

THÉORIE DES REPRÉSENTATIONS

Yves AUBRY, M-147A, yves.aubry@univ-tln.fr

2023-2024

Table des matières

1	Généralités sur les groupes	5
1.1	Rappels	5
1.2	Exemples de groupes	6
1.2.1	$(\mathbb{Z}, +)$	6
1.2.2	$\mathbb{Z}/n\mathbb{Z}$	6
1.3	Groupe diédral	7
1.3.1	Description du groupe D_3	8
1.4	Les théorèmes de Sylow	9
1.4.1	Groupes agissant sur un ensemble ou action de groupes	9
2	Représentations linéaires des groupes finis	13
2.1	Premières définitions	13
2.1.1	Sous-représentations	15
2.2	Théorème de Maschke	16
2.3	Caractère d'une représentation	17

Chapitre 1

Généralités sur les groupes

1.1 Rappels

Soit G un groupe. Soit H un sous-groupe de G (i. e. $H \neq 0$ et $\forall x, y \in H, xy^{-1} \in H$).

Considérons la relation binaire suivante sur G :

Pour $x, y \in G$, $x \equiv_d y \pmod H$ ssi $xy^{-1} \in H$. C'est une relation d'équivalence. Elle est dite de congruence à gauche modulo H .

Démonstration. En effet, si $x \in G$, alors $xx^{-1} = e \in H$, donc $x \pmod_g = x \pmod H$. La relation est donc réflexive.

De plus, si $x, y \in G$ tels que $x \equiv_g y \pmod H$, alors $xy^{-1} \in H$. H étant un sous-groupe de G , il est donc stable par passage au symétrique. D'où $(xy^{-1})^{-1} \in H$, i. e. $yx^{-1} \in H$, c'est-à-dire $y \equiv_g x \pmod H$.

Enfin, si $x, y, z \in G$ tels que $x \equiv_g y \pmod H$ et $y \equiv_g z \pmod H$, alors $xy^{-1} \in H$ et $yz^{-1} \in H$. Or, H étant un sous-groupe de G , donc H est stable pour la loi de composition interne. D'où $(xy^{-1})(yz^{-1}) \in H$. Par associativité, $x(yy^{-1})z^{-1} \in H$, ie $xz^{-1} \in H$.

Donc $x \equiv_g z \pmod H$ et la relation est transitive. \square

Soit $x \in G$. La classe d'équivalence de x pour cette relation d'équivalence est

$$\begin{aligned} cl_d(x) &= \{y \in G \mid xy^{-1} \in H\} \\ &= \{y \in G \mid \exists h \in H, xy^{-1} = h\} \\ &= \{y \in G \mid \exists h \in H, y = hx\} \\ &= \{hx, h \in H\} =: Hx \end{aligned}$$

De même, on considère, sur G , la relation de congruence à gauche modulo H :

$$x \equiv_g y \pmod H \text{ ssi } x^{-1}y \in H.$$

On montre de même que c'est une relation d'équivalence. Si $x \in G$, alors $cl_g(x) := xH = \{xh, h \in H\}$.

Remarque. Si G est abélien, alors les classes à gauche et à droite modulo H coïncident.

Définition 1.1.1. Un sous-groupe H d'un groupe G est dit distingué dans G (ou normal) si :

$$\begin{aligned} &\forall x \in G, xH = Hx, \\ \text{i. e. } &\forall x \in G, xHx^{-1} \subset H \\ \text{i. e. } &\forall x \in G, xHx^{-1} = H. \end{aligned}$$

On note alors $H \triangleleft G$.

Remarque. *Tout sous-groupe d'un groupe abélien est distingué.*

Proposition 1.1.1. *Soit G un groupe et H un sous-groupe distingué de G .*

On note G/H l'ensemble des classes à droite ou à gauche modulo H .

Si $x, y \in G$ et si l'on note \bar{a} la classe de a modulo H , on peut munir le quotient G/H d'une structure de groupe en posant

$$\bar{x} \cdot \bar{y} = \overline{xy}.$$

Démonstration. Cette loi est bien définie, i. e. elle ne dépend pas du choix des représentants des classes d'équivalence. \square

Remarque. Cette loi de la surjection canonique $\pi : \begin{array}{ccc} G & \longrightarrow & G/H \\ x & \longmapsto & \bar{x} \end{array}$ un morphisme de groupes.

Théorème 1 (Lagrange). *Soit G un groupe fini et H un sous-groupe de G .
Alors l'ordre de H divise l'ordre de G .*

Remarque. *L'ordre d'un groupe est simplement son cardinal.*

Remarque. *Si g est un élément de G , alors l'ordre de G est défini comme l'ordre du sous-groupe $\langle g \rangle$ engendré par g . S'il est fini, alors l'ordre de g est le plus petit entier n tel que $g^n = e$.*

D'après le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe.

Remarque. *Si G est un groupe fini et H un sous-groupe de G , alors les classes (à gauche) modulo H ont toutes le même cardinal, à savoir celui de H . En effet, l'application, pour $x \in G : f_x : \begin{array}{ccc} H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$ est bijective.*

1.2 Exemples de groupes

1.2.1 $(\mathbb{Z}, +)$

Groupe abélien.

$n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$ est un sous-groupe de \mathbb{Z} .

