Représentation linéaire, caractère et représentations linéaires irréductibles d'un groupe infini.

DEPARTEMENT DE MATHÉMATIQUES - INFORMATIQUE
Mémoire présenté par : SOUNKOUA Roger
Sous la direction du
Dr. Gilbert MANTIKA
(Chargée de Cours, UMa, FS)
Pr. Dieukam
(Maître de Conférences, UMa, FS)

29 mai 2025

Sommaire

Introduction

Les représentations linéaires d'un groupe G sur un espace vectoriel V sont des homomorphismes $\varphi : G \to \mathrm{GL}(V)$.

Un groupe infini est un groupe qui possède une infinité d'éléments.

L'objectif est d'étudier les représentations linéaires des groupes infinis et leurs applications dans des domaines comme la physique théorique, la géométrie et la cryptographie.

Les représentations linéaires d'un groupe G sur un espace vectoriel V sont des homomorphismes $\varphi : G \to \mathrm{GL}(V)$.

Un groupe infini est un groupe qui possède une infinité d'éléments.

L'objectif est d'étudier les représentations linéaires des groupes infinis et leurs applications dans des domaines comme la physique théorique, la géométrie et la cryptographie.

Les représentations linéaires d'un groupe G sur un espace vectoriel V sont des homomorphismes $\varphi : G \to \mathrm{GL}(V)$.

Un groupe infini est un groupe qui possède une infinité d'éléments.

L'objectif est d'étudier les représentations linéaires des groupes infinis et leurs applications dans des domaines comme la physique théorique, la géométrie et la cryptographie.

Définition d'un Groupe

Definition

Un groupe est un couple $(G, *)$ où G est un ensemble non vide et $*$ est une loi de composition interne

$$* : G \times G \longrightarrow G$$

$$(x, y) \longmapsto x * y$$

vérifiant :

i) $*$ est associative, c'est-à-dire, $\forall x, y, z \in G,\ (x * y) * z = x * (y * z)$;

ii) G possède un élément neutre pour la loi $*$, c'est-à-dire, $\exists e \in G$ tel que $\forall x \in G,\ x * e = e * x = x$;

iii) Tout élément de G est inversible (ou possède un élément symétrique) dans G, c'est-à-dire, $\forall x \in G,\ \exists y \in G$ tel que $x * y = y * x = e$.

Definition

Si $(G, *)$ est un groupe tel que la loi $*$ satisfasse à la propriété

$$\forall x, y \in G,\ x * y = y * x,$$

le groupe $(G, *)$ est dit **commutatif** ou encore **abélien**.

Definition

Soit $(G_i, \circ_i)$ une famille de groupes finis indexée par l'ensemble $\{1, 2, \ldots, n\}$, où $n \in \mathbb{N}^*$. Le *produit direct fini* de cette famille est un groupe $\left(\prod_{i=1}^{n} G_i, \circ\right)$, défini par les propriétés suivantes :

i) L'ensemble sous-jacent est constitué des familles indexées par $\{1, 2, \ldots, n\}$:

$$\prod_{i=1}^{n} G_i = \{(g_i)_{i=1}^{n} \mid g_i \in G_i \text{ pour tout } i \in \{1, 2, \ldots, n\}\}.$$

ii) La loi de composition $\circ$ est définie composante par composante :

$$(g_i)_{i=1}^{n} \circ (g_i')_{i=1}^{n} = (g_i \circ_i g_i')_{i=1}^{n},$$

où $\circ_i$ désigne l'opération du groupe G_i pour chaque $i \in \{1, 2, \ldots, n\}$.

iii) L'élément neutre de $\prod_{i=1}^{n} G_i$ est la famille $(e_i)_{i=1}^{n}$, où e_i est l'élément neutre de G_i pour tout $i \in \{1, 2, \ldots, n\}$.

iv) L'inverse d'une famille $(g_i)_{i=1}^{n} \in \prod_{i=1}^{n} G_i$ est donné par :

$$(g_i)_{i=1}^{n}{}^{-1} = (g_i^{-1})_{i=1}^{n},$$

où g_i^{-1} est l'inverse de g_i dans G_i pour chaque $i \in \{1, 2, \ldots, n\}$.

