# Théorie des groupes, théorie des algèbres linéaires
# Classe sino-française, USTC

Prof. Marc ROSSO

Polycopé par ZHANG Shengjun et PANG Yihao

Septembre 2020-Novembre 2021

**Résumé**

C'est le cours d'algèbre pour la classe sino-français de deuxième année donné par Prof. Rosso. Les sujets incluent principalement le théorie des groupes et les algèbres linéaires et l'algèbre tensoriel.

# Table des matières

# Première partie

# Groupes

## 1 Généralité sur les groupes

**Définition 1.1.** (sous-groupe distingués ou normaux)

Soient $G$ un groupe et $H \subset G$ son sous-groupe, $H$ est dit distingué ou normal si,

$$\forall g \in G,\ gHg^{-1} = H$$

on note $H \lhd G$

**Théorème 1.2.** *Soient $H, G$ deux groupes et $H \lhd G$, alors il existe une unique structure de groupe sur $G/H$, telle que*

$$\begin{aligned} \pi : G &\to G/H \\ g &\mapsto gH \end{aligned}$$

*soit un morphisme du groupe.*

*Démonstration.* Pour $g, g' \in G$, il suffit de définir

$$gHg'H = gg'H$$

pour que $\pi$ soit un morphisme du groupe.

On doit tout d'abord vérifier que $G/H$ est un group avec cette multiplication. Il reste à voir que cette multiplication est bien définie, c'est-à-dire que pour $g_1, g_1' \in G$, si $gH = g_1H$ et $g' = g_1'H$, alors

$$gg'H = g_1g_1'H$$

en effet, par hypothèses, $\exists h, h' \in H$, tels que

$$\begin{aligned} g_1 &= gh \\ g_1' &= g'h' \end{aligned}$$

alors, on a

$$g_1 g_1' H = ghg'h'H$$

puisque $H \lhd G$, $\exists h'' \in H$, tel que

$$g'^{-1} h g' = h''$$

alors, on a

$$\begin{aligned} g_1 g_1' H &= ghg'h'H \\ &= gg'h''h'H \\ &= gg'H \end{aligned}$$

donc, $G/H$ est bien un groupe avec cette multiplication.

Avec cette structure de groupe, il est facile de voir que $\pi$ est un morphisme du groupe, c'est-à-dire,

$$\pi(gg') = \pi(g)\pi(g')$$

$\square$

**Théorème 1.3.** *(Thérorème de factorisation)*

*Soient $G, H, L$ trois groupes et $H \lhd G$, soit $f : G \to L$ un morphisme du groupe. Alors, $\exists \bar{f}$ morphisme $G/H \to L$, tel que $f = \bar{f} \circ \pi$ si et seulement si $H \subset \ker f$. Et on a un diagramme*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & L \\ G/H \arrow[ur, dotted, "\bar{f}"'] & \end{tikzcd}$$

*Démonstration.* Si $\bar{f}$ morphisme $G/H \to L$, tel que

$$f = \bar{f} \circ \pi$$

alors pour $\forall h \in H$,

$$\begin{aligned} f(h) &= \bar{f}(\pi(h)) \\ &= \bar{f}(1_{G/H}) \\ &= 1_L \end{aligned}$$

donc, $H \subset \ker f$.

Si $H \subset \ker f$, pour $g \in G$, on définit $\bar{f}$ :

$$\bar{f}(gH) = f(g)$$

puisque $H \subset \ker f$, $\bar{f}$ est bien définie, en effet, pour $g, g' \in G$, tels que

$$gH = g'H'$$

$\exists h \in H$, tel que

$$g' = gh$$

alors,

$$\begin{aligned}
\bar{f}(g'H) &= f(g') \\
&= f(gh) \\
&= f(g)f(h) \\
&= f(g) \\
&= \bar{f}(gH)
\end{aligned}$$

donc $\bar{f}$ est bien définie.

Il est facile de vérifier que $\bar{f}$ est bien un morphisme avec la structure de groupe sur $G/H$ que l'on vient de définir, c'est-à-dire,

$$\begin{aligned}
\bar{f}(gHg'H) &= \bar{f}(gg'H) \\
&= f(gg') \\
&= f(g)f(g') \\
&= \bar{f}(gH)\bar{f}(g'H)
\end{aligned}$$

$\square$

**Théorème 1.4.** *(Sous-groupe de $G/H$)*

*Soient $G, H$ deux groupes et $H \lhd G$, alors il y a une correspondance bijective entre les sous-groupes de $G/H$ et les sous-groupes de $G$ contenant $H$.*

*Démonstration.* Soit $\pi$ un endomorphisme du groupe comme ci-dessous :

$$\pi : G \to G/H$$
$$g \mapsto gH$$

Si $K \subset G/H$ est un sous-groupe, comme $\pi$ est un morphisme, alors,

$$\pi^{-1}(K) = \{g \in G | \pi(g) \in K\}$$

est un sous-groupe de $G$ contenant $H$. Car si $h \in H$, $\pi(h) = H$ est le neutre de $G/H$. Ensuite, on a

$$\pi(\pi^{-1}(K)) = K$$

Si $H \subset L \subset H$, $L$ un sous-groupes de $G$, comme $H \lhd G$, par définition on sait que $H \lhd L$, alors,

$$\pi(L) = L/H \subset G/H$$

c'est-à-dire $\pi(L) \subset G/H$ est un sous-groupe de $G/H$. $\square$

*Remarque.* Si $M \subset G$ est un sous-groupe, alors $\pi(M)$ est un sous-groupe de $G/H$ même si $M$ ne contient pas $H$. $\pi^{-1}(\pi(M)$ est le sous-groupes de $G$ engendré par $M$ et $H$ et comme $H \lhd G$, c'est $HM = MH$, ainsi,

$$\pi(M) = MH/H$$

**Théorème 1.5.** *Soit $G, H, M$ trois groupes et $H \lhd G$, $M < G$. Alors, $H \cap M \lhd M$ et on a un isomorphisme de groupes :*

$$M/H \cap M \simeq MH/H$$

*Démonstration.* Il est clair que $H \cap M \lhd M$ par définition.

Pour le reste, soit $\pi$ un endomorphisme du groupe comme ci-dessous :

$$\pi : G \to G/H$$
$$g \mapsto gH$$

et on le restreint à $M$ : $\pi_1 : M \to \pi(M)$. $\pi_1$ est surjectif, de noyeau $M \cap H$ et par théorème de factorisation, on a

$$M/M \cap H \simeq \pi(M) = MH/H$$

$\square$

**Exemple 1.6.** (Conséquence)

Soit $m \in \mathbb{N}^*$, les sous-groupes de $\mathbb{Z}/m\mathbb{Z}$ sont en correspondence bijectif avec les sous-groupes de $\mathbb{Z}$ contenant $m\mathbb{Z}$, i.e. avec les $k\mathbb{Z} \supset n\mathbb{Z}$, i.e. $k|n$.

Posons $n = kd$, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$,

$$k\mathbb{Z}/n\mathbb{Z} = k\mathbb{Z}/dk\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$$

i.e. $\forall d|n$, $\exists!$ sous-groupe d'ordre $d$.

*Remarque.* Soit $G, H, K$ trois groupes et $H \lhd G$, $K \lhd H$, en général, on n'a pas que $K \lhd G$.

**Exemple 1.7.** Soient $A_4$ le groupe alterné d'ordre 4 et

$$V_4 = \{(12)(34), (13)(24), (14)(23), \mathrm{Id}\}$$

alors $V_4 \lhd A_4$ et on a

$$V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

est abélien.

Soit $a = (12)(34)$, alors $a^2 = \mathrm{Id}$, et

$$K :< a >\simeq \mathbb{Z}/2\mathbb{Z}$$

alors,

$$< a > \lhd V_4 \lhd A_4$$

mais on n'a pas que $< a > \lhd A_4$.

*Remarque.* Soient $G, H, K$ trois groupes et $H < G$, $K \lhd G$, $K \subset H$ (donc $K \lhd H$). On dispose $G/K \supset H/K$. Dans la correspondance bijective sur les sous-groupe, les groupes distingués se correspondent, ici,

$$H \lhd G \Rightarrow H/K \lhd G/K$$

**Théorème 1.8.** *Soient $G, H, K$ trois groupes et $H \lhd G$, $K \lhd G$, $K \subset H$ (donc $K \lhd H$), alors,*

$$(G/K)/(H/K) \simeq G/H$$

*Démonstration.* soient $\pi_1$ un endomorphisme du groupe :

$$\begin{aligned}\pi_1 : G &\to G/K \\ g &\mapsto gK\end{aligned}$$

et $\pi_2$ un endomorphisme du groupe :

$$\begin{aligned}\pi_2 : G/K &\to (G/K)/(H/K) \\ gK &\mapsto (gK)H/K\end{aligned}$$

posons $f = \pi_2 \circ \pi_1$, alors $f$ est un morphisme du groupe surjectif et

$$\ker f = \{g \in G | \pi_1(g) \in H/K\} = H$$

alors, par le théorème de factorisation, on a

$$(G/K)/(H/K) \simeq G/H$$

$\square$

# 2 Action d'un groupe sur un ensemble

**Définition 2.1.** Soient $G$ un groupe et $X$ un ensemble, on dit que $G$ agit sur $X$ si on a un morphise

$$\varphi : G \to \sigma(X)$$

des bijections de $X$.

Alors, on a

$$\forall g \in G,\ \varphi(g) : X \to X$$

on note $g \in G$, $x \in X$,

$$\varphi(g)(x) = g \cdot x$$

Ainsi, on a

$$e \cdot x = x$$

et pour $\forall g_1, g_2 \in G$,

$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$$

**Définition 2.2.** $\forall x \in X$, on note le stabilisateur de $x$,

$$\mathrm{stab}(x) = \{g \in G | g \cdot x = x\}$$

qui est un sous-groupe de $G$.

**Définition 2.3.** $\forall x \in X$, on note l'orbite de $x$,

$$\mathcal{O}(x) = \{g \cdot x | g \in G\}$$

qui est un sous-ensemble de $X$.

**Exemple 2.4.** (1)($G$ agit sur lui-même par translations à gauche), pour $\forall g \in G$,

$$\begin{aligned} \varphi(G) : & G \to G \\ & h \mapsto gh \end{aligned}$$

Ainsi, $\varphi : G \to \sigma(G)$ et

$$\ker \varphi = \{g \in G | \forall h \in G,\ gh = h\} = \{e\}$$

alors $\varphi$ est injective.

*Remarque.* (Théorème de cayley)

Soit $G$ un groupe fini de cardinal $n$, alors $G$ est isomorphe à un sous-groupe du groupe symétrique $\sigma_n$.

En effet, dans exemple (1), on a que

$$\sigma(G) \simeq \sigma_n$$

(2)($G$ agit sur lui-même par conjuaison)

$\forall g \in G$,

$$\begin{aligned} \psi(G) : & G \to G \\ & h \mapsto ghg^{-1} \end{aligned}$$

(3) Soit $K$ un corps, alors $\mathrm{GL}_n(K)$ agit par comjugaison sur $\mathrm{M}_n(K)$, les orbites est les classes de similitude des matrices.

(4) Soit $K$ un corps, $\mathrm{GL}_n(K)\times\mathrm{GL}_n(K)$ agit dans $\mathrm{M}_n(K)$ : $\forall g_1, g_2 \in \mathrm{GL}_n(K)$, $m \in \mathrm{M}_n(K)$,

$$(g_1 g_2) \cdot m = g_1 m g_2^{-1}$$

*Remarque.* Deux matrices sont dites équivalentes si elles sont dans la même orbite.

**Théorème 2.5.** *Deux matrices sont dites équivalentes si elles ont même rang.*

**Définition 2.6.** (Action transitive)

On dit que l'action ci-dessus est transitive, s'il y a une seule orbite, i.e.

$$\forall x, y \in X,\ \exists g \in G,\ y = g \cdot x$$

*Remarque.* Les actions transitives se décrivent à partir d'espaces quotients $G/H$.

Autre example d'action :

Soient $G$ un groupes et $H \subset G$ son sous-groupe, alors, $G$ agit sur $G/H$

$$\begin{aligned} \varphi : G & \to \sigma(G/H) \\ g & \mapsto \varphi(g)\ (\varphi(g)(xH) = gxH) \end{aligned}$$

est une translation à gauche.

**Proposition 2.7.** *Soit $G$ agissant sur $X$, $\forall x \in X$, il y a une bijection*

$$\begin{aligned} f \,:\, G/stab(x) &\to \mathcal{O}(x) \\ g \cdot stab(x) &\mapsto g \cdot x \end{aligned}$$

*telle que les actions de $G$ sur $G/stab(x)$ et $\mathcal{O}(x)$ se correspondent, i.e., pour $g_1, g \in G$, $x \in X$,*

$$f(g_1 \cdot gstab(x)) = g_1 f(gstab(x))$$

*En particulier, si l'action est transitive, il y a une bijection compatible avec les actions de $G$ entre $G/stab(x)$ et $X$, où $x \in X$ quelconque.*

*Remarque.* Si $x$ et $y$ sont dans la même orbite, $\mathrm{stab}(x)$ et $\mathrm{stab}(y)$ sont des sous-groupes conjugués de $G$, i.e. si $y = gx$, alors,

$$\mathrm{stab}(y) = g\mathrm{stab}(x)g^{-1}$$

En effet, si $h \in \mathrm{stab}(x)$, i.e. $h \cdot x = x$, alors,

$$\begin{aligned} ghg^{-1} \cdot y &= gh \cdot (g^{-1}gx) \\ &= ghg^{-1} \cdot gx \\ &= gh \cdot x \\ &= g \cdot hx \\ &= gx \\ &= y \end{aligned}$$

alors, $ghg^{-1} \in \mathrm{stab}(y)$.

De même, on peut déduire que si $h \in \mathrm{stab}(x)$, alors $g^{-1}hg \in \mathrm{stab}(y)$.

**Corollaire 2.8.** *Si $G$ est un groupe fini et que $X$ soit fini et que $G$ agisse sur $X$, alors, le cardinal de toute orbite divise le cardinal de $G$.*

*Démonstration.* En effet, on a

$$\mathcal{O}(x) \simeq G/\mathrm{stab}(x)$$

alors, on a

$$|\mathcal{O}(x)| = \frac{|G|}{|\mathrm{stab}(x)|}$$

qui divise le cardinal de $G$. $\square$

**Théorème 2.9.** *(Équations aux classes)*

*Soit $G$ un groupe fini agissant sur $X$ qui est un ensemble fini, les orbites forment une partition de $X$.*

*En effet, il y a une relation d'équivalence sur $X$ donnée par :*

$$\begin{aligned} x \sim y &\Leftrightarrow \mathcal{O}(x) = \mathcal{O}(y) \\ &\Leftrightarrow \exists g \in G, y = gx \end{aligned}$$

*Soient $(O_i)_{i\in I}$ les orbites distinctes et pour $i \in I$, $x_i$ un élément choisi de manière arbitaire dans $O_i$, alors*

$$\begin{aligned} |X| &= \sum_{i\in I} |O_i| \\ &= \sum_{i\in I} \frac{|G|}{|stab(x_i)|} \end{aligned}$$

**Définition 2.10.** ($p$-groupe)

Soit $p$ premier, $G$ est un $p$-groupe, si $|G|$ est une puissance de $p$, i.e. $\exists n \in \mathbb{N}$, tel que

$$|G| = p^n$$

Notation : Si $G$ agit sur $X$,

$$\begin{aligned} X^G &= \{\text{points fixes}\} \\ &= \{x \in X | \forall g \in G, g \cdot x = x\} \\ &= \{x \in X |\ |\mathcal{O}(x)| = 1\} \end{aligned}$$

**Proposition 2.11.** *Soit $G$ un $p$-group agissant sur l'ensemble fini $X$, alors,*

$$|X| \equiv |X^G| \mod p$$

*Démonstration.* Soient $(O_i)_{i\in I}$ les orbites distinctes et pour $i \in I$, on choisit un élément $x_i$ dans $O_i$. L'équation aux classes donne

$$X = X^G \cup \Big( \bigcup_{i\geq 2} O_i \Big)$$

or, on a

$$|O_i| = \frac{|G|}{|\text{stab}(x_i)|}$$

qui divise $|G|$. Et donc si $|O_i| \geq 2$, c'est une puissance non nulle de $p$, i.e.

$$p \mid |O_i|, \quad \text{si } |O_i| \geq 2$$

Alors, on sait que $\sum_{|O_i| \geq 2} |O_i|$ est divisé par $p$, on a donc

$$\begin{aligned} |X| &= |X^G| + \sum_{|O_i| \geq 2} |O_i| \\ &\equiv |X^G| \mod p \end{aligned}$$

□

**Corollaire 2.12.** *(Conséquence)*

*Soit $G$ un $p$-groupe, alors le centre de $G$,*

$$Z(G) = \{g \in G | \forall h \in G, gh = hg\}$$

*est non trivial. (Évidemment, $Z(G) \lhd G$), i.e.*

$$Z(G) \neq \{1\}, \quad |Z(G)| \geq 2$$

*Démonstration.* On a

$$\begin{aligned} Z(G) &= \{g \in G | \forall h \in G, gh = hg\} \\ &= \{g \in G | \forall h \in G, h^{-1}gh = g\} \end{aligned}$$

On considère l'action de $G$ sur lui-même par conjugaisons, ici

$$X = G, \quad X^G = Z(G)$$

Donc,

$$\begin{aligned} |X| &= |G| \\ &\equiv |Z(G)| \mod p \end{aligned}$$

Alors, on sait que

$$|Z(G)| \equiv 0 \mod p$$

Or,

$$e \in Z(G) \Rightarrow |Z(G)| \geq 1$$

donc, $p$ divise $|Z(G)|$ et $Z(G)$ est non trivial. $\square$

## 2.1 Formule de Burnside

**Théorème 2.13.** *Soit $G$ un groupe fini agissant sur un ensemble fini $X$, $|X| \geq 2$, alors le nombre $N$ d'orbites :*

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

*où*

$$Fix(g) = \{x \in X \mid g \cdot x = g\}$$

*Démonstration.* Tout d'abord, on remarque que pour $g \in G$ et $x \in X$, on a

$$g \in \text{stab}(x) \Leftrightarrow x \in \text{Fix}(g)$$

On considère :

$$\begin{aligned} E &= \{(g, x) \in G \times X \mid g \cdot x = x\} \\ &= \bigsqcup_{g \in G} \{g\} \times \text{Fix}(g) \\ &= \bigsqcup_{x \in X} \text{stab}(x) \times \{x\} \end{aligned}$$

alors, on a

$$\begin{aligned} |E| &= \sum_{g \in G} |\text{Fix}(g)| \\ &= \sum_{x \in X} |\text{stab}(x)| \end{aligned}$$

Or, on sait que

$$G/\text{stab}(x) \simeq \mathcal{O}(x)$$

alors,

$$|\mathcal{O}(x)| = \frac{|G|}{\text{stab}(x)} \Rightarrow |\text{stab}(x)| = \frac{|G|}{|\mathcal{O}(x)|}$$

alors, on a

$$\sum_{g \in G} |\text{Fix}(g)| = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|}$$

Soient $O_1, O_2, \ldots, O_N$ les orbites distinctes et pour $\forall x \in X$, $\exists! i \in \{1, \ldots, N\}$ tel que $\mathcal{O}(x) =$

$O_i$, de plus, on a

$$X = \bigsqcup_{i \in \{1,\dots,N\}} O_i$$

alors,

$$\begin{aligned}\sum_{x \in X} \frac{1}{|O(x)|} &= \sum_{i=1}^{N} \Big( \sum_{x \in O_i} \frac{1}{|O_i|} \Big) \\ &= \sum_{i=1}^{N} \frac{1}{|O_i|} |O_i| \\ &= N\end{aligned}$$

donc,

$$\begin{aligned}\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| &= \sum_{x \in X} \frac{1}{|O(x)|} \\ &= N\end{aligned}$$

$\square$

**Corollaire 2.14.** *Soit $G$ un groupe fini agissant transitivement sur un ensemble $X$ fini, alors, il y a au moins un $g \in G$ qui n'a pas de point fixe.*

*Démonstration.* Ici, par le formule de Burnside, on a

$$N = 1 = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

alors, comme $|X| \geq 2$ et

$$1 = \frac{1}{|G|} \big( |X| + \sum_{g \neq e} |\mathrm{Fix}(g)| \big)$$

d'où $\exists g \in G$, tel que $|\mathrm{Fix}(g)| = 0$, c'est-à-dire $g$ n'a pas de point fixe. $\square$

## 2.2 Application : sous-groupe finies du groupe SO(3)

Une rotation dans $\mathbb{R}^3$ donnée par son axe (qui est égale à son ensemble de points fixe) et le plan qui est perpendiculaire à l'axe.

Dans une base orthonormée convenable, une rotation s'exprime comme

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}$$

On considère la sphère unité $S^2 \subset \mathbb{R}^3$ et les intersections des axes des rotations avec cette sphrère.

Soit $G \subset SO(3)$ un sous-groupes fini, et $|G| = n$. $\forall r \in G$, l'axe de $r \neq e$ et rencontre $S^2$ en 2 points symétriques appelés pôles de $r$.

Soit $P = \{\text{pôle des } r \neq e \mid r \in G\}$

**Proposition 2.15.** *$G$ agit sur $P$*

*Démonstration.* Si $r \in G$, $r \neq e$ et de pôle $x, -x$ et que $s \in G$, alors $srs^{-1} \in G$ et $srs^{-1}$ est une rotation dont axe est l'image par $s$ et de l'axe de $r$.

Donc, prenant l'intersection avec $S^2$, on obtient que $s(x) \in P$ pour $x \in P$, alors $G$ agit sur $P$. □

Pour $x \in P$, notons :

$$G_x = \text{stab}(x) \subset G$$
$$e_x = |\text{stab}(x)| = |G_x|$$

évidemment, on a$2 \leq e_x \leq n$.

Soient $k$ le nombre d'orbites et $e_1, \ldots, e_k$ les cardinaux des stabilisateurs d'un élément choisi dans chaque orbite.

Par le formule de Burnside, on obtient

$$k = \frac{1}{n} \sum_{g \in G} |\text{Fix}(g)|$$

de plus, on sait que

$$\begin{aligned} g = e, &\quad \mathrm{Fix}(g) = P \\ g = r \neq 2, &\quad |\mathrm{Fix}(g)| = 2 \end{aligned}$$

alors,

$$\sum_{g \in G} |\mathrm{Fix}(g)| = |p| + (n-1)2$$

et on obtient

$$nk = |P| + 2(n-1)$$

de plus,

$$\begin{aligned} |P| &= \sum_{j=1}^{k} |O_j| \\ &= \sum_{j=1}^{k} \frac{n}{e_j} \end{aligned}$$

où $O_1, \ldots, O_n$ sont les orbites distinctes.

Alors, on a

$$\begin{aligned} 2(n-1) &= nk - n \sum_{j=1}^{k} \frac{1}{e_j} \\ &= n \sum_{j=1}^{k} \big(1 - \frac{1}{e_j}\big) \end{aligned}$$

résultat, on a

$$\sum_{j=1}^{k} \big(1 - \frac{1}{e_j}\big) = 2\big(1 - \frac{1}{n}\big)$$

avec $2 \leq e_j \leq n$.

Ce sont les contraintes numériques reliant les $e_j$ et $n$, on va voir que $k$ ne peut être que 2 ou 3 et pour chaque valeur de $k$, il y a un nombre restraint de possibilité.

Valeurs de $k$ possibles : Comme $2 \leq e_i \leq n$, on a

$$\frac{1}{2} \leq 1 - \frac{1}{e_i} \leq 1 - \frac{1}{n}$$

alors, on a (on sait que $k \geq 2$),

$$\frac{k}{2} \leq \sum_{i=1}^{k} \big(1 - \frac{1}{e_i}\big) = 2\big(1 - \frac{1}{n}\big) \leq k\big(1 - \frac{1}{n}\big)$$

donc,

$$k \leq 4\big(1 - \frac{1}{n}\big) < 4$$

résultat,

$$k \in \{2, 3\}$$

• $k = 2$ :

Par le formule qu'on vient de déduire, on obtient :

$$\frac{1}{e_1} + \frac{1}{e_2} = \frac{2}{n}$$

comme $2 \leq e_i \leq n$, on a

$$e_1 = e_2 = n$$

Alors, chaque orbite est fixée par $G$, en conséquence, elle est formée d'un seul élément. Alors, on sait que

$$P = \{x, -x\}$$

et il existe un seul axe de rotation, donc $G$ est isomorphe à un groupe fini de rotations planes. Par conséquent, $G$ est une groupe cyclique.