Remarque. *Tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$ pour un certain $n\mathbb{Z}$.*

1.2.2 $\mathbb{Z}/n\mathbb{Z}$

C'est l'ensemble des classes d'équivalence pour la relation d'équivalence suivante :

$$x, y \in \mathbb{Z}, x \equiv y \pmod{n\mathbb{Z}} \text{ ssi } x - y \in n\mathbb{Z}.$$

Remarque. $\bar{x} = \bar{y}$ ssi xRy .

On munit l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe (et même d'anneau) en posant, pour $x, y \in \mathbb{Z} : \bar{x} + \bar{y} = \overline{x + y}$ (et $\bar{x} \times \bar{y} = \overline{x \times y}$).

Remarque. $\mathbb{Z}/6\mathbb{Z}$ anneau non intègre, car $\bar{2} \times \bar{3} = \bar{0}$.

Remarque. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier.

Proposition 1.2.1. *Tous les groupes $\mathbb{Z}/n\mathbb{Z}$ sont cycliques. Les générateurs sont les \bar{a} tels que a et n sont premiers entre eux, i. e. $(a, n) = 1$. De plus, tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n = |G|$.*

Enfin, si G est cyclique d'ordre n alors pour tout diviseur d de n , G admet un sous-groupe d'ordre d , et celui-ci est unique, et celui-ci est cyclique.

Remarque. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{(\bar{a}, \bar{a}), \bar{a} \in \mathbb{Z}/2\mathbb{Z}, \bar{a} \in \mathbb{Z}/3\mathbb{Z}\}$.

Théorème 2 (Théorème des restes chinois). Soient n_1, \dots, n_r des entiers premiers entre eux deux à deux. Alors l'application

$$\begin{array}{ccc} \mathbb{Z} / \prod_{i=1}^r n_i \mathbb{Z} & \longrightarrow & \prod_{i=1}^r \mathbb{Z} / n_i \mathbb{Z} \\ a + (\prod_{i=1}^r n_i) \mathbb{Z} & \longmapsto & (a + n_1 \mathbb{Z}, \dots, a + n_r \mathbb{Z}) \end{array}$$

est un isomorphisme d'anneaux et la réciproque est vraie.

19-09-2023

1.3 Groupe diédral

Soit $n \geq 3$ un entier. Le groupe diédral de degré n est le groupe des isométries du plan laissant fixe le polygone régulier à n côtés. On le note D_n (ou D_{2n}).

D_n est un groupe d'ordre $2n$ constitué de n rotations et de n symétries.

Considérons le polygone régulier dont les sommets sont, dans le plan complexe, les n racines n -ièmes de l'unité :

$$e^{\frac{2ik\pi}{n}}, k = 0, 1, \dots, n-1.$$

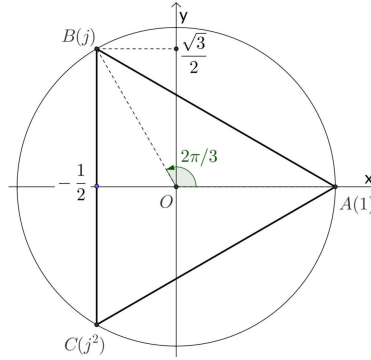


FIGURE 1.1 – Racines 3-ièmes de l'unité.

Soit $r = \text{rot}(0, \frac{2\pi}{n})$ la rotation de centre O et d'angle $\frac{2\pi}{n}$ et soit s la symétrie axiale d'axe la droite réelle (x, x) .

On a

$$r : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & e^{\frac{2i\pi}{n}} z \end{array}$$

et

$$s : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \bar{z} \end{array}.$$

On vérifie que l'on a $r^n = 1 = id$, $s^2 = 1 = id$ et $rs = r^{-1}$.

Démonstration. En effet, si $z \in \mathbb{C}$, alors

$$r^{-1}(z) = e^{-\frac{2i\pi}{n}} z \text{ et } srs(z) = sr(\bar{z}) = s\left(e^{\frac{2i\pi}{n}} \bar{z}\right) = e^{-\frac{2i\pi}{n}} z = r^{-1}(z),$$

donc $srs = r^{-1}$. □

On peut donc définir le groupe diédral D_n par “générateurs et relations” de la façon suivante :

$$D_n = \langle r, s \rangle \text{ avec } r^n = s^2 = 1 \text{ et } srs = r^{-1}.$$

Le sous-groupe de D_n engendré par r est un sous-groupe d'ordre n :

$$\langle r \rangle = \{r, r^2, \dots, r^{n-1}, id\} \simeq \mathbb{Z}/n\mathbb{Z}.$$

Il est d'indice 2 dans D_n , il est donc distingué dans D_n .

1.3.1 Description du groupe D_3

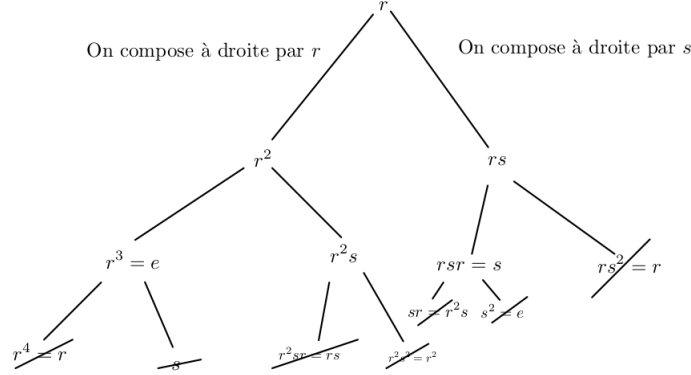


FIGURE 1.2 – Description explicite des éléments de D_3 .