Theorem

Si G est un groupe cyclique d'ordre $n \geq 1$, alors G est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Theorem

Tout groupe fini d'ordre premier est cyclique.

Definition

[**?**] Soient $(G, \cdot)$ et $(G', *)$ deux groupes. Un homomorphisme de groupes de G dans G' est une application $f : G \to G'$ vérifiant :

$$\forall (x, y) \in G \times G, \quad f(x \cdot y) = f(x) * f(y).$$

Definition

Une catégorie $\mathcal{C}$ consiste en les données suivantes :

i) Une classe $|\mathcal{C}|$, dont les éléments sont appelés objets de $\mathcal{C}$;

ii) À chaque couple d'objets (X, Y) de $\mathcal{C}$, est associé un ensemble $\mathcal{C}(X, Y)$ (ou $\mathrm{Hom}_{\mathcal{C}}(X, Y)$), dont les éléments sont appelés morphismes (ou flèches) de X dans Y ;

iii) À chaque triplet (X, Y, Z) d'objets de $\mathcal{C}$, une application (appelée application de composition)

$$\mathcal{C}(X, Y) \times \mathcal{C}(Y, Z) \to \mathcal{C}(X, Z), \quad (f, g) \mapsto g \circ f;$$

iv) À chaque objet $X \in \mathcal{C}$, est associé un élément $1_X \in \mathcal{C}(X, X)$ appelé morphisme d'identité de X.

Ces données vérifient les axiomes suivants :

Associativité de la composition : si $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$ sont des morphismes dans $\mathcal{C}$, alors on a

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Neutralité de l'identité : pour tous $X, Y \in |\mathcal{C}|$, et pour tout $f \in \mathcal{C}(X, Y)$, on a $f \circ 1_X = f \quad \text{et} \quad 1_Y \circ f = f$.

Définition d'un foncteur contravariant

Definition

Un *foncteur contravariant* est une loi de passage d'une catégorie $\mathcal{C}$ à une catégorie $\mathcal{D}$, $F : \mathcal{C} \to \mathcal{D}$, qui satisfait les propriétés suivantes :

i) À tout objet C de $\mathcal{C}$ associe un objet $F(C)$ de $\mathcal{D}$,

ii) À tout morphisme $X \xrightarrow{f} Y$ de $\mathcal{C}$ associe un morphisme $F(Y) \xrightarrow{F(f)} F(X)$ de $\mathcal{D}$, et les conditions suivantes doivent être vérifiées :

$F(1_X) = 1_{F(X)}$ pour tout objet X,

$F(g \circ f) = F(f) \circ F(g)$ pour tous morphismes $X \xrightarrow{f} Y \xrightarrow{g} Z$.

Définitions

Definition

Une propriété universelle (PU) est un énoncé sur les objets mathématiques qui stipule que sous certaines conditions, il existe un unique morphisme qui satisfait certaines propriétés.

Definition

Un ensemble partiellement ordonné est un couple $(I, \leq)$ où I est un ensemble non vide et $\leq$ est une relation binaire sur I vérifiant les propriétés suivantes pour tous $a, b, c \in I$:

i) **Réflexivité** : $a \leq a$;

ii) **Anti-symétrie** : si $a \leq b$ et $b \leq a$, alors $a = b$;

iii) **Transitivité** : si $a \leq b$ et $b \leq c$, alors $a \leq c$.

Definition

Un ensemble $(I, \leq)$ est dit ordonné filtrant si $(I, \leq)$ est un ensemble partiellement ordonné et si pour tous $i, j \in I$, il existe $k \in I$ vérifiant $i \leq k$ et $j \leq k$.

