

THÉORIE DES REPRÉSENTATIONS

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

2023-2024

I	Représentations linéaires des groupes finis	5
1	Généralités sur les groupes	7
1.1	Rappels	7
1.2	Exemples de groupes	8
1.2.1	$(\mathbb{Z}, +)$	8
1.2.2	$\mathbb{Z}/n\mathbb{Z}$	9
1.3	Groupe diédral	9
1.3.1	Description du groupe D_3	10
1.4	Les théorèmes de Sylow	11
1.4.1	Groupes agissant sur un ensemble ou action de groupes	12
2	Représentations linéaires des groupes finis	17
2.1	Premières définitions	17
2.1.1	Sous-représentations	20
2.2	Théorème de Maschke	20
2.3	Caractère d'une représentation	21
2.4	Orthogonalité des caractères irréductibles	24
2.5	Théorème de Frobenius	27
2.6	Le cas des groupes abéliens	30
2.7	Nombre de représentations irréductibles de degré 1	32

Première partie

Représentations linéaires des groupes finis

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 1.1.1 (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 $n \in \mathbb{Z}$.

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

Théorème 1.2.1 (Théorème des restes chinois). Soient n_1, \dots, n_r des entiers premiers entre eux deux à deux. Alors l'application

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

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 :

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

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 $rs = r^{-1}$.



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

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

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

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 (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.

Théorème 1.3.1 (De classification des groupes abéliens finis). *Tout groupe **abélien** fini est isomorphe à un produit de groupes cycliques de la forme*

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

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

Rappel 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^β est appelé un p sous-groupe de Sylow de G (ou encore un p -Sylow de G).

Théorème 1.4.1 (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 1.4.2 (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 1.4.3 (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. $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = \underbrace{(gg')}_{\text{LCI de } G} \cdot x$.

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 :

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

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 :

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

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

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 :

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

Théorème 1.4.4 (Formule des classes). *Soit G un groupe fini agissant sur un ensemble fini X . Alors*

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

Démonstration.

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

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 :

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

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

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

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

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**.

Exemple (De représentations).

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 $\varepsilon_x : X \rightarrow \mathbb{C}$:

$$y \mapsto \varepsilon_x(y) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sinon} \end{cases}$$

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) :

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

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

26-09-2023

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 (ici application linéaire bijective) $f : V \rightarrow V'$ tel que l'on ait :

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

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

$$\begin{array}{ccc} G & \xrightarrow{\rho} & GL(V) \\ \rho' \downarrow & \circlearrowleft & \swarrow \tilde{f} \\ & GL(V') & \end{array}$$

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. $\rho'_g \circ f = f \circ \rho_g$.

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ \rho_g \downarrow & \circlearrowleft & \downarrow \rho'_g \\ V & \xrightarrow{f} & V' \end{array}$$

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.

Démonstration personnelle. Soit $\rho : G \rightarrow GL(V)$ une représentation de degré 1. Alors $\dim(V) = 1$. Si W sous-espace vectoriel de V , alors

1. $\dim(W) = 0$ et dans ce cas $W = \{0\}$;
2. ou bien $\dim(W) = 1$ et dans ce cas $W = V$.

□

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 .

$$\begin{array}{ccc} V & \longrightarrow & V \\ \downarrow & & \downarrow \\ W & \longrightarrow & W \end{array}$$

L'application $p : v = \underbrace{w}_{\in W} + \underbrace{w'}_{\in W'} \longmapsto w$ 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 2.2.1 (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 2.2. 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 2.2.1. 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 (Propriétés du caractère d'une représentation). 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 $\rho' : G \longrightarrow GL(V')$ est une représentation de G .
5. Si ρ, ρ' sont équivalentes, alors $\chi_\rho = \chi_{\rho'}$.

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

1. Par définition, $\chi_\rho(e) = \text{Tr}(\rho_e)$. Puisque ρ est un morphisme de groupes, l'image de l'élément neutre de G par ρ est donc l'élément neutre de $GL(V)$, à savoir l'identité id_V sur V . D'où :

$$\chi_\rho(e) = \text{Tr}(\rho_e) = \text{Tr}(\text{id}_V) = \text{Tr}(I_{\dim(V)}).$$

C'est la matrice identité à $\dim(V)$ lignes et $\dim(V)$ colonnes.

2. Montrons que $\forall g \in G, \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

Remarquons que si G est fini et si $g \in G$, alors les valeurs propres de ρ_g (les racines du polynôme de cet endomorphisme) sont les racines de l'unité. En effet, si G est d'ordre n , alors, par le théorème de Lagrange, on a $g^n = e$. D'où

$$\rho_g^n = \rho_{g^n} = \rho_e = \text{id}_V,$$

donc le polynôme minimal de ρ_g divise $X^n - 1$. Or les racines du polynôme minimal de ρ_g sont les valeurs propres de ρ_g . Donc les valeurs propres de ρ_g sont les racines de l'unité.

En particulier, les valeurs propres de ρ_g sont des nombres complexes de module 1. Donc, si λ est une valeur propre de ρ_g , alors $|\lambda| = 1$ et donc $\lambda^{-1} = \bar{\lambda}$. De plus, les valeurs propres de $\rho_{g^{-1}} = \rho_g^{-1}$ (car ρ est un morphisme) sont les inverses de celles de ρ_g .

En effet, si $f(x) = \lambda x$ avec x non nul et $f \in GL(V)$, alors

$$x = f^{-1}(f(x)) = f^{-1}(\lambda x) = \lambda f^{-1}(x),$$

d'où $f^{-1}(x) = \lambda^{-1}(x)$ et donc x est vecteur propre de f^{-1} pour la valeur propre λ^{-1} .

Enfin, puisque la trace d'un endomorphisme est la somme de ses valeurs propres (comptées avec leur multiplicités), on en déduit que

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

3. Soient $g, h \in G$. On a

$$\begin{aligned} \chi_\rho(ghg^{-1}) &\stackrel{\text{déf}}{=} \text{Tr}(\rho_{ghg^{-1}}) \stackrel{\text{morphisme}}{=} \text{Tr}(\rho_g \circ \rho_h \circ \rho_{g^{-1}}) \\ &= \text{Tr}(\rho_g \circ \rho_h \circ \rho_g^{-1}) \stackrel{\text{Tr}(AB)=\text{Tr}(BA)}{=} \text{Tr}(\rho_g^{-1} \circ \rho_g \circ \rho_h) = \text{Tr}(\rho_h) = \chi_\rho(h). \end{aligned}$$

Donc χ_ρ est une fonction centrale sur G , i. e. qu'elle prend les mêmes valeurs sur les éléments d'une même classe de conjugaison.

4. Soient $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$ deux représentations de G . La somme directe de ρ et ρ' est la représentation

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

Si (e_1, \dots, e_n) est une base de V et (e'_1, \dots, e'_m) est une base de V' , alors

$$B = (e_1 + 0, \dots, e_n + 0, 0 + e'_1, \dots, 0 + e'_m)$$

est une base de $V \oplus V'$.

