Théorie des représentations

Yves Aubry
Bureau : M-147A
yves.aubry@univ-tln.fr
Joachim Asch

2023-2024

TABLE DES MATIÈRES

I Représentations linéaires des groupes finis **5**

1 Généralités sur les groupes **7**
- 1.1 Rappels . . . 7
- 1.2 Exemples de groupes . . . 9
  - 1.2.1 $(\mathbb{Z}, +)$ . . . 9
  - 1.2.2 $\mathbb{Z}/n\mathbb{Z}$ . . . 9
- 1.3 Groupe diédral . . . 10
  - 1.3.1 Description du groupe D_3 . . . 11
- 1.4 Les théorèmes de Sylow . . . 12
  - 1.4.1 Groupes agissant sur un ensemble ou action de groupes . . . 13

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 . . . 22
- 2.4 Orthogonalité des caractères irréductibles . . . 24
- 2.5 Théorème de Frobenius . . . 28
- 2.6 Le cas des groupes abéliens . . . 31
- 2.7 Nombre de représentations irréductibles de degré 1 . . . 33
- Exercices . . . 36

3 Groupes orthogonaux et unitaires **45**
- 3.1 Théorème de classification des endomorphismes orthogonaux de $\mathbb{R}^3$ . . . 45
  - 3.1.1 Cas particulier en dimension 2 et 3 . . . 46
- 3.2 Le groupe unitaire et spécial unitaire . . . 46

4 Groupes topologiques **49**

5 Algèbre d'un groupe fini **51**

II Représentations de groupes de Lie **53**

Introduction **55**
- Notations . . . 55
- Motivations . . . 55

6 Groupes de Lie matriciels (groupe de Lie linéaires) 57
6.1 Propriétés topologiques des groupes de Lie matriciels 61
6.2 Homomorphismes 65
6.3 Isomorphismes 65

7 Algèbre de Lie 67
7.1 Exponentielle et logarithme des matrices 67
7.2 Logarithme matriciel 69
7.3 Algèbre de Lie, exemples 72

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

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

De plus, si $x, y \in G$ tels que $x \equiv_g y \mod H$, 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 $y \equiv_g x \mod H$.

Enfin, si $x, y, z \in G$ tels que $x \equiv_g y \mod H$ et $y \equiv_g z \mod H$, 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 $x \equiv_g z \mod H$ et la relation est transitive. ♣

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 :

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

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 :

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

On note alors $H \lhd G$.

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 $\overline{a}$ la classe de a modulo H, on peut munir le quotient G/H d'une structure de groupe en posant

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

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

Remarque. Cette loi de la surjection canonique $\pi : \begin{array}{ccc} G & \longrightarrow & G/H \\ x & \longmapsto & \overline{x} \end{array}$ 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 $n\mathbb{Z}$.

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

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

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

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

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

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

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

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

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

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 :

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

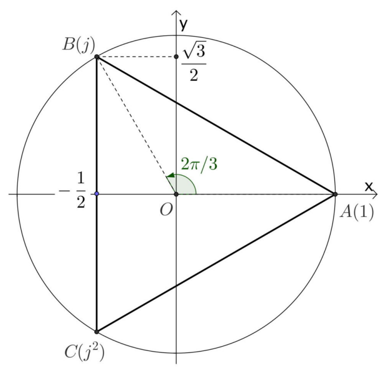

FIGURE 1.1 – Racines 3-ièmes de l'unité.

Soit $r = rot(0, \frac{2\pi}{n})$ 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

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

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

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

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

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 :

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

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

1.3.1 Description du groupe D_3

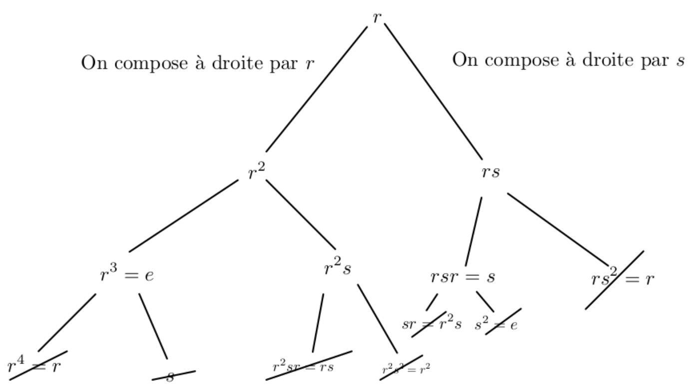

FIGURE 1.2 – Description explicite des éléments de D_3.

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.

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

$\mathbb{H}$ 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 $p3\alpha$ 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 :

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

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.

Dokaz. 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

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

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. ♣

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

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

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

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

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.

Απόδειξι.

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

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

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 :

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

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

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 :

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

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 $G/Stab(x)$ des classes à gauche modulo $Stab(x)$ sur l'orbite de x. Ainsi, le cardinal de l'orbite $Orb(x)$ est égal à l'indice du stabilisateur de x :

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

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

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

Prueba.

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

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

Exemple d'action de groupe On fait agit 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 ? 20-09-2023

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

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

On a $Orb(e) = \{e\}$. 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

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

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 ?*

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

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

La formule des classes s'écrit alors :

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

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

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

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.

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

On a bien

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

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

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

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

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

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 :

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

telle que

1. $\forall x \in V, e \cdot x = e$;
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 :

$$\begin{array}{cccc} \rho : & G & \longrightarrow & GL(V) \\ & g & \longmapsto & \begin{pmatrix} V & \longrightarrow & V \\ x & \longmapsto & g \cdot x \end{pmatrix} \end{array}$$

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

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

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

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

Remarque. Soient G un groupe fini et $\rho : G \to GL(V)$ 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) :

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

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 :

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

et

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

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 $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$. On définit la représentation canonique de degré n de $\mathfrak{S}_n$ en posant :

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

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) :

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

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) :

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

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 $\rho : G \to GL(V)$ et $\rho' : G \to GL(V')$ d'un groupe G 26-09-2023
sont dites **isomorphes** ou équivalentes s'il existe un isomorphisme d'espaces vectoriels (ici application linéaire bijective) $f : V \to V'$ 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 :

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\rho'"'] \arrow[dr, phantom, "\circlearrowleft"] & GL(V) \arrow[dl, "\tilde{f}"] \\ GL(V') & \end{tikzcd}$$

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

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\rho_g"'] \arrow[dr, phantom, "\circlearrowleft"] & V' \arrow[d, "\rho'_g"] \\ V \arrow[r, "f"'] & V' \end{tikzcd}$$

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 :

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

2.1.1 Sous-représentations

Définition 2.1.4. Si $\rho : G \to GL(V)$ 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**

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

Définition 2.1.5. Une représentation $\rho : G \to GL(V)$ 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 $\rho : G \to GL(V)$ 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.

L'application $p : \begin{array}{ccc} V & \longrightarrow & V \\ v = \underbrace{w}_{\in W} + \underbrace{w'}_{\in W'} & \longmapsto & w \end{array}$ est alors appelé le **projecteur** de V sur W associé à la décomposition $V = W \oplus W'$. On a $\mathrm{Im}(p) = W$ et $\mathrm{Ker}(p) = W'$ 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 $V = W \oplus \mathrm{Ker}(p)$, avec $\mathrm{Ker}(p) = \{v \in V, p(v) = 0\}$. On établit ainsi une **bijection** entre les projecteurs de V sur W et les **supplémentaires** de W dans V.

Définition 2.2.1. Soient $\rho : G \longrightarrow GL(V)$ et $\rho' : G \longrightarrow GL(V')$ 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

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

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. ⚠ 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 $g \longmapsto gh$ est une bijection de G sur lui-même.

Dimonstrazione del lemma 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 $\rho_{g^{-1}}(w) \in W$. ♣

Dokazatelstvo teoremy 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

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

où $\mathrm{Tr}(\rho_g)$ 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. $\chi_\rho(e) = \dim(V) =$ degré de $\rho =$ degré de χ_ρ.
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 $\chi_\rho = \chi_{\rho'}$.

27-09-2023 *Ꭻrodymas.*

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

1. Par définition, $\chi_\rho(e) = \mathrm{Tr}(\rho_e)$. 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 :

$$\chi_\rho(e) = \mathrm{Tr}(\rho_e) = \mathrm{Tr}(id_V) = \mathrm{Tr}(I_{\dim(V)}).$$

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

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

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 $\lambda^{-1} = \overline{\lambda}$. 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

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

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

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

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

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

est une base de $V \oplus V'$.
D'où

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

d'où

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

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

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

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 $V = \bigoplus_{x\in X} \langle e_x \rangle = \bigoplus_{x\in X} \mathbb{C}e_x$.

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

On a $\chi_\rho : G \longrightarrow \mathbb{C}$ tel que $\chi_\rho(g) = \mathrm{Tr}(\rho_g)$. 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 $\mathrm{Mat}_{(e_x)}(\rho_g) = (a_{ij})_{i,j}$, 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

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

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 $g \in G$:

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

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

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

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

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

où

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

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

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.

Dowód.

1. Montrons la contraposée : on suppose que f n'est pas l'application nulle.
   Le sous-espace $\mathrm{Ker}(f)$ de V est stable par ρ. En effet, si $g \in G$ et si $x \in \mathrm{Ker}(f)$, alors $\rho_g(x) \in \mathrm{Ker}(f)$, 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. $\mathrm{Ker}(f) \neq V$, on en déduit que $\mathrm{Ker}(f) = \{0\}$ par irréductibilité de ρ.
   De même, le sous-espace $\mathrm{Im}(f)$ de V' est stable par ρ'. En effet, si $g \in G$ et $y = f(x) \in \mathrm{Im}(f)$, alors $\rho'_g(y) \in \mathrm{Im}(f)$, 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. $\mathrm{Im}(f) \neq \{0\}$), on en déduit que $\mathrm{Im}(f) = V'$ 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 $\mathrm{SEP}(f, \lambda)$ de f pour la valeur propre λ est stable par ρ.
   En effet, si $g \in G$ et si $x \in \mathrm{SEP}(x, \lambda)$, alors $\rho_g(x) \in \mathrm{SEP}(f, \lambda)$, car
   $$f(\rho_g)(x) = \rho_g(f(x)) = \rho_g(\lambda x) = \lambda \rho_g(x).$$
   Donc $\underbrace{\mathrm{SEP}(f, \lambda)}_{\neq \{0\}} = V$ 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 $\mathscr{F}(G)$, 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.

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

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

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 :

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

   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

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

Tõend.

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 $\chi_0 : \begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & 1 \end{array}$ 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 $f_a : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & ag \end{array}$ 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

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

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

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

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

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

Sketch of proof. On a déjà vu que les caractères irréductibles forment un système libre de fonctions de $\mathscr{F}_C(G)$ (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 de lemme de Schur (cf 2.4). ♣

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.

Kanıt. D'après le théorème de Frobenius, le nombre de représentations irréductibles d'un groupe G est égal à la dimension de l'espace vectoriel $\mathscr{F}_C(G)$ 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 $\phi : G \longrightarrow \mathbb{C}$ peut donc s'écrire de manière unique sous la forme :

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

où $\mathrm{Conj}(G)$ 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 $C \in \mathrm{Conj}(G)$, forment donc une base de $\mathscr{F}_C(G)$, qui, de ce fait, est de dimension le cardinal de $\mathrm{Conj}(G)$. ♣

04-10-2023 **Remarque** (Notation)**.** Si G est un groupe fini, on note $\mathrm{Irr}(G)$ l'ensemble des (classes d'isomorphismes de) représentations irréductibles de G qu'on identifie parfois à l'espace de ces représentations irréductibles.

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

Corollaire 2 (Décomposition canonique d'une représentation)**.** Si $\rho : G \longrightarrow GL(V)$ est une représentation de G, et si $V = W_1 \oplus \cdots \oplus W_k$ est une décomposition de V en somme directe de représentations irréductibles de G (i. e. $\rho = \rho_1 \oplus \cdots \oplus \rho_k : G \longrightarrow GL(W_1 \oplus \cdots \oplus W_k)$, avec $\rho_i : G \longrightarrow GL(W_i)$

représentation irréductible pour $i \in \{1, \ldots, k\}$) et si $W \in \mathrm{Irr}(G)$, 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

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

Firndé. On a

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

D'où

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

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

Donc $\langle \chi_W, \chi_V \rangle = m_W$. ♣

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

Borhan. 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 :

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

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

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 $V \simeq \bigoplus_{W \in \mathrm{Irr}(G)} m_W W$, alors

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

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 :

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

♣

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

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

Ésbaat. Soit G un groupe fini. Considérons le $\mathbb{C}$-espace vectoriel $V = \mathscr{F}(G)$ 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

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

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 $V = \mathscr{F}(G)$ 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 $V = \mathscr{F}(G)$ donnée par

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

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

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

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

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

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

♣

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, $\mathrm{Irr}(G)$ 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 $\mathrm{Conj}(G)$ l'ensemble des classes de conjugaison de G, on a donc $\sharp\,\mathrm{Conj}(G) = |G|$.