On a donc

$$D_3 = \{e, r, r^2, s, rs, r^2 s\}$$

Remarque. Il n'existe que deux groupes d'ordre 6 à isomorphisme près, à savoir le groupe cyclique (abélien) $\mathbb{Z}/6\mathbb{Z}$ et le groupe symétrique (non abélien) \mathfrak{S}_3 .

Or D_3 n'est pas abélien, donc D_3 est isomorphe à \mathfrak{S}_3 .

Exercice 1. Déterminer l'ordre des éléments de D_3 ainsi que ses sous-groupes.

Exemple 1 (Groupe quaternionien). Soit \mathbb{H} le corps des quaternions d'Hamilton.

$$\mathbb{H} = \{a + ib + jc + kd \mid i^2 = j^2 = k^2 = 1, ij = -ji = k, jk = -kj = i, ki = -ik = j \text{ et } a, b, c, d \in \mathbb{R}\}.$$

\mathbb{H} est un corps non commutatif. On $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$.

Considérons le sous-ensemble suivant de \mathbb{H} :

$$\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Exercice 2. Montrer que \mathbb{H}_8 muni de la multiplication est un groupe.

C'est un groupe non abélien d'ordre 8.

Exercice 3. Déterminer l'ordre des éléments de \mathbb{H}_8 ainsi que ses sous-groupes.

Rappel

Théorème 3 (De classification des groupes abéliens finis). Tout groupe **abélien** fini est isomorphe à un produit de groupes cycliques de la forme

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}, \text{ avec } d_1 \mid d_2 \mid \dots \mid d_r.$$

Cette écriture est unique (à l'ordre près des facteurs).

On en déduit qu'il existe trois groupes abéliens d'ordre 8 à isomorphisme près :

$$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ et } (\mathbb{Z}/2\mathbb{Z})^3.$$

Question : a-t-on $\mathbb{H}_8 \simeq D_4$?

1.4 Les théorèmes de Sylow

Si H est un sous-groupe d'un groupe G , ses **conjugués** dans G sont gHg^{-1} , avec $g \in G$. En particulier, H est distingué dans G si et seulement si il est égal à tous ses conjugués.

Définition 1.4.1. Si G est un groupe fini d'ordre $p^\alpha q$, avec p premier, $\alpha \geq 1$ et q premier avec p , alors tout sous-groupe de G d'ordre $p^\beta q$ est appelé un p sous-groupe de Sylow de G (ou encore un p -Sylow de G).

Théorème 4 (Premier théorème de Sylow). Soit G un groupe d'ordre $p^\alpha q$, p premier, $\alpha \geq 1$, $(p, q) = 1$. Pour tout $1 \leq \beta \leq \alpha$, il existe un sous-groupe de G d'ordre p^β .

Théorème 5 (Deuxième théorème de Sylow). Le nombre n_p de p -Sylow de G vérifie :

$$\begin{cases} n_p \equiv 1 \pmod{p} \\ n_p \mid q. \end{cases}$$

Théorème 6 (Troisième théorème de Sylow).

1. Le conjugué d'un p -Sylow est un p -Sylow.
2. Tous les p -Sylow sont conjugués entre eux.

Exercice 4. Montrer qu'il n'existe pas de groupes simples d'ordre 15.

Démonstration. Soit G un groupe d'ordre $3 \times 5 = 15$. D'après le premier théorème de Sylow, G admet au moins un 3-Sylow.

Soit n_3 le nombre de 3-Sylow de G . Par le deuxième théorème de Sylow, on a

$$n_3 \equiv 1 \pmod{3} \text{ et } n_3 \mid 5.$$

G admet donc un unique 3-Sylow H .

D'après le (1) du troisième théorème de Sylow, les conjugués de H sont des 3-Sylow de G , donc sont égaux à H puisque c'est le seul 3-Sylow de G . Donc H est égal à tous ses conjugués et donc H est distingué dans G . Puisque $|H| = 3$, $H \neq \{e\}$ et $H \neq G$. Donc G admet un sous-groupe distingué propre. Donc G n'est pas simple. \square

1.4.1 Groupes agissant sur un ensemble ou action de groupes

Définition 1.4.2 (Action de groupe). Une action (à gauche) d'un groupe G sur un ensemble X est une application

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

telle que

1. $\forall x \in X, e \cdot x = x$ (où e est l'élément neutre de G);
2. $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = (gg') \cdot x$.

On peut voir une action comme un morphisme de groupes de G dans le groupe symétrique \mathfrak{S}_X de permutations dans X :

Proposition 1.4.1. Si un groupe G agit sur un ensemble X par

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x, \end{aligned}$$

alors pour tout $g \in G$, l'application

$$\pi_g : \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$$

est une permutation de X et l'application

$$\pi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_X \\ g & \longmapsto & \pi_g \end{array}$$

est un morphisme de groupes.