*Remarque.* Les stabilisateurs $G_i$ sont toujours des groupes cycliques car ce sont des rotations ayant un même axe.

• $k = 3$ :

Par le formule qu'on vient de déduire, on obtient :

$$\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} = 1 + \frac{2}{n}$$

suppsons que $e_1 \leq e_2 \leq e_3$, on a nécessairement que $e_1 = 2$. En effet, si $e_i \geq 3$ pour

$\forall i \in \{1,2,3\}$, on a
$$\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{e_3}\leq 1$$
c'est impossible.

Alors, on a
$$\frac{1}{e_2}+\frac{1}{e_3}=\frac{1}{2}+\frac{2}{n}$$
et on a forcément $e_2 \leq 3$, en effet, si $e_2 \geq 4$, on a que
$$\frac{1}{e_2}+\frac{1}{e_3}\leq\frac{1}{2}$$
qui est impossible.

$\circ$ $e_2 = 2$

Dans ce cas, on a
$$\frac{2}{n}=\frac{1}{e_3}\Rightarrow e_3=\frac{n}{2}$$
il y a 3 orbites et
$$|O_1|=|O_2|=\frac{n}{2},\quad |O_3|=2$$
Pour $x \in O_3$, comme $G_x = G_{-x}$, les cardinaux des orbites de $x$ et $-x$ sont égaux, alors,
$$O_3=\{x,-x\}$$
une seule orbite de cardinal 2 et $G_x$ est un groupe cyclique de cardinal $\frac{n}{2}$.

Pour $y \in O_1$, $|G_y| = 2$, $G_y$ est un groupe cyclique engendré par une rotation d'angle $\pi$.

De plus,
$$G_x\cap G_y=\{\mathrm{Id}\}$$
et comme $G_x$ est un sous-groupe d'indice 2
$$G_x \lhd G$$
Alors, $G = G_x \cdot G_y$ est d'ordre $n$, c'est le groupe diédral d'ordre $n$.

*Remarque.* $D_n$ : c'est le groupe des isométres du polygone régulier à $n$ côtés dans le plan qui est engendré par 2 éléments $s$ et $r$ satisfaisant :
$$s^2=\mathrm{Id},\quad r^n=\mathrm{Id},\quad srs^{-1}=r^{-1}$$

$\circ$ $e_2 = 3$ :

Comme $e_1 = 2$ et $e_2 = 3$, on a

$$\frac{1}{e_3} = \frac{1}{6} + \frac{2}{n}$$

alors, on obtient

$$e_3 < 6$$

$*$ $e_1 = 2$, $e_2 = e_3 = 3$ :

On a

$$\frac{1}{6} + \frac{2}{n} = \frac{1}{e_3} = \frac{1}{3} \Rightarrow n = 12$$

dans ce cas, on a

$$|O_1| = 6, \quad |O_2| = |O_3| = 4$$

Considérons que $G$ agit dans $O_2$, on obtient un morphisme $\varphi : G \to \sigma_4$.

On a $\varphi$ est injectif, en effet, si une rotation fixe 4 points de la sphère, elle va fixer un plan vectoriel et c'est donc Id. (On a toujours au moins 2 droites vectorielles indépendantes). Donc, $G$ est isomorphe à un sous-groupe de cardinal 12 de $\sigma_4$.

$|\sigma_4| = 24$. Or, $\sigma_4$ possède un unique sous-groupe d'ordre 12 qui est $A_4$ : le groupe alterné. Résultat :

$$G \simeq A_4$$

$*$ $e_1 = 2$, $e_2 = 3$, $e_3 = 4$ :

On a

$$\frac{1}{6} + \frac{2}{n} = \frac{1}{e_3} = \frac{1}{4} \Rightarrow n = 24$$

dans ce cas, on a

$$|O_1| = 12, \quad |O_2| = 8, |O_3| = 6$$

Soit $x \in O_2$, alors

$$G_x = G_{-x} \Rightarrow -x \in O_2$$

$O_2$ est consituée de 4 paires de points opposés : ces 4 points définissent 4 droites.

Comme $G$ agit dans $O_2$ donc $G$ agit sur l'ensemble de ces 4 droites, d'où un morphisme $\psi : G \to \sigma_4$

On a $\psi$ est injective (comme ci-dessus), $G$ est alors isomorphe à un sous-groupe de $\sigma_4$, mais

$|G| = |\sigma_4|$, résultat :

$$G \simeq \sigma_4$$

$*$ $e_1 = 2$, $e_2 = 3$, $e_3 = 5$ :

On a

$$\frac{1}{6} + \frac{2}{n} = \frac{1}{e_3} = \frac{1}{5} \Rightarrow n = 60$$

On va prouver plus tard que

$$G \simeq A_5$$

car il existe un unique groupe simple d'ordre 60 (à isomorphisme près), c'est $A_5$. (On va le voir plus tard).

**Définition 2.16.** Un groupe $G$ est dit simple si ses seuls sous-groupes distingués est $\{e\}$ et $G$.

Cette notion ets importante :

Soit $G$ un groupe simple, si $f : G \to H$ est un morphisme de groupe non trivial, alors $f$ est injectif.

## 2.3 Retour sur quelques propriétés

1. Sous groupe distingué :

Soit $G, H, K$ trois groupes, si $f : G \to H$ est un morphisme du groupe et que $K \lhd G$, $f(K)$ n'est pas toujours distingué dans $H$, si $f$ est surjectif, alors $f(K)$ est distingué.

*Démonstration.* Si $f$ est surjectif, pour $k' \in f(K)$, $h \in H$, il existe $g \in G$, $k \in K$, tels que $h = f(g)$ et $k' = f(K)$, alors,

$$\begin{aligned} hk'h^{-1} &= f(g)f(k)f(g)^{-1} \\ &= f(gkg^{-1}) \end{aligned}$$

comme $K \lhd G$, on sait que $gkg^{-1} \in K$, alors on sait que

$$hk'h^{-1} = f(gkg^{-1}) \in f(K)$$

alors, $f(K) \lhd H$.

Un contre-exemple :

On sait déjà que $< a > \lhd V_4 \lhd A_4$ mais on n'a pas $< a > \lhd A_4$, dans la première partie du texte, alors, on peut considérer un morphisme $f : V_4 \to A_4$, qui se définit par $f(g) = g$, alors, on a $< a > \leq V_4$, mais, $f(< a >) =< a >$ n'est pas distingué dans $A_4$. $\square$

2. Si $K \lhd G$, $K$ est une réunion de classes de conjugaison ($G$ agit sur lui-même par conjugaison : $g \cdot h = ghg^{-1}$, les orbites est les classes de conjugaison.)

3. Sur les théorème d'isomorphisme, on a vu : pour $K \subset H \subset G$ trois groupes, si $K \lhd G$, $H \lhd G$, alors $(G/K)/(H/K) \simeq G/H$, isomorphisme du groupe.

Autre situation :

(1) $K \simeq G$, $K \subset H \subset G$, on a $H/K \subset G/K$. L'ensemble des classes de $G/K$ modulo $H/K$ :

$$(G/K)/(H/K) \xrightarrow{\sim} G/H$$

est bijection.

*Démonstration.* Si $g, g' \in G$, alors

$$\begin{aligned} gK \equiv g'K \mod H/K &\Leftrightarrow \exists h \in H, \quad \text{tel que } gK = g'K \cdot hK = g'hK \\ &\Leftrightarrow \exists h \in H, \quad \text{tel que } g^{-1}g'h \in K \\ &\Leftrightarrow g^{-1}g' \in H \\ &\Leftrightarrow g' \equiv g \mod H \end{aligned}$$

□

(2) $K \subset H \subset G$, les sous-groupes, alors, pour multiplicativité des indices :

$$[G:H] = |G/H| = \frac{|G|}{|H|}$$

c'est l'indice de $H$ dans $G$, on a

$$[G:K] = [G:H][H;K]$$

*Démonstration.* On choisit du systèmes de représentants des classes à gauche pour $G/H$, on prendre $g_1, \dots, g_n \in G$, tels que les classes sont $g_1H, \dots, g_nH$.

Pour $H/K$, on prend $h_1, \dots, h_p \in H$, tels que les classes sont $h_1K, \dots h_pK$.

Soit $g \in G$, $\exists! i \in \{1, \dots, n\}$ et $h \in H$, tels que $g = g_ih$, pour ce $h \in H$, $\exists! j \in \{1, \dots, p\}$ et $k \in K$, tels que $h = h_jk$, ainsi,

$$g = g_ih_jk$$

i.e. $g \in g_ih_jK$.

On voit que ces classes sont 2 à 2 distinctes, alors les $(g_ih_j)_{1\leq i\leq n, 1\leq j\leq p}$ forment un système de représentants pour les classes $G/K$, alors, on a

$$[G:K] = np = [G:H][H;K]$$

□

**Construction de sous-groupes** :

**Définition 2.17.** Soient $G$ un groupe et $H, K$ ses sous-groupes, alors,

$$HK = \{g = h\dot{k} \mid h \in H, k \in K\}$$

est un sous-ensemble de $G$

**Proposition 2.18.** *$HK$ est un sous-groupe de $G \Leftrightarrow HK = KH$.*

*Démonstration.* On a

$$g = hk \in HK \Rightarrow (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$$

et pour $g' \in HK$, il existe $h' \in H$ et $K' \in K$, tels que $g' = k'h'$ alors,

$$gg' = hkk'h$$

de plus, comme $kk'h' \in KH = HK$, il existe $h'' \in H$ et $k'' inK$, tels que $kk'h' = h''k''$, alors,

$$\begin{aligned} gg' &= hkk'h' \\ &= hh''k'' \in HK \end{aligned}$$

alors on a aussi le stabilité par produit. □

*Remarque.* Cette propriété est vraie si $H$ ou $K$ est distingué.

Si $K \lhd G$, pour $hk \in HK$, on a

$$hk = (hkh^{-1})h \in KH$$

alors, $HK \subset KH$, de même $KH \subset HK$, alors, on obtient

$$HK = KH$$

En général, $HK$ n'est pas un groupe, mais on a la proposition ci-dessous :

**Proposition 2.19.** *Pour le cardinal de $HK$, on a*

$$|HK| = \frac{|H||K|}{|K \cap H|}$$

*Démonstration.* On considère l'action de $H$ sur $G/K$.

On sait que $G$ agit (transitivement) sur $G/K$ par translation à gauche et on restreint cette action à H :

cette restriction n'est plus transitive. On considère l'orbite de $K \in G/K$ : elle est formée de classes $hK$, 2 à 2 distinctes et dont la réunion est

$$HK = \{hk \mid h \in H, k \in K\}$$

Il faut donc compter le nombre d'éléments distincts dans l'orbites de $K$, mais

$$hK = h'K \Leftrightarrow h^{-1}h' \in K \cap H \subset H$$

Ainsi,

$$hK = h'K \Leftrightarrow hK \cap H = h'K \cap H$$

égalité dans $H/H \cap K$, le nombre d'éléments dans l'orbites de $K$ est alors $\frac{|H|}{H \cap K}$, donc,

$$|HK| = \frac{|H||K|}{|K \cap H|}$$

□

*Remarque.* Comparer avec la formule pour les espaces vectoriels :

Soient $E, F$ deux espaces vetoriels d'un espace vectoriel de $G$, alors,

$$\dim(E + F) = \dim(E) + \dim(F)$$

Ici, version mulplicative :

$$|HK| = \frac{|H||K|}{|K \cap H|}$$

*Remarque.* (Rappels)

Soit $G$ un groupe, alors tout sous-groupe d'indice 2 est distingué.

*Démonstration.* On suppose que $H \subset G$ un sous-groupes d'indice 2, c'est-à-dire,

$$|G/H| = 2$$

Alors pour $a \in G \setminus H$, on a

$$G/H = \{H, aH\}$$

et on a une partition,

$$G = H \cup aH$$

en considérant l'application $g \to g^{-1}$ pour $g \in G$, on a aussi

$$G = H \cup Ha$$

alors $Ha = aH$ puis $H \lhd G$. $\square$

## 2.4 Théorèmes de Sylow

Motivation :

Théorème de lagrange nous dit que : si $H \subset G$ est un sous-groupe, alors $|H|$ divise $|G|$. Cependant, la propriété inverse est fausse :

**Exemple.** $G = A_4$, alors $|G| = 12$, mais $G$ n'a pas de sous-groupe d'ordre 6.

Situation marche :

**Lemme 2.20.** *Soit $G$ un $p$-groupe, où $p$ est un nombre premier et $|G| = p^n$. Alors, $\forall i \in \{1, \ldots, n-1\}$, $G$ possède un sous-groupe d'ordre $p^i$.*

*Démonstration.* On démontre par récurrence sur $n$.

On a vu que le centre de $G$, $Z(G)$ est non trivial. Soit $g \in Z(G)$ un élément d'ordre $p^\alpha$, alors $g^{p^{\alpha-1}}$ est d'ordre $p$. Le sous-groupe $< g^{p^{\alpha-1}} >$ engendré par $g^{p^{\alpha-1}}$ est cyclique d'ordre $p$, et de plus, il est distingué car $g \in Z(G)$.

On considère :

$$G_1 := G/ < g^{p^{\alpha-1}} >$$

alors $G_1$ est un sous-groupe de cardinal $p^{n-1}$, auquel on peut appliquer une hypothèse de récurrence.

$\forall \beta \in \{1, \ldots, n-2\}$, $\exists H \subset G$, un sous-groupe de cardinal $p^\beta$. Pour l'application :

$$\begin{aligned} \pi : G &\to G_1 \\ g &\mapsto \bar{g} \end{aligned}$$

$\pi^{-1}(H)$ est un sous-groupe de $G$ de cardinal $|H| \cdot p$ :

$$\pi^{-1}(H)/\ker\pi \simeq H$$

d'où $\pi^{-1}(H)$ d'ordre $p^{\beta+1}$. □

**Définition 2.21.** Soient $G$ un groupe fini et $p$ un premier tels que $p \mid |G|$, on écrit :

$$|G| = p^\alpha \cdot m$$

avec $p \nmid m$.

Un $p$-sous-groupe de sylow de $G$ (on dit $p$-sylow) est un sous-groupe de $G$ de cardinal $p^\alpha$.

**Théorème 2.22.** *Soient $G$ un groupe et $p$ un nombre premier, si $p \mid |G|$, alors $G$ possède au moins un $p$-sylow.*

**Corollaire 2.23.** *Si $p \mid |G|$, $|G| = p^\alpha \cdot m$ avec $m \wedge p = 1$, alors $\forall \beta \leq \alpha$, $G$ possède un sous-groupe d'ordre $\beta$.*

On montra le théorème plus tard.

**Exemple.** Soient $p$ un premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ un corps. Soit $G$ un groupe classique

$$G = GL_n(\mathbb{F}_p) \subset M_n(\mathbb{F}_p)$$

$G$ est un groupe fini et

$$\begin{aligned} |G| &= (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \\ &= p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \end{aligned}$$

En effet, si $g \in G$ est une matrice inversible, i.e., les vecteurs colomes forment une base, tout revient à compter le nombre de bases de $\mathbb{F}_p^n$.

$1^{er}$ vecteur : comme $|\mathbb{F}_p^n| = p^n$, donc on a $p^n - 1$ possibilités.

$2^e$ vecteur : on compte le nombre de vecteur qui n'appatient à $\mathbb{F}_p^n e_1$, où $e_1$ est le premier vecteur qu'on vient de choisir. Il y a donc $p^n - p$ possibilités.

$3^e$ vecteur : on choisit ce vecteur dans $\mathbb{F}_n^p \backslash$le plan vectoriel engendré par les 2 premiers, il y a alors $p^n - 2$ possibilités.

$\ldots$

$(k+1)^e$ vecteur : il est choisi dans $\mathbb{F}_p^n$ privié de l'espace vectoriel de dimension $k$ engendré par les $k$ premiers vecteurs, d'où $p^n - p^k$ possibilités.

Ainsi,

$$\begin{aligned} |GL_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \\ &= p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \end{aligned}$$

alors, on a

$$|GL_n(\mathbb{F}_p)| = p^\alpha \cdot m, \quad \text{avec } \alpha = \frac{n(n-1)}{2}$$

En outre, il faut trouver un sous-groupes de cardinal $p^{\frac{n(n-1)}{2}}$ :

$$S = \left\{ \begin{pmatrix} 1 & & & * \\ & \ddots & & \\ & 0 & 1 & \\ & & & 1 \end{pmatrix} \right\}$$

il y a $\frac{n(n-1)}{2}$ termes strictement au dessus du diagonale, donc,

$$|S| = p^{\frac{n(n-1)}{2}}$$

$S$ est un $p$-sylow de $GL(\mathbb{F}_p)$

**Lemme 2.24.** *Soient $G$ un groupe et $p$ un premier, $|G| = p^\alpha \cdot m$, $p \nmid m$, on suppose que $S$ est un $p$-sylow de $G$. Soit $H \subset G$ un sous-groupe. Alors $\exists a \in G$, tel que $aSa^{-1} \cap H$ est aussi un $p$-sylow.*

*Remarque.* $\forall a \in G$, $aSa^{-1}$ est aussi un $p$-sylow.

*Démonstration.* (preuve du lemme)

On considère $G/S$ est l'action transitive de $G$ sur $G/S$. On le restreint à $H$.

Rapple : comme $S = \mathrm{stab}(S)$, on a

$$aSa^{-1} = \mathrm{stab}(aS)$$

donc, on a

$$aSa^{-1} \cap H = \mathrm{stab}_H(aS)$$

stabilisateur dans $H$ pour l'action de $H$.

*Remarque.* Dire $S$ est un $p$-syloe de $G$, c'est-à-dire : $S$ est un $p$-groupe et $[G : S] = |G/S|$ est premier avec $p$.

Ainsi, pour avoir un $p$-sylow de $H$, on cherche $a \in G$, tel que $[H : aSa^{-1} \cap H]$ est premier avec $p$, comme

$$aSa^{-1} \cap H = \mathrm{stab}_H(aS)$$

on sait que $[H : aSa^{-1} \cap H]$ est le cardinal de l'orbite de $aS$ sous l'action de $H$.

Il faut voir qu'il existe une orbite de $H$ dans $G/S$ dont le cardinal est premier avec $p$.

Or $|G/S|$ est premier avec $p$ est $G/S$ est le réunion disjointe d'orbite. Si on avait que $p$ divise les cardinaux de toutes les orbites, il diviserait aussi $|G/S|$, c'est impossible. $\square$

Preuve du thm de sylow :

Soient $G$ un groupe et $p$ un premier, $|G| = p^\alpha m$, $p \nmid m$.

**Proposition 2.25.** *$\exists$ un morphisme de groupes injectif : $G \to GL_n(\mathbb{F}_p)$.*

*Démonstration.* (1) On dispose du théorème de Cayley, il existe un morphisme injectif $\varphi$ :

$$\varphi : G \to \sigma_n$$

(2) Pour $\forall K$ un corps, on a un morphisme injectif :

$$\begin{aligned} \sigma_n &\hookrightarrow GL_n(K) \\ \sigma &\mapsto P_\sigma \end{aligned}$$

où $P_\sigma$ est une matrice de permutation, dans la base canonique :

$$P_\sigma(e_i) = e_{\sigma(i)}$$

Ainsi, $G$ est isomorphisme avec un sous-groupe de $GL_n(\mathbb{F}_p)$ et on peut appliquer le lemme. $\square$

**Théorème 2.26.** *(Sylow)*

*Soient $G$ un groupe et $p$ un premier, $|G| = p^\alpha m$, $p \nmid m$.*

*(1) Si $H \subset G$ est un p-groupe, alors il existe un p-sylow de $G$ contenant $H$.*

*(2) Tous les p-sylow de $G$ sont conjugués et donc leur nombre $k$ divise $|G|$. En particulier, $G$ possède un unique p-sylow $\Leftrightarrow$ il y a un p-sylow qui est un sous-groupe distingué.*

*(3) Le nombre $k$ de p-sylow satifait à :*

$$k \equiv 1 \mod p$$

*(donc $k \mid m$).*

*Démonstration.* (1)$H$ est un $p$-sous-groupe de $G$ et fixons $S$ un $p$-sylow de $G$.

D'après le lemme, $\exists a \in G$, tel que $aSa^{-1} \cap H \subset H$ est un $p$-sylow de $H$. Mais $H$ est son propre $p$-sylow, alors,

$$aSa^{-1} \cap H = H$$

i.e. $H \subset aSa^{-1}$ et $aSa^{-1}$ est bien un $p$-sylow de $G$.

(2) Soit $S'$ un autre $p$-sylow de $G$ et on applique (1) à $S'$ :

$$\exists a \in G, \quad S' \subset aSa^{-1}$$

en fait, $S' = aSa^{-1}$ à cause de leurs cardinaux égaux.

Alors, tous les $p$-sylow de $G$ sont conjugués et $G$ possède un unique $p$-sylow $\Leftrightarrow$ il y a un $p$-sylow qui est un sous-groupe distingué.

(3) Soit $X$ un ensemble :

$$X = \{p\text{-sylow de } G\}$$

sur lequel $G$ agit par conjugaison avec une seule orbite et on a

$$k = |X|$$

Soit $S$ un $p$-sylow, qu'on fait agit par restriction sur $X$. L'équation aux classes pour les $p$-groupes donne :

$$|X| \equiv |X^S| \mod p$$

On a $S \in X^S$ et on va montrer que $|X^S| = 1$, i.e. $X^S = \{S\}$.

Soit $T \in X^S$, alors $\forall s \in S$, $sTs^{-1} = T$. Soit $H$ le sous-groupe de $G$ engendré par $S$ et $T$.

Comme $sTs^{-1} = T$, pour $\forall s \in S$, on a que $T \lhd D$. De plus, $S$ et $T$ sont des $p$-sylows de $H$. Mais comme $T \lhd D$, d'après (2), c'est l'unique $p$-sylow de $H$, d'où $S = T$.

En résumé, $|X^S| = 1$ et

$$k = |X| \equiv |X^S| = 1 \mod p$$

$\square$

### 2.4.1 Application : simplicité, non simplicité selon le cardinal du groupe.

**Exemple.** Soit $G$ un groupe d'ordre 63, alors $G$ n'est pas simple.

En effet, $63 = 3^2 \times 7$, on regarde les 7-sylow :

$$\begin{cases} k \equiv 1 \mod 7 \\ k \mid 9 \end{cases} \Rightarrow k = 1$$

il existe un unique 7-sylow, donc distingué.

Alors, $G$ n'est pas simple.

**Exemple.** Soient $G$ un groupe d'ordre 48, alors, $G$ n'est pas simple.

*Démonstration.* On a $48 = 2^4 \times 3$, on utilise que $G$ agit sur les $p$-sylow, où $p = 2$ ou 3.

Si $k$ est le nombre de $p$-sylow, ceci donne un morphisme $\varphi : G \to \sigma_k$ et $\ker \varphi \triangleleft G$. Si $|G|$ ne divise pas $k!$, alors $\varphi$ ne peut pas être injectif, d'où $\ker \varphi \neq \{e\}$.

Ici, $p = 2$, $k \mid 3$, $k = 1$ ou 3.

• Si $k = 1$, le 2-sylow est distingué.

• Si $k = 3$, on a un morphisme $\varphi : G \to \sigma_3$. Comme $|\sigma_3| = 6$, $\varphi$ n'est pas injectif. Alors $\ker \varphi \triangleleft G$.