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

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

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

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. ♣

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

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

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 :

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

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

De plus, $\rho(\overline{1})^2 = \rho(\overline{1}+\overline{1}) = \rho(\overline{0}) = 1$. Donc $\rho(\overline{1})$ 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 :

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

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

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

♣

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,

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

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 $\chi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*$. Or, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique et est engendré par $\overline{1}$ (où $\overline{a} = a + n\mathbb{Z}$).

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

De plus, on a : $\chi(\overline{n}) = \chi(\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{n \text{ fois}}) = \chi(\overline{1})^n$. Donc $\chi(\overline{1})$ est une racine n-ième de l'unité dans $\mathbb{C}$. Il existe donc $k \in \{0, \ldots, n-1\}$ tel que $\chi(\overline{1}) = e^{\frac{2ik\pi}{n}}$.

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

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

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

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

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

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

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

2.7 Nombre de représentations irréductibles de degré 1

10-10-2023

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 $D(G) \lhd G$.
3. Soit $H \lhd G$. 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 $f \in \mathrm{Aut}(G)$, 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 $f_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array}$ pour $g \in G$). Donc $D(G) \lhd G$.
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 $\overline{a} = Ha = aH$, car $H \lhd G$. 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**. Donc $D(\mathfrak{A}_3) = \{e\}$.
2. On a $D(\mathfrak{S}_3) \lhd \mathfrak{S}_3$. 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 :
   $$\mathfrak{A}_4 = \{e\} \cup \{\text{3-cycles}\} \cup \{\text{type } (2,2)\}.$$
   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 $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ est distingué dans $\mathfrak{A}_4$, car stable par conjugaison : $V \lhd \mathfrak{A}_4$.
   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 $D(\mathfrak{A}_4) = V$.
4. *Extrait du cours de l'année 2022-2023.* $D(\mathfrak{S}_4) \lhd \mathfrak{S}_4$, donc $D(\mathfrak{S}_4) = \{e\}$ ou $\mathfrak{A}_4$ ou $\mathfrak{S}_4$. On ne peut avoir $D(\mathfrak{S}_4) \neq \{e\}$, car $\mathfrak{S}_4$ n'est pas abélien. De plus, le quotient $\mathfrak{S}_4/\mathfrak{A}_4$ a pour ordre 2 premier, donc il est cyclique, donc abélien. Par le 3 de la proposition précédente, on a $D(\mathfrak{S}_4) \subset \mathfrak{A}_4$. Comme $\mathfrak{A}_4 \subset D(\mathfrak{S}_4)$, on conclut que ces groupes sont égaux.

♣

Proposition 2.7.2.

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 $D(\mathfrak{A}_n) = \mathfrak{A}_n$. ♣

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 2.7.3. 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 $H \subset \mathrm{Ker}(f)$.

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

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

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

Réciproquement, si $H \subset \mathrm{Ker}(f)$, 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 $H \subset \mathrm{Ker}(f)$, donc $x^{-1}x' \in \mathrm{Ker}(f)$, 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. ♣

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 :

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

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

On en déduit par la proposition 2.7.3 que le morphisme χ se factorise par $G/D(G)$:

$$\begin{tikzcd} G \arrow[rr, "\chi"] \arrow[dr, "\pi"'] & \arrow[d, phantom, "\circlearrowright"] & \mathbb{C}^* \arrow[dl, dotted, "\check{\chi}"] \\ & C & \end{tikzcd}$$

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 $G/D(G)$:

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

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

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).

Exercices

11-10-2023 **Exercice 11.** On considère le groupe symétrique $\mathfrak{S}_n$ avec $n \geq 2$.

1. Soit $\rho : \mathfrak{S}_n \longrightarrow \mathbb{C}^*$ 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 le 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 $\rho : \mathfrak{S}_3 \longrightarrow GL(V)$ 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 $\mathrm{Vect}(x, \rho_\tau(x))$ 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 $\tau \circ \tau = \tau^2 = \mathrm{id}$. On a :

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

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 $\rho : \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathbb{C}^* \\ \sigma & \longmapsto & 1 \end{array}$ 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

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

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 $\mathrm{id}_V = \rho(e) = \rho(\sigma^3) = \rho_{\sigma^3} = \rho(\sigma)^3 = \rho_\sigma^3$. D'où

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

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_{ρ_σ} 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 :

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

Donc $\rho_\tau(x)$ est un vecteur propre de ρ_σ pour la valeur propre λ^2.
Posons $W := \mathrm{Vect}(x, \rho_\tau(x))$ 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 $\rho_\tau(\rho_\tau(x)) = \rho_{\tau^2}(x) = \rho_e(x) = \mathrm{id}(x) = x \in V$ 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

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

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

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

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

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

iv.

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

On a

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

Remarque (Personnelle)**.** 3 correpond au nombre de transpositions dans $\mathfrak{S}_3$ et 2 correspond au nombre de 3-cycles. Puisque les transpositions (respectivement les 3-cycles) sont conjugués dans $\mathfrak{S}_3$, la valeur de ρ_g et donc de $\chi(g)$ est identique pour chaque transposition (respectivement pour chaque 3-cycle), donc on multiplie par 3 (respectivement par 2).

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

(d) On a

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

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

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

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

♣

Exercice 12. Montrer que si $\sigma \in \mathfrak{A}_n$, alors les conjugués de σ dans $\mathfrak{S}_n$ forment une (respectivement deux) classe(s) de conjugaison dans $\mathfrak{A}_n$ s'il existe une permutation impaire commutant à σ (respectivement sinon (c'est-à-dire s'il n'existe pas de permutation impaire)). 16-10-2023

Démonstration.

Remarque. La classe de conjugaison dans $\mathfrak{S}_n$ et dans $\mathfrak{A}_n$ de σ est :

$$\mathrm{Conjug}_{\mathfrak{S}_n}(\sigma) = \{\tau\sigma\tau^{-1}, \tau \in \mathfrak{S}_n\} \text{ et } \mathrm{Conjug}_{\mathfrak{A}_n}(\sigma) = \{\tau\sigma\tau^{-1}, \tau \in \mathfrak{A}_n\}.$$

On peut faire agir le groupe $\mathfrak{S}_n$ sur lui-même par conjugaison :

$$\begin{array}{ccc} \mathfrak{S}_n \times \mathfrak{S}_n & \longrightarrow & \mathfrak{S}_n \\ (\sigma, \tau) & \longmapsto & \sigma \cdot \tau = \sigma\tau\sigma^{-1}. \end{array}$$

Si $\tau \in \mathfrak{S}_n$, alors :

$$\mathrm{Orb}_{\mathfrak{S}_n}(\tau) := \{\sigma \cdot \tau, \sigma \in \mathfrak{S}_n\} = \{\sigma\tau\sigma^{-1}, \sigma \in \mathfrak{S}_n\} = \mathrm{Conjug}_{\mathfrak{S}_n}(\tau).$$

$$\begin{aligned} \mathrm{Stab}_{\mathfrak{S}_n}(\tau) &= \{\sigma \in \mathfrak{S}_n \mid \sigma \cdot \tau = \tau\} = \{\sigma \in \mathfrak{S}_n \mid \sigma\tau\sigma^{-1} = \tau\} \\ &= \{\sigma \in \mathfrak{S}_n \mid \sigma\tau = \tau\sigma\} = \mathrm{centralisateur}_{\mathfrak{S}_n}(\tau). \end{aligned}$$

On a

$$\sharp\, \mathrm{Orb}_{\mathfrak{S}_n}(\tau) = [\mathfrak{S}_n : \mathrm{Stab}_{\mathfrak{S}_n}(\tau)].$$

On peut aussi faire agir le groupe alterné $\mathfrak{A}_n$ sur lui-même par conjugaison :

$$\begin{array}{ccc} \mathfrak{A}_n \times \mathfrak{A}_n & \longrightarrow & \mathfrak{A}_n \\ (\sigma, \tau) & \longmapsto & \sigma\tau\sigma^{-1}. \end{array}$$

Si $\tau \in \mathfrak{A}_n$, alors

$$\mathrm{Orb}_{\mathfrak{A}_n}(\tau) = \mathrm{Conjug}_{\mathfrak{A}_n}(\tau)$$

et

$$\mathrm{Stab}_{\mathfrak{A}_n}(\tau) = \mathrm{centralisateur}_{\mathfrak{A}_n}(\tau)$$

et on a :

$$\sharp\, \mathrm{Orb}_{\mathfrak{A}_n}(\tau) = [\mathfrak{A}_n : \mathrm{Stab}_{\mathfrak{A}_n}(\tau)].$$

Soit $\sigma \in \mathfrak{A}_n$. Supposons qu'il n'existe pas de permutation impaire qui commute avec σ. Alors $\mathrm{Stab}_{\mathfrak{S}_n}(\sigma) = \mathrm{Stab}_{\mathfrak{A}_n}(\sigma)$.

D'où

$$\begin{aligned} \sharp\, \mathrm{Orb}_{\mathfrak{S}_n}(\sigma) &= [\mathfrak{S}_n : \mathrm{Stab}_{\mathfrak{S}_n}(\sigma)] = [\mathfrak{S}_n : \mathrm{Stab}_{\mathfrak{A}_n}(\sigma)] \\ &= [\mathfrak{S}_n : \mathfrak{A}_n] \times [\mathfrak{A}_n : \mathrm{Stab}_{\mathfrak{A}_n}(\sigma)] = 2 \times [\mathfrak{A}_n : \mathrm{Stab}_{\mathfrak{A}_n}(\sigma)] = \sharp\, \mathrm{Orb}_{\mathfrak{A}_n}(\sigma). \end{aligned}$$

Si $\mathrm{Stab}_{\mathfrak{A}_n}(\sigma)$ est d'indice ≥ 2 dans $\mathrm{Stab}_{\mathfrak{S}_n}(\sigma)$, alors $\mathrm{Stab}_{\mathfrak{A}_n}(\sigma) \geq \sharp\, \mathrm{Orb}_{\mathfrak{S}_n}(\sigma)$, d'où l'égalité, car $\mathrm{Orb}_{\mathfrak{A}_n}(\sigma) \subset \mathrm{Orb}_{\mathfrak{S}_n}(\sigma)$. ♣

Exercice 13 (Problème donné au partiel en octobre 2022)**.**

1. Combien le groupe $\mathfrak{S}_n$ admet de classes d'isomorphismes de représentations irréductibles ?
2. On fait agir $\mathfrak{S}_4$ sur lui-même par conjugaison et on considère le 3-cycle $\sigma = (1\ 2\ 3)$ dans $\mathfrak{S}_4$.
   (a) Quel est l'ordre du stabilisateur de σ dans $\mathfrak{S}_4$?
   (b) En déduire qu'il n'existe pas de permutation impaire qui commute avec σ.
   (c) En déduire que les conjugués de σ dans $\mathfrak{S}_4$ forment deux classes de conjugaison de σ dans $\mathfrak{S}_4$.
3. Combien $\mathfrak{A}_4$ admet-il de classes d'isomorphisme de représentations irréductibles ?
4. Soit $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.
   (a) Montrer que K est un sous-groupe distingué de $\mathfrak{A}_4$.
   (b) Montrer que K est isomorphe au groupe de Klein.
   (c) Le groupe quotient $\mathfrak{A}_4/K$ est-il abélien ?
   (d) Déterminer le sous-groupe dérivé $D(\mathfrak{A}_4)$ de $\mathfrak{A}_4$.
   (e) En déduire le nombre de représentations irréductibles de degré 1 (à isomorphisme près) de $\mathfrak{A}_4$ et celui de degré supérieur.

17-10-2023

5. Soit χ un caractère linéaire $\mathfrak{A}_4$, i. e. un morphisme de groupes de $\mathfrak{A}_4$ et à valeurs dans $\mathbb{C}^*$.
   (a) Montrer que le morphisme χ se factorise par $\mathfrak{A}_4/D(\mathfrak{A}_4)$, i. e. qu'il existe un morphisme $\check{\chi} : \mathfrak{A}_4/D(\mathfrak{A}_4) \longrightarrow \mathbb{C}^*$ tel que $\check{\chi} \circ \pi = \chi$.
   (b) En déduire que $\chi(\tau)$ est d'ordre divisant 3 pour tout $\tau \in \mathfrak{A}_4$.
   (c) En déduire les caractères de degré 1, i. e. les représentations de degré 1, de $\mathfrak{A}_4$.
6. Soit $\rho : \mathfrak{A}_4 \longrightarrow GL(V)$ la représentation de permutation associée à l'action naturelle de $\mathfrak{A}_4$ sur $\{1, 2, 3, 4\}$. On rappelle que l'espace V de cette représentation est $\mathbb{C}^4$ muni de l'action de $\mathfrak{A}_4$ définie, dans la base canonique (e_1, e_2, e_3, e_4) par $\sigma \cdot e_i = e_{\sigma(i)}$ pour tout $\sigma \in \mathfrak{A}_4$.
   (a) Montrer que V se décompose sous la forme $V' \oplus W$ où V' est la droite engendrée par le vecteur $v' = e_1 + e_2 + e_3 + e_4$ et W est l'hyperplan d'équation $x_1 + x_2 + x_3 + x_4 = 0$.
   (b) Montrer que les sous-espaces vectoriels V' et W sont stables par la représentation ρ.