D'où

$$\text{Mat}_B((\rho \oplus \rho')_g) = \begin{pmatrix} \text{Mat}_{(e_1, \dots, e_n)}(\rho_g) & 0 \\ 0 & \text{Mat}_{(e'_1, \dots, e'_m)}(\rho'_g) \end{pmatrix},$$

d'où

$$\begin{aligned} \chi_{(\rho \oplus \rho')_g} &= \text{Tr}((\rho \oplus \rho')_g) = \text{Tr}(\text{Mat}_B((\rho \oplus \rho')_g)) \\ &= \text{Tr}(\text{Mat}_{(e_1, \dots, e_n)}(\rho_g)) + \text{Tr}(\text{Mat}_{(e'_1, \dots, e'_m)}(\rho'_g)) = \chi_\rho(g) + \chi_{\rho'}(g). \end{aligned}$$

5. Soient $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$ deux représentations équivalentes de G . Alors il existe une isomorphisme $f : V \longrightarrow V'$ tel que

$$\forall g \in G, \rho'_g = f \circ \rho_g \circ f^{-1}.$$

D'où, pour tout $g \in G$, on a

$$\chi_{\rho'}(g) = \text{Tr}(\rho'_g) = \text{Tr}(f \circ \rho_g \circ f^{-1}) = \text{Tr}(\rho_g) = \chi_\rho(g).$$

Donc $\chi_\rho = \chi_{\rho'}$.

□

Exemple (Calcul de caractères).

1. Si G opère sur un ensemble fini X , considérons la représentation de permutations ρ associée, avec $V = \bigoplus_{x \in X} \langle e_x \rangle = \bigoplus_{x \in X} \mathbb{C}e_x$.

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

On a $\chi_\rho : G \longrightarrow \mathbb{C}$ tel que $\chi_\rho(g) = \text{Tr}(\rho_g)$. Dans une base $(e_x)_{x \in X}$ de V , pour $g \in G$ fixé, la matrice de ρ_g est une matrice de permutations, i.e. a exactement un 1 par ligne et par colonne et tous les autres coefficients sont nuls.

De plus, si $\text{Mat}_{(e_x)}(\rho_g) = (a_{ij})_{i,j}$, alors le terme diagonal correspondant à $\rho_g(e_x)$ sera égal à 1 si et seulement si $g \cdot x = x$ si et seulement si x est un point fixe de g . Sinon il vaudra 0. Donc

$$\chi_\rho(g) = \text{Tr}(\rho_g) = \#\{x \in X \mid g \cdot x = x\}.$$

2. Caractère de la représentation régulière (c'est le cas particulier de la représentation de permutations ρ avec G fini, $X = G$, l'action étant la multiplication dans G).

On a alors, pour tout $g \in G$:

$$\chi_\rho(g) = \text{Tr}(\rho_g) = \# \{x \in G \mid gx = x\} = \begin{cases} |G| & \text{si } g = e \\ 0 & \text{si } g \neq e. \end{cases} \quad (2.1)$$

Définition 2.3.2. Un caractère d'un groupe G est dit **irréductible** si c'est le caractère d'une représentation irréductible de G .

2.4 Orthogonalité des caractères irréductibles

Soit G un groupe fini. On considère le \mathbb{C} -espace vectoriel $\mathcal{F}(G)$ des fonctions définies sur G et à valeurs dans \mathbb{C} . On munit le \mathbb{C} -espace vectoriel $\mathcal{F}(G)$ d'une structure hermitienne donnée par le produit scalaire suivant : pour $\varphi, \psi \in \mathcal{F}(G)$, on a

$$\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g).$$

Remarque. Si $f \in \mathcal{F}(G)$, alors

$$f = \sum_{g \in G} \lambda \text{Ind}_g = \sum_{g \in G} f(g) \text{Ind}_g,$$

où

$$\begin{aligned} \text{Ind}_g : G &\longrightarrow \mathbb{C} \\ x &\longmapsto \begin{cases} 1 & \text{si } x = g \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Donc $(\text{Ind}_g)_{g \in G}$ est une base de $\mathcal{F}(G)$. En particulier, $\dim_{\mathbb{C}}(\mathcal{F}(G)) = |G|$.

Lemme (De Schur). Soit $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$ deux représentations linéaires irréductibles d'un groupe fini G . Soit $f : V \longrightarrow V'$ une application linéaire vérifiant :

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

1. Si ρ et ρ' ne sont pas isomorphes, alors $f = 0$.
2. Si ρ et ρ' sont isomorphes, alors f est une homothétie.

Démonstration.

1. Montrons la contraposée : on suppose que f n'est pas l'application nulle.

Le sous-espace $\text{Ker}(f)$ de V est stable par ρ . En effet, si $g \in G$ et si $x \in \text{Ker}(f)$, alors $\rho_g(x) \in \text{Ker}(f)$, car :

$$f(\rho_g(x)) = (f \circ \rho_g)(x) = (\rho'_g \circ f)(x) = \rho'_g(f(x)) = \rho'_g(0) = \rho'_g(0) = 0.$$

Comme $f \neq 0$, i. e. $\text{Ker}(f) \neq V$, on en déduit que $\text{Ker}(f) = \{0\}$ par irréductibilité de ρ .

De même, le sous-espace $\text{Im}(f)$ de V' est stable par ρ' . En effet, si $g \in G$ et $y = f(x) \in \text{Im}(f)$, alors $\rho'_g(y) \in \text{Im}(f)$, car

$$\rho'_g(y) = \rho'_g(f(x)) = (\rho'_g \circ f)(x) = (f \circ \rho_g)(x) = f(\rho_g(x)).$$

Puisque $f \neq 0$ (i. e. $\text{Im}(f) \neq \{0\}$), on en déduit que $\text{Im}(f) = V'$ par irréductibilité de ρ' .

En conclusion, f est bijective. Donc f est un isomorphisme et donc ρ et ρ' sont deux représentations isomorphes.

2. On suppose que $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$. On peut donc identifier V et V' (et ρ et ρ'). Puisque \mathbb{C} est algébriquement clos (théorème de d'Alembert-Gauss), l'endomorphisme $f : V \longrightarrow V$ admet une valeur propre $\lambda \in \mathbb{C}$. Le sous-espace propre $\text{SEP}(f, \lambda)$ de f pour la valeur propre λ est stable par ρ .

En effet, si $g \in G$ et si $x \in \text{SEP}(f, \lambda)$, alors $\rho_g(x) \in \text{SEP}(f, \lambda)$, car

$$f(\rho_g(x)) = \rho_g(f(x)) = \rho_g(\lambda x) = \lambda \rho_g(x).$$

Donc $\underbrace{\text{SEP}(f, \lambda)}_{\neq \{0\}} = V$ par irréductibilité de ρ . D'où, $\forall x \in V, f(x) = \lambda x$, i. e. f est une homothétie de rapport λ .

□

Proposition 2.4.1. Les caractères irréductibles d'un groupe G forment un système orthonormal de fonctions de l'espace vectoriel hermitien $\mathcal{F}(G)$, i. e.

$$\langle \chi, \chi' \rangle = \begin{cases} 1 & \text{si } \chi = \chi' \\ 0 & \text{sinon,} \end{cases}$$

si χ, χ' ne sont pas des caractères irréductibles de G .

Démonstration. Soient $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$ deux représentations irréductibles de G et soient χ et χ' leurs caractères associés.

