

# Chapitre 1

## Rappels sur groupes et actions de groupes

### 1.1 Exercices de révisions

**Exercice 1.1.1.** Déterminer tous les groupes finis d'ordre  $< 6$  à isomorphisme près.

**Exercice 1.1.2.** On admet qu'il n'existe que deux groupes différents d'ordre 6 (à isomorphisme près). Quels sont ces groupes ?

**Exercice 1.1.3** (Théorème de Lagrange). Soit  $G$  un groupe fini et  $H$  un sous-groupe de  $G$ . Le Théorème de Lagrange dit :  $\text{card } G = \text{card } H \text{ card } G/H$ .

1. Le démontrer.
2. Le reformuler en termes d'actions de groupes.

**Rappel :** Un sous-groupe  $H$  d'un groupe  $G$  est *distingué* si  $gHg^{-1} = H$  pour tout  $g \in G$ . Un groupe  $G$  est *simple* si ses seuls sous-groupes distingués sont  $\{e\}$  et  $G$ .

**Exercice 1.1.4.** Soit  $G$  un groupe abélien non-trivial. Montrer que  $G$  est simple si et seulement si il est fini, cyclique, d'ordre premier.

**Exercice 1.1.5.** Soit  $G$  un groupe agissant sur un ensemble  $E$ . Soient  $x \in E$  et  $g \in G$ . Montrer que  $\text{Stab}(x)$  est isomorphe à  $\text{Stab}(g \cdot x)$ .

**Exercice 1.1.6.** Montrer que tout groupe d'ordre  $n$  admet un morphisme injectif vers  $\mathfrak{S}_n$ .

**Exercice 1.1.7** (Exemples d'invariants de conjugaison). Soit  $G$  un groupe fini. Soient  $a$  et  $b$  deux éléments conjugués dans  $G$ .

1. Montrer que  $a$  et  $b$  ont même ordre.
2. On suppose que  $G$  agit sur un ensemble  $E$ . Montrer que les fixateurs de  $a$  et de  $b$  ont même cardinal.
3. Soit  $\phi$  un morphisme de  $G$  vers  $\mathfrak{S}_n$ . Montrer que  $\phi(a)$  et  $\phi(b)$  ont même signature.
4. Soit  $\phi$  un morphisme de  $G$  vers  $\text{GL}_n(\mathbb{C})$ . Montrer que  $\phi(a)$  et  $\phi(b)$  ont même déterminant et même trace.

**Exercice 1.1.8.** Existe-t-il deux plongements de  $G$  dans  $\mathfrak{S}_n$  tels que les deux images de  $a$  aient des signatures différentes ?

**Exercice 1.1.9.** Si  $a$  et  $b$  sont deux matrices inversibles qui ont même déterminant et même trace, sont-elles nécessairement conjuguées.

## 1.2 Automorphismes de graphes

**Comment obtient-on des groupes naturels et intéressants ?** On part d'un ensemble  $E$ , on ajoute une "structure intéressante"  $T$  sur  $E$ , par exemple, une structure de groupe, une structure d'espace vectoriel, un produit scalaire, etc. Le groupe  $G$  des bijections qui préservent cette structure est intéressant. **Remarque additionnelle :** Souvent, le groupe  $\text{Bij}(E)$  des bijections de  $E$  agit sur les structures qu'on essaie de mettre, et  $G = \text{Stab}(T)$  est le stabilisateur de la structure choisie  $T$  pour cette action.

Dans cette section on regarde un exemple : les automorphismes de graphes.

On fixe  $S$  un ensemble, dont les éléments seront appelés *sommets*.

**Définition 1.2.1.** On appelle *graphe orienté* sur  $S$  la donnée d'un sous-ensemble

$$A \subset S \times S \setminus \text{diag}(S).$$

On note  $(S, A)$  le graphe orienté. Les éléments de  $A$  sont appelés les arêtes du graphe.

On rappelle que  $\text{diag}(S) = \{(s, s) \in S \times S \mid s \in S\}$ .

Le groupe  $\text{Bij}(S)$  agit sur l'ensemble des graphes sur  $S$  : pour  $\sigma$  une bijection de  $S$ ,

$$\sigma \cdot (S, A) = (S, \{(\sigma(d), \sigma(f)) \mid (d, f) \in A\}).$$

**Définition 1.2.2.** Le groupe des automorphismes de  $(S, A)$ , noté  $\text{Aut}(S, A)$ , est le stabilisateur de  $(S, A)$  sous l'action de  $\text{Bij}(S)$ .

Autrement dit,

$$\text{Aut}(S, A) = \{\sigma \in \text{Bij}(S) \mid \forall (d, f) \in A, (\sigma(d), \sigma(f)) \in A\}.$$

**Exemple 1.2.3.** On prendra toujours  $S = \{1, 2, \dots, n\}$ , donc  $\text{Bij}(S) = \mathfrak{S}_n$ . Pour  $n = 1$ , on n'a qu'un seul graphe (sans arêtes), et son groupe d'automorphismes est trivial comme le groupe des bijections  $\mathfrak{S}_1$ .

Pour  $n = 2$ , il n'y a que trois structures de graphes possibles :  $A_1 = \emptyset$ ,  $A_2 = \{(1, 2)\}$ ,  $A_3 = \{(2, 1)\}$  et  $A_4 = \{(1, 2), (2, 1)\}$ . Le groupe symétrique  $\mathfrak{S}_2$  consiste en l'identité et la transposition  $(12)$ . La transposition envoie  $A_2$  sur  $A_3$ , et laisse fixe  $A_1$  et  $A_4$ . On a donc  $\text{Aut}(S, A_1) = \text{Aut}(S, A_4) = \mathfrak{S}_2$ , alors que  $\text{Aut}(S, A_2)$  et  $\text{Aut}(S, A_3)$  sont triviaux.

**Exercice 1.2.4.** Prendre un graphe sur trois ou quatre sommets au hasard, regarder ses images par tous les éléments du groupe symétrique, en déduire son groupe d'automorphismes.

**Rappel :** Une action d'un groupe  $G$  sur un ensemble  $E$  est *transitive* si il existe  $x$  dans  $E$  tel que  $\text{orb}(x) = E$ . L'action est *libre* si pour tout  $x \in E$ ,  $\text{Stab}(x) = \{id\}$ . L'action est *fidèle* si l'intersection des  $\text{Stab}(x)$  pour tous les  $x \in E$  est triviale.

**Exercice 1.2.5.** Pour  $n = 4$ , on considère les quatre ensembles d'arêtes suivants.

$$A_1 = \{(1, 3), (2, 4), (3, 1), (4, 2)\}$$

$$A_2 = \{(1, 3)\}$$

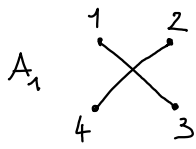
$$A_3 = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$$

$$A_4 = \{(1, 2), (2, 1), (3, 2), (2, 3), (3, 4), (4, 3), (1, 4), (4, 1)\}$$

1. Donner une représentation graphique (par convention, on dessine une flèche de  $a$  vers  $b$  pour l'arête  $(a, b)$ , et si  $\{(a, b), (b, a)\} \subset A$ , on dessine simplement un segment sans flèches (on dit que l'arête entre  $a$  et  $b$  est *non-orientée*).

2. Quels sont les groupes d'automorphismes ?
3. Dans chaque cas, est-ce que l'action induite par  $\text{Aut}(S, A_i)$  sur les sommets est libre ? transitive ? Même question pour l'action induite sur les arêtes.

**Exercice 1.2.6.** En trouvant un action non triviale et non fidèle de  $\mathfrak{A}_4$ , montrer que  $\mathfrak{A}_4$  n'est pas un groupe simple. (*indication* : considérer l'action de  $\mathfrak{A}_4$  sur certains graphes sur  $\{1, 2, 3, 4\}$ , par exemple inspirés de l'exercice précédent.)



$$\text{Aut}(S, A_4) = \{ \text{id}, (24), (13), (13)(24), (12)(34), (14)(32), (1234), (1432) \}$$

$$\#S_4 = \# \text{orb}(A_4) \# \text{Aut}(S, A_4)$$

$$24 = 3 \times 8$$

$$\text{orb}(A_4) = \left\{ A_4, \begin{array}{c} 1 & 3 \\ \diagdown & \diagup \\ 4 & 2 \end{array}, \begin{array}{c} 1 & 2 \\ \diagdown & \diagup \\ 3 & 4 \end{array} \right\}$$

L'action sur les sommets est transitive :

$$\begin{aligned} \text{orb}(1) &= \{ \text{id} \cdot 1, (1234) \cdot 1, (1234)^2 \cdot 1, (1234)^3 \cdot 1 \} \\ &= \{ 1, 2, 3, 4 \} = S \end{aligned}$$

\_\_\_\_\_ n'est pas libre :

$$(24) \cdot 1 = 1$$

$$(24) \in \text{Stab}_{\text{Aut}(S, A_4)}(1)$$

car c'est un élément non trivial.

$$\left( \text{on } \# \text{Aut} = \# \text{orb}(1) \# \text{Stab}(1) \Rightarrow \# \text{Stab}(1) = 2 \right)$$

$\begin{array}{ccc} \# & \# & \# \\ \parallel & \underbrace{\quad} & \parallel \\ 8 & 4 & 2 \end{array}$

Exercice : Montrer que le groupe alterné  $A_4$  n'est pas simple.

Indications: 1) Trouver une action de  $A_4$  non triviale et non fidèle.

Pourquoi ça permettrait de conclure ?

Rappel : \* Un sous-groupe  $H$  de  $G$  est distingué si

$$\forall g \in G, \quad gH = Hg.$$

$$(\text{on } gHg^{-1} = H)$$

\* Un groupe  $G$  est simple si ses seuls sous-groupes distingués sont  $\{ \text{id} \}$  et  $G$ .

Si  $A_4$  agit sur l'ensemble  $E$ , on a un morphisme  $\varphi: A_4 \rightarrow \text{Bij}(E)$ .

si l'action est non triviale,  $\text{Im } \varphi$  est non triviale, donc  $\text{Ker } \varphi \neq A_4$ .

si l'action n'est pas fidèle,  $\text{Ker } \varphi \neq \{ \text{id} \}$ .

Donc  $\text{Ker } \varphi$  est un sous-groupe distingué propre non trivial.



2) Considérer  $(S, A_4)$  de l'exercice précédent.

Rappel:  $A_4 \subset S_4$  est le noyau du morphisme signature  $\varepsilon: S_4 \rightarrow \{\pm 1\}$   
 $A_4 = \text{Ker } \varepsilon$   $\#A_4 = \#S_4/2 = 12.$   
 $= \{ \text{permutations de } \{1, 2, 3, 4\} \text{ de signature } 1 \}$   
 $= \{ \text{permutations qui s'écrivent comme produit d'un nombre pair de transpositions} \}$   
 $= \{ \text{id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243) \}$

$A_4$  agit aussi sur les graphes sur  $S = \{1, 2, 3, 4\}$  comme sous-groupe de  $S_4$ .

$A_4$  agit orb  $(S, A_4) = \left\{ \begin{array}{c} 1 & 2 \\ \diagdown & / \\ 4 & 3 \end{array}, \begin{array}{c} 1 & 3 \\ \diagdown & / \\ 4 & 2 \end{array}, \begin{array}{c} 1 & 2 \\ \diagdown & / \\ 3 & 4 \end{array} \right\}$

L'action est non-triviale: les 3-cycles ne stabilisent pas  $\begin{array}{c} 1 & 2 \\ \diagdown & / \\ 4 & 3 \end{array}$ .  
(par l'exercice précédent)

Par l'exercice précédent,  $\text{Stab}_{A_4} \left( \begin{array}{c} 1 & 2 \\ \diagdown & / \\ 4 & 3 \end{array} \right) = \{ \text{id}, (12)(34), (13)(24), (14)(23) \}$

Par symétrie des rôles des arêtes,  $\text{Stab} \left( \begin{array}{c} 1 & 3 \\ \diagdown & / \\ 4 & 2 \end{array} \right) = \text{Stab} \left( \begin{array}{c} 1 & 2 \\ \diagdown & / \\ 3 & 4 \end{array} \right)$

Si  $\varphi$  est le morphisme  $A_4 \rightarrow S_3$  induit par l'action,

$$\text{Ker } \varphi = \bigcap \text{Stab} = \{ \text{id}, (12)(34), (13)(24), (14)(23) \}$$

est un sous-groupe distingué propre non-trivial.  
 $\underbrace{\neq A_4}_{\text{propre}} \quad \underbrace{\neq \{ \text{id} \}}_{\text{non-trivial}}$

On dit qu'une action de  $G$  sur un ensemble  $E$  est triviale si  $g \cdot x = x \quad \forall g \in G, x \in E$ .

Autrement dit, le morphisme associé  $\varphi: G \rightarrow \text{Bij}(E)$  est trivial:  
c-à-d  $\forall g \in G \quad \varphi(g) = \text{id}$ .

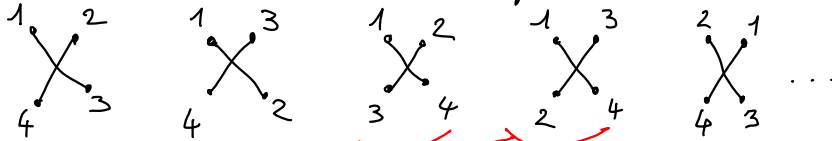
// Action de  $S_4$  sur les graphes sur  $\{1, 2, 3, 4\}$  :

si  $(S, A)$  graphe donné 

les éléments de l'orbite sont obtenus de la manière suivante :

• on oublie la numérotation des sommets 

• on renumérote de toutes les manières possibles



⚠ parmi les graphes obtenus, plusieurs sont les mêmes

## Produit semi-direct

Proposition : Étant donné deux groupes  $N$  et  $H$ ,

et  $\theta: H \rightarrow \text{Aut}(N)$  un morphisme de groupe,

*groupe des automorphismes de groupes de  $N$*

la loi sur l'ensemble  $N \times H$  définie par

$$(n, h) \cdot (n', h') = (n \theta(h)(n'), h h')$$

définit une structure de groupe sur l'ensemble  $N \times H$ .

$$\forall (n, h) \in N \times H \\ \forall (n', h') \in N \times H$$

Définition : On appelle ce groupe le produit semi-direct de  $N$  et  $H$  (par rapport à  $\theta$ )

et on le note  $N \rtimes_{\theta} H$ .

Preuve : Associativité -

$$n_1, n_2, n_3 \in N$$

$$h_1, h_2, h_3 \in H$$

$$\begin{aligned} (n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)) \\ = (n_1, h_1) \cdot (n_2 \theta(h_2)(n_3), h_2 h_3) \\ = (n_1 \theta(h_1)(n_2 \theta(h_2)(n_3)), h_1 h_2 h_3) \end{aligned}$$

$$\begin{aligned} \text{on veut } n_2 &= ((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) \\ &= (n_1 \theta(h_1)(n_2), h_1 h_2) \cdot (n_3, h_3) \\ &= (n_1 \theta(h_1)(n_2) \theta(h_1 h_2)(n_3), h_1 h_2 h_3) \end{aligned}$$

$$= (n_1, \theta(h_1)(n_2), \theta(h_1)(\theta(h_2)(n_3)), h_1 h_2 h_3)$$

$$\leftarrow \theta(h_i) \in \text{Aut}(N) \\ \theta(h_i)(ab) = \theta(h_i)(a)\theta(h_i)(b)$$

$$= (n_1, \theta(h_1)(n_2), \theta(h_1 h_2)(n_3), h_1 h_2 h_3)$$

$\leftarrow \theta: H \rightarrow \text{Aut}(N)$  est un morphisme  
La loi de groupe sur  $\text{Aut}(N)$  est  
la composition.

$$= ((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3)$$

\* Existence d'un élément neutre

$(e_N, e_H) \in N \times H$  est clairement un élément neutre pour cette loi

\* Inverse

$$(n, h)^{-1} = (\theta(h^{-1})(n^{-1}), h^{-1}) \quad ?$$

$$(n, h) \cdot (\theta(h^{-1})(n^{-1}), h^{-1}) = (n \theta(h)(\theta(h^{-1})(n^{-1})), h h^{-1})$$

$$= (n \underbrace{\theta(h h^{-1})}_{e_H}(n^{-1}), e_H)$$

$$= (n n^{-1}, e_H)$$

$$= (e_N, e_H)$$

□

Proposition: Soit  $N \rtimes_{\theta} H$  un produit semi direct. Alors  $N' := N \times \{e_H\}$

est un sous-groupe distingué de  $N \rtimes_{\theta} H$ , et

$$N \rtimes_{\theta} H / N' \simeq H.$$

Preuve: \*  $N'$  est un sous-groupe:

$$(n, e_H) \cdot (n', e_H) = (n \theta(e_H)(n'), e_H e_H) = (n n', e_H)$$

$$(n, e_H)^{-1} = (\theta(e_H^{-1})(n^{-1}), e_H^{-1}) = (n^{-1}, e_H)$$

\*  $N'$  est distingué:

pour tout  $(n, h) \in N \rtimes_{\theta} H$ ,  $(n', e_H) \in N'$ , on veut montrer qu'il

existe  $(n'', e_H) \in N'$  et

$$(n, h)(n', e_H) = (n'', e_H)(n, h)$$

||

$$(n \theta(h)(n'), h)$$

||

$$(n'' n, h)$$

L'unique possibilité est donc  $n'' = n \Theta(h)(n') n^{-1}$   
 et les m calculs montrent que ça marche.

$$* N \rtimes_{\Theta} H / N' \cong H$$

L'application  $N \rtimes_{\Theta} H \xrightarrow{\varphi} H$  est un morphisme de groupe.  
 $(n, h) \mapsto h$

C'est un morphisme surjectif.

$$\text{Ker } \varphi = N'$$

Par théorème d'isomorphisme,  $N \rtimes_{\Theta} H / N' \cong H$ .

□

Exercice: À quelle condition sur  $\Theta$  est-ce que  $N \rtimes_{\Theta} H$  est un produit direct?

$$(n, h) \cdot (n', h') = (nn', hh')$$

$$(n, h) \cdot (n', h') = (n \Theta(h)(n'), hh')$$

$$\Theta: H \longrightarrow \text{Aut}(N)$$

$$\Theta(h) = \text{id}_N \quad \forall h$$

Clair: c'est une condition suffisante.

C'est une condition nécessaire également:

$$\text{si } \forall n, n' \in N \text{ et } h, h' \in H, \quad nn' = n \Theta(h)(n')$$

$$\text{alors } \forall h \in H, \quad \forall n' \in N, \quad n' = \Theta(h)(n')$$

$$\text{alors } \forall h \in H, \quad \Theta(h) = \text{id}_N.$$

on est dans un groupe, on peut simplifier les n

Le produit semi-direct apparaît en général dans 2 situations:

i) Construction de groupes à partir de deux groupes  $N$  et  $H$ .

Par exemple, pour déterminer certains groupes finis d'ordre non premier.

→ dans ce cadre, on peut déterminer  $\text{Aut}(N)$

puis les morphismes possibles  $\Theta: H \longrightarrow \text{Aut}(N)$ .

ii) Étant donné un groupe  $G$ , l'écrire comme un produit semi-direct.

→ identifier deux ss-groupes possibles  $N$  et  $H$

(qui vérifient certaines propriétés : •  $N$  distingué dans  $G$ .


• l'application  $N \times H \rightarrow G$  est une bijection.  
 $(n, h) \mapsto nh$ )

→ identifier  $\theta$ .

Exercice (dans le cadre i): Déterminer tous les groupes d'ordre  $2p$   
 où  $p$  est un nombre premier.

Exercice (dans le cadre ii): Parmi les graphes, on appelle polygones les graphes

du type :  ...

(on appelle polygone orienté un graphe du type :  


Montrer que, si  $(S, A)$  est un polygone, alors  $\text{Aut}(S, A)$  est un produit semi-direct, et le décrire précisément.

Premier exercice: (supposons  $p \neq 2$ ) Soit  $G$  un groupe d'ordre  $2p$ .

(Les théorèmes de Sylow nous donnent l'existence d'un sous-groupe de  $G$  d'ordre  $p$ , donc isomorphe à  $\mathbb{Z}/p\mathbb{Z}$ .

Candidats pour  $G$ :

① le groupe cyclique d'ordre  $2p$  :  $\mathbb{Z}/2p\mathbb{Z}$ .

② on peut essayer d'en produire avec  $\mathbb{Z}/2\mathbb{Z}$  et  $\mathbb{Z}/p\mathbb{Z}$

produit direct:  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  plus: isomorphe à  $\mathbb{Z}/2p\mathbb{Z}$

$(\bar{1}, \bar{1})$  est un générateur du groupe  
 car  $p \neq 2$  donc  $p \nmid 2 = 1$

produit semi-direct? le candidat naturel pour  $N$  (par les thm de Sylow)  
 est  $\mathbb{Z}/p\mathbb{Z}$ .

le candidat pour  $H$  est  $\mathbb{Z}/2\mathbb{Z}$

Quel  $\theta: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})$  ?

$$\bar{0} \mapsto \text{id}_{\mathbb{Z}/p\mathbb{Z}}$$

$$\bar{1} \mapsto (\bar{a} \mapsto \overline{-a})$$

$$\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$$

Le groupe  $\mathbb{Z}/p\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$  est le groupe diédral.

Q: - quel est le groupe  $\text{Aut}(\mathbb{Z}/p\mathbb{Z})$  ?

- quels sont les morphismes possibles  $\mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})$  ?

- pourquoi est-ce que un groupe d'ordre  $2p$  est nécessairement un produit semi-direct ?

Prochaine fois : fin de ces exercices

+

début Chapitre 4: Groupes linéaires, aspects topologiques.

Exercice: Déterminer tous les groupes d'ordre  $2p$ , où  $p$  est un nombre premier  $> 2$ .

On en était arrivés aux questions:

Q1: Quel est le groupe  $\text{Aut}(\mathbb{Z}/p\mathbb{Z})$  ?

Q2: Quels sont les morphismes possibles  $\theta: \mathbb{Z}/2\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})$  ?

Q3: Pourquoi un groupe d'ordre  $2p$  est-il nécessairement un produit semi-direct ?

Pour Q1: Pour construire des morphismes à partir de  $\mathbb{Z}/p\mathbb{Z}$ , on peut construire des morphismes à partir de  $\mathbb{Z}$  et utiliser un thm d'isomorphisme.

Un morphisme  $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$  est déterminé par l'image  $\varphi(1)$  de 1. (De plus, pour tout choix de  $\varphi(1)$ , on a bien un morphisme  $\varphi$ )

Soit  $\varphi$  un tel morphisme, et  $\bar{k} = \varphi(1)$ . Alors  $\varphi(m) = m\bar{k}$   
 $\text{Ker}(\varphi) = \{m; m\bar{k} = 0\} = \{m; p \mid m\bar{k}\} = \{m; p \mid m \text{ ou } p \mid \bar{k}\}$

En particulier,  $p\mathbb{Z} \subset \text{Ker}(\varphi)$  donc  $\varphi$  définit un morphisme  $\bar{\varphi}: \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$   
 $\bar{m} \longmapsto \varphi(m) = m\bar{k}$

$\text{Ker}(\bar{\varphi}) = \{\bar{m}; p \mid m \text{ ou } p \mid \bar{k}\} = \{\bar{m}; \bar{m} = 0 \text{ ou } \bar{k} = 0\}$

Deux cas: si  $\bar{k} = 0$ , le morphisme  $\bar{\varphi}$  est trivial.  
sinon, le morphisme  $\bar{\varphi}$  est injectif.

Dans le second cas,  $\bar{\varphi}$  est un automorphisme par cardinaux.

De plus, tous les morphismes  $\mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$  sont obtenus de cette manière

$$\text{Donc } \text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^* \quad (\text{via } \varphi \mapsto \varphi(\bar{1}))$$

↑  
isomorphisme de groupe: si  $\varphi, \psi \in \text{Aut}(\mathbb{Z}/p\mathbb{Z})$

$$\varphi \circ \psi(\bar{1}) = \varphi(\bar{1}) \cdot \psi(\bar{1}) \text{ dans } \mathbb{Z}/p\mathbb{Z}.$$

Rem: on aurait pu s'en douter:  $\mathbb{Z}/p\mathbb{Z}$  est un corps.

