



REPUBLIQUE ALGERIENNE DEMOCRATIQUE
ET POPULAIRE
MINISTRE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE



Université Mohamed Boudiaf de M'sila

Faculté des Mathématiques et de l'Informatique

Département des Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Algèbre et Mathématiques Discrètes

Thème

*Représentations Linéaires des Groupes Finis et leurs Applications en
Cryptographie*

Présentée par :

MAHDI KHAWLA

Soutenu publiquement le : xx/06/2025.

Devant le jury composé de :

Président : DOUADI MIHOUBI

Encadreur : GHADBANE NACER

Examineur : HEBOUB LAKHDAR

Prof, Université de M'sila

M.C.A, Université de M'sila

M.C.B, Université de M'sila

Année universitaire 2024/2025.

Dédicace

À ceux qui ont été, après Dieu, la source de tout succès.

À ceux qui m'ont appris la patience et la persévérance.

À ceux qui ont soutenu mon cœur avant mon parcours.

À mes chers parents.

Je dédie ce travail en reconnaissance de vos sacrifices et de votre
amour.

Et à tous ceux qui m'ont encouragé, de près ou de loin,

Recevez toute ma gratitude.

Remerciements

Nous remercions Dieu Tout-Puissant qui nous a permis de mener à bien ce travail et qui l'a inspiré avec santé, bien-être et détermination.

Dieu merci, merci beaucoup. Nous adressons nos sincères remerciements et notre reconnaissance au professeur superviseur *Ghadbane Nacer* pour tous les précieux conseils et informations qu'il nous a fournis et qui ont contribué à compléter le sujet de notre étude dans ses différents aspects.

Et aux professeurs d'université respectés, nous vous disons merci beaucoup pour tous vos efforts.

Table des matières

Introduction

1	Notions de base	1
1.1	Groupe	1
1.1.1	Sous-groupe	1
1.1.2	Sous-groupe engendré	2
1.1.3	Groupe monogène et groupe cyclique	3
1.1.4	Ordre d'un groupe et ordre d'un élément	4
1.1.5	Groupe quotient	5
1.2	Homomorphisme de groupes	6
1.3	Corps	7
1.4	Espace vectoriel	7
1.4.1	Sous-espace vectoriel	8
1.4.2	Somme directe	8
1.4.3	Applications linéaires	9
1.4.4	Groupe général linéaire d'un espace vectoriel	10
1.4.5	Projection	10
2	Représentation linéaire des groupes finis	12
2.1	Représentation linéaire	12
2.2	Représentations semblables	13
2.3	Sous-représentation	16
2.3.1	Sous Espace vectoriel stable par une représentation	16
2.3.2	Sous-représentation	16
2.4	Représentation irréductibles	18
2.5	Produit tensoriel de deux représentations	19
2.5.1	Lemme de Schur	20
2.6	Représentation régulière	21
2.7	Représentations induites	21
3	Caractère d'une représentation et applications	23
3.1	Caractère d'une représentation linéaire	23
3.2	Orthonormalité des caractères irréductibles	25
4	Cryptosystème basé sur la représentation d'un groupe fini .	29
4.1	Un nouveau système de cryptographie à clé publique basé sur les représentations linéaires des groupes finis	29
4.1.1	Schéma de chiffrement proposé	29
4.1.2	Sécurité et efficacité	30
4.1.3	Exemple	31

4.2	Nouveau système de cryptographie à clé publique basé sur le problème d'isomorphisme des représentations matricielles des groupes finis	33
4.2.1	Schéma de chiffrement proposé	33
4.2.2	Sécurité et efficacité	33
4.2.3	Considérations pratiques	34
4.2.4	Exemple	34

Bibliographie	36
----------------------	-----------

Introduction

La théorie des représentations des groupes permet l'étude des groupes abstraits en représentant leurs éléments par des matrices inversibles. On dispose alors des méthodes de l'algèbre linéaire qui rendent souvent l'étude de ces groupes plus facile et permettent d'en obtenir de nouvelles propriétés. L'idée est de faire agir un groupe G sur un espace vectoriel V de telle sorte que l'action de chaque élément soit compatible avec la structure d'espace vectoriel, c'est-à-dire soit un élément de $GL(V)$ le groupe des automorphismes linéaires de V et plus seulement une bijection de V sur V .

Ce concept émerge à la fin du 19ème siècle et l'étude générale des représentations d'un groupe est largement développée par William Burnside et Ferdinand Georg Frobenius au début du 20ème siècle.

Notre travail est composé de trois parties :

Dans le premier chapitre, nous allons décrire quelques concepts et propriétés liés à la théorie des groupes et l'algèbre linéaire.

Le deuxième chapitre est dédié à l'introduction des concepts fondamentaux de la théorie des représentations linéaires des groupes finis (tels que la représentation linéaire, la sous-représentation, la représentation irréductible, la représentation induite, etc.).

Le troisième chapitre est consacré à l'étude des caractères des représentations linéaires ainsi qu'à leurs principales propriétés.

Dans la continuité des chapitres précédents, le quatrième chapitre concerne les applications de la théorie des représentations linéaires au domaine de la cryptographie. Il présente deux systèmes de cryptographie basés sur les représentations des groupes finis, avec une attention portée sur certains aspects liés à leur performance et à leur sécurité.

Chapitre 1

Notions de base

Ce premier chapitre contient les définitions et les propriétés des outils que nous utiliserons par la suite : groupe, sous-groupe, sous-groupe engendré, groupe cyclique, groupe monogène, ordre d'un groupe, ordre d'un élément, homomorphisme de groupes, corps, espace vectoriel, sous-espace vectoriel, somme directe, application linéaire, groupe général linéaire d'un espace vectoriel, projection et la trace d'une matrice.

1.1 Groupe

Définition

Un groupe est un ensemble muni d'une opération interne, associative, d'un élément neutre e , et tel que tout élément x possède un inverse x^{-1} . L'opération sera notée selon les cas $+$ (loi additive), ou $\times$, $\cdot$ (loi multiplicative), ou encore $*$, $\circ$, etc. On a donc :

$$\forall a, b \in G, \quad a \cdot b \in G \quad (1.1)$$

$$\forall a, b, c \in G, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad (1.2)$$

$$\exists e \in G, \forall a \in G, \quad a \cdot e = e \cdot a = a \quad (1.3)$$

$$\forall a \in G, \exists a^{-1} \in G, \quad a \cdot a^{-1} = a^{-1} \cdot a = e \quad (1.4)$$

L'opération peut être ou non commutative. Un groupe commutatif est aussi dit **abélien**.

Un groupe peut avoir un nombre d'éléments, ou *ordre*, fini ou infini. Dans le second cas, le groupe peut être *discret* ou *continu*.

Exemples

- . $(\mathbb{Z}, +)$: Le groupe des entiers relatifs muni de l'addition (commutatif).
- . $(\mathbb{R}, +)$: Le groupe des nombres réels muni de l'addition (commutatif).
- . $(\mathbb{C}^*, \cdot)$: L'ensemble des nombres complexes non nuls muni de la multiplication (commutatif).
- . $(GL_n(\mathbb{R}), \cdot)$: L'ensemble des matrices inversibles $n \times n$ à coefficients réels muni de la multiplication matricielle (non commutatif en général).

1.1.1 Sous-groupe

Définition

Un sous-groupe $(H, \cdot)$ est un sous-ensemble H d'un groupe $(G, \cdot)$ qui est lui-même un groupe pour la même loi de composition interne. C'est-à-dire :

. H contient l'élément neutre de G :

$$e \in H.$$

. H est stable par la loi de G :

$$\forall x, y \in H, \quad x \cdot y \in H.$$

. H est stable par l'inverse :

$$\forall x \in H, \quad x^{-1} \in H.$$

Si le groupe $(G, \cdot)$ est commutatif, alors le sous-groupe $(H, \cdot)$ est aussi commutatif.

proposition

Soit $(G, \cdot)$ un groupe et $H \subset G$, alors $(H, \cdot)$ est un sous-groupe de $(G, \cdot)$ si et seulement si :

. $H \neq \emptyset$.

. $\forall x, y \in H, \quad xy^{-1} \in H$.

Notation

On note $(H, \cdot) \leq (G, \cdot)$.

Définition

Un sous-groupe H est un sous-groupe **normal**, noté $H \triangleleft G$, si et seulement si :

$$\forall x \in G, \quad xH = Hx.$$

Exemples

Quelques exemples de sous-groupes :

. Les sous-groupes de $(\mathbb{Z}, +)$ est de la forme :

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}, \quad \text{où } n \in \mathbb{N}.$$

. $(\{1, -1\}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$

. $(\{0, 2, 4\}, +)$ est un sous-groupe de $(\mathbb{Z}/6\mathbb{Z}, +)$

1.1.2 Sous-groupe engendré

Définition

Soit G un groupe, et S une partie non vide de G .

Soit $\mathcal{H}_S$ l'ensemble des sous-groupes de G contenant S .

On appelle sous-groupe engendré par S le sous-groupe :

$$\langle S \rangle = \bigcap_{H \in \mathcal{H}_S} H$$

Exemple

. $3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$

$(3\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ engendré par 3.

1.1.3 Groupe monogène et groupe cyclique .

Définition

Un groupe est monogène s'il est engendré par un seul élément. Un groupe d'ordre fini engendré par un élément est cyclique.

Définition

Soit $(G, \cdot)$ un groupe. Le sous-groupe engendré par un élément $g \in G$, noté $\langle g \rangle$, est défini par :

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Un groupe est dit cyclique s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$, et g est d'ordre fini.

Remarque

- . Si un groupe G peut être écrit sous la forme $G = \langle g \rangle$, alors g est appelé un **générateur** de G .
- . Si G est un groupe infini et admet un unique générateur g , c'est-à-dire si $G = \langle g \rangle$, alors on dit que G est un **groupe monogène**.

Exemple

Le groupe des racines n -ièmes de l'unité dans $\mathbb{C}$ est un groupe cyclique :

$$G = \{\zeta \in \mathbb{C} : \zeta^n = 1\}.$$

Par exemple, pour $n = 4$:

$$\zeta^4 = 1 \Leftrightarrow \zeta \in \{1, -1, i, -i\}.$$

Donc, ce groupe est cyclique car il peut être engendré par un seul élément, comme $\zeta = e^{2i\pi/4} = i$.

Propositions

1. Tout sous-groupe d'un groupe cyclique est cyclique.
2. Un groupe cyclique $G = \langle g \rangle$, engendré par un élément g , est toujours un groupe abélien (commutatif).

Démonstrations

1. Soit $G = \langle g \rangle$ un groupe cyclique, c'est-à-dire que tout élément de G est de la forme g^k , avec $k \in \mathbb{Z}$. Soit $H \leq G$ un sous-groupe de G .

- . Si $H = \{e\}$, alors H est cyclique, car engendré par l'élément neutre : $H = \langle e \rangle$.
- . Supposons maintenant que $H \neq \{e\}$. Comme $H \subseteq G$, chaque élément de H est de la forme g^k . Considérons l'ensemble

$$S = \{k \in \mathbb{N}^* \mid g^k \in H\}.$$

Cet ensemble est non vide et admet un plus petit élément m , d'après le principe du bon ordre.