Soit $g \in G$, notons $\text{Mat}(\rho_g) = (a_{ij}(g))_{1 \leq i, j \leq d}$, $\text{Mat}(\rho'_g) = (a'_{ij}(g))_{1 \leq i, j \leq d'}$, où $d = \deg(\chi) = \dim(V)$ et $d' = \deg(\chi') = \dim(V')$. On a :

$$\chi(g) = \text{Tr}(\rho_g) = \sum_{i=1}^d a_{ii}(g) \text{ et } \chi'(g) = \sum_{i=1}^{d'} a'_{ii}(g).$$

D'où

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) = \frac{1}{|G|} \sum_{g \in G} \sum_{i, j} \overline{a_{ii}(g)} a'_{ii}(g) = \begin{cases} 0 & \text{si } \rho \text{ et } \rho' \text{ non isomorphes,} \\ 1 & \text{si } \rho \text{ et } \rho' \text{ son isomorphes.} \end{cases}$$

□

03-10-2023

Exercice 5. On note \hat{G} l'ensemble des caractères linéaires d'un groupe G , i. e. l'ensemble des morphismes $\chi : G \longrightarrow \mathbb{C}^*$ (ce sont les caractères des représentations de degré 1 (donc irréductibles) de G). On définit le produit $\chi\chi'$ de deux caractères linéaires de G : pour $g \in G$,

$$(\chi\chi')(g) = \chi(g)\chi'(g).$$

1. Montrer que \hat{G} , muni de ce produit, est un groupe abélien.

2. On rappelle que le caractère trivial est défini par :

$$\begin{aligned} \chi_0 : G &\longrightarrow \mathbb{C}^* \\ g &\longmapsto 1. \end{aligned}$$

Montrer que si G est fini et si $\chi \in \hat{G}$, alors

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & \text{si } \chi = \chi_0 \\ 0 & \text{sinon.} \end{cases}$$

3. En déduire les relations d'orthogonalité des caractères linéaires : si $\chi, \chi' \in \hat{G}$, alors

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) = \begin{cases} 1 & \text{si } \chi = \chi' \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.

1. ★ Le produit est bien une loi de composition interne dans \hat{G} car si $\chi, \chi' \in \hat{G}$, alors $\chi\chi' : G \longrightarrow \mathbb{C}^*$ est bien un morphisme de groupes.
En effet, si $g, g' \in G$, alors

$$(\chi\chi')(gg') = \chi(gg')\chi'(gg') = \chi(g)\chi(g')\chi'(g)\chi'(g') = (\chi(g)\chi'(g))(\chi(g')\chi'(g')) = (\chi\chi')(g)(\chi\chi')(g').$$

★ La loi est associative, car la multiplication l'est dans \mathbb{C} .

★ L'application $\chi_0 : \begin{matrix} G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & 1 \end{matrix}$ est bien un morphisme de groupes et est l'élément neutre de \hat{G} .

★ Si $\chi \in \hat{G}$, alors le caractère linéaire $\chi' : G \longrightarrow \mathbb{C}^*$ défini par

$$\chi'(g) = \frac{1}{\chi(g)} = (\chi'(g))^{-1} = \chi(g^{-1})$$

vérifie $\chi\chi' = \chi_0 = \chi'\chi$, et donc $\chi^{-1} = \chi'$ est le symétrique de χ dans \hat{G} , car χ^{-1} est encore un morphisme de groupes. En effet, si $g, g' \in G$, alors

$$\chi^{-1}(gg') = \chi((gg')^{-1}) = \chi((g')^{-1}g^{-1}) = \chi((g')^{-1})\chi(g^{-1}) = \chi^{-1}(g')\chi^{-1}(g) = \chi^{-1}(g)\chi^{-1}(g').$$

De plus, $\chi\chi' = \chi'\chi, \forall \chi, \chi' \in \hat{G}$, c'est-à-dire \hat{G} est un groupe abélien.

2. Si $\chi = \chi_0$, alors

$$\frac{1}{|G|} \sum_{g \in G} \chi_0(g) = \frac{1}{|G|} \sum_{g \in G} 1 = 1.$$

Soit maintenant $\chi \in \hat{G}$ tel que $\chi \neq \chi_0$. Il existe alors $a \in G$ tel que $\chi(a) \neq 1$. On a :

$$\frac{\chi(a)}{|G|} \sum_{g \in G} \chi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(a)\chi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(ag) = \frac{1}{|G|} \sum_{g \in G} \chi(g),$$

car l'application f_a définie par $f_a : \begin{matrix} G & \longrightarrow & G \\ g & \longmapsto & ag \end{matrix}$ est une bijection. D'où :

$$(\chi(a) - 1) \left(\frac{1}{|G|} \sum_{g \in G} \chi(g) \right) = 0.$$

Cette égalité a lieu dans \mathbb{C} qui est un corps, donc en particulier un anneau intègre et donc ne contient pas de diviseurs de 0. Or $\chi(a) - 1 \neq 0$, car $\chi(a) \neq 1$. Donc

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = 0.$$

3. Si $\chi \in \hat{G}$, alors on a :

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi(g) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\chi(g)} \chi(g),$$

car, G étant fini, on a pour tout $g \in G$, $g^{|G|} = e$ (par le théorème de Lagrange) et donc $\chi(g^{|G|}) = \chi(g)^{|G|}$, donc $\chi(g)$ est une racine de l'unité dans \mathbb{C} ! En particulier, $\chi(g)$ est un nombre complexe de module 1, et donc son conjugué est égal à son inverse

$$\overline{\chi(g)} = \frac{1}{\chi(g)}.$$

$$\text{Donc } \langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} 1 = \frac{|G|}{|G|} = 1.$$

Soient $\chi, \chi' \in \hat{G}$ tels que $\chi \neq \chi'$. Il existe donc $a \in G$ tel que $\chi(a) \neq \chi'(a)$. On a :

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(ag)} \chi'(ag)$$

grâce au même argument que dans la question précédente. D'où

$$\begin{aligned} \langle \chi, \chi' \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(a) \chi(g) \chi'(a) \chi'(g) \\ &= \frac{\overline{\chi(a)} \chi'(a)}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) = \overline{\chi(a)} \chi'(a) \langle \chi, \chi' \rangle, \end{aligned}$$

d'où $(\overline{\chi(a)} \chi'(a) - 1) \langle \chi, \chi' \rangle = 0$. On a donc $\overline{\chi(a)} \chi'(a) - 1 = 0$ ou $\langle \chi, \chi' \rangle = 0$. Or $\overline{\chi(a)} \chi'(a) = 1 \iff \chi'(a) = \frac{1}{\overline{\chi(a)}} = \chi(a)$. Or on a $\chi'(a) \neq \chi(a)$. Donc $\langle \chi, \chi' \rangle = 0$.

□

2.5 Théorème de Frobenius

Soit G un groupe et soit $\mathcal{F}(G) = \{\text{fonctions } f : G \longrightarrow \mathbb{C}\}$ l'ensemble des fonctions définies sur G à valeurs dans \mathbb{C} . Les fonctions $\mathcal{F}(G)$ qui sont **constantes** sur **les classes de conjugaison** de G sont appelées fonctions **centrales** sur G . On note $\mathcal{F}_C(G)$ l'ensemble des fonctions centrales :

$$\mathcal{F}_C(G) := \{f : G \longrightarrow \mathbb{C}^*, \forall g, h \in G, f(ghg^{-1}) = f(h)\}.$$

On a vu que les caractères χ_ρ des représentations ρ de G sont des fonctions centrales sur G . $\mathcal{F}_C(G)$ est un sous-espace vectoriel de $\mathcal{F}(G)$.