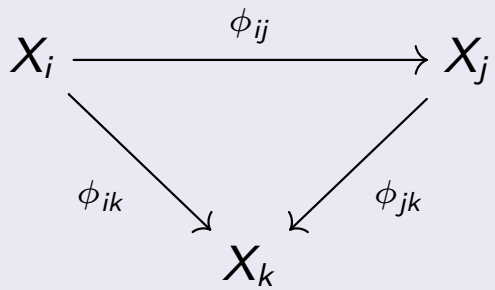
Definition

[?] Soit $(I, \leq)$ un ensemble ordonné filtrant. Un système inductif de groupes sur I est la donnée d'un couple $(X_i, \phi_{ij})_{i,j \in I}$ où X_i sont les groupes et les $\phi_{ij} : X_i \to X_j$ (pour $i \leq j$) sont des homomorphismes de groupes, vérifiant :

i) Pour tout $i \in I$, $\phi_{ii} = \mathrm{Id}_{X_i}$;

ii) Pour tous $(i, j, k) \in I^3$, $i \leq j \leq k \Rightarrow \phi_{jk} \circ \phi_{ij} = \phi_{ik}$.

Ce qui se traduit par le diagramme commutatif suivant :



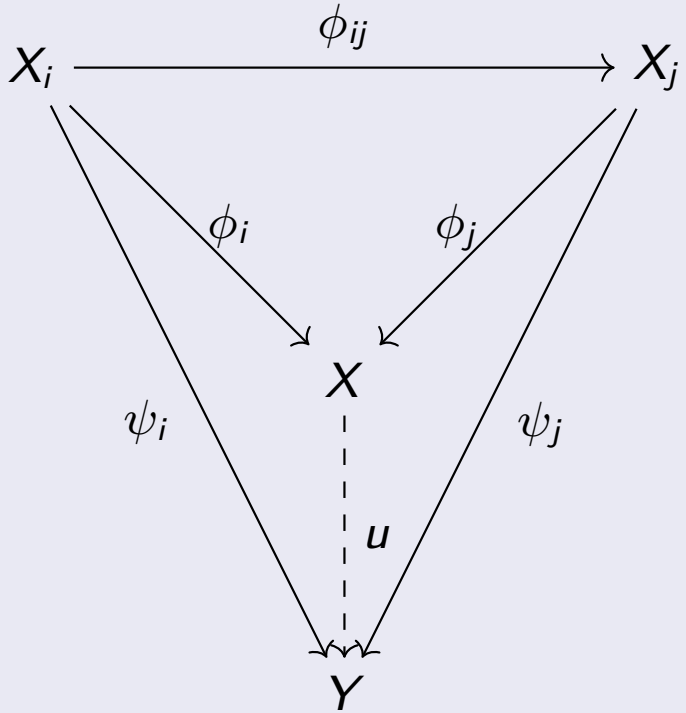
Definition

[?] Soit X un groupe et (X_i, ϕ_{ij}) un système inductif de groupes. La famille $(X, \phi_i : X_i \to X)$ est dite compatible avec (X_i, ϕ_{ij}) si pour tous $i, j \in I$ tels que $i \leq j$, on a $\phi_i = \phi_j \circ \phi_{ij}$. Ce qui est illustré par le diagramme commutatif suivant :

Definition

[?] Soit (X_i, ϕ_{ij}) un système inductif de groupes. La limite inductive ou limite directe, lorsqu'elle existe, est une famille compatible $(X, \phi_i : X_i \to X)$ avec (X_i, ϕ_{ij}) vérifiant la propriété universelle (PU) suivante :

> *Pour toute autre famille $(X, \psi_i)_{i \in I}$ compatible avec (X_i, ϕ_{ij}), il existe un unique homomorphisme de groupes $u : X \to Y$ tel que le diagramme suivant soit commutatif pour tous $i \leq j$:*



Notation

La limite inductive $(X, \phi_i)_{i\in I}$ *d'un système inductif* $(X_i, \phi_{ij})_{j\in I}$ *est notée* $X = \varinjlim X_i$.

Soit $(I, \leq)$ un ensemble ordonné filtrant.