Soit $h = g^m$. Montrons que $H = \langle h \rangle$.

- . Puisque $h = g^m \in H$, on a $\langle h \rangle \subseteq H$.

- . Soit $g^k \in H$. Par division euclidienne, il existe des entiers q, r avec $0 \leq r < m$ tels que

$$k = qm + r.$$

Alors

$$g^k = g^{qm+r} = g^{qm} \cdot g^r = (g^m)^q \cdot g^r = h^q \cdot g^r.$$

Comme $g^k \in H$ et $h^q \in H$, on a $g^r = g^k \cdot (h^q)^{-1} \in H$.

Or $0 \leq r < m$, et m est le plus petit entier strictement positif tel que $g^m \in H$.

Par conséquent, $r = 0$.

Donc $g^k = h^q \in \langle h \rangle$, ce qui montre que $H \subseteq \langle h \rangle$.

Finalement, on a $H = \langle h \rangle$, donc H est cyclique.

2. Soit $G = \langle g \rangle$ un groupe cyclique. Tout élément de G est de la forme g^m avec $m \in \mathbb{Z}$.

Soient $a = g^m$ et $b = g^n$ deux éléments de G . Alors :

$$ab = g^m \cdot g^n = g^{m+n}, \quad \text{et} \quad ba = g^n \cdot g^m = g^{n+m}.$$

Mais comme l'addition dans $\mathbb{Z}$ est commutative, $m + n = n + m$, donc $ab = ba$.

Ainsi, G est abélien.

1.1.4 Ordre d'un groupe et ordre d'un élément

Définition

Soit G un groupe fini. L'ordre de G est le cardinal de G , c'est-à-dire le nombre d'éléments qu'il contient. Il est noté :

$$|G| = n.$$

L'ordre d'un élément $x \in G$ est défini comme le cardinal du sous-groupe engendré par x . Autrement dit, c'est le plus petit entier positif k tel que :

$$x^k = e.$$

Remarque

- . L'ordre d'un élément x est donné par :

$$O(x) = \min\{k \in \mathbb{N}^* : x^k = e\}.$$

- . Si un tel k n'existe pas, on dit que x a un ordre infini.
- . Si G est un groupe fini d'ordre n , alors l'ordre de tout élément de G divise n (théorème de Lagrange).

Exemples

Le groupe symétrique S_3 (ensemble des permutations de trois éléments) :

- . $|S_3| = 6$, car il contient 6 permutations distinctes.
- . L'ordre de la permutation (123) est 3, car appliquer trois fois cette permutation donne l'identité :

$$(123) \circ (123) \circ (123) = e.$$

1.1.5 Groupe quotient

Définition

Soit E un ensemble. Une relation R définie sur E est dite **relation d'équivalence** si elle satisfait les trois propriétés suivantes :

1. **Réflexivité** : Tout élément de E est en relation avec lui-même, c'est-à-dire :

$$\forall x \in E, \quad x R x.$$

2. **Symétrie** : Si un élément x est en relation avec un élément y , alors y est aussi en relation avec x , c'est-à-dire :

$$\forall x, y \in E, \quad x R y \Rightarrow y R x.$$

3. **Transitivité** : Si un élément x est en relation avec un élément y et que y est en relation avec un élément z , alors x est en relation avec z , c'est-à-dire :

$$\forall x, y, z \in E, \quad (x R y \text{ et } y R z) \Rightarrow x R z.$$

Définition

Soit G un groupe et H un sous-groupe de G . On définit deux relations d'équivalence sur G par :

$$x \sim_g y \Leftrightarrow x^{-1}y \in H$$

$$x \sim_d y \Leftrightarrow xy^{-1} \in H$$

Ces relations sont appelées **relation d'équivalence modulo H** à gauche, respectivement à droite et permettent de partitionner G en classes à gauche et à droite (respectivement).

. Cas 1 : Classes à gauches

La classe à gauche d'un élément $x \in G$ est définie par :

$$\bar{x}_g = xH = \{xh \mid h \in H\}$$

L'ensemble des classes à gauche est noté G/H .

. Cas 2 : Classes à droite

La classe à droite d'un élément $x \in G$ est définie par :

$$\bar{x}_d = Hx = \{hx \mid h \in H\}$$

L'ensemble des classes à droite est noté $H \backslash G$.

Remarque

- . Si G est commutatif, alors $Q_g = Q_d$, ce qui implique que les classes à gauche et à droite coïncident :

$$xH = Hx, \quad \forall x \in G$$

- . Si G n'est pas commutatif, alors les classes à gauche et à droite peuvent être différentes :

$$xH \neq Hx$$

- . Si G est abélien, alors G/H l'est aussi.

Propriétés

- . G/H est un groupe si H est un sous-groupe normal, l'opération de multiplication est bien définie .
- . La classe de l'élément neutre est égale à H :

$$eH = H$$

- . Si $H \triangleleft G$, alors G/H est un groupe dit groupe quotient.
- . Si G est un groupe fini et H un sous-groupe normal, alors

$$|G/H| = \frac{|G|}{|H|}$$

(Théorème de Lagrange).

Exemple

- . Groupe des entiers modulo n , $(\mathbb{Z}/n\mathbb{Z}, +)$.

1.2 Homomorphisme de groupes

Définition

Soient $(G, \star)$ et $(H, \cdot)$ deux groupes. Un morphisme de groupes (ou homomorphisme de groupes) est une application :

$$f : G \rightarrow H$$

telle que pour tout couple (x, y) d'éléments de G ,

$$f(x \star y) = f(x) \cdot f(y).$$

Propriétés

- . $f(e_G) = e_H$, où e_G et e_H sont les éléments neutres de G et H respectivement.
- . $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$.
- . Le noyau d'un morphisme f est défini par :

$$\ker(f) = \{x \in G \mid f(x) = e_H\}$$

- . L'image d'un morphisme f est définie par :

$$\text{Im}(f) = \{f(x) \mid x \in G\}$$

- . $\ker(f)$ est un sous-groupe normal de G .
- . $\text{Im}(f)$ est un sous-groupe de H .

Exemples

- . On considère les deux groupes $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$. L'application $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$, $x \rightarrow e^x$ est un homomorphisme de groupes, car :

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x)f(y)$$

- . L'application $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ est un homomorphisme de groupe :

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Définitions

Soit $f : G \rightarrow H$ un homomorphisme de groupes :

- . Si f est bijective, on dit que f est un isomorphisme de groupes et que $G \cong H$.
- . Un homomorphisme de G dans G est appelé un endomorphisme de G .
- . Un endomorphisme bijectif est appelé un automorphisme de G .

1.3 Corps

Définition

Un corps $(K, +, \times)$ est une structure algébrique composée d'un ensemble K muni de deux lois de composition qui satisfont les conditions suivantes :

- . $(K, +)$ est un groupe abélien, dont l'élément neutre est noté 0.
- . $(K \setminus \{0\}, \times)$ est un groupe abélien, dont l'élément neutre est 1.
- . La multiplication est distributive par rapport à l'addition (à gauche comme à droite), c'est-à-dire que :

$$\forall (a, b, c) \in K^3, \quad a \times (b + c) = a \times b + a \times c$$

$$(b + c) \times a = b \times a + c \times a$$

On parle alors du **corps commutatif** $(K, +, \times)$.

Exemples

- . $(\mathbb{Z}/p\mathbb{Z}, +, \times)$, où p est un nombre premier est un corps.
- . $(\mathbb{R}, +, \times)$ est un corps.

1.4 Espace vectoriel

Soit $\mathbb{K}$ un corps commutatif.

Définition

Un **$\mathbb{K}$ -espace vectoriel** est un ensemble E muni :

- . d'une **loi de composition interne** notée "+" :

$$+ : E \times E \rightarrow E, \quad (x, y) \mapsto x + y$$

- . d'une **loi de composition externe** (multiplication par un scalaire) définie par :

$$\cdot : \mathbb{K} \times E \rightarrow E, \quad (\lambda, x) \mapsto \lambda \cdot x$$

L'ensemble E est un **$\mathbb{K}$ -espace vectoriel** si :

- . $(E, +)$ est un **groupe abélien** (c'est-à-dire que 0 est l'élément neutre et + est commutatif).
- 1. La loi " $\cdot$ " satisfait les quatre propriétés suivantes :
 - . **Multiplication scalaire par 1** :

$$\forall x \in E, \quad 1 \cdot x = x.$$

. **Distributivité sur l'addition des vecteurs :**

$$\forall x, y \in E, \quad \forall \lambda \in \mathbb{K}, \quad \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y.$$

. **Distributivité sur l'addition des scalaires :**

$$\forall x \in E, \quad \forall \lambda, \mu \in \mathbb{K}, \quad (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x.$$

. **Associativité de la multiplication scalaire :**

$$\forall x \in E, \quad \forall \lambda, \mu \in \mathbb{K}, \quad (\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x).$$

Exemples

Voici quelques exemples d'espaces vectoriels :

- . $(\mathbb{R}^n, +, \cdot)$ est un $\mathbb{R}$ -espace vectoriel.
- . $(\mathbb{P}_n(\mathbb{R}), +, \cdot)$, l'ensemble des polynômes de degré inférieur ou égal à n à coefficients réels, est un espace vectoriel.
- . $(M_{m \times n}(\mathbb{R}), +, \cdot)$, l'ensemble des matrices $m \times n$ à coefficients réels, est un espace vectoriel.

1.4.1 Sous-espace vectoriel

Définition

Soit E un espace vectoriel et soit F une partie de E . On dit que F est un **sous-espace vectoriel** de E si et seulement si :

1. F contient le vecteur nul de E :

$$0 \in F.$$

2. F est stable par addition :

$$\forall u, v \in F, \quad u + v \in F.$$

3. F est stable par multiplication par un scalaire :

$$\forall u \in F, \quad \forall \lambda \in \mathbb{K}, \quad \lambda u \in F.$$

Exemples

- . $F = \{(x, y, z) \in \mathbb{R}^3 : x - 2y + z = 0\}$ est sous-espace vectoriel de $\mathbb{R}^3$.
- . Soit G l'ensemble des matrices triangulaires supérieures .

$$G = \{A = (a_{ij}) : a_{ij} = 0 \text{ pour } i > j\}$$

G est sous-espace vectoriel de $M_n(\mathbb{R})$

1.4.2 Somme directe

Soient F et G deux sous-espaces vectoriels de E . On dit que la somme de F et G est **directe** si :

$$F \cap G = \{0\}, F + G = E.$$

Dans ce cas, on note :

$$F \oplus G = E.$$

On dit aussi que F et G sont supplémentaires dans E .

Théorème

Soit E un espace vectoriel et F, G deux sous-espaces vectoriels de E . Alors

$$\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G).$$

Si $E = F \oplus G$, alors

$$\dim(E) = \dim(F) + \dim(G).$$

1.4.3 Applications linéaires

Définition

Soient E et F des espaces vectoriels sur un même corps K . Une application f de E dans F est appelée application linéaire si elle vérifie les deux propriétés suivantes :

. **Additivité** : $\forall x, y \in E, f(x + y) = f(x) + f(y)$.

. **Homogénéité** : $\forall x \in E, \forall \lambda \in K, f(\lambda x) = \lambda f(x)$.