Théorème 2.5.1 (De Frobenius). *Les caractères **irréductibles** d'un groupe G forment une **base orthonormale** de l'espace $\mathcal{F}_C(G)$ de fonctions centrales sur G .*

Sketch of proof. On a déjà vu que les caractères irréductibles forment un système libre de fonctions de $\mathcal{F}_C(G)$ (proposition 2.4.1). Notons F le sous-espace vectoriel engendré par les caractères irréductibles de G . L'idée de la preuve est de vérifier que l'orthogonal F^\perp de F est réduit à 0 en utilisant le lemme de Schur (cf 2.4). \square

Corollaire 1. *Le nombre de (classes d'isomorphismes de) représentations irréductibles d'un groupe G est égal au nombre de classes de conjugaison de G .*

Démonstration. D'après le théorème de Frobenius, le nombre de représentations irréductibles d'un groupe G est égal à la dimension de l'espace vectoriel $\mathcal{F}_C(G)$ des fonctions centrales sur G . Or une fonction est centrale si et seulement si elle est constante sur chaque classe de conjugaison ; une fonction centrale $\phi : G \rightarrow \mathbb{C}$ peut donc s'écrire de manière unique sous la forme :

$$\phi = \sum_{C \in \text{Conj}(G)} \lambda_C 1_C,$$

où $\text{Conj}(G)$ est l'ensemble de classes de conjugaison de G et 1_C est la fonction indicatrice de C , i. e. $1_C(g) = \begin{cases} 1 & \text{si } g \in C \\ 0 & \text{sinon} \end{cases}$ et où $\lambda_C \in \mathbb{C}$ (on a $\lambda_C = \phi(g)$ où g est n'importe quel élément de C). Les fonctions indicatrices 1_C , pour $C \in \text{Conj}(G)$, forment donc une base de $\mathcal{F}_C(G)$, qui, de ce fait, est de dimension le cardinal de $\text{Conj}(G)$. \square

Remarque (Notation). Si G est un groupe fini, on note $\text{Irr}(G)$ l'ensemble des (classes d'isomorphismes de) représentations irréductibles de G qu'on identifie parfois à l'espace de ces représentations irréductibles.

$$\begin{aligned} \text{Irr}(G) &= \{ \rho : G \rightarrow W, \text{ représentations irréductibles de } G \text{ à isomorphisme près} \} \\ &= \{ \mathbb{C} - \text{espaces vectoriels } W, \text{ espaces des représentations irréductibles de } G \}. \end{aligned}$$

Corollaire 2 (Décomposition canonique d'une représentation). *Si $\rho : G \rightarrow GL(V)$ est une représentation de G , et si $V = W_1 \oplus \dots \oplus W_k$ est une décomposition de V en somme directe de représentations irréductibles de G (i. e. $\rho = \rho_1 \oplus \dots \oplus \rho_k : G \rightarrow GL(W_1 \oplus \dots \oplus W_k)$, avec $\rho_i : G \rightarrow GL(W_i)$ représentation irréductible pour $i \in \{1, \dots, k\}$) et si $W \in \text{Irr}(G)$, alors le nombre m_W de W_i qui sont isomorphes à W (i. e. l'ordre de multiplicité de W dans cette représentation) est égal à $\langle \chi_W, \chi_V \rangle$ où χ_W et χ_V sont les caractères associés aux représentations de G d'espaces W et V .*

En particulier, il ne dépend de la décomposition et

$$V \simeq \bigoplus_{W \in \text{Irr}(G)} \langle \chi_W, \chi_V \rangle W.$$

Démonstration. On a

$$\chi_V = \chi_{W_1} + \dots + \chi_{W_k}.$$

D'où

$$\langle \chi_W, \chi_V \rangle = \langle \chi_W, \chi_{W_1} \rangle + \dots + \langle \chi_W, \chi_{W_k} \rangle.$$

$$\text{Or } \langle \chi_W, \chi_{W_i} \rangle = \begin{cases} 1 & \text{si } W_i \simeq W \\ 0 & \text{sinon.} \end{cases}$$

$$\text{Donc } \langle \chi_W, \chi_V \rangle = m_W. \quad \square$$

Corollaire 3 (Les caractères caractérisent les représentations). *Deux représentations d'un même groupe fini sont isomorphes si et seulement si elles ont même caractère.*

Démonstration. D'après le corollaire 2, si $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$ sont deux représentations de G ayant même caractère χ alors V et V' sont tous les deux isomorphes à :

$$\bigoplus_{W \in \text{Irr}(G)} \langle \chi_W, \chi \rangle W.$$

Réciproquement, si ρ et ρ' sont isomorphes, alors $\chi_\rho = \chi_{\rho'}$ (déjà vu). \square

Corollaire 4 (Critère d'irréductibilité). *Une représentation $\rho : G \longrightarrow GL(V)$ d'un groupe G est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$ où χ est le caractère de ρ .*

Démonstration. Si $V \simeq \bigoplus_{W \in \text{Irr}(G)} m_W W$, alors

$$\langle \chi_V, \chi_V \rangle = \left\langle \sum_{w \in \text{Irr}(G)} m_W \chi_W, \sum_{w \in \text{Irr}(G)} m_W \chi_W \right\rangle = \sum_{w \in \text{Irr}(G)} m_W^2,$$

car les caractères irréductibles de G forment une base orthonormale de l'espace vectoriel des fonctions centrales sur G par le théorème de Frobenius. Puisque les $m_W \in \mathbb{N}$, on en déduit que :

$\langle \chi_V, \chi_V \rangle = 1$ ssi tous les m_W sont égaux à 0 sauf un qui est égal à 1
ssi $V \simeq W$ ssi $V \in \text{Irr}(G)$ ssi $\rho : G \longrightarrow GL(V)$ est une représentation irréductible. \square

Corollaire 5 (Formule de Burnside). *Si G est un groupe fini, alors on a :*

$$\sum_{W \in \text{Irr}(G)} (\dim(W))^2 = |G|.$$

Démonstration. Soit G un groupe fini. Considérons le \mathbb{C} -espace vectoriel $V = \mathcal{F}(G)$ des fonctions définies sur G et à valeurs dans \mathbb{C} .

Une base de V est donnée par les fonctions indicatrices des éléments de G : pour $x \in G$, on considère la fonction indicatrice de $\{x\}$, à savoir la fonction

$$\begin{aligned} \varepsilon_x : G &\longrightarrow \mathbb{C} \\ y &\longmapsto \delta_{xy} = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Toute fonction $f : G \longrightarrow \mathbb{C}$ s'écrit alors de manière unique sous la forme :

$$f = \sum_{x \in G} f(x) \varepsilon_x.$$

La famille $\{\varepsilon_x\}$ est donc une base du \mathbb{C} -espace vectoriel $V = \mathcal{F}(G)$ de dimension égale à l'ordre de G :

$$V = \bigoplus_{x \in G} \mathbb{C}\varepsilon_x.$$

Considérons la représentation régulière de G , à savoir la représentation d'espace $V = \mathcal{F}(G)$ donnée par

$$\begin{aligned} \rho : G &\longrightarrow GL(V) \\ g &\longmapsto \rho_g : \begin{pmatrix} V &\longrightarrow V \\ \varepsilon_x &\longmapsto \varepsilon_{gx} \end{pmatrix}. \end{aligned}$$

Montrons que si W est une représentation irréductible de G , alors W apparaît dans la représentation régulière de G avec la multiplicité $\dim(W)$.

En effet, le caractère χ de la représentation régulière est donné par :

$$\chi(e) = |G| \text{ et } \chi(g) = 0 \text{ pour tout } g \in G \setminus \{e\}.$$

Or, d'après le corollaire 2, la multiplicité de W dans V est égale à :

$$\langle \chi_W, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_W(g)} \chi(g) = \frac{1}{|G|} \overline{\chi_W(e)} |G| = \overline{\chi_W(e)} = \dim(W).$$

On en déduit que

$$\chi = \sum_{W \in \text{Irr}(G)} (\dim(W)) \cdot \chi_W.$$

En appliquant cette égalité à $g = e$, on trouve :

$$|G| = \chi(e) = \sum_{W \in \text{Irr}(G)} \dim(W) \chi_W(e) = \sum_{W \in \text{Irr}(G)} (\dim(W))^2.$$

□

2.6 Le cas des groupes abéliens

Théorème 2.6.1 (Le cas commutatif). *Si G est abélien, alors toute représentation irréductible de G est de degré 1. Autrement dit, $\text{Irr}(G)$ coïncide avec l'ensemble \hat{G} des caractères linéaires de G .*

Démonstration. Soit G un groupe abélien fini. Les classes de conjugaison de G sont toutes réduites à un élément. Il y a donc autant de classes de conjugaison dans G que d'éléments de G .