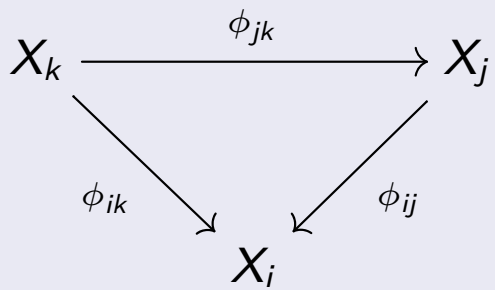
Definition (Système projectif de groupes)

[?] Un système projectif de groupes sur $(I, \leq)$ est un couple $(X_i, \phi_{ij})_{i,j\in I}$ où les X_i sont les groupes et les $\phi_{ij} : X_j \to X_i$ $(i \leq j)$ sont les homomorphismes de groupes vérifiant :

i) $\phi_{ii} = \mathrm{Id}_{X_i}$ pour tout $i \in I$;

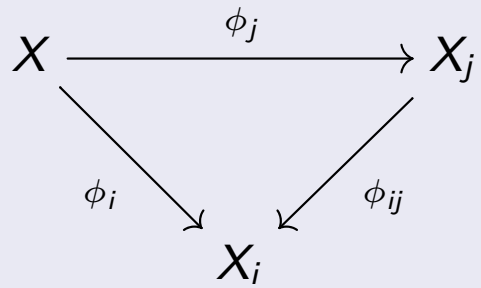
ii) pour tout $(i, j, k) \in I^3$ tels que $i \leq j \leq k$, on a $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$.

Autrement dit, le diagramme suivant est commutatif :



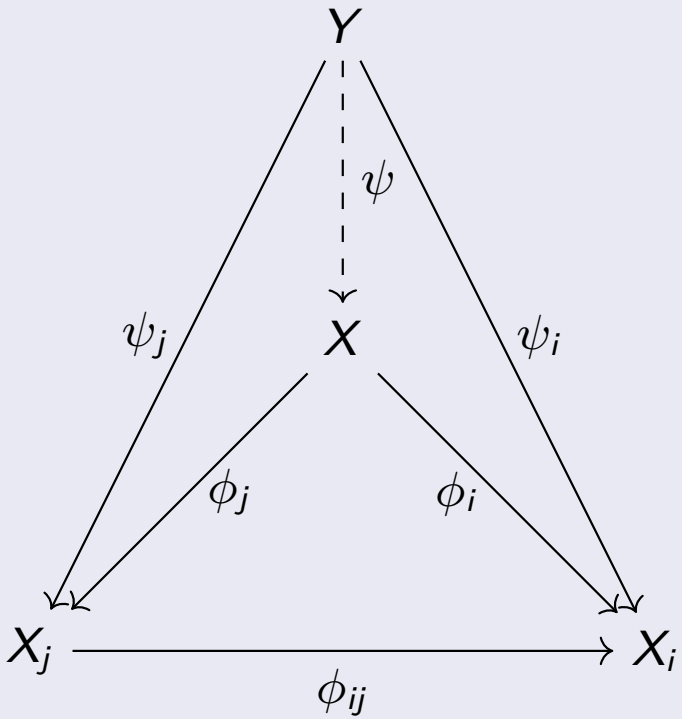
Definition (Famille compatible avec le système projectif)

[?] Soient X un groupe et $(X_i, \phi_{ij})_{i,j\in I}$ un système projectif de groupes. La famille de homomorphismes $(\phi_i : X \to X_i)_{i\in I}$, qu'on note (X, ϕ_i), est dite compatible avec le système projectif $(X_i, \phi_{ij})_{i,j\in I}$ si pour tous $i, j \in I$ tels que $i \leq j$, on a : $\phi_{ij} \circ \phi_j = \phi_i$. Ce qui se traduit par le diagramme commutatif suivant :



Definition (Limite projective)