(c) Soient χ_V, $\chi_{V'}$ et χ_W les caractères respectivement des représentations V, V' et W. Montrer que $\chi_V = \chi_{V'} + \chi_W$.

(d) Rappeler que vaut le caractère d'une représentation de permutation. En déduire les valeurs de χ_V sue les classes de conjugaison de $\mathfrak{A}_4$.

(e) Montrer que $\chi_{V'}$ est le caractère trivial et en déduire les valeurs du caractère χ_W.

(f) Montrer que le caractère χ_W est irréductible.

Démonstration.

1. La partition de $\mathfrak{S}_4$ en classes de conjugaison est la suivante (car deux permutations de $\mathfrak{S}_4$ sont conjuguées si et seulement si elles ont le même type). Dans $\mathfrak{S}_4$, on a :

$$\mathfrak{S}_4 = \underbrace{\mathrm{Conjug}(\mathrm{id})}_{=\{\mathrm{id}\}} \cup \underbrace{\mathrm{Conjug}((1\ 2))}_{\text{transpositions},\sharp=6} \cup \underbrace{\mathrm{Conjug}((1\ 2\ 3))}_{\text{3-cycles},\sharp=8} \cup \underbrace{\mathrm{Conjug}((1\ 2)(3\ 4))}_{\text{type }(2,2),\sharp=3} \cup \underbrace{\mathrm{Conjug}((1\ 2\ 3\ 4))}_{\text{4-cycles},\sharp=6}.$$

Le nombre de représentations irréductibles de $\mathfrak{S}_4$ est égal au nombre de ses classes de conjugaison, à savoir 5.

2. (a) On a

$$[\mathfrak{S}_4 : \mathrm{Stab}_{\mathfrak{S}_4}(\sigma)] = \sharp\,\mathrm{Orb}_{\mathfrak{S}_4}(\sigma) = \sharp\,\mathrm{Conjug}_{\mathfrak{S}_4}(\sigma) = \sharp\{\text{3-cycles de } \mathfrak{S}_4\}.$$

D'où

$$|\mathrm{Stab}_{\mathfrak{S}_4}(\sigma)| = \frac{|\mathfrak{S}_4|}{\sharp\,\mathrm{Orb}_{\mathfrak{S}_4}(\sigma)} = \frac{24}{8} = 3.$$

Remarque. Le nombre de r-cycles dans $\mathfrak{S}_n$ $(r \leq n)$ est égal à :

$$\frac{A_n^r}{r} = \frac{n!}{r(n-r)!}.$$

Par exemple, le nombre de 3-cycles dans $\mathfrak{S}_4$ est

$$\frac{4!}{3 \times 1!} = 8.$$

(b) Le stabilisateur de σ dans $\mathfrak{S}_4$ est le centralisateur de σ dans $\mathfrak{S}_4$ (dans ce cas précis), à savoir l'ensemble des permutations de $\mathfrak{S}_4$ qui commutent avec σ. Or :
— e commute avec σ ;
— σ commute avec σ ;
— $\sigma^{-1} = \sigma^2$ commute avec σ.
Puisque $\mathrm{Stab}_{\mathfrak{S}_4}(\sigma)$ est d'ordre 3, on a donc :

$$\mathrm{Stab}_{\mathfrak{S}_4}(\sigma) = \{e, \sigma, \sigma^2\}.$$

Or les permutations e, σ, σ^2 sont toutes paires, d'où le résultat.

(c) On a

$$\mathrm{Conjug}_{\mathfrak{S}_4}(\sigma) = \{\text{3-cycles de } \mathfrak{S}_4\} = \{(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}.$$

Cette classe de conjugaison dans $\mathfrak{S}_4$ se décompose en deux classes de conjugaison dans $\mathfrak{S}_4$ en quatre éléments chacune.

$$\mathrm{Conjug}_{\mathfrak{A}_4}((1\ 2\ 3)) = \{(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)\}$$

et

$$\mathrm{Conjug}_{\mathfrak{S}_4}((1\ 3\ 2)) = \{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}.$$

Remarque. En revanche, les types (2,2) constituent une classe de conjugaison dans $\mathfrak{A}_4$, car il existe une permutation impaire qui commute avec (1 2)(3 4), à savoir (1 2).

3. On a :

$$\begin{aligned}\mathfrak{A}_4 &= \{\text{permutations paires de } \mathfrak{S}_4\} = \{\text{id}\} \cup \{\text{3-cycles}\} \cup \{\text{type (2,2)}\} \\ &= \mathrm{Conjug}_{\mathfrak{A}_4}(\text{id}) \cup \mathrm{Conjug}_{\mathfrak{A}_4}((1\ 2\ 3)) \cup \mathrm{Conjug}_{\mathfrak{S}_4}((1\ 3\ 2)) \cup \mathrm{Conjug}_{\mathfrak{A}_4}((1\ 2)(3\ 4)).\end{aligned}$$

   $\mathfrak{A}_4$ admet donc 4 représentations irréductibles à isomorphisme près.

4. *Ceci est ma rédaction personnelle des questions, car elles n'étaient pas corrigées par écrit en classe.*

   (a) K contient l'élément neutre ainsi que toutes les permutations de type (2,2). On sait que dans $\mathfrak{S}_n$, deux permutations sont conjuguées si et seulement si elles ont le même type. Cela implique que K est stable par conjugaison. Donc il est distingué dans $\mathfrak{S}_n$.

   (b) *Merci à Abdoulaye pour son aide à la rédaction de cette question !* Il existe deux groupes d'ordre 4 à isomorphisme près : le groupe cyclique $\mathbb{Z}/4\mathbb{Z}$ et le groupe de Klein. Les éléments de K sont tous d'ordre 2 (sauf l'élément neutre). En effet, comme toute transposition est d'ordre 2, le produit de deux permutations est d'ordre $\mathrm{ppcm}(2,2) = 2$. Il est forcément isomorphe au groupe de Klein.

   (c) Le quotient $\mathfrak{A}_4/K$ est d'ordre $\frac{|\mathfrak{A}_4|}{|K|} = \frac{12}{4} = 3$. Comme 3 est premier, le quotient $\mathfrak{A}_4/K$ est cyclique, donc abélien.

   (d) On a d'une part $K \subset D(\mathfrak{A}_4)$. D'autre part, $K \triangleleft D(\mathfrak{A}_4)$. Par la proposition 2.7.1, comme $\mathfrak{A}_4/K$ est abélien, $D(\mathfrak{A}_4) \subset K$. Par conséquent, $D(\mathfrak{A}_4) = K$.

   (e) Par le théorème 2.7.1, comme $\mathfrak{A}_4$ est un groupe fini, le nombre de ses représentations irréductibles de degré 1 est égal à l'indice $[\mathfrak{A}_4 : D(\mathfrak{A}_4)]$ dans $\mathfrak{A}_4$. Or $D(\mathfrak{A}_4) = K$. Par conséquent,

$$[\mathfrak{A}_4 : D(\mathfrak{A}_4)] = \frac{|\mathfrak{A}_4|}{|K|} = \frac{12}{4} = 3,$$

   ce qui implique qu'il y a trois représentations irréductibles de degré 1 dans $\mathfrak{A}_4$.

   De plus, le nombre de représentations irréductibles de $\mathfrak{A}_4$ est égal au nombre de ses classes de conjugaison. On a va précédemment qu'il y a quatre classes de conjugaison dans $\mathfrak{A}_4$. De plus, par la formule de Burnside, on a

$$\sum_{W \in \mathrm{Irr}(\mathfrak{A}_4)} \dim(W)^2 = |\mathfrak{A}_4| = 12. \tag{2.2}$$

   On a trois représentations de degré 1 et une représentation de degré supérieur d. L'égalité 2.2 devient :

$$1^2 + 1^2 + 1^2 + d^2 = 12,$$

   ce qui donne $d^2 = 9$. On obtient ainsi $d = 3$.

5. (a) Le morphisme χ se factorise par π si et seulement si $\mathrm{Ker}(\chi)$ contient $D(\mathfrak{A}_4)$ (cf proposition 2.7.3). Or, d'après le premier théorème d'isomorphisme, on a :

$$\mathfrak{A}_4/\,\mathrm{Ker}(\chi) \simeq \mathrm{Im}(\chi) = \chi(\mathfrak{A}_4) \subset \mathbb{C}^*,$$

on en déduit que $\mathrm{Im}(\chi)$ est abélien (car tout sous-groupe d'un groupe abélien est abélien), et donc que le quotient $\mathfrak{A}_4/\operatorname{Ker}(\chi)$ est abélien (en tant que groupe isomorphe à un groupe abélien). Or, si G est un groupe et H un sous-groupe distingué de G, alors le quotient G/H est abélien si et seulement si $D(G) \subset H$. On en déduit donc que $\operatorname{Ker}(\chi)$ contient le sous-groupe dérivé de $\mathfrak{A}_4$. En conclusion, le morphisme χ se factorise par $\mathfrak{A}_4/D(\mathfrak{A}_4)$.

(b) Soit $\tau \in \mathfrak{A}_4$. Considérons $\pi(\tau) = \overline{\tau} \in \mathfrak{A}_4/D(\mathfrak{A}_4)$. Puisque $D = K$, alors $|\mathfrak{A}_4/D(\mathfrak{A}_4)| = \frac{|\mathfrak{A}_4|}{|K|} = \frac{12}{4} = 3$. Par le théorème de Lagrange, $\overline{\tau}$ est donc d'ordre divisant 3, i. e. $(\overline{\tau})^3 = \overline{e}$.
D'où $\check{\chi}(\overline{e}) = \check{\chi}(\overline{\tau}^3) = (\check{\chi}(\tau))^3$. Donc $\chi(\overline{\tau})$ est d'ordre divisant 3, i. e. $\check{\chi}(\pi(\tau))$ est d'ordre divisant 3, i. e. $\chi(\tau)$ est d'ordre divisant 3.

(c) On rappelle que $\mathfrak{A}_4$ comprend 4 classes de conjugaison :

$$\begin{gathered}\mathrm{Conjug}_{\mathfrak{S}_4}(e) = \{e\};\\ \mathrm{Conjug}_{\mathfrak{S}_4}((1\ 2)(3\ 4)) = \text{type } (2{,}2);\\ \mathrm{Conjug}_{\mathfrak{S}_4}((1\ 2\ 3));\\ \mathrm{Conjug}_{\mathfrak{S}_4}((1\ 3\ 2)).\end{gathered}$$

D'autre part, on a :

$$\pi((1\ 2)(3\ 4)) = \overline{(1\ 2)(3\ 4)} = (1\ 2)(3\ 4)D(\mathfrak{A}_4) = \overline{e},$$

car $(1\ 2)(3\ 4) \in D(\mathfrak{A}_4)$.
D'où $\check{\chi} \circ \pi((1\ 2)(3\ 4)) = \check{\chi}(\overline{e}) = 1$, donc $\chi((1\ 2)(3\ 4)) = 1$. Puisque les racines cubiques de l'unité dans $\mathbb{C}$ sont 1, j et j^2, où $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, les caractères de degré 1 de $\mathfrak{A}_4$ sont donc :

$$\begin{array}{rccc}\chi_0: & \mathfrak{A}_4 & \longrightarrow & \mathbb{C}^* \\ & \tau & \longmapsto & 1,\end{array}$$

$$\begin{array}{rccc}\chi_1: & \mathfrak{A}_4 & \longrightarrow & \mathbb{C}^* \\ & \mathrm{id} & \longmapsto & 1 \\ & (1\ 2)(3\ 4) & \longmapsto & 1 \\ & (1\ 2\ 3) & \longmapsto & j \\ & (1\ 3\ 2) & \longmapsto & j^2,\end{array}$$

$$\begin{array}{rccc}\chi: & \mathfrak{A}_4 & \longrightarrow & \mathbb{C}^* \\ & \mathrm{id} & \longmapsto & 1 \\ & (1\ 2)(3\ 4) & \longmapsto & 1 \\ & (1\ 2\ 3) & \longmapsto & j^2 \\ & (1\ 3\ 2) & \longmapsto & j,\end{array}$$

et de même sur les classes de conjugaison.

6. (a) On a $V' \cap W = \{0\}$. En effet, si $v \in V' \cap W$, alors il existe $\lambda \in \mathbb{C}$ tel que $v = \lambda v' = \lambda e_1 + \dots + \lambda e_4$, et on a également : $\lambda + \lambda + \lambda + \lambda = 0$. D'où $\lambda = 0$ et donc $v = 0_{\mathbb{C}^4}$.
De plus, $\dim(V') = 1$ et $\dim(W) = 3$, d'où $\dim(V') + \dim(W) = 4 = \dim(V) = \dim(\mathbb{C}^4)$.
Donc $V = V' \oplus W$.