Si l'on note $\text{Conj}(G)$ l'ensemble des classes de conjugaison de G , on a donc $\# \text{Conj}(G) = |G|$.

Or, d'après le corollaire 1, on a $\# \text{Irr}(G) = \# \text{Conj}(G)$. De plus, d'après la formule de Burnside, on a :

$$\sum_{W \in \text{Irr}(G)} (\dim(W))^2 = |G|.$$

Or, on a $\dim(W) \geq 1$ pour tout $W \in \text{Irr}(G)$ et puisqu'il y a $|G|$ éléments dans $\text{Irr}(G)$, on en déduit que $\dim(W) = 1, \forall W \in \text{Irr}(G)$. □

Corollaire 6. *Si G est abélien, alors toute fonction de G dans \mathbb{C} est combinaison linéaire de caractères linéaires.*

Démonstration. D'après le théorème de Frobenius, toute fonction centrale (et donc toute fonction puisque G est abélien) est combinaison linéaire de caractères irréductibles. Le théorème précédent permet de conclure. \square

Remarque. Comme les caractères linéaires d'un groupe abélien G forment une base orthonormale des fonctions de G dans \mathbb{C} , il est facile de décomposer une fonction quelconque comme une combinaison linéaire de caractères linéaires. Si ϕ est une fonction sur G , on définit la transformée de Fourier $\hat{\phi}$ comme la fonction définie sur \hat{G} par :

$$\hat{\phi}(x) = \langle \chi, \phi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \phi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g)^{-1} \phi(g).$$

La formule d'inversion de Fourier s'exprime alors sous la forme :

$$\phi = \sum_{\chi \in \hat{G}} \hat{\phi}(\chi) \chi.$$

C'est la conséquence immédiate du fait que les χ , pour $\chi \in \hat{G}$, forment une famille orthonormale. Par exemple, si on applique ce qui précède à la fonction

$$\begin{aligned} \phi_a : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \begin{cases} 1 & \text{si } g = a \\ 0 & \text{sinon} \end{cases}, \end{aligned}$$

on a :

$$\phi_a(\chi) = \frac{1}{|G|} \overline{\chi(a)}$$

et on obtient

$$\frac{1}{|G|} \sum_{x \in \hat{G}} \overline{\chi(a)} \chi(x) = \begin{cases} 1 & \text{si } x = a \\ 0 & \text{sinon.} \end{cases}$$

Exercice 6. Ecrire la table de caractères irréductibles de $\mathbb{Z}/2\mathbb{Z}$.

Démonstration. Le groupe $\mathbb{Z}/2\mathbb{Z}$ est abélien. Ses représentations irréductibles sont toutes de degré 1. Elles coïncident donc avec leurs caractères linéaires. Leur nombre est égal à celui des classes de conjugaison de $\mathbb{Z}/2\mathbb{Z}$, à savoir 2, car $\mathbb{Z}/2\mathbb{Z}$ est abélien. Les représentations irréductibles de $\mathbb{Z}/2\mathbb{Z}$ les représentations irréductibles de degré 1, à savoir les morphismes de groupes : $\rho : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^*$.

On a la représentation triviale :

$$\begin{aligned} \rho_0 : \mathbb{Z}/2\mathbb{Z} &\longrightarrow \mathbb{C}^* \\ \bar{0} &\longmapsto 1 \\ \bar{1} &\longmapsto 1 \end{aligned}$$

dont le caractère est $\chi_0 = \rho_0$.

De plus, $\rho(\bar{1})^2 = \rho(\bar{1} + \bar{1}) = \rho(\bar{0}) = 1$. Donc $\rho(\bar{1})$ est une racine carrée de 1 dans \mathbb{C} , i. e. vaut 1 ou -1. L'autre représentation irréductible de $\mathbb{Z}/2\mathbb{Z}$ est donc :

$$\begin{aligned} \rho : \mathbb{Z}/2\mathbb{Z} &\longrightarrow \mathbb{C}^* \\ \bar{0} &\longmapsto 1 \\ \bar{1} &\longmapsto -1 \end{aligned}$$

et son caractère coïncide avec ρ . La table des caractères irréductibles de $\mathbb{Z}/2\mathbb{Z}$ est donc :

	Conjug($\bar{0}$) = $\bar{0}$	Conjug($\bar{1}$) = $\bar{1}$
χ_0	1	1
χ	1	-1

\square

Exercice 7. Ecrire la table des caractères irréductibles de $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

Exercice 8. Déterminer les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 1$.

Démonstration. Le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ est abélien, il admet donc n représentations irréductibles à isomorphisme près (car il possède n classes de conjugaison). De plus, par la formule de Burnside,

$$\sum_{W \in \text{Irr}(\mathbb{Z}/n\mathbb{Z})} (\dim(W))^2 = \mathbb{Z}/n\mathbb{Z} = n.$$

On en déduit que les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ sont toutes de degré 1.

Elles coïncident donc avec les caractères linéaires de $\mathbb{Z}/n\mathbb{Z}$, à savoir les morphismes de groupes $\chi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^*$. Or, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique et est engendré par $\bar{1}$ (où $\bar{a} = a + n\mathbb{Z}$).

Le morphisme χ est donc entièrement déterminé par la valeur $\chi(\bar{1})$ de χ en $\bar{1}$.

De plus, on a : $\chi(\bar{n}) = \chi(\underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{n \text{ fois}}) = \chi(\bar{1})^n$. Donc $\chi(\bar{1})$ est une racine n -ième de l'unité dans

\mathbb{C} . Il existe donc $k \in \{0, \dots, n-1\}$ tel que $\chi(\bar{1}) = e^{\frac{2ik\pi}{n}}$.

On a alors, pour tout $r : \chi(\bar{r}) = \chi(\bar{1})^r = e^{\frac{2ik\pi r}{n}} =: \chi_k(\bar{r})$. On obtient donc les n représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ en considérant $\chi_0, \dots, \chi_{n-1}$ définis par

$$\begin{aligned} \chi_k : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{C}^* \\ \bar{r} &\longmapsto \chi_k(\bar{r}) = e^{\frac{2ik\pi r}{n}}. \end{aligned}$$

C'est aussi la liste des caractères irréductibles de $\mathbb{Z}/n\mathbb{Z}$. χ_0 est alors le caractère trivial de $\mathbb{Z}/n\mathbb{Z}$. \square

Remarque. L'ensemble $\widehat{\mathbb{Z}/n\mathbb{Z}}$ des caractères de $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la loi

$$\chi_k \cdot \chi_{k'} = \chi_{k+k' \pmod n}.$$

Le groupe $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est cyclique d'ordre n , engendré par

$$\begin{aligned} \chi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{C}^* \\ \bar{r} &\longmapsto \chi_k(\bar{r}) = e^{\frac{2i\pi r}{n}}. \end{aligned}$$

2.7 Nombre de représentations irréductibles de degré 1

Définition 2.7.1. Soit G un groupe. Un **commutateur** de G est un élément de la forme :

$$xyx^{-1}y^{-1} \text{ avec } x, y \in G.$$

Définition 2.7.2. Soit G un groupe. Le **groupe dérivé** de G , noté $D(G)$ ou G' est le sous-groupe de G engendré par les commutateurs :

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

Remarque. $D(G)$ est donc le plus petit sous-groupe de G contenant tous les commutateurs de G .