De plus, si $E = F$, on dit que f est un endomorphisme de E .

Remarque

Si $f : E \rightarrow F$ est une application linéaire, alors :

1. $f(0_E) = 0_F$.

2. $\forall x, y \in E, f(x - y) = f(x) - f(y)$.

Exemple

Soit l'application

$$\begin{aligned} f : \mathbb{R}^3 &\rightarrow \mathbb{R}^2 \\ (x, y, z) &\mapsto (x + 2y, y + 3z) \end{aligned}$$

f est une application linéaire :

. Soient $(x, y, z), (x', y', z') \in \mathbb{R}^3$

$$f[(x, y, z) + (x', y', z')] = f(x + x', y + y', z + z')$$

$$= (x + x' + 2(y + y'), y + y' + 3(z + z'))$$

$$= (x + 2y + x' + 2y', y + 3z + y' + 3z')$$

$$= (x + 2y, y + 3z) + (x' + 2y', y' + 3z')$$

$$= f(x, y, z) + f(x', y', z')$$

. Soit $(x, y, z) \in \mathbb{R}^3$ et $\lambda \in \mathbb{R}$

$$f(\lambda \cdot (x, y, z)) = f(\lambda x, \lambda y, \lambda z)$$

$$= (\lambda x + 2\lambda y, \lambda y + 3\lambda z)$$

$$= \lambda \cdot (x + 2y, y + 3z)$$

$$= \lambda \cdot f(x, y, z)$$

1.4.4 Groupe général linéaire d'un espace vectoriel

Définition

Soit V un espace vectoriel sur le corps $\mathbb{K}$. Le groupe général linéaire de V noté $GL(V)$ est l'ensemble des applications linéaires bijectives de V dans lui-même, muni de la loi de composition.

Comme tout élément du groupe $GL(V)$ est bijectif, son application réciproque est définie. Pour tout élément $f \in GL(V)$, l'application inverse f^{-1} de f est également une application linéaire.

Matrice d'une application linéaire

Soit E et F deux espaces vectoriels de dimensions finies sur un corps $\mathbb{K}$, avec $\dim(E) = n$ et $\dim(F) = m$. Une application linéaire $f : E \rightarrow F$ peut être représentée par une matrice une fois que l'on a choisi des bases dans E et F .

Définition

Soient $B = (e_1, e_2, \dots, e_n)$ une base de E et $C = (f_1, f_2, \dots, f_m)$ une base de F .

Si f est une application linéaire, alors pour tout i , on peut écrire :

$$f(e_i) = a_{1i}f_1 + a_{2i}f_2 + \dots + a_{mi}f_m$$

où les scalaires sont les coefficients de la matrice de f dans les bases B et C .

La matrice de f dans ces bases est alors :

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \in M_{m,n}(K)$$

Propriétés

- Composition et produit matriciel : Si $g : F \rightarrow G$ est une autre application linéaire avec une base D de G alors la matrice de la composée $g \circ f$ est donnée par :

$$M_{B,D}(g \circ f) = M_{C,D}(g) \cdot M_{B,C}(f)$$

- Si f est un isomorphisme, M_f est inversible et $(M_f)^{-1} = M_{f^{-1}}$
- Si on fixe une base B de V , on a $GL_n(K) \cong GL(V)$

1.4.5 Projection

Définition

Soient E un espace vectoriel et F, G deux sous-espaces de E tels que :

$$E = F \oplus G$$

Cela signifie que tout vecteur $x \in E$ peut s'écrire de manière unique sous la forme : $x = u + v$ avec $u \in F$ et $v \in G$.

La projection sur F parallèlement à G est l'application linéaire

$P : E \rightarrow F$, définie par :

$$P(x) = u \quad \text{où} \quad x = u + v \text{ avec } u \in F, v \in G$$

Propriétés

- . P est linéaire.
- . P est une projection donc idempotente :

$$P \circ P = P$$

- . $\text{Im}(P) = F$ (l'image de P est le sous-espace sur lequel on projette).
- . $\text{Ker}(P) = G$ (le noyau est constitué des vecteurs de G , car ils sont envoyés sur zéro).

Définition

Soit A une matrice carrée de taille $n \times n$ à coefficients réels, telle que :

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

La **trace** de A , notée $\text{tr}(A)$, est donnée par :

$$\text{tr}(A) = a_{11} + a_{22} + \cdots + a_{nn} = \sum_{i=1}^n a_{ii}$$

Exemple

Soit

$$A = \begin{bmatrix} 1 & 1 & 3 \\ 4 & -3 & 11 \\ 2 & 0 & 114 \end{bmatrix}$$

Alors :

$$\text{tr}(A) = 1 + (-3) + 114 = 112$$

Propriétés

Soient A et B deux matrices carrées $n \times n$.

- . $\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B)$
- . $\text{tr}(AB) = \text{tr}(BA)$
- . $\text{tr}(A^T) = \text{tr}(A)$
- . $\text{tr}(aA) = a \text{tr}(A)$
- . $\text{tr}(aI_n + A) = a \cdot n + \text{tr}(A)$

Chapitre 2

Représentation linéaire des groupes finis

On considère un groupe fini G . Soit V un espace vectoriel de dimension finie sur le corps des complexes. On note $GL(V)$ le groupe des applications linéaires bijectives de V dans lui-même, muni de la composition des applications, que l'on notera également de manière multiplicative. Le choix d'une base de V permet alors d'identifier au groupe $GL(n, \mathbb{C}) = GL_n(\mathbb{C})$, formé de toutes les matrices inversibles de taille n à coefficients complexes.

2.1 Représentation linéaire

Définition

Soit G un groupe fini, d'élément neutre e et de loi de composition interne $(s, t) \mapsto st$.

Une représentation linéaire de G dans un espace vectoriel V est un homomorphisme de groupes $\rho : G \rightarrow GL(V)$.

En d'autres termes : pour tout $s, t \in G$, on a $\rho(s) \in GL(V)$ et $\rho(st) = \rho(s) \cdot \rho(t)$.

On a les propriétés suivantes :

- $\rho(e) = I$ (l'identité de $GL(V)$)
- $\rho(s^{-1}) = \rho(s)^{-1}$.

Exemples

1. Si pour tout $g \in G$, $\rho(g) = I$, alors ρ est appelée la représentation triviale de G .

2. Représentation de S_3 sur $\mathbb{C}^3$:

Soit $G = S_3$, le groupe symétrique des permutations de 3 éléments. Il contient 6 éléments : $S_3 = \{\text{id}, (12), (13), (23), (123), (132)\}$

On définit une représentation linéaire $\rho : S_3 \rightarrow GL_3(\mathbb{C})$, en associant à chaque permutation σ la matrice $\rho(\sigma)$ qui envoie la base canonique (e_1, e_2, e_3) sur $(e_{\sigma(1)}, e_{\sigma(2)}, e_{\sigma(3)})$. Ainsi, $\rho(\sigma)(e_i) = e_{\sigma(i)}$.

Les matrices associées :

$$\begin{aligned} \cdot \rho(\text{id}) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \rho((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \rho((13)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ \cdot \rho((23)) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \rho((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \rho((132)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \end{aligned}$$

3. Représentation linéaire de $\mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{R}^3$:

Soit $G = \langle 1 \rangle = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, un groupe cyclique d'ordre 3. On définit une représentation linéaire $\rho : G \rightarrow GL_3(\mathbb{R})$ par :

$$\cdot \rho(0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \rho(1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \rho(2) = (\rho(1))^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Définition

Soit un espace vectoriel de dimension finie n , on appelle alors le degré de la représentation.

Exemple

. Dans l'exemple 2 et 3 ρ est une représentation de degré $3 = \dim \mathbb{R}^3$, et dans l'exemple 1, le degré de la représentation est 1.

Définition

Soit G un groupe fini et V un espace vectoriel complexe de dimension n . On considère une représentation $\rho : G \rightarrow GL(V)$, c'est-à-dire une application qui associe à chaque élément $s \in G$ un automorphisme $\rho(s)$ de V .

Soit $(e_i)_{1 \leq i \leq n}$ une base de V . Pour tout élément $s \in G$, la transformation linéaire $\rho(s)$ peut être représentée par une matrice $R_s \in GL_n(\mathbb{C})$, appelée **matrice de la représentation** de s dans la base choisie.

Cette représentation vérifie les propriétés suivantes :

. $\det(R_s) \neq 0$, car R_s est inversible.

. $R_{st} = R_s R_t$ pour tous $s, t \in G$, ce qui exprime la compatibilité avec la loi du groupe.

Si l'on note $r_{ij}(s)$ les coefficients de la matrice R_s , alors les coefficients de la matrice R_{st} sont donnés par la formule :

$$r_{ik}(st) = \sum_j r_{ij}(s) \cdot r_{jk}(t).$$

Une telle construction est appelée une **représentation sous forme matricielle** du groupe G .

2.2 Représentations semblables

Définition

Soient $\rho : G \rightarrow GL(V)$ et $\rho' : G \rightarrow GL(W)$ deux représentations d'un même groupe G , où V et W sont deux $\mathbb{C}$ -espaces vectoriels de même dimension.

On dit que les deux représentations ρ et ρ' sont **isomorphes** s'il existe un isomorphisme linéaire $T : V \rightarrow W$ tel que, pour tout élément $g \in G$, le diagramme suivant commute :

$$T \circ \rho(g) = \rho'(g) \circ T$$

et on a le schéma suivant :

$$\begin{array}{ccc} V & \xrightarrow{\rho(g)} & V \\ T \downarrow & & \downarrow T \\ W & \xrightarrow{\rho'(g)} & W \end{array}$$

Autrement dit, pour tout vecteur $v \in V$, on a :

$$T(\rho(g)(v)) = \rho'(g)(T(v))$$

Cela signifie que l'action du groupe G sur V via ρ est identique, à un changement de base près, à son action sur W via ρ' .

Interprétation matricielle :

Si l'on exprime les représentations sous forme de matrices, alors il existe une matrice inversible P telle que, pour tout $g \in G$, on ait :

$$R'_g = P R_g P^{-1}$$

où R_g et R'_g sont les matrices représentant respectivement $\rho(g)$ et $\rho'(g)$ dans des bases choisies de V et W .

Remarque

Comme T est un isomorphisme linéaire, alors V et W sont de même dimension. En particulier, ρ et ρ' ont le même degré.

Exemples

1. On considère le groupe fini :

$$G = \{e, a\}, \quad \text{avec } a^2 = e$$

On définit deux représentations linéaires de G dans $\text{GL}_2(\mathbb{R})$:

Première représentation ρ :

$$\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Deuxième représentation ρ' :

$$\rho'(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho'(a) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Nous allons montrer que ρ et ρ' sont **semblables**, c'est-à-dire qu'il existe une matrice inversible T telle que :

$$\rho'(g) = T^{-1} \cdot \rho(g) \cdot T \quad \text{pour tout } g \in G$$

Prenons la matrice :

$$T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Calculons son inverse :

$$T^{-1} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

Effectuons le calcul :

$$T^{-1} \cdot \rho(a) \cdot T = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \rho'(a)$$

Donc, les deux représentations ρ et ρ' sont semblables.