(b) Montrons que, pour tout $\tau \in \mathfrak{A}_4$, on a $\rho_\tau(V') \subset V'$ et $\rho_\tau(W) \subset W$, i. e. $\forall \tau \in \mathfrak{A}_4, \forall v \in V', \rho_\tau(v) \in V'$ et $\forall \tau \in \mathfrak{A}_4, \forall w \in W, \rho_\tau(w) \in W$.
Soient $\tau \in \mathfrak{A}_4$. Il existe donc $\lambda \in \mathbb{C}$ tel que $v = \lambda v' = \lambda e_1 + \dots + \lambda e_4$. On a

$$\begin{aligned}\rho_\tau(v) &= \rho_\tau(\lambda v') = \lambda\rho_\tau(v') = \lambda\rho_\tau(e_1 + \dots e_4)\\ &= \lambda(\rho_\tau(e_1) + \dots + \rho_\tau(e_4)) = \lambda(e_{\tau(1)} + \dots + e_{\tau(4)}) = \lambda v',\end{aligned}$$

car τ est un élément de $\mathfrak{A}_4$. Conclusion : $\rho_\tau(v) \in V'$.

Soient $\tau \in \mathfrak{A}_4$ et $w \in W$. Posons $w = \sum_{i=1}^{4} w_i e_i$. On a

$$\rho_\tau(w) = \rho_\tau\left(\sum_{i=1}^{4} w_i e_i\right) = \sum_{i=1}^{4} w_i \rho_\tau(e_i) = \sum_{i=1}^{4} w_i e_{\tau(i)}.$$

Donc $\rho_\tau(w) \in W$, car $w_1 + \cdots + w_4 = 0$ (car $w \in W$). Conclusion : W est stable par la représentation ρ.

(c) En effet, puisque $V = V' \oplus W$ et que V' et W' sont stables par ρ, on obtient le résultat.

(d) Puisque ρ est la représentation de permutations de $\mathfrak{A}_4$, on en déduit que, pour tout $\tau \in \mathfrak{A}_4$, la trace de ρ_τ, i. e. $\chi_V(\tau)$, est égale au nombre de points fixes de τ agissant sur $\{1,2,3,4\}$. On a donc $\chi_V(\mathrm{id}) = 4$, $\chi_V((1\ 2)(3\ 4)) = 0$, $\chi_V((1\ 3\ 2)) = 1$.

(e) Le vecteur $e_1 + \cdots + e_4$ est laissé fixé par toute permutation de $\mathfrak{A}_4$. On en déduit que $\chi_{V'}$ est le caractère trivial $\chi_V(\tau) = 1, \forall \tau \in \mathfrak{A}_4$. De plus, on a

$$\chi_V = \chi_{V'} + \chi_W,$$

d'où

— $\chi_V(\mathrm{id}) = \chi_V(\mathrm{id}) - \chi_{V'}(\mathrm{id}) = 4 - 1 = 3$;
— $\chi_W((1\ 2)(3\ 4)) = \chi_V((1\ 2)(3\ 4)) - \chi_{V'}((1\ 2)(3\ 4)) = 0 - 1 = -1$;
— $\chi_W((1\ 2\ 3)) = \chi_V((1\ 2\ 3)) - \chi_{V'}((1\ 2\ 3)) = 1 - 1 = 0$;
— $\chi_W((1\ 3\ 2)) = \chi_V((1\ 2\ 3)) - \chi_{V'}((1\ 2\ 3)) = 1 - 1 = 0$.

(f) On utilise le critère d'irréductibilité des caractères 4.

$$\langle \chi_W, \chi_W \rangle = \frac{1}{|\mathfrak{A}_4|} \sum_{\tau \in \mathfrak{A}_4} \overline{\chi(\tau)}\chi(\tau) = \frac{1}{12}(1 \cdot 3^2 + 3 \cdot (-1)^2 + 4 \cdot 0 + 4 \cdot 0) = \frac{12}{12} = 1.$$

Cela permet de conclure que χ_W est irréductible.

♣

CHAPITRE 3

GROUPES ORTHOGONAUX ET UNITAIRES

3.1 Théorème de classification des endomorphismes orthogonaux de $\mathbb{R}^3$

23-10-2023

Définition 3.1.1. Une matrice $M \in \mathcal{M}_n(\mathbb{R})$ est dite **orthogonale** si ${}^tMM = I$.
L'ensemble

$$O_n = \{M \in \mathcal{M}_n(\mathbb{R}) \mid^t MM = I\}$$

est un sous-groupe de $GL_n(\mathbb{R})$ appelé **le sous-groupe orthogonal** de degré n sur $\mathbb{R}$.

Remarque. Si $M \in O_n(\mathbb{R})$, alors $\det(M)^2 = 1$, ce qui implique que $\det(M) = \pm 1$.

Proposition 3.1.1 (Rappel)**.** Les assertions suivantes sont équivalentes :

1. $M \in O_n(\mathbb{R})$;
2. Les colonnes de M forment une base orthonormale de $\mathbb{R}^n$;
3. L'endomorphisme f associé à $\mathbb{R}^n$ est un endomorphisme **orthogonal** ;
4. f conserve la norme $\|f(x)\| = \|x\|$ pour tout $x \in \mathbb{R}^n$;
5. Pout toute base orthonormée $\mathcal{B}$ de $\mathbb{R}^n$, $f(\mathcal{B})$ est encore une base orthonormée de $\mathbb{R}^n$.

Définition 3.1.2. Le sous-ensemble

$$SO_n(\mathbb{R}) := \{M \in O_n(\mathbb{R}) \mid \det(M) = \pm 1\}$$

est un sous-groupe de $O_n(\mathbb{R})$, appelé **groupe spécial orthogonal** de degré n sur $\mathbb{R}$.

3.1.1 Cas particulier en dimension 2 et 3

Dimension 2

En dimension 2 (pour $n = 2$), on a :

$$\begin{aligned} O_2(\mathbb{R}) &= \left\{ \begin{pmatrix} \cos(\theta) & -\varepsilon\sin(\theta) \\ \sin(\theta) & -\varepsilon\cos(\theta) \end{pmatrix}, \theta \in \mathbb{R}, \varepsilon = \pm 1 \right\} \\ &= \left\{ R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \theta \in \mathbb{R} \right\} \bigcup \left\{ S_\varphi = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}, \varphi \in \mathbb{R} \right\}, \end{aligned}$$

où R_θ est la rotation d'angle θ et S_φ est la réflexion (symétrie orthogonale par rapport à un hyperplan) par rapport à la droite D passant par l'origine et faisant un angle $\dfrac{\varphi}{2}$ avec l'axe des abscisses.

Dimension 3

En dimension 3 (pour $n = 3$), on a :

Théorème 3.1.1 (De classification des endomorphismes orthogonaux de $\mathbb{R}^3$)**.** Soit $f \in O_3(\mathbb{R}) \setminus \{\mathrm{id}\}$.

1. Si $\det(f) = 1$, alors f est une **rotation** de $\mathbb{R}^3$.
2. Si $\det(f) = -1$, alors :
   (a) Ou bien f est une **réflexion** de $\mathbb{R}^3$;
   (b) Ou bien f est **la composée d'une rotation** de $\mathbb{R}^3$ et de la **réflexion** par rapport au plan orthogonal à l'axe de cette rotation.

3.2 Le groupe unitaire et spécial unitaire

Définition 3.2.1. Si $M \in \mathcal{M}_n(\mathbb{C}), M = (a_{ij})_{i,j}$, on définit l'adjointe (ou transconjuguée) de M la matrice :

$$M^* :=^t \overline{M} = (b_{ij}), \text{ avec } b_{ij} = \overline{a_{ji}}.$$

Rappelons que l'espace vectoriel $\mathbb{C}^n$ est muni du produit scalaire hermitien

$$\begin{array}{ccc} \mathbb{C}^n \times \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ (v, w) & \longmapsto & (v \mid w) = \sum_{i=1}^n \overline{v_i} w_i. \end{array}$$

C'est une forme sesquilinéaire, ce qui veut dire qu'elle est

1. antilinéaire par rapport à la première place, i. e.
$$\forall \lambda \in \mathbb{C}, \langle \lambda v + v' \mid w \rangle = \overline{\lambda} \langle v \mid w \rangle,$$
2. linéaire par rapport à la seconde place,
3. hermitienne, i. e. $\langle w \mid v \rangle = \overline{\langle v \mid w \rangle}$,
4. définie positive.

Définition 3.2.2. Une matrice est dite **unitaire** si $M^*M = I$.

On vérifie que

$$U_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{C}) \mid M^*M = I\}$$

est un sous-groupe de $GL_n(\mathbb{C})$ appelé **groupe unitaire** de degré n.

On définit le groupe spécial unitaire par :

$$SU_n(\mathbb{C}) = \{M \in U_n(\mathbb{C}) \mid \det(M) = 1\}.$$

CHAPITRE 4

GROUPES TOPOLOGIQUES

On va travailler sur les groupes des topologies compatibles avec la loi de groupes.

Définition 4.0.1. Un groupe topologique est la donnée d'un groupe $(G, *)$ et d'une topologie sur l'ensemble G telle que, si l'ensemble $G \times G$ est muni de la topologie produit, la loi interne

$$* : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, g') & \longmapsto & g * g' \end{array}$$

et le passage au symétrique

$$\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1} \end{array}$$

sont continues.

Remarque (Rappel : topologie produit sur $G \times G$)**.** U est un ouvert de $G \times G$ si pour tout $x \in U$, il existe U_1 ouvert de G et il existe U_2 ouvert de G tels que $x \in U_1 \times U_2 \subset U$, i. e. si U est une réunion de produits d'ouverts de G. C'est la topologie la moins fine qui rend les projections continues.

Exemple. Les topologies usuelles sur $\mathbb{R}^n, \mathbb{C}^n$ et $\mathbb{R}^*$ font de $(\mathbb{R}^n, +), (\mathbb{C}^n, +)$ et $(\mathbb{R}^*, \times)$ des groupes topologiques.

Soit $K = \mathbb{R}$ ou $\mathbb{C}$, l'espace vectoriel $\mathcal{M}_n(K)$ s'identifie à K^{n^2}. On peut définir une norme sur cet espace en posant

$$\|M\| = \max\{|a_{ij}, 1 \leq i, j \leq n|\} \text{ si } M = (a_{ij})_{1 \leq i,j \leq n}.$$

On a donc une distance d sur $\mathcal{M}_n(K)$ définie par :

$$d(M, N) = \|M - N\|$$

et cette distance induit une topologie sur cet espace. L'application déterminant $\det : \mathcal{M}_n(K) \longrightarrow K$ est continue, car le déterminant d'une matrice $M = (a_{ij})$ est un polynôme des a_{ij}. On en déduit que $GL_n(K) = \det^{-1}(K^*)$ est un ouvert de $\mathcal{M}_n(K)$ et que $SL_n(K) = \det^{-1}(\{1\})$ est un fermé.

Théorème 4.0.1. Les groupes $SO_n(\mathbb{R}), O_n(\mathbb{R}), SU_n(\mathbb{C})$ et $U_n(\mathbb{C})$ sont compacts.

Pierādījums. L'application $\psi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ M & \longmapsto & {}^tMM \end{array}$ est continue et donc $O_n(\mathbb{R}) = \psi^{-1}(\{I\})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$.

Si $M = (a_{ij}) \in O_n(\mathbb{R})$, le produit scalaire de la j-ième colonne de M avec elle-même est égal à 1 (car les colonnes de M forment une base orthonormée), ce qui implique que $|a_{ij}| \leq 1$ pour $i = 1, \ldots, n$ (car $\sum_{i=1}^{n} a_{ij}^2 = 1$). On en déduit que $\|M\| \leq 1$.

Le groupe orthogonal $O_n(\mathbb{R})$ est fermé et borné dans $\mathcal{M}_n(\mathbb{R})$ (qui est un espace vectoriel de dimension finie n^2), il est donc compact. La compacité de $U_n(\mathbb{C})$ se montre de manière analogue. Comme $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$, $SO_n(\mathbb{R})$ est un fermé dans un compact, il est donc lui-même compact. ♣

CHAPITRE 5

ALGÈBRE D'UN GROUPE FINI

Soit G un groupe fini. Soit $\mathscr{F}(G)$ le $\mathbb{C}$-espace vectoriel des fonctions définies sur G à valeurs dans $\mathbb{C}$. Il est de dimension $|G|$, car une base de cet espace vectoriel est donnée par les fonctions suivantes (pour $g \in G$) :

$$\begin{array}{rccc} \varepsilon_g : & G & \longrightarrow & \mathbb{C} \\ & x & \longmapsto & \varepsilon_g(x) = \begin{cases} 1 \text{ si } g = x \\ 0 \text{ sinon} \end{cases} \end{array}.$$

Tout élément a de $\mathscr{F}(G)$ s'écrit donc de manière unique sous la forme

$$a = \sum_{g \in G} a_g \varepsilon_g \text{ avec } a_g \in G (a_g = a(g)).$$

Les éléments de cette bas seront maintenant notés $g, g \in G$. On identifie les élements de $\mathscr{F}(G)$ à des sommes formelles :

$$\sum_{g \in G} a_g g, a_g \in \mathbb{C}.$$

Définition 5.0.1. L'algèbre de groupe $\mathbb{C}[G]$ du groupe fini G est le $\mathbb{C}$-espace vectoriel de fonctions de G dans $\mathbb{C}$:

$$\mathbb{C}[G] = \left\{ a = \sum_{g \in G} a_g g, a_g \in \mathbb{C} \right\}$$

muni d'une structure d'algèbre pour la multiplication suivante (appelée produit de convolution) : $\varepsilon_g \varepsilon_t = \varepsilon_{gt}$ et prolongé par linéarité, i. e.

$$ab = \left(\sum_{g \in G} a_g g \right) \left(\sum_{t \in G} b_t t \right)$$

où gt est donné par la loi de composition interne de G.