Pour Q2: Un morphisme  $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\theta} \text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^*$

est défini par l'image de  $\bar{1}$ .

Un tel morphisme est bien défini si et seulement si

$$\theta(\bar{1})^2 = \bar{1} \quad (\text{dans } (\mathbb{Z}/p\mathbb{Z})^*).$$

C'est le casssi  $\theta(\bar{1}) = \pm \bar{1}$  dans  $\mathbb{Z}/p\mathbb{Z}$

$$(\text{en effet } \bar{k}^2 = \bar{1} \Leftrightarrow \exists m, k^2 = mp + 1)$$

$$\Leftrightarrow p \mid (k^2 - 1)$$

$$\Leftrightarrow p \mid (k-1) \text{ ou } p \mid (k+1)$$

$$\Leftrightarrow \bar{k} = \bar{1} \text{ ou } \bar{k} = -\bar{1} \text{ dans } \mathbb{Z}/p\mathbb{Z})$$

→  $\mathcal{G}$ :  $\theta(\bar{1}) = \bar{1}$ , alors le morphisme  $\theta$  obtenu est trivial.  
↑ élément neutre de  $(\mathbb{Z}/p\mathbb{Z})^*$

donc le produit semi-direct associé est un produit direct  $\cong \mathbb{Z}/2p\mathbb{Z}$ .

→  $\mathcal{G}$ :  $\theta(\bar{1}) = -\bar{1}$  et  $p > 2$ , alors  $-\bar{1} \neq \bar{1}$ , donc  $\theta$  n'est pas trivial,

donc le produit semi-direct  $\mathbb{Z}/p\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$  n'est pas isomorphe à  $\mathbb{Z}/2p\mathbb{Z}$ .



On a montré qu'il y a exactement deux produits semi-directs de  $\mathbb{Z}/p\mathbb{Z}$  par  $\mathbb{Z}/2\mathbb{Z}$  possibles:  $\mathbb{Z}/2p\mathbb{Z}$  et le groupe diédral.

Pour Q3:

D'abord des remarques générales sur les produits semi-directs.

Soit  $G$  un groupe,  $N$  un sous-groupe distingué de  $G$ ,  
 $H$  un sous-groupe quelconque de  $G$ .

On a un morphisme  $\theta: H \rightarrow \text{Aut}(N)$   
 $h \mapsto (n \mapsto hnh^{-1})$

donc un produit semi-direct  $N \rtimes_{\theta} H$ .

L'application  $N \rtimes_{\theta} H \xrightarrow{\varphi} G$  est un morphisme de groupe.  
 $(n, h) \mapsto nh$

En effet:  $\varphi(n, h) \cdot \varphi(n', h') = nh \cdot n'h'$   
 $= nhn'h^{-1}hh'$   
 $= \varphi(nhn'h^{-1}, hh')$   
 $= \varphi((n, h) \cdot (n', h'))$ .

⚠  $\varphi$  morphisme n'est pas, en général, un isomorphisme!

Dans le cas de l'exercice:

$G$  est un groupe d'ordre  $2p$ .

Par théorème de Sylow, il existe: • un sous-groupe  $H$  d'ordre 2 (donc  $H \cong \mathbb{Z}/2\mathbb{Z}$ )  
 • un sous-groupe  $N$  d'ordre  $p$  (donc  $N \cong \mathbb{Z}/p\mathbb{Z}$ ).

de plus, le sous-groupe  $N$  est distingué.

On a donc un morphisme  $\varphi: \mathbb{Z}/p\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z} \rightarrow G$   
 $(n, h) \mapsto nh$

On va montrer que  $c$  est un isomorphisme.

Les groupes de départ et d'arrivée ont cardinal  $2p$ , donc il suffit de montrer que  $\varphi$  est injectif.

$$\varphi(n, h) = e \iff nh = e \iff n = h^{-1}$$

$$\text{or } \begin{cases} n \text{ est d'ordre } p \text{ si } n \neq e \\ h^{-1} \text{ est d'ordre } 2 \text{ si } h \neq e \end{cases}$$

$$\text{or } p \neq 2, \text{ donc } n = h^{-1} \implies n = e \text{ et } h = e.$$

Donc  $\varphi$  est bien un isomorphisme.

On a résolu l'exercice:

Tout groupe d'ordre  $2p$  est isomorphe soit à  $\mathbb{Z}/2p\mathbb{Z}$

soit au groupe diédral  $D_{2p} := \mathbb{Z}/p\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$

$$\text{où } \theta: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^{\times}$$
$$\bar{1} \mapsto -\bar{1}$$

Exercice: Montrer que le groupe d'automorphisme d'un graphe polygone est un produit semi direct, et le décrire précisément.



nb sommets

3

4

5

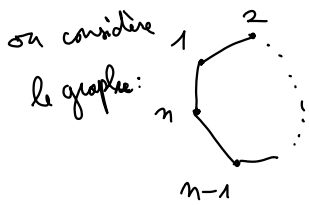
6

$$\text{Aut}(S, A) =: G$$

Si le nb de sommets  $p$  est premier, intuition:  $G$  est d'ordre  $2p$ .

Par l'exercice précédent,  $G$  serait un produit semi direct, qu'on imagine non direct, donc  $G$  serait le groupe diédral  $D_{2p}$ .

Intuition: en général,  $G \cong D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$  où  $\theta: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z})$   
 $\bar{1} \mapsto (\bar{k} \mapsto -\bar{k})$



On a un sous-groupe naturel de  $G$ :

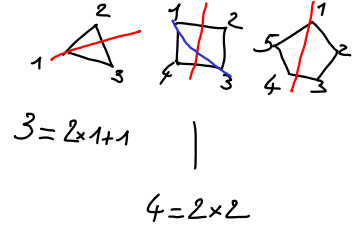
le sous-groupe  $N$  engendré par le cycle  
 $(1\ 2\ 3\ \dots\ n-1\ n)$

- On veut :
- trouver un candidat  $H$  d'ordre 2.
  - montrer que  $N$  est distingué.

Un élément d'ordre 2:

si  $n = 2k+1$        $(2\ n)\ (3\ n-1)\ (4\ n-2)\ \dots\ (k+1\ k+2)$

si  $n = 2k$        $(2\ n)\ (3\ n-1)\ \dots\ (k\ k+2)$



Admettons que  $N$  est distingué pour l'instant.

On a donc  $\varphi: N \rtimes_{\theta} H \longrightarrow G$       morphisme de groupe  
 $(\underline{n}, \underline{h}) \longmapsto \underline{nh}$

Il reste à montrer que  $\varphi$  est un isomorphisme.

Par ex, on  $\varphi$  est injectif et que l'ordre de  $G$  est  $2n$ .

Injectivité:  $\underline{nh} = e \iff \underline{n} = \underline{h}^{-1}$        $\underline{h}^{-1}$  d'ordre 2 ou  $h = e$   
 $\underline{n}$  d'ordre un diviseur de  $n$   
 un particulier, si  $n$  pair, l'ordre peut être 2!

L'ordre ne suffit pas à conclure.

À rédiger pour jeudi 24:

- 1) l'ordre de  $G$  est  $2n$
- 2)  $\varphi$  est injective.

## Chapitre 2

# Les groupes linéaires, aspects topologiques

### 2.1 Rappels sur le groupe linéaire

Soit  $\mathbb{K}$  un corps (commutatif). Soit  $V$  un  $\mathbb{K}$ -espace vectoriel de dimension finie.

**Définition 2.1.1.** Le *groupe général linéaire* sur  $V$ , noté  $\mathrm{GL}(V)$ , est le groupe formé par les applications linéaires bijectives de  $V$  dans  $V$ .

**Remarque 2.1.2.** C'est le sous-groupe des bijections de  $V$  qui préservent la structure de  $\mathbb{K}$ -espace vectoriel.

Le choix d'une base  $(e_1, \dots, e_d)$  de  $V$  fournit un isomorphisme de  $V$  avec  $\mathbb{K}^n$  (qui envoie  $x_1e_1 + \dots + x_n e_n$  sur  $(x_1, \dots, x_n)$ ). Cet isomorphisme fournit aussi un isomorphisme entre  $\mathrm{GL}(V)$  et le groupe des matrices inversibles  $\mathrm{GL}_d(\mathbb{K})$  (muni de la multiplication de matrices). On décrit plus succinctement l'inverse de cet isomorphisme, qui envoie une matrice inversible  $M$  sur l'application  $x_1e_1 + \dots + x_n e_n \mapsto MX$  où  $X$  est le vecteur colonne de coefficients  $(x_1, \dots, x_n)$ .

On se rappelle que sur les matrices carrées, on a deux applications très utiles : la trace  $\mathrm{tr} : \mathrm{M}_d(\mathbb{K}) \rightarrow \mathbb{K}, A \mapsto \sum_{i=1}^d a_{i,i}$ , et le déterminant  $\det : \mathrm{M}_d(\mathbb{K}) \rightarrow \mathbb{K}, A \mapsto \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^d a_{\sigma(i),i}$ .

On a  $\mathrm{GL}_d(\mathbb{K}) = \det^{-1}(\mathbb{K}^*)$ , et le déterminant, restreint à  $\mathrm{GL}_d(\mathbb{K})$ , est un morphisme de groupes.

**Définition 2.1.3.** Le *groupe spécial linéaire*, noté  $\mathrm{SL}_d(\mathbb{K})$ , est le sous-groupe de  $\mathrm{GL}_d(\mathbb{K})$  formé des matrices de déterminant égal à un.

Le *centre*  $Z(G)$  d'un groupe  $G$  est le sous-groupe formé des éléments qui commutent avec tous les autres :

$$Z(G) = \{z \in G \mid zg = gz \quad \forall g \in G\}.$$

On remarque que  $Z(G)$  est toujours un sous-groupe distingué de  $G$ .

**Proposition 2.1.4.** *Le centre de  $\mathrm{GL}_d(\mathbb{K})$  est formé des matrices scalaires :*

$$Z(\mathrm{GL}_d(\mathbb{K})) = \{\lambda I_d \mid \lambda \in \mathbb{K}^*\}.$$

**Exercice 2.1.5.** Prouver ce résultat. Quel est le centre de  $\mathrm{SL}_d(\mathbb{K})$  ?

**Définition 2.1.6.** Le *groupe projectif linéaire* est le groupe quotient  $\mathrm{PGL}_d(\mathbb{K}) = \mathrm{GL}_d(\mathbb{K})/Z(\mathrm{GL}_d(\mathbb{K}))$ . Le *groupe projectif spécial linéaire* est le groupe quotient  $\mathrm{PSL}_d(\mathbb{K}) = \mathrm{SL}_d(\mathbb{K})/Z(\mathrm{SL}_d(\mathbb{K}))$ .

**Exercice 2.1.7.** Montrer que  $\mathrm{PGL}_d(\mathbb{C})$  et  $\mathrm{PSL}_d(\mathbb{C})$  sont isomorphes. Attention ce n'est pas vrai pour un corps quelconque  $\mathbb{K}$ .

**Exercice 2.1.8.** Montrer que  $\mathrm{GL}_n(\mathbb{K})$  est isomorphe à un produit semi-direct de  $\mathrm{SL}_n(\mathbb{K})$  avec  $\mathbb{K}^*$ . Trouver des conditions suffisantes pour que ce produit soit direct.

**Exercice 2.1.9.** Soit  $\mathbb{F}_p$  un corps fini ( $p$  nombre premier).

1. Quel est l'ordre de  $\mathrm{GL}_n(\mathbb{F}_p)$  ?
2. Quel est l'ordre de  $\mathrm{SL}_n(\mathbb{F}_p)$  ?
3. Quel est l'ordre de  $\mathrm{PGL}_n(\mathbb{F}_p)$  ?
4. Quel est l'ordre de  $\mathrm{PSL}_n(\mathbb{F}_p)$  ?
5. En déduire que  $\mathrm{PGL}_n(\mathbb{K})$  et  $\mathrm{PSL}_n(\mathbb{K})$  ne sont pas isomorphes en général.

## 2.2 Notion de groupe topologique

**Définition 2.2.1.** Un *groupe topologique* est un groupe  $G$  dont l'ensemble sous-jacent est muni d'une topologie telle que :

1. Le produit de groupe  $G \times G \rightarrow G, (g, h) \mapsto gh$  est une application continue, et
2. l'inverse  $G \rightarrow G, g \mapsto g^{-1}$  est une application continue.

**Exemple 2.2.2.** Le groupe additif  $(\mathbb{C}, +)$  est un groupe topologique pour la topologie usuelle de  $\mathbb{C}$ .

Le groupe multiplicatif  $(\mathbb{C}^*, \times)$  est un groupe topologique pour la topologie induite de  $\mathbb{C}^* \subset \mathbb{C}$ .

On remarque que  $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$ . Plus généralement, on va montrer que  $\mathrm{GL}_n(\mathbb{C})$  est un groupe topologique.

**Théorème 2.2.3.** *Le groupe  $\mathrm{GL}_n(\mathbb{C})$ , muni de la topologie induite de  $\mathrm{GL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ , est un groupe topologique.*

**Remarque 2.2.4.** Le déterminant est une application continue de  $\mathrm{M}_n(\mathbb{C})$  dans  $\mathbb{C}$ . En effet, d'après l'expression rappelée plus tôt dans ce cours :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^n a_{\sigma(i), i},$$

c'est un polynôme en les coefficients de la matrice.

Comme première conséquence de cette remarque, on note que  $\mathrm{GL}_n(\mathbb{C}) = \det^{-1}(\mathbb{C}^*)$  est un ouvert de  $\mathrm{M}_n(\mathbb{C})$ . On va aussi utiliser la remarque pour prouver que l'inverse de matrice est une application continue.

La topologie induite par  $\mathrm{GL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$  fournit bien une topologie sur l'ensemble sous-jacent au groupe. Pour montrer que c'est un groupe topologique, il faut vérifier que le produit et l'inverse sont des applications continues.

La loi de groupe sur  $\mathrm{GL}_n(\mathbb{C})$  est la restriction du produit de matrices  $\mathrm{M}_n(\mathbb{C}) \times \mathrm{M}_n(\mathbb{C}) \rightarrow \mathrm{M}_n(\mathbb{C})$  défini en terme des coefficients par :

$$((a_{i,j})_{1 \leq i,j \leq n}, (b_{k,l})_{1 \leq k,l \leq n}) \mapsto \left( \sum_{r=1}^n a_{p,r} b_{r,q} \right)_{1 \leq p,q \leq n}$$

C'est une application polynomiale (chaque application composante est un polynôme), donc c'est une application continue. Sa restriction à  $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$  muni de la topologie induite est donc continue.

Pour l'inverse, on peut utiliser l'expression de l'inverse d'une matrice (inversible) à l'aide de la comatrice : si  $A \in \mathrm{GL}_n(\mathbb{C})$ , alors

$$A^{-1} = \frac{1}{\det(A)} \mathrm{com}(A)^T$$

où  $(-1)^{i+j}(\mathrm{com}(A))_{i,j}$  est le déterminant de la matrice carrée obtenue en supprimant la  $i$ ème ligne et la  $j$ ème colonne de  $A$  (on appelle les matrices ainsi obtenues des *mineurs* de  $A$ ). Le déterminant et les applications  $A \mapsto (\mathrm{com}(A))_{i,j}$  sont continues, donc l'application  $A \mapsto A^{-1}$  l'est aussi là où  $\det$  ne s'annule pas, c'est-à-dire sur  $\mathrm{GL}_n(\mathbb{C})$ .

On a ainsi bien démontré que  $\mathrm{GL}_n(\mathbb{C})$  est un groupe topologique.

**Corollaire 2.2.5.** *Les groupes  $\mathrm{GL}_n(\mathbb{R})$ ,  $\mathrm{SL}_n(\mathbb{C})$ ,  $\mathrm{SL}_n(\mathbb{R})$ , sont des groupes topologiques pour la topologie induite (par leur inclusion dans  $\mathrm{GL}_n(\mathbb{C})$ ).*

## 2.3 Action de $\mathrm{GL}(V) \times \mathrm{GL}(W)$ sur $L(V, W)$

### 2.3.1 Description de l'action et matrices équivalentes

Soit  $V$  un  $\mathbb{K}$ -espace vectoriel de dimension  $n$ , et  $W$  un  $\mathbb{K}$ -espace vectoriel de dimension  $m$ . On note  $L(V, W)$  le  $\mathbb{K}$ -espace vectoriel formé par les applications linéaires de  $V$  dans  $W$ .

Il y a une action naturelle du groupe produit  $\mathrm{GL}(V) \times \mathrm{GL}(W)$  sur  $L(V, W)$  définie par

$$\forall (g, h) \in \mathrm{GL}(V) \times \mathrm{GL}(W), \forall f \in L(V, W), \quad (g, h) \cdot f = h \circ f \circ g^{-1}$$

(vérifier que ça définit bien une action).

Choisissons une base de  $V$  et une base de  $W$ . Ces choix fournissent un isomorphisme entre  $L(W, W)$  et  $M_{m \times n}(\mathbb{K})$ , entre  $\mathrm{GL}(V)$  et  $\mathrm{GL}_n(\mathbb{K})$  et entre  $\mathrm{GL}(W)$  et  $\mathrm{GL}_m(\mathbb{K})$ . Sous ces isomorphismes, l'action décrite ci-dessus se traduit en l'action de  $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$  sur  $M_{m \times n}(\mathbb{K})$  définie par  $(A, B) \cdot M = BMA^{-1}$  et appelée *action par équivalences*.

**Définition 2.3.1.** Deux matrices  $M$  et  $N$  dans  $M_{m \times n}(\mathbb{K})$  sont *équivalentes* s'il existe  $A \in \mathrm{GL}_n(\mathbb{K})$  et  $B \in \mathrm{GL}_m(\mathbb{K})$  telles que  $N = BMA^{-1}$ .

Autrement dit, deux matrices sont équivalentes si et seulement si elles sont dans la même orbite pour l'action ci-dessus.

**Remarque 2.3.2.** Deux matrices sont équivalentes si et seulement si elles représentent la même application  $\mathbb{K}^n \rightarrow \mathbb{K}^m$ , écrite dans des choix de bases différentes au départ et/ou à l'arrivée.

### 2.3.2 Description des orbites

On rappelle que, si  $M \in M_{m \times n}(\mathbb{K})$ , le rang de  $M$ , noté  $\mathrm{rg}(M)$ , est la dimension de l'image de  $M$  vu comme sous-espace vectoriel de  $\mathbb{K}^m$ .

**Proposition 2.3.3.** *Soient  $M$  et  $N$  deux matrices équivalentes, alors  $\mathrm{rg}(M) = \mathrm{rg}(N)$ .*

*Démonstration.* Écrivons  $N = BMA^{-1}$  avec  $A \in \mathrm{GL}_n(\mathbb{K})$  et  $B \in \mathrm{GL}_m(\mathbb{K})$ . De manière équivalente,  $NA = BM$ . Comme  $A$  définit un isomorphisme de  $\mathbb{K}^n$  dans  $\mathbb{K}^n$ , on a  $A(\mathbb{K}^n) = \mathbb{K}^n$ , et donc  $NA(\mathbb{K}^n) = N(\mathbb{K}^n)$ , d'où  $\mathrm{rg}(N) = \mathrm{rg}(NA)$ .

Par le théorème du rang,  $\text{rg}(NA) = n - \dim \ker(NA) = n - \dim \ker(BM)$ .

Comme  $B$  est un isomorphisme,  $Bx = 0$  si et seulement si  $x = 0$ . On en déduit que  $\ker(BM) = \ker(M)$ .

Donc  $\text{rg}(N) = n - \dim \ker(M)$ . Par le théorème du rang à nouveau, c'est égal au rang de  $M$ .  $\square$

En fait, une orbite est complètement déterminée par le rang de ses éléments.

**Théorème 2.3.4.** *Il y a exactement  $\min(m, n) + 1$  orbites pour l'action de  $\text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K})$  par équivalences, et les orbites sont les matrices de rang fixé égal à  $r$ , pour  $r$  compris entre 0 et  $\min(m, n)$ .*

### 2.3.3 Une manière de prouver le théorème : le pivot de Gauss

**Notations :** on note  $E_{k,l} \in M_{m \times n}$  la matrice dont les coefficients sont  $\delta_{k,i} \delta_{j,l}$ , c'est-à-dire que des zéros partout sauf à l'intersection de la  $i$ ème ligne et de la  $j$ ème colonne.

On pose  $I_r = \sum_{i=1}^r E_{i,i} \in M_{m \times n}$ .

Le pivot de Gauss permet, par des opérations sur les lignes et sur les colonnes, de transformer une matrice  $A$  quelconque de  $M_{m \times n}$  en une matrice de la forme  $I_r$  pour un  $r$  compris entre 0 et  $\min(m, n)$ . Plus précisément,  $r = \text{rg}(A)$ . Voici l'algorithme.

**Étape 0 :** (cas d'arrêt) si  $A = 0_{m \times n}$ , alors on s'arrête.

**Étape 1 :** si  $a_{1,1} = 0$ , on échange des lignes et des colonnes pour avoir  $a_{1,1} \neq 0$ .

**Étape 2 :** si  $a_{1,1} \neq 1$ , on multiplie la première ligne par  $a_{1,1}^{-1}$  pour avoir  $a_{1,1} = 1$ .

**Étape 3 :** par une suite de transvections sur les lignes et les colonnes ( $L_i$  remplacée par  $L_i - a_{i,1}L_1$ ,  $C_j$  remplacée par  $C_j - a_{1,j}C_1$ ), on s'assure que  $a_{1,j} = 0$  pour  $j \neq 1$  et  $a_{i,1} = 0$  pour  $i \neq 1$ .

**Étape 4 :** la matrice  $A$  est maintenant diagonale par blocs de forme  $A = \text{diag}(1, A')$  avec  $A' \in M_{(m-1) \times (n-1)}(\mathbb{K})$ . On reprends à l'étape 0 avec  $A'$  à la place de  $A$ .

Le processus s'arrête après au plus  $\min(m, n)$  répétitions.

Le lien avec l'action de  $\text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K})$  est obtenu de la manière suivante.

**Définition 2.3.5.** 1. Soit  $\sigma \in \mathfrak{S}_n$  une permutation. La *matrice de permutation* associée à  $\sigma$  est la matrice

$$P_\sigma = \sum_{i=1}^n E_{\sigma(i),i} \in M_n(\mathbb{K}).$$

2. Soit  $\lambda \in \mathbb{K}^*$  et  $i \in \{1, 2, \dots, n\}$ . La *matrice de dilatation* associée à  $\lambda$  et  $i$  est la matrice

$$D_i(\lambda) = I_n + (\lambda - 1)E_{i,i} \in M_n(\mathbb{K}).$$

3. Soit  $\lambda \in \mathbb{K}^*$  et  $i \neq j$  dans  $\{1, 2, \dots, n\}$ . La *matrice de transvection* associée à  $\lambda$ ,  $i$  et  $j$  est la matrice

$$T_{i,j}(\lambda) = I_n + \lambda E_{i,j}.$$

**Exercice 2.3.6.** Faire des schémas pour représenter ces matrices.

On appelle génériquement ces matrices des matrices d'opérations élémentaires.