Proposition 2.7.1. Soit G un groupe.

1. On a $D(G) = \{e\}$ si et seulement si G est abélien.
2. On a que $D(G) \triangleleft G$.
3. Soit $H \triangleleft G$. On a G/H est abélien si et seulement si $D(G) \subset H$.

Démonstration.

1. Si G est abélien, alors tous les commutateurs de G sont égaux à e et donc $D(G) = \langle e \rangle = \{e\}$. Réciproquement, si $D(G) = \{e\}$, alors tous les commutateurs de G valent e , i. e. $\forall x, y \in G, xyx^{-1}y^{-1} = e$, i. e. $\forall x, y \in G, xy = yx$, i. e. G est abélien.
2. $D(G)$ est stable par tout automorphisme (on dit que $D(G)$ est un sous-groupe caractéristique de G), car si $f \in \text{Aut}(G)$, on a :

$$\forall x, y \in G, f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1}$$

qui est encore un commutateur. Donc, a fortiori, $D(G)$ est stable par tout automorphisme intérieur de G (i. e. les automorphismes de la forme $f_g : \begin{matrix} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{matrix}$ pour $g \in G$). Donc $D(G) \triangleleft G$.

3. On a :

$$\begin{aligned} D(G) \subset H &\iff \forall x, y \in G, xyx^{-1}y^{-1} \in H \iff \forall x, y \in G, xy(yx)^{-1} \in H \\ &\iff \forall x, y \in G, Hxy = Hyx \iff \forall x, y \in G, HxHy = HyHx \iff \forall x, y \in G, \overline{xy} = \overline{yx}, \end{aligned}$$

où $\bar{a} = Ha = aH$, car $H \triangleleft G$. Donc G/H est abélien.

□

Remarque. On a donc $G/D(G)$ est abélien.

Exercice 9. Déterminer $D(\mathfrak{A}_3), D(\mathfrak{S}_3), D(\mathfrak{A}_4), D(\mathfrak{S}_4)$.

Démonstration.

1. $|\mathfrak{A}_3| = \frac{3!}{2} = 3$, or 3 est premier, donc \mathfrak{A}_3 est **cyclique**, donc **abélien**.
2. On a $D(\mathfrak{S}_3) \triangleleft \mathfrak{S}_3$. Or les seuls sous-groupes distingués de \mathfrak{S}_3 sont $\{id\}, \mathfrak{S}_3, \mathfrak{A}_3$. Donc $D(\mathfrak{S}_3) = \{e\}$ ou $D(\mathfrak{S}_3)\mathfrak{S}_3$ ou $D(\mathfrak{S}_3) = \mathfrak{A}_3$.
Or \mathfrak{S}_3 n'est pas abélien, donc $D(\mathfrak{S}_3) \neq \{id\}$. De plus, la signature d'un commutateur est égale à 1, car la signature est un morphisme de groupes et donc, pour tous $x, y \in G$:

$$\varepsilon(xyx^{-1}y^{-1}) = \varepsilon(x)\varepsilon(y)\varepsilon(x^{-1})\varepsilon(y^{-1}) = \varepsilon(x)\varepsilon(x^{-1})\varepsilon(y)\varepsilon(y^{-1}) = \varepsilon(e)\varepsilon(e) = 1.$$

D'où $D(\mathfrak{S}_3) \subset \mathfrak{A}_3$. Donc $D(\mathfrak{S}_3) = \mathfrak{A}_3$.

3. Quels sont les sous-groupes distingués de \mathfrak{A}_4 ?

Remarque. D'après le théorème de Galois, \mathfrak{A}_n est simple si et seulement si $n \neq 4$, i. e. \mathfrak{A}_n n'admet pas de sous-groupes distingués propres si et seulement si $n \neq 4$.

On en déduit que \mathfrak{A}_4 n'est pas simple. Déterminons la partition de \mathfrak{A}_4 en classes de conjugaison :

$$\mathfrak{A}_4 = \{e\} \cup \{3\text{-cycles}\} \cup \{\text{type } (2, 2)\}.$$

Les types $(2, 2)$ de \mathfrak{A}_4 , à savoir les produits de deux transpositions à support disjoint sont :

$$(12)(34), (13)(24), (14)(23).$$

Le sous-groupe $V = \{id, (12)(34), (13)(24), (14)(23)\}$ est distingué dans \mathfrak{A}_4 , car stable par conjugaison : $V \triangleleft \mathfrak{A}_4$.

On montre que c'est le seul sous-groupe distingué propre de \mathfrak{A}_4 .

On en déduit que $D(\mathfrak{A}_4) = \{e\}$ ou $D(\mathfrak{A}_4) = V$ ou $D(\mathfrak{A}_4) = \mathfrak{A}_4$. Or \mathfrak{A}_4 n'est pas abélien, donc $D(\mathfrak{A}_4) \neq \{e\}$.

Considérons le groupe quotient \mathfrak{A}_4/V . Il est d'ordre

$$|\mathfrak{A}_4/V| = \frac{|\mathfrak{A}_4|}{|V|} = \frac{12}{4} = 3,$$

premier, donc est cyclique, donc est abélien. On en déduit que $D(\mathfrak{A}_4) \subset V$. Donc $D(\mathfrak{A}_4) = V$. \square

Exercice 10. Montrer que, pour $n > 4$, on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Remarque. On a $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$, car les 3-cycles sont des commutateurs. En effet,

$$(abc) = \tau\sigma\tau^{-1}\sigma^{-1},$$

avec $\tau = (bc)$ et $\sigma = (ab)$. Or, \mathfrak{A}_n est engendré par les 3-cycles. D'où $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$.

Démonstration. Puisque les commutateurs ont pour signature 1, on a donc $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$. Donc $D(\mathfrak{S}_n) = \mathfrak{A}_n$. Enfin, $D(\mathfrak{A}_n) \triangleleft \mathfrak{A}_n$. Par le théorème de Galois, \mathfrak{A}_n est simple si et seulement si $n \neq 4$. Donc $D(\mathfrak{A}_n) = \{e\}$ ou \mathfrak{A}_n . Or, \mathfrak{A}_n n'est pas abélien pour $n > 4$, donc $D(\mathfrak{A}_n) \neq \{e\}$. Donc $D(\mathfrak{A}_n) = \mathfrak{A}_n$. \square

Remarque. $\mathfrak{A}_4 \subset D(\mathfrak{S}_4)$ par la remarque précédente. Or $D(\mathfrak{S}_4) \neq \mathfrak{S}_4$, car $D(\mathfrak{S}_4) \subset \mathfrak{A}_4$. Donc $D(\mathfrak{S}_4) = \mathfrak{A}_4$.

Proposition 2.7.2. Soit $f : G \longrightarrow G'$ un morphisme de groupes et soit H un sous-groupe distingué de G . Le morphisme f se factorise par la surjection canonique

$$\pi : G \longrightarrow G/H$$

(i. e. il existe un morphisme $\psi : G/H \longrightarrow G'$ tel que $f = \psi \circ \pi$) si et seulement si $H \subset \text{Ker}(f)$.

Démonstration. Si f se factorise, alors pour tout $h \in H$, on a

$$f(h) = (\psi \circ \pi)(h) = \psi(\pi(h)) = \psi,$$

donc $h \in \text{Ker}(f)$, donc $H \subset \text{Ker}(f)$.