En somme, $G$ n'est pas simple. □

**Proposition 2.27.** *Soient $G$ un groupe, $N \triangleleft G$, $P$ un $p$-sylow de $G$. Alors, $PN/N$ est un $p$-sylow de $G/N$ et $P \cap N$ est un $p$-sylow de $N$.*

*Démonstration.* On a tout d'abord,

$$[G/N : PN/N] = [G : PN]$$

$PN/N$ est l'image de $P$ dans $G/N$ et

$$(G/N)/(PN/N) \simeq G/PN$$

Comme $P \subset PN \subset G$, on sait que

$$[G : P] = [G : PN][PN : P]$$

alors, comme $[G; PN]$ divise $[G : P]$, $p$ ne peut pas diviser $[G : PN]$.

De plus,

$$PN/N \simeq P/P \cap N$$

qui est bien un $p$-groupe, alors, $PN/N$ est un $p$-sylow de $G/N$.

On a

$$[N : P \cap N] = [PN : P]$$

car on a vu $|PN| = \frac{|P||N|}{|P \cap N|}$, d'où

$$p \nmid [PN : P]$$

alors, $P \cap N$ est un $p$-sylow de $N$. $\square$

# 3 Rappels et compléments sur les groupes symétriques

Notons $\sigma_n$ le groupe symétrique et $A_n \subset \sigma_n$ le groupe alterné, alors, $A_n = \ker \varepsilon$, où $\varepsilon : \sigma_n \to \{\pm 1\}$.

## 3.1 Générateurs

**Définition 3.1.** Soit $k$ un entier tel que $k \leq n$, un $k$-cycle et une permutation de la forme suivante : $i_1, \ldots, i_k$ distincts dans $\{1, \ldots, n\}$, le cycle associé est la permutation :

$$\sigma = (i_1, \ldots, i_k)$$

telle que

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \sigma(i_k) = i_1$$

et si $j \notin \{i_1, \ldots, i_k\}$, $\sigma(j) = j$.

**Définition 3.2.** Le support de cycle est $\{i_1, i_2, \ldots, i_k\}$.

**Théorème 3.3.** *(Générateurs)*

*(1) $\sigma_n$ est engendré par les transposition,*

*(2) $A_n$ est engendré par les 3-cycles.*

*Démonstration.* (1) On regarde les points fixes.

Si $\sigma \in \sigma_n$ a $n$ points fixes, $\sigma = \mathrm{Id}$.

Si $\sigma$ a $n-1$ points fixes, $\sigma = \mathrm{Id}$.

Si $\sigma$ a $n-2$ points fixes, $\sigma$ est une transposition.

On fait une récurrence fini sur $n -$ le nombre de points fixes.

Soit $\sigma \in \sigma_n$, $\sigma \neq \mathrm{Id}$, $\exists i \in \{1, \ldots n\}$, tel que

$$\sigma(i) = j \neq i$$

Soit $\sigma' = (ij) \circ \sigma$, alors $\sigma'(i) = i$ et

$$\sigma(k) = k \Rightarrow \sigma'(k) = k$$

car si $\sigma(i) = j$, $\sigma(j) \neq j$.

Donc, $\sigma'$ a un point fixe de plus que $\sigma$, alors, par récurrence, $\sigma'$ est le produit de transposition, comme $\sigma = (ij)\sigma'$, $\sigma$ l'est aussi.

(2) On sait que $\varepsilon(\text{transposition}) = -1$, donc $A_n$ est engendré par les produits de 2 transpositions. Comme on a

$$(ij)(jk) = (ijk)$$

et si $i, j, k, l$ distincts, on a

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

En résumé, $A_n$ est engendré par les 3-cycles. $\square$

## 3.2 Propriétés importantes

**Proposition 3.4.** *Dans $\sigma_n$, les $k$-cycles sont conjugués :*

*Si $\sigma, \sigma'$ sont deux $k$-cycles, alors,*

$$\exists \tau \in \sigma_n, \quad \sigma' = \tau\sigma\tau^{-1}$$

*Démonstration.* On a que pour $\tau \in \sigma_n$,

$$\tau(i_1, \ldots, i_k)\tau^{-1} = (\tau(i_1), \ldots, \tau(i_k))$$

□

**Proposition 3.5.** *Dans $A_n$, si $n \geq 5$, les 3-cycles sont conjugués.*

*Démonstration.* Deux 3-cycles sont conjugués dans $\sigma_n$, mais dans le cas où $\sigma(abc)\sigma^{-1} = (a'b'c')$ et que $\varepsilon(\sigma) = -1$. Comme $n \geq 5$, $\exists e', d' \notin \{a', b', c'\}$ et $e' \neq d'$,

$$(e'd')(a'b'c')(e'd') = (a'b'c')$$

alors, on pose

$$\tilde{\sigma} = (e'd')\sigma \in A_n$$

et on a

$$\tilde{\sigma}(abc)\tilde{\sigma}^{-1} = (a'b'c')$$

□

*Remarque.* Si on a un sous-groupe distingué de $A_n$ qui contient un 3-cycle, alors, il les contient tous, et donc il est égal à $A_n$.

**Proposition 3.6.** *Il existe un unique morphisme de groupe non trivial $\sigma_n \to \mathbb{C}^*$, c'est la signature $\varepsilon$.*

*Démonstration.* Soit $\varphi : \sigma_n \to \mathbb{C}^*$ un tel morphisme.

Alors, si $\tau$ est une transposition, alors $\tau^2 = e$, alors

$$\varphi(\tau)^2 = 1, \quad , \varphi(\tau) \in \{\pm 1\}$$

ainsi, $\varphi$ est à valeur dans $\{\mp 1\}$.

Comme $\varphi$ est non trivial, alors

$$\exists \tau \text{ transposition}, \quad \varphi(\tau) = -1$$

sinon, comme $\sigma_n$ est engendré par les transposition, $\varphi$ est toujours égal à 1.

Comme de plus les transpositions sont conjugué dans $\sigma_n$,

$$\forall \tau \text{ transposition}, \quad \varphi(\tau') = -1$$

(on utilise ici que $\mathbb{C}^*$ est commutatif.)

Ainsi, $\varphi = \varepsilon$. □

Décomposition en produit de cycles à supports disjoints :

**Théorème 3.7.** *Soit $\sigma \in \sigma_n$, il existe des cycles $c_1, \ldots, c_r$ à supports 2 à 2 disjoints, tels que $\sigma = c_1 \cdots c_r$, de plus, cette composition est unique à l'ordre près des facteur.*

*Démonstration.* Tous d'abord, on observe que comme les supports sont disjoints,

$$\forall i, j \in \{1, \ldots, r\}, \quad c_i c_j = c_j c_i$$

Soit $\sigma \in \sigma_n$, on regarde le sous-groupe $< \sigma >$ de $\sigma_n$ engendré par $\sigma$ et l'action de ce sous-groupe sur $\{1, \ldots, n\}$, on considère les orbits $F_1, \ldots, F_n$.

Soit $k \in F_1$ est $s$ le plus petit entier tel que $\sigma_s(k) = k$, alors, $k, \sigma(k), \sigma^2(k), \ldots, \sigma^{s-1}(k)$ sont distincts, sinon,

$$\exists i < j \leq s-1, \quad \sigma^i(k) = \sigma^j(k)$$

alors on a

$$\sigma^{j-i}(k) = k$$

mais $j - i < s - 1$ impossible.

Alors, on a

$$F_1 = \{k, \sigma(k), \ldots, \sigma^{s-1}(k)\}$$

si $p \in \mathbb{N}$, $p = sq + r$ et $0 \leq r \leq s-1$, alors,

$$\sigma^p(k) = \sigma^r(k)$$

Dans l'orbite $F_1$, $\sigma$ agit comme un cycle $(k, \sigma(k), \dots, \sigma^{s-1}(k))$. On obtient ainsi un cycle pour chaque orbite, dont l'orbite est exatement le support et $\sigma$ est le produit des cycles ainsi obtenus. $\square$

Conséquence : déspription des classes de conjugaison dans $\sigma_n$.

**Proposition 3.8.** *Deux permutations $\sigma$ et $\sigma'$ sont conjuguées dans $\sigma_n$ si et seulement si $\forall k \in \{1, \dots, n\}$, elles ont le même nombre de cycles de longueur $k$ dans leur décomposition en produit de cycles à supports disjoints.*

*Remarque.* La longueur d'un cycle est le cardinal de son support.

*Démonstration.* Soit $\sigma = c_1 \cdots c_r$ produit de cycles à supports disjoints, alors

$$\forall \tau \in \sigma_n, \quad \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1}) \cdots (\tau c_r \tau^{-1})$$

on a vu que chaque $\tau c_i \tau^{-1}$ est un cycle de même longueur que $c_i$. de support l'image par $\tau$ du support de $c_i$.

Inversement, si $\sigma = c_1 \cdots c_r$ et $\sigma' = c'_1 \cdots c'_r$ avec la longueur de $c_i$ = la longueur de $c'_i$.

On construit une permutation $\tau$ envoyant le support de $c_i$ bijectivement sur le support de $c'_i$ en respectant l'ordre.

Comme les supports sont disjoints, de réunion $\{1, \dots, n\}$, $\tau$ est bien une bijection. $\square$

*Remarque.* Les cycles de longueur 1 sont les points fixes.

Conséquence : l'ordre d'une permutation est le ppcm des longueurs des cycles de sa décomposition.

*Remarque.* Si $c$ est un cycle de longueur $k$, alors, $\varepsilon(c) = (-1)^{k-1}$.

## 3.3 Questions de simplicité

**Théorème 3.9.** *Pour $n = 4$, $A_n$ est un groupe simple.*

*Démonstration.* Pour $n = 4$, $A_4$ n'est pas simple, car il contient le sous-groupe distingué :

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

Pour $n = 3$, on a

$$A_3 \simeq \mathbb{Z}/3\mathbb{Z}$$

alors $A_3$ est simple.

Cas crucial : $n = 5$.

Simplicité de $A_5$ : $|A_5| = 60$. On va tout d'abord calculer les ordres de ses éléments :

• $e$ : d'ordre 1.

• Produits de 2 transpositions à support disjoints : 5 choix pour le points fixes et on a 3 possibilités pour décomposer ($\frac{1}{2}C_4^2$), d'où 15 éléments d'ordre 2.

• Éléments d'ordre 3 : 3-cycle, support $C_5^3$ (2 éléments sont fixées et les 3 autres permutes circulairement), et ensuite comme si $\sigma = (abc)$, alors $\sigma^2 = (acb)$, il y a donc 20 éléments d'ordre 3.

• Éléments d'ordre 5 : 5-cycle, en fixant 1 au première position (par exemple, $(i_1, i_2, i_3, i_4, i_5) = (1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$), on peut choisir $\alpha_2, \alpha_3, \alpha_4, \alpha_5$ par harsard, alors il y a $4! = 24$ éléments d'ordre 5.

On a obtenu tous les éléments de $A_5$ : $1 + 15 + 20 + 24 = 60$.

On a :

• Tous les 3-cycle sont conjugués (on a déjà vu).

• Tous les éléments d'ordre 2 sont conjugué : en effet, soit $\sigma = (ab)(cd)(e)$ et $\sigma' = (a'b')(c'd')(e')$ les deux telles éléments, alors,

$$\exists \tau \in \sigma_5, \quad \tau\sigma\tau^{-1} = \sigma'$$

si $\varepsilon(\tau) = -1$, on a

$$(a'b')\sigma'(a'b') = \sigma', \quad (a'b')\tau \in A_5$$

• Les 5-cycles ne peuvent pas être conjugué car $24 \nmid 60$, cependant $60 = 2 \times 3 \times 5$, les 5-cycles engendrent chacun un groupe cyclique d'ordre 5 qui est un 5-sylow.

Soit $H \lhd A_5$, $H \neq \{e\}$.

Si $H$ contient un élément d'ordre 2, il les contient tous, idem pour les éléments d'ordre 3. Comme les 5-sylow sont conjugués, si $H$ contient un élément d'ordre 5, il contient le 5-sylow engendré par cet élément et donc tous les 5-sylows, donc $H$ contient tous les éléments d'ordre 5.

De plus, $H$ ne peut pas contenir qu'un seul type de ces 3 types d'éléments car ni $25 = 24+1$, ni $21 = 20+1$, ni $16 = 15+1$ ne divise 60. Donc il contient au moins 2 des 3 types, donc, on sait que

$$|H| \geq 1 + 15 + 20 = 36$$

et comme $|H| \mid 60$, $|H| = 60$, alors $H = A_5$.

Cas général : on se ramène au cas $n = 5$.

Si $H \lhd A_n$ (ici, $n \geq 6$). $H \neq \{e\}$ à partir de $\sigma \neq e$ dans $H$, on construit un autre éléments $\sigma'$ de $H$ qui aura au moins $n-5$ points fixés et $\sigma' \neq e$.

Si $F =$ complémentaire de l'ensemble des points fixes de $\sigma'$, $|F| \leq 5$ (qu'en peut supposer égal à 5).

On considère $A_F$ le sous-groupe des permutations paire fixant le complémentaire de $F$, alors, comme $|F| = 5$, on sait que

$$A_F \simeq A_5$$

De plus, on sait que

$$H \lhd A_n \Rightarrow H \cap A_F \lhd A_F$$

et on a

$$\sigma' \in H \cap A_F \Rightarrow H \cap A_F \neq \{e\}$$

Comme $A_5$ est simple, on a $H \cap A_F = A_F$, en particulier $H$ contient les 3-cycles de $A_F$.

Comme les 3-cycles sont conjugués dans $A_n$, $H$ contient tous les 3-cycles et $H = A_n$.

Ainsi, on s'est ramené à construire $\sigma'$.

On dispose de $\sigma \neq e$ dans $H$.

Idée :

$$\forall \tau \in A_n, \tau\sigma\tau^{-1} \in H \Rightarrow \tau\sigma\tau^{-1}\sigma^{-1} = \tau(\sigma\tau^{-1}\sigma^{-1}) \in H$$

si $\tau$ a beaucoup de points fixe, $\sigma\tau^{-1}\sigma^{-1}$ aussi et le produit certainement aussi.

Il faut choisir convenablement $\tau$ en fonction de $\sigma$.

On sait que $\sigma \neq e$, alors,

$$\exists a \in \{1, \ldots, n\}, \quad b = \sigma(a) \neq a$$

Soit $c \in \{1, \ldots, n\}$ avec $c \notin \{a, b, \sigma(b)\}$ (on a que $n \geq 5$. On pose

$$\tau = (acb) \Rightarrow \tau^{-1} = (abc)$$

donc,

$$\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} = (acb)(\sigma(a)\sigma(b)\sigma(c))$$

comme $\sigma(a) = b$, on sait que

$$F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$$

a au plus 5 éléments et $\sigma^{-1}$ fixe le complémentaire de $F$.

On a $\sigma' \neq e$ car on a

$$\sigma'(b) = \tau\sigma(b) \neq b$$

car $\sigma(b) \neq \tau^{-1}(b) = c$. □

**Théorème 3.10.** *Soit $G$ un groupe simple d'ordre 60, alors $G \simeq A_5$*

*Démonstration.* Soit $H$ un sous-groupe d'indice $n$, alors $G$ agit sur $G/H$, d'où un morphisme :

$$\varphi : G \to \sigma(G/H)$$

comme $G$ est simple, alors $\varphi$ est injectif. Alors, on sait que

$$|G| \mid n!$$

d'où $n > 4$ car $4! = 24$.

• Si $G$ a un sous-groupe d'indice 5, alors $G \hookrightarrow \sigma_5$, comme $|\sigma_5| = 120$, $G$ sera d'indice 2 dans $\sigma_5$, donc $G \lhd \sigma_5$, alors,

$$G \simeq A_5$$

• On suppose que $G$ n'a pas de sous-groupe d'indice 5.

○ On regarde les 5-sylow de $G$ : le nombre :

$$k_5 \equiv 1 \mod 5, \quad k \mid 12$$

comme $G$ simple, $k_5 = 1$ impossible, alors, on sait que

$$k_5 = 6$$

d'où 24 éléments d'ordre 5.

○ On regarde les 2-sylow : leur nombre divise 15. Comme ils sont conjugués, leur nombre est l'indice du stabilisateur de l'un d'eux.

Comme on suppose : pas de sous-groupe d'indice $\leq 5$, ce nombre est 15.

Soient $S_1, S_2$ deux 2-sylows et $S_1 \neq S_2$, alors

$$S_1 \cap S_2 = \{e\}$$

Sinon, on a $S_1 \cap S_2 = \{e, u\}$. Or $S_1$ et $S_2$ sont abéliens, on regarde le centralisateur de $u$ :

$$C(u) = \{g \in G \mid gu = ug\}$$

alors, on a

$$S_1 \subset C(u) \Rightarrow 4 \mid |C(u)|$$

Comme $S_1, S_2 \subset C(u)$, on sait que $|C(u)| \geq 6$, de plus $|C(u)| \mid 60$ et son indice $> 5$, alors

$$C(u) = G$$

donc, $u \in Z(G)$.

Or, $Z(G)$ est distingué, alors, $Z(G) = \{e\}$.

Donc les 2-sylow ne se rencontent qu'en $\{e\}$.

On obtient ainsi $15 \times 3 = 45$ éléments d'ordre 2 ou 4 : contradiction avec $|G| = 60$.

Conclusion : $G$ doit contenir un sous-groupe d'indice 5.

En résumé,

$$G \simeq A_5$$

□

## 3.4 Quelques conséquence de la simplicié de $A_n$

**Proposition 3.11.** *Soit $n \geq 5$, alors les seuls sous-groupes distingués de $\sigma_n$ sont $\{e\}, A_n, \sigma_n$.*

*Démonstration.* Soit $H \lhd \sigma_n$, $H \neq \{e\}$.

Alors, comme on a

$$H \cap A_n \lhd A_n$$

on a

$$H \cap A_n = A_n \text{ ou } H = \sigma_n$$

• Si $H \cap A_n = A_n$, alors,

$$A_n \subset H \Rightarrow H = A_n \text{ ou } H = \sigma_n$$

• Si $H \cap A_n = \{e\}$, soit $\varepsilon : \sigma_n \to \{\pm 1\}$ la signature, alors comme

$$\ker \varepsilon|_H = H \cap A_n = \{e\}$$

on sait que $\varepsilon_H$ est injective, alors,

$$|H| = 1 \text{ ou } 2$$

Si $|H| = 2$, alors $H = \{e, u\}$ avec $\varepsilon(u) = -1$, alors,

$$H \lhd \sigma_n \Rightarrow \forall \tau \in \sigma_n, \quad \tau u \tau^{-1} \in H$$

on sait que $\tau u \tau^{-1} \neq e$ car $u \neq e$, donc $\tau u \tau^{-1} = u$ et $\tau u = u \tau$, ainsi $u \in Z(\sigma_n)$.

Mais $Z(\sigma_n) = \{e\}$, contradiction. En effet pour $\sigma \in Z(\sigma_n)$, on a

$$(ij) = \sigma(ij)\sigma^{-1} = (\sigma(i), \sigma(j))$$

donc $\sigma(i) \in \{i, j\}$ pour $\forall j \neq i$, alors,

$$\sigma(i) = i$$

□

**Proposition 3.12.** *Soit $H \subset \sigma_n$ un sous-groupe d'indice $n$, alors $H \simeq \sigma_{n-1}$.*

*Démonstration.* • Pour $n \leq 3$, clair.

• pour $n = 4$, $|H| = 6$, alors,

$$H \simeq \mathbb{Z}/6\mathbb{Z} \text{ ou } H \simeq \sigma_3$$

mais $H \simeq \mathbb{Z}/6\mathbb{Z}$ impossible car $\sigma_4$ n'a pas d'éléments d'ordre 6.

On suppose que $n \geq 5$.

On considère l'action de $\sigma_n$ sur $\sigma_n/H$, d'où un morphisme

$$\varphi : \sigma_n \to \sigma(\sigma_n/H) \simeq \sigma_n$$

comme $\ker \varphi \lhd \sigma_n$, on a que $\ker \varphi = \{e\}, A_n$ ou $\sigma_n$ (proposition précédente).

De plus, on a

$$\ker \varphi = \bigcap_{g \in G} gHg^{-1}$$

car le stabilisateur $\mathrm{stab}(gH) = gHg^{-1}$.

Ainsi, $\ker \phi \subset H$ et donc $\ker \varphi = \{e\}$, alors $\varphi$ est injectif et même bijective.

$H$ agit dans $\sigma_n/H$ et il est de stabilisateur de $H \in \sigma_n/H$. Par $\varphi$, il se transforme en le stabilisateur d'un élément et donc, il est isomorphisme à $\sigma_{n-1}$. $\square$

## 3.5 Sous-groupe dérivé

**Définition 3.13.** Soit $G$ un groupe, le sous groupe dérivé de $G$, noté $\mathcal{D}(G)$ ou $[G:G]$, est le sous-groupe engendré par les commutateurs $ghg^{-1}h^{-1}$, $g,h \in G$.

Notation : $[g,h] = ghg^{-1}h^{-1}$.

Attention : les $[g,h]$ ne forment pas un sous-groupe a priori.

**Proposition 3.14.** $\mathcal{D}(G) \lhd G$

*Démonstration.* Pour $x,g,h \in G$, on a

$$x[g,h]x^{-1} = [xgx^{-1}, xhx^{-1}]$$

comme $\mathcal{D}$ est engendré par ces éléments, on sait que

$$\mathcal{D} \lhd G$$

□

*Remarque.* (1) Si $A$ un groupe abélien, $f : G \to A$ un morphisme de groupes, alors $\mathcal{D}(G) \subset \ker f$, en effet

$$\begin{aligned} f(ghg^{-1}h^{-1}) &= f(g)f(h)f(g^{-1})f(h^{-1}) \\ &= e \end{aligned}$$

ainsi, $f$ se factorise à travers $\mathcal{D}(G)$.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & A \\ G/\mathcal{D}(G) \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

(2) $G/\mathcal{D}(G)$ est un groupe abélien, c'est le plus gros quotient abélien de $G$.

$\mathcal{D}(G)$ est même caractérisé par cette propriété de passage au quotient pour les morphismes vers un groupe abélien.

**Proposition 3.15.** *Pour $n \geq 5$, $\mathcal{D}(A_n) = A_n$, pour $n \geq 2$, $\mathcal{D}(\sigma_n) = A_n$.*

*Démonstration.* Comme $A_n = \ker\varepsilon$ où $\varepsilon$ est la signature, on a

$$\mathcal{D}(A_n) \subset \mathcal{D}(\sigma_n) \subset A_n$$

Pour $n \geq 5$, $\mathcal{D}(A_n) \lhd A_n$, et $\mathcal{D}(A_n) \neq \{e\}$ car $A_n$ n'est pas abélien, alors,

$$\mathcal{D}(A_n) = \mathcal{D}(\sigma_n) = A_n$$

$\square$

## 3.6 Sous groupes finis de $SO(3)$ : fin

Il reste à voir le cas où $e_1 = 2, e_2 = 3, e_3 = 5, n = 60$.

Orbites : $|O_1| = 30, |O_2| = 20, |O_3| = 12$.

Si $x \in O_1$, alors $G_x = G_{-x}$, puis $-x \in O_1$ car c'est le seule orbite de cardinal 30.

De même pour les autres.

Les pôles opposés sont donc dans une même orbite et on obtient :

15 axes de rotations pour $O_1$ d'angle $\pi$ (ordre 2).

10 axes de rotations pour $O_2$, 10 groupes cyclique d'ordre 3.

6 axes de rotation pour $O_3$, donc 6 groupes cyclique d'ordre 5.

De plus, pour chaque orbite, les stabilisateurs sont conjugués, donc tous les groupes cycliques de même ordres sont conjugués.

On a ainsi :

1 élément d'ordre 1

15 éléments d'ordre 2

20 éléments d'ordre 3

24 éléments d'ordre 5

On a alors tous les éléments de $G$.

Montrer que $G$ est simple :

Soit $H \lhd G$, $H = \{e\}$, si $H$ contient un éléments d'ordre 5, il contient le sous-groupe cyclique qu'il engendre et donc ainsi tous les groupes cycliques d'ordre 5 ($H \lhd G$), d'où 25 éléments dans $H$

De plus, $|H| \mid 60$, $H$ contient aussi un élément d'ordre 2 ou d'ordre 3, alors,

$$|H| = 60, \quad H = G$$

De même, si $H$ contient un élément d'ordre 2, alors il les contient tous, plus $|H| \geq 16$, donc $|H| \in \{20, 30\}$, puis $5 \mid |H|$ et $H$ contient un élément d'ordre 5, situation au-dessus.