Réciproquement, si $\begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_X \\ g & \longmapsto & p_g \end{array}$ est un morphisme de groupes, alors $(g, x) \mapsto g \cdot x := p_g(x)$ est une action de G sur X .

Démonstration.

Supposons que G agisse sur un ensemble X par $\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$.

Soit $g \in G$. Considérons l'application $\pi_g : \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$.

Montrons que π_g est injective. Soient $x, y \in X$ tq $\pi_g(x) = \pi_g(y)$. D'où $g \cdot x = g \cdot y$. D'où $g^{-1} \cdot g \cdot x = g^{-1} \cdot g \cdot y$. D'où $(g^{-1}g) \cdot x = (g^{-1}g) \cdot y$. D'où $e \cdot x = e \cdot y$. Donc π_g est injective. Montrons que π_g est surjective. Soit $y \in X$. On a $y = \pi_g(g^{-1}y) = g \cdot g^{-1} \cdot y$. Donc π_g est surjective. Donc π_g est bijective.

On peut donc considérer l'application $\pi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_X \\ g & \longmapsto & \pi_g \end{array}$.

Montrons que π est un morphisme de groupes. Montrons que $\forall g, g' \in G, \pi_{gg'} = \pi_g \circ \pi_{g'}$.

Soient $g, g' \in G$. Soit $x \in X$.

$$\pi_{gg'}(x) = (gg') \cdot x = g \cdot g' \cdot x = g \cdot (\pi_{g'}(x)) = \pi_g(\pi_{g'}(x)).$$

Donc $\pi_{gg'} = \pi_g \circ \pi_{g'}$.

Réciproquement, si on se donne un morphisme de groupes d'un groupe G dans un groupe de permutations \mathfrak{S}_X :

$$p : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_X \\ g & \longmapsto & p_g, \end{array}$$

alors l'application

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x := p_g(x) \end{array}$$

est une action de groupes.

En effet,

1. Soit $x \in X$, on a $e \cdot x = p_e(x) = id_X(x) = x$, car p est un morphisme de groupes et l'image de l'élément neutre par un morphisme de groupes est l'élément neutre.
2. Soient $g, g' \in G$ et soit $x \in X$; on a

$$g \cdot (g' \cdot x) = g \cdot (p_{g'}(x)) = p_g(p_{g'}(x)) = (p_g \circ p_{g'})(x) = p_{gg'}(x) = (gg') \cdot x,$$

car p est un morphisme de groupes.

□

Cela établit deux bijections réciproques entre l'ensemble des actions de G sur X et celui des morphismes de G dans \mathfrak{S}_X .

Définition 1.4.3. Si un groupe G agit sur un ensemble X , alors la relation sur X définie par : pour $x, y \in X, x \sim y$ ssi $\exists g \in G, y = g \cdot x$ est une relation d'équivalence. La classe d'équivalence de X pour cette relation s'appelle **l'orbite** de X :

$$\text{Orb}(x) := \{g \cdot x, g \in G\}.$$

Ainsi, l'ensemble des orbites forme une **partition** de X .

On dit que g agit **transitivement** s'il n'y a qu'une seule orbite.

Le **noyau** de l'action est le noyau du morphisme associé :

$$\pi : \begin{array}{ccc} G & & \\ g & \longmapsto & \left(\begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array} \right) \end{array} \quad \mathfrak{S}_X$$

$$\text{Ker}(\pi) = \{g \in G \mid \forall x \in X, g \cdot x = x\}.$$

On dit que l'action est **fidèle** si son noyau est réduit à $\{e\}$ (i. e. si le morphisme π est injectif).

Le **stabilisateur** (ou groupe d'isotropie) d'un élément $x \in X$ est l'ensemble :

$$\text{Stab}(x) = \{g \in G \mid g \cdot x = x\}.$$

C'est un sous-groupe de G (en exercice).

Proposition 1.4.2. Pour x fixé dans X , l'application

$$\begin{array}{ccc} G & \longrightarrow & X \\ g & \longmapsto & g \cdot x \end{array}$$

définit une bijection de l'ensemble $G/\text{Stab}(x)$ des classes à gauche modulo $\text{Stab}(x)$ sur l'orbite de x . Ainsi, le cardinal de l'orbite $\text{Orb}(x)$ est égal à l'indice du stabilisateur de x :

$$\sharp(\text{Orb}(x)) = [G : \text{Stab}(x)].$$

Théorème 7 (Formule des classes). Soit G un groupe fini agissant sur un ensemble fini X . Alors

$$\sharp(X) = \sum_{\substack{x \text{ décrivant un système} \\ \text{des représentants des orbites}}} [G : \text{Stab}(x)].$$

Démonstration.

$$\sharp(X) = \sum_{i=1}^m \sharp(\text{Orb}(x_i)),$$

où $\{x_1, \dots, x_n\}$ est un système des représentants des orbites pour l'action de G sur X . □

Exemple d'action de groupe On fait agir un groupe G sur lui-même par conjugaison

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g \cdot x := gxg^{-1}. \end{array}$$

C'est bien une action de groupes, car

1. Soit $x \in G$, on a $e \cdot x = exe^{-1} = x$.
2. Soient $g, g' \in G$ et $x \in G$. On a :

$$g \cdot (g' \cdot x) = g \cdot (gx'g^{-1}) = g(g'x(g')^{-1})g^{-1} = (gg')x((g')^{-1}g^{-1}) = (gg')x(gg')^{-1} = (gg') \cdot x.$$

Cette action est-elle transitive, fidèle ? Quelle est l'orbite d'un élément ?