**Proposition 2.3.7.** *La multiplication d'une matrice  $A \in M_{m \times n}(\mathbb{K})$  par une matrice  $m \times m$  de transposition, de dilatation, de transvection, à gauche réalise l'opération correspondante sur les lignes de la matrice  $A$ . La multiplication d'une matrice  $A \in M_{m \times n}(\mathbb{K})$  par une matrice  $n \times n$  de transposition, de dilatation, de transvection, à droite réalise l'opération correspondante sur les colonnes de la matrice  $A$ .*

*Démonstration.* En exercice. Écrire précisément à quelle opérations correspond la multiplication par  $P_\sigma$ , par  $D_i(\lambda)$ , par  $T_{i,j}(\lambda)$  à gauche, puis à droite.  $\square$

**Proposition 2.3.8.** *Les matrices de permutations, de dilatations et de transvections sont inversibles.*

*Démonstration.* En exercice. Déterminer explicitement leurs inverses et montrer que cela reste des matrices d'opérations élémentaires.  $\square$

*Fin de la preuve du Théorème.* L'algorithme du pivot de Gauss se traduit, d'après les propositions ci-dessus, en l'existence, pour toute matrice  $M \in M_{m \times n}(\mathbb{K})$ , d'une matrice  $A \in GL_n(\mathbb{K})$  (produit d'inverse de matrices d'opérations élémentaires), et d'une matrice  $B \in GL_m(\mathbb{K})$  (produit de matrices d'opérations élémentaires) telles que

$$BMA^{-1} = I_r.$$

De plus, comme on l'a déjà remarqué,  $r = \text{rg}(M)$ .

Toutes les possibilités de rang sont réalisées par les matrices  $I_r$  pour  $0 \leq r \leq \min(m, n)$ , et  $I_r$  n'est pas équivalente à  $I_s$  pour  $r \neq s$  puisque leur rangs sont différents.  $\square$

### 2.3.4 Aspects topologiques de l'action par équivalences

On se place dans le cas  $\mathbb{K} = \mathbb{C}$ .

**Théorème 2.3.9.** *La partie  $GL_n(\mathbb{C}) \subset M_n(\mathbb{C})$  est une partie dense.*

*Démonstration.* Le principe est de construire, pour  $M \in M_n(\mathbb{C})$  quelconque, une suite  $(M_k)$  de matrices inversibles qui converge vers  $M$ . Il y a de nombreuses preuves différentes. En voici une utilisant l'action par équivalences. Soit  $r$  le rang de  $M$ . Alors il existe  $A$  et  $B$  dans  $GL_n(\mathbb{C})$  telles que  $M = BI_rA^{-1}$ . On considère la suite  $(M_k)_{k \geq 1}$  d'élément général

$$M_k = B \text{diag}(1, 1, \dots, 1, 1/k, 1/k, \dots, 1/k)A^{-1}$$

où les 1 sont répétés  $r$  fois, et les  $1/k$  sont répétés  $n-r$  fois. La matrice diagonale  $\text{diag}(1, \dots, 1, 1/k, \dots, 1/k)$  est inversible, donc  $M_k$  aussi. La suite  $\text{diag}(1, \dots, 1, 1/k, \dots, 1/k)$  converge vers  $I_r$ . Le produit de matrice étant continu,  $(M_k)$  converge vers  $BI_rA^{-1} = M$ .  $\square$

**Exercice 2.3.10.** Déterminer l'adhérence de l'ensemble des matrices de rang  $r$  dans  $M_{m \times n}(\mathbb{C})$ , où  $0 \leq r \leq \min(m, n)$ .

## 2.4 Action de $GL(V)$ sur $L(V, V)$ par conjugaisons

### 2.4.1 Description de l'action et terminologie

On rappelle que  $L(V, V)$  est l'espace vectoriel des applications linéaires du  $\mathbb{K}$ -espace vectoriel  $V$  dans lui-même.

Le groupe  $GL(V)$  agit sur  $L(V, V)$  par

$$\forall g \in GL(V), \forall f \in L(V, V), \quad g \cdot f = g \circ f \circ g^{-1}.$$

Par le choix d'une base pour se ramener à des matrices, il suffit de considérer l'action correspondante de  $GL_n(\mathbb{K})$  sur  $M_n(\mathbb{K})$  donnée par  $A \cdot M = AMA^{-1}$  pour  $A \in GL_n(\mathbb{K})$  et  $M \in M_n(\mathbb{K})$ .



**Définition 2.4.1.** Deux matrices  $M$  et  $N$  dans  $M_n(\mathbb{K})$  sont *semblables* si elles sont dans la même orbite pour l'action ci-dessus, appelée *action par similitudes*. On appelle *classes de similitudes* les orbites pour cette action.

**Remarque 2.4.2.** Cette action par similitude (on dit aussi par conjugaison) peut se retrouver en considérant la restriction de l'action par équivalences de  $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$  sur  $M_n(\mathbb{K})$  au sous-groupe diagonal  $\mathrm{diag}(\mathrm{GL}_n(\mathbb{K})) = \{(A, A) \in \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K}) \mid A \in \mathrm{GL}_n(\mathbb{K})\}$ , qui est bien sûr isomorphe à  $\mathrm{GL}_n(\mathbb{K})$ . En particulier, deux matrices semblables sont équivalentes et ont même rang.

## 2.4.2 Invariants de similitude

Rappelons d'abord quelques définitions. Soit  $M \in M_n(\mathbb{K})$ .

Le *polynôme caractéristique* de  $M$ , noté  $\chi_M$ , est le polynôme en la variable  $X$  défini par  $\chi_M(X) = \det(XI_n - M)$ .

Le *polynôme minimal* de  $M$ , noté  $P_M$ , est le polynôme en la variable  $X$ , de degré minimal et de coefficient directeur égal à un, tel que si on remplace  $X$  par  $M$  dans l'expression de  $P_M$ , on a  $P_M(M) = 0$ .

**Proposition 2.4.3.** *Si  $A$  et  $B$  sont semblables, alors  $\chi_A = \chi_B$ .*

*Démonstration.* Écrivons  $B = gAg^{-1}$ , pour un  $g \in \mathrm{GL}_n(\mathbb{K})$ . On a

$$\begin{aligned} \chi_B(X) &= \det(XI_n - B) \\ &= \det(Xgg^{-1} - gAg^{-1}) \\ &= \det(g(XI_n - A)g^{-1}) \\ &= \det(g) \det(XI_n - A) \det(g)^{-1} && \text{car } \det \text{ est un morphisme} \\ &= \det(XI_n - A) && \text{car } \mathbb{K} \text{ est commutatif} \\ &= \chi_A(X), \end{aligned}$$

ce qu'il fallait démontrer. □

**Corollaire 2.4.4.** *Si  $A$  et  $B$  sont semblables, alors  $\det(A) = \det(B)$  et  $\mathrm{tr}(A) = \mathrm{tr}(B)$ .*

*Démonstration.* Le déterminant est (au signe près), le coefficient constant du polynôme caractéristique. La trace est l'opposé de son coefficient sous-directeur (le coefficient de  $X^{n-1}$ ). □

**Proposition 2.4.5.** *Si  $A$  et  $B$  sont semblables, alors  $P_A = P_B$ .*

*Démonstration.* Il suffit de montrer que pour tout polynôme  $Q$ ,  $Q(A) = 0$  si et seulement si  $Q(B) = 0$ . Par symétrie des rôles de  $A$  et  $B$ , il suffit de montrer que pour tout polynôme  $Q$ ,

$$Q(A) = 0 \implies Q(B) = 0.$$

Supposons  $Q(A) = 0$ , notons  $Q(X) = a_0 + a_1X + \dots + a_kX^k$ , et  $B = gAg^{-1}$  pour un  $g \in \mathrm{GL}_n(\mathbb{K})$ . Alors

$$\begin{aligned} Q(B) &= a_0 + a_1gAg^{-1} + a_2gAg^{-1}gAg^{-1} + \dots + a_k(gAg^{-1})^k \\ &= g(a_0 + a_1A + \dots + a_kA^k)g^{-1} \\ &= gQ(A)g^{-1} \\ &= 0 \end{aligned}$$

□

**Proposition 2.4.6.** *Si  $A$  et  $B$  sont semblables,  $\lambda \in \mathbb{K}$  et  $k \in \mathbb{N}$ , alors*

$$\dim \ker \left( (A - \lambda I_n)^k \right) = \dim \ker \left( (B - \lambda I_n)^k \right).$$

*Démonstration.* Notons  $B = gAg^{-1}$ . On a aussi  $(B - \lambda I_n)^k = g(A - \lambda I_n)^k g^{-1}$  par la simplification habituelle  $g^{-1}g = I_n$ . Alors on voit en particulier que les matrices  $(B - \lambda I_n)^k$  et  $(A - \lambda I_n)^k$  sont équivalentes. Elles ont par conséquent même rang. La conclusion du théorème suit par application du Théorème du rang.  $\square$

### 2.4.3 Description des classes de similitude pour $\mathbb{K} = \mathbb{C}$

On va utiliser, sans le redémontrer, un résultat vu l'an dernier : la réduction de Jordan.

**Définition 2.4.7.** Un bloc de Jordan de taille  $k \in \mathbb{N}^*$  et de valeur propre  $\lambda \in \mathbb{C}$  est la matrice

$$J_{k,\lambda} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix} = \lambda I_k + \sum_{i=1}^{k-1} E_{i,i+1} \in M_k(\mathbb{K})$$

**Théorème 2.4.8** (Réduction de Jordan complexe). *Toute matrice  $A \in M_n(\mathbb{C})$  est semblable dans  $M_n(\mathbb{C})$  à une matrice  $B$  diagonale par blocs, dont les blocs sont des blocs de Jordan. De plus, la matrice  $B$  de cette forme est unique à permutation des blocs diagonaux près, et on l'appelle la forme de Jordan de  $A$ .*

**Corollaire 2.4.9.** *Une classe de similitude est déterminée par la forme de Jordan de ses éléments.*

Remarquons par ailleurs qu'on peut encoder la forme de Jordan par la donnée d'une partition de l'ensemble  $\{1, 2, \dots, n\}$  et d'un nombre complexe pour chaque part de la partition.

### 2.4.4 Description des classes de similitudes pour $\mathbb{K} = \mathbb{R}$

**Définition 2.4.10.** Étant donné un angle  $\theta \in [0, 2\pi[$ , on note

$$R_\theta := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

la matrice de rotation associée.

Si on se donne de plus un entier  $k \in \mathbb{N}^*$  et un réel non-nul  $\lambda \in \mathbb{R}^*$ , on note  $K_{k,\lambda,\theta}$  la matrice définie par blocs par

$$K_{k,\lambda,\theta} = \begin{pmatrix} \lambda R_\theta & I_2 & 0_2 & \cdots & 0_2 \\ 0_2 & \lambda R_\theta & I_2 & \cdots & 0_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0_2 & 0_2 & 0_2 & \cdots & \lambda R_\theta \end{pmatrix} \in M_{2k}(\mathbb{R}).$$

**Théorème 2.4.11** (Réduction de Jordan réelle). *Toute matrice  $A \in M_n(\mathbb{R})$  est semblable dans  $M_n(\mathbb{R})$  à une matrice  $B$  diagonale par blocs, dont chaque bloc est soit de la forme  $K_{k,\lambda,\theta}$  pour  $k \in \mathbb{N}^*$ ,  $\lambda \in \mathbb{R}_+^*$ ,  $\theta \in ]0, \pi[$ , soit de la forme  $J_{k,\lambda}$  pour  $k \in \mathbb{N}^*$  et  $\lambda \in \mathbb{R}$ . On appelle  $B$  la forme de Jordan réelle de  $A$ , et elle est unique à permutation des blocs diagonaux près.*

**Exercice 2.4.12.** La matrice  $R_\theta$  est sa propre forme de Jordan réelle. Quelle est sa forme de Jordan complexe ?

**Théorème:**  $GL_n(\mathbb{C})$  est connexe par arcs.

On commence par le cas particulier  $GL_1(\mathbb{C}) = \mathbb{C}^*$ .

Rappelons d'abord qu'il suffit de relier tout  $z \in \mathbb{C}^*$  à 1 par un chemin continu pour montrer que  $\mathbb{C}^*$  est connexe par arcs.

En effet, si pour tout  $z$  il existe un chemin

$$\gamma_{1,z}: [0,1] \rightarrow \mathbb{C}^* \text{ continu, tq } \gamma_{1,z}(0) = 1 \text{ et } \gamma_{1,z}(1) = z,$$

alors pour tous  $z_1, z_2 \in \mathbb{C}^*$ , le chemin

$$\gamma_{z_1, z_2}: [0,1] \rightarrow \mathbb{C}^*$$

$$t \mapsto \begin{cases} \gamma_{1,z_1}(1-2t) & \text{pour } t \in [0, \frac{1}{2}] \\ \gamma_{1,z_2}(2t-1) & \text{pour } t \in [\frac{1}{2}, 1] \end{cases}$$

est un chemin continu entre  $z_1$  et  $z_2$ .

Ce raisonnement est valable en général pour la connexité par arcs: il suffit de trouver un chemin continu entre un point fixé et n'importe quel autre point.

Dans  $\mathbb{C}$  (plutôt que  $\mathbb{C}^*$ ), c'est facile de trouver un chemin continu entre deux points  $a$  et  $b$ : il suffit de prendre le segment  $t \mapsto (1-t)a + tb$ .

Dans  $\mathbb{C}^*$ , le problème est que le segment peut passer par zéro.

Ce n'est pas le cas si  $a=1$  et  $b \notin \mathbb{R}_-^*$ .

On a donc un chemin continu entre 1 et tout  $z \in \mathbb{C}^* \setminus \mathbb{R}_-^*$ .

Si  $z \in \mathbb{R}_-^*$ , on peut d'abord suivre le segment entre 1 et  $i$ , puis celui entre  $i$  et  $z$ : en formules,

$$\gamma: [0,1] \longrightarrow \mathbb{C}^*$$

$$t \longmapsto \begin{cases} (1-2t) + 2ti & \text{pour } t \in [0, \frac{1}{2}] \\ (2t-1)z + (2-2t)i & \text{pour } t \in [\frac{1}{2}, 1] \end{cases}$$

est un chemin continu entre  $\gamma(0) = 1$  et  $\gamma(1) = z$ .

Passons au cas général.

Pour  $GL_n(\mathbb{C})$  on va utiliser l'achèvement par similitudes et la réduction de Jordan pour construire un chemin entre  $I_n$  et une matrice  $A \in GL_n(\mathbb{C})$  quelconque.

Il existe une matrice  $P \in GL_n(\mathbb{C})$  telle que  $B := PAP^{-1}$  soit la forme de Jordan de  $A$ . En particulier,  $B$  est triangulaire supérieure avec des coefficients diagonaux non nuls. On note  $B = (b_{ij})$ .

On construit d'abord un chemin  $\tilde{\gamma}: [0,1] \longrightarrow M_n(\mathbb{C})$  par ses coefficients de la manière suivante :

$$(\tilde{\gamma}(t))_{i,j} = t b_{i,j} \quad \text{si } i \neq j$$

et pour  $(\tilde{\gamma}(t))_{i,i}$ , on choisit un chemin  $(\tilde{\gamma}(t))_{i,i}: [0,1] \longrightarrow \mathbb{C}^*$

entre 1 et  $b_{i,i}$  donné par la connexité par arcs de  $\mathbb{C}^*$ .

Alors pour tout  $t \in [0,1]$ , la matrice  $\tilde{\gamma}(t)$  est triangulaire supérieure, à coefficients diagonaux non nuls, donc inversible.

De plus,  $\tilde{\gamma}$  est continue, car toutes ses applications composantes  $(\tilde{\gamma})_{i,j}$  le sont.

Donc  $\tilde{\gamma}: [0,1] \longrightarrow GL_n(\mathbb{C})$  est un chemin continu entre  $\tilde{\gamma}(0) = I_n$  et  $\tilde{\gamma}(1) = B$ .

Pour finir, on en déduit un chemin continu  $\gamma: [0,1] \longrightarrow GL_n(\mathbb{C})$  entre  $I_n$  et  $A$  par  $\gamma(t) = P^{-1} \tilde{\gamma}(t) P$ .

(C'est bien continu car  $GL_n(\mathbb{C})$  est un groupe topologique)

□



Théorème:  $GL_n(\mathbb{R})$  n'est pas connexe.

Le cas  $n=1$  est instinctif ici aussi:  $GL_1(\mathbb{R}) = \mathbb{R}^*$   
et  $\mathbb{R}^* = ]-\infty, 0[ \cup ]0, +\infty[$  est une réunion disjointe d'ouverts non-vides.

Dans le cas général, on se ramène à  $\mathbb{R}^*$  via le déterminant:

$\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$  est une application continue et surjective, donc  $GL_n(\mathbb{R}) = \det^{-1}(]-\infty, 0[) \cup \det^{-1}(]0, +\infty[)$  est une réunion disjointe d'ouverts non vides.

Théorème:  $SL_n(\mathbb{C})$  est connexe par arcs.

C'est un corollaire du résultat sur  $GL_n(\mathbb{C})$ .

Comment peut-on utiliser ce résultat?

Soient  $A, B \in SL_n(\mathbb{C})$ , alors en particulier ce sont des éléments de  $GL_n(\mathbb{C})$ , donc il existe un chemin continu  $\tilde{\gamma}: [0, 1] \rightarrow GL_n(\mathbb{C})$  avec  $\tilde{\gamma}(0) = A$  et  $\tilde{\gamma}(1) = B$ .

Le problème est que  $\tilde{\gamma}$  prend ses valeurs dans  $GL_n(\mathbb{C})$  et pas  $SL_n(\mathbb{C})$ .

Considérons le chemin  $\gamma: [0, 1] \rightarrow GL_n(\mathbb{C})$  défini par

$$\gamma(t) = \text{diag}(\det(\tilde{\gamma}(t))^{-1}, 1, \dots, 1) \tilde{\gamma}(t) \quad \text{où } \text{diag}(a_1, \dots, a_n) \text{ désigne la matrice diagonale de coeffs diagonaux } a_1, \dots, a_n.$$

Alors  $\gamma$  est continue (continuité des composantes + produit continu) à valeurs dans  $SL_n(\mathbb{C})$ , et  $\gamma(0) = A$ ,  $\gamma(1) = B$ .  $\square$

Question: Est-ce que  $SL_n(\mathbb{R})$  est connexe?

Indication:  $SL_1(\mathbb{R}) = \{1\}$  est connexe

- Si on veut imiter la preuve pour  $GL_n(\mathbb{C})$ , il faut ici utiliser la réduction de Jordan réelle.

les formes de Jordan possibles sont:

$$\begin{pmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{pmatrix} \quad \begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix} \quad \text{et } \pm R_\theta \quad \text{pour } \lambda \in \mathbb{C}^* \\ \text{et } \theta \in ]0, \pi[.$$

Exercices en lien direct: Exercice 7.

Exercices à regarder pour lundi: 9 à 12.

Compléments topologiques:

1) Connexe par arcs  $\implies$  connexe

Mais la réciproque est fautive. Un contre exemple usuel est l'adhérence du graphe de  $x \mapsto \sin(\frac{1}{x})$  dans  $\mathbb{R}^2$ .

2) Si  $f: X \rightarrow Y$  est une application continue entre espaces topologiques, et si  $X$  est connexe, alors  $f(X)$  est connexe.

Preuve: Par contraposée. Si  $f(X)$  n'est pas connexe, alors

$\exists U, V$  ouverts non vides disjoints tq  $f(X) = U \sqcup V$ .

Alors  $X = f^{-1}(U) \sqcup f^{-1}(V)$  est une réunion de deux ouverts non vides disjoints.

5) Action de  $GL(V)$  sur les droites de  $V$ , géométrie projective.

a) Description et propriétés de l'action

$K$  corps commutatif,  $V$  espace vectoriel de dim finie sur  $K$ .

On note  $\mathbb{P}(V)$  l'ensemble des droites vectorielles de  $V$ .

*sous-espaces vectoriels de dimension 1*

(On l'appelle cet ensemble l'espace projectif, ou le projectivisé de  $V$ )

Une telle droite est engendrée par un vecteur non nul  $v \in V$ , on la note dans ce cas  $[v] \in \mathbb{P}(V)$ .

Le groupe  $GL(V)$  agit sur  $\mathbb{P}(V)$  par :

$$\forall g \in GL(V), \forall v \in V - \{0\}, \quad g \cdot [v] = [g(v)].$$

Proposition : Cette action est transitive.

Preuve : Soient  $v_1$  et  $w_1$  deux vecteurs non nuls de  $V$ .

On veut trouver un automorphisme  $g \in GL(V)$  tq  $g \cdot [v_1] = [w_1]$ .

Il suffit d'avoir  $g(v_1) = w_1$  (mais ce n'est pas nécessaire).

On peut compléter  $v_1$  en une base  $(v_1, \dots, v_n)$  de  $V$

et  $w_1$  en une base  $(w_1, \dots, w_n)$  de  $V$ .

L'unique application linéaire inversible  $g$  qui envoie la base  $(v_1, \dots, v_n)$  sur la base  $(w_1, \dots, w_n)$  de  $V$  satisfait bien  $g(v_1) = w_1$ , donc  $g \cdot [v_1] = [w_1]$ .

□

$$g: V \longrightarrow V$$

$$x_1 v_1 + \dots + x_n v_n \longmapsto x_1 w_1 + \dots + x_n w_n$$

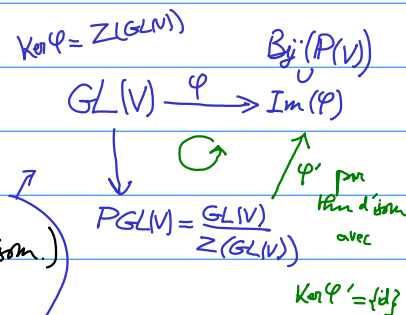
linéaire, injective car  $(w_1, \dots, w_n)$  libre

surjective car  $(w_1, \dots, w_n)$  générés

Exercice: Déterminer, en fonction de la dimension de  $V$ , le plus grand entier  $m$  tel que l'action de  $GL(V)$  sur  $P(V)$  soit  $m$ -transitive.  
 (c'est-à-dire que pour  $[v_1], \dots, [v_m], [w_1], \dots, [w_m]$  dans  $P(V)$ , il existe un élément  $g \in GL(V)$  tq pour tout  $i$  compris entre 1 et  $m$ ,  $g \cdot [v_i] = [w_i]$ )

Proposition: L'action de  $GL(V)$  sur  $P(V)$  n'est pas fidèle.  
 Son noyau est  $Z(GL(V))$ .

Conséquence: L'action de  $PGL(V)$  sur  $P(V)$  induite (par un d'isom.) est fidèle (et toujours transitive).



Preuve: On va montrer: i)  $g \in GL(V)$  agit trivialement  $\Rightarrow g$  est une homothétie  
 (càd  $\exists \lambda \in \mathbb{K}^*, \forall v \in V, g(v) = \lambda v$ )

ii) si  $g \in Z(GL(V))$  alors  $g$  agit trivialement sur  $P(V)$ .  
 rem  $[\lambda v] = [v]$

i) Soit  $g \in GL(V)$  qui agit trivialement sur  $P(V)$ .

C'est-à-dire  $\forall [v] \in P(V), g \cdot [v] = [v]$   
 $\parallel$   
 $[g(v)]$

C'est équivalent à  $\forall v \in V - \{0\}, g(v) \in \mathbb{K}^* v$ .

Si  $v, w \in V - \{0\}$ , alors  $\exists \lambda, \mu \in \mathbb{K}^*$  tq  $g(v) = \lambda v$   
 $g(w) = \mu w$

On a  $g(v+w) = \lambda v + \mu w$ .

$\parallel$   
 $\mathbb{K}^*(v+w)$  donc  $\exists \sigma \in \mathbb{K}^*$  tq  $g(v+w) = \sigma(v+w)$

Remarque: si  $v$  et  $w$  sont colinéaires, alors  $\lambda = \mu$  (car  $g$  est linéaire).

on peut donc supposer que  $v$  et  $w$  ne sont pas colinéaires.

Si  $v$  et  $w$  ne sont pas colinéaires et  $\lambda v + \mu w = \sigma v + \sigma w$   
 alors  $\lambda = \sigma = \mu$ .

On a bien montré que  $g$  est une homothétie.

En particulier,  $g \in Z(GL(V))$



ii) Soit  $g \in Z(GL(V))$  (supposons qu'on ne sache pas que  $Z(GL(V)) = \{\text{homothéties}\}$ )  
 Par l'absurde, supposons qu'il existe  $v \in V$  tq  $g(v) \notin K^*v$ .