Cas restant, $|H| = 3$, impossible car $H$ devrait contenir tous les éléments d'ordre 3.

Conclusion :

$$G \simeq A_5$$

**Retour sur le cas** : $e_1 = 2, e_2 = 3, e_3 = 4, n = 24$,

On a $|O_2| = 8$, si $x \in O_2$ alors $-x \in O_2$, d'où 4 droites déterminées par les éléments de $O_2$.

$g(-x) = -g(x)$, alors $G$ agit sur l'ensemble de ces 4 droites, d'où une application :

$$\varphi : G \to \sigma_4$$

Montrons $\phi$ injectif :

Soit $g \in \ker \varphi$ : $g$ fixe les 4 droites et la restriction de $g$ à chacune des droites est Id ou $-$Id, alors on a

$$g = \mathrm{Id}$$

sur $\mathbb{R}^3$.

Les pôles de $g$ ne sont pas dans $O_2$, car les stabilisateurs d'éléments de $O_2$ sont d'ordre 3, donc l'axe de $g$ n'est pas parmi les 4 droites, donc,

$$z \in O_2 \Rightarrow g(z) = -z$$

Pour $h \in G$, comme $\ker \varphi \lhd G$, alors

$$hgh^{-1} \in \ker \varphi$$

et $hgh^{-1}$ vaut $-$Id sur les 4 droites, donc son axe est le même que celui de $g$, i.e. l'ensemble des pôles de $g$ est stable par $G$. Impossible car il n'y a pas d'orbite de cardinal 2.

Ainsi, $\varphi$ est injectif et on a

$$G \simeq \sigma_4$$

*Remarque.* Ces sous-groupes se réalisent comme groupe d'isométries stabisant les polyèdres réguliers.

**Exemple.** Pour $\sigma_4$, considérons le cube dans $\mathbb{R}^3$, $G$ le groupe des isométries stabiliseur de cube permute les 4 grandes disgonales et ceci donne un isomorphisme avec $\sigma_4$.

# 4 Produit semi direct

Suite exacte de groupes :

$$\{0\} \longrightarrow N \xrightarrow{i} M \xrightarrow{p} P \longrightarrow \{0\}$$

où $N, M, P$ sont trois groupes, $i$ est injectif, $p$ est surjectif, $\operatorname{Im} i = \ker p$, et on a

$$i(N) \lhd M, \quad P \simeq M/i(N)$$

On se demande dans quelles conditions cette suite est scindée, i.e. $\exists s : P \to M$ un morphisme de groupes, tel que

$$p \circ s = \mathrm{Id}_P$$

Si un tel existe, $P_1 := s(P)$ est un sous-groupe de $M$, et le morphisme :

$$p|_{P_1} : P_1 \to P$$

est injective, car si $p_1 = s(x) \in P_1$ et $p(p_1) = e$, alors,

$$x = p \circ s(x) = e \Rightarrow p_1 = s(x) = e$$

i.e. on a un sous-groupe $P_1 \subset M$, tel que

$$p|_{P_1} : \ P_1 \xrightarrow{\sim} P$$

De plus, on peut montrer que

$$P_1 \cap N = \{e\}, \quad M = NP_1 = P_1N$$

Si $x \in P_1 \cap N$, alors $\exists p \in P$, $x = s(p)$ et $e = p(x) = p \circ s(p) = p$, alors $x = e$. (En effet, on a déjà montrer que $p|_{P_1}$ est injective et $P_1 \cap N = \ker p|_{P_1}$.)

Si $m \in M$, alors $p(m) \in P$ et $m' = s \circ p(m) \in P_1$, alors

$$p(m') = p \circ s \circ p(m) = p(m)$$

et alors
$$m'^{-1}m \in \ker p = N(= i(N)) \Rightarrow m \in P_1N$$
alors $M = P_1N$ car $P_1N \subset M$. De même, $M = NP_1$ (ou on peut le voir par le fait que $N \lhd M$).

De plus, comme $N(= i(N))$ est distingué, $P_1$ agit sur $N$ par conjugaison :
$$x \in P_1, \quad xmx^{-1} \in N, \ \forall m \in N$$

Alors, $f : P_1 \to Aut(N)$ groupe des automorphismes de $N$ et pour $x \in P_1$,
$$\begin{aligned} f(x) : N &\to N \\ n &\mapsto xnx^{-1} \end{aligned}$$

on retrouve la loi de groupe de $M$ à partir des lois de $N$, $P_1$ et de $f$.

En effet, l'application
$$\begin{aligned} \varphi : N \times P_1 &\to M \\ (n, x) &\mapsto nx \end{aligned}$$

est bijective. Et pour $n, n' \in N, x, x' \in P_1$,
$$nxn'x' = n(xn'x^{-1})xx', \quad xn'x^{-1} \in N$$

Si on munit $N \times P_1$ de la loi :
$$(n, x) \cdot (n', x') = (n \cdot f(x)(n'), xx')$$

$\varphi$ devient un isomorphisme de groupes.

Ceci sous entend :

**Proposition 4.1.** *L'application*
$$\begin{aligned} (N \times P_1) \times (N \times P_1) &\to N \times P_1 \\ ((n, x), (n', x')) &\mapsto (nf(x)(n'), xx') \end{aligned}$$

*munit $N \times P_1$ une structure de groupe.*

**Définition 4.2.** $N \times P_1$ muni de cette structure de groupe est appelé produit semi-direct de $N$ par $P_1$ via $f$.

Notation : $N \rtimes_f P_1$.

Cadre : 2 groupes $N, P$, un morphisme $f : P \to Aut(N)$.

*Démonstration.* (de la proposition).

Il faut vérifier l'associativie, on utilise que $f$ est un morphisme. □

On a ainsi une construction générale, ce qui nous y a conduit indique que :

avoir une suite exacte scindée équivaut à avoir sur $M$ une structure de produit semi-direct.

En effet, si $M = N \rtimes_f P_1$, alors on constate que le groupe

$$\bar{N} = \{(n, e) \mid n \in N\}$$

est un sous-groupe distingué (isomorphe à $N$), que le groupe

$$\bar{P}_1 = \{(e, x) \mid x \in P_1\}$$

est un sous-groupe de $M$ (isomorphe à $P_1$) et que l'action de $\bar{P}_1$ par conjugaison sur $\bar{N}$ est essentiellement donnée via $f$.

Pour $x \in P_1, n \in N$, on a

$$(e, x)(n, e)(e, x)^{-1} = (f(x)(n), e)$$

le produit semi-direct rend l'action de $P_1$ par automorphismes de $N$ comme une action (de $\bar{P}_1$) par automorphismes intérieur (sur $\bar{N}$).

## 4.1 Situations typiques et exemples

Soient $M$ un groupe, $N, P$ ses sous-groupes tels que :

(1) $N \lhd M$.

(2) $N \cap P = \{e\}$.

(3) $M = NP = PN$.

Alors, $M \simeq N \rtimes_f P$ pour un certain $f$.

En effet, $N \lhd M$, $P$ agit par automorphisme,

$$\begin{aligned} f : P &\to AutN \\ x &\mapsto (n \mapsto xnx^{-1}) \end{aligned}$$

et la loi de $M = NP$ est

$$nxn'x' = n(xn'x^{-1})xx'$$

**Exemple.** (1)

$$\{1\} \longrightarrow A_n \xrightarrow{i} \sigma_n \xrightarrow{\varepsilon} \{\pm 1\} \longrightarrow \{1\}$$

Si $\tau$ est une tranposition, $P = \{\mathrm{Id}, \tau\}$, alors,

$$\sigma_n \simeq A_n \rtimes P$$

$P$ est obtenu par relèvement :

$$\begin{aligned} s : \{\pm 1\} &\to \sigma_n \\ 1 &\to \mathrm{Id} \\ -1 &\to \tau \end{aligned}$$

La suite exaxte est scindée.

(2) Soit $K$ un corps et on considère $GL_n(K)$, on a

$$\{1\} \longrightarrow SL_n(K) \longrightarrow GL_n(K) \xrightarrow{\det} K^* \longrightarrow \{1\}$$

$SL_n(K) = \ker(\det)$.

La suite exaxte est scindée :

$$\begin{aligned} s : K^* &\to GL_n(K) \\ \lambda &\mapsto \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \end{aligned}$$

Alors,

$$GL_n(K) \simeq SL_n(K) \rtimes H$$

où

$$H = \left\{ \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \mid \lambda \in K^* \right\}$$

(3) Groupe diédral

On regarde dans le plan euclidien.

On considère le polygone régulier à $n$ côtés, $p_n$, et le groupe des isométries préservant $p_n$.

Il y a les rotations d'angles $\frac{2k\pi}{n}$, $k \in \{0, \dots, n-1\}$ et les symétriques par rapport aux droites passant par 0 et un sommet ou un milieu des côté.

On appelle $D_n$ ce groupe,

Le groupe des rotations est cyclique d'ordre $n$ et distingué (donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$).

$$\{0\} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_n \xrightarrow{\det} \{\pm 1\} \longrightarrow 1$$

Si $s \in D_n$ symétrie, $P = \{\mathrm{Id}, s\}$ agit sur $\mathbb{Z}/n\mathbb{Z}$, alors,

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

Si $r$ est une rotation, alors $srs^{-1} = r^{-1}$.

**Cas particuliers :**

Soit $N, P$ deux groupes, $f : P \to Aut(N)$, et pour $N \rtimes_f P$ :

$$(n,p) \cdot (n',p') = (nf(p)(n'), pp')$$

• Si $N \times P$ est un produit direct, $f(p) = \text{Id}$, $\forall p$ (action triviale).

• Des morphismes $f$ et $g$ différents peuvent donner des produit semi-directs isomorphes.

Deux situations :

(1) Les actions $f$ et $g$ se correspondent par un automorphisme de $p$,

$$\begin{tikzcd} P \arrow[r, "f"] \arrow[d, "\alpha"'] & Aut(N) \\ P \arrow[ur, "g"'] & \end{tikzcd}$$

où $\alpha \in Aut(P)$ et $g \circ \alpha = f$.

Alors,

$$\begin{aligned} N \rtimes_f P &\to N \rtimes_g P \\ (n,p) &\mapsto (n, \alpha(p)) \end{aligned}$$

est un isomorphisme de groupe.

Appelons $\varphi$ cette application, on a

$$\begin{aligned} \varphi((n,p) \cdot_f (n',p')) &= \varphi(nf(p)(n'), pp') \\ &= (nf(p)(n'), \alpha(pp')) \\ &= (ng \circ \alpha(p)(n'), \alpha(p)\alpha(p') \\ &= (n, \alpha(p)) \cdot_g (n', \alpha(p')) \end{aligned}$$

(2) Soit $h \in Aut(N)$, alors on peut considérer l'automorphisme intérieur de $Aut(N)$ défini par $h$ et si $f : P \to Aut(N)$, on a une autre action g :

$$\begin{aligned} g : P &\to Aut(N) \\ p &\to hf(p)h^{-1} \end{aligned}$$

**Proposition 4.3.** *$N \rtimes_f P \simeq N \rtimes_g P$ via :*

$$\begin{aligned} \theta : N \rtimes_f P &\to N \rtimes_g P \\ (n,p) &\mapsto (h(n),p) \end{aligned}$$

*Démonstration.* Exercice. $\square$

## 4.2 Automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$

Ceci conduit à s'intéresser aux groupes d'automorphismes d'un groupe donné.

$(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par $\bar{1}$, on connaît tous ses générateurs.

**Proposition 4.4.** *Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les $\bar{s}$ où $s \in \mathbb{Z}$ et $s \wedge n = 1$. (Ce sont donc exactement les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$).*

Leur nombre : $\varphi(n)$, fonction d'Euler.

**Proposition 4.5.** *$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})*$ le groupe des éléments inversible pour le produit.*

*Démonstration.* Si $u \in Aut(\mathbb{Z}/n\mathbb{Z})$, $u$ complètement déterminé par $u(1)$ qui doit être un générateurs $u(1) \in (\mathbb{Z}/n\mathbb{Z})^*$.

On voit que l'application :

$$\begin{aligned} Aut(\mathbb{Z}/n\mathbb{Z}) &\to (\mathbb{Z}/n\mathbb{Z})^* \\ u &\mapsto u(1) \end{aligned}$$

est un morphisme.

En effet,

$$u(\bar{s}) = u(1 + \cdots + 1) = \bar{s}u(1)$$

et pour $u, v \in Aut(\mathbb{Z}/n\mathbb{Z})$, on a

$$u \circ v(1) = u(1)v(1)$$

□

On déterminera la structure du groupe $(\mathbb{Z}/n\mathbb{Z})^*$.

**Structure de** $(\mathbb{Z}/n\mathbb{Z})^*$ :

Rappelle : lemme chinois : si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $p_i$ des premiers distincts, alors $\exists$ un isomorphimes d'anneaux :

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

d'où un isomorphisme de groupe :

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

**Proposition 4.6.** *Si $p$ est un premier, alors*

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

*plus généralement, si $F$ est un corps fini de cardinal $q$, alors*

$$F^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$$

*Démonstration.* $|F^*| = q-1$. Soit $x \in F^*$, d'ordre $d \mid q-1$, $x^d = 1$, tout élément $y$ du groupe cyclique $< x >$ est tel que $y^d = 1$.

Ainsi, le polynôme $X^d - 1 \in F[X]$ a exactement pour racines ces $y$ et ce sont ses seules racines, ceci signifie que $F^*$ possède un unique sous-groupe cyclique d'ordre $d$.

Soit $N(d)$ le nombre d'éléments d'ordre $d$ de $F^*$.

On a : $N(d)$ vaut 0 ou $\varphi(d)$ ($\varphi$ est la fonction d'Euler). De plus, on a

$$\sum_{d|q-1} \varphi(d) = q - 1 = \sum_{d|q-1} N(d)$$

alors, on sait que

$$\forall d, \quad \varphi(d) = N(d)$$

En particulier, $N(q-1) = \varphi(q-1) \geq 1$. □

Rappel : on peut calculer le cardinal :

$$|(\mathbb{Z}/p^\alpha\mathbb{Z})^*| = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

**Théorème 4.7.** *Si $p \geq 3$ et $\alpha \geq 2$, alors,*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

*Démonstration.* On va chercher dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ un élément d'ordre $p^{\alpha-1}$ et un élément d'ordre $p-1$. □

**Lemme 4.8.** *Si $k \in \mathbb{N}^*$, alors*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

*avec $\lambda \neq 0$, premier avec $p$.*

*Démonstration.* Par récurrence sur $k$ :

$k = 1$ :

$$(1+p)^p = 1 + C_p^1 p + C_p^2 p^2 + \cdots + p^p$$

on a : Si $1 \leq r \leq p-1$, $p \mid C_p^r$ ; Si $r \geq 2$, $p^3 \mid C_p^r p^r$.

Comme $p \geq 3$, $p^3 \mid p^p$, donc,

$$\begin{aligned}(1+p)^p &= 1 + p^2 + up^3 \\ &= 1 + p^2(1+up)\end{aligned}$$

où on note $\lambda = 1 + up$.

Si c'est vrai pour $k$ : $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, alors,

$$\begin{aligned}(1+p)^{p^{k+1}} &= (1+\lambda p^{k+1})^p \\ &= 1 + \sum_{k=1}^{p-1} C_p^r \lambda^r p^{r(k+1)} + \lambda^p p^{p(k+1)}\end{aligned}$$

pour $r = 1$, $\lambda p^{k+2}$ et pour $r \geq 2$, $p^{k+3}$ est en facteur, alors

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up)$$

$\square$

Conséquence :

$1 + p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^*$ :

$$\begin{aligned}(1+p)^{p^{\alpha-1}} &= 1 + \lambda p^{\alpha} \equiv 1 \mod p^{\alpha} \\ (1+p)^{p^{\alpha-2}} &= 1 + \lambda p^{\alpha-1} \neq 1 \mod p^{\alpha}\end{aligned}$$

*Remarque.*

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p\mathbb{Z} \\ \mathbb{Z}/p^{\alpha}\mathbb{Z} \arrow[ur, "\varphi"'] & \end{tikzcd}$$

$\varphi$ est un morphime surjectif, d'où un morphisme :

$$\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

surjectif.

Soit $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tel que $\psi(x)$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$. Alors, $p-1$ divise l'ordre de $x$. Ainsi, dans le groupe cyclique engendré par $x$, il y a un élément d'ordre $p-1$.

Si $y$ d'ordre $p-1$, alors $(1+p)y$ est d'ordre $p^{\alpha-1}(p-1)$.

En effet :

**Proposition 4.9.** *Soit $G$ un groupe, $a, b \in G$ d'ordres $r$ et $s$, avec $r \wedge s = 1$, $ab = ba$, alors $ab$ est d'ordres $rs$.*

*Démonstration.* On a

$$(ab)^{rs} = a^{rs}b^{rs} = e$$

alors l'ordre de $ab$ divise $rs$.

Si $n$ est l'ordre de $(ab)$, alors

$$(ab)^n = a^n b^n = e \Rightarrow a^n = b^{-n}$$

d'où $a^{ns} = e$, alors $r \mid ns$, et

$$r \wedge s = 1 \Rightarrow r \mid n$$

De même, $s \mid n$, alors $rs \mid n$. □

**Cas** $p = 2$ :

**Proposition 4.10.** $(\mathbb{Z}/2\mathbb{Z})^* \simeq \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z}$, *et pour* $\alpha \geq 3$,

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

**Lemme 4.11.** *Soit $k \in \mathbb{N}^*$, allors*

$$5^{2^k} = 1 + \lambda 2^{k+2}$$

*où $\lambda$ impair.*

*Démonstration.* Par récurrence :

$k=1$, $5^2 = 1 + 3 \cdot 8$.

Si $5^{2^k} = 1 + \lambda 2^{k+2}$, alors,

$$\begin{aligned} 5^{2^{k+1}} &= (1+\lambda 2^{k+2})^2 \\ &= 1 + \lambda 2^{k+3} + \lambda^2 2^{2k+4} \end{aligned}$$

□

*Démonstration.* (de la proposition).

On regarde le morphisme surjectif :

$$\psi : (\mathbb{Z}/2^\alpha\mathbb{Z})^* \to (\mathbb{Z}/4\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z}$$

Si $N = \ker\psi$, $|N| = 2^{\alpha-2}$, mais par le lemme 5 est d'ordre $2^{\alpha-2}$, donc $N$ est cyclique :

$$N \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

et on a une suite exacte :

$$0 \longrightarrow N \longrightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^* \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$, $1 \neq -1 \mod 4$, donc le sous-groupe $\{1,-1\}$ de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ donne une section de $p$, le suite est scindée, donc on a un produit semi direct

$$N \rtimes \mathbb{Z}/2\mathbb{Z}$$

Mais le groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est commutatif, donc produit semi direct est en fait un produit direct, alors,

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

□

## 4.3 Autres exemples

**Proposition 4.12.** *Soit $G$ un groupe abélien, $p$ un nombre premier. On suppose que $\forall x \in G$ et $x \neq e$, $x$ est d'ordre $p$ (on dit que $G$ est d'exposant $p$), alors,*

$$Aut(G) \simeq GL_n(\mathbb{Z}/p\mathbb{Z})$$

*et*

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^n$$

*Démonstration.* $G$ groupe abélien est un $\mathbb{Z}$-module et $p\mathbb{Z} \subset \mathbb{Z}$ :

$\forall x \in G$, $x^p = e$, donc transforme tout élément en le neutre. Ainsi, $\mathbb{Z}/p\mathbb{Z}$ agit sur $G$.

Donc, $G$ est en fait un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel de dimention fini (car $G$ fini), alors,

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^n$$

□

**Applications :** groupes d'ordre $pq$, $p$ et $q$ premier, $p < q$.

**Théorème 4.13.** *Soit $G$ un groupe d'ordre $pq$, $p$ et $q$ premier, $p < q$*

*(1) Si $p \nmid q-1$, alors $G$ est cyclique*

$$G \simeq \mathbb{Z}/pq\mathbb{Z}$$

*(ex. $pq = 15, 35, 51, \dots$)*

*(2) Si $p \mid q-1$, à isomorphisme près, il y a 2 groupes d'ordre $pq$, le groupe cyclique est un produit semi-direct non commutatif.*

*(ex. $pq = 21, 39, \dots$)*

*Démonstration.* Soit $G$ d'ordre $pq$ et soit $Q$ un $q$-sylow :

le nombre de $q$-sylow satisfait :

$$k_q \equiv 1 \mod q$$
$$k \mid p$$

Mais $p < q$, alors $k_q = 1$ : $Q$ est l'unique $q$-sylow, donc $Q \lhd G$ et

$$Q \simeq \mathbb{Z}/q\mathbb{Z}$$

et le quotient

$$G/Q \simeq \mathbb{Z}/p\mathbb{Z}$$

d'où une suite exacte :

$$0 \longrightarrow Q \longrightarrow G \xrightarrow{p} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

On se demande s'il existe une section $s : \mathbb{Z}/p\mathbb{Z} \to G$ ou de façon équivalente, un sous-groupe $H \subset G$, tel que

$$p|_H : H \to \mathbb{Z}/p\mathbb{Z}$$

est un isomorphisme.

Or $G$ possède au moins un $p$-sylpw $P \simeq \mathbb{Z}/p\mathbb{Z}$, $P \cap Q = \{e|$, et

$$p|_P : P \to \mathbb{Z}/p\mathbb{Z}$$

une section, ainsi

$$G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$$

Quels sont à isomorphismes près les produits semi-direct ?

Il faut considérer les morphismes :

$$\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$$

i.e. $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$.

$\varphi$ est trivial ou injectif.

- Si $\varphi$ trivial, le produit est direct et

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}$$

- Si $\varphi$ non trivial, $\varphi(\mathbb{Z}/p\mathbb{Z})$ sous-groupe d'ordre $p$ de $\mathbb{Z}/(q-1)\mathbb{Z}$, donc, on a

$$p \mid q-1$$

$\varphi$ non trivial ne se produit que pour $p \mid q-1$.

Dans ce cas, tous les produits semi-directs non trivaux sont isomorphes.

Ceci repose sur le premier cas d'isomorphisme entre produits simi-directs :

$$\begin{tikzcd} \mathbb{Z}/p\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & \mathbb{Z}/(q-1)\mathbb{Z} \\ \mathbb{Z}/p\mathbb{Z} \arrow[ur, "\psi"'] & \end{tikzcd}$$

alors, $\exists \alpha \in Aut(\mathbb{Z}/p\mathbb{Z})$, tel que $\psi = \varphi \circ \alpha$.

En effet, $\varphi(\mathbb{Z}/p\mathbb{Z})$ et $\psi(\mathbb{Z}/p\mathbb{Z})$ sont des sous-groupes d'ordre $p$ de $\mathbb{Z}/(p-1)\mathbb{Z}$, donc ils sont égaux.

Soit $x$ un générateur de $\mathbb{Z}/p\mathbb{Z}$, $\varphi(x)$ et $\psi(x)$ engendrent le même sous-groupe de $\mathbb{Z}/(q-1)\mathbb{Z}$ d'ordre $p$. Donc, $\exists a \in \{1, \dots, p-1\}$, tel que

$$\psi(x) = \varphi(x)^a = \varphi(x^a)$$

alors $\forall h \in \mathbb{Z}/p\mathbb{Z}$,

$$\psi(h) = \varphi(h^a)$$

et on prend donc $\alpha(h) = h^a$. $\square$

*Remarque.* De même pour $pq^\alpha, \dots$

# 5 Structure des groupes abéliens finis

**Théorème 5.1.** *Soit $A$ un groupe abélien fini, alors $\exists$ des entiers $d_1, \dots d_r \geq 2$ avec $d_1 \mid d_2 \mid \cdots \mid d_r$, tels que*

$$A \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$$

*En particulier, $|A| = d_1 \cdots d_r$ et $\forall x \in A$, $x^{d_r} = e$.*

**Définition 5.2.** Soit $G$ un groupe, l'exposant de $G$ est le ppcm des ordres des éléments de $G$.

**Proposition 5.3.** *$G$ abélien fini $e$ l'exposant de $G$, alors $\exists x \in G$ dont l'ordre est $e$.*

*Remarque.* L'exposant de $G$ est donc aussi le maximum des ordres des éléments de $G$.