20-09-2023

Soit $x \in G$. L'orbite de x est :

$$\text{Orb}(x) = \{g \cdot x, g \in G\} = \{gxg^{-1}, g \in G\} = \text{classe de conjugaison de } x \text{ dans } G.$$

On a $\text{Orb}(e) = \{e\}$. Si G n'est pas réduit à $\{e\}$, il y a plusieurs orbites : l'action n'est donc pas transitive (il y a autant d'orbites que de classes de conjugaison).

L'action est-elle fidèle ? Etudions le noyau du morphisme π associé à cette action

$$\pi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_G \\ g & \longmapsto & \left(\pi_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array} \right) \end{array}.$$

On a

$$\begin{aligned} \text{Ker}(\pi) &= \{g \in G \mid \pi_g = \text{id}_G\} = \{g \in G \mid \forall x \in G, \pi_g(x) = x\} \\ &= \{g \in G \mid \forall x \in G, gxg^{-1} = x\} = \{g \in G \mid \forall x \in G, gx = xg\} = Z(G). \end{aligned}$$

L'action est fidèle si et seulement si le centre de G est réduit à l'élément neutre.

Soit $x \in G$. Quel est le stabilisateur de x ?

$$\text{Stab}(x) = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = \text{centralisateur de } x.$$

Etudions un exemple avec $G = \mathfrak{S}_3$. Les orbites de \mathfrak{S}_3 pour cette action sont les classes de conjugaison de \mathfrak{S}_3 . Elles constituent une partition de \mathfrak{S}_3 .

1. $\text{Orb}(e) = \{e\}$.
2. $\text{Orb}(\tau_3) = \{\sigma\tau_3\sigma^{-1}, \sigma \in \mathfrak{S}_3\} = \{\text{transpositions de } \mathfrak{S}_3\} = \{\tau_1, \tau_2, \tau_3\}$.
3. $\text{Orb}(\sigma_1) = \{\sigma\sigma_1\sigma^{-1}, \sigma \in \mathfrak{S}_3\} = \{3\text{-cycles de } \mathfrak{S}_3\} = \{\sigma_1, \sigma_2\}$.

La formule des classes s'écrit alors :

$$|\mathfrak{S}_3| = \sum [\mathfrak{S}_3 : \text{Stab}(x_i)],$$

où $\{x_1, x_2, x_3\}$ est un système des représentants de l'orbite, avec $x_1 = e, x_2 = \tau_1, x_3 = \sigma_1$.

On a

$$|\mathfrak{S}_3| = \sum_{i=1}^3 \# \text{Orb}(x_i) = \# \text{Orb}(x_1) + \# \text{Orb}(x_2) + \# \text{Orb}(x_3) = 1 + 3 + 2 = 6.$$

L'action est fidèle, car $Z(\mathfrak{S}_3) = \{e\}$. L'action n'est pas transitive, car il y a trois orbites, à savoir les trois classes de conjugaison.

$$\text{Stab}(e) = \{\sigma \in \mathfrak{S}_3 \mid \sigma e = e\sigma\} = \mathfrak{S}_3.$$

On a bien

$$[\mathfrak{S}_3 : \text{Stab}(e)] = \frac{|\mathfrak{S}_3|}{|\text{Stab}(e)|} = \frac{3!}{3!} = 1 = \# \text{Orb}(e).$$

On a $[\mathfrak{S}_3 : \text{Stab}(\tau_3)] = \# \text{Orb}(\tau_3) = 3$, donc $|\text{Stab}(\tau_3)| = 2$. D'où

$$\text{Stab}(\tau_3) = \{\text{permutations de } \mathfrak{S}_3 \text{ qui commutent avec } \tau_3\} = \{e, \tau_3\}.$$

On a $[\mathfrak{S}_3 : \text{Stab}(\sigma_1)] = \# \text{Orb}(\sigma_1) = 2$, donc $|\text{Stab}(\sigma_1)| = 3$. Puisque l'indice du stabilisateur est 2, on en déduit que $\text{Stab}(\sigma_1) \triangleleft \mathfrak{S}_3$. Or les seuls sous-groupes distingués de \mathfrak{S}_n sont $\{e\}, \mathfrak{S}_n$ et \mathfrak{A}_n . Donc

$$\text{Stab}(\sigma_1) = \mathfrak{A}_3 = \{e, \sigma_1, \sigma_2\}.$$

Chapitre 2

Représentations linéaires des groupes finis

Théorie introduite par Frobenius à la fin du XIX siècle.

2.1 Premières définitions

Définition 2.1.1. Une représentation linéaire d'un groupe G est la donnée d'un \mathbb{C} -espace vectoriel V muni d'une action de groupes (à gauche) de G agissant de manière linéaire :

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

telle que

1. $\forall x \in V, e \cdot x = x$;
2. $\forall g, g' \in G, \forall x \in V, g \cdot (g' \cdot x) = (gg') \cdot x$;
3. $\forall g \in G, \forall x, x' \in V, \forall \lambda, \lambda' \in \mathbb{C}, g \cdot (\lambda x + \lambda' x') = \lambda g \cdot x + \lambda' g \cdot x$.