Considérons un élément  $h \in GL(V)$  tel que  $h(v) = v$  et  $h(g(v)) = v + g(v)$

(c'est possible car  $v$  et  $g(v)$  sont linéairement indépendants par hypothèse)

(donc on peut compléter  $(v, g(v))$  en une base  $(v, g(v), v_3, \dots, v_n)$ )

et prendre  $h$  dont la matrice dans cette base est

$$\begin{pmatrix} 1 & & & \\ 0 & 1 & & \\ & 1 & 0 & \\ & 0 & & \ddots \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

On utilise maintenant le fait que  $g \in Z(GL(V))$ : ça implique

$$gh = hg, \text{ et donc } g(h(v)) = h(g(v)).$$

$$\begin{array}{ccc} \parallel & & \parallel \\ g(v) & & v + g(v) \end{array}$$

On en déduit  $v = 0$ , qui est une contradiction.  $\square$

Le choix d'une base de  $V$  fournit un isomorphisme entre  $V$  et  $K^n$

$GL(V)$  et  $GL_n(K)$

Pour  $V = K^n$ , on note  $P^{n-1}(K) := P(V)$  "l'espace projectif de dimension  $n-1$  sur  $K$ ",  
 et les éléments de  $P^{n-1}(K)$  sont notés  $[x_1 : \dots : x_n]$  pour la droite engendrée  
 par le vecteur  $(x_1, \dots, x_n) \in K^n \setminus \{0\}$ .

Proposition: Le stabilisateur de  $[1:0:\dots:0] \in P^{n-1}(K)$  sous l'action de  $GL_n(K)$   
 est le sous-groupe  $P$  formé des matrices triangulaires supérieures par blocs  
 de la forme  $\begin{pmatrix} * & & \\ & A' & \\ & & * \end{pmatrix}$ . Plus précisément

$$P = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ & & & \\ & & A' & \\ & & & \end{pmatrix} \mid a_{1,1} \in K^*, A' \in GL_{n-1}(K), a_{1,2}, \dots, a_{1,n} \in K \right\}$$

Preuve: Supposons que  $A \in GL_n(K)$  soit tel que  $A \cdot [1:0:\dots:0] = [1:0:\dots:0]$ .

Cela équivaut à  $A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in K^* \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$  donc à ce que la 1<sup>ère</sup> colonne de  $A$   
 soit de la forme  $\begin{pmatrix} a_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$  avec  $a_{1,1} \in K^*$ .  $\square$

## b) Aspects topologiques: topologie quotient

On va se contenter, dans ce paragraphe, d'introduire la notion topologique qui permet de mettre une topologie utile et naturelle sur les espaces impliqués dans le paragraphe précédent ( $IP(V)$  et  $PGL(V)$ ).

On se place dans le cas où  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ .

Définition (topologie quotient): Soit  $X$  un espace topologique, et  $\mathcal{R}$  une relation d'équivalence sur  $X$ . On note  $X/\mathcal{R}$  l'ensemble des classes d'équivalences et  $p: X \rightarrow X/\mathcal{R}$  la projection qui à  $x \in X$  associe sa classe d'équivalence. Alors la topologie quotient sur  $X/\mathcal{R}$  est la topologie sur  $X/\mathcal{R}$  dont les ouverts sont les parties  $U \subset X/\mathcal{R}$  telles que  $p^{-1}(U)$  soit ouvert dans  $X$ .

Exercice: Vérifier que ça définit bien une topologie.

Par exemple, pour tout sous-groupe  $H$  d'un groupe topologique  $G$ , on a une topologie quotient sur  $G/H$ .

↳ topologie naturelle sur  $\mathbb{P}^{n-1}(\mathbb{C}) = GL_n(\mathbb{C}) / \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$

Exercice\*\*:  $\mathbb{C}^*$  agit sur  $\mathbb{C}^n$  par:  $\lambda \cdot x = \lambda x$  pour  $\lambda \in \mathbb{C}^*$ ,  $x \in \mathbb{C}^n$ .

Cela définit une relation d'équivalence sur  $\mathbb{C}^n$  (dont les classes d'équivalences sont les orbites).

Montrer  $\mathbb{P}^{n-1}(\mathbb{C}) \cong \mathbb{C}^n \setminus \{0\} / \mathbb{C}^*$

et que la topologie quotient donnée par cette écriture coïncide avec la précédente.

(On reviendra dessus si on a le temps + l'occasion)

Proposition: Si  $G$  est un groupe topologique, et  $H$  est un sous-groupe distingué de  $G$ , alors  $G/H$ , muni de la topologie quotient, est un groupe topologique.

Corollaire: Le groupe  $PGL_n(\mathbb{C})$  est un groupe topologique pour la topologie quotient  $\frac{GL_n(\mathbb{C})}{Z(GL_n(\mathbb{C}))}$ .

Rem: Si on a le temps et l'occasion, on verra une autre manière d'obtenir la même topologie sur  $PGL_n(\mathbb{C})$ .

Preuve: Il s'agit de vérifier que le produit  $\bar{\varphi}: G/H \times G/H \rightarrow G/H$  et l'inverse  $\bar{I}: G/H \rightarrow G/H$  sont des applications continues.

On a: • le produit  $\varphi: G \times G \rightarrow G$  et l'inverse  $I: G \rightarrow G$  pour  $G$  sont continues

• la projection  $p: G \rightarrow G/H$  est continue.

Soit  $U$  un ouvert de  $G/H$ .

Alors par définition de la topologie quotient,  $p^{-1}(U)$  est ouvert dans  $G$ .

On a aussi  $I^{-1}(p^{-1}(U))$  ouvert, car  $I$  est continue.

$$p^{-1}(p(I^{-1}(p^{-1}(U))))$$

On a  $\bar{I}^{-1}(U) = p(I^{-1}(p^{-1}(U)))$  donc  $\bar{I}^{-1}(U)$  est ouvert  
(par définition de la topologie quotient).

→  $\bar{I}(p(A)) = I(A)$  (définition de  $\bar{I}$ )  
soit  $p(A) \in \bar{I}^{-1}(U)$  si  $A \in I^{-1}(p^{-1}(U))$

Même raisonnement pour le produit  $\bar{\varphi}$ . □

⊆ Cas  $n=2$ ,  $K=\mathbb{C}$

↳ en TD, Exercices 13 et 14.

# Chapitre 2: Groupes unitaires et orthogonaux

## 1) Formes Hermitiennes et groupes unitaires

Soit  $V$  un espace vectoriel complexe de dimension finie  $n$ .

Définition: Une forme Hermitienne sur  $V$  est une application  $\phi: V \times V \rightarrow \mathbb{C}$  telle que pour tout  $\lambda \in \mathbb{C}$ ,  $u, v, w \in V$ , on a:

- 1)  $\phi(\lambda u + v, w) = \bar{\lambda} \phi(u, w) + \phi(v, w)$
  - 2)  $\phi(u, \lambda v + w) = \lambda \phi(u, v) + \phi(u, w)$
  - 3)  $\phi(u, v) = \overline{\phi(v, u)}$
- ) sesqui-linéaire

Remarques:  
• Ce n'est pas une forme bilinéaire!  
• 2+3  $\Rightarrow$  1.

Définition: Une forme Hermitienne  $\phi$  est définie positive si:

$$\forall u \in V, \quad \phi(u, u) \in \mathbb{R}_+ \quad \text{et} \quad \phi(u, u) = 0 \Rightarrow u = 0.$$

Proposition (immédiate): Le groupe linéaire  $GL(V)$  agit sur l'ensemble des formes Hermitiennes sur  $V$  par précomposition (si  $\phi$  est la forme Hermitienne,  $g \in GL(V)$ ,  $u, v \in V$ ,

$$(g \cdot \phi)(u, v) = \phi(g^{-1}(u), g^{-1}(v))$$

Définition: Soit  $\phi$  une forme Hermitienne sur  $V$ . Le groupe unitaire  $U(\phi)$  est le stabilisateur de  $\phi$  pour cette action:

$$\begin{aligned} U(\phi) &= \{g \in GL(V) \mid g \cdot \phi = \phi\} \\ &= \{g \in GL(V) \mid \forall u, v \in V, \quad \phi(g^{-1}(u), g^{-1}(v)) = \phi(u, v)\} \\ &= \{g \in GL(V) \mid \forall u, v \in V, \quad \phi(g(u), g(v)) = \phi(u, v)\} \end{aligned}$$

Exemple / exercice: Si  $V = \mathbb{C}$  de dimension 1 ?

$\phi$  forme Hermitienne.  $\phi(u, v) = \bar{u} v \phi(1, 1) \quad \forall u, v \in \mathbb{C}$   
par les conditions 1 et 2 de la defa

condition 3 :  $\phi(u, v) = \overline{\phi(v, u)}$  ici  $\bar{u}v \phi(1, 1) = \bar{u}v \overline{\phi(1, 1)}$

$\Rightarrow \overline{\phi(1, 1)} = \phi(1, 1)$  donc  $\phi(1, 1) \in \mathbb{R}$ .

Sur  $\mathbb{C}$ , forme Hermitienne  $\Leftrightarrow$  un réel

$$\phi \Leftrightarrow \phi(1, 1)$$

De plus  $\phi$  est définie positive si  $\phi(1, 1) \in \mathbb{R}_+^*$ .

$$U(\phi) = \left\{ t \in GL_n(\mathbb{C}) \simeq \mathbb{C}^* \mid \overline{(tu)}^t v \overset{\phi(tu, tv)}{\phi(1, 1)} = \bar{u}v \phi(1, 1) \quad \forall u, v \in \mathbb{C} \right\}$$
$$= \{ t \in \mathbb{C}^* \mid |t| = 1 \} \quad \text{si } \phi(1, 1) \neq 0$$
$$(= \mathbb{C}^* \text{ si } \phi(1, 1) = 0) \quad //$$

## 2) Base orthonormée adaptée à une application unitaire

Soit  $\phi$  une forme Hermitienne définie positive sur  $V$ .

Définition : • On appelle base orthonormée de  $(V, \phi)$  une base  $(e_1, \dots, e_n)$  de  $V$  tq  $\phi(e_i, e_j) = \delta_{ij}$ .

• On appelle application unitaire un élément de  $U(\phi)$ .

Théorème : Si  $f \in U(\phi)$ , alors il existe une base orthonormée de  $(V, \phi)$  formée de vecteurs propres pour  $f$ , et toutes les valeurs propres ont module 1.

Lemme : Si  $f \in U(\phi)$ , et  $\lambda$  est une valeur propre de  $f$ , alors  $|\lambda| = 1$ .

Preuve : Soit  $u$  un vecteur propre pour la valeur propre  $\lambda$ .

$$\begin{aligned} \text{On a } \phi(u, u) &= \phi(f(u), f(u)) && \text{car } f \in U(\phi) \\ &= \phi(\lambda u, \lambda u) && \text{car } u \text{ vecteur propre} \\ &= \bar{\lambda} \lambda \phi(u, u) \end{aligned}$$

Comme  $\phi$  est définie positive et  $u \neq 0$ ,  $\bar{\lambda} \lambda = 1$   $\square$

Lemme: Soit  $f \in U(\Phi)$ , et  $u$  un vecteur propre pour  $f$  pour une valeur propre  $\lambda$  quelconque.  
 Alors  $u^\perp := \{v \in V \mid \Phi(u, v) = 0\}$  est stable pour  $f$ .  
 (c'est-à-dire : si  $\Phi(u, v) = 0$  alors  $\Phi(u, f(v)) = 0$ )

Preuve: Soit  $v \in u^\perp$ . On a  $\Phi(u, f(v)) = \Phi\left(\frac{1}{\lambda} f(u), f(v)\right)$  ( $\lambda \neq 0$  car  $f \in GL(V)$ )  
 $= \frac{1}{\lambda} \Phi(f(u), f(v))$  par sesquilinearité  
 $= \frac{1}{\lambda} \Phi(u, v)$  car  $f \in U(\Phi)$   
 $= 0$  car  $v \in u^\perp$

□

Preuve du théorème: Par récurrence sur  $n = \dim V$

→ si  $n=1$ , alors  $f$  est la multiplication par  $\lambda$ , avec  $|\lambda|=1$   
 (cas de la dimension déjà traité en exemple)

→ Supposons le résultat prouvé pour toute forme Hermitienne définie positive sur un espace vectoriel de dimension  $\leq n$ .

→ Soit  $V$  un espace vectoriel de dimension  $n+1$ , muni d'une forme Hermitienne définie positive  $\Phi$ . Soit  $f \in U(\Phi)$ .

Comme on travaille sur les complexes,  $f$  admet au moins une valeur propre  $\lambda$  et un vecteur propre  $e_{n+1}$  pour  $\lambda$ . Quitte à multiplier par un réel non nul, on peut supposer que  $\Phi(e_{n+1}, e_{n+1}) = 1$ .

Le sous-espace  $W := e_{n+1}^\perp$  est un sous-espace de dimension  $\leq n$ , stable par  $f$  (par le deuxième lemme). De plus  $\Phi|_{W \times W}$  définit encore une forme Hermitienne définie positive sur  $W$ , et  $f|_W \in U(\Phi|_{W \times W})$ .  
car  $\Phi(e_{n+1}, e_{n+1}) \neq 0$   
 ( $\Phi$  définie positive)

On peut appliquer l'hypothèse de récurrence pour obtenir une base orthonormée  $(e_1, \dots, e_n)$  de  $W$ , formée de vecteurs propres pour  $f|_W$ .

La base  $(e_1, \dots, e_n, e_{n+1})$  fournit la base orthonormée recherchée dans l'énoncé du théorème et les valeurs propres ont module 1 par le premier lemme.

□

Exercice : Si  $\phi$  forme Hermitienne définie positive et  $u \in V \setminus \{0\}$ , montrer que  $\dim(u^\perp) = n$ .

### 3) Interprétation matricielle, groupe unitaire usuel

Soit  $V$  un  $\mathbb{C}$ -ev de dimension  $n$ ,  $\phi$  forme Hermitienne sur  $V$ .

Choisissons  $(e_1, \dots, e_n)$  une base de  $V$ . On a :

$$\begin{aligned} \phi(z_1 e_1 + \dots + z_n e_n, z'_1 e_1 + \dots + z'_n e_n) \\ = \sum_{i,j=1}^n \phi(z_i e_i, z'_j e_j) = \sum_{i,j=1}^n \bar{z}_i z'_j \phi(e_i, e_j) \end{aligned}$$

Notons  $J$  la matrice non dont les coefficients sont les  $\phi(e_i, e_j)$

$Z$  le vecteur colonne  $\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ ,  $Z' = \begin{pmatrix} z'_1 \\ \vdots \\ z'_n \end{pmatrix}$

$$\text{alors : } \phi(z_1 e_1 + \dots + z_n e_n, z'_1 e_1 + \dots + z'_n e_n) = \underbrace{\bar{Z}^T}_{(\bar{z}_1 \dots \bar{z}_n)} J Z'$$

Réciproquement, certains choix de matrices  $J$  permettent de définir des formes Hermitiennes. On reviendra là-dessus plus tard.

Pour le moment, considérons le cas particulier  $J = I_n$ , qui correspond à la forme Hermitienne "standard" sur  $\mathbb{C}^n$  :

$$\phi((z_1, \dots, z_n), (z'_1, \dots, z'_n)) = \sum_{i=1}^n \bar{z}_i z'_i$$

(qui est clairement définie positive :  $\sum_{i=1}^n |z_i|^2 \geq 0$  avec égalité ssi  $z_i = 0 \forall i$ .)

Identifions aussi les éléments de  $GL(\mathbb{C}^n)$  avec les matrices  $GL_n(\mathbb{C})$ .

On note  $U(n) \subset GL_n(\mathbb{C})$  le sous-groupe identifié à  $U(\phi)$ .

C'est le groupe unitaire usuel.

On appelle matrices unitaires les éléments de  $U(n)$ .

Proposition: Les assertions suivantes sont équivalentes pour  $M \in M_n(\mathbb{C})$ :

a)  $M \in U(n)$

b)  $M^*M = I_n$

(où  $M^* = \bar{M}^T$  matrice transposée conjuguée)

c)  $MM^* = I_n$

d)  $M$  est inversible et  $M^{-1} = M^*$

e) les colonnes de  $M$  forment une base orthonormée pour la forme Hermitienne définie positive standard sur  $\mathbb{C}^n$ .



$U(n)$  groupe unitaire de la forme Hermitienne standard sur  $\mathbb{C}^n$ :

$$\phi((z_1, \dots, z_n), (z'_1, \dots, z'_n)) = \sum_{i=1}^n \bar{z}_i z'_i = \bar{Z}^T Z' \quad \text{où } Z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \quad Z' = \begin{pmatrix} z'_1 \\ \vdots \\ z'_n \end{pmatrix}$$

Proposition: Les assertions suivantes sont équivalentes:

- a)  $M \in U(n)$
- b)  $M^*M = I_n$  (où  $M^* = \bar{M}^T$  matrice "adjointe" ou "transconjuguée")
- c)  $M$  inversible et  $M^{-1} = M^*$
- d)  $MM^* = I_n$
- e) les colonnes de  $M$  forment une base orthonormée pour  $\phi$ .

On appelle matrices unitaires les éléments de  $U(n)$ .

Preuve: \*  $b \Leftrightarrow c \Leftrightarrow d$  clair

\* Les coefficients de  $M^*M$  sont les  $C_i^* C_j = \phi(C_i, C_j)$  où  $C_k$  est la  $k^e$  colonne de  $M$ . Si  $M^*M = I_n$  alors  $\phi(C_i, C_j) = \delta_{ij}$  alors  $(C_1, \dots, C_n)$  forme une base orthonormée pour  $\phi$ . Donc  $b) \Rightarrow e)$ , et la réciproque marche pareil. Donc  $b) \Leftrightarrow e)$

\* Enfin,  $M \in U(n) \Leftrightarrow \forall Z, Z' \in \mathbb{C}^n, \phi(MZ, MZ') = \phi(Z, Z')$   
 $\Leftrightarrow \text{---}, (MZ)^* MZ' = Z^* Z'$   
 $\Leftrightarrow \text{---}, Z^* M^* MZ' = Z^* Z'$

Clair:  $M^*M = I_n \Rightarrow M \in U(n)$ .

Réciproquement, il suffit de considérer les  $Z, Z'$  parmi les vecteurs de la base canonique de  $\mathbb{C}^n$  pour obtenir

$$C_i^* C_j = c_i^* M^* M e_j = e_i^* e_j = \delta_{ij}$$

donc  $M^*M = I_n$ . Donc a)  $\Leftrightarrow$  b). □

Proposition: Si  $M \in U(n)$ , alors  $|\det(M)| = 1$ .

Preuve.  $|\det(M)|^2 = \det(M) \overline{\det(M)}$

$$= \det(M) \det(\overline{M})$$

$$= \det(M) \det(M^*)$$

$$= \det(MM^*)$$

$$= \det(I_n) = 1 \quad \square$$

Définition: Le groupe spécial unitaire  $SU(n)$  est le groupe  $SL_n(\mathbb{C}) \cap U(n)$ .

Remarque: C'est un sous-groupe distingué de  $U(n)$  (le noyau de la restriction du déterminant à  $U(n)$ ).

Théorème (réduction des matrices unitaires)

Soit  $U \in U(n)$  une matrice unitaire. Alors il existe une matrice unitaire

$P \in U(n)$ , et  $\lambda_1, \dots, \lambda_n$  des nombres complexes de module 1, tq

$$U = P \operatorname{diag}(\lambda_1, \dots, \lambda_n) P^{-1}$$

Remarque: \* En particulier, les classes de conjugaison dans  $U(n)$  contiennent toutes un représentant diagonal.

\* En particulier, toute matrice unitaire est diagonalisable.

\*  $\operatorname{diag}(\mu_1, \dots, \mu_n) \in U(n) \iff \bar{\mu}_i \mu_i = 1 \quad \forall i \iff |\mu_i| = 1 \quad \forall i$ .

\*  $P \in U(n) \Rightarrow P^{-1} = P^*$

Preuve: C'est une conséquence directe du théorème de la section 2, appliqué à l'endomorphisme  $f=U$  et à  $\phi$  la forme Hermitienne standard sur  $\mathbb{C}^n$ , qui est bien définie positive.

Soit  $\mathcal{B}$  la b.o.n. de  $\mathbb{C}^n$  (pour  $\phi$ ) formée de vecteurs propres de  $U$ . ← pour le thm 2

Soit  $P$  la matrice de passage de la base canonique à la base  $\mathcal{B}$ .

Les vecteurs colonnes de  $P$  sont les éléments de  $\mathcal{B}$ , donc  $P \in U(n)$ .

Alors  $U = P \operatorname{diag}(\lambda_1, \dots, \lambda_n) P^{-1}$  avec  $|\lambda_i| = 1 \quad \forall i$ . □

#### 4) Aspects topologiques

Remarque:  $U(n)$  est un groupe topologique comme  $s$ -groupe de  $GL_n(\mathbb{C})$ .

Théorème 1: Les groupes  $U(n)$  et  $SU(n)$  sont compacts.

Théorème 2: Les groupes  $U(n)$  et  $SU(n)$  sont connexes par arcs.

Preuve du théorème 1:  $SU(n) = SL_n(\mathbb{C}) \cap U(n)$  est un fermé de  $U(n)$ , donc est compact si  $U(n)$  l'est.

Il suffit de montrer que  $U(n)$  est fermé et borné.

$U(n)$  est fermé:  $M \in U(n) \Leftrightarrow M^*M = I_n$

donc  $U(n) = f^{-1}(\{I_n\})$  où  $f: M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$   
 $M \mapsto M^*M$

(application continue car polynomiale)

donc  $U(n)$  est l'image inverse d'un fermé par une application continue, donc  $U(n)$  est fermé,

$U(n)$  est borné:

Notons  $Z \mapsto \|Z\| = \sqrt{Z^*Z}$  norme standard sur  $\mathbb{C}^n$ .

Considérons la norme matricielle associée:

$$\|M\| := \sup_{\|z\|=1} \|Mz\| \quad \text{pour } M \in M_n(\mathbb{C})$$

$$\begin{aligned} \text{Si } M \in U(n), \text{ alors } \|Mz\|^2 &= (Mz)^*Mz = z^*M^*Mz = z^*z = \|z\|^2 \\ &= 1 \text{ si } \|z\|=1 \end{aligned}$$

$$\text{donc } \|M\| = 1.$$

Donc  $U(n)$  est borné.  $\square$

Preuve du Théorème 2 :

D'après le théorème de réduction des matrices unitaires, il suffit de trouver un chemin continu dans  $U(n)$  entre  $I_n$  et  $\text{diag}(\lambda_1, \dots, \lambda_n)$  pour tout  $(\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n$  tq  $|\lambda_i| = 1 \forall i$ .

En effet si  $\gamma$  est un tel chemin, alors pour  $P \in U(n)$ ,  
 $t \mapsto P\gamma(t)P^{-1}$  est un chemin continu dans  $U(n)$  entre  $I_n$  et  $P\text{diag}(\lambda_1, \dots, \lambda_n)P^{-1}$ .

$$1 = I_n$$
$$U(1) = \{\text{nb cplx de module } 1\}$$



$$\lambda_j = e^{i\theta_j}$$

$$\gamma(t) = \text{diag}(e^{it\theta_1}, \dots, e^{it\theta_n})$$

chemin continu entre  $\gamma(0) = \text{diag}(e^0, \dots, e^0) = I_n$

$$\text{et } \gamma(1) = \text{diag}(\lambda_1, \dots, \lambda_n).$$

Manque  $SU(n) \rightarrow \mathbb{T}$

□

5) Passer du complexe au réel : matrices orthogonales

$$U(n) = \{M \in GL_n(\mathbb{C}) \mid M^*M = I_n\} \subset GL_n(\mathbb{C})$$

$$GL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{C}) \mid \bar{M} = M\}$$

$$U(n) \cap GL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{C}) \mid M^*M = I_n \text{ et } \bar{M} = M\}$$

$$= \{M \in GL_n(\mathbb{R}) \mid M^T M = I_n\}$$

$$=: O(n)$$

Définition : Le groupe orthogonal standard  $O(n)$  est le groupe des matrices  $M \in GL_n(\mathbb{R})$  tq  $M^T M = I_n$ .