[?] Soit $(X_i, \phi_{ij})_{i,j\in I}$ un système projectif de groupes. La limite projective ou limite inverse du système projectif $(X_i, \phi_{ij})_{i,j\in I}$ est une famille $(X, (\phi_i)_{i\in I})$ de homomorphismes compatibles avec $(X_i, \phi_{ij})_{i,j\in I}$, vérifiant la propriété universelle suivante :
Si $(\psi_i : Y \to X_i)_{i\in I}$ $(Y \in |\mathcal{C}|)$ est une famille de morphismes compatibles, alors il existe un unique morphisme $\psi : Y \to X$ tel que le diagramme suivant commute pour tous $i \leq j$:



$$\psi_i = \phi_i \circ \psi$$

$$\psi_j = \phi_j \circ \psi$$

Proposition sur le Complété Profini

Proposition (Unicité de la limite projective)

Si une limite projective d'un système projectif existe, elle est unique à isomorphisme près.

Notation

Une telle limite est notée $\varprojlim_I X_i$ *ou* $\varprojlim_{i \in I} X_i$.

Definition (Groupe profini)

La limite projective d'un système projectif de groupes finis est appelée groupe profini.

Proposition

Le complété profini d'un groupe est unique à isomorphisme près, c'est-à-dire si $(\widehat{G}_1, j_1)$ *et* $(\widehat{G}_2, j_2)$ *sont deux complétés de* G*, alors il existe un isomorphisme* $\widehat{\alpha} : \widehat{G}_1 \to \widehat{G}_2$ *tel que* $\widehat{\alpha} j_1 = j_2$.

Propriété

Lorsque G est doté de la topologie profinie, alors on a un homomorphisme continu $j : G \to \widehat{G}$ vérifiant la propriété universelle suivante : pour tout $\theta : G \to H$ un homomorphisme continu dans un groupe discret H, il existe un unique homomorphisme continu $\widehat{\theta} : \widehat{G} \to H$ tel que $\theta = \widehat{\theta} j$. On dit que le couple $(\widehat{G}, j)$ est le complété profini de G.

Proposition

Soit $(\widehat{G}, j)$ le complété profini de G. Alors :

(a) $j(G)$ est dense dans $\widehat{G}$.

(b) $\ker j = \bigcap_{K \in \mathcal{N}} K$.

Definition

On dit que les groupes G_1 et G_2 sont *profiniment équivalents* si leurs complétions profinies sont isomorphes, c'est-à-dire si $\widehat{G_1} \cong \widehat{G_2}$.

Theorem

Des groupes de type fini avec la même collection de quotients finis ont des complétions profinies isomorphes, autrement dit sont profiniment équivalents.

Definition

[?] Soit $\mathbb{K}$ un corps. Une *représentation* $\mathbb{K}$*-linéaire* d'un groupe fini G est un homomorphisme de groupes

$$\rho : G \to \mathrm{GL}(V)$$

où V est un $\mathbb{K}$-espace vectoriel et $\mathrm{GL}(V)$ est le groupe des applications linéaires bijectives de V sur lui-même.

Remarque

[?] Si V est un $\mathbb{K}$-espace vectoriel de dimension finie n, on dit que n est le degré de la représentation. De plus, en choisissant une base de V, le groupe $\mathrm{GL}(V)$ est isomorphe au groupe

$$\mathrm{GL}(n, \mathbb{K}) = \{A \in \mathrm{M}(n, \mathbb{K}) \mid \det(A) \neq 0\},$$

où $\mathrm{GL}(n, \mathbb{K})$ est le groupe des matrices inversibles de taille $n \times n$ équipées de la multiplication des matrices à coefficients dans $\mathbb{K}$, et $\det(A)$ désigne le déterminant de la matrice A.

Représentations linéaires et sous-représentations

Definition

[?] Soient $(V, \rho)_G$ et $(W, \psi)_G$ deux représentations linéaires. Un opérateur d'entrelacement, ou morphisme de représentations, est une application linéaire $\alpha : V \to W$ telle que

$$\alpha \circ \rho(g) = \psi(g) \circ \alpha, \quad \forall g \in G.$$

On dit que α est équivariante. Lorsque $\alpha : V \to W$ est un isomorphisme, on dit que les représentations $(V, \varphi)_G$ et $(W, \psi)_G$ sont isomorphes.