*Démonstration.* (de la proposition)

Posons $e = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $p_i$ premier.

$\forall i$, $p_i^{\alpha_i}$ est la plus grande puissance de $p_i$ qui divise l'ordre d'un élément de $G$, donc $\exists x_i \in G$, d'ordre $p_i^{\alpha_i} m_i$ avec $p_i \nmid m_i$.

On considère $y_i = x_i^{m_i}$, alors $y_i$ est d'ordre $p_i^{\alpha_i}$.

Alors $y = y_1 \cdots y_n$ est d'ordre $e$. $\square$

**Définition 5.4.** Soit $A$ un groupe abélien fini, un caractère de $A$ est un morphisme $\chi : A \to \mathbb{C}^*$.

*Remarque.* $\forall x \in A$, $\chi(x)$ est une racine de l'unité. Si $e$ est l'exposant de $A$, $\chi(x)$ est une racine $e$-ième de 1.

**Cas d'un groupe cyclique**

**Définition 5.5.** $\hat{A} = \{\text{caractères de } A\}$

**Proposition 5.6.** *$\hat{A}$ est un groupe pour la loi :*

$$\chi_1, \chi_2 \in \hat{A},\ (\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$$

**Proposition 5.7.** *Si $A$ est cyclique d'ordre $n$, de générateur $a$, alors, l'application*

$$\bar{A} \to \mathbb{U}_n$$
$$\chi \mapsto \chi(a)$$

*est un isomorphisme de groupes.*

*($\mathbb{U}_n$ est le groupe des racines $n$-ième de 1 : $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$).*

*Démonstration.* $\chi(a) \in \mathbb{U}_n$ détermine $\chi$ complètement car $a$ est un générateur. $\square$

**Proposition 5.8.** *(Prolongement des caractères)*

*Soit $A$ un abélien fini, $B \subset A$ le sous-groupe, si $\chi \in \hat{B}$, il exists $\hat{\chi} \in \hat{A}$, tel que*

$$\hat{\chi}|_B = \chi$$

*Démonstration.* Par récurrence sur l'indice $[A : B]$.

• Ok, si $[A : B] = 1$.

• Soit $\chi \in \hat{B}$, soit $x \in A \setminus B$, on veut définir $\chi(x)$.

On regarde l'image de $x$ dans $A/B$. Soit $r$ son ordre, alors $r$ |ordre de $x$ et $x^r \in B$.

Si $s$ est tel que $x^s \in B$, alors $r \mid s$.

On dispose de $\chi(x^r) \in \mathbb{C}^*$.

Soit $\alpha \in \mathbb{C}^*$, tel que $\alpha^r = \chi(x^r)$.

Soit $B'$ le sous-groupe de $A$ engendré par $B$ et $x$ et on prolonge $\chi$ à $B'$ :

Si $y = bx^t$, $b \in B$, $t \in \mathbb{N}$,

$$\hat{\chi}(y) = \chi(b)\alpha^t$$

Ceci est bien défini : si $bx^t = b'x^{t'}$, alors $b'^{-1}b = x^{t'-t} \in B$, alors

$$r \mid t' - t$$

posons $t' - t = ru$, alors

$$\chi(b')\alpha^{t'} = \chi(b')\alpha^{t+ru} = \chi(b')\alpha^t\chi(x^r)^u$$

comme on a

$$b' = bx^{t-t'} = bx^{-ru}$$

alors,

$$\chi(b') = \chi(b)\chi(x^r)^{-u}$$

on a donc,

$$\chi(b')\alpha^{t'} = \chi(b)\alpha^t$$

On vérifie que $\bar{\chi} \in \bar{B}'$, puis comme $[A : B'] < [A : B]$, on applique l'hypothèse de récurrence à $B'$ et on obtient un prolongement. $\square$

*Remarque.* Si $G$ est un groupe cyclique, $G \simeq \mathbb{Z}/n\mathbb{Z}$, alors

$$\hat{G} = \mathbb{U}_n = \mathbb{Z}/n\mathbb{Z}$$

isomorphisme de groupe. $\chi \in \hat{G}$ est complètement déterminé par $\chi(1) \in \mathbb{U}_n$.

**Corollaire 5.9.** *Soit $G$ un abélien. Si $x \in G$, $x \neq e$, alors $\exists \chi \in \hat{G}$, tel que $\chi(x) \neq 1$.*

*Démonstration.* Considérons $H =< x >$ cyclique, on peur choisir $\chi \in \hat{H}$, $\chi(x) \neq 1$, ensuite on peut prolonger $\chi$ à $G$. $\square$

**Théorème 5.10.** *(Théorème de structure)*

*Soit $G$ un abélien fini, alors $\exists d_1 \mid d_2 \mid \cdots \mid d_r$, tels que*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_r\mathbb{Z}$$

*$d_r$ : exposant de $G$.*

*Démonstration.* Posons $n$ le exposant de $G$ et soit $x \in G$ d'ordre $n$.

Soit $H =< x >$ cyclique, on veut trouver un sous-groupe $K$ de $G$ tel que

$$G \simeq K \times H$$

alors, on aura $|K| < |G|$ et on peurra faire une récurrence sur $|G|$.

$H$ est cyclique, soit $\chi \in \hat{H}$ tel que $\chi(x)$ est le racine primitive $n^e$ du 1.

Alors, l'application

$$\begin{aligned} \chi : H &\to \mathbb{U}_n \\ x &\mapsto \xi \end{aligned}$$

est un morphisme bijectif.

Soit $K = \ker \chi \subset G$, on a :

$$K \cap H = \{e\}$$

car $\chi$ est injectif. et on a

$$G = K \cdot H$$

car si $g \in G$, $\chi(g) \in \mathbb{U}_n$ et $\exists k \in \{0, \ldots, n-1\}$ tel que $\chi(g)\chi(x^k$, alors $g \cdot (\chi^k)^{-1} \in K$, d'où isomorphisme

$$\begin{aligned} K \times H &\simeq G \\ (k, h) &\mapsto kh \end{aligned}$$

Par hypothèse de récurrence, $\exists d_1 \mid d_2 \mid \cdots \mid d_{r-1}$ tels que :

$$K \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_{r-1}\mathbb{Z}$$

et de plus, $d_{r-1}$ est l'exposant de $K$ qui divise $n$ (exposant de $G$), d'où le résultat pour $G$.

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_r\mathbb{Z}$$

on note $d_r = n$. $\square$

**Quelques proprités des caractères :**

Soient $G$ un abélien fini et $\hat{G}$ le groupe des caractères.

(1) Si $G$ est cyclique, $G \simeq \hat{G}$.

(2) $\widehat{G_1 \times G_2} \simeq \hat{G}_1 \times \hat{G}_2$ :

Si $\chi \in \widehat{G_1 \times G_2}$, on note pour $g_1 \in G_1, g_2 \in G_2$,

$$\begin{aligned} \chi_1(g_1) &= \chi(g_1, e) \\ \chi_2(g_2) &= \chi(e, g_2) \end{aligned}$$

alors, $\chi_1 \in \hat{G}_1, \chi_2 \in \hat{G}_2$, et on a

$$\chi(g_1, g_2) = \chi_1(g_1) \cdot \chi_2(g_2)$$

(3) Si $G$ abélien, alors $G \simeq \hat{G}$, grâce au théorème de structure.

(4)Bidual

On a un isomorphisme canonique :

$$\begin{aligned}\varphi : G &\to \hat{\hat{G}} \\ x &\mapsto \tilde{x}\ [\chi \mapsto \chi(x)]\end{aligned}$$

En effet :

$$\begin{aligned}\tilde{x}(\chi_1\chi_2) &= \chi_1\chi_2(x) \\ &= \chi_1(x)\chi_2(x) \\ &= \tilde{x}(\chi_1)\tilde{x}(\chi_2)\end{aligned}$$

ainsi, $\tilde{x} \in \hat{\hat{G}}$.

De plus, $\varphi$ est un morphisme de groupe :

on a

$$\begin{aligned}\widetilde{xy}(\chi) &= \chi(xy) \\ &= \chi(x)\chi(y) \\ &= \tilde{x}(\chi)\tilde{y}(\chi) \\ &= (\tilde{x} \cdot \tilde{y})(\chi)\end{aligned}$$

alors,

$$\begin{aligned}\varphi(xy) &= \widetilde{xy} \\ &= \tilde{x} \cdot \tilde{y} \\ &= \varphi(x)\varphi(y)\end{aligned}$$

En plus, ce morphisme est injectif :

Si $x \in G$, $x \neq e$, $\exists \chi \in \hat{G}$ tel que $\chi(x) \neq 1$, i.e. $\tilde{x}(\chi) \neq 1$.

Donc, $\tilde{x}$ n'est pas le neutre.

Comme $|G| = |\hat{G}| = |\hat{\hat{G}}|$, on a bien un isomorphisme.

(5) Relation d'orthogonalité des caractères

Les caractères sont des application : $G \to \mathbb{C}$.

Soit $\mathcal{F}$ l'espace vectoriel des application $f : G \to \mathbb{C}$, c'est un espace vectoriel de dimension finie ($= |G|$).

Relation d'orthogonalité :

Si $\chi_1, \chi_2 \in \hat{G}$, alors

$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)} \chi_2(g) = \begin{cases} 0, & x_1 \neq x_2 \\ 1, & x_1 = x_2 \end{cases}$$

*Remarque.* Comme le module est 1, on a

$$\overline{\chi_1(g)} = \chi_1(g)^{-1} = \chi_1^{-1}(g)$$

Alors,

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)} \chi_2(g) &= \frac{1}{|G|} \sum_{g \in G} \chi_1^{-1}(g) \chi_2(g) \\ &= \frac{1}{|G|} \sum_{g \in G} (\chi^{-1} \chi_2)(g) \end{aligned}$$

Soit $\chi \in \hat{G}$, on note

$$S_\chi = \sum_{g \in G} \chi(g)$$

**Lemme 5.11.** *On a*

$$S_\chi = \begin{cases} |G|, & \chi = 1 \\ 0, & \chi \neq 1 \end{cases}$$

*Démonstration.* On a

$$\forall y \in G, \quad S_\chi = \sum_{x \in G} \chi(xy)$$

En effet, l'application :

$$\begin{aligned} G &\to G \\ x &\mapsto xy \end{aligned}$$

est une bijection, alors

$$\sum_{x \in G} \chi(xy) = \sum_{x' \in G} \chi(x') = S_\chi$$

Alors, on a

$$\begin{aligned} S_\chi &= \sum_{x\in G} \chi(x)\chi(y) \\ &= \big(\sum_{x\in G} \chi(x)\big)\chi(y) \end{aligned}$$

donc,

$$S_\chi = S_\chi \cdot \chi(y), \quad \forall y \in G$$

- Si $\chi \neq 1$, $\exists y$, tel que $\chi(y) \neq 1$ et alors $S_\chi = 0$.
- Si $\chi = 1$, alors $S_\chi = |G|$. □

*Remarque.* On a fait une moyenne sur tous les éléments de $G$.

# 6 Classification des groups d'ordre petit

Bilan :

(1) Groupes abéliens finis.

(2) Constructions : produits semi-directs :

$$H \to \mathrm{Aut}(N), \quad N \rtimes H$$

**Exemple.** Groupes d'ordre $pq$, $p < q$, $p, q$ premier.

**Classification des groupes d'ordre $\leq 15$ :**

• $n = 1$ : $\{e\}$.

• $n \leq 15$ et $n$ premier $(n = 2, 3, 5, 7, 11, 13)$ :

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

• $n = pq$, $p < q$, $p, q$ premier $(n = 6, 10, 14, 15)$ : déjà vu.

Cas restant : $n = 4, 8, 9, 12$.

• $n = 4$ :

$$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

*Remarque.* Un groupe fini dans lequel tous les éléments sont d'ordre 1 ou 2 est abélien.

• $n = 9 = 3^2$ :

Si $p$ est premier, un groupe d'ordre $p^2$ est abélien, d'où

$$\mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

• $n = 8$ :

(1) Cas abéliens :

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

(2) Cas non abélien :

Les éléments $\neq e$ sont d'ordre 2 ou 4.

Ils ne peuvent pas être tous d'ordre 2 car $G$ non abélien. Donc, il existe un élément d'ordre 4.

Soit $H \simeq \mathbb{Z}/4\mathbb{Z}$ le sous-groupe qu'il engendre, alors, comme $[G : H] = 2$, on a

$$H \lhd G$$

et alors

$$0 \longrightarrow H \longrightarrow G \longrightarrow G/H(\simeq \mathbb{Z}/2\mathbb{Z}) \longrightarrow 0$$

Cette suite est-elle scindée ?

C'est le cas si et seulement s'il existe un élément d'ordre 2 dans $G - H$.

On a alors un produit semi-direct :

$$\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

via un morphisme

$$\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$$

donc soit $\varphi$ est trivial, soit $\varphi =$Id.

Si $\varphi$ est trivial : cas commutatif.

Sinon, on a un vrai produit semi-direct : groupe diédral.

<u>2$^e$ situation</u> : Il n'existe pas d'éléments d'ordre 2 dans $G - H$.

Ainsi $\alpha^2 \in H$ est le seul élément d'ordre 2 de $G$, alors $\alpha^2$ est dans le centre de $G$ : $\forall g \in G$, $g\alpha^2 g^{-1}$ est d'ordre 2, d'où

$$g\alpha^2 g^{-1} = \alpha^2$$

Considérons $G - H$, il y a 4 éléments d'ordre 4, soit $J$ est l'un d'eux, alors $J^2$ est d'ordre 2, alors,

$$J^2 = \alpha^2$$

Posons $\alpha^2 = -1$, alors

$$H = \{1, -1, \alpha, -\alpha\}$$
$$G = \{1, -1, \alpha, -\alpha, J, -J, \alpha J, -\alpha J\}$$

et on a

$$\alpha J \alpha J = (\alpha J)^2 = -1 = \alpha^2$$

alors,

$$J\alpha J = \alpha$$

Soit $K = \alpha J$, $I = \alpha$, on reconnaît la loi de multiplication des quaternions $I, J, K$.

Le groupe d'ordre 8 obtenu est le groupe des quaternions :

$$\mathbb{H}_8 =< 1, I, J, K >$$

Est-ce que $\mathbb{H}_8$ est isomorphe au produit semi-direct obtenu ci-dessus ? Non, car $\mathbb{H}_8$ n'est pas isomorphe à un produit semi-direct.

**Proposition 6.1.** $\mathbb{H}_8$ *n'est pas isomorphe à un produit semi-direct.*

*Démonstration.* Si c'était le cas, il y aurait $N \lhd \mathbb{H}_8$ et $K$ un sous-groupe, tel que

$$\mathbb{H}_8 \simeq N \rtimes K$$

et soit $|N| = 4$, soit $|N| = 2$.

• Si $|N| = 4$, $|K| = 2$, alors $K = \{1, k\}$ avec $k^2 = 1$. Mais dans $\mathbb{H}_8$, il y a un unique élément d'ordre 2, qui est $-1$.

Dans $N$, il y a nécessairement des éléments d'ordre 2 : $h \in \mathbb{N}$.

Contradictoire avec $N \cap K = \{e\}$.

• Si $|N| = 2$, alors $N = \{1, -1\}$ qui est central, donc le produit semi-direct est en fait un produit direct de 2 groupes abéliens, ceci dirait que $\mathbb{H}_8$ abélien, ce qui est faux. □

**cas** $n = 12$ **:**

• Groupes abéliens :

$$\mathbb{Z}/12\mathbb{Z}, \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

• Groupes non abéliens : $12 = 2^2 \cdot 3$.

On regarde les 3-sylows, soit $n_3$ leur nombre, alors,

$$n_3 \equiv 1 \mod 3$$
$$n_3 \mid 4$$

alors, $n_3 \in \{1, 4\}$.

$\underline{1^{er} \text{ cas}}$ $n_3 = 4$ : 4 groupes cycliques d'ordre 3 qui ne s'intersectent qu'en $\{e\}$, d'où 8 éléments d'ordre 3 dans $G$, les 4 autres éléments forment nécessairement un 2-sylow.

Alors, $N \cap K = \{e\}$, on a donc

$$G \simeq N \rtimes K$$

Il y a 2 situations :

(1) Si $N \simeq \mathbb{Z}/4\mathbb{Z}$, alors $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ et tout morphisme de $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ est trivial.

Dans ce cas, on a un produit direct, qui est abélien.

(2) $N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \simeq GL_2(\mathbb{F}_2)$.

On a

$$|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 6$$

d'où

$$GL_2(\mathbb{F}^2) \simeq \sigma_3$$

car il est non abélien.

On recherche les morphismes non trivaux :

$$\varphi : \mathbb{Z}/3\mathbb{Z} \to \sigma_3$$

$\varphi$ est déterminé par $\varphi(1)$, qui doit être un 3-cycle.

Alors,

$$\varphi(1) = (123) \text{ ou } (132)$$

($A_3 \subset \sigma_3$ est l'unique sous-groupe d'indice 2).

Les 2 morphismes possibles $\varphi_1$ et $\varphi_2$ ne différent que par un automorphisme de $\mathbb{Z}/3\mathbb{Z}$, alors

$$\varphi_2 = \varphi_1 \circ \varphi,\ \varphi(1) = 2$$

Les produits semi-direct

$$(\mathbb{Z}/2\mathbb{Z})^2 \rtimes_{\varphi_1} \mathbb{Z}/3\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_{\varphi_2} \mathbb{Z}/3\mathbb{Z}$$

sont isomorphes et en fait isomorphes à

$$A_4 = V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$$

<u>$2^e$ cas</u> $n_3 = 1$.

Soit $N$ l'unique 3 sylow, $N \lhd G$, soit $H \subset G$ un 4-sylow, donc $N \cap H = \{e\}$, donc

$$G \simeq N \rtimes H$$

via un morphisme :

$$\varphi : H \to \mathrm{Aut}(N) \simeq \mathbb{Z}/4\mathbb{Z}$$

Ici $|H| = 4$, donc on a 2 possibilités.

(a) $H = \mathbb{Z}/4\mathbb{Z}$, il y a un unique morphisme non trivial $H \to \mathbb{Z}/2\mathbb{Z}$, d'où

$$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$$

(b) $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^2$.

On cherche

$$\varphi : H \to \mathbb{Z}/2\mathbb{Z}$$

ce qui revient à donner les formes linéaires sur le $\mathbb{Z}/2\mathbb{Z}$ espace vectoriel $(\mathbb{Z}/2\mathbb{Z})^2$.

Il y en 3 non nulles : $(1,0), (0,1), (1,1)$. Mais elle se correspondent via des automorphismes de $H$ :

$$(1,0) = (0,1)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$(1,1) = (0,1)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Donc, les 3 produits semi-directs sont isomorphes :

$$\mathbb{Z}/3\mathbb{Z} \rtimes V_4$$

Bilan :

$V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$ : quatre 3-sylows

$\mathbb{Z}/3\mathbb{Z} \rtimes V_4$ : un seul 3-sylow, n'a pas d'élément d'ordre 4.

$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ : un seul 3-sylow, a des éléments d'ordre 4.

Ils ne sont pas isomorphes.

# 7 Groupe linéaire et Groupe spécial linéaire

Soient $K$ un crops et $E$ un $K$-espace vectoriel de dimension finie $n$. On a

$$GL(E) \simeq GL_n(K)$$

une fois fixée une base de $E$.

Un morphisme :

$$\det : GL_n(K) \to K^*$$

et on note

$$SL_n(K) = \ker(\det)$$

le groupe spécial linéaire.

**Suite exacte scindée :**

$$1 \longrightarrow SL_n(K) \longrightarrow GL_n(K) \xrightarrow{\det} K^* \longrightarrow 1$$

et on a

$$H = \left\{ \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \mid \lambda \in K^* \right\} \subset GL_n(K)$$

**Centre :**

**Proposition 7.1.** *Pour le centre, on a*

$$\begin{aligned} Z(GL_n(K)) &= K^* Id \\ Z(SL_n(K)) &= SL_n(K) \cap Z(GL_n(K)) \\ &= \mu_n(K) Id \end{aligned}$$

*où*

$$\mu_n(K) = \{\textit{racines } n^e \textit{ de 1 dans } K\}$$

Ceci repose sur :

**Proposition 7.2.** *Soit $u \in End(E)$, tel que $\forall x \in E$, $x$ et $u(x)$ colinéaires, alors $u$ est une homothétie.*

**Générateurs :**

• Matrices de transvections élémentaires :

$$E_{ij}(\lambda) = \mathrm{Id} + \lambda E_{ij},\ \ \lambda \in K^*,\ \ i \neq j$$

$E_{ij}$ : tous les coefficients sont nuls sauf $(i, j)$, qui vaut 1.

• Matrices de dilatation :

$$\begin{array}{cc} & \begin{array}{ccccccc} \phantom{1} & \phantom{\ddots} & \phantom{1} & i & \phantom{1} & \phantom{\ddots} & \phantom{1} \end{array} \\ i & \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array} = D_i(\lambda),\ \ \lambda \in K^*$$

Les opérations élémentaires sur les lignes ou les colonnes d'une matrice et l'algorithme du pivot de Gauss donnent :

**Théorème 7.3.** *Soit $g \in GL_n(K)$, alors il existe un produit $L$ de matrices de transvections élémentaires tel que*

$$g = L \cdot diag(1, \ldots, 1, \det g)$$

**Corollaire 7.4.** *(1) $GL_n(K)$ est engendré par les transvections élémentaires et les dilatations.*

*(2) $SL_n(K)$ est engendré par les transvections élémentaires.*

**Propriétés des $E_{ij}(\lambda)$ :**

(1) Un morphisme de groupe :

$$\begin{aligned} (K, +) &\to GL_n(K) \\ \lambda &\mapsto E_{ij}(\lambda) \end{aligned}$$

(2) Si $\omega \in \sigma_n$, soit $P_\omega \in GL_n(K)$ une matrice de permutation, alors,

$$P_\omega E_{ij}(\lambda) P_\omega^{-1} = E_{\omega(i)\omega(j)}(\lambda)$$

(3) On a

$$D_i(\lambda)E_{ij}(\mu)D_i(\lambda)^{-1} = E_{ij}(\lambda\mu)$$

Ainsi, les $E_{ij}(\lambda)$ sont conjuguées dans $GL_n(K)$ et si $n \geq 3$, elles sont conjuguées dans $SL_n(K)$.

*Démonstration.* (Preuve pour $SL_n(K)$) : Si $\det(P_\omega) = \varepsilon(\omega) = -1$, on peut corriger en conjuguant par un matrice $D_l(-1)$, $l$ convenable, $l \neq i$, $l \neq j$.

On peut aussi utiliser, au lieu de $D_i(\lambda)$, des matrices :

$$\begin{array}{cc} & \begin{matrix} \phantom{1} & \phantom{\ddots} & \phantom{1} & i & \phantom{1} & \phantom{\ddots} & \phantom{1} & l & \phantom{1} & \phantom{\ddots} & \phantom{1} \end{matrix} \\ \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ l \\ \\ \\ \\ \end{matrix} & \begin{pmatrix} 1 &&&&&&&&&& \\ & \ddots &&&&&&&&& \\ && 1 &&&&&&&& \\ &&& \lambda &&&&&&& \\ &&&& 1 &&&&&& \\ &&&&& \ddots &&&&& \\ &&&&&& 1 &&&& \\ &&&&&&& \lambda^{-1} &&& \\ &&&&&&&& 1 && \\ &&&&&&&&& \ddots & \\ &&&&&&&&&& 1 \end{pmatrix} \end{array}, \ l \neq i, \ l \neq j$$

□

**Proposition 7.5.** *(1) Pour $n = 2$, les matrices $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées dans $SL_2(K)$ si et seulement si $\frac{\lambda}{\mu}$ est un carré dans $K$.*

*(2) On a*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}$$

*Démonstration.* Exercice. □

(4) Si $i, j, k$ est deux à deux différent, alors,

$$[E_{ij}(\lambda), E_{jk}(\mu)] = E_{ik}(\lambda\mu)$$

*Démonstration.* Exercice. □

**Groupes dérivés** :

**Théorème 7.6.** *(1) Sauf pour $n = 2$, $K = \mathbb{F}_2$,*

$$D(GL_n(K)) = SL_n(K)$$

*(2) Sauf pour $n = 2$, $K = \mathbb{F}_2$ ou $\mathbb{F}_3$,*

$$D(SL_n(K)) = SL_n(K)$$

*Démonstration.* Comme on sait que $SL_n(K) \subset GL_n(K)$ et $GL_n(K)/SL_n(K) \simeq K^*$ est abélien, on a

$$D(SL_n(K)) \subset D(GL_n(K)) \subset SL_n(K)$$

• Pour $n \geq 3$, on a

$$\forall i \neq j \neq k \neq i,\ [E_{ij}(\lambda), E_{jk}(1)] = E_{ik}(\lambda)$$

donc, on obtient

$$SL_n(K) \subset D(SL_n(K))$$

d'où (1) et (2).