Les éléments de  $O(n)$  s'appellent les matrices orthogonales.

Corollaire (de la compacité de  $U(n)$ ) : Le groupe  $O(n)$  est compact.

Preuve :  $U(n)$  est compact,  $GL_n(\mathbb{R})$  est un fermé de  $GL_n(\mathbb{C})$

$O(n)$  fermé dans un compact, donc compact. □

Jeu : réduction des matrices orthogonales d'après réduction des matrices unitaires.

## 5) Passer du complexe au réel

Rappel:  $O(n) = \{M \in GL_n(\mathbb{R}) \mid M^T M = I_n\} = GL_n(\mathbb{R}) \cap U(n)$

$U(n)$  compact  $\Rightarrow O(n)$  compact.

$U(n)$  est connexe. Q:  $O(n)$  est connexe?

rappel:  $GL_n(\mathbb{R}) = \det^{-1}(\mathbb{R}_+^*) \cup \det^{-1}(\mathbb{R}_-^*)$  n'est pas connexe.

Q:  $\exists$ ? matrice de déterminant négatif dans  $O(n)$ ?

Prop:  $\forall M \in O(n)$ ,  $\det(M) = \pm 1$ .

Preuve:  $M \in U(n)$  donc  $|\det(M)| = 1$ .

$M \in GL_n(\mathbb{R})$  donc  $\det(M) \in \mathbb{R}$   $\square$

Remarque: Une matrice diagonale  $\text{diag}(t_1, \dots, t_n)$  est dans  $O(n)$

ssi  $t_j = \pm 1$  pour tout  $1 \leq j \leq n$ .

En particulier,  $\text{diag}(-1, 1, \dots, 1)$  est dans  $O(n)$

et son déterminant vaut  $-1$ .

$$\begin{array}{l} \text{diag}(t_1, \dots, t_n)^T \text{diag}(t_1, \dots, t_n) \\ \parallel \\ \text{diag}(t_1^2, \dots, t_n^2) \\ \parallel \\ I_n \quad \text{ssi } t_j^2 = 1 \quad \forall j \end{array}$$

"Théorème": Le groupe orthogonal  $O(n)$  n'est pas connexe.

Preuve:  $O(n) = \varphi^{-1}(\mathbb{R}_+^*) \cup \varphi^{-1}(\mathbb{R}_-^*)$   
 $\varphi: O(n) \rightarrow \mathbb{R}, M \mapsto \det M$  continue  
 $\varphi^{-1}(\mathbb{R}_+^*) = I_n$   
 $\varphi^{-1}(\mathbb{R}_-^*) = \text{diag}(-1, 1, \dots, 1)$

Définition: Le groupe spécial orthogonal  $SO(n)$  est le groupe

$$SO(n) = O(n) \cap SL_n(\mathbb{R}) = SU(n) \cap GL_n(\mathbb{R}) = U(n) \cap SL_n(\mathbb{R}) \dots$$

formé des matrices orthogonales de déterminant 1.

Remarque: (c'est un sous-groupe distingué de  $O(n)$  (le noyau de la restriction du déterminant)).

Q: Est-ce que  $SO(n)$  est connexe?  $\rightarrow$  Réduction des matrices orthogonales?



$$M \in U(2), \exists \varphi \in \mathbb{R}, e^{i\varphi} M \in SU(2)$$

$$e^{2i\varphi} = \det M$$

Soit maintenant  $M \in O(2) - SO(2)$ .

Remarque : ici l'exercice de la dernière fois ne donne rien d'intéressant, car  $\pm i \notin \mathbb{R}$ .

Par contre, on connaît un élément  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O(2) - SO(2)$ .

Alors  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M \in SO(2)$  donc  $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R_\theta$  pour un  $\theta \in \mathbb{R}$ .

$$M = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

On veut montrer que  $M$  est conjuguée à  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  par une matrice de  $O(2)$ .

(interprétation géométrique :  $M$  est la réflexion orthogonale par rapport à une droite vectorielle,  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  est la réflexion orthogonale par rapport à l'axe des abscisses. Pour passer d'une droite vectorielle à une autre dans  $\mathbb{R}^2$ , il suffit d'une rotation. Donc on peut chercher la matrice de changement de passage parmi les matrices de rotation.)

$$\begin{aligned} \text{Soit } \varphi \in \mathbb{R}, \quad R_\varphi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R_{-\varphi} &= \begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos \varphi & -\sin \varphi \\ -\sin \varphi & -\cos \varphi \end{pmatrix} \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos^2 \varphi - \sin^2 \varphi & -2 \sin \varphi \cos \varphi \\ -2 \sin \varphi \cos \varphi & \sin^2 \varphi - \cos^2 \varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos(2\varphi) & -\sin(2\varphi) \\ -\sin(2\varphi) & -\cos(2\varphi) \end{pmatrix} \\ &= \begin{pmatrix} \cos(-2\varphi) & \sin(-2\varphi) \\ \sin(-2\varphi) & -\cos(-2\varphi) \end{pmatrix} \end{aligned}$$

$$\text{Donc } M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R_\theta = R_{-\frac{\theta}{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R_{\frac{\theta}{2}}. \quad \square$$

Preuve dans le cas général : plus tard //

Théorème : Le groupe  $SO(n)$  est connexe.

Preuve: Il suffit de construire un chemin continu entre  $I_n$  et toute matrice  $M \in SO(n)$ .

Par réduction,  $M = P^{-1} \text{diag}(I_p, -I_q, R_{\theta_1}, \dots, R_{\theta_r}) P$  avec  $q = 2p$  pair.

On peut aussi écrire  $M = P^{-1} \text{diag}(I_p, \underbrace{R_{\pi}, \dots, R_{\pi}}_{p \text{ fois}}, R_{\theta_1}, \dots, R_{\theta_r}) P$

Considérons le chemin  $\gamma: [0, 1] \rightarrow M_n(\mathbb{R})$

$$t \mapsto P^{-1} \text{diag}(I_p, R_{t\pi}, \dots, R_{t\pi}, R_{t\theta_1}, \dots, R_{t\theta_r}) P$$

C'est un chemin continu, à valeurs dans  $SO(n)$ , tq

$$\gamma(0) = I_n \text{ et } \gamma(1) = M. \quad \square$$

Proposition: Une matrice  $M \in M_n(\mathbb{R})$  est orthogonale ssi l'une des conditions suivantes est satisfaite:

1)  $M^T M = I_n$

2)  $M M^T = I_n$

3)  $M \in GL_n(\mathbb{R})$  et  $M^{-1} = M^T$

4) les colonnes de  $M$  forment une b.o.n. de  $\mathbb{R}^n$  pour le produit scalaire standard sur  $\mathbb{R}^n$ :

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$$

$$\langle X, Y \rangle = X^T Y = \sum_{i=1}^n x_i y_i$$

5)  $\mathbb{R}^n \rightarrow \mathbb{R}^n$  est une isométrie linéaire de  $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$

$$X \mapsto MX$$

$$(\text{cà-d } \forall X \in \mathbb{R}^n, \|MX\|^2 = \|X\|^2$$

$$\text{ou } \|X\|^2 = \langle X, X \rangle)$$

6)  $\forall X, Y \in \mathbb{R}^n, \langle MX, MY \rangle = \langle X, Y \rangle$ .

Preuve: exercice. 6)  $\Leftrightarrow$  5): 6)  $\Rightarrow$  5) en prenant  $Y = X$

5)  $\Rightarrow$  6) la norme détermine le produit scalaire par polarisation

$$\|X+Y\|^2 = \langle X+Y, X+Y \rangle = \langle X, X \rangle + 2\langle X, Y \rangle + \langle Y, Y \rangle$$

$$\langle X, Y \rangle = \frac{1}{2} (\|X+Y\|^2 - \|X\|^2 - \|Y\|^2)$$



$$(X+Y)^*(X+Y) = X^*X + \underbrace{X^*Y + Y^*X}_{X^*Y = Y^*X} + Y^*Y$$

mais en général  $X^*Y \neq Y^*X$   
donc le  $\ddot{a}$  raisonnement ne marche pas.

## 6) Les éléments de $O(3)$ et $SO(3)$

Par le thm de réduction, on a les cas suivants possibles pour  $M \in O(3)$

\*  $p=3$ ,  $M = I_3$

\*  $p=1, q=0$  }  $M$  conjuguée à  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & R_\theta & 0 \end{pmatrix}$  avec  $\theta \in ]0, 2\pi[$   
ou  $p=1, q=2$  }

géométriquement :  $M$  est une rotation dans  $\mathbb{R}^3$

d'axe l'espace propre pour la vp 1

d'angle  $\theta$ .

\*  $p=2, q=1$ ,  $M$  conjuguée à  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

:  $M$  est une réflexion orthogonale

par rapport au plan des vecteurs propres pour la vp 1.

\*  $p=0, q=1$ ,  $M$  conjuguée à  $\begin{pmatrix} -1 & 0 & 0 \\ 0 & R_\theta & 0 \end{pmatrix}$

:  $M$  est une réflexion

d'axe l'espace propre pour la vp -1  
et d'angle  $\theta$ .

\*  $q=3$ ,  $M = -I_3$ .

$M$  est la symétrie centrale.

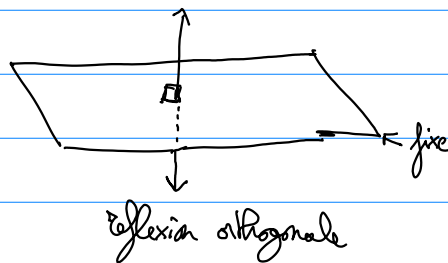
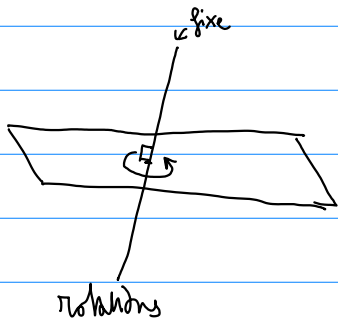
## 6) Les éléments de $O(3)$ et $SO(3)$

Les éléments de  $O(3)$  sont les isométries vectorielles de  $\mathbb{R}^3$ .

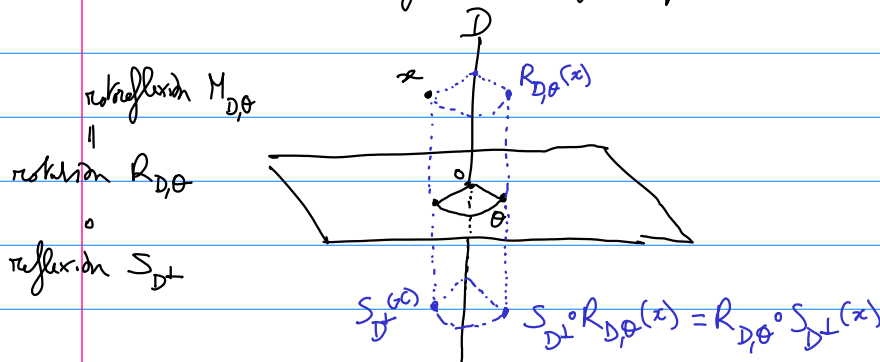
← préserve le produit scalaire

→ préserve la structure de  $\mathbb{R}$ -ev

\_\_\_\_\_ de  $SO(3)$  \_\_\_\_\_ qui préservent l'orientabilité.  
 On appelle aussi  $SO(3)$  le groupe des rotations de  $\mathbb{R}^3$ .



Une rotoreflexion d'axe  $D$  et d'angle  $\theta$  est la composée (dans n'importe quel ordre) de la rotation d'axe  $D$  et d'angle  $\theta$  avec la réflexion par rapport à  $D^\perp$ .  
 Rem: une rotoreflexion ne fixe que  $O$ .



Proposition: Soit  $M \in O(3)$

1) Si  $\det(M) = 1$ , alors  $M$  est une rotation (et réciproquement)  
 (ou  $M$  est l'identité (≈ rotation d'angle 0 pour n'importe quel axe))

2) Si  $\det(M) = -1$  et 1 est valeur propre de  $M$ , alors  $M$  est une réflexion orthogonale.

3) Sinon,  $M$  est une rotoreflexion (ou  $M = -I_3$  ≈ rotoreflexion d'angle  $\pi$  pour n'importe quel axe)

Preuve du théorème de réduction pour  $O(3)$ :

$M \in O(3)$

Fun de réduction sur  $M \iff$  il existe une base orthonormée pour le produit scalaire standard de  $\mathbb{R}^3$  dans laquelle l'application linéaire  $\mathbb{R}^3 \rightarrow \mathbb{R}^3$   
 $X \mapsto MX$

s'écrit sous la forme  $\text{diag}(I_p, -I_q, R_{\theta_1}, \dots, R_{\theta_k})$ .

$\chi_M$  polynôme caractéristique de  $M$  est réel car  $M$  l'est.  
est de degré 3.

$\implies \chi_M$  a au moins une racine réelle

De plus, ces valeurs propres de  $M$  ont module 1. (car  $M \in U(3)$ )

$\implies \chi_M$  a 1 ou -1 comme racine.

Soit  $v$  un vecteur propre (réel) pour une valeur propre (réelle) de  $M$ .

Alors la décomposition  $\mathbb{R}^3 = \mathbb{R}v \oplus (\mathbb{R}v)^\perp$  est stable par  $M$ . (immédiat, à écrire)

On peut choisir une base orthonormée  $(e_1, e_2, e_3)$  adaptée à cette décomposition.

Dans cette base, l'application  $X \mapsto MX$  s'écrit:

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \text{ avec } \lambda = \pm 1 \text{ et } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O(2)$$

On a prouvé le théorème de réduction pour  $O(2)$ , donc quitte à modifier la base orthonormée  $(e_2, e_3)$ , la matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  est de la forme  $R_\theta$  ou  $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ . □

7) Preuve du théorème de réduction pour  $n$  quelconque.

Lemme: Soit  $V \subset \mathbb{C}^n$  un sous-espace vectoriel complexe de dimension complexe égale à  $k$ , stable par conjugaison (c-à-d  $X \in V \implies \bar{X} \in V$ ). Alors  $V \cap \mathbb{R}^n$  est un sous-espace vectoriel réel de dimension réelle égale à  $k$ .

Preuve: On a  $V = (V \cap \mathbb{R}^n) \oplus (V \cap i\mathbb{R}^n)$ .

en effet:  $\bullet \mathbb{R}^n \cap i\mathbb{R}^n = \{0\}$

$$\bullet \forall x \in V, x = \underbrace{\frac{x+\bar{x}}{2}}_{\in V} + \frac{x-\bar{x}}{2}$$

$\in V$  car  $V$  est stable par conjugaison.

De plus, la multiplication par  $i$  est une application  $\mathbb{R}$ -linéaire qui réalise un isomorphisme entre  $V \cap \mathbb{R}^n$  et  $V \cap i\mathbb{R}^n$  (d'inverse la multiplication par  $-i$ ).

$$\text{Donc } \dim_{\mathbb{R}}(V) = 2 \dim_{\mathbb{R}}(V \cap \mathbb{R}^n). \quad \square$$

$2\mathbb{R}^n$

Preuve finale du thm de réduction:

$M \in O(n)$ . On se rappelle (comme dans le cas  $n=3$ ) qu'il suffit de trouver une base orthonormée de  $\mathbb{R}^n$  dans laquelle l'application  $X \mapsto MX$  s'écrit  $\text{diag}(I_p, -I_q, R_{\theta_1}, \dots, R_{\theta_k})$ .

On raisonne par récurrence forte.

- Si  $M$  admet une valeur propre réelle (nécessairement  $\pm 1$ ), alors on se ramène à l'hypothèse de récurrence par la méthode que pour le cas  $n=3$ .
- Sinon, soit  $v$  un vecteur propre complexe de  $M$ , pour une valeur propre complexe  $\lambda \notin \mathbb{R}$ .

Comme  $M$  est réelle, on a

$$\overline{Mv} = \overline{\lambda v}$$

$$M\bar{v} = \bar{\lambda} \bar{v} \quad \text{c-à-d} \quad \bar{v} \text{ est vecteur propre de } M \text{ pour la valeur propre } \bar{\lambda} \neq \lambda.$$

En particulier,  $(v, \bar{v})$  est une famille libre de  $\mathbb{C}^n$ .

Par le lemme,  $P := (\mathbb{C}v \oplus \mathbb{C}\bar{v}) \cap \mathbb{R}^n$  est un sous-espace vectoriel réel de dimension 2.

De plus,  $P$  est stable par  $M$ :

$$\text{on a } P = \{z v + \bar{z} \bar{v} \mid z \in \mathbb{C}\}$$

$$\text{or } M(z v + \bar{z} \bar{v}) = z Mv + \bar{z} M\bar{v} = z \lambda v + \bar{z} \bar{\lambda} \bar{v} \in P.$$

L'orthogonal de  $P$  est stable par  $M$  (car  $M$  est une isométrie).

Donc par hypothèse de récurrence appliquée à  $M|_{P^\perp}$  et par le cas  $n=2$  déjà montré, appliqué à  $M|_P$ , on obtient le théorème.  $\square$

## 8) Les groupes orthogonaux en général.

De manière générale:

- à toute forme hermitienne  $\varphi$  sur un  $\mathbb{C}$ -ev  $V$  est associé son groupe unitaire  $U(\varphi)$  (son stabilisateur sous l'action de  $GL(V)$  sur les formes hermitiennes)
- à toute forme bilinéaire symétrique  $B$  sur un  $\mathbb{K}$ -espace vectoriel  $V$  est associé son groupe orthogonal  $O(B)$  (son stabilisateur sous l'action de  $GL(V)$  sur les formes bilinéaires symétriques:  
( $g \cdot B(x, y) := B(g^{-1}x, g^{-1}y)$ .)

Remarque: •  $O(n) :=$  stabilisateur du produit scalaire standard sur  $\mathbb{R}^n$   
• Si  $(V, \langle \cdot, \cdot \rangle)$  est un espace euclidien de dimension finie, alors  $O(\langle \cdot, \cdot \rangle) \simeq O(n)$ .  
• On n'a pas besoin de cas particulier pour travailler avec les formes bilinéaires symétriques.

Exemples:

1) L'application  $\mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$  définit toujours une forme bilinéaire symétrique sur  $\mathbb{C}^n$ .  
 $(X, Y) \mapsto X^T Y$

Le groupe (classique)  $O_n(\mathbb{C})$  "groupe orthogonal complexe" est le groupe orthogonal de cette forme bilinéaire symétrique.

Exercice: • décrire  $O_2(\mathbb{C})$  explicitement.

- est-ce que  $O_n(\mathbb{C})$  est connexe?
- Montrer que  $O_n(\mathbb{C})$  n'est pas compact.

2) Remarque: Une forme bilinéaire symétrique est déterminée par la forme quadratique associée.

(plusialia:  $B(X+Y, X+Y) = B(X, X) + B(Y, Y) + 2 B(X, Y)$ )

Le groupe orthogonal indéfini  $O(p, q)$  est le groupe orthogonal associé à la forme quadratique  $(x_1, \dots, x_{p+q}) \mapsto \sum_{i=1}^p x_i^2 - \sum_{i=1}^q x_{p+i}^2$  sur  $\mathbb{R}^n$ .

Exercice: •  $O(p, q)$  n'est pas compact pour  $p, q \neq 0$

•  $O(p, q) = \{M \in GL_n(\mathbb{R}) \mid M^T J_{p,q} M = J_{p,q}\}$

où  $J_{p,q} = \text{diag}(I_p, I_q)$ .

• Si on considère la  $n$  forme quadratique sur  $\mathbb{C}^n$ , alors le groupe orthogonal associé est isomorphe à  $O_n(\mathbb{C})$ .

---

Fin du Chapitre 2.

# Chapitre 3: Décomposition polaire et exponentielle

doit faire préciser aut matrices symétriques:  $M^T = M$

## ① Matrices hermitiennes et anti-hermitiennes

Définition: Une matrice  $M \in M_n(\mathbb{C})$  est hermitienne si  $M^* = M$ . (rappel  $M^* = \overline{M}^T$ )

Remarque Exemples: •  $n=1$ ,  $M=(z) \in M_1(\mathbb{C})$  est hermitienne si  $\bar{z}=z$  si  $z \in \mathbb{R}$ .

- Une matrice diagonale est hermitienne si ses coefficients sont réels.
- Les coefficients diagonaux d'une matrice hermitienne quelconque sont réels.
- $n=2$ ,  $M = \begin{pmatrix} a & b \\ \bar{c} & d \end{pmatrix}$  est hermitienne si  $\begin{cases} a, d \in \mathbb{R} \\ b = \bar{c} \end{cases}$   
 $M^* = \begin{pmatrix} \bar{a} & \bar{c} \\ b & d \end{pmatrix}$

On peut donc l'écrire en terme de quatre coefficients réels  $\alpha, \beta, \gamma, \delta$ :

$$M = \begin{pmatrix} \alpha & \beta + i\gamma \\ \beta - i\gamma & \delta \end{pmatrix}$$

- Si  $M$  est hermitienne, alors  $\mathbb{C}^n \times \mathbb{C}^n \xrightarrow{\varphi} \mathbb{C}$  définit une forme hermitienne sur  $\mathbb{C}^n$ :  
 $(X, Y) \mapsto X^* M Y$

$$\varphi(\lambda X + Y, Z) = \bar{\lambda} \varphi(X, Z) + \varphi(Y, Z)$$

$$\varphi(X, \lambda Y + Z) = \lambda \varphi(X, Y) + \varphi(X, Z)$$

$$\varphi(X, Y) = \overline{\varphi(Y, X)}$$

$$\parallel$$

$$X^* M Y$$

$$\begin{aligned} \parallel & \overline{\varphi(Y, X)} \\ \parallel & \overline{Y^* M X} \\ \parallel & \overline{Y^T M^T \overline{X}} = \overline{Y^* M^* X} = \overline{Y^* M X} \\ & \uparrow \\ & M \text{ hermitienne} \end{aligned}$$

- Réciproquement, si  $\varphi: V \times V \rightarrow \mathbb{C}$  est une forme hermitienne sur un  $\mathbb{C}$ -ev de dim finie, la matrice associée via le choix d'une base de  $V$  est une matrice hermitienne.

Définition: Une matrice  $M \in M_n(\mathbb{C})$  est anti-hermitienne si  $M^* = -M$ .

Remarques et exemples: •  $n=1$ , matrice anti-hermitienne  $\Leftrightarrow$  imaginaire pure.

- $n=2$ ,  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = -M^* \Leftrightarrow \begin{cases} a, d \in i\mathbb{R} \\ b = -\bar{c} \end{cases}$

en termes de coeffs réels  $\alpha, \beta, \gamma, \delta$ , 
$$M = \begin{pmatrix} i\alpha & \beta + i\gamma \\ -\beta + i\gamma & i\delta \end{pmatrix}$$

• Les coeffs diagonaux d'une matrice anti-hermitienne sont dans  $i\mathbb{R}$ .

Notation: On note  $H_n$  l'ensemble des matrices hermitiennes dans  $M_n(\mathbb{C})$ .

$AH_n$  - - - - - anti-hermitiennes - - - - -

Proposition: i)  $H_n$  et  $AH_n$  sont des sous espaces vectoriels réels de  $M_n(\mathbb{C}) \simeq \mathbb{R}^{2n^2}$ .

ii) Ce ne sont pas des sev complexes de  $M_n(\mathbb{C})$ .

iii) Ils fournissent une décomposition en somme directe:  $M_n(\mathbb{C}) = H_n \oplus AH_n$ .

iv) Les dimensions de  $H_n$  et  $AH_n$  sont égales à  $n^2$ .