Une représentation linéaire d'un groupe G est donc la donnée d'un \mathbb{C} -espace vectoriel V et d'un morphisme de groupes :

$$\begin{aligned} \rho : G &\longrightarrow GL(V) \\ g &\longmapsto \left(\begin{array}{ccc} V &\longrightarrow & V \\ x &\longmapsto & g \cdot x \end{array} \right) \end{aligned}$$

où $GL(V)$ est le groupe des automorphismes du \mathbb{C} -espace vectoriel V .

On a bien $\forall g, g' \in G, \rho_{gg'} = \rho_g \circ \rho_{g'}$ et $\rho_e = id_V$ et $\rho_{g^{-1}} = \rho_g^{-1}$ comme vu précédemment.

De plus, $\forall g \in G$, la bijection ρ_g est un endomorphisme de V , i. e. une application linéaire de V dans V et donc $\rho_g \in GL(V)$. En effet, si $x, x' \in V$ et $\lambda, \lambda' \in \mathbb{C}$, alors

$$\rho_g(\lambda x + \lambda' x') = g \cdot (\lambda x + \lambda' x') \stackrel{(3)}{=} \lambda g \cdot x + \lambda' g \cdot x' = \lambda \rho_g(x) + \lambda' \rho_g(x').$$

Définition 2.1.2. L'espace vectoriel V est appelé **l'espace de la représentation**.

La dimension de V (en tant que \mathbb{C} -espace vectoriel) est appelé le **degré** ou la dimension de la représentation.

Lorsque ρ est injectif, la représentation est dite **fidèle** ; le groupe G se représente alors de manière concrète comme un sous-groupe de $GL(V)$; lorsque V est de dimension finie (ce que nous allons supposer dorénavant), le choix d'une base du \mathbb{C} -espace vectoriel V fournit alors une représentation encore plus concrète comme groupe de matrice.

Remarque (Personnelle). Si ρ est une représentation fidèle, alors

$$\text{Ker}(\rho) = \{g \in G \mid \forall x \in V, g \cdot x = x\} = \{e\}.$$

Remarque. Soient G un groupe fini et $\rho : G \rightarrow GL(V)$ une représentation (linéaire) de G . Soit $g \in G$ un élément d'ordre n . On a alors

$$(\rho_g)^n = \rho_{g^n} = \rho_e = id_V.$$

Donc l'endomorphisme ρ_g est racine du polynôme $X^n - 1$ qui n'a que des racines simples. Le polynôme minimal de ρ_g divise donc le polynôme $X^n - 1$ et n'a donc aussi que des racines simples. Le polynôme minimal de ρ_g est donc scindé sur \mathbb{C} et à racines simples, on en déduit que l'endomorphisme de ρ_g est **diagonalisable**.

Exemples

1. La représentation triviale (ou représentation unité) :

$$\begin{aligned} \rho : G &\longrightarrow GL(\mathbb{C}) \simeq \mathbb{C}^* \\ g &\longmapsto \left(\rho_g : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & x \end{array} \right). \end{aligned}$$

2. Les représentations de degré 1 : ce sont les morphismes de groupes

$$\rho : G \longrightarrow \mathbb{C}^*$$

puisque si $\dim V = 1$, alors $GL(V) \simeq \mathbb{C}^*$, car les endomorphismes de V sont des homothéties :

$$\begin{aligned} f_\lambda : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\longmapsto \lambda x \end{aligned}$$

et

$$\begin{aligned} GL(V) &\longrightarrow \mathbb{C}^* \\ f_\lambda &\longmapsto \lambda \end{aligned}$$

qui a une homothétie fait correspondre son rapport induit un isomorphisme. Si G est **fini**, tout élément de G est d'ordre fini (par le théorème de Lagrange) et donc, pour tout $g \in G$, ρ_g est une racine de l'unité dans \mathbb{C} , et en particulier ρ_g est un nombre complexe de module 1 :

$$|\rho_g| = 1.$$

3. Soient \mathfrak{S}_n le groupe symétrique et (e_1, \dots, e_n) la base canonique de \mathbb{C}^n . On définit la représentation canonique de degré n de \mathfrak{S}_n en posant :

$$\begin{aligned} \rho : \mathfrak{S}_n &\longrightarrow GL(\mathbb{C}^n) \\ \sigma &\longmapsto \left(\rho_\sigma : \begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C}^n \\ e_i & \longmapsto & \rho_\sigma(e_i) := e_{\sigma(i)} \end{array} \right). \end{aligned}$$