Réciproquement, si $H \subset \text{Ker}(f)$, alors pour $x \in G$, $f(x)$ ne dépend que de la classe xH de x . En effet, si $xH = x'H$, alors $x^{-1}x' \in H$. Or $H \subset \text{Ker}(f)$, donc $x^{-1}x' \in \text{Ker}(f)$, donc $f(x^{-1}x') = e'$, i. e. $f(x)^{-1}f(x') = e'$, i. e. $f(x') = f(x)$. Donc la formule $\psi(xH) = f(x)$ définit bien une application $\psi : G/H \longrightarrow G'$ qui est bien un morphisme. \square

Théorème 2.7.1. Si G est un groupe fini, le nombre de ses (classes d'isomorphismes de) représentations irréductibles de degré 1 est égal à l'indice $[G : D(G)]$ dans G .

Démonstration. Soit ρ une représentation irréductible de degré 1 de G et χ le caractère (linéaire) de degré 1 associé ($\chi = \rho$) :

$$\chi : G \longrightarrow \mathbb{C}^*.$$

On a $\chi(G) \subset \mu_n(\mathbb{C})$, où $n = |G|$.

Puisque (\mathbb{C}^*, \times) est un groupe abélien, on a donc que $\chi(G)$ est abélien. D'après le premier théorème d'isomorphisme, on a :

$$G/\text{Ker}(\chi) \simeq \text{Im}(\chi) = \chi(G).$$

On en déduit que le quotient $G/\text{Ker}(\chi)$ est abélien. D'après le 3 de la proposition sur les groupes dérivés 2.7.1, cela entraîne que $D(G) \subset \text{Ker}(\chi)$.

On en déduit par la proposition 2.7.2 que le morphisme χ se factorise par $G/D(G)$:

$$\begin{array}{ccc} G & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \pi & \swarrow \check{\chi} \\ & C & \end{array} \quad \circ$$

Il y a donc une bijection entre l'ensemble des représentations irréductibles de degré 1 de G et l'ensemble des représentations irréductibles de degré 1 de $G/D(G)$:

$$\begin{array}{ccc} \sim : \{ \text{rep. irréductibles de degré 1 de } G \} & \xrightarrow{\chi} & \{ \text{rep. irréductibles de degré 1 de } G/D(G) \} \\ & \longmapsto & \check{\chi}. \end{array}$$

Remarque. C'est une bijection, car si $\psi : G/D(G) \rightarrow \mathbb{C}^*$ est une représentation irréductible de degré 1 de $G/D(G)$, alors $\chi : \psi \circ \pi : G \rightarrow \mathbb{C}^*$ est une représentation irréductible de degré 1 de G et $\check{\chi} = \psi$.

Or $G/D(G)$ est abélien, donc toutes ses représentations irréductibles sont de degré 1. Il y en a le nombre de classes de conjugaison de $G/D(G)$, i. e. $|G/D(G)|$, car $G/D(G)$ est abélien, i. e. $[G : D(G)]$. \square

Application Quel est le nombre de classes d'isomorphismes de représentations irréductibles de degré 1 du groupe symétrique \mathfrak{S}_n pour $n \geq 3$?

On a $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 3$. Or $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$. Donc $[\mathfrak{S}_n : D(\mathfrak{S}_n)] = 2$. \mathfrak{S}_n admet donc deux représentations irréductibles de dimension 1 (à isomorphisme près).

11-10-2023

Exercice 11. On considère le groupe symétrique \mathfrak{S}_n avec $n \geq 2$.

1. Soit $\rho : \mathfrak{S}_n \rightarrow \mathbb{C}^*$ un morphisme de groupes.
 - (a) Montrer que \mathfrak{S}_n est engendré par les transpositions.
 - (b) Si τ est une transposition, montrer que $\rho(\tau) = \pm 1 \in \{1, -1\}$.
 - (c) Montrer que si τ et τ' sont deux transpositions de \mathfrak{S}_n , alors $\rho(\tau) = \rho(\tau')$.
 - (d) En déduire que les seules représentations de degré 1 de \mathfrak{S}_n sont la représentation triviale et la signature.
2. On considère le groupe symétrique \mathfrak{S}_3 .
 - (a) Montrer que \mathfrak{S}_3 admet une unique représentation linéaire irréductible de degré 2.
 - (b) Montrer que la transposition $\tau = (2 \ 3)$ et le 3-cycle $\sigma = (1 \ 2 \ 3)$ engendrent à elles deux \mathfrak{S}_3 et que $\sigma\tau = \tau\sigma^2$.
 - (c) Soit $\rho : \mathfrak{S}_3 \rightarrow GL(V)$ une représentation linéaire irréductible de degré 2 de \mathfrak{S}_3 .
 - i. Déterminer les valeurs propres possibles de l'endomorphisme ρ_σ .
 - ii. Soit $x \in V$ un vecteur propre de ρ_σ . Montrer que $\rho_\tau(x)$ est un vecteur propre de ρ_σ . En déduire que le sous-espace vectoriel $\text{Vect}(x, \rho_\tau(x))$ est stable par la représentation ρ et qu'il est égal à V .
 - iii. Déterminer les matrices de ρ_σ et ρ_τ dans la base $\mathcal{B} = (x, \rho_\tau(x))$.
 - iv. On note χ le caractère de la représentation ρ . Quelles sont les valeurs prises par χ ? Montrer que χ est irréductible.
 - (d) Dresser la table des caractères irréductibles du groupe \mathfrak{S}_3 .

Correction.

1. (a) Toute permutation peut s'écrire comme produit de cycles (à supports disjoints). De plus, tout cycle $(i_1 \dots i_r)$ s'écrit comme produit de transpositions :

$$(i_1 \dots i_r) = (i_1 \ i_2)(i_2 \ i_3) \dots (i_{r-1} \ i_r).$$

En conclusion, toute permutation peut s'écrire comme produit de transpositions : \mathfrak{S}_n est bien engendré par les transpositions.

- (b) Puisque τ est une transposition, on a $\tau \circ \tau = \tau^2 = \text{id}$. On a :

$$1 = \rho(\text{id}) = \rho(\tau \circ \tau) \underset{\rho \text{ morphisme}}{=} \rho(\tau)\rho(\tau) = \rho(\tau)^2$$

Donc $\rho(\tau)$ est une racine carrée de 1 dans \mathbb{C} , d'où $\rho(\tau) = 1$ ou $\rho(\tau) = -1$

- (c) Puisque deux permutations de \mathfrak{S}_n sont conjuguées entre elles si et seulement si elles ont le même type, on en déduit que les transpositions (qui sont des permutations de type (2)) sont conjuguées dans \mathfrak{S}_n . Il existe donc $\sigma \in \mathfrak{S}_n$ telle que :

$$\tau' = \sigma\tau\sigma^{-1}.$$

D'où

$$\rho(\tau') = \rho(\sigma\tau\sigma^{-1}) = \rho(\sigma)\rho(\tau)\rho(\sigma^{-1}) = \rho(\sigma)\rho(\sigma^{-1})\rho(\tau),$$

car (\mathbb{C}^*, \times) est abélien.

Donc $\rho(\tau') = \rho(\tau)$.

- (d) Ou bien $\rho(\tau) = 1$ pour toute transposition de \mathfrak{S}_n et alors on aura que $\rho(\sigma) = 1$ pour tout $\sigma \in \mathfrak{S}_n$ et $\rho : \begin{matrix} \mathfrak{S}_n & \longrightarrow & \mathbb{C}^* \\ \sigma & \longmapsto & 1 \end{matrix}$ est alors la représentation triviale.

Ou bien $\rho(\tau) = -1$ pour toute transposition de \mathfrak{S}_n et alors $\rho = \varepsilon$ est le morphisme signature.