• Pour $n = 2$ et $|K| > 3$, on obtient $E_{12}(\lambda)$ et $E_{21}(\lambda)$ comme commutateur,

$$\begin{aligned}\begin{pmatrix}\beta & 0\\ 0 & \beta\end{pmatrix}\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}\begin{pmatrix}\beta^{-1} & 0\\ 0 & \beta\end{pmatrix}\begin{pmatrix}1 & -\lambda\\ 0 & 1\end{pmatrix} &= \begin{pmatrix}1 & \beta^2\lambda\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -\lambda\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & \lambda(\beta^2-1)\\ 0 & 1\end{pmatrix}\end{aligned}$$

Si $|K| > 3$, $\exists \beta \in K \setminus \{0, 1-1\}$, d'où $\beta^2 - 1 \neq 0$.

Si $\mu \in K$, on pose $\lambda = \frac{\mu}{\beta^2-1}$, alors,

$$E_{12}(\mu) = \Big[\begin{pmatrix}\beta & 0\\ 0 & \beta^{-1}\end{pmatrix}, E_{12}(\lambda)\Big]$$

ceci donne (2).

Pour $n = 2$, $K = \mathbb{F}_2, \mathbb{F}_3$ (cas particulier).

On a

$$|SL_2(\mathbb{F}_2)| = \frac{(2^2-1)(2^2-2)}{1} = 6$$

non abélien, alors, on obtient

$$SL_2(\mathbb{F}_2) \simeq \sigma_3$$

De plus, on a

$$D(\sigma_3) = A_3$$

d'où le cas exclus.

Et $|GL_2(\mathbb{F}_2)| = |SL_2(\mathbb{F}_2)|$.

Il reste le cas où $n = 2$, $K = \mathbb{F}_3$. $\square$

## 7.1 Question de simplicité

On sait déjà :

$$Z(GL_n(K)) \simeq K^*$$
$$Z(SL_n(K)) = SL_n(K) \cap Z(GL_n(K))$$

On s'intérèsse aux groupes quotients :

**Définition 7.7.** On note

$$PGL_n(K) = GL_n(K)/Z(GL_n(K))$$
$$PSL_n(K) = SL_n(K)/Z(SL_n(K))$$

Le groupe $GL_n(K)$ agit dans $K^n$ et donc aussi sur $\mathbb{P}(K^n)$, l'ensemble des droites de $K^n$, de même pour $SL_n(K)$.

*Remarque.* Ces actions sont transitives et même 2 fois transitive

**Définition 7.8.** Soit $G$ un groupe agissant sur un ensemble $X$, on sit que l'action est 2 fois transitive, si pour $\forall x_1, x_2 \in X$, $\forall y_1 \neq y_2 \in X$, il existe $g \in G$, tel que

$$g(x_1) = y_1, \quad g(x_2) = y_2$$

Ici, $SL_n(K)$ agit 2 fois transitivement sur $\mathbb{P}(K^n)$ (aussi noté $\mathbb{P}^{n-1}(K)$), ceci résulte essentiellement du théorème de la base incomplète.

Prenons $e_1$ et $e_2$ deux vecteurs non colinéaire (i.e. deux droites $ke_1$ et $ke_2$ sont distinctes) et de même 2 autres droites distinctes de vecteurs directeurs $f_1$ et $f_2$ (donc non colinéaires)

Alors, on peut compléter $(e_1, e_2)$ en une base $(e_1, \ldots, e_n)$ et $(f_1, f_2)$ en une base $(f_1, \ldots, f_n)$.

Alors, $\exists A \in GL_n(K)$, tel que

$$Ae_i = f_i, \quad \forall i$$

Soit $B \in GL_n(K)$ et

$$Bf_1 = \frac{1}{\det A} f_1, \quad Bf_i = f_i, \ \forall i \geq 2$$

Alors, $B \times A \in SL_n(K)$ et envoie $ke_1$ sur $kf_1$ et $ke_2$ sur $kf_2$.

**Définition 7.9.** Soit $G$ un groupe, un sous-groupe $H$ de $G$ est dit maximal si les seuls sous-groupes de $G$ qui le contiennent sont $H$ et $G$, i.e. si $K \subset G$ un sous-groupe et $H \subset K \subset G$, alors, on a

$$K = H \text{ ou } K = G$$

**Proposition 7.10.** *Soit $G$ un groupe agissant sur un ensemble $X$ 2 fois transitivement, alors le stabilisateur de tout $x \in X$ est un sous-groupe maximal : $\forall x \in X$, $stab(x) = G_x$ est maximal.*

*Démonstration.* On a que l'action est transitive, donc on sait que

$$X = \text{orbite}(x) \simeq G/G_x$$

et l'actions de $G$ sur $X$ se transforme en l'action à gauche de $G$ sur $G/G_x$.

Maintenant montrons que $G_x$ est maximal :

Sinon, $\exists$ un sous-groupe $K$ de $G$ avec $G_x \subsetneqq K \subsetneqq G$, donc $\exists k \in K - G_x$ et $\exists g \in G - K$.

On regarde, dans $G/G_x$, les éléments : $G_x, kG_x, gG_x$, par double transitivité de l'action de $G$, $\exists u \in G$, tel que

$$u(G_x) = G_x,\ u(kG_x) = gG_x$$

Alors, on a

$$uG_x = G_x \Rightarrow u \in G_x$$
$$ukG_x = gG_x \Rightarrow g^{-1}uk \in G_x$$

Mais, $uk \in K$ car $G_x \subset K$, donc $g^{-1}uk \in K$ et $g \in K$, c'est une contradiction. □

**Théorème 7.11.** *Sauf pour $n = 2$ et $K = \mathbb{F}_2$ ou $\mathbb{F}_3$, le groupe $PSL_n(K)$ est simple.*

*Démonstration.* Par l'absurde, on utilise la correspondance bijective entre sous-groupes distingués de $PSL_n(K)$ est sous-groupes distingués de $SL_n(K)$ contenant le centre $Z(SL_n(K))$.

Soit $N \lhd SL_n(K)$ contenant le centre $Z$.

<u>$1^{er}$ cas</u> :

Supposons qu'il existe une droite vectorielle stable par tous les éléments de $N$, alors toutes les droites vectorielles sont stables par $N$. En effet, $\forall s \in SL_n(K)$, on a

$$sNs^{-1} = N$$

Par ailleurs, $SL_n(K)$ agit transitivement sur l'ensemble des droits.

Si $D$ est la droites stable par $N$ et si $D'$ est une autre droite, alors, $\exists s \in SL_n(K)$, tel que

$$D = s(D')$$

Mais alors, on a

$$\mathrm{stab}(D') = s \cdot \mathrm{stab}(D) \cdot s^{-1}$$

comme $N \subset \mathrm{stab}(D)$, on a

$$N = sNs^{-1} \subset \mathrm{stab}(D')$$

Conclusion : si $\exists$ une droite stable par tous les éléments de $N$, alors toutes les droites sont stable par chaque élément de $N$ et donc $\forall n \in N$, $n$ est une homothétie, donc $N = Z$.

<u>$2^e$ cas</u> :

Aucune droite n'est stable par tous les éléments de $N$.

Fixons $(e_1, \ldots, e_n)$ une base standard de $K^n$, soit $P = \mathrm{stab}(ke_1)$, alors on a

$$P = \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \in SL_n(K) \right\}$$

alors $N \not\subseteq P$.

Le sous-groupes engendré par $N$ et $P$ sont $NP$ qui contient $P$ strictement :

$$P \subsetneqq NP \subset SL_n(K)$$

Or, comme $SL_n(K)$ agit 2 fois transitivemnt sur l'ensemble droites, on sait que $P$ est un sous-groupe maximal car c'est un stabilisateur, alors, on a

$$NP = SL_n(K)$$

Comme $N \lhd SL_n(K)$, on regarde le quotient :

$$\pi : SL_n(K) \to SL_n(K)/N$$

alors, on a

$$\pi(P) = NP/N = SL_n(K)/N$$

Considère le sous groupe $K$ de $P$ et

$$K = \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ & 1 & 0 & \cdots & 0 \\ & & 1 & \cdots & 0 \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix} \right\}$$

$K$ est un sous-groupes commutatif de $P$ et $K \subset P$.

$K$ est engendré par les transvection élémentaire $E_{12}(\lambda), E_{13}(\lambda), \ldots, E_{1n}(\lambda)$.

On regarde :

$$\pi(K) = KN/N = \pi(KN)$$

Comme $K \triangleleft P$, on a

$$\pi(K) \subset \pi(P) = SL_n(K)/N$$

donc $\pi(K)$ est distingué dans $SL_n(K)/N$ et en vertu du théorème de correspondance, on a

$$KN \triangleleft SL_n(K)$$

Or les $E_{1j}(\lambda) \in K$, $\forall j \in \{1, \ldots, n\}$, donc tous leurs conjugués sont dans $KN$.

Mais, les sous-groupes à un paramètre $\lambda \mapsto E_{1j}(\lambda)$ sont toujours conjugués dans $SL_n(K)$. [OK, si $n \geq 3$ via les matrices de permutations et les $D_i(\lambda)$, mais pour $n = 2$, on a

$$P_\sigma E_{ij}(\lambda) P_\sigma^{-1} = E_{\sigma(i)\sigma(j)}(\lambda)$$

si $\det(P_\sigma) = -1$, on a

$$D_1(-1) P_\sigma E_{ij}(\lambda) P_\sigma^{-1} D_1(-1) = E_{\sigma(i)\sigma(j)}(\lambda)$$

et $D_1(-1)P_\sigma \in SL_n(K)$.]

Ainsi, tous les générateurs $E_{ij} \in KN$, d'où $KN = SL_n(K)$.

Intéret : $K$ est abélien, le morphisme :

$$\pi|_K : K \to SL_n(K)/N$$

est surjectif, alors $SL_n(K)/N$ est abélien, donc $D(SL_n(K)) \subset N$.

Or, sauf pour $n = 2$ et $K = \mathbb{F}_2$ ou $\mathbb{F}_3$, $D(SL_n(K)) = SL_n(K)$, contradiction. $\square$

Étude des cas $n = 2$, $K = \mathbb{F}_2$ ou $\mathbb{F}_3$.

(1) $n = 2$, $K = \mathbb{F}_2$, on a vu

$$GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \sigma_3$$

non simple.

(2) $n = 2$, $K = \mathbb{F}_3$.

On va utiliser l'action de $GL_n(K)$ ou $SL_n(K)$ sur $\mathbb{P}^{n-1}(K)$ :

$$\varphi : GL_n(K) \to \sigma(\mathbb{P}^{n-1}(K))$$

et

$$\ker \varphi = \{g \in GL_n(K) \mid \varphi(g) = \mathrm{Id}\} = K^*\mathrm{Id}$$

$\varphi$ passe au quotient par le centre et donne une action fidèle de $PGL_n(K)$ sur $\mathbb{P}^{n-1}(K)$.

Cas des corps fini :

On connaît les corps $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$, $p$ est premier.

On prend $n = 2$, on a

$$PGL_2(\mathbb{F}_p) \to \sigma(\mathbb{P}^1(\mathbb{F}_p))$$

Or, $|\mathbb{P}^1(\mathbb{F}_p)| = p + 1$. En effet, se donner une droite, c'est se donner un vecteur $\neq 0$ (il y a $p^2 - 1$ possibilités) à un multiple non nul près (division par $p - 1$), ainsi, on a un morphisme injectif :

$$\varphi : PGL_2(\mathbb{F}_p) \to \sigma_{p+1}$$

Pour $p = 3$, on a

$$|PGL_2(\mathbb{F}_p)| = \frac{(p^2-1)(p^2-p)}{p-1} = (p-1)p(p+1)$$

ici, $|PGL_2(\mathbb{F}_3)| = 24 = |\sigma_4|$, d'où
$$PGL_2(\mathbb{F}_3) \simeq \sigma_4$$

$PSL_2(\mathbb{F}_3)$ est l'image de $SL_2(\mathbb{F}_3)$, c'est un sous-groupe d'indice 2, d'où

$$PSL_2(\mathbb{F}_3) \simeq A_4$$

On voit que $n = 2$, $K = \mathbb{F}_3$ est bien exclu du théorème car $A_4$ n'est pas simple :

$$V \lhd A_4$$

*Remarque.* (Au sujet des groupes dérivés)

Il restait à traiter :
$$D(GL_2(\mathbb{F}_3)) = SL_2(\mathbb{F}_3)$$

On a
$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^2 = \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$$
dans $GL_2(\mathbb{F}_3)$, d'où

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1} \in D(GL_n(\mathbb{F}_3))$$

## 7.2 Complément : Interprétation géométrique des transvections et des dilatations

$E = K^n$, on considère les $u \in GL(E)$, $u \neq$Id qui laissent stables un hyperplan $H$ point par point, i.e. $u|_H =$Id$_H$.

2 situations possibles :

**Proposition 7.12.** *Sous les hypothèses ci-dessus, les conditions suivantes sont équivalentes :*

*(1)* $\det u = \lambda \neq 1$.

*(2) $u$ diagonalisable.*

*(3)* $\mathrm{Im}(u - Id) \cap H = 0$.

*(4) Dans une base convenable, la matrice de $u$ est*

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \lambda \end{pmatrix}$$

**Proposition 7.13.** *Sous les hypothèses ci-dessus, les conditions suivantes sont équivalentes :*

*(1)* $\det(u) = 1$.

*(2) $u$ n'est pas diagonalisable.*

*(3)* $\mathrm{Im}(u - Id) \subset H$.

*(4) Dans une base convenable, la matrices de $u$ est*

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix} = E_{n-1,n}(1)$$

En effet, soir $v \in E - H$, $(e_1, \ldots, e_{n-1})$ une base de $H$.

Alors, dans la base $(e_1, \ldots, e_{n-1}, v)$ la matrice de $u$ est :

$$\left(\begin{array}{ccc|c} 1 & & & * \\ & \ddots & & \vdots \\ & & 1 & * \\ \hline & & & \lambda \end{array}\right)$$

$\det u = \lambda$.

Si $\lambda \neq 1$, alors $u$ est diagonalisable, car 1 est valeur propre de multiplicité 1 (espace propre $H$) et $\lambda$ est valeur propre.

Si $\lambda = 1$, alors $u$ ne peut pas être diagonalisable car 1 est le seule valeurs propre possible et $u \neq$Id.

**Exercice 7.14.** Terminer/donner les détails de la preuve.

## Deuxième partie

# Algèbre linéaire

## 8 Réduction de Jordan

Soient $K$ un corps, $E$ un $K$-espace vectoriel de dimension finie.

**Théorème 8.1.** *Soit $u$ un endomorphisme de $E$ ($u \in \mathcal{L}(E)$) dont le polynôme caractéristique est scindé. Alors, il existe une base de $E$, dans laquelle la matrice de $u$ est diagonale par bloc, avec des blocs de la forme :*

$$J_{\lambda,r} = \underbrace{\left.\begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}\right\} r}_{r} \quad , \quad \lambda \in K$$

*De plus, l'ensemble (avec multiplicité) des couples $(\lambda, r)$ qui apparaissent ne dépend que de $u$ (et pas de la base).*

*Démonstration.* Outils : théorème de Cayley Hamelton.

Soit $\chi$ le polynôme caractéristique de $u$, alors

$$\chi(u) = 0$$

On décompose $\chi$ en produit de polynôme irréductibles :

$$\chi(X) = P_1(X)^{\alpha_1} \cdots P_s(X)^{\alpha_s}$$

où les $P_i$ sont irréductibles et 2 à 2 distincts.

Par le lemme des noyaux, on a

$$\ker \chi(u) = \bigoplus_{i=1}^{s} \ker(P_i^{\alpha}(u))$$

Ici, $\chi$ est scindé, $P_i(X) = X$, et on a

$$\ker P_i^{\alpha_i}(u) = \ker(u - \lambda_i \mathrm{Id})^{\alpha_i}$$

est un sous-espace caractéristique.

On se ramène à étudier dans chaque sous-espace caractérisitique, où

$$u = \lambda_i \mathrm{Id} + n_i$$

avec $n_i^{\alpha_i} = 0$, i.e. $n_i$ est un endomorphisme nilpotent.

Ainsi, on se ramène à montrer le théorème pour les endomorphismes nilpotents.

Situation : $E$ un e.v. de dimention $n$, $u \in \mathcal{L}(E)$ avec $u^s = 0$, $u^{s-1} \neq 0$. ($s$ est l'indice de nilpotence de $u$).

Comme $u^{s-1} \neq 0$, $\exists x \in E$, $u^{s-1} \neq 0$.

**Lemme 8.2.** *$x, u(x), \ldots, u^{s-1}(x) \neq 0$ sont linéairement indépendants.*

*Démonstration.* Par l'absurde s'il existe $a_0, a_1, \ldots, a_{s-1} \in K$, tels que

$$a_0 x + a_1 u(x) + \cdots a_{s-1} u^{s-1}(x) = 0$$

on applique $u^{s-1}$, on obtient

$$a_0 u^{s-1}(x) = 0$$

d'où $a_0 = 0$.

On recommence en appliquant $u^{s-2}$, d'où $a_1 = 0$.

Et on poursuit. □

Alors, on pose

$$E_1 = \mathrm{Vect}(u^{s-1}(x), u^{s-2}(x), \ldots, x)$$

alors, $\dim E_1 = s$.

Et la matrice de la restriction de $u$ à $E_1$ dans la base $(u^{s-1}, \ldots, x)$ est le bloc de Jordan $J_{0,s}$.

On va établir le théorème par récurrence sur $\dim E$.

- $\dim E = 1$, OK.

• Si c'est vrai au rang $n-1$, on commence par construire le sous-espace $F_1$ comme ci-dessus (si $u \neq 0$, $s \geq 2$).

On cherche un supplémentaire à $F_1$, qui soit stable par $u$, ainsi, on pourra lui appliquer l'hypothèse de récurrence.

Idée : utiliser la dualité et les sous-espace orthogonaux entre $E$ et $E^*$.

Comme $u^{s-1}(x) \neq 0$, $\exists \varphi \in E^*$, telle que

$$\varphi(u^{s-1}(x)) \neq 0$$

On dispose de ${}^t u : E* \to E^*$, on a

$$({}^t u)^s = 0,\ ({}^t u)^{s-1} \neq 0$$

ainsi, on a

$$({}^t u)^{s-1}(\varphi) \neq 0$$

Soit $G$ le sous-espace vectoriel de $E^*$ engendré par $\varphi, {}^t u(\varphi), ({}^t u)^{s-1}(\varphi)$. On a (comme pour $F_1$ ci-dessus), $\dim G = s$ et de plus, $G$ est stable par ${}^t u$ (car $({}^t u)^s = 0$).

$$\mathrm{Mat}({}^t u, (({}^t u)^{s-1}(\varphi), \ldots, \varphi)) = J_{0,s}$$

Alors, l'orthogonal de $G$ dans $E$, i.e.

$$F = \{y \in E \mid \forall k \in \{0, \ldots, s-1\}, ({}^t u)^k(\varphi)(y) = 0\}$$

est un sous-espace vectoriel de dimension $n-s$, stable par $u$.

Il suffit de montrer que $F \cap F_1 = 0$ et on aura

$$E = F_1 \oplus F$$

avec $F$ stable.

Soit $y \in F \cap F_1$, alors

$$y = \sum_{k=0}^{s-1} a_k u^k(x)$$

et $\forall t \in \{0, \ldots, s-1\}$,

$$({}^t u)^t(\varphi)(y) = 0, \quad \text{i.e. } \varphi(u^t(y)) = 0$$

Soit $i$ le plus petit indice tel que $a_i \neq 0$, alors pour $t = s - 1 - i$, on a

$$a_i \varphi(u^{s-1}(x)) = 0$$

d'où $a_i = 0$, contradiction.

Alors, on applique l'hypothèse de récurrence à $F$, on a

$$F = F_2 \oplus \cdots \oplus F_n$$

où $u|_{F_i}$ est donné par une matrice de Jordan.

Unicité :

Les $\lambda$ sont nécessairement les valeurs propres de $u$, on se ramène à étudier l'unicité pour un endomorphisme nilpotent.

Appelons $b_i$ le nombre de blocs de Jordan de taille $i$, la taille maximale est $s$ : indice de nilpotentce.

Il faut voir que les $b_i$ ne dépendent que de $u$.

Il s'exprime en fait en fonction des dimensions des noyaux des puissances de $u$.

On considère la suite

$$\{0\} \subsetneq \ker u \subsetneq \ker u^2 \subsetneq \cdots \subsetneq u^{s-1} \subset E$$

Chaque bloc de Jordan (y compris de taille 1) contribue pour 1 au noyaux de $u$.

De façon générale, en regardant

$$(J_{0,r})^k = \begin{pmatrix} 0 & & & 1 & & 0 \\ & 0 & & & \ddots & \\ & & 0 & \iddots & & 1 \\ & & & \ddots & & \\ & & & & 0 & \\ & & & & & 0 \end{pmatrix}$$

on obtient :

$$\dim \ker u^k - \dim \ker u^{k-1} = \sum_{i \geq k} b_i$$

Si on pose

$$\delta_k = \dim \ker u^k - \dim \ker u^{k-1}$$

on a

$$\delta_k = \sum_{i \geq k} b_i$$

d'où $b_1 = \delta_1 - \delta_2, b_2 = \delta_2 = \delta_2, \dots$. □

Jordanisation :

On a obtenu les classes de similitude de matrices nilpotentes par décomposition en blocs de Jordans.

Si $M$ est nilpotente, il y a une unique suite décroissante d'entiers $n_1 \geq n_2 \geq \cdots \geq n_p \geq 1$, tels que $M$ semblable à

$$\begin{pmatrix} J_{n_1} & & & \\ & J_{n_2} & & \\ & & \ddots & \\ & & & J_{n_p} \end{pmatrix}$$

le nombre de blocs de taille $i$ est $\delta_i - \delta_{i+1}$ où

$$\delta_i = \dim \ker M^i - \dim \ker M^{i-1}$$

Fait général :

**Proposition 8.3.** *Soit $u \in \mathcal{L}(E)$, alors, la suite des noyaux est croissante et stationnaire,*

$$\ker u \subset \ker u^2 \subset \cdots \ker u^r \subset \cdots$$

*De plus, elle s'essouffle, c'est-à-dire, la suit des sautes de dimension*

$$\delta_i = \dim \ker u_i - \dim \ker u^{i-1} \geq 0$$

*est décroissante.*

*Démonstration.* Soit $k$ un entier, on a

$$\begin{tikzcd} \ker u^{k+1} \arrow[r, "u"] \arrow[dr, dotted, "\bar{u}"] & \ker u^k \arrow[d] \\ & \ker u^k / \ker u^{k-1} \end{tikzcd}$$

Pour l'application :

$$\bar{u} : \ker u^{k+1} \to \ker u^k / \ker u^{k-1}$$

on a $\ker \bar{u} = \ker u^k$ car

$$\bar{u}(x) = 0 \Leftrightarrow u(x) \in \ker u^{k-1}$$

Ainsi, $\bar{u}$ se factorise en une application injective :

$$\ker u^{k+1} / \ker u^k \to \ker u^k / \ker u^{k-1}$$

d'où

$$\dim(\ker u^{k+1} / \ker u^k) \leq \dim(\ker u^k / \ker u^{k-1})$$

et le résultat. $\square$

Autre approche à la construction des bloc de Jordan :

<u>Cadre</u> : $u$ nilpotent d'indice $p$, $\exists x$ tel que $u^{p-1}(x) \neq 0$, posons

$$F = \mathrm{Vect}(x, \dots, u^{p-1}(x))$$

alors, on a

$$\ker u \subsetneq \ker u^2 \subsetneq \cdots \subsetneq \ker u^{p-1} \subsetneq E$$

Comment privilégier tels $x$ :

Choisissons un supplémentaire $E_p$ de $\ker u^{p-1}$ :

$$u(E_p) \subset \ker u_{p-1}$$

et on a $u|_{E_p}$ est injective (car $\ker u \subset \ker u^{p-1}$).