4. *La représentation de permutations.* Soit $\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$ une action d'un groupe sur un ensemble fini X . Soit V un \mathbb{C} -espace vectoriel de dimension égale au cardinal de X (par exemple, on peut voir V comme le \mathbb{C} -espace vectoriel des fonctions définies sur X et à valeurs dans \mathbb{C} dont

une base peut être donnée par les fonctions indicatrices $\varepsilon_x : \begin{array}{ccc} X & \longrightarrow & \mathbb{C} \\ y & \longmapsto & \varepsilon_x(y) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sinon} \end{cases} \end{array}$

pour x décrivant X) muni d'une base indexée par les éléments de X : $\{\varepsilon_x, x \in X\}$. On peut écrire $V = \bigoplus_{x \in X} \mathbb{C}\varepsilon_x$. On définit une représentation linéaire (complexe de dimension finie) :

$$\begin{aligned} \rho : G &\longrightarrow GL(V) \\ g &\longmapsto \left(\rho_g : \begin{array}{ccc} V & \longrightarrow & V \\ \varepsilon_x & \longmapsto & \rho_g(\varepsilon_x) := \varepsilon_{g \cdot x} \end{array} \right) \end{aligned}$$

C'est la représentation de permutations associée à l'action de G sur X (c'est l'application qui envoie un vecteur de base sur un autre vecteur de base).

5. *La représentation régulière.* C'est l'exemple précédent avec $X = G$ agissant sur lui-même (par translation à gauche) :

$$\begin{aligned} \rho : G &\longrightarrow GL(V) \\ g &\longmapsto \left(\rho_g : \begin{array}{ccc} V & \xrightarrow{\quad} & V \\ \varepsilon_x & \longmapsto & \varepsilon_{gx} \end{array} \right) \end{aligned}$$

Ici, il s'agit de la loi de composition interne de G et on a $\dim(V) = |G|$.

Définition 2.1.3. Deux représentations linéaires $\rho : G \rightarrow GL(V)$ et $\rho' : G \rightarrow GL(V')$ d'un groupe G sont dites **isomorphes** ou **équivalentes** s'il existe un isomorphisme d'espaces vectoriels $f : V \rightarrow V'$ tel que l'on ait :

$$\forall g \in G, \rho'_g \circ f = f \circ \rho_g.$$

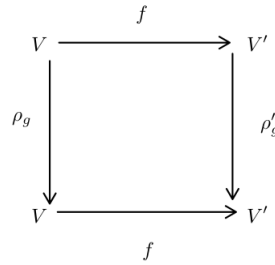


FIGURE 2.1 – Représentations linéaires isomorphes.

On peut exprimer cette condition par la commutativité du diagramme suivant :

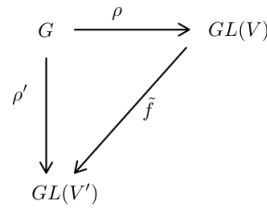


FIGURE 2.2 – Diagramme commutatif de deux représentations isomorphes.

Remarque. Dire que le diagramme ci-dessus commute, c'est dire que

$$\tilde{f} \circ \rho = \rho'.$$

D'où, pour tout $g \in G$, $\rho'_g = \tilde{f}(\rho_g) = f \circ \rho_g \circ f^{-1}$, i. e. $\rho'_g \circ f = f \circ \rho_g$.

Remarque. En termes de matrices, cela signifie que les matrices associées à la première représentation sont semblable à leurs homologues dans la deuxième, via la même matrice de passage :

$$\forall g \in G, \text{Mat}(\rho'_g) = \text{Mat}(f) \times \text{Mat}(\rho_g) \times \text{Mat}(f)^{-1}.$$

2.1.1 Sous-représentations

Définition 2.1.4. Si $\rho : G \rightarrow GL(V)$ est une représentation linéaire d'un groupe G et si W est un sous-espace vectoriel de V stable par la représentation (i.e. stable par les automorphismes ρ_g pour $g \in G$, i.e. $\forall g \in G, \rho_g(W) \subset W$, i. e. $\forall g \in G, \forall w \in W, \rho_g(w) \in W$), alors cela nous permet de définir une **sous-représentation**

$$\begin{aligned} \rho|_W : G &\longrightarrow GL(W) \\ g &\longmapsto \left(\rho_{g|_W} : \begin{array}{ccc} W & \longrightarrow & W \\ w & \longmapsto & \rho_g(w) \end{array} \right). \end{aligned}$$

Définition 2.1.5. Une représentation $\rho : G \rightarrow GL(V)$ est dite **irréductible** si les seuls sous-espaces stables de V sont $\{0\}$ et V .

Remarque. Les représentations de degré 1 sont bien évidemment des représentations irréductibles.

2.2 Théorème de Maschke

On définit tout d'abord la notion de **somme directe** de représentations. On rappelle que si V est un espace vectoriel et si W, W' sont deux sous-espaces vectoriels de V , alors on dit que V est **somme directe** de W et W' si tout $x \in V$ peut s'écrire de façon unique sous la forme :

$$x = w + w', \text{ avec } w \in W, w' \in W'.$$

Il revient au même de dire que

$$W \cap W' = \{0\} \text{ et } \dim(V) = \dim(W) + \dim(W').$$

On écrit alors $V = W \oplus W'$ et l'on dit que W' est un **supplémentaire** de W dans V .

$$V \longrightarrow V$$

L'application $p : \begin{array}{ccc} \in W & \in W' & \\ v = w + w' & \longmapsto & w \end{array}$ est alors appelé le **projecteur** de V sur W associé à la

décomposition $V = W \oplus W'$. On a $\text{Im}(p) = W$ et $\text{Ker}(p) = W'$ et $p(x) = x$ si $x \in W$.