Preuve: Soit  $t \in \mathbb{C}$ ,  $M, N \in M_n(\mathbb{C})$ . Alors  $(tM + N)^* = \bar{t}M^* + N^*$

$\rightarrow$  si  $t \in \mathbb{R}$ ,  $(tM + N)^* = tM^* + N^*$  donc  $H_n$  et  $AH_n$  sont des sev réels  
 $\text{Ker}(M \mapsto M - M^*) = \text{Ker}(M \mapsto M + M^*)$

Si  $M \in H_n \cap AH_n$ , alors  $M = M^* = -M$  donc  $M = 0$ , d'où  $H_n \cap AH_n = \{0\}$ .

Si  $M \in H_n$ , alors  $(iM)^* = -iM^* = -iM$ , donc  $iM \in AH_n$ , donc  $iM \notin H_n$ .

Donc  $H_n$  n'est pas un sev complexe.

En fait, la multiplication par  $i$  est un isomorphisme  $\mathbb{R}$ -linéaire (d'inverse la multiplication par  $-i$ ) entre  $H_n$  et  $AH_n$ . En particulier,  $\dim_{\mathbb{R}} H_n = \dim_{\mathbb{R}} AH_n$ .

Si  $M \in M_n(\mathbb{C})$ , alors  $M = \underbrace{\frac{M+M^*}{2}}_{\in H_n} + \underbrace{\frac{M-M^*}{2}}_{\in AH_n}$ , donc  $M_n(\mathbb{C}) = H_n \oplus AH_n$ .

Donc  $2n^2 = \dim_{\mathbb{R}} M_n(\mathbb{C}) = \dim_{\mathbb{R}} H_n + \dim_{\mathbb{R}} AH_n = 2 \dim_{\mathbb{R}} H_n = 2 \dim_{\mathbb{R}} AH_n$ .

□

Remarque: On pourrait aussi déterminer des bases explicites de  $H_n$  et  $AH_n$ .

Par exemple pour  $n=2$ ,

$\left( \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \right)$  forme une base de  $H_2$

$\left( \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right)$  forme une base de  $AH_2$



## ② Réduction des matrices hermitiennes

$H^*$  "matrice adjointe"

On note  $\langle X, Y \rangle = X^* Y$  la forme hermitienne standard sur  $\mathbb{C}^n$ .

Proposition: Si  $H \in M_n(\mathbb{C})$  est hermitienne, alors pour tout  $X, Y \in \mathbb{C}^n$ ,

$$\langle X, HY \rangle = \langle HX, Y \rangle.$$

Preuve: On a

$$\begin{aligned} \langle HX, Y \rangle &= (HX)^* Y \\ &= X^* H^* Y \\ &= X^* H Y \quad \text{car } H \in H_n \\ &= \langle X, HY \rangle \quad \square \end{aligned}$$

Théorème (de réduction des matrices hermitiennes): Soit  $H \in H_n$ , alors il existe une matrice unitaire  $P \in U(n)$  et une matrice diagonale réelle  $D$  telle que

$$H = P D P^*.$$

Rem.:  $P \in U(n) \Leftrightarrow P^{-1} = P^*$ .

• Énoncé équivalent: Il existe une bon  $\mathbb{C}^n$  (pour la forme hermitienne standard) formée de vecteurs propres de  $H$ , et les valeurs propres sont réelles.

• Énoncé équivalent: Si  $V$   $\mathbb{C}$ -ev de dim finie

via le choix  
d'une bon  
pour  $\varphi$ .

$\varphi$  forme hermitienne définie positive  
 $f \in \text{End}(V)$  tq  $\forall x, y \in V, \varphi(f(x), y) = \varphi(x, f(y))$   
alors il existe une bon de  $V$  (pour  $\varphi$ ) formée  
de vecteurs propres pour  $f$ , et les valeurs propres sont réelles.

La preuve du théorème de réduction des matrices hermitiennes suit le même schéma que celle pour les matrices unitaires, par récurrence sur la dimension.  
Elle est  $\approx$  identique modulo les deux lemmes modifiés suivants.

Lemme: Les valeurs propres d'une matrice hermitienne sont réelles.

Preuve: Soit  $\lambda$  une valeur propre pour  $H \in \mathbb{H}_n$ , et  $X$  un vecteur propre pour  $\lambda$ .

$$\begin{aligned} \text{Aby} \quad \langle HX, X \rangle &= \langle \lambda X, X \rangle = \bar{\lambda} \langle X, X \rangle \\ &\parallel \\ \langle X, HX \rangle &= \langle X, \lambda X \rangle = \lambda \langle X, X \rangle \end{aligned}$$

Donc  $\bar{\lambda} = \lambda$ . □

Lemme: Soit  $X$  un vecteur propre pour  $H \in \mathbb{H}_n$ , alors  $X^\perp$  est stable par  $H$ .

orthogonal par rapport à  $\langle \cdot, \cdot \rangle$   
 $= \{Y \in \mathbb{C}^n \mid X^\dagger Y = 0\}$

(On a  $\mathbb{C}X \oplus X^\perp = \mathbb{C}^n$ )

Preuve: Soit  $Y \in X^\perp$ , on a:

$$\langle X, HY \rangle = \langle HX, Y \rangle = \langle \lambda X, Y \rangle = \bar{\lambda} \langle X, Y \rangle = 0 \quad \square$$

On utilisera aussi un résultat de réduction simultanée.

Théorème: Soient  $A_1$  et  $A_2$  deux matrices hermitiennes qui commutent.

Alors il existe une matrice unitaire  $P$  et deux matrices diagonales réelles  $D_1$  et  $D_2$  telles que  $A_1 = PD_1P^{-1}$  et  $A_2 = PD_2P^{-1}$ .

Preuve: Le pm de réduction appliqué à  $A_1$  donne une base de vecteurs propres pour  $A_1$ . En particulier,  $\mathbb{C}^n$  est la somme directe orthogonale des sous-espaces propres  $E_1, \dots, E_r$  de  $A_1$ .

De m  $\mathbb{C}^n$  est la somme directe orthogonale des sous-espaces propres  $F_1, \dots, F_s$  de  $A_2$ .

Comme  $A_1$  et  $A_2$  commutent,  $A_2$  laisse stable les sous-espaces propres de  $A_1$ .

↗

$$\Leftrightarrow E_1 = (E_1 \cap F_1) \oplus \dots \oplus (E_1 \cap F_s) \text{ etc}$$

( Soit  $x \in \text{Ker}(A_1 - \lambda I_n)$ ,  $(A_1 - \lambda I_n)(A_2 x) = A_1 A_2 x - \lambda A_2 x = A_2 (A_1 - \lambda I_n) x = 0$   
donc  $A_2 x \in \text{Ker}(A_1 - \lambda I_n)$ .

$$\text{Donc } \mathbb{C}^n = E_1 \oplus E_2 \oplus \dots \oplus E_n$$

$$\mathbb{C}^n = (E_1 \cap F_1) \oplus (E_1 \cap F_2) \oplus \dots \oplus (E_1 \cap F_s) \oplus (E_2 \cap F_1) \oplus \dots \oplus (E_n \cap F_s)$$

$$= \bigoplus_{\substack{1 \leq i \leq n \\ 1 \leq j \leq s}} (E_i \cap F_j)$$

En prenant une base adaptée à cette décomposition, on obtient une base  
formée de vecteurs propres communs à  $A_1$  et  $A_2$ . □

### 3) Racines carrées de matrices hermitiennes définies positives

Rappel:  $H$  matrice hermitienne  $\Leftrightarrow H \in H_n \Leftrightarrow H^* = H \Leftrightarrow \begin{matrix} \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C} \\ (X, Y) \mapsto X^* H Y \\ \text{forme hermitienne} \end{matrix}$

Définition: Soit  $H \in H_n$ . On dit que  $H$  est positive si  $\forall X \in \mathbb{C}^n, X^* H X \geq 0$ .  
On dit que  $H$  est définie positive si  $\forall X \in \mathbb{C}^n \setminus \{0\}, X^* H X > 0$ .

On note  $H_n^+$  l'ensemble des matrices hermitiennes positives.  $\left. \begin{matrix} H \geq 0 \\ H > 0 \end{matrix} \right\} \begin{matrix} H_n^+ \\ \text{définies positives.} \end{matrix}$

Remarque:  $H > 0$  si la forme hermitienne sur  $\mathbb{C}^n$  associée à  $H$  est définie positive.

Exemples: • l'identité  $I_n \in H_n^{++}$

•  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in H_n^+ \setminus H_n^{++}$  :  $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$   $X^* \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} X = |x_1|^2 \geq 0, = 0$  pour  $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \neq 0$ .

•  $\begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} \notin H_n^+$   $X^* \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} X = -|x_1|^2$  pas positif pour  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ .

•  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin H_n^+$   $X^* \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X = (\bar{x}_1 \ \bar{x}_2) \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \bar{x}_1 x_2 + \bar{x}_2 x_1 = 2 \operatorname{Re}(x_1 x_2) < 0$   
par ex pour  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

Proposition: Soit  $H \in H_n$ . Alors  $H \in H_n^+$  si toutes ses valeurs propres sont positives.

Et  $H \in H_n^{++}$  strictement positives.

Preuve: • Supposons que  $\lambda$  est une valeur propre de  $H$ , et  $X$  un vecteur propre associé.

$$X^* H X = X^* (\lambda X) = \lambda X^* X \quad \text{or } X^* X = \sum_{i=1}^n |x_i|^2 > 0 \text{ si } X \neq 0.$$

$$\text{Donc } H \in H_n^+ \Rightarrow \lambda \geq 0$$

$$H \in H_n^{++} \Rightarrow \lambda > 0.$$

• Réciproquement, supposons que toutes les valeurs propres de  $H$  sont positives.

Par le théorème de réduction des matrices hermitiennes,  $H = P^{-1} D P$  avec  $P \in U(n)$

et  $D$  matrice diagonale à coefficients diagonaux réels positifs,  $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$  avec  $\lambda_j \in \mathbb{R}_+$ .

Pour tout  $Y \in \mathbb{C}^n$ ,  $Y^* D Y = \sum_{j=1}^n \lambda_j |y_j|^2 \geq 0$ .

"  $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

Pour  $H$  et  $X \in \mathbb{C}^n$ ,  $X^* H X = (X^* P^*) D (P X)$   $P^{-1} = P^*$  car  $P \in U(n)$   
 $= (P X)^* D (P X) \geq 0$  par le raisonnement ci-dessus avec  $Y = P X$ .

(si raisonnement pour  $H \in H_n^{++}$ ) □

- Corollaire:
- Si  $H \in H_n^+$ , alors  $\text{tr}(H) \geq 0$  et  $\det(H) \geq 0$ .
  - Si  $H \in H_n^{++}$ , alors  $\text{tr}(H) > 0$  et  $\det(H) > 0$ .
  - Soit  $H \in H_n^+$ , alors  $H \in H_n^{++}$ ssi  $\det(H) \neq 0$ .
- (cà d  $H_n^{++} = H_n^+ \cap GL_n(\mathbb{C})$ )

Théorème (racines carrées de matrices hermitiennes positives): Soit  $H \in H_n^+$ , alors il existe une unique matrice  $P \in H_n^+$  telle que  $P^2 = H$ . De plus si  $H \in H_n^{++}$ , alors  $P \in H_n^{++}$ .

On notera  $\sqrt{H} := P$  cette racine carrée dans  $H_n^+$ .

⚠ Attention: en général, une matrice admet beaucoup de racines carrées distinctes.

Par exemple,  $\sqrt{I_2} = I_2$ , mais toutes les matrices suivantes vérifient  $R^2 = I_2$ :

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \dots \quad (\text{il y en a une infinité}).$$

Preuve: Supposons que  $P \in H_n^+$  satisfait  $P^2 = H$ .

On a  $PH = PP^2 = P^3 = P^2P = HP$  donc  $H$  et  $P$  commutent.

Par réduction simultanée, il existe une base  $(e_1, \dots, e_n)$  de  $\mathbb{C}^n$  formée de vecteurs propres communs à  $P$  et  $H$ .

Notons  $\lambda_j, \mu_j \in \mathbb{R}_+$  tq  $He_j = \lambda_j e_j$   $Pe_j = \mu_j e_j$ ,

alors  $\lambda_j e_j = He_j = PPe_j = \mu_j Pe_j = \mu_j^2 e_j$

donc  $\mu_j^2 = \lambda_j$ .

Or  $\mu_j \in \mathbb{R}_+$ , donc  $\mu_j = \sqrt{\lambda_j}$ .

Sur le sous-espace propre associé à une valeur propre  $\lambda$  de  $H$ ,  $P$  agit comme l'homothétie  $X \mapsto \sqrt{\lambda} X$ . Ça me détermine  $P$  de manière unique sur chaque sous-espace propre de  $H$ , donc sur  $\mathbb{C}^n$  qui est la somme directe de ces sous-espaces propres.

Réciproquement, si  $P$  est défini par la propriété ci-dessus, alors  $P \in H_n^+$  et  $P^2 = H$ .

Enfin si  $H \in H_n^{++}$ , alors  $\det(H) \neq 0$ , donc  $(\det(P))^2 = \det(H) \neq 0$ , donc  $\det(P) \neq 0$ , donc  $P \in H_n^{++}$ .  $\square$

#### 4) Décomposition polaire de $GL_n(\mathbb{C})$ .

Théorème (Décomposition polaire): Soit  $A \in GL_n(\mathbb{C})$ . Il existe un unique couple  $(U, P)$  tel que  $U \in U(n)$ ,  $P \in H_n^{++}$  et  $A = UP$ .

Remarque: Pour  $n=1$ , on a  $GL_1(\mathbb{C}) = \mathbb{C}^*$ ,  $H_1^{++} = \mathbb{R}_+^*$  et  $U(1) = \{z \in \mathbb{C} ; |z|=1\}$ .

Pour  $a \in \mathbb{C}^*$ ,  $\exists!(u, p) \in U(1) \times \mathbb{R}_+^*$  tq  $a = up$  :

en effet,  $p = |u|p = |a|$  et  $u = \frac{a}{|a|} = \frac{a}{p}$

(en notant  $u = e^{i\theta}$ ,  $p = r$ ,  
 $a = re^{i\theta}$  coordonnées polaires dans  $\mathbb{C}$ )

Preuve: Commençons par l'unicité. Soient  $U \in U(n)$ ,  $P \in H_n^{++}$  tq  $A = UP$ .

$$\begin{aligned} A^*A &= (UP)^*UP = P^*U^*UP \\ &= P^*P \quad \left. \begin{array}{l} \text{car } U \in U(n) \\ \text{car } P \in H_n \end{array} \right\} \\ &= P^2 \end{aligned}$$

Or  $A^*A$  est une matrice hermitienne définie positive :

$$(A^*A)^* = A^*A^{**} = A^*A \quad \text{donc } A^*A \in H_n$$

si  $X \in \mathbb{C}^n \setminus \{0\}$ ,  $X^*A^*AX = (AX)^*(AX) > 0$  car  $A$  inversible, donc  $AX \in \mathbb{C}^n \setminus \{0\}$ .

donc  $A^*A \in H_n^{++}$ .

On en déduit, par le théorème de la section précédente, que  $P = \sqrt{A^*A}$  est l'unique racine carrée de  $A^*A$  dans  $H_n^{++}$ .

Et  $U = AP^{-1}$  donc  $U$  est aussi déterminée de manière unique.

Pour l'existence, il faut vérifier que  $P := \sqrt{A^*A}$  et  $U := A(\sqrt{A^*A})^{-1}$  marchent, c'est-à-dire  $A = UP$ ,  $P \in H_n^{++}$  et  $U \in U(n)$ .

*évident* *conséquence du thm précédent*

$$\begin{aligned} \text{On calcule } U^*U &= (AP^{-1})^*AP^{-1} = (P^{-1})^*A^*AP^{-1} \\ &= (P^*)^{-1}P^2P^{-1} \quad \left. \begin{array}{l} \\ \end{array} \right\} P^* = P \text{ car } P \in H_n \\ &= P^{-1}P^2P^{-1} \\ &= I_n \end{aligned}$$

$\square$

$O(n) \times S_n^{++} \rightarrow GL_n(\mathbb{R})$  ← matrices symétriques réelles définies positives.

Théorème (décomposition polaire topologique): L'application  $\Phi: U(n) \times H_n^{++} \rightarrow GL_n(\mathbb{C})$   
 $(U, P) \mapsto UP$

est un homéomorphisme. (pour les topologies induites de  $U(n) \subset \text{Mat}_{n \times n}(\mathbb{C}) \cong \mathbb{C}^{n^2}$ )  
 $H_n^{++}$   
 $GL_n(\mathbb{C})$

Preuve: Par le théorème de décomposition polaire précédent,  $\Phi$  est bijective.

De plus  $\Phi$  est continue car le produit de matrices est continu.

Il reste à montrer que son inverse  $\Phi^{-1}$  est continue.

Par la preuve de la décomposition polaire,  $\Phi^{-1}(A) = (U, P)$  avec  $P = \sqrt{A^*A}$  et  $U = AP^{-1}$ .

Il suffit donc de montrer que la racine carrée  $\sqrt{\cdot}: H_n^{++} \rightarrow H_n^{++}$  est continue.

On montre ceci par critère séquentiel de continuité.

Soit  $(B_k)$  une suite dans  $H_n^{++}$ , qui converge vers  $C \in H_n^{++}$ . On veut que

$$\lim_{k \rightarrow +\infty} \sqrt{B_k} = \sqrt{C}.$$

Lemme: La suite  $(B_k)$  est bornée, donc la suite  $(\sqrt{B_k})$  est bornée. → voir en TD

Donc la suite  $(\sqrt{B_k})$  est dans un compact, donc elle converge ssi elle admet une unique valeur d'adhérence. (c'est un résultat standard de topologie)   
exercice

Considérons une sous-suite convergente  $(\sqrt{B_{k_j}})_j$ , qui converge vers une limite  $Q$ .

Lemme:  $H_n^{++}$  est fermé. → en TD

Donc  $Q \in H_n^{++}$ .

Par continuité du produit de matrices,  $\lim_{j \rightarrow \infty} B_{k_j} = \lim_{j \rightarrow \infty} (\sqrt{B_{k_j}})^2 = Q^2$ , et  $C \in H_n^{++}$ , donc  $Q = \sqrt{C}$  par unicité dans le lemme sur les racines carrées dans  $H_n^{++}$ .

Donc  $(\sqrt{B_k})$  converge vers  $\sqrt{C}$ . Donc  $\sqrt{\cdot}$  est une application continue.  $\square$

## 5) Décomposition polaire réelle

Rappel:  $M_n(\mathbb{R}) = \{M \in M_n(\mathbb{C}) ; \bar{M} = M\}$   
 $O(n) = U(n) \cap M_n(\mathbb{R})$

Définition: Une matrice  $M \in M_n(\mathbb{C})$  est symétrique réelle si  $\bar{M} = M$  et  $M^T = M$ .  
On note  $S_n$  l'ensemble des matrices symétriques réelles.

Remarque:  $S_n = H_n \cap M_n(\mathbb{R})$

De même, on note  $S_n^+ = H_n^+ \cap M_n(\mathbb{R})$  l'ensemble des matrices symétriques réelles positives, et  $S_n^{++} = H_n^{++} \cap M_n(\mathbb{R})$  l'ensemble des matrices symétriques réelles définies positives.

On se rappelle que  $M \in S_n^{++}$  définit un produit scalaire (euclidien) sur  $\mathbb{R}^n$  par l'application  $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$   
 $(X, Y) \mapsto X^T M Y$

Enfin, on note  $AS_n = AH_n \cap M_n(\mathbb{R})$  l'ensemble des matrices antisymétriques réelles.

Proposition: On a  $M_n(\mathbb{R}) = S_n \oplus AS_n$  et  $\dim(S_n) = \frac{n(n+1)}{2}$  (donc  $\dim(AS_n) = \frac{n(n-1)}{2}$ ).

Preuve: Sa découle immédiatement de  $M_n(\mathbb{C}) = H_n \oplus AH_n$  par la somme directe.

Pour la dimension, le plus simple est de donner une base de  $S_n$ :

les  $E_{i,i}$  pour  $1 \leq i \leq n$  et les  $E_{i,j} + E_{j,i}$  pour  $1 \leq i < j \leq n$ .

$n$

$$1+2+\dots+(n-1) = \frac{n(n-1)}{2}$$

□

Théorème (Racines carrées de matrices symétriques réelles positives):

Soit  $M \in S_n^+$ . Alors  $\exists ! P \in S_n^+$  tq  $P^2 = M$ . De plus, si  $M \in S_n^{++}$ , alors  $P \in S_n^{++}$ .

Preuve:  $M \in S_n^+ \subset H_n^+$  donc  $\exists ! P \in H_n^+$  tq  $P^2 = M$ . On veut mq  $P \in S_n^+$ , ie  $\bar{P} = P$ .

On a  $(\bar{P})^* = \bar{P}^* = \bar{P}$  donc  $\bar{P} \in H_n$ .

$\uparrow$   
 $P \in H_n$



Les valeurs propres de  $P$  sont réelles, donc ce sont les mêmes que celles de  $\bar{P}$ . Elles sont donc positives (car  $P \in H_n^+$ ), donc  $\bar{P} \in H_n^+$ .

On calcule  $\bar{P}^2 = (\bar{P}^2) = \bar{M} = M$  car  $M \in M_n(\mathbb{R})$ .

Par unicité de la racine carrée hermitienne positive, on a  $\bar{P} = P$ .  $\square$

Théorème (décomposition polaire réelle): L'application  $\Phi: O(n) \times S_n^{++} \longrightarrow GL_n(\mathbb{R})$   
 $(U, P) \longmapsto UP$   
est un homéomorphisme.

Preuve: Par définition,  $\Phi$  est la restriction à  $O(n) \times S_n^{++} \subset U(n) \times H_n^{++}$  de l'homéomorphisme donné par la décomposition polaire complexe.

Il s'agit donc d'un homéomorphisme sur son image (pour les topologies induites).

Il faut vérifier que  $\text{Im}(\Phi) = GL_n(\mathbb{R})$ .

L'inclusion  $\text{Im}(\Phi) \subset GL_n(\mathbb{R})$  est immédiate.

L'autre inclusion est une conséquence de l'expression explicite de la décomposition polaire: soit  $A \in GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$ , alors  $P := \sqrt{A^*A}$  et  $U := AP^{-1}$  dans la décomposition polaire complexe. Ici  $A^*A = A^T A \in S_n^{++} = H_n^{++} \cap M_n(\mathbb{R})$  donc  $P \in S_n^{++}$ , et  $U \in U(n) \cap M_n(\mathbb{R}) = O(n)$ . Donc  $A = UP \in \text{Im}(\Phi)$ .  $\square$

Remarque: On pourrait aussi tout montrer en réel sans utiliser le cas complexe, en imitant ce qu'on a fait en complexe. Il faut pour ça:

Théorème (Réduction des matrices symétriques réelles): Soit  $M \in S_n$ . Alors il existe une matrice orthogonale  $P \in O(n)$  et une matrice diagonale réelle  $D$  tq  
 $M = P^{-1}DP = P^T DP$ .

Preuve: en exercice. (imiter une preuve de réduction déjà faite).

## ⑥ Exponentielle de matrices

$$\text{On note } f_k : M_n(\mathbb{C}) \longrightarrow M_n(\mathbb{C})$$
$$A \longmapsto \sum_{j=0}^k \frac{A^j}{j!}$$

Ce sont les sommes partielles d'une série (à valeurs dans  $M_n(\mathbb{C})$ ) de terme général  $\frac{A^j}{j!}$ , dont on note  $\exp(A)$  la somme si elle est convergente.

Proposition: La série converge pour tout  $A \in M_n(\mathbb{C})$ . De plus, en restriction à n'importe quel compact de  $M_n(\mathbb{C})$ , la fonction  $\exp$  ainsi définie est une limite uniforme des  $(f_k)$ .

$$\|AB\| \leq \|A\| \|B\|$$

Première: Fixons une norme sous-multiplicative  $\|\cdot\|$  sur  $M_n(\mathbb{C})$ , par exemple la norme matricielle associée à la norme hermitienne sur  $\mathbb{C}^n$ .

Montrons d'abord que la série converge.