Idée : choisir dans $\ker u^{p-1}$ un supplémentaire à $\ker u^{p-2}$ qui contient $u(E_p)$ et procéder par récurrence descendante.

*Remarque.*

$$u(E_p) \cap \ker u^{p-2} = \{0\}$$

car $E_p \cap \ker u^{p-1} = \{0\}$.

Pour $i \in \{1, 2, \dots, p-1\}$, on suppose avoir choisi $E_{i+1} \subset \ker u^{i+1}$ supplémentaire de $\ker u^i$, alors

$$
\begin{aligned}
&u(E_{i+1}) \subset \ker u^i \\
&u(E_{i+1}) \cap \ker u^{i-1} = \{0\}
\end{aligned}
$$

car $E_{i+1} \cap \ker u^i = \{0\}$.

Ansin,il existe dans $\ker u^i$ un supplémentaire $E_i$ à $\ker u^{i-1}$ et qui contient $u(E_{i+1})$.

Bilan(lemme) : il y des sous-espaces vectoriels $E_1, \ldots, E_p$ de $E$, tels que

$$
\begin{aligned}
&\forall i,\ \ker u^i = E_i \oplus \ker u^{i-1} \\
&\forall i,\ u(E_i) \subset E_{i-1}
\end{aligned}
$$

De plus, on a

$$E = \bigoplus_{i=1}^{p} E_i$$

et pour $i \geq 2$, la restriction de $u$ à $E_i$ est injectif.

On construit les blocs de Jordan en prenant des bases adaptées à cette situation.

On part d'une base $\mathcal{B}_p$ de $E_p$,

$$\mathcal{B}_p = \{v_{p,j} \mid 1 \leq j \leq n_p\}$$

Les $u(v_{p,j})$ forment une famille libre dans $E_{p-1}$, on la complète en une base de $E_{p-1}$.

Soit

$$\mathcal{B}'_{p-1} = \{v_{p-1,j} \mid 1 \leq j \leq n_{p-1}\}$$

tel que $u(\mathcal{B}_p) \cup \mathcal{B}'_{p-1} = \mathcal{B}_{p-1}$ est une base de $E_{p-1}$.

Puis on poursuit, pour $i$ descendant de $p$ à 2, $u(\mathcal{B}_i)$ une famille libre de $E_{i-1}$, qu'on complète en une base $\mathcal{B}_{i-1}$ de $E_{i-1}$ en rajoutant

$$\mathcal{B}_{i-1} = \{v_{i-1,j} \mid 1 \leq j \leq n_{i-1}\}$$

On obtient :

$$
\begin{array}{ccccccccccc}
E_p & \xrightarrow{u} & E_{p-1} & \xrightarrow{u} & E_{p-1} & \longrightarrow & \cdots & \longrightarrow & E_2 & \xrightarrow{u} & E_1 \\
v_{p,1} & & u(v_{p,1}) & & & & & & & & u^{p-1}(v_{p,1}) \\
\vdots & & \vdots & & & & & & & & \vdots \\
v_{p,n_p} & & u(v_{p,n_p}) & & & & & & & & u^{p-1}(v_{p,n_p}) \\
 & & v_{p-1,1} & & & & & & & & u^{p-2}(v_{p-1,1}) \\
 & & \vdots & & & & & & & & \vdots \\
 & & v_{p-1,n_{p-1}} & & & & & & & & u^{p-2}(v_{p-1,n_{p-1}}) \\
 & & & & & & & & & & \vdots \\
 & & & & & & & & & & u(v_{2,1}) \\
 & & & & & & & & & & \vdots \\
 & & & & & & & & & & u(v_{2,n_2}) \\
 & & & & & & & & & & v_{1,1} \\
 & & & & & & & & & & \vdots \\
 & & & & & & & & & & v_{1,n_1}
\end{array}
$$

On regarde le tableau horizontalement, de la droite vers la gauche.

On considère

$$\mathrm{Vect}(u^{p-1}(e_{p-1}), \ldots, e_{p-1})$$

la restriction de $u$ est un bloc de taille $p$, de même pour les $\mathrm{Vect}(u^{p-1}(e_{p,j}), \ldots, e_{p,j})$ pour $j \leq n_p$.

On poursuit :

$$(u^{i-1}(e_{i-1}, \ldots, e_{i-1}))$$

donne un bloc de taille $i$ et on en obtient $n_i$ stables dans lesquels la restriction de $u$ a pour matrice dans la base horizontal indiquée un bloc de Jordan.

On voit directement ici que le nombre de blocs de Jordan de taille $i$ est

$$\dim E_i - \dim E_{i+1} : \delta_i - \delta_{i+1}$$

car on a

$$\ker u^i = \ker u^{i-1} \oplus E_i$$

## 8.1 Quelques applications

**Théorème 8.4.** *Soit $K$ un corps de caractéristique 0, $M \in M_n(K)$. Soit $\lambda \neq 0, 1$ dans $K$. Alors les matrices $M$ et $\lambda M$ sont semblables $\Leftrightarrow$ $M$ est nilpotente.*

*Démonstration.* Si $M$ est $\lambda M$ sont semblables, alors elle ont les mêmes valeurs propre (prises dans une clôture algébrique de $K$).

Si $\alpha$ est un valeur propre $\Rightarrow$ $\lambda\alpha$ aussi et $\forall r \in \mathbb{N}$, $\lambda^r \alpha$ aussi.

Mais $M$ n'a qu'un nombre fini de valeurs propres et $\text{car}(K) = 0$, nécessairement $\alpha = 0$.

Si $M$ n'a que 0 pour valeur propre, alors $M$ est nilpotente car son polynôme caractéristique est $X^n$.

Invertisement :

Si $M$ est nilpotente, alors $\lambda M$ aussi. On regarde leurs décompositions de Jordan puisqu'elle caractérise les classes de similitude.

Le nombre de blocs de Jordan de taille $i$ est fonction des dimensions des $\ker M^j$ et ici, $\forall j$, $M^j$ et $(\lambda M)^j$ ont même noyau. $\square$

**Semblable et similitude :**

$M$ et $N$ semblables :

$$\exists P \in GL_n(K), \quad N = PNP^{-1}$$

"Être semblable" est une relation d'équivalence dont les classes d'équivalence sont appelées "classes de similitude".

On dit parfois aussi "matrices conjuguées" et on parle de "classe de conjugaison".

**Théorème 8.5.** *Soit $K = \mathbb{R}$ ou $\mathbb{C}$, alors toute matrice de $M_n(K)$ est semblable à sa transposée.*

*Démonstration.* Pour $K = \mathbb{C}$, on dispose du théorème de Jordan, on se ramène à montrer le résultat pour un bloc de Jordan :

$$J_{\lambda,r} = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

alors, on a

$$J_{\lambda,r} = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

On passe de l'un à l'autre par changement de base en renversant l'ordre des vecteurs de base :

$$(e_1, \dots, e_r) \to (e_r, \dots, e_1)$$

on a alors ${}^tJ = PJP^{-1}$, où $P = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$. □

<u>$K = \mathbb{R}$</u> :

**Proposition 8.6.** *Soit $M, N \in M_n(\mathbb{R})$, si $M$ et $N$ sont semblables sur $\mathbb{C}$, alors elles sont semblables sur $\mathbb{R}$.*

*Démonstration.* $\exists P \in GL_n(\mathbb{C})$, $PMP^{-1} = N$ et $P = R + iS$ avec $R, S \in M_n(\mathbb{R})$, on a

$$(R + iS)M = N(R + iS)$$

d'où $RM = NR$ et $SM = NS$.

On veut une matrice réelle et inversible et $\forall t \in \mathbb{R}$, on a

$$(R + tS)M = N(R + tS)$$

Il suffit de trouver $t \in \mathbb{R}$, tel que

$$\det(R + tS) \neq 0$$

On a une fonction polynomiale $p \in \mathbb{R}[t]$ :

$$t \mapsto \det(R + ts) = p(t)$$

et on a $p(i) \neq 0$ car $P \in GL_n(\mathbb{C})$, $p$ n'est pas le polynôme null, donc n'a qu'un nombre fini de racines, d'où $\exists t \in K$, $p(t) \neq 0$. □

**Théorème 8.7.** *Dans $M_n(\mathbb{C})$, toute matrice est semblable à une matrice symétrique.*

Rappel :

Dans $M_n(\mathbb{R})$, les matrices symétriques sont diagonalisables, donc un tel résultat ne peut avoir lien.

Ex. Dans $\mathbb{C}$, soit $M = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$, $M^2 = 0$, c'est une matrice nilpotante d'indice 2, semblable à $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

*Démonstration.* La réduction de Jordan permet de se ramener au cas d'un bloc de Jordan, on a vu :

$$^tJ = PJP^{-1}$$

avec $P = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$.

On pense aux matrices symétriques comme à des matrices de formes bilinéaires symétriques.

Rappel :

Si $\varphi$ est une forme bilinéaire symétrique et $(e_1, \ldots, e_n)$ une base, $M = (\varphi(e_i, e_j))$.

Classification des formes bilinéaires symétrique sous l'action par congruence du groupe linéaire, $M = \mathrm{Mat}_e(\varphi)$.

Si $F = (f_1, \ldots, f_n)$ est une autre bas et $P$ est la matrice de passage, alors

$$\mathrm{Mat}_F(\varphi) = P \cdot M \cdot^t P$$

Théorème de réduction des formes bilinéaires symétriques sur $\mathbb{C}$, dit :

2 formes bilinéaires symétriques sont congruence si et seulement si elles ont le même rang.

Ici, pour notre prolème, on a $P = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$, qui est symétrique.

Elle définit une forme bilinéaire symétrique sur $\mathbb{C}^n$ qui est de rang $n$, elle est donc congruente à $I_n$.

Donc, $\exists Q \in GL_n(\mathbb{C})$, tel que

$$P = Q \cdot^t Q$$

On avait $^tJ = PJP^{-1}$, ici $P^{-1} = P = Q \cdot^t Q$.

Alors,

$$ {}^tJ = Q({}^tQJQ){}^tQ $$

avec $Q$ former une matrice symétrique semblable à $J$ du type $QJQ^{-1}$ ou $Q^{-1}JQ$. $\square$

# 9 Réduction de Frobenius

Soit $E$ un $K$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$.

**Définition 9.1.** (1) $x \in E$ est dit cyclique si $\mathrm{Vect}(u^k(x), k \in \mathbb{N}) = E$.

(2) $u \in \mathcal{L}(E)$ est dit endomorphisme cyclique s'il existe un vecteur cyclique.

(3) $F \subset E$ sous-espace de $E$ est dit cyclique si $F$ est stable par $u$ et la restriction de $u$ à $F$ est cyclique

**Définition 9.2.** (Polynôme minimal relatif à un vecteur)

$u \in \mathcal{L}(E), x \in E$, posons

$$I = \{P \in K[X] \mid P(u)(x) = 0\}$$

Alors, $I$ est un idéal de $K[x]$, on appelle polynôme minimal de $x$ le générateur unitaire de $I$. On le note $\mu_{u,x}$ ou $\mu_x$ si $u$ est sous-entendu. (On note $\mu_u$ ou $\mu$ le polynôme minimal de $u$)

Ainsi, $\forall x \in E$, $\mu_x \mid \mu$.

De plus, si $\deg(\mu_x) = r$, on a $(x, u(x), \dots, u^{r-1}(x))$ est libre et

$$\mathrm{Vect}(u^k(x), k \geq 0) = \mathrm{Vect}(x, \dots, u^{r-1}(x))$$

et ceci est un sous-espace cyclique.

Noton

$$\mu_x = a_0 + a_1 X + \cdots + X^r$$

dans la base $(x, u(x), \dots, u^{r-1}(x))$, la matrice de la restriction de $u$ est :

$$\begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{r-1} \end{pmatrix} = C_{\mu_x}$$

c'est la matrice compagnon du polynôme : $X^r + a_{r-1}X^{r-1} + \cdots a_0$.

**Définition 9.3.** De façon générale pour tout polynôme $P(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0$, on annonce la matrice

$$C_P = \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{r-1} \end{pmatrix}$$

appelée matrice compagnon de $P$, qui s'interprète aussi :

On considère $K[X]/(P)$, c'est un $K$-espace vectoriel de $\dim r$, de base $(\overline{1}, \overline{X}, \dots, \overline{X^{r-1}})$, on considère l'action de la multiplication par $x$.

Dans cette base, la matrice de cette action est donnée par $C_p$.

**Proprieté caractéristique des matrices compagnon :**

**Proposition 9.4.** *Le polynôme caractéristique est égale au polynôme minimal et est égal à $P$ :*

$$\chi_{C_P} = \mu_{C_P} = P$$

*Démonstration.* Le calcul du polynôme caractéristique se fait directement.

On remarque que $(e_1, C_P(e_1), \dots, C_P(e_r)) = (e_1, e_2, \dots, e_r)$, donc le polynôme minimal est de degré $\geq r$, donc exactement de degré $r$, et donc nécessairement et égal au polynôme caractéristique.

De plus, on voit que

$$C_P^r(e_1) = -a_0 e_1 - a_1 C_P(e_1) - \dots - a_{r-1} C_P^{r-1}(e_1)$$

d'où $P(C_P(e_1)) = 0$, d'où le polynôme minimal de $e_1 = P$ (car on sait qu'il est de degré $\geq r$, puisque $(e_1, C_P(e_1), \dots, C_P(e_r))$ est libre.

Finalement, on a obtenu :

- Polynôme minimal de $e_1 = P$.
- Polynôme minimale de $C_P = P$.
- Polynôme caractéristique est $P$ (ici sans calcul). $\square$

**Proposition 9.5.** *Soit $u \in \mathcal{L}(E)$, alors, $\exists x \in E$, tel que $\mu_{u,x} = \mu_u$.*

*Démonstration.* $\forall x \in E$, $\mu_x \mid \mu$, soit $\mu(X) = P_1(X)^{\alpha_1} \cdots P_s(X)^{\alpha_s}$ : la décomposition de $\mu$ est produit de polynômes irréductibles.

Le lemme des noyaux nous donne :

$$E = \ker \mu(u) = \bigoplus_{i=1}^{s} \ker(P_i(u)^{alpha_i})$$

chaque $\ker(P_i(u)^{alpha_i})$ est stable par $u$ et la restriction de $u$ à ce sous-espace a pour polynôme minimal $P_i^{\alpha_i}$ (Sinon, ce polynôme minimal serait $P_i^{\beta^i}$ avec $\beta_i < \alpha_i$, alors le polynôme minimal de $u$ aurait $\beta_i$ comme exposant de $P_i$.)

Soit $x_i \in \ker P_i^{\alpha_i}(u)$, $x_i \notin \ker P_i^{\alpha_{i-1}}(u)$ (On a $\ker P_i^{\alpha_i}(u) \subsetneq \ker P_i^{\alpha_{i-1}}(u)$), posons

$$x = x_1 + \cdots + x_s$$

alors $x$ est tel que $\mu_x = \mu$.

En effet, soit $P \in K[X]$ tel que

$$0 = P(u)(x) = \sum_{i=1}^{s} P(u)(x_i),\ \ P(u)(x_i) \in \ker(P_i^{\alpha_i}(u))$$

d'où $P(u)(x_i) = 0$, alors, on a

$$P(u)(x_i) = 0 \Rightarrow P_i^{\alpha_i} \mid P \Rightarrow \mu \mid P$$

□

**Retour la caractérisation des matrices compagnons :**

**Proposition 9.6.** *Soit $u \in \mathcal{L}(E)$, tel que $\chi_u = \mu_u$, alors $u$ est cyclique et il existe une base dans laquelle la matrice de $u$ est une matrice compagnon.*

*Démonstration.* Soit $x \in E$, tel que $\mu_x = \mu$.

Alors, la dimension du sous-espace cyclique engendré par $x$ est

$$\deg \mu_x = \deg \mu = \deg \chi_u = \dim E$$

□

**Théorème 9.7.** *(Réduction de Frobenius)*

*Soit $u \in \mathcal{L}(E)$, alors il existe une suite $(P_1, \dots P_r)$ de polynômes unitaires et une suite $(F_1, \dots, F_r)$ de sous-espaces stables telle que*

*(1)* $E = F_1 \oplus \cdots \oplus F_r$*.*

*(2)* $\forall i$*,* $u|_{F_i}$ *est cyclique de polynôme minimal* $P_i$*.*

*(3)* $P_r \mid P_{r-1} \mid \cdots \mid P_1$*.*

*Cette suite* $(P_1, \ldots, P_r)$ *est appelé suites des invariants de similitude de* $u$ *et elle caractérise sa classe de similitude.*

*Remarque.* Ainsi, $u, v \in \mathcal{L}(E)$ sont semblables $\Leftrightarrow$ ils ont les mêmes invariants de similitude.

Ainsi, il existe de $E$ dans laquelle $u$ a pour matrice :

$$\begin{pmatrix} C_{P_1} & & & \\ & C_{P_2} & & \\ & & \ddots & \\ & & & C_{P_r} \end{pmatrix}$$

diagonale par blocs.

On a de plus

$$\mu_u = P_1,\ \chi_u = P_1 \cdots P_r$$

**Exemple.** (Lien avec la réduction de Jordan)

Un bloc de Jordan est (la tranposée) de la matrice compagnon de $X^r$, et si $u$ est nilpotent, sa réduction de Jordan est sa réduction de Frobenius lorsqu'on écrit les blocs de Jordan par taille décroissante.

NB : pour Frobenius, pas d'hypothèse sur le polynôme caractéristique.

*Démonstration.* (Preuve du théorème)

Par récurrence sur $\dim E$.

Posons $P_1 = \mu$ le polynôme minimal de $u$, alors,

$$\exists x \in E,\ \mu_x = P_1$$

Soit $d = \deg \mu$, alors

$$F_1 = \mathrm{Vect}(x, u(x), \ldots, u^{d-1}(x))$$

est cyclique, de dimension $d$, et le polynôme minimal de $u|_{F_1}$ est $P_1$.

On cherche un supplémentaire stable à $F_1$.

Poser $e_1 = x, e_2 = u(x), \dots, e_d = u^{d-1}(x)$, on complète cette famille libre en une base $(e_1, \dots, e_n)$ de $E$.

On dispose de la base duale $(e_1^*, \dots, e_n^*)$.

On considère $\varphi = e_d^*$, on a

$$\varphi(e_1) = 0, \dots, \varphi(e_{d-1}) = 0, \varphi(e_d) = 1$$

Alors, la famille $\varphi, {}^t u(\varphi), \dots, ({}^t u)^{d-1}(\varphi)$ est libre dans $E^*$.

Supposons $\exists \lambda_0, \dots, \lambda_{d-1} \in K$, tel que

$$\sum_{i=1}^{d-1} \lambda_i ({}^t u)^i(\varphi) = 0$$

On applique à $e_1$, alors,

$$\begin{aligned} 0 &= \sum_{i=0}^{d-1} \lambda_i \varphi(u^i(e_1)) \\ &= \sum_{i=0}^{d-1} \lambda_i \varphi(e_{1+i}) \\ &= \lambda_{d-1} \end{aligned}$$

alors, $\lambda_{d-1} = 0$.

On applique à $e_2$, puis on peut obtenir $\lambda_{d-2}$, etc.

Soit $G = (\varphi, {}^t u(\varphi), \dots, ({}^t u)^{d-1}(\varphi))$ et $\dim G = d$

$G$ est stable par ${}^t u$, en effet, on a

$$\mu_{{}^t u} = \mu_u$$

donc $({}^t u)^d(\varphi)$ est combilinaison linéaire de $\varphi, {}^t u(\varphi), \dots, ({}^t u)^{d-1}(\varphi)$.

Soit $E' = G^\circ \subset E$, on a $\dim E' = n - d$.

Montrons que $E'$ est un supplémentaire stable de $F_1$ :

- Stabilité due à celle de $G$ par ${}^t u$.

- Supplémentaire :

Soit $y \in F_1 \cap E'$, alors
$$y = \sum_{i=0}^{d-1} \alpha_i u^i(x)$$

On applique $\varphi$, $\varphi(y) = 0$ :

$$\sum_{i=0}^{d-1} \alpha_i ({}^t u)^i(\varphi)(x) = \sum_{i=0}^{d-1} \alpha_i \varphi(e_{i+1}) = 0$$

alors, $\alpha_{d-1} = 0$.

On poursuit en appliquant $\varphi \circ u =^t u(\varphi), \ldots, ({}^t u)^{d-1}(\varphi)$ et on obtient :

$$\forall i,\ \alpha_i = 0$$

d'où $F_1 \cap E = \{0\}$.

On applique l'hypothèse de récurrence à $E', u|_{E'}$.

On trouve des polynômes unitaires $P_2, \ldots, P_r$, des sous-espaces stables $F_2, \ldots, F_r$, tels que

$$E' = F_2 \oplus \cdots \oplus F_r$$

et $(u|_{E_1})|_{F_i} = u|_{F_i}$ est cyclique de polynôme minimal $P_i$, et on a

$$P_r \mid P_{r-1} \mid \cdots \mid P_2$$

Ainsi, on a
$$E = F_1 \oplus \cdots \oplus F_r$$

il suffit, pour conclure, de voir que $P_2 \mid P_1$, ce qui est le cas par $P_1 = \mu_u$ est donc $P_1(u) = 0$, en particulier sa restriction à $F_2$.

Unicité des polynômes :

Supposons que, à côté de $(P_1, \ldots, P_r)$ et $(F_1, \ldots, F_r)$, on ait $Q_1, \ldots, Q_s$ des polynômes unitaires. $G_1, \ldots, G_s$ des sous-espases stables qui satisfait aux conclusions du théorème.

Il faut voir : $r = s$ et $\forall i, P_i = Q_i$.

*Remarque.* Nécessairement $Q_1 = \mu_u$, donc $P_1 = Q_1$ (d'où $\dim F_1 = \dim G_1$).

Soit $j$ le plus petit indice $i$, tel que $P_i \neq Q_i$.

Comme $P_r \mid P_{r-1} \mid \cdots \mid P_{j+1} \mid P_j$, $P_j(u)$ s'annule sur les $F_k$, $k \geq j$, on a

$$P_j(u)(E) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_{j-1})$$

Comme $E = G_1 \oplus \cdots \oplus G_s$, on a

$$P_j(u)(E) = P_j(u)(G_1) \oplus \cdots \oplus P_j(u)(G_s)$$

On sait que $u|_{F_i}$ est cyclique de polynôme minimal $P_i$.

Donc, pour $i \leq j-1$, on a $u|_{F_i}$ et $u|_{G_i}$ sont semblables, car dans des bases convenables, ils sont donnés par la matrice compagnon $C_{P_i} = C_{Q_i}$.