2. On considère le groupe cyclique d'ordre 4 :

$$G = \{e, a, a^2, a^3\} \cong \mathbb{Z}/4\mathbb{Z}$$

soit ρ une représentation linéaire définie par :

$$\rho : G \rightarrow GL(\mathbb{R}^4), \quad \rho(a)(x, y, z, w) = (y, z, w, x)$$

Dans la base canonique de $\mathbb{R}^4$, la matrice associée à $\rho(a)$ est :

$$R_a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Soit l'isomorphisme linéaire $\tau : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ défini par :

$$\tau(x, y, z, w) = (x + y, x - y, z + w, z - w)$$

La matrice associée à τ dans la base canonique est :

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

On cherche une représentation ρ' semblable à ρ telle que :

$$\rho'(a) = T R_a T^{-1}$$

on a l'inverse de T est :

$$T^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

Le calcul donne :

$$\rho'(a) = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

Donc, ρ' est une représentation semblable à ρ via le changement de base défini par τ .

2.3 Sous-représentation

2.3.1 Sous Espace vectoriel stable par une représentation

Définition

Soit $\rho : G \rightarrow GL(V)$ une représentation. Un sous-espace vectoriel W de V est dit stable par ρ si : $(\forall s \in G), \rho_s(W) \subset W$

2.3.2 Sous-représentation

Définition

Soit $\rho : G \rightarrow GL(V)$ une représentation linéaire, et soit W un *sous-espace vectoriel* de V . Supposons que W stable pour les opérations de G , autrement dit supposons que $x \in W$ entraîne $\rho_s(x) \in W$ pour tout $s \in G$. La restriction de ρ_s à W est alors un isomorphisme de W sur lui-même, et l'on a évidemment $\rho_{st}^W = \rho_s^W \cdot \rho_t^W$. Ainsi $\rho^W : G \rightarrow GL(W)$ est une représentation linéaire de G dans W ; on dit que W est une *sous-représentation* de V .

Exemples

1. On considère le groupe $G = \{e, a\}$ avec $a^2 = e$, et la représentation $\rho : G \rightarrow GL_2(\mathbb{R})$ définie par $\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\rho(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Soit $V = \mathbb{R}^2$. On considère les sous-espaces vectoriels :

$$W_1 = \text{Vect} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right), \quad W_2 = \text{Vect} \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \right).$$

On vérifie que : $\rho(a) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in W_1$, $\rho(e) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in W_1$, donc W_1 est stable.

$\rho(a) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} \in W_2$, $\rho(e) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in W_2$, donc W_2 est stable.

Ainsi, W_1 et W_2 sont des sous-représentations de V .

2. Soit $G = S_n$, le groupe des permutations de n éléments. On définit une représentation naturelle $\rho : G \rightarrow GL_n(\mathbb{R})$ par permutation des coordonnées :

$$\rho(\sigma)(x_1, \dots, x_n) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}).$$

Considérons deux sous-espaces vectoriels de $\mathbb{R}^n$:

$$W_{\text{triv}} = \{(t, t, \dots, t) \in \mathbb{R}^n \mid t \in \mathbb{R}\}, \quad W_{\text{std}} = \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n \mid \sum_{i=1}^n x_i = 0 \right\}.$$

• W_{triv} C'est le sous-espace formé des vecteurs dont toutes les composantes sont égales. Ce sous-espace est invariant par l'action de car permuter les coordonnées d'un tel vecteur ne le modifie pas.

• W_{std} C'est le sous-espace des vecteurs dont la somme des composantes est nulle. Il est aussi stable par l'action de , car permuter les coordonnées ne change pas leur somme.

• Ces deux sous-espaces sont stables par l'action de S_n , donc ils définissent des sous-représentations de $\mathbb{R}^n$.

Définition

Soit $\rho : G \rightarrow \text{GL}(V)$ une représentation linéaire d'un groupe G dans un espace vectoriel V .

Si on peut écrire V comme une somme directe de sous-espaces vectoriels stables par ρ , c'est-à-dire :

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

et pour tout $g \in G$ et pour tout i , on a $\rho(g)(V_i) \subseteq V_i$, alors on dit que ρ est la **somme directe des sous-représentations**

$$\rho_i : G \rightarrow \text{GL}(V_i),$$

où $\rho_i(g)$ est la restriction de $\rho(g)$ à V_i .

On note alors :

$$\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_r.$$

Théorème 1 : (Maschke)

Soit G un groupe fini, V un K -espace vectoriel de dimension finie, et $\rho : G \rightarrow \text{GL}(V)$ une représentation linéaire de G .

Soit $W \subset V$ un sous-espace vectoriel G -stable, c'est-à-dire $\rho(g)(W) \subset W$ pour tout $g \in G$.

Alors, il existe un supplémentaire G -stable de W dans V , c'est-à-dire un sous-espace G -stable $W' \subset V$ tel que $V = W \oplus W'$.

Preuve

On commence par choisir un supplément quelconque W_0 de W dans V , donc $V = W \oplus W_0$.

On appelle $p : V \rightarrow W$ le projecteur sur W parallèlement à W_0 .

Soit $g = |G|$ le cardinal de G , et on pose :

$$p' = \frac{1}{g} \sum_{t \in G} \rho(t) \circ p \circ \rho(t)^{-1}.$$

On remarque que l'image de p' est contenue dans W puisque $\text{Im}(p) = W$ et W sont stables par ρ .

Pour tout $x \in W$, on a $\rho(t)^{-1}(x) \in W$ car W est stable, donc

$$p(\rho(t)^{-1}(x)) = \rho(t)^{-1}(x).$$

Ainsi,

$$p'(x) = \frac{1}{g} \sum_{t \in G} \rho(t) p \rho(t)^{-1}(x) = \frac{1}{g} \sum_{t \in G} \rho(t) \rho(t)^{-1}(x) = \frac{1}{g} \sum_{t \in G} x = x.$$

Il en résulte que p' est un projecteur de V sur W .

Définissons

$$W' = \ker(p').$$

Montrons que W' est stable par ρ .

Pour tout $s \in G$,

$$\rho(s)p'\rho(s)^{-1} = \frac{1}{g} \sum_{t \in G} \rho(s)\rho(t)p\rho(t)^{-1}\rho(s)^{-1} = \frac{1}{g} \sum_{t \in G} \rho(st)p\rho(st)^{-1} = p',$$

car l'application $t \mapsto st$ est une bijection de G sur lui-même.

Donc,

$$\rho(s)p' = p'\rho(s),$$

et par conséquent,

$$\rho(s)(\ker(p')) \subseteq \ker(p'),$$

ce qui montre que W' est stable par ρ .

Finalement,

$$V = W \oplus W',$$

avec W' stable par ρ , ce qui conclut la preuve.

2.4 Représentation irréductibles

Définition

Soit $f : G \rightarrow \text{GL}(V)$ une représentation linéaire d'un groupe G . On dit qu'elle est **irréductible** (ou **simple**) si :

1. V n'est pas l'espace nul ($V \neq 0$).
2. Les seuls sous-espaces vectoriels de V stables par G sont $\{0\}$ et V lui-même

. D'après le Théorème 1, cette condition équivaut à dire que V ne peut pas être décomposé en une somme directe non triviale de sous-représentations.

Remarques

- . Toute représentation de degré 1 est irréductible.
- . Tout groupe non commutatif possède au moins une représentation irréductible de degré ≥ 2 .

Théorème 2

Toute représentation linéaire V de G est isomorphe à une somme directe de représentations irréductibles.

Démonstration

Cela provient d'une récurrence immédiate sur la dimension, en utilisant le théorème de Maschke.

Notation

Soit U un $K[G]$ -module à gauche. On notera

$$U^G = \{x \in U \mid \forall s \in G, s \cdot x = x\}$$

l'espace des invariants par l'action de G sur U .

Exemples

1. On considère $G = \{e\}$ le groupe trivial avec élément neutre uniquement. La représentation de G est $\rho(e) = \text{Id}$ (opérateur identité sur $\mathbb{R}$)
 - . ρ est irréductible car il n'existe aucun sous-espace invariant non trivial ($\mathbb{R}^1$)
2. Soit le groupe $G = \langle r \rangle$ engendré par un élément r tel que $r^4 = e$. C'est donc un groupe cyclique d'ordre 4, isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

On définit une représentation linéaire :

$$\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{R})$$

par :

$$\rho(r)(x, y) = (-y, x)$$

ce qui correspond à une rotation de $\frac{\pi}{2}$ (ou 90 degrés) dans le sens trigonométrique.

La matrice associée est :

$$\rho(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Considérons un sous-espace propre $W \subset \mathbb{R}^2$, par exemple une droite vectorielle :

$$W = \{(x, ax) \mid x \in \mathbb{R}\}, \quad \text{où } a \in \mathbb{R}$$

Prenons un vecteur $(x, ax) \in W$, alors :

$$\rho(r)(x, ax) = (-ax, x)$$

Ce vecteur n'appartient pas à W en général, car il ne vérifie pas $y = ax$. Donc :

$$\rho(r)(W) \not\subset W$$

Ainsi, aucun sous-espace propre (autre que $\{0\}$ ou $\mathbb{R}^2$) n'est stable par ρ . Cela signifie que la représentation ρ est **irréductible**.

Théorème 3

Si G est commutatif Alors toutes les représentations irréductibles de G sont de degré 1

2.5 Produit tensoriel de deux représentations

Définition

Soient d'abord V_1 et V_2 deux espaces vectoriels. On appelle **produit tensoriel** de V_1 et V_2 un espace vectoriel W muni d'une application.

$$(x, x') \mapsto x \otimes x' \quad \text{de } V_1 \times V_2 \text{ dans } W,$$

cette application vérifie les deux conditions suivantes :

1. $x \otimes x'$ dépend linéairement de chacune des variables x et x' .
2. Si (e_i^1) est une base de V_1 et (e_j^2) est une base de V_2 , la famille des produits $e_i^1 \otimes e_j^2$ est une base de W .

Exemple

1. Soient :
 - . $V_1 = \mathbb{R}^2$ avec la base canonique (e_1, e_2)
 - . $V_2 = \mathbb{R}^2$ avec la base canonique (f_1, f_2)

Le produit tensoriel $V_1 \otimes V_2$ est un espace vectoriel de dimension $2 \times 2 = 4$ avec la base suivante :

$$(e_1 \otimes f_1, e_1 \otimes f_2, e_2 \otimes f_1, e_2 \otimes f_2)$$

Tout élément de $V_1 \otimes V_2$ s'écrit comme :

$$x = a_{11}(e_1 \otimes f_1) + a_{12}(e_1 \otimes f_2) + a_{21}(e_2 \otimes f_1) + a_{22}(e_2 \otimes f_2)$$

2. Soient $x = 2e_1 + 3e_2 \in V_1$ et $y = f_1 - f_2 \in V_2$. Alors leur produit tensoriel est donné par :

$$\begin{aligned} x \otimes y &= (2e_1 + 3e_2) \otimes (f_1 - f_2) \\ &= 2e_1 \otimes f_1 - 2e_1 \otimes f_2 + 3e_2 \otimes f_1 - 3e_2 \otimes f_2 \end{aligned}$$

3. On peut identifier $\mathbb{R}^2 \otimes \mathbb{R}^2$ avec l'espace des matrices $M_{2 \times 2}(\mathbb{R})$. Par exemple :

$$e_1 \otimes f_1 \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_2 \otimes f_2 \longleftrightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Ainsi, les éléments du produit tensoriel peuvent être vus comme des matrices.