On montre que le centre de $\mathbb{C}[G]$ est de dimension égale au nombre s de classes de conjugaison de G et une base de sous-espace vectoriel donnée par :

$$\left\{ z_i = \sum_{g \in c_i} g, i = 1, \dots, s \right\}$$

où les c_i sont les classes de conjugaison.

Deuxième partie

Représentations de groupes de Lie

INTRODUCTION

Notations

06-11-2023

1. $\mathbb{K}$ est un corps réel ou complexe $\mathbb{R}$ ou $\mathbb{C}$;
2. Produit scalaire (complexe) $\langle \cdot, \cdot \rangle : V \times V \longrightarrow \mathbb{C}$ tel que

$$\langle v, dw_1 + w_2 \rangle = d\langle v, w_1 \rangle + \langle v, w_2 \rangle$$
$$\langle v, w \rangle = \overline{\langle w, v \rangle}$$
$$\langle v, v \rangle \geq 0 \text{ et } \langle v, v \rangle = 0 \iff v = 0.$$

Exemple standart dans $\mathbb{C}^n$:

$$\langle v, w \rangle = \sum_{j=1}^{n} \overline{v_j} w_j.$$

Motivations

Exemple. L'équation qui décrit l'émission de l'hydrogène pour $\psi \in L^2(\mathbb{R}^3, \mathbb{C})$:

$$-\sum_{j=1}^{3} \frac{\partial^2 \psi(x)}{\partial x_j^2} - \frac{1}{|x|}\psi(x) = E\psi(x). \tag{$\star$}$$

On considère

$$R \in \mathbb{M}(3; \mathbb{R}) = \{(A_{jk}), A_{jk} \in \mathbb{R}, j, k \in \{1, 2, 3\}\}.$$

Une matrice orthogonale est telle que

$$\sum_{k=1}^{3} R_{ik} R_{jk} = \delta_{ji} = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ sinon.} \end{cases}$$

Alors

$$\sum_{j=1}^{3} \frac{\partial^2 \psi(Rx)}{\partial x_j^2} = \sum_{j=1}^{3} \left(\frac{\partial^2 \psi}{\partial x_j^2} \right)(Rx).$$

Or on a $|Rx| = |x|$. Donc si on définit $\psi_R \in L^2, \psi_R(x) := \psi(Rx)$, alors ψ est solution de $\star$ si et seulement si ψ_R est solution de $\star$.

Prenons

$$O(3) = \left\{ A \in \mathbb{M}(3;\mathbb{R}); \sum_{j=1}^{3} R_{ik}R_{jk} = \delta_{ji}, i, j \in \{1,2,3\} \right\}.$$

$O(3)$ est un groupe.

Soit $\pi(R) : L^2(\mathbb{R}^3, \mathbb{C}) \longrightarrow L^2(\mathbb{R}^3, \mathbb{C})$ telle que $\pi(R)\psi(x) := \psi(R^{-1}x)$, donc $\psi(R)\psi(S) = \pi(RS)$. Ainsi

$$R \in O(3) \longmapsto \pi(R) \in \mathbb{B}(L^2(\mathbb{R}^3, \mathbb{C}))$$

(sur l'ensemble de fonctions linéaires continues sur L^2) est une représentation.

La connaissance des représentations donne les possibilités de l'espace des solutions.

Exemple. Les interactions fondamentales connues à ce jour :

1. l'interaction nucléaire forte (quark) ;
2. l'interaction nucléaire faible (radioactivité) ;
3. l'interaction électromagnétique ;
4. la gravitation.

Les équations qui décrivent les trois premières interactions sont invariantes par $SU(3) \times SU(2) \times U(1)$.

Remarque. On considère l'ensemble des matrices unitaires :

$$U(n) = \left\{ A \in \mathbb{M}(n;\mathbb{C}); \sum_{1}^{n} \overline{A_{ki}} A_{kj} = \delta_{ij} = \sum_{1}^{n} A_{ik}\overline{A_{jk}} \right\}.$$

Le groupe des matrices unitaires telle que le déterminant vaut 1 est appelé le groupe spécial unitaire :

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

CHAPITRE 6

GROUPES DE LIE MATRICIELS (GROUPE DE LIE LINÉAIRES)

Un groupe de Lie dépend continuellement de certains paramètres et le cadre naturel est celui d'une variété différentielle.

Exemple. On rappelle la définition du groupe spécial linéaire $SL(2;\mathbb{R}) = \{A \in \mathbb{M}(2;\mathbb{R}), \det(A) = 1\}$.

$$A \in \mathbb{M}(2;\mathbb{R}) \iff A = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, x_1, \ldots, x_4 \in \mathbb{R}.$$

Alors $A \in SL(2;\mathbb{R})$ si et seulement si $f(x) := x_1x_4 - x_2x_3 = 1$. Donc $SL(2;\mathbb{R}) = f^{-1}(\{1\})$. On remarque que $f \in \mathcal{C}^\infty(\mathbb{R}^4, \mathbb{R})$, on a

$$\nabla f(x) = \begin{pmatrix} x_4 \\ -x_3 \\ -x_2 \\ x_1 \end{pmatrix} \neq 0 \text{ si } f(x) = 1.$$

Donc (par le théorème de géométrie différentielle) $SL(2;\mathbb{R})$ est une sous-variété.

Dans ce cours, on ne s'intéresse ici qu'au cas des sous-groupes **fermés** de

$$GL(n,\mathbb{C}) = \{A \in \mathbb{M}(n;\mathbb{C}), A \text{ inversible}\}$$

et on démontrera que ce sont des surfaces (théorème de Cartan et son corollaire 3.4.5).

Définition 6.0.1.

1. On considère l'espace $\mathbb{M}(n;\mathbb{K})$ muni de la topologie produit.
2. $GL(n;\mathbb{K})$ est le sous-groupe des matrices inversibles.

Proposition 6.0.1 (Propriétés)**.**

1. La topologie produit est la moins fine rendant les projections

$$\begin{array}{rccc} p_{jk} : & \mathbb{M}(2;\mathbb{K}) & \longrightarrow & \mathbb{K} \\ & p_{jk}(A) & \longmapsto & A_{jk} \end{array}$$

continues (les antécédents des A_{jk} sont en fait des ouverts de $\mathbb{M}(2;\mathbb{K})$).

2. Soit $(A^{(m)})_{m\in\mathbb{N}}$ une suite de matrices $n\times n$. Elle est convergente vers A dans la topologie produit si et seulement si tous les coefficients de la suite des matrices convergent vers les coefficients de A, autrement dit

$$\left|A^{(m)}_{jk} - A_{jk}\right| \underset{m\to\infty}{\longrightarrow} 0, \forall j,k.$$

3. C'est aussi la topologie définie par la norme

$$\|A\|_\infty := \sup_{j,k} |A_{jk}|\,.$$

4. Les topologies d'un espace vectoriel dimension finie définies par les normes sont toutes équivalentes, donc la topologie produit est aussi donnée par la norme

$$\|A\|_F = \sqrt{\sum_{j,k=1}^{n} |A_{jk}|^2}$$

qui a la propriété d'être une norme d'**algèbre**, autrement dit

$$\|AB\|_F \leq \|A\|_F\,\|B\|_F\,.$$

5. Le déterminant est une fonction continue, i.e. $\det \in \mathcal{C}^0(\mathbb{M}(n;\mathbb{K}),\mathbb{K})$, car c'est un polynôme des les projections p_{jk} qui sont continues.
6. $GL(n;\mathbb{K}) = \det^{-1}(\mathbb{K}\setminus\{0\})$ est un ouvert (antécédent d'un ouvert (car complémentaire d'un singleton fermé)).
7. Les applications qui associent une matrice inversible à une matrice inversible

$$\begin{array}{rccc} f: & GL(n;\mathbb{K}) & \longrightarrow & GL(n;\mathbb{K}) \\ & A & \longmapsto & f(A) := BA \\ & A & \longmapsto & f(A) := A^{-1} \\ & A & \longmapsto & f(A) := A^{*} \end{array}$$

ont toutes la propriété que les projections $p_{jk}\circ f$ s'écrivent comme un polynôme dans les projections qui ne s'annullent pas. Donc $f \in \mathcal{C}^0(GL(n;\mathbb{K}), GL(n;\mathbb{K}))$.

Définition 6.0.2. Un **groupe de Lie matriciel** (aussi appelé groupe de Lie linéaire) est un sous-groupe ***fermé*** dans $GL(n;\mathbb{C})$.

Proposition 6.0.2. G est fermé si et seulement si $G = F\cap G$ avec F un fermé de $GL(n;\mathbb{C})$. Donc F est fermé dans $GL(n;\mathbb{C})$ si $F = GL(n;\mathbb{C})\cap\mathscr{F}$, avec $\mathscr{F}$ un fermé de $\mathbb{M}(n;\mathbb{C})$.

1. $G\subset GL(n;\mathbb{K})$, i.e. si G est fermé dans $\mathbb{M}(n,\mathbb{K})$, alors G est fermé dans $GL(n;\mathbb{K})$.
2. Si G est fermé dans $GL(n;\mathbb{K})$, on n'a pas G fermé dans $\mathbb{M}(n;\mathbb{K})$. Par exemple, $(0,1]$ est fermé dans $(0,2)$ mais n'est pas fermé dans $\mathbb{R}$.
3. G est fermé dans $GL(n,\mathbb{K})$ si et seulement si pour toute suite $(A^{(m)})_{m\in\mathbb{N}}$ dans G si $\lim_{m\to\infty} A^{(m)} = A$, alors $A\in G$ ou $A\notin GL(n;\mathbb{K})$.
4. $G = GL(n,\mathbb{Q})$ est un sous-groupe de matrices inversibles $GL(n;\mathbb{K})$, mais n'est pas un groupe fermé.

Proposition 6.0.3. Les groupes suivants sont les groupes de Lie matriciels : 13-11-2023

1. $GL(n;\mathbb{C})$;
2. $GL(n;\mathbb{R})$;
3. $SL(n;\mathbb{C}) = \{A \in GL(n,\mathbb{C}) \mid \det(A) = 1\} = \det^{-1}(\{1\})$ (qui est un fermé de $GL(n;\mathbb{C})$) ;
4. $SL(n;\mathbb{R}) = \{A \in GL(n;\mathbb{R}), \det(A) = 1\}$;
5. $U(n) = \{A \in GL(n,\mathbb{C}), A^*A = \mathrm{id}\}$;
6. $SU(n) = \{A \in U(n), \det(A) = 1\}$;
7. $O(n) = \{A \in \mathbb{M}(n;\mathbb{R}), A^tA = \mathrm{id}\}$;
8. $SO(n) = \{A \in O(n), \det(A) = 1\}$;
9. Groupe de Heisenberg
$$H = \left\{ A \in \mathbb{M}(3;\mathbb{R}), A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \text{ pour } x,y,z \in \mathbb{R} \right\}.$$
10. Soient $p,q \in \{0,\dots,n\}$ tels que $p+q=n$. Le groupe unitaire généralisé
$$U(p,q) = \left\{ A \in \mathbb{M}(n,\mathbb{C}), A^* \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix} \right\},$$
où 1 apparait p fois $et - 1$ q fois . On a aussi
$$SU(p,q) = \{1 \in U(p,q), \det(A) = 1\}.$$
11. Le groupe orthogonal généralisé :
$$O(p,q) = \left\{ A \in \mathbb{M}(n;\mathbb{R}) = A^t \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix} \right\},$$
où 1 apparait p fois $et - 1$ q fois .
Dans le cas de $O(3,1)$, on parle de **groupe de Lorentz**.
12. Le groupe symplectique
$$Sp(2n;\mathbb{R}) = \left\{ A \in \mathbb{M}(2n,\mathbb{R}), A^t \begin{pmatrix} 0 & \mathrm{id}_n \\ -\mathrm{id}_n & 0 \end{pmatrix} A = \begin{pmatrix} 0 & \mathrm{id}_n \\ -\mathrm{id}_n & 0 \end{pmatrix} \right\}$$

Démonstration.

1.
2. C'est un sous-groupe (évident). Vérifions que c'est un fermé dans $GL(n;\mathbb{C})$. En effet, si $(A^{(m)})_{m\in\mathbb{N}}$ est une suite de $GL(n;\mathbb{R})$, alors
$$\lim_{m\to\infty} A^{(m)} = A \in GL(n;\mathbb{R})$$

ou bien, si A n'est pas inversible, alors $A \notin GL(n;\mathbb{R})$.