On a, pour tout  $m \leq l \in \mathbb{N}$ ,

$$\textcircled{*} \quad \|f_l(A) - f_{m-1}(A)\| = \left\| \sum_{k=m}^l \frac{A^k}{k!} \right\| \leq \sum_{k=m}^l \left\| \frac{A^k}{k!} \right\| \leq \sum_{k=m}^l \frac{(\|A\|)^k}{k!}$$

↑  
par inégalité triangulaire

↑  
sous-multiplicativité

La série réelle de terme général  $\frac{(\|A\|)^k}{k!}$  converge vers  $\exp(\|A\|)$ , donc la suite de ses sommes partielles est de Cauchy.

Donc l'inégalité  $\textcircled{*}$  montre que la suite des  $f_k(A)$  est de Cauchy dans  $M_n(\mathbb{C})$  (qui est complet) donc converge (vers  $\exp(A)$  par définition).

Pour la convergence uniforme, plaçons nous sur un compact  $K \subset M_n(\mathbb{C})$ . Un tel ensemble est borné. Soit  $M \in \mathbb{R}$  tq  $\|A\| \leq M$  pour tout  $A \in K$ . On a, par passage à la limite ( $l \rightarrow +\infty$ ) dans  $\textcircled{*}$ ,

$$\|\exp(A) - f_{m-1}(A)\| \leq \sum_{k=m}^{+\infty} \frac{\|A\|^k}{k!} \leq \sum_{k=m}^{+\infty} \frac{M^k}{k!} = \left( \exp(M) - \sum_{k=0}^{m-1} \frac{M^k}{k!} \right)$$

Cette inégalité implique la convergence uniforme de  $f_m$  vers  $\exp$  sur  $K$  quand  $m \rightarrow +\infty$ . □

Corollaire: La fonction  $\exp: M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$  est continue.

(Preuve: Une limite uniforme de fonctions continue est continue.

• Les fonctions  $f_k$  sont polynomiales donc continues.

•  $M_n(\mathbb{C}) = \bigcup_{M \in \mathbb{R}_+^+} B_{\| \cdot \|}(0, M)$  réunion de compacts. )

Proposition: Si  $A$  et  $B$  commutent, alors  $\exp(A+B) = \exp(A)\exp(B)$ .

Preuve: On considère le produit de Cauchy des deux séries définissant  $\exp(A)$  et  $\exp(B)$ . La somme partielle est

$$U_m := \left( \sum_{k=0}^m \frac{A^k}{k!} \right) \left( \sum_{p=0}^m \frac{B^p}{p!} \right)$$

$$= \sum_{k,p=0}^m \frac{A^k B^p}{k! p!}$$

La somme partielle de la série définissant  $\exp(A+B)$  est:

$$V_m := \sum_{q=0}^m \frac{(A+B)^q}{q!}$$

$$= \sum_{q=0}^m \sum_{p=0}^q \frac{1}{q!} \binom{q}{p} A^p B^{q-p}$$

$$= \sum_{\substack{k,p=0 \\ k+p \leq m}} \frac{A^k B^p}{k! p!}$$

par binôme de Newton,  
comme  $AB=BA$

$\binom{q}{p} = \frac{q!}{p!(q-p)!}$   
notons  $k=p$   
 $p=q-p$

$$\text{On a } \|U_m - V_m\| = \left\| \sum_{\substack{k,p=0 \\ k+p > m}} \frac{A^k B^p}{k! p!} \right\|$$

$$\leq \sum_{\substack{k,p=0 \\ k+p > m}} \frac{\|A\|^k \|B\|^p}{k! p!}$$

$$\leq u_m - v_m$$

où  $u_m$  est la somme partielle du produit de Cauchy des séries définissant  $\exp(\|A\|)$  et  $\exp(\|B\|)$ ,

$v_m$  ————— de la série définissant  $\exp(\|A\| + \|B\|)$ .

Or  $\exp(\|A\| + \|B\|) = \exp(\|A\|) \exp(\|B\|)$  (et la convergence est absolue) donc  $(u_m - v_m)$  converge vers zéro.

On en déduit que  $\|u_m - v_m\| \xrightarrow{m \rightarrow \infty} 0$ , donc  $\lim_{m \rightarrow \infty} u_m = \lim_{m \rightarrow \infty} v_m = \exp(A+B)$   
 $\parallel$   
 $\exp(A) \exp(B)$  □

Proposition: L'application  $\exp$  est à valeurs dans  $GL_n(\mathbb{C})$ . Plus précisément, pour  $A \in M_n(\mathbb{C})$ ,  $\exp(A)$  est inversible d'inverse  $\exp(-A)$ .

Preuve: On commence par le cas particulier évident: pour  $0 \in M_n(\mathbb{C})$ ,  $f_k(0) = I_n$  pour tout  $k$ , donc  $\exp(0) = I_n$ .

En général,  $A$  et  $-A$  commutent, donc  $\exp(A - A) = \exp(A) \exp(-A)$   
 $\exp(0) = I_n$  □

Proposition: Pour tout  $A \in M_n(\mathbb{C})$ , on a  $\exp(\bar{A}) = \overline{\exp(A)}$ ,  $\exp(A^T) = (\exp(A))^T$ ,  
 $\exp(A^*) = (\exp(A))^*$ .

Preuve: Par exemple pour l'adjoint. Par définition,

$$f_k(A^*) \xrightarrow{k \rightarrow \infty} \exp(A^*)$$

$$\sum_{j=0}^k \frac{(A^*)^j}{j!} \parallel \parallel$$

$$\left( \sum_{j=0}^k \frac{A^j}{j!} \right)^* \xrightarrow{k \rightarrow \infty} (\exp(A))^*$$

car  $M \mapsto M^*$  est continue.  
 (application R-linéaire)

□

Proposition : Soit  $A \in M_n(\mathbb{C})$  et  $P \in GL_n(\mathbb{C})$ . Alors  $\exp(PAP^{-1}) = P \exp(A) P^{-1}$ .

Preuve :

$$\begin{aligned} f_k(PAP^{-1}) &= \sum_{j=0}^k \frac{(PAP^{-1})^j}{j!} = P \left( \sum_{j=0}^k \frac{A^j}{j!} \right) P^{-1} = P f_k(A) P^{-1} \\ &\downarrow \qquad \qquad \qquad \qquad \qquad \qquad \downarrow \text{par définition} \\ \exp(PAP^{-1}) &= \qquad \qquad \qquad \qquad \qquad \qquad P \exp(A) P^{-1} \end{aligned}$$

+  
continuité du  
produit de matrices.

□

## ⑦ Exponentielle et décomposition polaire

Théorème : On a  $\exp(H_n) = H_n^{++}$ .

Preuve : Montrons d'abord que  $\exp(H_n) \subset H_n^{++}$ .

Soit  $A \in H_n$  (c-à-d.  $A^* = A$ ).

On a  $(\exp(A))^* = \exp(A^*) = \exp(A)$  donc  $\exp(A) \in H_n$ .

$$\begin{aligned} \text{Soit } z \in \mathbb{C}^n - \{0\} \quad z^* \exp(A) z &= z^* \exp\left(\frac{A}{2} + \frac{A}{2}\right) z \\ &= z^* \exp\left(\frac{A}{2}\right) \exp\left(\frac{A}{2}\right) z \\ &= z^* \exp\left(\frac{A}{2}\right)^* \exp\left(\frac{A}{2}\right) z \\ &= \left(\exp\left(\frac{A}{2}\right) z\right)^* \left(\exp\left(\frac{A}{2}\right) z\right) \\ &> 0 \quad \text{car } \exp\left(\frac{A}{2}\right) \in GL_n(\mathbb{C}) \\ &\qquad \qquad \qquad \text{donc } \exp\left(\frac{A}{2}\right) z \neq 0 \end{aligned}$$

Donc  $\exp(A) \in H_n^{++}$ .

Il reste à montrer l'autre inclusion.

Soit  $B \in H_n^{++}$ . Par réduction des matrices hermitiennes, on a

$$B = U^* \text{diag}(\lambda_1, \dots, \lambda_n) U \quad \text{avec } U \in U(n), \lambda_j \in \mathbb{R}_+ \forall j.$$

Considérons la matrice  $A := U^* \text{diag}(e_n \lambda_1, \dots, e_n \lambda_n) U$ .

$$\begin{aligned} \text{C'est une matrice hermitienne: } A^* &= (U^* \text{diag}(e_n \lambda_1, \dots, e_n \lambda_n) U)^* \\ &= U^* \text{diag}(e_n \lambda_1, \dots, e_n \lambda_n) U = A. \end{aligned}$$

$$\begin{aligned} \text{Et } \exp(A) &= \exp(U^* \text{diag}(e_n \lambda_1, \dots, e_n \lambda_n) U) \\ &= \exp(U^{-1} \text{diag}(e_n \lambda_1, \dots, e_n \lambda_n) U) \\ &= U^{-1} \exp(\text{diag}(e_n \lambda_1, \dots, e_n \lambda_n)) U \end{aligned}$$

Or l'exponentielle d'une matrice diagonale  $\text{diag}(a_1, \dots, a_n)$  est  $\exp(\text{diag}(a_1, \dots, a_n)) = \text{diag}(\exp(a_1), \dots, \exp(a_n))$ . (exercice)

donc

$$\exp(A) = U^{-1} \text{diag}(\lambda_1, \dots, \lambda_n) U = B.$$

Donc  $H_n^{++} \subset \exp(H_n)$ . □

Plus précisément, on a le théorème suivant (admis, on verra des éléments de preuve en TD):

Théorème: L'application  $\exp: H_n \rightarrow H_n^{++}$  est un homéomorphisme.

Remarque: On a déjà montré que  $\exp$  est continue et  $\exp(H_n) = H_n^{++}$ .

Il reste à montrer que  $\exp|_{H_n}$  est injective, puis que l'inverse " $\exp^{-1}$ ":  $H_n^{++} \rightarrow H_n$  est continu.

Corollaire: Le groupe topologique  $GL_n(\mathbb{C})$  est homéomorphe à  $U(n) \times \mathbb{R}^{n^2}$ .

"Preuve": L'homéo de la décomposition polaire  $\phi: U(n) \times H_n^{++} \rightarrow GL_n(\mathbb{C})$  peut être composé à droite avec l'exponentielle.  $(U, P) \mapsto UP$

$\psi: U(n) \times H_n \rightarrow GL_n(\mathbb{C})$  est un homéomorphisme.

$$(U, M) \mapsto U \exp(M)$$

Et  $H_n$  est un espace vectoriel réel de dimension  $n^2$ . □

Corollaire:  $GL_n(\mathbb{C})$  est connexe par arcs.

Preuve:  $GL_n(\mathbb{C})$  est homéomorphe à  $U(n) \times \mathbb{R}^{n^2}$ ,  $U(n)$  est connexe par arcs et  $\mathbb{R}^{n^2}$  est connexe par arcs.  $\square$

Remarque: Pour  $n=1$ , coordonnées polaires  $z = re^{i\theta}$ .

Le résultat  $\exp(\mathbb{H}_n) = \mathbb{H}_n^{++}$  correspond à  $\exp(\mathbb{R}) = \mathbb{R}_+$ ,

ie. à écrire  $r = \exp(s)$   $s \in \mathbb{R}$ .

$$z = \exp(s)\exp(i\theta)$$

$$s = \ln|z| \text{ bien défini}$$

$\theta$  seulement défini modulo  $2\pi$ . ~~///~~

Théorème: On a  $\exp(\mathbb{A}\mathbb{H}_n) = U(n)$ .

Remarque: Attention ici ce n'est pas un homéomorphisme, ce n'est même pas injectif.

Preuve: • Si  $A \in \mathbb{A}\mathbb{H}_n$ , alors  $(\exp(A))^* = \exp(A^*)$   
 $= \exp(-A)$   
 $= (\exp(A))^{-1}$

donc  $\exp(A) \in U(n)$ .

Donc  $\exp(\mathbb{A}\mathbb{H}_n) \subset U(n)$

• Soit  $B \in U(n)$ . Par réduction des matrices unitaires,  
 $B = U^* \text{diag}(e^{i\theta_1}, \dots, e^{i\theta_n}) U$  avec  $U \in U(n)$ .

Posons  $A := U^* \text{diag}(i\theta_1, \dots, i\theta_n) U$ ,

alors  $A^* = U^* \text{diag}(-i\theta_1, \dots, -i\theta_n) U = -A$  donc  $A \in \mathbb{A}\mathbb{H}_n$

et  $\exp(A) = U^{-1} \exp(\text{diag}(i\theta_1, \dots, i\theta_n)) U$   
 $= U^{-1} \text{diag}(\exp(i\theta_1), \dots, \exp(i\theta_n)) U = B.$   $\square$

Remarque: On a fait cette dernière réduction dans le cas complexe. On peut sous problème l'appliquer dans le cas réel.  $\rightarrow$  à faire en exercice.

On reprends à 10h35 sur le TD du chapitre 3  
on reviendra sur le TD du chapitre 2 jeudi

# Chapitre 4: Représentations linéaires de groupes finis

- Plan:
- 1) Définitions
  - 2) Représentations irréductibles
  - 3) Décomposition en représentations irréductibles
  - 4) Caractères
  - 5) Théorie des caractères: résultats
  - 6) Tables de caractères
  - 7) Théorie des caractères: preuves

## 1) Définitions

$G$  désignera un groupe fini (sauf exceptions explicites)  
 $K$  corps /  $K = \mathbb{C}$  à partir du point 2

Définitions: • Une représentation linéaire de  $G$  à coefficients dans  $K$  est la donnée de:

- i) un  $K$ -espace vectoriel  $V$
- ii) et un morphisme de groupe  $\rho: G \rightarrow GL(V)$ .

On dira en général juste "représentation".

• Deux représentations  $\rho_1: G \rightarrow GL(V_1)$  et  $\rho_2: G \rightarrow GL(V_2)$  sont équivalentes s'il existe un isomorphisme d'e.v.  $\phi: V_1 \xrightarrow{\sim} V_2$  tq  
 $\forall g \in G, \quad \rho_2(g) \circ \phi = \phi \circ \rho_1(g)$  (comme application  $V_1 \rightarrow V_2$ ).

Remarques: \* Le morphisme  $\rho$  donne en particulier une action de  $G$  sur  $V$ .  
\* La donnée d'un morphisme  $\rho: G \rightarrow GL_n(K)$  donne directement une représentation avec  $V = K^n$ .  
\* Réciproquement, si  $V$  est de dimension finie (comme on le supposera toujours dans ce cours), le choix d'une base identifie une représentation



à un morphisme vers  $GL_n(\mathbb{K})$ .

\* Si  $\rho_1$  et  $\rho_2$  sont deux morphismes  $G \rightarrow GL_n(\mathbb{K})$ , les représentations associées sont équivalentes si elles sont conjuguées, c-à-d :

$$\exists h \in GL_n(\mathbb{K}) \quad \forall g \in G, \quad h\rho_1(g)h^{-1} = \rho_2(g).$$

Terminologie: La dimension de  $V$  est appelée le degré de la représentation.

Dans ce cours, on considère uniquement (sauf pour des remarques culturelles)

le cas où :

- $G$  est un groupe fini

- $\mathbb{K} = \mathbb{C}$

- les représentations sont de degré fini.

Exemples:

1. Représentation triviale.

- Pour tout groupe  $G$  et tout espace vectoriel  $V$ , le morphisme trivial  $\rho: G \rightarrow GL(V)$

$$g \mapsto Id_V$$

définit une représentation, appelée représentation triviale sur  $V$ .

- Une représentation est équivalente à la représentation triviale sur  $V_1$  si c'est la représentation triviale sur  $V_2$  avec  $V_2$  isomorphe à  $V_1$ .

- On appelle représentation triviale de degré  $n$  la représentation triviale sur  $\mathbb{C}^n$ .

2.  $G = \mathbb{Z}/2\mathbb{Z}$

$$\rho_1: G \rightarrow GL_2(\mathbb{C})$$

$$\bar{k} \mapsto (-1)^k I_2$$

$$\rho_2: G \rightarrow GL_2(\mathbb{C})$$

$$\bar{k} \mapsto \begin{pmatrix} (-1)^k & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho_3: G \rightarrow GL_2(\mathbb{C})$$

$$\bar{k} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & (-1)^k \end{pmatrix}$$

sont des morphismes, donc définissent des représentations.  $\rho_2$  et  $\rho_3$  sont équivalentes mais pas  $\rho_1$  et  $\rho_2$  ( $-I_2$  n'est pas conjugué à  $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ )

3. Plus généralement, pour  $G = \mathbb{Z}/2\mathbb{Z}$ ,  
représentation  $\Leftrightarrow$  morphisme  $\rho: \mathbb{Z}/2\mathbb{Z} \rightarrow GL_n(\mathbb{C}) \Leftrightarrow$  donnée de  $\rho(\bar{1})$ , matrice  
 $n \times n$  d'ordre 2.

4. Pour  $G = S_n$ , on a déjà vu un morphisme remarquable  $\rho: S_n \rightarrow GL_n(\mathbb{C})$   
donné par l'isomorphisme entre  $S_n$  et le sous-groupe des matrices de permutation.

### 5. Représentations de permutations.

Si  $G$  agit sur un ensemble fini  $\{1, \dots, n\}$ , on peut construire une représentation  
de  $G$  dans  $\mathbb{C}^n$  comme suit:

si  $(e_1, \dots, e_n)$  base standard de  $\mathbb{C}^n$ , on pose  $\rho(g) \left( \sum_{i=1}^n z_i e_i \right) = \sum_{i=1}^n z_i e_{g \cdot i}$ .

( $\rho(g)$  est l'isomorphisme qui envoie la base  $(e_1, \dots, e_n)$  sur la base  $(e_{g \cdot 1}, e_{g \cdot 2}, \dots, e_{g \cdot n})$ )

(se rattache au point 4 en composant le morphisme  $G \rightarrow S_n$  associé  
à l'action de  $G$  sur  $\{1, \dots, n\}$  avec l'isomorphisme entre  $S_n$  et les  
matrices de permutation)

### 6. Représentation régulière

Un groupe fini  $G$  agit sur lui-même par multiplications à gauche.

La représentation de permutation associée (de degré  $\#G$ ) est appelée la  
représentation régulière de  $G$ .

7. Pour  $G = \mathbb{Z}/2\mathbb{Z}$ , la représentation régulière est donnée par  
 $\rho(\bar{1}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

Définition: Soit  $\rho: G \rightarrow GL(V)$  une représentation de  $G$ . Si  $W \subset V$  est un  
sev de  $V$  stable par tous les  $\rho(g)$  pour  $g \in G$  (on dira stable par  $\rho(G)$ ), alors  
on obtient une représentation dans  $W$  par  $\rho|_W: G \rightarrow GL(W)$ .

Les représentations obtenues de cette manière sont appelées sous-représentations de  $\rho$ .

Exemple: Pour la représentation régulière de  $\mathbb{Z}/2\mathbb{Z}$  (donnée par  $\rho(\bar{1}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ) la droite engendrée par  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  est stable par  $\rho(\bar{0}) = I_2$  et  $\rho(\bar{1})$ , donc définit une sous-représentation.

Définition: Soient  $\rho_1: G \rightarrow GL(V_1)$  et  $\rho_2: G \rightarrow GL(V_2)$  deux représentations. La somme directe de  $\rho_1$  et  $\rho_2$  est la représentation définie par le morphisme  $\rho_1 \oplus \rho_2: G \rightarrow GL(V_1 \oplus V_2)$

$$g \mapsto (v_1, v_2) \mapsto (\rho_1(g)(v_1), \rho_2(g)(v_2))$$

- \* De la même manière, on peut le définir pour un nombre arbitraire de représentations.
- \* En pratique, si  $\rho_1: G \rightarrow GL_{n_1}(\mathbb{C})$ ,  $\rho_2: G \rightarrow GL_{n_2}(\mathbb{C})$ , la somme directe est définie par des matrices diagonales par blocs:

$$(\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$$

$\begin{matrix} \downarrow n_1 \\ \uparrow n_2 \end{matrix}$ 
 $\begin{matrix} \leftarrow n_1 & \leftarrow n_2 \end{matrix}$

Exemples: • La représentation de  $\mathbb{Z}/2\mathbb{Z}$  donnée par  $\rho(\bar{1}) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  est la somme directe de  $\rho_1$  et  $\rho_2$  où  $\rho_1(\bar{1}) = -1$  et  $\rho_2(\bar{1}) = 1$ .

• La représentation triviale de degré  $n$  de  $G$  est la somme directe de  $n$  copies de la représentation triviale de degré 1 de  $G$ .

Remarque: • Si  $\rho = \rho_1 \oplus \rho_2$ , alors (à équivalence près)  $\rho_1$  et  $\rho_2$  sont des sous-représentations de  $\rho$ .

But de ce chapitre: comprendre comment décomposer de manière "optimale" une représentation en somme directe de sous-représentations.

## 2) Représentations irréductibles

Définition: Une représentation  $\rho: G \rightarrow GL(V)$  est irréductible si les seuls sev de  $V$  stables par  $\rho(G)$  sont  $\{0\}$  et  $V$ .  
ces deux là sont toujours stables!

Exemple (immédiat mais fondamental): Toute représentation de degré 1 est irréductible. Soit  $\rho: G \rightarrow GL(V)$  de degré 1, c-à-d  $\dim V = 1$ . Les seuls sev de  $V$  sont  $\{0\}$  et  $V$  (par dimension). Donc la condition de la définition est satisfaite.

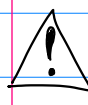
Proposition: Soit  $G$  un groupe fini abélien. Une représentation de  $G$  est irréductible ssi elle est de degré 1.

La preuve repose sur le lemme:

Lemme: Soit  $G$  un groupe fini et  $\rho: G \rightarrow GL_n(\mathbb{C})$  un morphisme. Alors pour tout  $g \in G$ , la matrice  $\rho(g)$  est diagonalisable.

Preuve du lemme: Soit  $g \in G$ , soit  $m$  l'ordre de  $g$ . Comme  $\rho$  est un morphisme,  $\rho(g^m) = (\rho(g))^m = I_n$ , donc le polynôme  $X^m - 1$  annule  $\rho(g)$ . Autrement dit, le polynôme minimal de  $\rho(g)$  divise  $X^m - 1$ . Or  $X^m - 1$  est scindé à racines simples (dans  $\mathbb{C}$ ), donc le polynôme minimal de  $\rho(g)$  aussi.  $\square$

Preuve de la proposition: Soit  $\rho: G \rightarrow GL_n(\mathbb{C})$  une représentation de  $G$ . Par le lemme, toutes les matrices  $\rho(g)$  sont diagonalisables. Comme  $G$  est abélien, ces matrices commutent, donc elles sont simultanément diagonalisables. Il existe une base de  $\mathbb{C}^n$  formée de vecteurs communs à chaque  $\rho(g)$ . Chacune des droites engendrées par un de ces vecteurs propres est stable par  $\rho(G)$ , donc définissent des sous-représentations  $\neq \{0\}, \mathbb{C}^n$  sauf si  $n = 1$ .  $\square$

 Faux sur un corps quelconque!

Par exemple,  $\rho: \mathbb{Z}/3\mathbb{Z} \rightarrow GL_2(\mathbb{R})$  est irréductible comme représentation réelle.  
 $\mathbb{Z}/3\mathbb{Z} \longmapsto R_{\frac{2\pi k}{3}}$

Un résultat fondamental de théorie des représentations:

Lemme de Schur: Soient  $\rho_1: G \rightarrow GL(V_1)$  et  $\rho_2: G \rightarrow GL(V_2)$  deux représentations irréductibles de  $G$ . Soit  $\phi: V_1 \rightarrow V_2$  une application linéaire telle que  $\phi \circ \rho_1(g) = \rho_2(g) \circ \phi \quad \forall g \in G$ .

Alors: 1. Si  $\phi$  n'est pas identiquement nulle, alors  $\phi$  est un isomorphisme.  
2. si de plus  $V_1 = V_2$ , alors il existe  $\lambda \in \mathbb{C}^*$  tq  $\phi = \lambda \text{Id}_{V_1}$ .