2.5.1 Lemme de Schur

Soient deux représentations de G irréductibles, V et W , sur K . Alors :

- . Si elles ne sont pas isomorphes, $(\text{Hom}(V, W))^G = \{0\}$;
- . Si elles sont égales, $(\text{Hom}(V, V))^G$ est un corps, non nécessairement commutatif, qui est une extension de K . De plus, si K est algébriquement clos, alors $(\text{Hom}(V, V))^G = K \cdot \text{id}_V$.

Démonstration

- . Supposons que V et W ne soient pas isomorphes. Soit $f \in (\text{Hom}(V, W))^G$. f est un morphisme de représentations, donc $\text{Ker}(f)$ (resp. $\text{Im}(f)$) est une sous-représentation de V (resp. de W). Par irréductibilité de V et de W :

$$\text{Ker}(f) = \{0\} \text{ ou } V \quad \text{et} \quad \text{Im}(f) = \{0\} \text{ ou } W.$$

Mais V et W ne sont pas isomorphes, donc f ne peut pas être bijectif : soit $\text{Ker}(f) = \{0\}$ (défaut d'injectivité), soit $\text{Im}(f) = W$ (défaut de surjectivité). Nécessairement, $f = 0$.

- . Supposons à présent que $V = W$. On note $E_G(V) := (\text{Hom}(V, V))^G$. Pour montrer que $E_G(V)$ est un corps, il suffit de montrer que tous ses éléments non nuls sont inversibles, car $E_G(V)$ possède déjà une structure d'anneau.

Soit $f \in E_G(V)$, non nul. Par le même raisonnement qu'au point précédent, on montre que $\text{Ker}(f) = \{0\}$ et $\text{Im}(f) = V$. Ainsi f est bijectif, et son inverse est encore un point fixe de l'action de G sur V .

On pose :

$$\phi: K \rightarrow E_G(V), \quad k \mapsto k \cdot \text{id}_V.$$

ϕ est un morphisme de corps, ce qui fait bien de $E_G(V)$ une extension de K .

De plus, si K est algébriquement clos, toute extension finie est l'extension triviale, donc $E_G(V) = K \cdot \text{id}_V$.

2.6 Représentation régulière

Définition

La représentation régulière R de G est la représentation associée à l'action de G sur lui-même : on pose $V = \mathbb{C}^{|G|}$, muni d'une base $(e_s)_{s \in G}$ indexée par les éléments de G , et pour tout $s, t \in G$, on définit :

$$R_s(e_t) = e_{st}$$

En termes de $K[G]$ -modules, la représentation régulière consiste à voir $K[G]$ comme un module sur lui-même.

Exemples

1. Soit $G = \mathbb{Z}_3 = \{e, a, a^2\}$ avec $a^3 = e$, et l'espace $V = \mathbb{C}^3$ de base (e_e, e_a, e_{a^2}) . La représentation régulière R est donnée par :

$$R(e) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R(a) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad R(a^2) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

2. Soit $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$, et $V = \mathbb{C}^6$ de base $(e_\sigma)_{\sigma \in S_3}$. La représentation régulière R est définie par : pour tout $\tau \in G$,

$$R(\tau)(e_\sigma) = e_{\tau\sigma}$$

Les matrices $R(\tau)$ sont des matrices de permutation 6×6 , correspondant à l'action à gauche de S_3 sur elles-mêmes.

2.7 Représentations induites

Définition

Soit H un sous-groupe de G et S un système de représentants des classes de G/H . On dit qu'une représentation V de G est *induite* par une représentation W de H lorsque :

$$V = \bigoplus_{s \in S} s \cdot W$$

On note alors $V = \text{Ind}_H^G(W)$ ou simplement $V = W^G$ lorsqu'il n'y a pas de confusion possible.

Exemples

1. Soit $G = S_3$ et $H = \{e, (12)\}$, un sous-groupe d'ordre 2. Considérons W la représentation triviale de H , de dimension 1 : $h \cdot w = w$ pour tout $h \in H$.

Alors la représentation induite $V = \text{Ind}_H^G(W)$ est de dimension :

$$\dim V = [G : H] \cdot \dim W = 3 \cdot 1 = 3$$

L'espace V s'écrit :

$$V = \bigoplus_{s \in S} s \cdot W, \quad \text{où } S = \{e, (13), (23)\}$$

L'action de G sur V est définie en permutant les copies de W selon les représentants de G/H .

2. Soit $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ et $H = \{0, 2\} \cong \mathbb{Z}_2$.

Prenons W une représentation de H définie par :

$$W(0) = 1, \quad W(2) = -1$$

Alors la représentation induite $V = \text{Ind}_H^G(W)$ est de dimension :

$$\dim V = [G : H] \cdot \dim W = 2 \cdot 1 = 2$$

Les représentants des classes à gauche de G/H peuvent être $S = \{0, 1\}$. L'action de G est construite à partir de ces représentants sur les copies de W .

Chapitre 3

Caractère d'une représentation et applications

Dans ce chapitre, nous allons voir une généralisation de la notion de caractère d'un groupe abélien.

3.1 Caractère d'une représentation linéaire

Dans toute la suite, on prend $K = \mathbb{C}$

Définition

Soit $\rho : G \rightarrow \mathrm{GL}_n(V)$ une représentation. On appelle *caractère* de ρ l'application suivante :

$$\chi : G \rightarrow \mathbb{C}, \quad s \mapsto \mathrm{Tr}(\rho(s))$$

Remarque

Toute représentation de degré 1 coïncide avec son caractère : on parle de *caractère linéaire*.

Propriété

Soit χ le caractère d'une représentation de G . On a :

- (1) $\chi(1) = \dim(V)$
- (2) $\forall s \in G, \chi(s^{-1}) = \overline{\chi(s)}$
- (3) χ est une fonction de classe, c'est-à-dire constante sur chaque classe de conjugaison de G
- (4) $\forall s \in G, |\chi(s)| \leq \chi(1)$

Démonstration

- (1) $\rho(1) = \mathrm{id}_V$ donc $\mathrm{Tr}(\rho(1)) = \dim(V)$.
- (2) Les valeurs propres de $\rho(s)$ sont des racines de l'unité, donc $\rho(s^{-1}) = \rho(s)^{-1}$ a pour valeurs propres leurs conjuguées. La trace étant la somme des valeurs propres, on obtient le résultat.
- (3) Immédiat car $\mathrm{Tr}(\rho(tst^{-1})) = \mathrm{Tr}(\rho(t)\rho(s)\rho(t)^{-1}) = \mathrm{Tr}(\rho(s))$.
- (4) Par l'inégalité triangulaire, avec les valeurs propres de module 1.

Propriété

Soient $\rho_1 : G \rightarrow \text{GL}(V_1)$ et $\rho_2 : G \rightarrow \text{GL}(V_2)$ deux représentations de G , de caractères χ_1 et χ_2 respectivement. Alors :

- (1) Le caractère de $V_1 \oplus V_2$ vaut $\chi_1 + \chi_2$
- (2) Le caractère de $V_1 \otimes V_2$ vaut $\chi_1 \cdot \chi_2$

Démonstration

- (1) Dans une base adaptée :

$$\text{Tr}(\rho_1 \oplus \rho_2(s)) = \text{Tr}(\rho_1(s)) + \text{Tr}(\rho_2(s))$$

- (2) Les valeurs propres du produit tensoriel sont les produits :

$$\text{Tr}(\rho_1 \otimes \rho_2(s)) = \left(\sum_{i=1}^n \lambda_i \right) \left(\sum_{j=1}^m \mu_j \right) = \text{Tr}(\rho_1(s)) \cdot \text{Tr}(\rho_2(s))$$

Exemple

- 1. On considère $G = \{e, h\}$ tel que $h^2 = e$ et $V = \mathbb{C}^2$. Définissons :

$$\rho_e = \psi_e = I_2, \quad \rho_h = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}, \quad \psi_h = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Les caractères vérifient :

$$\chi_\rho(e) = \chi_\psi(e) = 2, \quad \chi_\rho(h) = 2, \quad \chi_\psi(h) = 0.$$

- 2. On considère $G = \{e, g, g^2\}$ un groupe cyclique d'ordre 3 tel que $g^3 = e$. Soit $V = \mathbb{C}^2$. On définit deux représentations linéaires ρ et ϕ de G dans $GL_2(\mathbb{C})$ par :

$$\begin{aligned} \rho(e) = \phi(e) &= I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \rho(g) &= \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad \rho(g^2) = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} \\ \phi(g) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \phi(g^2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

où $\omega = e^{2\pi i/3}$ est une racine cubique primitive de l'unité.

Les caractères associés sont :

$$\chi_\rho(e) = \text{tr}(\rho(e)) = 2, \quad \chi_\rho(g) = \omega + \omega^2 = -1, \quad \chi_\rho(g^2) = \omega^2 + \omega = -1$$

$$\chi_\phi(e) = \text{tr}(\phi(e)) = 2, \quad \chi_\phi(g) = \text{tr}(\phi(g)) = 0, \quad \chi_\phi(g^2) = \text{tr}(\phi(g^2)) = 0$$

Définition

Soit (V, ρ) une représentation de G , de caractère χ . On peut construire la **représentation duale** V^* par : $\forall s \in G, \quad \rho_s^* = {}^t \rho_{s^{-1}}$, où ${}^t \rho_{s^{-1}}$ est la transposée de la matrice de $\rho_{s^{-1}}$.

Propriété

Le caractère dual associé à V sera alors : $\chi^* = \overline{\chi}$.

Démonstration

En effet, pour $s \in G$, les valeurs propres de $\rho^*(s)$ sont les inverses des valeurs propres de $\rho(s)$. Comme ce sont des racines de l'unité, leur inverse est égal à leur conjugué, donc la somme des valeurs propres de $\rho^*(s)$ est le conjugué de la somme des valeurs propres de $\rho(s)$. Autrement dit :

$$\chi^*(s) = \overline{\chi(s)}$$

3.2 Orthonormalité des caractères irréductibles

Lemme

Soit $\rho : G \rightarrow \text{GL}(U)$ une représentation de caractère χ . Alors l'espace des vecteurs invariants $U^G := \{u \in U \mid \forall g \in G, \rho(g)u = u\}$ vérifie :

$$\dim(U^G) = \frac{1}{|G|} \sum_{s \in G} \chi(s).$$

Démonstration

Considérons l'endomorphisme :

$$f := \frac{1}{|G|} \sum_{s \in G} \rho(s).$$

C'est un projecteur sur U^G . En effet, on a $f \circ f = f$ (car ρ est une représentation), et l'image de f est précisément U^G , l'ensemble des vecteurs invariants.