2. (a) La partition de \mathfrak{S}_3 en classes de conjugaison est la suivante : $\{\{id\}, \{\text{transpositions}\}, \{\text{3-cycles}\}\}$. On en déduit que \mathfrak{S}_3 admet 3 représentations irréductibles (à isomorphisme près).

De plus, d'après la formule de Burnside, on a

$$\sum_{W \in \text{Irr}(\mathfrak{S}_3)} (\dim(W))^2 = |\mathfrak{S}_3|.$$

De plus, \mathfrak{S}_3 admet exactement deux représentations irréductibles de degré 1. D'où

$$1^2 + 1^2 + d^2 = 6,$$

où d est le degré de la représentation irréductible non de degré 1 de \mathfrak{S}_3 . D'où $d = 2$.

En conclusion, \mathfrak{S}_3 admet 3 représentation irréductibles : deux de degré 1 et une de degré 2.

- (b) Posons $H = \langle \tau, \sigma \rangle$ le sous-groupe de \mathfrak{S}_3 engendré par τ et σ .

On a $\tau^2 = e \in H$, $\tau \in H$, $\sigma \in H$, $\sigma^2 = (1 \ 3 \ 2)$, $\sigma\tau = (1 \ 2) \in H$, $\tau\sigma = (1 \ 3) \in H$.

Conclusion : $H = \mathfrak{S}_3$, donc τ et σ engendrent \mathfrak{S}_3 .

- (c) i. Puisque σ est un 3-cycle, c'est donc un élément de \mathfrak{S}_3 d'ordre 3 et donc on a $\sigma^3 = e$. D'où $\text{id}_V = \rho(e) = \rho(\sigma^3) = \rho_{\sigma^3} = \rho(\sigma)^3 = \rho_{\sigma}^3$. D'où

$$\rho_{\sigma}^3 - \text{id}_V = 0.$$

Donc ρ_{σ} est une racine du polynôme $X^3 - 1$. Le polynôme **minimal** m de ρ_{σ} est donc un diviseur de $X^3 - 1$ et les racines de $m_{\rho_{\sigma}}$ sont précisément les valeurs propres de ρ_{σ} . Les valeurs propres de ρ_{σ} sont donc les racines cubiques de l'unité dans \mathbb{C} , à savoir appartiennent à $\{1, j, j^2\}$, avec $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

- ii. Notons $\lambda \in \{1, j, j^2\}$ la valeur propre de ρ_{σ} associée au vecteur propre x . On a :

$$\begin{aligned} \rho_{\sigma}(\rho_{\tau}(x)) &= (\rho_{\sigma} \circ \rho_{\tau})(x) = \rho_{\sigma\tau}(x) = \rho_{\tau\sigma^2}(x) = (\rho_{\tau} \circ \rho_{\sigma^2})(x) \\ &= \rho_{\tau}(\underbrace{\rho_{\sigma}(x)}_{\lambda x}) = \lambda^2 \rho_{\tau}(x). \end{aligned}$$

Donc $\rho_\tau(x)$ est un vecteur propre de ρ_σ pour la valeur propre λ^2 .

Posons $W := \text{Vect}(x, \rho_\tau(x))$ et montrons que W est stable par la représentation ρ . On doit montrer que $\forall g \in \mathfrak{S}_3, \rho_g(W) \subset W$.

Or $\mathfrak{S}_3 = \langle \tau, \sigma \rangle$. Il suffit donc de montrer que $\rho_\tau(W) \subset W$ et $\rho_\sigma(W) \subset W$.

D'une part, on a : $\rho_\tau(x) \in W$ (évident) et $\rho_\tau(\rho_\tau(x)) = \rho_{\tau^2}(x) = \rho_e(x) = \text{id}(x) = x \in W$ et donc $\rho_\tau(W) \subset W$.

D'autre part : $\rho_\sigma(x) = \lambda x \in W$ et $\rho_\sigma(\rho_\tau(x)) = \lambda^2 \rho_\tau(x) \in W$. Donc $\rho_\sigma(W) \subset W$.

Enfin, par irréductibilité de la représentation ρ d'espace V , on en déduit, puisque W est un sous-espace vectoriel de V stable par ρ , que $W = V$.

- iii. Remarquons que le vecteur propre x de ρ_τ ne peut avoir pour valeur propre $\lambda = 1$, car sinon la droite engendrée par le vecteur $x + \rho_\tau(x)$ serait invariante par la représentation ρ , ce qui contredirait l'irréductibilité de ρ .

En effet, si $y = x + \rho_\tau(x)$ et si $\lambda = 1$, alors

$$\rho_\tau(y) = \rho_\tau(x + \rho_\tau(x)) = \rho_\tau(x) + \rho_{\tau^2}(x) = \rho_\tau(x) + x = y$$

et

$$\begin{aligned} \rho_\sigma(y) &= \rho_\sigma(x + \rho_\tau(x)) = \rho_\sigma(x) + \rho_{\sigma\tau}(x) = \lambda x + \rho_\sigma(\rho_\tau(x)) \\ &= \lambda x + \lambda^2 \rho_\tau(x) \underset{\lambda=1}{=} x + \rho_\tau(x) = y. \end{aligned}$$

Quitte à remplacer x par $\rho_\tau(x)$, on peut supposer que $\lambda = j$ (car si x est vecteur propre de ρ_σ de valeur propre λ , alors $\rho_\tau(x)$ est vecteur propre de ρ_σ de valeur propre λ^2).

On calcule $\rho_\sigma(x) = jx$ et $\rho_\sigma(\rho_\tau(x)) = j^2 \rho_\tau(x)$. D'où

$$\text{Mat}_{\mathcal{B}}(\rho_\sigma) = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}.$$

De même, on a $\rho_\tau(x) = \rho_\tau(x)$ et $\rho_\tau(\rho_\tau(x)) = \rho_{\tau^2}(x) = x$, d'où

$$\text{Mat}_{\mathcal{B}}(\rho_\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

iv.

$$\begin{array}{ccc} \chi : \mathfrak{S}_3 & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & \text{Tr}(\rho_g) \\ e & \longmapsto & \text{Tr}(\text{id}) = 2 \\ \tau & \longmapsto & \text{Tr}(\text{Mat}(\rho_\tau)) = 0 \\ \sigma & \longmapsto & \text{Tr}(\text{Mat}_{\mathcal{B}}(\rho_\sigma)) = j^2 + j = -1. \end{array}$$

On a

$$\langle \chi, \chi \rangle = \frac{1}{|\mathfrak{S}_3|} \sum_{g \in \mathfrak{S}_3} \overline{\chi(g)} \chi(g) = \frac{1}{6} (2^2 + 3 \times 0^2 + 2 \times (-1)^2) = \frac{6}{6} = 1.$$

Donc χ est bien un caractère **irréductible** de \mathfrak{S}_3 .

(d) On a

$$\begin{array}{ccc} \rho_0 : \mathfrak{S}_3 & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & 1 \text{ et } \chi_0 = \rho_0, \end{array}$$

$$\begin{array}{ccc} \rho_\varepsilon : \mathfrak{S}_3 & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & \varepsilon(g) \text{ et } \chi_\varepsilon = \rho_\varepsilon, \end{array}$$

$$\begin{aligned}
\rho : \quad \mathfrak{S}_3 &\longrightarrow GL_2(\mathbb{C}) \\
\tau = (1\ 2) &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\sigma = (1\ 2\ 3) &\longmapsto \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}
\end{aligned}
\text{ avec pour caractère } \chi.$$

On obtient la table des caractères suivante :

\mathfrak{S}_3	e	$(1\ 2)_3$	$(1\ 2\ 3)_2$
χ_0	1	1	1
χ_ε	1	-1	1
χ	2	0	-1

□