est-à-dire des transformations linéaires bijectives de l'espace vectoriel E préservant une forme bilinéaire non dégénérée antisymétrique fixée.

Généralités

$Sp(2n, \Bbbk)$ est le groupe des matrices symplectiques $2n \times 2n$ à coefficients dans $\Bbbk$, muni de la multiplication matricielle.

Comme toutes les matrices symplectiques ont pour déterminant 1, le groupe symplectique est un sous-groupe du groupe spécial linéaire $SL(2n, \Bbbk)$.

Si $n = 1$, la condition symplectique sur une matrice est satisfaite si et seulement si son déterminant est égal à 1, si bien que $Sp(2, \Bbbk) = SL(2, \Bbbk)$. Pour $n > 1$, d'autres conditions s'y ajoutent.

Typiquement, le corps $\Bbbk$ est le corps des nombres réels $\mathbb{R}$ ou des nombres complexes $\mathbb{C}$.

Dans ce cas, $Sp(2n, \Bbbk)$ est un groupe de Lie réel ou complexe, de dimension réelle ou complexe $n(2n + 1)$.

Ces groupes sont connexes mais pas compacts.

$Sp(2n, \mathbb{C})$ est simplement connexe tandis que $Sp(2n, \mathbb{R})$ possède un groupe fondamental isomorphe à $\mathbb{Z}$.

L'algèbre de Lie de $Sp(2n, \Bbbk)$ est donnée par l'ensemble des matrices $2n \times 2n$ réelles ou complexes A satisfaisant : $JA + A^t J = 0$.

Où A^t est la transposée de A et J est la matrice antisymétrique
$J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$.

Relations entre les groupes symplectiques La relation entre les groupes $Sp(2n, \mathbb{R})$, $Sp(2n, \mathbb{C})$ et $Sp(n)$ est la plus évidente au niveau de leur algèbre de Lie.

Les algèbres de Lie de ces trois groupes, considérés comme groupes de Lie réels, partagent la même complexification.

Dans la classification des algèbres de Lie simples de Cartan, cette algèbre est notée C_n.

L'algèbre de Lie complexe $\mathbb{C}_n$ est juste l'algèbre $Sp(2n, \mathbb{C})$ du groupe de Lie complexe $Sp(2n, \mathbb{C})$.

Cette algèbre possède deux formes réelles différentes : la forme compacte, $Sp(n)$, qui est l'algèbre de Lie de $Sp(n)$, la forme normale, $Sp(2n, \mathbb{R})$, qui est l'algèbre de Lie de $Sp(2n, \mathbb{R})$.

3.5 La norme de matrice de frobenius

La norme de matrice de frobenius $A \in C^{m\times n}$ defini par :
$\|A\|_F^2 = \sum_{i,j} \mid a_{ij} \mid^2 = \sum_i \|A_{i\,*}\|_2^2 = \sum_j \|A_{*\,\mathrm{j}}\|_2^2 = tarce\,(A^*A)\,.$

Bibliographie

[1] Amara Hitta : Cours d'Algebre et Exercices corriges,Place centrale de Ben-Aknoun $(Alger)$, OPU.

[2] Corina Reischer ;A.Paradis :Éléments d'algébre linéaire ,Presses de l'Université du Québec(1992)

[3] Daniel Matrignon et P.Derbez ; Groupes Linéaires Classiques ; 13453 ;Marseille Cedex 13(2010) .

[4] JEAN-ChARLESSAVIOZ :Algebre linéaire ,Vuibert,20 Octobre 2003.

[5] Jean-Marie Monier :Algébre et géometrie MP ; DUNOD,Paris,1996,2004.

[6] Marie.A-Chevalier.oudot :algébre et géométrie euclidienne ;Hachette Livre.2003.

[7] Mohamed Zitouni : Algébre , Place centrale de Ben-Aknoun$(Alger)$, OPU Re$impression$ 1993.

[8] Myrian Maumy : Mathématiques Algebre et Géométrie en 30 fiches,Dunod,pais,2009.

Abstract

We are study the important section of theory groups which related the laniary algebra with the abstract algebra. In our memory we study the special groups in deferent space as the matricial groups of special cases the matrix which has determinant equal ± 1.

In the first study the algebra structure vector space, Euclidian space, hermitien space and the linear application space to defined idea about properties of matrix groups in finally funded the Frobenuis matrix groups as used in applied algebra and Informatics and in the Cryptography.

Key words: Groups, vector space, Euclidian space, hermitien space, Matrix, groups of Frobenuis.

Résumé

Nous avons étudier un importante section de théories groupes qui lie l'algèbre linéaire avec l'algèbres abstract. Evidement nous aborde les groupes matricielles de spécial cas les matrices a déterminant ± 1.

Nous abordons les divers structures algébriques, l espace vectoriel, espace euclidien, espace hermitien espace des application linéaire et leur certain propretés pour définir les groupe matricielles sur tous les groupes matricielles de Frobenuis qui sont utiliser dans l'algèbre applique et informatique et cryptographie .

Mors clés: Groupes, espace vectoriel, espace euclidien, espace hermitien, Matrices, Groupes de Frobenuis.

الملخص

هدفنا في هذا العمل هو دراسة فرع مهم من فروع نظرية الزمر التي تربط بين الجبر الخطي و الجبر المجرد. ولهذا درسنا زمر المصفوفات الخاصة بالمصفوفات التي محددها 1+ أو 1- .

ولهذا تطرقنا إلى البنى الجبرية التالية الفضاء الشعاعي و الفضاء الاقليدي و الفضاء الهرمتي و فضاء التطبيقات الخطية و توضيح خواصها لكي نعرف زمر المصفوفات وخاصة زمر مصفوفات فروبنيوس التي تستعمل في الجبر التطبيقي و الإعلام الآلي و التشفير.

الكلمات المفتاحية :

الزمر، الفضاء الشعاعي، الفضاء الاقليدي، الفضاء الهرميتي، المصفوفات، زمر فروبنيوس.