Par conséquent :

$$\dim(U^G) = \text{Tr}(f) = \frac{1}{|G|} \sum_{s \in G} \text{Tr}(\rho(s)) = \frac{1}{|G|} \sum_{s \in G} \chi(s).$$

Propriété

Soit ρ_r la représentation régulière de G , et χ_r son caractère. Alors :

$$\chi_r(s) = \begin{cases} |G| & \text{si } s = 1 \\ 0 & \text{sinon} \end{cases}$$

Démonstration

Soit ρ_r la représentation régulière de G . Pour tout $s \in G$, notons $R_s = \rho_r(s)$ l'opérateur linéaire correspondant.

Soit $s \in G$. Pour tout $t \in G$, on a $R_s(e_t) = e_{st}$. Ainsi, dans la base $(e_s)_{s \in G}$, la matrice de R_s a des 1 exactement aux positions correspondant à l'action $t \mapsto st$.

On remarque que R_s a un 1 sur la diagonale (i.e. $st = t$) si et seulement si $s = 1$, car cela implique $st = t \Leftrightarrow s = 1$.

Donc la matrice R_s n'a que des zéros sur la diagonale sauf si $s = 1$, auquel cas R_1 est la matrice identité de taille $|G| \times |G|$.

Ainsi :

$$\chi(s) = \text{Tr}(R_s) = \begin{cases} |G| & \text{si } s = 1 \\ 0 & \text{sinon} \end{cases}$$

Propriété : Première relation d'orthogonalité

Soient V, W deux représentations irréductibles de G , de caractères respectifs χ_V et χ_W . Alors :

$$\frac{1}{|G|} \sum_{s \in G} \chi_V(s) \overline{\chi_W(s)} = \begin{cases} 1 & \text{si } V \simeq W \\ 0 & \text{sinon} \end{cases}$$

Remarque

Dans le cas d'un corps quelconque K , cette formule se réécrit :

$$\frac{1}{|G|} \sum_{s \in G} \chi_V(s) \chi_W(s) = \begin{cases} \dim_K(\text{Hom}_G(V, W)) & \text{si } V \simeq W \\ 0 & \text{sinon} \end{cases}$$

Et la démonstration est identique au cas complexe.

Démonstration

Appliquons le lemme à $U = \text{Hom}(V, W)$. Dans la première partie, on a vu que :

$$\text{Hom}_{\mathbb{C}}(V, W) \simeq \text{Hom}_{\mathbb{C}}(V, \mathbb{C}) \otimes W \simeq V^* \otimes W$$

donc :

$$U \simeq V^* \otimes W$$

et on peut écrire, grâce au lemme 1 :

$$\dim(U^G) = \dim((V^* \otimes W)^G) = \frac{1}{|G|} \sum_{s \in G} \chi_{V^* \otimes W}(s) = \frac{1}{|G|} \sum_{s \in G} \overline{\chi_V(s)} \chi_W(s)$$

Le lemme de Schur permet de conclure.

Exemple : vérification de la première relation d'orthogonalité

Soit $G = \mathbb{Z}_2 = \{e, a\}$ avec $a^2 = e$. Ce groupe admet deux représentations irréductibles de dimension 1 :

Représentation triviale ρ_1 :

$$\rho_1(e) = 1, \rho_1(a) = 1$$

Caractère associé : $\chi_1(e) = 1, \chi_1(a) = 1$

Représentation signe ρ_2 :

$$\rho_2(e) = 1, \rho_2(a) = -1$$

Caractère associé : $\chi_2(e) = 1, \chi_2(a) = -1$

Calculons le produit scalaire $\langle \chi_1, \chi_2 \rangle$:

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{s \in G} \chi_1(s) \overline{\chi_2(s)} = \frac{1}{2} (\chi_1(e) \cdot \overline{\chi_2(e)} + \chi_1(a) \cdot \overline{\chi_2(a)}) = \frac{1}{2} (1 \cdot 1 + 1 \cdot (-1)) = 0$$

Ce résultat confirme que $\rho_1 \not\simeq \rho_2$ (ils ne sont pas isomorphes).

Vérifions maintenant $\langle \chi_2, \chi_2 \rangle$:

$$\langle \chi_2, \chi_2 \rangle = \frac{1}{2} (1 \cdot 1 + (-1) \cdot (-1)) = \frac{1}{2} (1 + 1) = 1$$

Ce qui est conforme à la première relation d'orthogonalité des caractères irréductibles.

Propriété : Seconde relation d'orthogonalité

Soient $g, h \in G$. Alors :

$$\sum_{\chi \in \text{Irr}(G)} \chi(g) \overline{\chi(h)} = \begin{cases} 0 & \text{si } g \text{ et } h \text{ ne sont pas conjugués} \\ \frac{|G|}{|\text{Cl}(g)|} & \text{sinon} \end{cases}$$

Où

$$\text{Cl}(g) = \{h \in G, h = xgx^{-1}, x \in G\}$$

Démonstration

Soient $C_1, \dots, C_r$ les classes de conjugaison de G et $g_1, \dots, g_r$ des représentants de ces classes. On note X la matrice de coefficients $\chi_i(g_j)$ et D la matrice diagonale de coefficients $(\delta_{ij}|C_i|)_{ij}$. D'après la première relation d'orthogonalité, on a :

$$|G|I = XDX^t$$

Donc l'inverse à droite de X est :

$$\frac{1}{|G|}DX^t$$

C'est aussi son inverse à gauche, donc :

$$DX^tX = |G|I$$

En particulier, pour le coefficient (i, j) :

$$\sum_{k=1}^r |C_i| \chi_k(g_i) \chi_k(g_j) = |G| \delta_{ij}$$

Comme les caractères sont des fonctions de classe, le résultat s'ensuit.

Exemple : Seconde relation d'orthogonalité avec S_3

Considérons le groupe symétrique S_3 , qui contient 6 éléments :

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

Ce groupe admet trois classes de conjugaison :

$$\text{Cl}_1 = \{e\}$$

$$\text{Cl}_2 = \{(12), (13), (23)\}, \text{ de taille } 3$$

$$\text{Cl}_3 = \{(123), (132)\}, \text{ de taille } 2$$

Il possède trois représentations irréductibles de caractères χ_1, χ_2, χ_3 , avec la table suivante :

Élément de s_3	Classe	Taille	χ_1 (triviale)	χ_2 (signe)	χ_3 (dimension 2)
e	Cl_1	1	1	1	2
(12)	Cl_2	3	1	-1	0
(123)	Cl_3	2	1	1	-1

Vérification de la relation :

Cas 1 : $g = (12)$ et $h = (123)$ (non conjugués)

Alors, selon la propriété, on doit avoir :

$$\sum_{\chi \in \text{Irr}(S_3)} \chi(g) \overline{\chi(h)} = 0$$

Calcul :

$$\begin{aligned} \chi_1((12)) \cdot \overline{\chi_1((123))} + \chi_2((12)) \cdot \overline{\chi_2((123))} + \chi_3((12)) \cdot \overline{\chi_3((123))} = \\ 1 \cdot 1 + (-1) \cdot 1 + 0 \cdot (-1) = 1 - 1 + 0 = 0 \end{aligned}$$

Cas 2 : $g = h = (12)$ (même classe de conjugaison)

Alors, selon la propriété :

$$\sum_{\chi \in \text{Irr}(S_3)} |\chi((12))|^2 = \frac{|S_3|}{|\text{Cl}((12))|} = \frac{6}{3} = 2$$

Calcul :

$$|\chi_1((12))|^2 + |\chi_2((12))|^2 + |\chi_3((12))|^2 = |1|^2 + |-1|^2 + |0|^2 = 1 + 1 + 0 = 2$$

La seconde relation d'orthogonalité est bien vérifiée dans les deux cas.

Chapitre 4

Cryptosystème basé sur la représentation d'un groupe fini .

En cryptographie, les systèmes cryptographiques jouent un rôle fondamental dans la protection et la confidentialité des informations. On distingue généralement deux grandes catégories : la cryptographie symétrique et la cryptographie asymétrique. Dans un système symétrique, la même clé est utilisée pour chiffrer et déchiffrer les messages, ce qui nécessite un échange sécurisé de la clé entre les parties. En revanche, les systèmes asymétriques utilisent une paire de clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement, permettant ainsi une communication plus flexible et plus sécurisée. Avec l'évolution des concepts algébriques, notamment la théorie des groupes finis, de nouvelles approches cryptographiques ont émergé, s'appuyant sur les représentations linéaires des groupes pour concevoir des méthodes de chiffrement à la fois robustes et mathématiquement élégantes.

4.1 Un nouveau système de cryptographie à clé publique basé sur les représentations linéaires des groupes finis

Dans cette section, nous proposons un nouveau schéma de chiffrement basé sur la représentation linéaire de l'espace vectoriel associée au groupe G .

4.1.1 Schéma de chiffrement proposé

Soit V un espace vectoriel de dimension finie, muni d'une base $(b_i)_{1 \leq i \leq n}$, et soit $\rho : G \rightarrow GL(V)$ une représentation du groupe fini G dans l'espace V . Puisque ρ_s est un isomorphisme de V sur lui-même, son action sur V est entièrement déterminée par son action sur les vecteurs de base. Plus précisément, si un vecteur $u \in V$ s'écrit sous la forme $u = \sum_{i=1}^n c_i b_i$, alors l'image de u par ρ_s est donnée par :

$$\rho_s(u) = \sum_{i=1}^n c_i \rho_s(b_i)$$

Autrement dit, pour connaître complètement l'isomorphisme ρ_s , il suffit de connaître les images des vecteurs de base $\rho_s(b_i)$ pour $1 \leq i \leq n$.

Le schéma de chiffrement de base peut alors être décrit comme suit :

Clé publique : ρ_s , où $\rho_{s^\alpha} = \rho_s^\alpha$

Clé secrète : α

Étapes du chiffrement (Encryption)

1. Alice représente le message clair $m \in V$ comme une combinaison linéaire des vecteurs de base $(b_i)_{1 \leq i \leq n}$.
2. Alice choisit un élément arbitraire β et calcule $(\rho_s^\alpha)^\beta$, ce qui implique de déterminer $(\rho_s^\alpha)^\beta(b_i)$ pour chaque vecteur de base b_i .
3. Alice calcule ensuite le message chiffré $E = (\rho_s^\alpha)^\beta(m) = \rho_s^{\alpha\beta}(m)$.
4. Alice évalue ensuite l'application $\tau = \rho_s^\beta$, c'est-à-dire qu'elle calcule $\rho_s^\beta(b_i)$ pour chaque b_i .
5. Enfin, Alice envoie le couple (E, τ) au destinataire.

Déchiffrement

1. Bob représente E comme une combinaison linéaire des vecteurs de base $(b_i)_{1 \leq i \leq n}$.
2. Bob calcule $\tau^{-\alpha}$, ce qui implique de déterminer $\tau^{-\alpha}(b_i)$ pour chaque vecteur de base b_i .
3. Bob calcule ensuite $\tau^{-\alpha}(E)$.

Pour mettre en œuvre notre schéma, nous devons représenter ρ_s^α à l'aide d'une représentation binaire compacte. Étant donné que V est un espace vectoriel de type fini, ρ_s^α peut être exprimée en fonction de son action sur les vecteurs de base $\rho_s^\alpha(b_i)$. Toutefois, si nous ne disposons pas d'un algorithme efficace permettant d'exprimer tout vecteur $u \in V$ comme une combinaison linéaire des vecteurs de base $(b_i)_{1 \leq i \leq n}$, nous serons incapables de représenter efficacement ρ_s^α .