Réciproquement, si p est une application linéaire de V sur lui-même vérifiant ces deux propriétés, on vérifie que $V = W \oplus \text{Ker}(p)$, avec $\text{Ker}(p) = \{v \in V, p(v) = 0\}$. On établit ainsi une **bijection** entre les projecteurs de V sur W et les **supplémentaires** de W dans V .

Définition 2.2.1. Soient $\rho : G \rightarrow GL(V)$ et $\rho' : G \rightarrow GL(V')$ deux représentations d'un groupe G . On définit la somme directe $\rho \oplus \rho'$ comme étant la représentation d'espace vectoriel $V \oplus V'$ définie par

$$\begin{aligned} \rho \oplus \rho' : G &\longrightarrow GL(V \oplus V') \\ g &\longmapsto \left((\rho \oplus \rho')_g : \begin{array}{ccc} V \oplus V' & \longrightarrow & V \oplus V' \\ v + v' & \longmapsto & \rho_g(v) + \rho'_g(v') \end{array} \right). \end{aligned}$$

Théorème 8 (De Maschke). Toute représentation linéaire complexe de dimension finie d'un groupe fini est **somme directe de représentations irréductibles**.

Lemme. Tout sous-espace stable d'une représentation linéaire complexe de degré fini d'un groupe fini admet un sous-espace **supplémentaire stable**.

Remarque. \triangle Il existe un produit scalaire hermitien sur l'espace de la représentation qui est stable par l'action du groupe. En effet, si $\langle \cdot, \cdot \rangle$ désigne un produit scalaire quelconque sur V , le produit suivant est stable par ρ :

$$\forall x, y \in V, \langle x, y \rangle_\rho := \frac{1}{|G|} \sum_{g \in G} \langle \rho_g(x), \rho_g(y) \rangle.$$

En effet, si $h \in G$, alors on a :

$$\begin{aligned} \langle \rho_h(x), \rho_h(y) \rangle_\rho &= \frac{1}{|G|} \sum_{g \in G} \langle \rho_g(\rho_h(x)), \rho_g(\rho_h(y)) \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \langle \rho_{gh}(x), \rho_{gh}(y) \rangle = \langle x, y \rangle_\rho, \end{aligned}$$

car $g \mapsto gh$ est une bijection de G sur lui-même.

Démonstration du lemme. Si W est un sous-espace vectoriel de V stable sous l'action de G , alors le supplémentaire **orthogonal** de W est lui aussi stable sous l'action puisque : $W \subset V$ stable sous l'action de G par ρ , i. e. $\forall g \in G, \rho_g(W) \subset W$. On a

$$W^\perp := \{x \in V \mid \langle x, w \rangle_\rho = 0, \forall w \in W\}.$$

Montrons que W^\perp est stable par ρ . Soit $g \in G$, soit $x \in W^\perp$, montrons que $\rho_g(x) \in W^\perp$. Soit $w \in W$, montrons que $\langle \rho_g(x), w \rangle_\rho = 0$. On a

$$\langle \rho_g(x), w \rangle_\rho = \langle \rho_{g^{-1}}(\rho_g(x)), \rho_{g^{-1}}(w) \rangle_\rho = \langle x, \rho_{g^{-1}}(w) \rangle_\rho = 0,$$

car $\rho_{g^{-1}}(w) \in W$. □

Démonstration du théorème. Si $\dim(V) = 1$ ou si V est irréductible, c'est démontré.

Si $\dim(V) \geq 2$ et V est non irréductible, alors V possède une sous-représentation W distincte de $\{0\}$ et V . Si $\langle \cdot, \cdot \rangle_\rho$ est un produit scalaire hermitien sur V invariant sous l'action de G , le supplémentaire orthogonal W^\perp de W est lui aussi stable par G . On a alors $V = W \oplus W'$ et W et W' sont de dimensions inférieures à celle de V .

Par l'hypothèse de récurrence, on peut les décomposer en sommes directes de représentations irréductibles. □

2.3 Caractère d'une représentation

Définition 2.3.1. On appelle **caractère** de la représentation $\rho : G \longrightarrow GL(V)$ l'application

$$\begin{aligned} \chi_\rho : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \chi_\rho(g) := \text{Tr}(\rho_g). \end{aligned}$$

où $\text{Tr}(\rho_g)$ désigne la **trace** de l'endomorphisme ρ_g .

Le degré du caractère χ_ρ est défini comme le degré de la représentation ρ .

Proposition 2.3.1. Soit $\rho : G \longrightarrow GL(V)$ une représentation d'un groupe fini G de caractère χ_ρ .

1. $\chi_\rho(e) = \dim(V) = \text{degré de } \rho = \text{degré de } \chi_\rho$.
2. $\forall g \in G, \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$ (conjugaison complexe).
3. $\forall g, h \in G, \chi_\rho(ghg^{-1}) = \chi_\rho(h)$, i. e. χ_ρ est une fonction centrale sur G , i. e. χ_ρ est constante sur les classes de conjugaison.
4. $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$, si $\rho' : G \longrightarrow GL(V')$.
5. Si ρ, ρ' sont équivalentes, alors $\chi_\rho = \chi_{\rho'}$.