3. On a $\det(A)\det(B) = \det(AB)$. Donc si $\det(A)\det(A^{-1}) = 1$, alors $\det(A^{-1}) = 1$. Ainsi
$$SL(n;\mathbb{C}) = \det{}^{-1}(\{1\}).$$
4. Pareil que dans $\mathbb{C}$.
5. Vérifions que c'est un sous groupe. On a
$$(AB)^*AB = B^* \underbrace{A^*A}_{=\mathrm{id}} B = \mathrm{id}$$
$$\text{et } (A^{-1})^*A^{-1} = (A^*)^{-1}A^{-1} = (AA^*)^{-1} = \mathrm{id}\,.$$
Vérifions que c'est un fermé. Soit $f(A) = A^*A - \mathrm{id}$. f est continue, car produit de fonctions continues. On a $U(n) = f^{-1}(\{0\})$, or $\{0\}$ est un fermé dans $\mathbb{M}(n;\mathbb{C})$, donc $U(n)$ est un fermé de $\mathbb{M}(n;\mathbb{C})$, donc de $GL(n;\mathbb{C})$.
6.
7.
8.
9. On a
$$AB = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & b+xc+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$
et
$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix}.$$
Donc c'est un sous-groupe. On a
$$H = \mathbb{M}(3;\mathbb{R}) \cap p_{11}^{-1}(\{1\}) \cap p_{22}^{-1}(\{1\}) \cap p_{33}^{-1}(\{1\}) \cap p_{31}^{-1}(\{0\}) \cap p_{21}^{-1}(\{0\}) \cap p_{32}^{-1}(\{0\}).$$
Donc c'est un fermé.
10. En TD.

♣

Proposition 6.0.4. Les groupes suivants sont isomorphes à des groupes de Lie matriciels :

1. **Le groupe euclidien :**
$$E(n) := \{f : \mathbb{R}^n \longrightarrow \mathbb{R}^n, f(x) = Ax + b \text{ avec } b \in \mathbb{R}^2, A \in O(n)\}.$$
2. **Le groupe de Poincaré :**
$$P(n,1) := \{f \in \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^{n+1}, f(x) = Ax + b, b \in \mathbb{R}^{n+1}, A \in O(n,1)\}.$$
3. $(\mathbb{R}^*, \times) \simeq GL(1,\mathbb{R})$;
4. $(\mathbb{C}, \times) \simeq GL(1,\mathbb{C})$;
5. $S^1 = \{z \in \mathbb{C}, |z| = 1\} \simeq \varphi(1)$.
6. $(\mathbb{R}, +) \simeq GL(1,\mathbb{R})^+ = \{A \in \mathbb{M}(1;\mathbb{R}), \det(A) > 0\}$.

6.1 Propriétés topologiques des groupes de Lie matriciels

Nous nous intéressons aux propriétés suivantes : compacité, connexité, supplémentaire connexe.

Définition 6.1.1. Un groupe de Lie matriciel est **compact** s'il est un sous-ensemble compact de $\mathbb{M}(n;\mathbb{C})$.

Proposition 6.1.1 (Propriétés)**.** fonction

1. La topologie de $\mathbb{M}(n;\mathbb{C})$ est celle d'un espace vectoriel normé, donc G est compact si et seulement si G est fermé et borné.
2. G compact si et seulement si $\forall (A^{(m)})_{m\in\mathbb{N}} \subset G$. Si $\lim A^{(m)} = A$, alors $A \in G$ et

$$\exists c > 0, \forall A \in G, \forall j,k \in \{1,\dots,n\}, |A_{j,k} < c| .$$

Proposition 6.1.2.

1. $O(n), SO(n), U(n), SU(n)$ sont compacts.
2. $SL(n,\mathbb{C})$ si $n \geq 2$, $Sp(2n,\mathbb{R}), GL(n,\mathbb{K})$ et $O(p,q)$ si $p \neq q \neq 0$ ne sont pas compacts.

Démonstration.

1. On a vu que ce sont des fermés de $\mathbb{M}(n;\mathbb{C})$ et les colonnes sont de longueur 1, donc bornés.
2. On a $A \in \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & \frac{1}{x} & \dots & 0 \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix} \in SL(n,\mathbb{C})$ pour $x \neq 0$. Donc si $SL(n,\mathbb{C})$ n'est pas borné, alors $GL(n,\mathbb{K})$ non borné. Les autres groupes sont donnés en exercice.
   Remarque importante : $Sp(2,\mathbb{R}) = SL(2,\mathbb{R})$.

♣

Définition 6.1.2.

1. Un groupe de Lie matriciel G est **connexe** (par arcs) si

$$\forall A,B \in G, \exists c \in \mathcal{C}^0([0,1],G), c(0) = A, c(1) = B.$$

2. La composante connexe de l'identité est

$$G_0 := \{A \in G, \exists c \in \mathcal{C}^0([0,1],G), c(0) = \mathrm{id}, c(1) = A\}.$$

   Les groupes de Lie matriciels connexes par arcs sont connexes (ce sont deux notions équivalentes pour les groupes de Lie).

Proposition 6.1.3. G_0 est un sous-groupe distingué.

Démonstration. La multiplication de groupe et l'inverse étant continues, on a, pour $A, B \in G_0$, c_A, c_B des arcs connectant à l'identité :

$$t \longmapsto (c_A(t))^{-1} \in \mathcal{C}^0, c_A(t)^{-1} \big|_{t=0} = \mathrm{id}, (c_A(1))^{-1} = A^{-1}.$$

De plus, on a

$$t \longmapsto c_A(t)c_B(t) \in \mathcal{C}^0, c_A(t)c_B(t) \big|_{t=0} = \mathrm{id}, c_A(1)c_B(1) = AB,$$

donc G_0 est un groupe. Pour $B \in GL(n, \mathbb{K})$, on a

$$t \longmapsto Bc_A(t)B^{-1} \in \mathcal{C}^0, Bc_A(0)B^{-1} = \mathrm{id}, Bc_A(1)B^{-1} = BAB^{-1},$$

donc $BAB^{-1} \in G_0$. ♣

Proposition 6.1.4.

1. L'image d'un connexe par une fonction continue est connexe (TVI généralisé), donc AG_0 est connexe pour $A \in G$. C'est la composante connexe de A.
2. G/G_0 est un groupe (groupe des composantes connexes).
3. $\mathbb{C}^* = GL(1, \mathbb{C})$ est connexe.
4. De même, $U(1) \subset GL(1; \mathbb{C})$ est connexe.
5. $GL(1; \mathbb{R}) \subset GL(1; \mathbb{C})$ n'est pas connexe (2 composantes) ;
6. $O(2)$ a deux composantes connexes (TD).
7. $O(1, 1)$ a deux composantes connexes (TD).

Proposition 6.1.5. $GL(n, \mathbb{C})$ est connexe $\forall n \in \mathbb{N}$.

Démonstration. Soit $A \in GL(n; \mathbb{C})$ et $C \in GL(n; \mathbb{C})$ tels que $C^{-1}AC$ soit une matrice triangulaire. Les λ_j sont les valeurs propres, $\lambda_j \in \mathbb{C}^*$ qui est connexe. Soit $\lambda_j(\cdot) \in \mathcal{C}^0([0, 1], \mathbb{C}^*), \lambda_j(0) = 1, \lambda_j(1) = \lambda_j$.

Soit

$$A(t) = C \begin{pmatrix} \lambda_1(t) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n(t) \end{pmatrix} C^{-1} + tCNC^{-1},$$

alors $A(\cdot) \in \mathcal{C}^0([0, 1], GL(n, \mathbb{C})), A(0) = \mathrm{id}, A(1) = A$. Donc $GL(n, \mathbb{C})$ est connexe. ♣

Proposition 6.1.6. Pour $A \in \mathbb{M}(n; \mathbb{C})$, il existe $C \in GL(n; \mathbb{C})$ tel que $C^{-1}AC$ est triangulaire supérieure.

Corollaire 7.

1. Les éléments diagonaux sont les valeurs propres.
2. C peut être choisie unitaire.

Proposition 6.1.7.

1. $SL(n,\mathbb{C})$ est connexe.
2. $U(n), SU(n)$ sont connexes.
3. $SO(n)$ est connexe.

Démonstration.

1. Dans la preuve pour $GL(n,\mathbb{R})$, choisir les mêmes $\lambda_n(1),\ldots,\lambda_{n-1}(t)$ et $\lambda_n(t) := \dfrac{1}{\lambda_1(1)\ldots\lambda_{n-1}(t)}$.
   Alors $\lambda_n(\cdot) \in \mathcal{C}^0, \lambda_1(0) = 1, \lambda_n(1) = \lambda_n$, car $\lambda_1 \ldots \lambda_n = \det(A) = 1$ et $\det(A(t)) = 1, \forall t$.
2. $A \in U(n)$ est unitairement diagonalisable et ses valeurs propres sont de $U(1)$.
   On pose
   $$A = C \begin{pmatrix} e^{i\theta_1} & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & e^{i\theta_n} \end{pmatrix}.$$
   $t \longmapsto A(t)$ est continue, $A(t) \in U(n)$, $A(0) = \mathrm{id}, A(1) = 1$, donc $U(n)$ est connexe.
   Pour $A \in SU(n)$, on remplace $e^{i\theta_n t}$ par $e^{-it(\theta_1+\cdots+\theta_{n-1})}$.

♣

Définition 6.1.3. Soit G un espace topologique connexe par arcs. On dit que G est simplement connexe si pour tout lacet $C \in \mathcal{C}^0([0,1],G), c(0) = c(1)$, il existe $H_C \in \mathcal{C}^0([0,1]\times[0,1],G)$ tel que 15-11-2023

1. $H_C(S,0) = H_C(S,1)$ pour tout S (famille de lacets),
2. $H_C(0,t) = C(t)$ pour tout t (départ C),
3. $H_S(1,t) = H_C(1,0)$ pour tout t (arrivée en un point).

On dit alors que H_C est une homotopie qui pour chaque lacet S déforme le lacet C en un point, ou encore que C est une homotopie en un point.

Exemple. On pose $G = \mathbb{C}\setminus\{0\}$, $c(t) = 2+\cos(2\pi t) + i\sin(t)$ et $H_c(s,t) = (2+(1-s)\cos(2\pi t)) + i(1-s)\sin(2\pi)$. C'est un lacet pour chaque s.

1. $H_c(0,t) = c(t)$;
2. $H_c(1,t) = 2$ (lacet constant).

Proposition 6.1.8.

1. $\mathbb{R}^n$ est simplement connexe.
2. $\mathbb{C}\setminus\{0\}$ n'est pas simplement connexe.
3. $U(1)$ n'est pas simplement connexe.
4. $SO(2)$ n'est pas simplement connexe.
5. $U(n), GL(n;\mathbb{C})$ ne sont pas simplement connexes.
6. $SU(2)$ est simplement connexe.
7. $SO(3)$ n'est pas simplement connexe.

Démonstration.

1. Soit c un lacet, alors pour $p \in \mathbb{R}^n$,
$$H_c(s,t) = (1-s)c(t) + sp$$
est une homotopie qui déforme le lacet c dans le lacet constant $t \longmapsto p$.
2. Soit le lacet $c(t) = e^{i2\pi 3}$. On ne peut pas le déformer en un lacet constant, car toute déformation doit tourner une fois autour de 0.
3. $t \longmapsto e^{i2\pi t}$ ne peut être contracté.
4. Il est homéomorphe à $cl(1)$.
5. $\begin{pmatrix} e^{i2\pi t} & 0 & \dots & \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ ne peut être contracté.
6. $SU(2)$ est homéomorphe à S^3 (exercice) qui est simplement connexe (exercice).
7. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$ ne peut être contracté en $SO(3)$.

♣

On va détailler la preuve du 2.

Lemme. Il existe une fonction $\theta : \mathcal{C}^0(S^1 \setminus \{-1\}, (-\pi,\pi))$ telle que $x = \cos(\theta(x)), \sin(\theta(x)))$.

Démonstration. Pour $(x_1, x_2) \in S^1 \cap H_1$, $\theta(x) = \arcsin(x_2)$ qui est continue, car réciproque d'une fonction strictement croissante. On a
$$0 < \cos(\theta(x)) = \sqrt{1 - \sin^2(\theta(x))} = \sqrt{1 - x_2^2} = x_1.$$
Pour $(x_1, x_2) \in S^1 \cap H_2$, $\theta(x) = \arccos(x_1)$ est continue.
$$0 > \sin(\theta(x)) = -\sqrt{1 - \cos^2(\theta(x))} = -\sqrt{1 - x_1^2} = x_2.$$
On a $(x_1, x_2) \in (S^1 \cap H_2) \cap (S^1 \cap H_1)$ et $\arccos(x_1) = \arcsin(x_2)$. De même pour H_S, donc θ est continue. ♣

Proposition 6.1.9.

1. $z \longmapsto e^z = \displaystyle\sum_{n=0}^{\infty} \frac{z^n}{n} \in \mathcal{C}^0(\mathbb{C}, \mathbb{C} \setminus \{0\})$.
2. Il existe $e \in \mathcal{C}^0(\mathbb{C} \setminus (-\infty, 0], \mathbb{C})$ tel que
$$\forall z \in \mathbb{C} \setminus (-\infty, 0], e \circ p \circ e(z) = z.$$

Démonstration. On a $e(z) = \log(z) + i\theta\left(\frac{z}{|z|}\right)$, avec $\log(r) = \int_1^r \frac{1}{x} dx$. ♣

Proposition 6.1.10. Soit $c \in \mathcal{C}^0([0,1],\mathbb{C}), c(0) = c(1)$ un lacet et $p \in \mathbb{C} \setminus \{0\}$. S'il existe une homotopie qui déforme c en le point p, alors

$$c(t) = pe^{i2\pi\theta(t)},$$

avec $g \in \mathcal{C}^0([0,1],\mathbb{C}), g(1) = g(0)$.