4.1.2 Sécurité et efficacité

La sécurité et l'efficacité du cryptosystème décrit dépendent de plusieurs facteurs.

Sécurité

Fondements de la sécurité

1. Le cryptosystème repose sur la difficulté de calculer la clé secrète α à partir des clés publiques ρ_s et ρ_s^α . Si α est suffisamment grand ou choisi de manière sécurisée, ce problème devient difficile à résoudre pour un attaquant, ce qui renforce la sécurité du système.
2. La sécurité dépend également de la difficulté à calculer $(\rho_s^\alpha)^\beta$ ou son inverse sans connaître α .

Hypothèses

1. Difficulté computationnelle : La sécurité cryptographique repose sur l'hypothèse que retrouver α à partir de ρ_s et ρ_s^α est infaisable d'un point de vue computationnel. Cela implique généralement des problèmes liés à l'exponentiation de matrices ou aux logarithmes discrets dans le contexte matriciel.

2. Problème d'inversion : Pour que Bob puisse retrouver le message clair m à partir du message chiffré E , il doit calculer $\tau^{-\alpha}(E)$. Si le calcul de τ ou de son inverse est computationnellement difficile, cela ajoute une couche supplémentaire de sécurité.

Vulnérabilités potentielles

1. Représentation matricielle : Comme ρ_s et ρ_s^α sont représentées par des matrices, la sécurité peut être affectée par le choix de la base ou par certaines propriétés spécifiques de ces matrices. En particulier, certaines formes matricielles peuvent faciliter le calcul de l'inverse ou la récupération de la clé si elles ne sont pas choisies avec soin.

2. Capacités de l'attaquant : Si un attaquant est capable de résoudre efficacement des problèmes d'algèbre linéaire, ou dispose d'algorithmes efficaces pour l'exponentiation matricielle, la sécurité pourrait être compromise. Le cryptosystème doit donc garantir que de tels problèmes soient réellement difficiles à résoudre en pratique.

Efficacité

Encodage et Décodage

1. Représentation : Un encodage et un décodage efficaces nécessitent des représentations compactes de la transformation ρ_s^α et de sa puissance $(\rho_s^\alpha)^\beta$. Si les vecteurs de base b_i et leurs images par ρ_s peuvent être représentés de manière compacte, le système devient plus efficace.

2. Combinaison linéaire : L'expression des vecteurs comme combinaisons linéaires des vecteurs de base b_i et l'application des transformations doivent être optimisées. Si un algorithme rapide pour exprimer les vecteurs dans cette base est disponible, cela améliore considérablement l'efficacité du système.

Complexité Computationnelle

1. Calcul des transformations : Le calcul de $(\rho_s^\alpha)^\beta$ et son application aux vecteurs doivent être optimisés afin d'éviter une surcharge computationnelle excessive. Des opérations matricielles efficaces sont essentielles pour une implémentation pratique.

2. Inversion et déchiffrement : Le calcul de $\tau^{-\alpha}(E)$ implique l'inversion de matrices et leur application. Des algorithmes performants pour ces opérations sont nécessaires afin de garantir un déchiffrement réalisable dans un temps raisonnable.

Scalabilité

1. Taille de l'espace vectoriel : L'efficacité du schéma peut être affectée par la taille de l'espace vectoriel V . Plus l'espace est grand, plus les ressources computationnelles nécessaires pour les opérations matricielles et la représentation de la base augmentent.

2. Taille de la base : Le choix de la taille de la base n a un impact à la fois sur la sécurité et sur l'efficacité. Des bases plus grandes renforcent la sécurité, mais demandent aussi plus de ressources pour le calcul et la représentation.

4.1.3 Exemple

Représentation régulière de S_3 et application à la cryptographie

Soit S_3 le groupe symétrique de l'ensemble $\{1, 2, 3\}$. On a :

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

Soit V un espace vectoriel de dimension $6 = |S_3|$, de base $(b_\sigma)_{\sigma \in S_3}$ indexée par les éléments de S_3 .

Pour $s \in S_3$, on définit une application linéaire $\rho(s) : V \rightarrow V$ envoyant $b_\sigma \mapsto b_{s\sigma}$. C'est la représentation régulière de S_3 .

Par exemple, pour $\rho_{(123)} : V \rightarrow V$, on a :

$$\begin{aligned}\rho_{(123)}(b_{(1)}) &= b_{(123)}, \\ \rho_{(123)}(b_{(12)}) &= b_{(13)}, \\ \rho_{(123)}(b_{(13)}) &= b_{(23)}, \\ \rho_{(123)}(b_{(23)}) &= b_{(12)}, \\ \rho_{(123)}(b_{(123)}) &= b_{(132)}, \\ \rho_{(123)}(b_{(132)}) &= b_{(1)}.\end{aligned}$$

La matrice associée $M_{(123)}$ est :

$$M_{(123)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

De même, pour $\rho_{(132)} : V \rightarrow V$, on a :

$$\begin{aligned}\rho_{(132)}(b_{(1)}) &= b_{(132)}, \\ \rho_{(132)}(b_{(12)}) &= b_{(23)}, \\ \rho_{(132)}(b_{(13)}) &= b_{(12)}, \\ \rho_{(132)}(b_{(23)}) &= b_{(13)}, \\ \rho_{(132)}(b_{(123)}) &= b_{(1)}, \\ \rho_{(132)}(b_{(132)}) &= b_{(123)}.\end{aligned}$$

La matrice associée $M_{(132)}$ est :

$$M_{(132)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Clé publique et clé secrète

Clé publique : $\rho_{(123)}$, $\rho_{(123)}^{2024} = \rho_{(123)}^{2024} = \rho_{(123)}^{3*674+2} = \rho_{(123)}^2 = \rho_{(132)}$.

Clé secrète : 2024.

Chiffrement

1. Alice représente le message en clair $m \in V$ comme une combinaison linéaire des vecteurs de base $(b_\sigma)_{\sigma \in S_3}$, par exemple

$$m = b_{(1)} + 2b_{(12)} + 3b_{(13)} + 4b_{(23)} + 5b_{(123)} + 6b_{(132)}.$$

2. Alice choisit un entier aléatoire $\beta = 2027$ et calcule $(\rho_{(132)})^{2027} \rho_{(132)}^{2027} = \rho_{(132)}^{675*3+2} = \rho_{(123)}$. Ce qui implique de déterminer $\rho_{(123)}(b_\sigma)$ pour chaque vecteur de base b_σ
3. Alice calcule ensuite le message chiffré $E = \rho_{(123)}(b_{(1)} + 2b_{(12)} + 3b_{(13)} + 4b_{(23)} + 5b_{(123)} + 6b_{(132)}) = 6b_{(1)} + 4b_{(12)} + 2b_{(13)} + 3b_{(23)} + b_{(123)} + 5b_{(132)}$
4. Alice calcule $\tau = \rho_{(123)}^{(2027)} = \rho_{(123)}^{(2027)} = \rho_{(132)}$, ce qui consiste à évaluer $\rho_{(132)}(b_\sigma)$ pour chaque vecteur de base b_σ .
5. Alice envoie la paire (E, τ)

Déchiffrement

1. Bob exprime E comme une combinaison linéaire de base $(b_\sigma)_{\sigma \in S_3}$:

$$E = 6b_{(1)} + 4b_{(12)} + 2b_{(13)} + 3b_{(23)} + b_{(123)} + 5b_{(132)}.$$

2. Bob calcule τ^{-2024} , ce qui consiste à déterminer $\tau^{-2024}(b_\sigma)$ pour chaque vecteur de base b_σ : $\tau^{-2024} = \rho_{(132)}^{-2024} = \rho_{(132)}^{2025-2024} = \rho_{(132)}$.
3. Bob calcule ensuite $\tau^{-2024}(E)$: $\tau^{-2024}(E) = \rho_{(132)}(E) = \rho_{(132)}(6b_{(1)} + 4b_{(12)} + 2b_{(13)} + 3b_{(23)} + b_{(123)} + 5b_{(132)}) = b_{(1)} + 2b_{(12)} + 3b_{(13)} + 4b_{(23)} + 5b_{(123)} + 6b_{(132)} = m$.

4.2 Nouveau système de cryptographie à clé publique basé sur le problème d'isomorphisme des représentations matricielles des groupes finis

Dans cette section, nous proposons un nouveau schéma de chiffrement basé sur le problème d'isomorphisme dans les représentations matricielles des groupes finis.

Soient ρ et τ deux représentations isomorphes du groupe G , où ρ agit sur l'espace vectoriel V et ρ' agit sur l'espace vectoriel W .

4.2.1 Schéma de chiffrement proposé

Considérons deux représentations isomorphes ρ et ρ' du même groupe G , agissant respectivement sur les espaces vectoriels V et W . Soit T une matrice inversible telle que la condition suivante soit satisfaite pour tout élément $g \in G$:

$$N_g = TM_gT^{-1}$$

où :

M_g est la matrice représentant l'élément g selon la représentation ρ .

N_g est la matrice représentant l'élément g selon la représentation ρ' .

T est la matrice représentant l'isomorphisme entre les espaces vectoriels V et W .

Le schéma de base se décrit comme suit :

Clé publique : la représentation ρ' et un élément $g \in G$, tel que N_g soient difficiles à inverser.

Clé secrète : la représentation ρ , où M_g est également difficile à inverser, mais où $M_{g^{-1}} = \rho(g^{-1})$ est facile à calculer, ainsi que la matrice T .

Chiffrement

1. Alice représente le message en clair $m \in W$.
2. Alice calcule ensuite le message chiffré $E = N_g m$.
3. Alice envoie le message chiffré E .

Déchiffrement

Bob calcule alors : $m = TM_g^{-1}T^{-1}(E)$.

Pour implémenter notre schéma, nous devons utiliser les équivalences suivantes :

$$N_g = TM_gT^{-1} \quad \text{si et seulement si} \quad N_g^{-1} = TM_g^{-1}T^{-1}$$

$$\text{ce qui équivaut à} \quad N_g^{-1} = TM_{g^{-1}}T^{-1}$$

4.2.2 Sécurité et efficacité

La sécurité et l'efficacité du système de cryptographie décrit dépendent de plusieurs facteurs.

Analyse de la sécurité

1. **Difficulté d'inversion** : La sécurité du schéma repose sur la difficulté d'inverser N_g . Si N_g est difficile à inverser, un attaquant ne peut pas facilement retrouver le message en clair m à partir du message chiffré E .

2. **Représentation matricielle et isomorphisme** : La relation $N_g = TM_gT^{-1}$ implique que N_g et M_g sont des matrices semblables, liées par la matrice d'isomorphisme T . Un attaquant devrait casser l'isomorphisme pour exploiter le schéma, ce qui rend l'inversion de N_g non triviale si T et M_g sont bien choisis.
3. **Clé publique et clé secrète** : Dans ce schéma, la clé publique fournit la représentation ρ' et la matrice N_g difficile à inverser, tandis que la clé secrète comprend $M_{g^{-1}} = \rho(g^{-1})$ (facile à calculer) ainsi que la matrice T . L'opération de chiffrement est simple, mais le déchiffrement dépend de la clé privée. La difficulté d'inverser N_g garantit que, même si un attaquant intercepte le message chiffré E , le déchiffrer sans connaître M_g et T reste un défi important.