Definition

[?] Soit W un sous-espace vectoriel de V et G un groupe. On dit que W est stable (ou invariant) sous l'action de G, ou encore G-stable, si pour tout $g \in G$ et tout $w \in W$, on a $\rho_g(w) \in W$.

Definition

[?] Une sous-représentation de $(V, \rho)_G$ est la restriction $\rho_W : G \to \mathrm{GL}(W)$ où W est stable sous G. Elle est définie par

$$\rho_W(g) = \rho(g)|_W, \quad \forall g \in G.$$

Proposition

[?] Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire sur G telle que W soit un sous-espace vectoriel de V stable sous l'action de G. Alors, l'application restreinte $\rho_W : G \to \mathrm{GL}(W)$ définie par $\rho_W(g) = \rho(g)|_W$ pour tout $g \in G$ est un homomorphisme de groupes.

Lemma

[?] Soient $\varphi : G \to \mathrm{GL}(V_1)$ et $\psi : G \to \mathrm{GL}(V_2)$ deux représentations linéaires de G. Soit $f : V_1 \to V_2$ un morphisme de représentations linéaires. Alors :

i) $\rho_{\ker(f)} : G \to \mathrm{GL}(\ker(f))$ *est une sous-représentation linéaire de* $\varphi : G \to \mathrm{GL}(V_1)$;

ii) L'image $\mathrm{im}(f)$, $\rho_{\mathrm{im}(f)} : G \to \mathrm{GL}(\mathrm{im}(f))$, *est une sous-représentation linéaire de* $\psi : G \to \mathrm{GL}(V_2)$;

iii) $V_1/\ker(f) \cong \mathrm{im}(f)$ *au sens de représentations linéaires de* G.

Definition

[?] Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire sur G. Le caractère de V, noté χ_V, est la fonction

$$\chi_V : G \to \mathbb{C}$$

définie pour tout $g \in G$ par

$$\chi_V(g) := \mathrm{Tr}(\rho(g)),$$

où Tr désigne la trace.

Theorem

Soit $(\rho, V)_G$ une représentation linéaire. On peut munir V d'un produit hermitien $(.,.)_V$ qui rend la représentation linéaire $(\rho, V)_G$ unitaire.

Proposition

Soient $\rho_V : G \to \mathrm{GL}(V)$ *et* $\rho_W : G \to \mathrm{GL}(W)$ *deux représentations linéaires sur* G *de degrés* n *et* m ($n, m \in \mathbb{N}^*$), *et de caractères* χ_V *et* χ_W *respectivement. On a :*

i) $\chi_V(1) = \dim V$;

ii) $\chi_{V \oplus W} = \chi_V + \chi_W$;

iii) $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ *pour* $\forall g \in G$.

Theorem (Frobenius)

Pour tout groupe fini G, *le nombre de représentations irréductibles non-isomorphes deux à deux de* G *est exactement égal au nombre* $c(G)$ *de classes de conjugaison de* G.

Proposition

Deux représentations d'un groupe G *sont isomorphes si et seulement si elles ont le même caractère.*

Definition

On dit qu'une représentation linéaire $\rho : G \to \mathrm{GL}(V)$ est *irréductible* si l'espace vectoriel V n'est pas réduit à $\{0\}$ et si V ne possède aucun sous-espace invariant par ρ autre que $\{0\}$ et V.

Theorem

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G dans V et soit W un sous-espace vectoriel de V stable sous G. Alors, il existe un complément W^0 de W dans V qui est stable sous G.

Theorem (Théorème de Maschke)

Toute représentation linéaire $\rho : G \to \mathrm{GL}(V)$ sur G dans un espace vectoriel complexe de dimension finie se décompose en somme directe de représentations irréductibles.

Theorem (Lemme de Schur)

Soient $\rho_1 : G \to V_1$ et $\rho_2 : G \to V_2$ deux représentations irréductibles de G.
Soit $f : V_1 \to V_2$ une application linéaire vérifiant

$$\forall g \in G, \quad f \circ \rho_1(g) = \rho_2(g) \circ f.$$

On a les propriétés suivantes :

(i) Si ρ_1 et ρ_2 ne sont pas isomorphes, alors $f = 0$.