Corollaire 8. $c(t) = e^{i2\pi t}$ ne peut pas être déformé en p.

6.2 Homomorphismes

Définition 6.2.1. Soient G, H deux groupes de Lie.

1. $f : G \longrightarrow H$ est appelé homomorphisme de groupes de Lie si

$$\forall A, B \text{ et } f \in \mathcal{C}^0(G,H), f(AB) = f(A)f(B).$$

2. Si un homomorphisme f est bijectif et $f^{-1} \in \mathcal{C}^0$, (donc f est un homéomorphisme), alors f est appelé **isomorphisme de groupes de Lie**.

Proposition 6.2.1 (Propriété)**.** On va démontrer ultérieurement que G, H sont des sous-[...] et que $f \in \mathcal{C}^\infty$.

Exemple.

1. $\det : GL(U,\mathbb{C}) \longrightarrow \mathbb{C}^*$ est continu et $\det(AB) = \det(A)\det(B)$.
2. $f : \mathbb{R} \longrightarrow U(1)$, $f(x) = e^{2\pi ix}$ homéomorphisme et $f(x+y) = f(x) + f(y)$, donc c'est un homéomorphisme de groupes de Lie.
3. $f : U(1) \longrightarrow SO(2), f(z) = \begin{pmatrix} \Re(z) & -\Im(z) \\ \Im(z) & \Re(z) \end{pmatrix}$.

6.3 Isomorphismes

Un exemple important est l'homomorphisme $SU(2) \longrightarrow SO(z)$ qui n'est pas un isomorphisme.

Proposition 6.3.1. Soit

$$V = \{X \in \mathbb{M}(z,\mathbb{C}), X = X^*, \mathrm{Tr}(X) = 0\}$$

et $\langle X, Y\rangle = \mathrm{Tr}(X^*Y)$ le produit scalaire.

Soit, pour $U \in SU(2)$, $f(U) : V \longrightarrow V$, $f(U)(X) = U^*XU$ (on aura $\mathrm{Tr}(f(U)(X)) = \mathrm{Tr}(U^*XU) = \mathrm{Tr}(UU^*X) = \mathrm{Tr}(X)$). Alors

$$\forall X, Y \in V, \langle f(U)(X), f(U)(Y)\rangle = \langle X, Y\rangle.$$

$f : SU(2) \longrightarrow O(V)$ est un homomorphisme surjectif sur $SO(V)$ tel que $\mathrm{Ker}(f) = \{\mathrm{id}, -\mathrm{id}\}$.
V est un espace vectoriel réel de dimension 3. Soit pour une base orthonormée $\{b_1, b_2, b_3\}$,

$$i : V \longrightarrow \mathbb{R}^3, i\left(\sum_{j=1}^{3} x_j b_j\right) = (X_1, X_2, X_3).$$

$SU(2) \in A \longrightarrow i \circ f(A) \circ i^{-1} \longrightarrow SO(3)$ est un homomorphisme surjectif de $\mathrm{Ker}\{\mathrm{id}, -\mathrm{id}\}$.

Démonstration. On a

$$\begin{gathered} f(U)(\lambda X + Y) = \lambda f(U)X + f(U)Y, \\ (f(U)(X))^* = U^*XU = f(U)(X), \\ \langle f(U)X, f(U)Y\rangle = \mathrm{Tr}(U^*XUU^*YU) = \mathrm{Tr}(X^*Y) = \langle X, Y\rangle, \\ f(U)f(V) = f(UV), f(U^*) = (f(U))^{-1}. \end{gathered}$$

$f \in \mathcal{C}^0$, car $A \in \mathbb{M}(2, \mathbb{C}) \longrightarrow A^*XA$ est une composée de fonctions continues. Pour tout $X \in \mathbb{M}(2, \mathbb{C}), SU(2)$ est connexe, donc $f(SU(2))$ est connexe et $\mathrm{id} = f(\mathrm{id}(SU(2)))$, donc $f(SU(2)) \subset SO(V)$, car c'est le plus petit ensemble connexe qui contient id. On démontrera la surjectivité en TD.

De plus, on a

$$f(U) = \mathrm{id} \iff U^*XU \iff UU^*XU = UX, \forall X \in V.$$

♣

Plus généralement :

Définition 6.3.1. Un groupe de Lie est une variété différentielle qui est un groupe tel que le produit $G \times G \longrightarrow G$ et l'inverse $(\cdot)^{-1} : G \longrightarrow G$ sont des fonctions différentiables.

Proposition 6.3.2 (Propriétés)**.**

1. Les groupes de Lie matriciels sont des groupes de Lie.
2. Il existe des groupes de Lie tels qu'il n'existe aucun homomorphisme injectif et continu à valeurs dans $GL(U, \mathbb{C})$.

Exemple. $G = \mathbb{R} \times \mathbb{R} \times S^1$,
$(a, b, c) \cdot (x, y, z) = a + x, b + y, e^{iay} \subset z$ (calcul à faire).

CHAPITRE 7

ALGÈBRE DE LIE

7.1 Exponentielle et logarithme des matrices

Proposition 7.1.1. Pour $A \in \mathbb{M}(n, \mathbb{C})$,

$$\exp(A) = e^A := \sum_{m=0}^{\infty} \frac{A^m}{m!}$$

est bien définie et $\exp \in \mathcal{C}^0(\mathbb{M}(n,\mathbb{C}), \mathbb{M}(n,\mathbb{C}))$.

Démonstration. On peut choisir la norme $\|A\|_F$ pour laquelle on a $\|A^m\|_F \leq \|A\|_F^m$, donc $\sum_0^\infty \frac{\|A\|^m}{m!}$ est convergente, donc $\sum_0^\infty \frac{A^m}{m!}$, car $\mathbb{M}(n,\mathbb{C})$ est complet.

Pour chaque N, $f_N(A) := \sum_{m=0}^N \frac{A^m}{m!} \in \mathcal{C}^0$, car polynôme des projections et

$$\sup_{\|A\|_F < R} \|f_N(A) - f_M(A)\| \leq \sum_N^M \frac{R^m}{m!} \underset{N,M \to \infty}{\longrightarrow} 0.$$

$\mathcal{C}^0(\mathbb{M}(n,\mathbb{C}), \mathbb{M}(n,\mathbb{C}))$ est complet, donc $\exp \in \mathcal{C}^0$. ♣

Proposition 7.1.2. Pour $A, B \in \mathbb{M}(n,\mathbb{C})$, 20-11-2023

1. $[A,B] = 0 \implies e^A e^B = e^{A+B}$.
2. Pour $C \in GL(n,\mathbb{C}), Ce^AC^{-1} = e^{CAC^{-1}}$.
3. $e^0 = \mathrm{id} = A$.
4. $e^{A^*} = (e^A)^*$.
5. $\exp : \mathbb{M}(n,\mathbb{C}) \longrightarrow GL(n,\mathbb{C})$ et
$$(e^A)^{-1} = e^{-A}.$$
6. $e^{(\lambda+\mu)A} = e^{\lambda A}e^{\mu A}, \forall \lambda, \mu \in \mathbb{C}$.

Démonstration.

1. Si $[A,B] = AB - BA = 0$, alors

$$(A+B)^m = \sum_0^m \frac{m!}{j!(m-j)!} A^j B^{m-j}.$$

2. Argument principal : continuité de la multiplication.
3.
4. L'opération $A \longmapsto A^*$ est continue.
5. $[-A, A] = 0$, doc $e^{-A+A} = e^0 = 1 = e^{-A}e^A$.
6. $[\lambda A, \mu A] = 0$.

♣

Remarque. Pour $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, on a $A^2 = B^2 = 0$ (matrices nilpotentes).

Alors

$$e^{tA} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, e^{tB} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, e^{tA}e^{tB} = \begin{pmatrix} 1+t^2 & t \\ t & 1 \end{pmatrix} \neq e^{t(A+B)} \text{ (preuve en TD).}$$

Proposition 7.1.3. Pour $A \in \mathbb{M}(n, \mathbb{C}), c(t) := e^{tA}, t \in \mathbb{R}$, on a $c \in \mathcal{C}^1(\mathbb{R}, \mathbb{M}(n, \mathbb{C}))$ et $\frac{d}{dt}c(t) = Ac(t), c(0) = \mathrm{id}$.

Démonstration. Pour tous j, k, $(e^{tA})_{jk}$ est une série entière avec

$$\frac{d}{dt}\sum = \sum \frac{d}{dt}.$$

♣

Remarque. En général on n'a pas

$$\frac{d}{dt}e^{X+tY} \neq e^{X+tY}Y \neq Ye^{X+tY}.$$

Exemple avec les matrices définies dans la remarque précédente.

Remarque (Calcul de $\exp(A)$ en pratique)**.**

1. Si A est diagonalisable, alors

$$A = C^{-1} \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix} C$$

et

$$e^A = C^{-1} \begin{pmatrix} e^{\lambda_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & e^{\lambda_n} \end{pmatrix} C.$$

2. Si A est nilpotente avec $A^j = 0$, alors
$$e^A = 1 + A + \frac{1}{2!}A^2 + \cdots + \frac{1}{(j-1)!}A^{j-1}.$$
3. Pour $A \in \mathbb{M}(n, \mathbb{C})$, il existe S diagonalisable et N nilpotente telles que $[S, N] = 0$ et $A = S + N$, alors $e^A = e^S e^N$.

Exemple.
$$\exp\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a & b + \frac{ac}{2} \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

7.2 Logarithme matriciel

Remarque. $z \in \mathbb{C} \longmapsto \exp z \in \mathbb{C} \setminus \{0\}$ est surjective, elle n'est pas injective, c'est un logarithme continu qui ne peut être défini que sur $\mathbb{C} \setminus (-\infty, 0]$.

Lemme.
1. $\log(z) := \sum_1^\infty -\frac{1}{m}(1-z)^m$, avec $z \in B(1,1)$, est analytique et $e^{\log(z)} = z$.
2. $\exp(B(0, \log(z))) \subset B(1,1)$ et $\log(e^z) = z$ $(z \in B(0, \log(z)))$.

Démonstration.
1. Pour $x \in \mathbb{R}, |x| < 1$,
$$\log(x) = \int_1^x \frac{1}{1-(1-y)} dy = \int_1^x \sum_{n=0}^\infty (1-y)^n dy = -\sum_{n=0}^\infty \frac{(1-x)^n}{n}$$
par analycité pour $z \in \mathbb{C}$.
2. On a
$$|e^z - 1| \leq \sum_{n=1}^\infty \frac{|z|^n}{n!} \leq e^{|z|} - 1 < z - 1$$
si $|z| \leq \log(z)$. On a $\log(e^z) = z$ pour $z \in B(0, \log(z)) \cap \mathbb{R}$ et $e^{\log(z)} = z$ pour $B(1,1) \cap \mathbb{R}$, donc par analycité c'est vrai partout.

♣

Proposition 7.2.1.

1. Soit $B(\mathrm{id}, 1) = \{A \in \mathbb{M}(n, \mathbb{C}), \|A - \mathrm{id}\| < 1\}$.

$$\log A = \sum_{n=1}^{\infty} -\frac{1}{n}(\mathrm{id} - A)^n,$$

   alors $\log \in \mathcal{C}^0(B(\mathrm{id}, 1), \mathbb{M}(n, \mathbb{C}))$ et $e^{\log A} = A, \forall A \in B(\mathrm{id}, 1)$.
2. Soit $B(0, \log z) := \{A \in \mathbb{M}(n, \mathbb{C}), \|A\|_F < \log z\}$, alors $\exp(B(0, \log z)) \subset B(\mathrm{id}, 1)$ et $\log e^A = A, \forall A \in B(0, \log z)$.

Proposition 7.2.2 (Propriété)**.** Pour $A = 2\pi i \,\mathrm{id}, e^A = \mathrm{id} \in B(\mathrm{id}, 1)$, mais $\log e^A = 0 \neq A$.

Théorème 7.2.1 (Formule de produit de Lie)**.** Pour $A, B \in \mathbb{M}(n, \mathbb{C})$,

$$e^{A+B} = \lim_{m\to\infty} (e^{A/m} e^{B/m})^m.$$

Lemme. Il existe $c > 0$ tel que $\forall B \in B(0, \frac{1}{2}) \subset \mathbb{M}(n, \mathbb{C})$, $\|\log(\mathrm{id} + B) - B\| \leq c \|B\|^2$.