Analyse de l'efficacité

1. **Efficacité du chiffrement** : Le processus de chiffrement consiste à multiplier le message en clair m par la matrice N_g . La multiplication matricielle est généralement efficace, mais sa complexité dépend de la taille de N_g et de m . Étant donné que N_g est une matrice, cette opération est réalisable avec les ressources informatiques actuelles, à condition que les dimensions soient raisonnables.
2. **Efficacité du déchiffrement** : Le déchiffrement nécessite de calculer $TM_g^{-1}T^{-1}$, puis d'appliquer cette matrice à E . L'efficacité du déchiffrement dépend des facteurs suivants :
 - (a) **Inversion de matrice** : Le calcul est supposé être facile puisque $M_{g^{-1}}$ fait partie de la clé secrète.
 - (b) **Multiplication matricielle** : La multiplication de $TM_g^{-1}T^{-1}$ avec E implique des opérations de multiplication matricielle, qui sont généralement efficaces si T , M_g^{-1} et E sont de taille raisonnable.

4.2.3 Considérations pratiques

1. **Taille des matrices** : La taille des matrices N_g , M_g et T affecte les performances du chiffrement et du déchiffrement. Les grandes matrices nécessitent davantage de ressources de calcul, donc le choix d'une taille appropriée est crucial pour garantir l'efficacité.
2. **Surcharge de calcul** : Bien que l'inversion de matrice soit supposée facile pour $M_{g^{-1}}$, elle ajoute une certaine charge au processus de déchiffrement. Des algorithmes efficaces pour l'inversion et la multiplication de matrices peuvent atténuer cette surcharge.
3. **Hypothèses de sécurité** : La sécurité du schéma repose sur la difficulté d'inverser les matrices dans la représentation de la clé publique, ainsi que sur le bon choix de T et $M_{g^{-1}}$. Si T ou $M_{g^{-1}}$ sont mal choisis, la sécurité du système peut être compromise.

4.2.4 Exemple

Soit C_n un groupe cyclique d'ordre n , engendré par un élément a , où $n \in \mathbb{N}$ et $n \geq 2$. Le groupe C_n est constitué des éléments $\{e, a, a^2, \dots, a^{n-1}\}$, avec $a^n = e$, où e est l'élément neutre.

Définissons la représentation $\rho : C_n \rightarrow GL(\mathbb{C}^2)$ par :

$$\rho(a^k) = \rho_{a^k} = \begin{pmatrix} e^{\frac{2\pi i k}{n}} & 0 \\ 0 & e^{-\frac{2\pi i k}{n}} \end{pmatrix} \quad \text{pour } 0 \leq k \leq n-1.$$

Définissons la représentation $\rho' : C_n \rightarrow GL(\mathbb{R}^2)$ par :

$$\rho'(a^k) = \rho'_{a^k} = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix} \quad \text{pour } 0 \leq k \leq n-1,$$

qui représente une rotation d'angle $\frac{2\pi k}{n}$.

Montrons que les représentations ρ et ρ' sont isomorphes.

Pour tout $0 \leq k \leq n-1$, on calcule $\chi(\rho_{a^k})$ et $\chi(\rho'_{a^k})$.

$$\chi(\rho_{a^k}) = \text{tr}(\rho_{a^k}) = e^{\frac{2\pi i k}{n}} + e^{-\frac{2\pi i k}{n}} = 2 \cos\left(\frac{2\pi k}{n}\right).$$

$$\chi(\rho'_{a^k}) = \text{tr}(\rho'_{a^k}) = \cos\left(\frac{2\pi k}{n}\right) + \cos\left(\frac{2\pi k}{n}\right) = 2 \cos\left(\frac{2\pi k}{n}\right).$$

Ainsi, ρ et ρ' ont la même trace pour tout a^k , ce qui suggère qu'elles sont isomorphes.

Considérons maintenant la matrice :

$$T = \begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix} \quad \text{et son inverse} \quad T^{-1} = \frac{1}{2i} \begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix}.$$

Pour tout $0 \leq k \leq n-1$, on vérifie :

$$T \cdot \rho_{a^k} \cdot T^{-1} = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} e^{\frac{2\pi i k}{n}} & 0 \\ 0 & e^{-\frac{2\pi i k}{n}} \end{pmatrix} \cdot \left(\frac{1}{2i} \begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix} \right) = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix} = \rho'_{a^k}.$$

Clé publique : la représentation $\rho' : C_n \rightarrow GL(\mathbb{R}^2)$ définie par :

$$\rho'(a^k) = \rho'_{a^k} = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix} \quad \text{pour } 0 \leq k \leq n-1, \quad \text{avec } a^3 \in C_n.$$

Clé secrète : la représentation $\rho : C_n \rightarrow GL(\mathbb{C}^2)$ donnée par :

$$\rho(a^k) = \rho_{a^k} = \begin{pmatrix} e^{\frac{2\pi i k}{n}} & 0 \\ 0 & e^{-\frac{2\pi i k}{n}} \end{pmatrix} \quad \text{pour } 0 \leq k \leq n-1,$$

et la matrice $T = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}.$

Chiffrement

1. Alice représente le message clair $m \in \mathbb{C}^2$, par exemple :

$$m = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

2. Alice calcule ensuite le message chiffré $E = N_{a^3} \cdot m$, où :

$$N_{a^3} = \begin{pmatrix} \cos\left(\frac{6\pi}{n}\right) & -\sin\left(\frac{6\pi}{n}\right) \\ \sin\left(\frac{6\pi}{n}\right) & \cos\left(\frac{6\pi}{n}\right) \end{pmatrix}, \quad m = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$\Rightarrow E = N_{a^3} \cdot m = \begin{pmatrix} \cos\left(\frac{6\pi}{n}\right) - 2\sin\left(\frac{6\pi}{n}\right) \\ \sin\left(\frac{6\pi}{n}\right) + 2\cos\left(\frac{6\pi}{n}\right) \end{pmatrix}$$

3. Alice envoie le message chiffré :

$$E = \begin{pmatrix} \cos\left(\frac{6\pi}{n}\right) - 2\sin\left(\frac{6\pi}{n}\right) \\ \sin\left(\frac{6\pi}{n}\right) + 2\cos\left(\frac{6\pi}{n}\right) \end{pmatrix}$$

Déchiffrement

Bob calcule :

$$m = T \cdot M_{a^3}^{-1} \cdot T^{-1}(E) = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} e^{-\frac{6\pi i}{n}} & 0 \\ 0 & e^{\frac{6\pi i}{n}} \end{pmatrix} \cdot \left(\frac{1}{2i} \begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix} \right) \cdot E = \begin{pmatrix} 1 \\ 2 \end{pmatrix} = m$$

Ainsi, Bob retrouve le message original m .

Bibliographie

- [1] Jean-Bernard Zuber, *Introduction à la Théorie des Groupes et leurs Représentations*, 2006.
- [2] Odile Lecacheux, *LM325 - Introduction à la Théorie des Groupes*, 12 novembre 2008.
- [3] Robert Cabane, Christian Leboeuf, *Algèbre Linéaire : Espaces Vectoriels et Polynômes*, 2005.
- [4] Cédric Lecouvey, *Introduction à la Théorie des Représentations des Groupes*, 2004.
- [5] Jean-Pierre Serre, *Représentations linéaires des Groupes Finis*, Hermann Éditeurs des Sciences et des Arts, Paris, janvier 1998.
- [6] Perrine Jouteur, *Représentations Linéaires des Groupes Finis – Application au Théorème de Burnside*, Rapport de stage, mai-juin 2020.
- [7] Daniel Barsky , Ghislain Dartois, *Cours , Cryptographie Paris 13 (version 2010/2011), 1 octobre 2010*
- [8] C. Meshram and X. Li, *New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group , Journal of Information and Optimization Sciences, Vol, 39, No.2, pp. 391-400, (2018).*
- [9] W. Stallings, *"Cryptography and Network Security : Principles and Practice," Pearson, (latest edition 2024).*
- [10] C. Paar, J. Pelzl, *"Understanding Cryptography", Springer, (2010).*
- [11] J. H. Hoarestein, J. Piper, J. H. Silverman, *An Introduction to Mathematical Cryptography, Springer, (2014).*
- [12] J. Katz, Y. Lindell, *"Introduction to Modern Cryptography : Principles and Protocols," MIT Press, (2007).*
- [13] N. Koblitz, *"A Course in Number Theory and Cryptography," Springer, (latest edition 1994).*
- [14] R. McEliece, *"Algebraic Methods in Cryptography," Springer, (1998).*
- [15] W. Diffie, M. E. Hellman , *"New Direction in Cryptography," IEEE Trans, on Inform Theory, 22(6), P. 644-665, (1976).*
- [16] W. Mao , *"Modern Cryptography : Theory and Practice," Prentice Hall, (2003).*

ملخص

يهدف هذا البحث إلى دراسة نظرية التمثيلات الخطية للزمر المنتهية واستكشاف تطبيقاتها في مجال التشفير. ويركز على استثمار الخصائص الجبرية لهذه التمثيلات في تصميم أنظمة تشفير أكثر قوة وكفاءة.

يتناول العمل المفاهيم الأساسية لتمثيل الزمر، ونظرية المحارف، والعلاقات البنيوية التي تربط بينها، مع تسليط الضوء على كيفية توظيف هذه الأدوات الرياضية المتقدمة في تحسين البروتوكولات التشفيرية الحالية وتطوير آليات جديدة، بما يساهم في تعزيز أمن المعلومات وفتح آفاق جديدة في هذا المجال الحيوي.

كلمات مفتاحية

الزمر المنتهية، التمثيلات الخطية، نظرية المحارف، التشفير الجبري، نظرية التمثيل، أنظمة التشفير.

Abstract

The objective of this work is to investigate the theory of linear representations of finite groups and their applications in cryptography. We particularly focus on utilizing the algebraic properties of these representations to design robust encryption systems.

This research thoroughly examines the fundamental concepts of group representations, character theory, and their structural relationships. It demonstrates how these sophisticated mathematical tools can be employed to enhance existing cryptographic protocols and develop new ones, thereby offering promising prospects for information security.

Key words

Finite groups , linear representations , character theory , algebraic cryptography , representation theory , encryption systems.

Résumé

L'objectif de ce travail est d'étudier la théorie des représentations linéaires des groupes finis et ses applications en cryptographie. Nous nous intéressons particulièrement à l'exploitation des propriétés algébriques de ces représentations pour concevoir de nouveaux systèmes de chiffrement robustes.

Cette recherche examine en détail les concepts fondamentaux des représentations de groupes, de la théorie des caractères et de leurs relations structurelles. Elle démontre comment ces outils mathématiques sophistiqués peuvent être mobilisés pour améliorer les protocoles cryptographiques existants et en développer de nouveaux, offrant ainsi des perspectives intéressantes pour la sécurité informatique.

Mot-clés

Groupes finis , représentations linéaires , théorie des caractères , cryptographie algébrique , théorie des représentations , systèmes de chiffrement .