(ii) Si $V_1 = V_2$ et $\rho_1 = \rho_2$, alors f est une homothétie.

Corollary

Soit $h : V \to W$ une application linéaire. Posons :

$$h_0 = \frac{1}{N} \sum_{g \in G} (\rho_W(g))^{-1} \circ h \circ \rho_V(g),$$

où $N = \mathrm{Card}(G)$. Alors :

i) Si ρ_V et ρ_W ne sont pas isomorphes, on a $h_0 = 0$.

ii) Si $V = W$ et $\rho_V = \rho_W$, alors h_0 est une homothétie de rapport $\frac{1}{n} Tr(h)$, où $n = \dim(V)$.

Remarque

Une traduction matricielle du corollaire précédent est : si φ et ψ sont des fonctions $G \to \mathbb{C}$, alors

$$\langle \varphi, \psi \rangle = \frac{1}{g} \sum_{t \in G} \varphi(t^{-1})\psi(t) = \frac{1}{g} \sum_{t \in G} \varphi(t)\psi(t^{-1}). \tag{1}$$

Proposition

Pour $g \in G$, soient $(r_{i_1 j_1}(g))$ et $(u_{i_2 j_2}(g))$ les matrices respectives de $\rho_V(g)$ et $\rho_W(g)$ dans les bases $\mathcal{B}_1$, $\mathcal{B}_2$ de V_1, V_2. Alors :

i) Si ρ_V et ρ_W ne sont pas isomorphes, on a $\langle u_{i_2 j_2}, r_{j_1 i_1} \rangle = 0$ pour tous indices i_1, j_1, i_2, j_2.

ii) Si $V_1 = V_2$ est de dimension n et $\rho_V = \rho_W$ (auquel cas on prend $\mathcal{B}_1 = \mathcal{B}_2$ et on a $r_{ij} = u_{ij}$ pour tous indices i, j), alors $\langle r_{i_2 j_2}, r_{j_1 i_1} \rangle = 0$ si $i_1 \neq i_2$ ou $j_1 \neq j_2$, et $\langle r_{ij}, r_{ji} \rangle = \frac{1}{n}$ pour tous indices i, j.

Theorem

i) Soit χ le caractère d'une représentation irréductible ρ de G. Alors, $(\chi|\chi) = 1$.

ii) Soient χ_1 et χ_2 les caractères de deux représentations irréductibles non isomorphes ρ_1 et ρ_2. Alors, $(\chi_1|\chi_2) = 0$.

Theorem

Soit G un groupe. Les propriétés suivantes sont équivalentes :

(i) G est abélien.

(ii) Toutes les représentations irréductibles de G sont de degré 1.

Les groupes non abéliens infinis, comme les groupes de Lie, sont plus complexes et ne se décomposent pas facilement.

Exemple : Le groupe de Heisenberg, utilisé en mécanique quantique.

La théorie des représentations de ces groupes nécessite des outils avancés comme l'analyse spectrale et la cohomologie des groupes.

Applications en Physique

Les groupes de symétrie et leurs représentations jouent un rôle crucial en physique théorique, en particulier dans les théories quantiques.

Exemple : Les groupes de Lie sont utilisés pour décrire les symétries des systèmes physiques.

Les représentations unitaires des groupes de Lie sont fondamentales pour l'étude des particules élémentaires.

Applications en Cryptographie et Géométrie

En cryptographie, les représentations des groupes de matrices sont utilisées dans les systèmes de chiffrement et les algèbres de Lie.

En géométrie, les représentations des groupes de symétrie sont essentielles pour l'étude des surfaces de Riemann et des variétés.

Conclusion

Les représentations linéaires des groupes infinis sont essentielles pour la compréhension des symétries dans des domaines variés tels que la physique, la géométrie et la cryptographie.

Les méthodes modernes, comme la cohomologie des groupes et l'analyse catégorique, ouvrent de nouvelles perspectives dans ce domaine.