Démonstration. $\mathrm{id} + B \in B(\mathrm{id}, 1)$ et

$$\log(\mathrm{id} + B) - B = \sum_{m=2}^{\infty} \frac{(-1)^{m+1}}{m} B^m = B^2 = \sum_{2}^{\infty} \frac{(-1)^{m+1}}{m} B^{m-2}.$$

De plus, on a

$$\sum_{2}^{\infty} \left\| \frac{B^{m-2}}{m} \right\| < \sum \frac{1}{2^{m-2}} = c < \infty.$$

♣

Démonstration du théorème 7.2.1. On a

$$e^{X/m} e^{Y/m} = \mathrm{id} + \frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right),$$

donc $e^{X/m} e^{Y/M} \in B(\mathrm{id}, 1)$ pour un m suffisamment grand. Donc $\log e^{X/m} e^{Y/m} = \frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)$. Alors

$$\exp(\log e^{X/m} e^{Y/m}) = e^{X/m} e^{Y/m} = \exp\left(\frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)\right),$$

donc

$$(e^{X/m} e^{Y/m})^m = \exp\left(m\left(\frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)\right)\right) = \exp\left(X + Y + O\left(\frac{1}{m}\right)\right).$$

Par continuité

$$\exp(X + Y) = \lim_{m\to\infty} (e^{X/m} e^{Y/m})^m.$$

♣

Proposition 7.2.3. Pour $X \in \mathbb{M}(n, \mathbb{C})$, $\det(e^X) = e^{\mathrm{Tr}(X)}$.

Démonstration. On rappelle que $Ce^X C^{-1} = e^{CXC^{-1}}$, donc si X est diagonalisable avec les valeurs propres z_j, alors e^X est diagonalisable avec les valeurs propres e^{z_j}. Donc

$$\mathrm{Tr}(X) = \sum_{j=1}^{m} z_j, e^{\mathrm{Tr}(A)} = \prod e^{z_j} = \det(e^X).$$

Soit $X \in \mathbb{M}(n, \mathbb{C})$ et $A \lim_{m\to\infty} X_m$, avec X_m diagonalisable, alors

$$\det(e^X) = \det(e^{\lim X_m}) = \lim \det(e^{X_m}) = \lim e^{\mathrm{Tr}(X_m)} = e^{\mathrm{Tr}(X)}.$$

♣

Définition 7.2.1. $A(\cdot) \in \mathcal{C}^0(\mathbb{R}, GL(n, \mathbb{C}))$ est appelé sous-groupe à un paramètre de $GL(n, \mathbb{C})$. Si $A(0) = \mathrm{id}$ et $A(t+s) = A(t)A(s), \forall s, t \in \mathbb{R}$.

Théorème 7.2.2. Soit $A(\cdot)$ un sous-groupe à un paramètre de $GL(n, \mathbb{C})$, alors il existe un unique $X \in \mathbb{M}(n, \mathbb{C})$ tel que

$$A(t) = e^{tX}.$$

Donc $A \in \mathcal{C}^1(\mathbb{R}, GL(n, \mathbb{C}))$ et $X = \frac{d}{dt} A(t) \big|_{t=0}$.

Pour la preuve on utilise

Lemme. Soit $\varepsilon < \frac{1}{2}\log(z)$ et $B \in V = \exp(B(0, \varepsilon)) = \{e^D, D \in \mathbb{M}(n, \mathbb{C}), \|D\| < \varepsilon\}$, alors

$$\sqrt{B} := e^{\frac{1}{2}\log(B)} \in V$$

est l'unique racine carrée dans V telle que $\sqrt{B}\sqrt{B} = B$.

Démonstration. On avait démontré qu'il y avait une correspondance entre $B(0, \log(z))$ et $\exp(B(0, \log(z))) \subset B(\mathrm{id}, 1)$ grâce aux fonctions log et exp. C'est un homéomorphisme.

De plus, $\log(B)$ et $\frac{1}{2}\log(B) \in B(0, \varepsilon)$ et $\sqrt{B}\sqrt{B} = e^{\log(B)} = B$.

Soit $C \in V$ tel que $C^2 = B$, alors $e^{\log(C)} = C$ et $e^{2\log(C)} = C^2 = B = e^{\log(B)}$. Comme $\|2\log(C)\| < \log(2)$, on a $2\log(C) = \log(B)$ et $C = \sqrt{B}$. ♣

Démonstration du théorème 7.2.2. Si X existe, alors il est unique, car $X = \frac{d}{dt} A(t) \big|_{t=0}$. Le V du lemme est ouvert, donc $A(t) \in V$ pour $|t| \leq t_0$ pour $t_0 > 0$.

Soit $X := \frac{1}{t_0}\log(A(t_0))$. Alors $X \in B(0, \varepsilon)$ et $A(t_0) = e^{t_0 X}$. Par ailleurs, $A(\frac{t_0}{2}) \in V$ et $(A(t_0/2))^2$, Par unicité de la racine,

$$A(t_0/2) = e^{t_0/2X}.$$

Par récurrence,

$$A\left(\frac{t_0}{2^k}\right) = e^{\frac{t_0}{2^k}X}, k \in \mathbb{N}.$$

C'est vrai aussi pour $m \in \mathbb{Z}$. $\left\{\frac{mt_0}{2}\right\}_{m\in\mathbb{Z},k\in\mathbb{N}}$ est dense dans $\mathbb{R}$, donc par continuité $A(t) = e^{tA}, \forall t \in \mathbb{R}$. ♣

Proposition 7.2.4. $\exp \in \mathcal{C}^\infty(\mathbb{M}(n,\mathbb{C}), \mathbb{M}(n,\mathbb{C}))$.

Démonstration. $(X^m)_{jk}$ est polynomiale. $\exp X$ est une série absolument convergente de rayon ∞, donc toutes les dérivées partielles existent et sont continues. ♣

7.3 Algèbre de Lie, exemples

Définition 7.3.1. Une **algèbre de Lie** (de dimension finie) sur $\mathbb{K}$ est un espace vectoriel $\mathfrak{g}$ (sur $\mathbb{K}$ de dimension finie) muni d'un **crochet de Lie** $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \longrightarrow \mathfrak{g}$ tel que

1. $[\cdot,\cdot]$ est bilinéaire ;
2. $[\cdot,\cdot]$ est antisymétrique ;
3. **L'identité de Jacobi** est satisfaite : on a, pour tout $X, Y, Z \in \mathfrak{g}, \lambda \in \mathbb{K}$,
   (a) $[X, \lambda Y + Z] = \lambda[X,Y] + [X,Z]$;
   (b) $[X,Y] = -[Y,X]$;
   (c) $[X,[Y,Z]] + [Z,[X,Y]] + [Y,[Z,X]] = 0$.

Si $[X,Y] = 0$, on dit que X et Y commutent. Si tous les éléments commutent, on dit que $\mathfrak{g}$ est abélienne.

Exemple.

1. Soit $\mathbb{V}$ un espace vectoriel, $\dim(\mathbb{V}) < \infty$ et $B(\mathbb{V})$ l'ensemble des applications linéaires, alors $B(\mathbb{V})$ est une algèbre de Lie, avec
$$[X,Y] = XY - YX.$$
2. $\mathfrak{g} \subset B(\mathbb{V})$ un sous-espace tel que $[\mathfrak{g},\mathfrak{g}] \subset \mathfrak{g}$.
3. $\mathfrak{g}(\mathbb{V}) := \{X \in B(\mathbb{V}), \mathrm{Tr}(X) = 0\}$. En effet,
$$\mathrm{Tr}(XY - YX) = \mathrm{Tr}(XY) - \mathrm{Tr}(YX) = 0.$$
4. $\mathfrak{g} := \mathbb{R}^3, [X,Y] = x \wedge y$. En effet,
   (a) bilinéaire ;
   (b) antisymétrique par construction $x \wedge y = -y \wedge x$;
   (c) $x \wedge (y \wedge z) + z \wedge (x \wedge y) + y \wedge (z \wedge x)$, car pour la base canonique, on a
      i. pour i, j, k différents,
      $$e_i \wedge (e_j \wedge e_k) + e_k \wedge (e_i \wedge e_j) + e_j \wedge (e_k \wedge e_i) = 0.$$
      ii. $i \neq j = k$: $e_i \wedge (e_j \wedge e_k) + e_k \wedge (e_i \wedge e_j) + e_j \wedge (e_k \wedge e_i) = 0$.
      iii. Si tous les indices sont les mêmes, les trois termes s'annullent.

Définition 7.3.2. Soit $(\mathfrak{g}, [\cdot, \cdot])$ une algèbre de Lie et $\mathfrak{h} \subset \mathfrak{g}$ un sous-espace tel que $[\mathfrak{h}, \mathfrak{h}] \subset \mathfrak{h}$ est 22-11-2023

1. appelé sous-algèbre de Lie de $\mathfrak{g}$ et
2. idéal si $[X, Y] \in \mathfrak{h}$
3. Le centre de $\mathfrak{g}$ est l'idéal $\{X \in \mathfrak{g}, [Y, X] = 0, \forall Y \in \mathfrak{g}\}$.

Définition 7.3.3. Soient $\mathfrak{g}, \mathfrak{h}$ des algèbres de Lie de dimension finie. φ est appelé **homomorphisme d'algèbres de Lie** si $\varphi([X, Y]) = [\varphi(X), \varphi(Y)], \forall X, Y \in \mathfrak{g}$. Si φ est une bijection, on l'appelle **isomorphisme d'algèbre de Lie** et **automorphisme d'algèbre de Lie** si $\mathfrak{g} = \mathfrak{h}$.

Proposition 7.3.1. $\mathrm{Ker}(\varphi)$ est un idéal.

Exemple. $\mathfrak{g} = \mathbb{R}^3$ avec le produit vectoriel et $\mathfrak{h} = \{X \in \mathbb{M}(3, \mathbb{R})\}$ avec le commutateur. On pose $\varphi : \mathfrak{g} \longrightarrow \mathfrak{h}$,

$$\varphi(x_1, x_2, x_3) = \begin{pmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{pmatrix}$$

est un isomorphisme d'algèbres de Lie.

Exemple. $\mathbb{K} = \{X \in \mathbb{M}(2, \mathbb{C}), \mathrm{Tr}(X) = 0\}$ avec commutateur. $\psi : \mathfrak{h} \longrightarrow \mathbb{K}$ défini comme suit :

$$\begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ b & a & 0 \end{pmatrix} \longmapsto \frac{1}{2i} \begin{pmatrix} c & a - ib \\ a + ib & -c \end{pmatrix}$$

est un isomorphisme d'algèbres de Lie.

Définition 7.3.4. Pour $x \in \mathfrak{g}$ une algèbre de Lie, soit $\mathrm{ad}_X : \mathfrak{g} \longrightarrow \mathfrak{g}, \mathrm{ad}_X := [X, Y]$. $\mathrm{ad} : \mathfrak{g} \longrightarrow \mathbb{B}(\mathfrak{g}), X \mapsto \mathrm{ad}_X$ est appelé l'application adjointe (ou représentation adjointe).

Proposition 7.3.2. $\mathrm{ad} : \mathfrak{g} \longrightarrow \mathbb{B}(\mathfrak{g})$ est un homomorphisme d'algèbres de Lie, i. e.

$$\mathrm{ad}_{[X,Z]} = [\mathrm{ad}_X, \mathrm{ad}_Z].$$

Théorème 7.3.1. Toute algèbre de Lie (de dimension finie) est isomorphe à une sous-algèbre de Lie de $\mathbb{M}((n,\mathbb{K}))$.

Démonstration. Cas où $\mathfrak{g}$ n'admet pas d'idéal non trivial, alors Ker(ad) = centre de $\mathfrak{g}$ est trivial, $\mathfrak{g}$ est isomorphe à $\mathrm{Im(ad)} = \mathbb{B}(\mathfrak{g})$.

Dans le cas général, c'est admis. ♣

Définition 7.3.5. La somme directe de deux algèbres de Lie $\mathfrak{g}_1, \mathfrak{g}_2$ est l'algèbre de Lie

$$\mathfrak{g}_1 \oplus \mathfrak{g}_2 = \{(x_1, x_2) \in \mathfrak{g}_1 \times \mathfrak{g}_2, x_j \in \mathfrak{g}_j\}$$
$$[(x_1, x_2), (y_1, y_2)] := ([x_1, y_1], [x_2, y_2]).$$

Définition 7.3.6. Une algèbre de Lie $\mathfrak{g}$ est appelée :

1. **irréductible** si elle n'admet pas d'idéal différent de $\{0\}$ et $\mathfrak{g}$;
2. **simple** si elle est irréductible et $\dim(\mathfrak{g}) > 1$ (si et seulement si elle est irréductible et non abélienne) ;
3. **semi-simple** si

$$g = \bigoplus_{i=1}^{n} \mathfrak{g}_i,$$

avec $\mathfrak{g}_i \subset \mathfrak{g}$ des sous-algèbres de Lie.

Exemple. $\mathfrak{Sl}(2, \mathbb{C}) = \{X \in \mathbb{M}(2, \mathbb{C}), \mathrm{Tr}(X) = 0\}$ est simple.

Démonstration. $X \in \mathfrak{Sl} \iff X = \begin{pmatrix} b & a \\ c & -b \end{pmatrix}, a, b, c \in \mathbb{C}$.

Donc $\mathfrak{Sl}$ est un espace vectoriel sur $\mathbb{C}$ engendré par H, X, Y avec

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

On a $[X, Y] = H, [H, X] = 2X, [H, Y] = -2Y$.

$\mathfrak{Sl}$ ♣