Preuve: 1. Le noyau de  $\phi$  est un sev de  $V_1$ , stable par  $\rho_1(G)$  d'après  $\forall$ .

Si  $\phi$  n'est pas identiquement nulle,  $\text{Ker } \phi \neq V_1$ .

$\rho_1$  est irréductible, donc  $\text{Ker } \phi = \{0\}$ . Donc  $\phi$  est injective.

L'image de  $\phi$  est un sev de  $V_2$ , stable par  $\rho_2(G)$  d'après  $\forall$ .

Comme  $\rho_2$  est irréductible,  $\phi(V_1)$  est soit  $\{0\}$ , soit  $V_2$ .

Si  $\phi$  n'est pas identiquement nulle,  $\phi(V_1) \neq \{0\}$ , donc  $\phi(V_1) = V_2$ .

Donc  $\phi$  est surjective.

2. Soit  $\lambda \in \mathbb{C}$ . En appliquant le premier point à l'application  $\phi - \lambda \text{Id}_{V_1}$ ,  
(qui satisfait  $\forall$ ), on a: soit  $\phi - \lambda \text{Id}_{V_1}$  est un isomorphisme,  
soit  $\phi - \lambda \text{Id}_{V_1}$  est identiquement nulle.

Puisque  $\phi$  admet au moins une valeur propre (on travaille sur  $\mathbb{C}$ )  
il existe un  $\lambda \in \mathbb{C}$  tq  $\phi - \lambda \text{Id}_{V_1}$  ne soit pas un isomorphisme.

Donc  $\phi = \lambda \text{Id}_{V_1}$  pour ce  $\lambda$ .

□

### 3) Décomposition en représentations irréductibles.

Théorème: Toute représentation de  $G$  est une somme directe de représentations irréductibles.

(dans le cadre énoncé plus tôt  
 $G$  fini,  $\mathbb{K} = \mathbb{C}$ , représentation de degré fini)

Preuve: Il suffit d'appliquer récursivement le résultat suivant. □

Lemme de Maschke: Soit  $\rho: G \rightarrow GL(W)$  une représentation, et  $V_1$  un sous-espace stable par  $\rho(G)$ ,  $V_1 \neq \{0\}$ ,  $W$ . Alors il existe un seul  $V_2$  de  $W$ ,  $\rho(G)$ -stable, tel que  $W = V_1 \oplus V_2$ , et  $\rho = \rho|_{V_1} \oplus \rho|_{V_2}$ .

Preuve du lemme de Maschke:

Choisissons une base de  $W$  pour identifier  $\rho$  avec un morphisme  $\rho: G \rightarrow GL_n(\mathbb{C})$  (où  $n = \dim W$ ).

Considérons la matrice:  $H := \sum_{g \in G} \rho(g)^* \rho(g)$

C'est un élément de  $H_n^{++}$  (c-à-d c'est une matrice hermitienne définie positive).

En effet, chaque terme de la somme l'est (on a déjà vu ce raisonnement dans la preuve de la déc. polaire) et la somme reste dans  $H_n^{++}$  (car  $H_n^{++}$  est un cône convexe).

L'espace  $W \simeq \mathbb{C}^n$  est donc muni de la forme hermitienne définie positive  $(X, Y) \mapsto X^* H Y$ .

Cette forme est invariante par  $\rho(G)$ :

$$\begin{aligned} \forall h \in G, \forall X, Y \in \mathbb{C}^n, \quad \phi(\rho(h)X, \rho(h)Y) &= (\rho(h)X)^* H (\rho(h)Y) \\ &= \sum_{g \in G} X^* \rho(h)^* \rho(g)^* \rho(g) \rho(h) Y \\ &= \sum_{g \in G} X^* \rho(g)^* \rho(g) Y \quad \begin{array}{l} G \rightarrow G \\ g \mapsto gh \\ \text{bijection} \end{array} \\ &= \sum_{g \in G} X^* \rho(g)^* \rho(g) Y \\ &= X^* H Y = \phi(X, Y). \end{aligned}$$

(en d'autres termes,  $\rho(h)$  est dans le groupe unitaire  $U(\phi)$  de  $\phi$ ).

Donc si  $V_1$  est un sev de  $W$  stable par  $\rho(G)$ , alors son orthogonal par rapport à  $\phi$  est aussi stable par  $\rho(G)$ .

Si on le note  $V_2$ , on a bien  $W = V_1 \oplus V_2$  et  $\rho = \rho|_{V_1} \oplus \rho|_{V_2}$ . □

⚠ Le résultat est faux pour un groupe infini.

Par exemple:  $\rho: \mathbb{Z} \rightarrow GL_2(\mathbb{C})$  définit une représentation de  $\mathbb{Z}$  de degré 2.  
 $k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$

La droite engendrée par  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  est  $\rho(\mathbb{Z})$ -stable, mais n'a pas de supplémentaire  $\rho(\mathbb{Z})$ -stable.

## ④ Caractères

Définition: Soit  $\rho: G \rightarrow GL(V)$  une représentation de  $G$ .

Le caractère de  $\rho$  est la fonction  $\chi_\rho: G \rightarrow \mathbb{C}$   
 $g \mapsto \text{tr}(\rho(g))$

Exemples: 1. Si  $\rho: G \rightarrow GL_1(\mathbb{C}) = \mathbb{C}^*$  représentation de degré 1, alors  $\chi_\rho = \rho$ .

2. Pour la représentation régulière de  $\mathbb{Z}/2\mathbb{Z}$  ( $\rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ), on a  
 $\chi_\rho(\bar{0}) = 2$  et  $\chi_\rho(\tau) = 0$ .

3. L'image de l'élément neutre par  $\chi_\rho$  est toujours égale au degré de la représentation  $\rho$ .

4. Pour une représentation de permutation:

si  $G$  agit sur  $\{1, \dots, n\}$  et  $\rho: G \rightarrow GL_n(\mathbb{C})$  est la représentation de permutation associée, on a:  $\chi_\rho(g) =$  nombre de points fixes par  $g$  dans  $\{1, \dots, n\}$

(rappel  $\rho(g)(e_i) = e_{g \cdot i}$ )

5. En particulier, pour la représentation régulière de  $G$  (associée à l'action de  $G$  sur lui-même par multiplication à gauche), on a  $\chi_\rho(g) = 0$  pour  $g \neq e$ ,  
et  $\chi_\rho(e) = \#G$ .

Propriété: Soit  $\rho$  une représentation et  $\chi_\rho$  son caractère. La fonction  $\chi_\rho: G \rightarrow \mathbb{C}$  est invariante par conjugaison:  $\forall g, h \in G, \chi_\rho(ghg^{-1}) = \chi_\rho(h)$ .

(c'est une conséquence immédiate de l'invariance de la trace par conjugaison).

Conséquence: Deux représentations équivalentes ont le même caractère.

Terminologie: On appelle fonctions centrales les fonctions  $G \rightarrow \mathbb{C}$  qui sont invariante par conjugaison.

Remarque: Si on connaît les classes de conjugaison de  $G$ , alors pour déterminer complètement  $\chi_\rho$ , il suffit de le calculer sur un représentant de chaque classe.

Proposition: Soient  $\rho_1: G \rightarrow GL_{n_1}(\mathbb{C})$  et  $\rho_2: G \rightarrow GL_{n_2}(\mathbb{C})$  deux représentations, alors  $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$ .

Preuve directe en exercice.

## 5) Théorie des caractères: résultats

Buts:  $\rightarrow$  montrer que le caractère d'une représentation la détermine complètement à équivalence près.  
 $\rightarrow$  la décomposition en représentations irréductibles se détermine "facilement" à l'aide des caractères.

On munit l'espace vectoriel complexe des fonctions de  $G$  dans  $\mathbb{C}$  de la forme hermitienne définie positive:

$$(f | f') := \frac{1}{\#G} \sum_{g \in G} f(g) \overline{f'(g)}$$

pour  $f: G \rightarrow \mathbb{C}$   
 $f': G \rightarrow \mathbb{C}$

(Exercice: vérifier que c'est bien une forme hermitienne définie positive.)

## Résultats principaux de la théorie des caractères

### A - Sur les représentations irréductibles

Théorème: Soient  $\rho$  et  $\pi$  deux représentations irréductibles de  $G$ .

1. Si  $\rho$  n'est pas équivalente à  $\pi$ , alors  $(\chi_\rho | \chi_\pi) = 0$

2. Si  $\rho$  est équivalente à  $\pi$ , alors  $(\chi_\rho = \chi_\pi \text{ et }) (\chi_\rho | \chi_\rho) = 1$ .



## B - Sur la décomposition en représentations irréductibles

Soit  $\rho: G \rightarrow GL(V)$  une représentation.

D'après la section 3, il existe des sous-espaces  $V_1, \dots, V_m$  de  $V$ , stables par  $\rho(G)$ , tels que  $\rho = \rho|_{V_1} \oplus \dots \oplus \rho|_{V_m}$  et chaque  $\rho|_{V_i}$  est irréductible.

Soient  $\rho_1, \dots, \rho_k$  des représentations irréductibles de  $G$ , non équivalentes deux à deux, telles que chaque  $\rho|_{V_i}$  (pour  $1 \leq i \leq m$ ) est équivalente à l'une des  $\rho_j$  (pour  $1 \leq j \leq k$ ).

On note  $a_j$  le nombre de  $i$  tels que  $\rho|_{V_i}$  soit équivalente à  $\rho_j$ .

On a donc  $\rho \sim \underbrace{\rho_1 \oplus \dots \oplus \rho_1}_{a_1 \text{ fois}} \oplus \underbrace{\rho_2 \oplus \dots \oplus \rho_2}_{a_2} \oplus \dots \oplus \rho_k$

on écrit  $\rho \sim \rho_1^{\oplus a_1} \oplus \rho_2^{\oplus a_2} \oplus \dots \oplus \rho_k^{\oplus a_k}$  et on appelle  $a_j$  la

multiplicité de  $\rho_j$  dans  $\rho$ .

Théorème: 1. Pour tout  $j$ ,  $a_j = (\chi_\rho | \chi_{\rho_j})$ .

| En particulier, si deux représentations ont même caractère, alors elles sont équivalentes.

2. On a  $(\chi_\rho | \chi_\rho) = \sum_{j=1}^k a_j^2$ .

| En particulier,  $\rho$  est irréductible si et seulement si  $(\chi_\rho | \chi_\rho) = 1$ .

## C - Sur la représentabilité régulière

Théorème: Toute classe d'équivalence de représentations irréductibles de  $G$  a un représentant  $\rho_j$  qui apparaît comme sous-représentation de la représentation régulière  $\pi$  de  $G$ .  
De plus  $(\chi_\pi | \chi_{\rho_j})$  est égal au degré de  $\rho_j$ .

En particulier, l'ordre de  $G$  est égal à la somme des degrés au carré des (classes d'équivalence de) représentations irréductibles de  $G$ .

Corollaire: Tout groupe fini a un nombre fini de représentations irréductibles à équivalence près.

## D - Nombre de représentations irréductibles

Théorème: Il y a autant de classes d'équivalence de représentations irréductibles de  $G$  que de classes de conjugaison dans  $G$ .

↳ on ne le prouvera pas, preuve détaillée par étapes dans le dernier exo de TD.

## 6) Table des caractères

Étant donné les résultats de la théorie des caractères, on peut résumer toute l'information sur les représentations de  $G$  dans un tableau appelé table des caractères:

- les lignes sont indexées par les caractères des représentations irréductibles de  $G$ .
- les colonnes sont indexées par les classes de conjugaison de  $G$   
(on inclut en général dans l'en-tête de la colonne le cardinal  $\#C$  de la classe de conjugaison)

→ Dans la case à la ligne indexée par le caractère  $\chi$   
et à la colonne indexée par la classe de conjugaison  $\mathcal{C}$ ,

on place le nombre complexe  $\chi(x)$  pour  $x \in \mathcal{C}$  (c'est indépendant  
du choix de  $x \in \mathcal{C}$   
par invariance par  
conjugaison)

⚠ En général, c'est très difficile à remplir.

Il faudrait en principe déterminer toutes les classes de conjugaison et toutes les  
représentations irréductibles et tous leurs caractères.

Par contre, il y a certaines propriétés qui aident. On y reviendra en TD.

Par convention: • on met toujours le caractère  $\mathbb{1}$  de la représentation triviale  
de degré 1 sur la 1<sup>ère</sup> ligne. Donc tous les coeffs de la 1<sup>ère</sup> ligne sont égaux à 1.  
• la première colonne correspond à la classe de conjugaison  $\{e\}$  de l'élément  
neutre  $e$ . Donc les coeffs de la première colonne sont les degrés  
des représentations irréductibles.

## 7) Théorie des caractères : preuves

Lemme 1: Soit  $\rho: G \rightarrow GL(V)$  une représentation, et  $\chi_\rho$  son caractère.

Soit  $\mathbb{1}: G \rightarrow \mathbb{C}$  la fonction constante égale à 1 (caractère de la représentation triviale de degré 1). Alors

$$(\chi_\rho | \mathbb{1}) = \dim(V^G)$$

où  $V^G$  est le sev de  $V$  formé des vecteurs invariants par  $\rho$ .

$$(v \in V^G \Leftrightarrow \forall g \in G, \rho(g)v = v)$$

Preuve: Soit  $P: V \rightarrow V$  l'endomorphisme de  $V$  défini par  $P := \frac{1}{\#G} \sum_{g \in G} \rho(g)$ .

$$\text{On a } (\chi_\rho | \mathbb{1}) = \frac{1}{\#G} \sum_{g \in G} \chi_\rho(g) \mathbb{1}(g) = \frac{1}{\#G} \sum_{g \in G} \text{tr}(\rho(g)) = \text{tr}(P).$$

L'endomorphisme  $P$  satisfait  $P \cdot P = P$ :

$$\begin{aligned} P \cdot P &= \frac{1}{\#G} \sum_{g \in G} \rho(g) \frac{1}{\#G} \sum_{h \in G} \rho(h) && \left. \begin{array}{l} \rho(g)\rho(h) = \rho(gh) \\ \downarrow \\ G \rightarrow G \\ h \mapsto gh \text{ bijection} \end{array} \right\} \\ &= \frac{1}{\#G} \sum_{g \in G} \frac{1}{\#G} \sum_{h \in G} \rho(gh) \\ &= \frac{1}{\#G} \sum_{g \in G} \frac{1}{\#G} \sum_{k \in G} \rho(k) \\ &= \frac{1}{\#G} \sum_{g \in G} P = P \end{aligned}$$

Il s'agit donc d'un projecteur:  $V = \text{Ker}(P) \oplus \text{Im}(P)$  et  $P(x+y) = y$  si  $x \in \text{Ker}(P)$  et  $y \in \text{Im}(P)$ .

La trace d'un projecteur est égale à la dimension de son image.

Il reste à montrer que  $\text{Im}(P) = V^G$ .

$$y \in V^G \Leftrightarrow \rho(g)y = y \quad \forall g$$

Première inclusion: si  $y \in V^G$ , on a  $P(y) = \frac{1}{\#G} \sum_{g \in G} \rho(g)y = y$  donc  $y \in \text{Im}(P)$ .

Deuxième inclusion: si  $y \in \text{Im}(P)$ , soit  $\tilde{y} \in V$  tq  $P(\tilde{y}) = y$ . Alors  $\forall h \in G$ , on a

$$\rho^{(h)}(y) = \rho^{(h)}(P(\tilde{y})) = \frac{1}{\#G} \sum_{g \in G} \rho^{(hg)}(\tilde{y}) = P(\tilde{y}) = y$$

□

↳ montre les résultats sur le produit scalaire hermitien de caractères avec 11.

Comment s'y ramener?

Soient  $V$  et  $W$  deux  $\mathbb{C}$ -ev (de dim finie). On note  $L(V, W)$  le  $\mathbb{C}$ -ev formé des applications linéaires de  $V$  dans  $W$ .

Définition: Étant données deux représentations  $\rho: G \rightarrow GL(V)$  et  $\pi: G \rightarrow GL(W)$ , on définit une représentation  $L(\rho, \pi): G \rightarrow GL(L(V, W))$  en posant

$$\text{pour } g \in G, \quad L(\rho, \pi)(g): L(V, W) \rightarrow L(V, W) \quad \textcircled{*}$$

$$\phi \mapsto \pi(g) \circ \phi \circ \rho(g^{-1})$$

Lemme 2: Le caractère de  $L(\rho, \pi)$  est donné par  $\chi_{L(\rho, \pi)}(g) = \chi_{\rho}(g^{-1}) \chi_{\pi}(g)$ .

Preuve: Il s'agit d'un calcul de trace. (de l'endomorphisme  $\textcircled{*}$ )

Pour cela, on va fixer une base de  $L(V, W)$ .

D'abord, soit  $(e_1, \dots, e_n)$  une base de  $V$  et soit  $(f_1, \dots, f_m)$  une base de  $W$ .

Ceci permet de penser à  $L(V, W)$  comme l'espace vectoriel des matrices  $n \times m$ .

On note  $(E_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$  les matrices élémentaires correspondantes:

$$E_{ij}: V \rightarrow W$$

$$\sum_{k=1}^n z_k e_k \mapsto z_i f_j$$

Elles forment une base de  $L(V, W)$ .

Pour  $g \in G$ ,  $\chi_{L(\rho, \pi)}(g)$  est la trace de l'application  $L(V, W) \rightarrow L(V, W)$ ,  
 $\phi \mapsto \pi(g) \circ \phi \circ \rho(g^{-1})$

donc la somme pour tout  $(i, j) \in \{1, \dots, n\} \times \{1, \dots, m\}$  des coefficients de  $E_{ij}$  dans  $L(\rho, \pi)(g)(E_{ij})$   
 $= \pi(g) \circ E_{ij} \circ \rho(g^{-1})$ .

Notons  $(\rho(g^{-1}))_{k,p}$  les coeffs de  $\rho(g^{-1}) \in GL(V)$  dans la base  $(e_1, \dots, e_n)$

$(\pi(g))_{k,p}$  les coeffs de  $\pi(g) \in GL(W)$  dans la base  $(f_1, \dots, f_m)$

On a :

$$\begin{aligned}(\pi(g) \circ E_{ij} \circ \rho(g^{-1}))(e_i) &= (\pi(g) \circ E_{ij}) \left( \sum_{p=1}^m (\rho(g^{-1}))_{p,i} e_p \right) \\ &= (\pi(g)) \left( (\rho(g^{-1}))_{i,i} f_j \right) \\ &= (\rho(g^{-1}))_{i,i} \sum_{k=1}^m (\pi(g))_{k,j} f_k\end{aligned}$$

Donc le coeff de  $E_{ij}$  dans  $\pi(g) \circ E_{ij} \circ \rho(g^{-1})$  est égal à  $(\rho(g^{-1}))_{i,i} (\pi(g))_{i,i}$ .

$$\begin{aligned}\text{On a, pour conclure, } \chi_{\rho, \pi}(g) &= \sum_{i=1}^n \sum_{j=1}^m (\rho(g^{-1}))_{i,i} (\pi(g))_{i,i} \\ &= \left( \sum_{i=1}^n (\rho(g^{-1}))_{i,i} \right) \left( \sum_{j=1}^m (\pi(g))_{i,i} \right) \\ &= \text{tr}(\rho(g^{-1})) \text{tr}(\pi(g)) \\ &= \chi_{\rho}(g^{-1}) \chi_{\pi}(g).\end{aligned}$$

□

Lemme 3 (propriété à connaître des caractères) : Soit  $\rho$  une représentation,  $\chi_{\rho}$  son caractère. Alors  $\forall g \in G$ ,  $\chi_{\rho}(g^{-1}) = \overline{\chi_{\rho}(g)}$ .

Preuve : Soit  $g \in G$ . Notons  $\lambda_1, \dots, \lambda_n$  les valeurs propres de  $\rho(g)$  (répétées selon leurs multiplicités). Alors  $\chi_{\rho}(g) = \text{tr}(\rho(g)) = \lambda_1 + \dots + \lambda_n$

$$\text{et } \chi_{\rho}(g^{-1}) = \text{tr}(\rho(g^{-1})) = \frac{1}{\lambda_1} + \dots + \frac{1}{\lambda_n}$$

Les valeurs propres de  $\rho(g)$  sont de module 1 :

on a déjà vu (pour les repr. irréd. de groupes abéliens finis) : si  $g$  est d'ordre  $m$  (fini car  $G$  est un groupe fini), alors le polynôme minimal de  $\rho(g)$  divise  $X^m - 1$ , dont les racines sont les racines  $m$ -ièmes de l'unité, toutes de module 1.

Pour un nb complexe  $\lambda$  de module 1,  $\frac{1}{\lambda} = \bar{\lambda}$ .

$$\text{Donc } \chi_{\rho}(g^{-1}) = \frac{1}{\lambda_1} + \dots + \frac{1}{\lambda_n} = \bar{\lambda}_1 + \dots + \bar{\lambda}_n = \overline{\chi_{\rho}(g)}.$$

□

### Preuve des résultats principaux:

Théorème A: Soient  $\rho$  et  $\pi$  deux représentations irréductibles, alors

$$(\chi_{\pi} | \chi_{\rho}) = \begin{cases} 0 & \text{si } \rho \text{ et } \pi \text{ ne sont pas équivalentes} \\ 1 & \text{si } \rho \text{ et } \pi \text{ sont équivalentes.} \end{cases}$$

Preuve: Par définition de (1.1),

$$(\chi_{\pi} | \chi_{\rho}) = \frac{1}{\#G} \sum_{g \in G} \chi_{\pi}(g) \overline{\chi_{\rho}(g)}$$

$$\begin{aligned} \rho: G &\rightarrow GL(V) \\ \pi: G &\rightarrow GL(W) \end{aligned}$$

$$= \frac{1}{\#G} \sum_{g \in G} \chi_{\pi}(g) \chi_{\rho}(g^{-1})$$

$$= \frac{1}{\#G} \sum_{g \in G} \chi_{L(\rho, \pi)}(g)$$

$$= (\chi_{L(\rho, \pi)} | 1)$$

$$= \dim (L(V, W)^G)$$

$$= \begin{cases} 0 & \text{si } \rho \text{ n'est pas équivalente à } \pi \\ 1 & \text{si } \rho \sim \pi \end{cases}$$

□

Théorème B: Si  $\rho \sim \rho_1^{\oplus a_1} \oplus \dots \oplus \rho_k^{\oplus a_k}$  avec  $\rho_1, \dots, \rho_k$  rep. irred. deux à deux non équivalentes

alors  $\forall i$ ,

$$a_i = (\chi_{\rho} | \chi_{\rho_i}).$$

Preuve: Il suffit d'appliquer le thm A en développant:

$$(\chi_{\rho} | \chi_{\rho_i}) = \left( \sum_{j=1}^k a_j \chi_{\rho_j} \mid \chi_{\rho_i} \right) = \sum_{j=1}^k a_j \underbrace{(\chi_{\rho_j} | \chi_{\rho_i})}_{\delta_{ij}} = a_i$$

□

Théorème C: Soit  $\chi$  la représentation régulière, et  $\rho$  une représentation irréductible, on a  $(\chi_\pi | \chi_\rho) = \deg(\rho)$ .

Preuve: On a déjà calculé  $\chi_\chi$ :  $\chi_\chi(\text{id}) = \#G$  et  $\chi_\chi(g) = 0$  pour  $g \neq \text{id}$ .

Pour toute représentation  $\pi$  de  $G$ , on a:

$$\begin{aligned} (\chi_\chi | \chi_\pi) &= \frac{\chi_\chi(\text{id}) \chi_\pi(\text{id})}{\#G} \\ &= \overline{\chi_\pi(\text{id})} \\ &= \overline{\deg(\pi)} \\ &= \deg(\pi) \end{aligned}$$

□

Exercice: Appliquez intelligemment les résultats ci-dessus pour retrouver tous les énoncés de la semaine dernière.

Pour la partie D, la preuve est détaillée par étapes dans la feuille de TD.

/// fin du cours.

On reprend à 9h 35, exercices 6, 7, 8 du TD.