Alors, pour tout polynôme $P$, $P(u|_{F_i})$ et $P(u|_{G_i})$ sont semblables et en particulier on a

$$\forall i \leq j-1,\ \dim P_j(u)(G_i) = \dim P_j(u)(F_i)$$

On a alors, en prenant les dimensions, que

$$\dim P_j(u)(G_i) = \dim P_j(u)(G_{i+1}) = \cdots = \dim P_j(u)(G_s) = 0$$

d'où $P_j(u)(G_j) = 0$, alors

$$P_j(u|_{G_j}) = 0 \Rightarrow Q_j \mid P_j$$

Par symétries, on a aussi $P_j \mid Q_j$, d'où

$$P_j = Q_j$$

Contradiction. $\square$

## 9.1 Compléments et applications

*Remarque.* Un endomorphisme cyclique a un unique invariant de similitude :

$$P_i = \mu = \chi$$

**Proposition 9.8.** *Soit $u$ un endomorphisme cyclique, alors, $u$ et ${}^tu$ sont semblables.*

*Démonstration.* Comme on a

$$\mu_{{}^tu} = \mu_u$$
$$\chi_{{}^tu} = \chi_u$$

donc, ${}^tu$ est cyclique. □

**Proposition 9.9.** *$\forall M \in M_n(K)$, $M$ et ${}^tM$ sont semblables.*

*Démonstration.* $M$ est semblable à une matrice diagonable par blocs matrices compagnons et c'est vrai pour les matrices compagnons. □

**Proposition 9.10.** *Soit $k, K$ deux corps, $k \subset K$, si $A, B \in M_n(k)$ sont semblables dans $M_n(K)$, alors, elles le sont dans $M_n(k)$.*

*Démonstration.* On regarde les invariants de similitude de $A$ sur $k$ :

Ce sont aussi, par unicité, ses invariants de similitude dans $M_n(K)$, les invariants de similitude ne dépendent que "au plus petit corps" sur lequel on définit la matrice.

Si $A$ et $B$ sont semblables sur $M_n(K)$, alors elles ont mêmes invariants sur $k$, donc elles sont semblables sur $k$. □

*Remarque.* Les conditions de divisibilité entre les polynômes sont fondamentaux.

**Exemple.** Soit $P, Q \in k[X]$ deux polynômes unitaires avec $P \wedge Q = 1$.

La matrice

$$\begin{pmatrix} C_P & 0 \\ 0 & C_Q \end{pmatrix}$$

représente un endomorphisme cyclique de polynôme minimal $PQ$.

En effet : on a vu que $C_P$ est la matrice de multiplication par $X$ dans $k[X]/(P)$. Ainsi, on peut voir $M$ comme la matrice de multiplication par $X$ dans

$$k[X]/(P) \times k[X]/(Q)$$

$k[X]$ est principal et le lemme de chinois donne un isomorphisme d'anneaux, et donc de $k[X]$-modules :

$$k[X]/(P) \times k[X]/(Q) \simeq k[X]/(PQ)$$

espace cyclique de polynôme minimal $PQ$.

De façon générale :

**Proposition 9.11.** $P, Q \in k[X]$ *unitaires, les invariants de similitude de* $\begin{pmatrix} C_P & 0 \\ 0 & C_Q \end{pmatrix}$ *sont :*

$$(ppcm(P,Q), pgcd(P,Q))$$

*Démonstration.* Posons $P = R_1^{\alpha_1} \cdots R_k^{\alpha_k}$, $Q = R_1^{\beta_1} \cdots R_k^{\beta_k}$, où $R_i$ sont unitaires irréductibles. Alors,

$$pgcd(P,Q) = P \wedge Q = \prod_{i=1}^{k} R_i^{\min(\alpha_i, \beta_i)}$$
$$ppcm(P,Q) = P \vee Q = \prod_{i=1}^{k} R_i^{\max(\alpha_i, \beta_i)}$$

Considérer $\begin{pmatrix} C_P & 0 \\ 0 & C_Q \end{pmatrix}$ revient à considérer la multiplication par $X$ dans

$$\begin{aligned} k[X]/(P) \times k[X]/(Q) &\simeq \prod_{i=1}^{k} k[X]/(R_i^{\alpha_i}) \times \prod_{i=1}^{k} k[X]/(R_i^{\beta_i}) \\ &\simeq \prod_{i=1}^{k} k[X]/(R_i^{\min(\alpha_i,\beta_i)}) \times \prod_{i=1}^{k} k[X]/(R_i^{\max(\alpha_i,\beta_i)}) \\ &\simeq k[X]/(P \wedge Q) \times k[X]/(P \vee Q) \end{aligned}$$

donné par

$$\begin{pmatrix} C_{P\vee Q} & 0 \\ 0 & C_{P\wedge Q} \end{pmatrix}$$

avec $P \wedge Q \mid P \vee Q$. $\square$

**Caractérisations des endomorphismes cycliques**

**Définition 9.12.** Soit $u \in \mathcal{L}(E)$, le commutant de $u$ est

$$Com(u) = \{v \in \mathcal{L}(E) \mid, v \circ u = u \circ v\}$$

**Proposition 9.13.** *$u \in \mathcal{L}(E)$ est cyclique $\Leftrightarrow$ $Com(u) = k[u] = \{P(u) \mid P \in k[X]\}$*

*Remarque.* Pour tout endomorphisme, on a$k[u] \subset Com(u)$.

*Démonstration.* Supposons $u$ cyclique et soit $v \in Com(u)$.

On dispose d'une base de $E$ :

$$(x, u(x), \cdots, u^{d-1}(x))$$

On écrit :

$$v(x) = \sum_{j=0}^{d-1} \alpha_j u^j(x)$$

alors, $\forall k \in \{1, \ldots, d-1\}$, on a

$$\begin{aligned} v(u^k(x)) &= u^k(v(x)) \\ &= \sum_{j=0}^{d-1} \alpha_j u^k(u^j(x)) \\ &= \sum_{j=0}^{d-1} \alpha_j u^j(u^k(x)) \end{aligned}$$

ainsi, $v$ coïnde avec $\sum_{j=0}^{d-1} \alpha_j u^j$ sur la base.

Donc, on a

$$v = \sum_{j=0}^{d-1} \alpha_j u^j$$

Inversement : supposons $Com(u) = k[u]$ et montrons que $u$ est cyclique.

Si $u$ n'est pas cyclique, il y a au moins 2 invariants de similitude $P_1, P_2$ avec $P_2 \mid P_1$.

Les sous-espace cyclique correspondants $F_1, F_2$ sont stables par $u$ (pour simplifier, supposons qu'il y en a juste 2).

Alors, la projection $p$ sur $F_1$ parallèment à $F_2$ est dans $Com(u)$, si $p = Com(u)$ polynôme en $u$, alors $P(u)|_{F_2} = 0$, donc $P_2 \mid P$.

De plus, $(p(u) - \mathrm{Id})|_{F_1} = 0$, donc $P_1 \mid P - 1$.

Comme $P_2 \mid P_1$, c'est impossible : $P_2$ ne divise pas 1. □

**Proposition 9.14.** *Supposons $k$ infini, alors $u \in \mathcal{L}(E)$ est cyclique si et seulement si $u$ ne possède qu'en nombre fini de sous-espace stables.*

*Démonstration.* Supposons $u$ soit cyclique, alors

$$E \simeq k[X]/(P),\ P = \mu_u$$

où $u$ agit par multiplication par $X$ dans $k[X]/(P)$.

Un sous-espace stable est un idéal de l'anneau $k[X]/(P)$, on utilise alors la correspondance bijective entre idéaux du quotient $k[X]/(P)$ et les idéaux de $k[X]$ contenant l'idéal $(P)$.

De tels ideaux sont principaux, de la forme $(Q)$ avec $Q \mid P$, or $P$ n'a qu'un nombre fini de diviseurs de degré $\geq 1$.

Réciproque :

Dire que $u$ est cyclique, c'est dire

$$\exists x,\ Vect(x, u(x), \ldots, u^k(x)) = E_x = E$$

Si ce n'est pas le cas, alors, $E_x \subsetneq E$.

S'il n'y a qu'un nombre fini de sous-espaces stables, considérons $E_1, \ldots, E_r$, ces sous-espaces $\neq E$.

On a alors, $\forall x \in E$, $E_x = E_j$ pour un $j \in \{1, \ldots, r\}$.

Ceci donne

$$E = \bigcup_{i=1}^{n} E_i$$

Or, si $k$ est infini, ceci n'est possible que si l'un des $E_i$ vaut $E$. □

### Lien entre réduction de Frobenius et décomposition de Jordan

On considère $u \in \mathcal{L}(E)$ de polynôme caractéristique scindée.

<u>De Frobenius à Jordan</u>

Il faut savoir calculer la décomposition de Jordan d'une matrice compagnon $C_P$, si $P(X) = \prod (X - \lambda_i)^{\alpha_i}$, alors

$$E = \bigoplus \ker(u - \lambda_i \mathrm{Id})^{\alpha_i}$$

Dans chaque $\ker(u - \lambda_i \mathrm{Id})^{\alpha_i}$, on a le bloc

$$\begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix}$$

ceci car on a une matrice compagonnon et $C_P$ possède la propriété suivante :

Chaque valeur propre $\lambda_i$ est de multiplicité 1.

En effet,

$$C_P = \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{r-1} \end{pmatrix}$$

alors, on a

$$\lambda \mathrm{Id} - C_P = \begin{pmatrix} \lambda & & & & a_0 \\ -1 & \lambda & & & a_1 \\ & \ddots & \ddots & & \vdots \\ & & -1 & \lambda & a_{r-2} \\ & & & -1 & \lambda + a_{r-1} \end{pmatrix}$$

multiplicité de $\lambda$ est la dimension du noyau de cette matrice.

Mais cette matrice est de rang $n-1$ (bloc avec les $-1$ sous le diagonale).

Ainsi, pour chaque valeur propre $\lambda_i$, il ne peut y avoir qu'un seul bloc de Jordan.

<u>De Jordan à Frobenius</u>

Parmi les matrices de Jordan, quels sont les endomorphisme cycliques ?

**Lemme 9.15.** *Considérons une matrice diagonale par blocs, avec blocs de Jordan $J_{\lambda_i, r_i}$. Alors, elle est cyclique si et seulement si les $\lambda_i$ sont 2 à 2 distincts.*

*Démonstration.* On veut polynôme minimal = polyôme caractéristique.

Or on a :

(1) Le polynôme caractéristique d'un matrice triangulaire par blocs est le produit.

(2) Le polynôme minimal est le ppcm.

Concrètement, si on dispose de la décompositions de Jordan de $M$ : $J_{\lambda_i,r_i}$, pour chaque $\lambda_i$, on regarde les $(X-\lambda_i)^{r_i}$ et on choisit un $(X-\lambda_i)^{r_i}$ avec $r_i$ minimal.

On fait le produit avec les $\lambda_i$ distincts : ça donne $P_1$, puis procède de même avec les blocs restant. □

# 10 Formes sesquilinéaires

Soit $E$ un $\mathbb{C}$-espace vectoriel.

**Définition 10.1.** Une application semi-linéaire $f : E \to E$ est une application additive

$$\forall x, y \in E,\ f(x+y) = f(x) + f(y)$$

et satisfait

$$\forall \lambda \in \mathbb{C}, x \in E,\ f(\lambda x) = \overline{\lambda} f(x)$$

**Exemple.** Si $\varphi \in E^*$, alors, l'application

$$\overline{\varphi} : x \mapsto \overline{\varphi(x)}$$

est semi-linéaire.

**Définition 10.2.** Soit $E$ un $\mathbb{C}$-espace vectoriel, une forme sesquilinéaire sur $E$ est une application $\varphi : E \times E \to \mathbb{C}$, telle que :

$\varphi$ est semi-linéaire par rapport à la première variable et linéaire par rapport à la deuxième variable : pour $\forall x, y, x', y' \in E$,

$$\varphi(x, \lambda y + y') = \lambda \varphi(x, y) + \varphi(x, y')$$
$$\varphi(\lambda x + x', y) = \overline{\lambda} \varphi(x, y) + \varphi(x', y)$$

**Définition 10.3.** Une forme sesquilinéaire est dite à symétrie hermitienne si

$$\forall x, y \in E,\ \varphi(y, x) = \overline{\varphi(x, y)}$$

*Remarque.* On a alors :

$$\forall x,\ \varphi(x, x) \in \mathbb{R}$$

**Définition 10.4.** Soit $\varphi$ une forme sesquilinéaire, $x, y \in E$ sont dits orthogonaux, si

$$\varphi(x, y) = 0$$

*Remarque.* Si $\varphi$ est de plus à symétrie hermitienne, cette relation est symétrique.

**Constructions :**

Soit $\varphi$ sesquilinéaire, alors $\forall x \in E$, l'application

$$\begin{aligned} E &\to \mathbb{C} \\ y &\mapsto \varphi(x,y) \end{aligned}$$

est dans $E^*$ et on construit aussi une application :

$$\begin{aligned} \overline{\varphi} : E &\to E* \\ x &\mapsto \varphi_x = \varphi(x,\cdot) \end{aligned}$$

$\overline{\varphi}$ est semi-linéaire.

**Définition 10.5.** On dit que $\varphi$ est non dégénérée si $\overline{\varphi}$ est injective, i.e. si

$$\ker \overline{\varphi} = \{x \in E \mid \forall y \in E, \varphi(x,y) = 0\} = \{0\}$$

i.e. si les seuls vecteurs $x$ orthogonaux à tout $E$ sont 0.

En dimension finie, ceci équivaut à $\overline{\varphi}$ est bijective.

**Matrice d'une forme sesquilinéaire :**

$E$ est de dimension finie et $(e_1, \cdots, e_n)$ une base de $E$, si $\varphi$ est une forme sesquilinéaire, elle est complètement déterminée par les $\varphi(e_i, e_j)$, $1 \leq i, j \leq n$.

En effet, si $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{i=1}^n y_i e_i$, alors,

$$\varphi(x,y) = \sum_{1 \leq i,j \leq n} \varphi(e_i, e_j) \overline{x_i} y_j$$

La matrice $(\varphi(e_i, e_j))_{1 \leq i,j \leq n}$ est appelée matrice de $\varphi$ dans la base $(e_1, \ldots, e_n)$.

**Proposition 10.6.** *$\varphi$ est non dégénérée si et seulement si sa matrice est inversible.*

En effet, la matrice de $\varphi$ est aussi la transposée de $\overline{\varphi}$ dans les bases $e = (e_1, \ldots, e_n)$ et $e^* = (e_1^*, \ldots, e_n^*)$ la base duale.

*Remarque.* On est en train de considérer la matrice d'une application semi-linéaire.

Si $E, E'$ sont des $\mathbb{C}$-espace vectoriel de dimension finie, $e = (e_1, \ldots, e_n)$ une base de $E$, $f = (f_1, \ldots, f_p)$ une base de $E'$, alors, une application semi-linéaire $u : E \to E'$ est complètement déterminée par la matrice $(u_{ij})_{i\geq n, j\geq p}$ donée par

$$u(e_j) = \sum_{i=1}^{p} u_{ij} f_i,\ u_{ij} \in \mathbb{C}$$

$\forall x \in E$, $x = \sum_{i=1}^{n} x_i e_i$, alors les coordonnées de $u(x)$ dans $f$ sont donées par

$$A \cdot \overline{x},\ A = (u_{ij})$$

**Proposition 10.7.** $\dim E$ *est finie,* $\varphi$ *est non dégénérée, alors la relation d'orgonalité est symétrique (on dit que* $\varphi$ *est réflexive) si et seulement si* $\exists \psi$ *sesquilinéaire à symétrie hermitienne et* $\lambda \in \mathbb{C}$*, tel que* $\varphi = \lambda \psi$.

*Démonstration.* $\varphi$ est non dégénérée, alors,

$$\begin{aligned} \overline{\varphi} : E &\to E* \\ x &\mapsto \varphi_x = \varphi(x, \cdot) \end{aligned}$$

est bijective.

Considérons $y \mapsto \overline{\varphi(y,x)}$, c'est une forme linéaire $\widetilde{\varphi_x}$.

Comme la relation d'orthogonalité est symétrique :

$$\overline{\varphi(x,y)} \Rightarrow \varphi(x,y)$$

ainsi,

$$\widetilde{\varphi_x}(y) = 0 \Leftrightarrow \varphi_x(y) = 0$$

Ainsi, $\forall x \in E$, les formes linéaires $\varphi_x$ et $\widetilde{\varphi_x}$ ont même noyau.

On sait alors qu'il existe $\alpha(x) \in \mathbb{C}$, tel que

$$\widetilde{\varphi_x} = \alpha(x) \varphi_x$$

$\overline{\varphi}$ et $\widetilde{\varphi}$ sont bijectives et semilinéaires.

Considérons $(\overline{\varphi})^{-1} \circ \widetilde{\varphi}$ : cette application est linéaire et on a, si $h = (\overline{\varphi})^{-1} \circ \widetilde{\varphi}$, alors,

$$\begin{aligned} h(x) &= (\overline{\varphi})^{-1} \circ \widetilde{\varphi_x} \\ &= (\overline{\varphi})^{-1}(\alpha(x)\varphi_x) \\ &= \overline{\alpha(x)}x \end{aligned}$$

Alors, $h : E \to E$ est donc une homothétie, donc

$$\exists \alpha \in \mathbb{C}, \forall x,\ h(x) = \alpha x$$

i.e. $\widetilde{\varphi_x} = \alpha\overline{\varphi_x}$, i.e.

$$\forall y, x,\ \overline{\varphi(y,x)} = \alpha\varphi(x,y)$$

Alors, on a

$$\begin{aligned} \varphi(y,x) &= \overline{\overline{\varphi(x,y)}} \\ &= \overline{\alpha}\overline{\varphi(x,y)} \\ &= \overline{\alpha}\alpha\varphi(y,x) \\ &= |\alpha|^2\varphi(y,x) \end{aligned}$$

donc, $|\alpha|^2 = 1$.

Posons $\lambda = \alpha^{\frac{1}{2}}$, $\psi(x,y) = \lambda(x,y)$, on a

$$\begin{aligned} \overline{\psi(y,x)} &= \overline{\lambda} \cdot \overline{\varphi(y,x)} \\ &= \overline{\lambda}\alpha\varphi(x,y) \\ &= \overline{\lambda}\lambda^{-1}\alpha\psi(x,y) \\ &= \lambda^{-2}\alpha\psi(x,y) \\ &= \psi(x,y) \end{aligned}$$

□

Dorénavant, on considère des formes sesquilinéaires à symétrie hermitienne, on la associe une forme quadratique hermitienne, on dit aussi forme hermitienne :

**Définition 10.8.** Si $\varphi$ est sesquilinéaire à symétrie hermitienne, on pose

$$\begin{aligned} h : E &\to \mathbb{C} \\ x &\mapsto \varphi(x,x) \end{aligned}$$

*Remarque.* $h(x) \in \mathbb{R}$ et

$$\forall \lambda \in \mathbb{C},\ h(\lambda x) = |\lambda|^2 h(x)$$

**Identité du polarisation**

On retrouve $\varphi$ à partir de $h$, via :

$$\varphi(x,y) = \frac{1}{4}(h(x+y) - h(x-y) + ih(x-iy) - ih(x+iy))$$

*Remarque.* On a

$$h(x+y) = h(x) + h(y) + 2\,\mathrm{Re}(\varphi(x,y))$$

Propriété : Soit $h$ une forme hermitienne, la matrice de $h$ dans une base de $E$ est la matrice de $\varphi$ dans cette base : $H = (\varphi(e_i, e_j))$

Cette matrice est une matrice hermitienne, i.e.

$$H = (h_{ij}),\ h_{ij} = \overline{h_{ji}}$$

Inversement, toute matrice hermitienne $H \in M_n(\mathbb{C})$ détermine une forme hermitienne sur $\mathbb{C}^n$ via :

$$(x,y) \to^t \overline{x} H y$$

Notation : Si $H = (h_{ij}) \in M_n(\mathbb{C})$, $H^* = (\widetilde{h_{ij}})$ avec $\widetilde{h_{ij}} = \overline{h_{ji}}$ : $H^* =^t \overline{H}$.

**Proposition 10.9.** *Les matrices forment un $\mathbb{R}$-sous espace vectoriel de $M_n(\mathbb{C})$, de plus, si on note $H_n(\mathbb{C}) = \{H \text{ hermitienne}\}$, alors,*

$$M_n(\mathbb{C}) = H_n(\mathbb{C}) \oplus iH_n(\mathbb{C})$$

*où $iH_n(\mathbb{C}) = \{\text{matrices antihermitiennes i.e. tel que } M^* = -M\}$*

*Démonstration.* On pose

$$H = \frac{1}{2}(A + A^*)$$
$$R = \frac{1}{2i}(A - A^*)$$

Alors, $A = H + iR$, $H^* = H$, $R^* = -R$. □

On a vu l'effet d'un changement de base, soit $h$ est une forme hermitienne, $H$ est sa matrice dans une base $e$ et $H'$ est sa matrice dans une autre base $e'$.

Si $P$ est la matrice de passage, alors

$$H' = P^* H P$$

On constate qu'on a une action de $GL_n(\mathbb{C})$ sur les matrices hermitiennes $P \in GL_n(\mathbb{C})$, $H \in H_n(\mathbb{C})$,

$$P \cdot H = (P^{-1})^* H P^{-1}$$

## 10.1 Orthogonalité

Soit $h$ une forme hermitienne non dégérée (i.e. sa matrice dans une base quelconque est inversible).

**Définition 10.10.** $A \subset E$, alors,

$$A^{\perp} = \{x \in E \mid \forall y \in A, \varphi(x,y) = 0\}$$

est un sous espace vectoriel.

**Proposition 10.11.** *Si $V \subset E$ est un sous espace vectoriel de dimension $p$ et $\dim E = n$, alors $V^{\perp}$ est de dimension $n-p$.*

*Démonstration.* Soit $\overline{\varphi} : E \to E^*$ antilinéaire bijective, $\overline{\varphi}(V^{\perp})$ est l'orthogonal est de $V$ dans $E^*$.

On sait que cet orthogonal est de dimension $n-p$ ($V^{\circ}$(vu dans $E*$) $\simeq (E/V)^*$).

Et comme $\overline{\varphi}$ est bijective, on a

$$\dim V^{\perp} = n - p$$

□

Attention : on n'a pas toujours que $V \cap V^{\perp} = \{0\}$.

**Exemple.** $\varphi(x,y) = \overline{x_1}y_1 - \overline{x_2}y_2$ sur $\mathbb{C}^2$, $h(x) = |x_1|^2 - |x_2|^2$, alors,

$$\varphi(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}) = 0$$

**Définition 10.12.** $x \in E$ est dit isotrope si $\varphi(x,x) = 0$.

**Définition 10.13.** Un sous espace vectoriel $V$ est dit isotrope si $V \cap V^{\perp} \neq \{0\}$.

**Proposition 10.14.** *Si $V$ est un espace vectoriel non isotrope, alors,*

$$E = V \oplus V^{\perp}$$

**Proposition 10.15.** *Si $E$ est de dimension finie, $V$ et $W$ sont des sous espace vectoriel de $E$, alors,*

*(1) $(V^{\perp})^{\perp} = V$.*

*(2)* $(V+W)^\perp = V^\perp \cap W^\perp$.

*(3)* $(V \cap W)^\perp = V^\perp + W^\perp$.

*Démonstration.* (1) On a $V \subset (V^\perp)^\perp$, d'où égalité via les dimensions.

(2)immédiate.

(3) S'en déduit par passage à l'orthogonal. □

**Définition 10.16.** Soit $\varphi$ sesquilinéaire à symétrie hermitienne sur $E$ de dimension finie, une base $(e_1, \ldots, e_n)$ de $E$ est dit orthogonale si $\forall i \neq j$, $\varphi(e_i, e_j) = 0$. Dans cette base, la matrice de $\varphi$ est diagonale.

**Définition 10.17.** Soit $\varphi$ comme ci-dessus, on appelle rang de $\varphi$, noté $\mathrm{rg}(\varphi)$, le rang de sa matrice dans une base quelconque.

**Théorème 10.18.** *Soient $E$ un $\mathbb{C}$-espace vectoriel de dimension $n$, $\varphi$ sesquilinéaire à symétrie hermitienne, alors, il existe une base de $E$ dans laquelle la matrice de $\varphi$ est de la forme :*

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

*Soient $r$ le nombre de $1$ et $s$ le nombre de $-1$, le couple $(r, s)$ est appelé la signature de $\varphi$ et il est complètement déterminé par $\varphi$, on a*

$$r + s = rg(\varphi)$$

*Démonstration.* On se ramène au cas où $\varphi$ est non dégénérée.

Si $N$ est le noyau de $\varphi$, i.e.

$$N = \{x \in E \mid \forall y, \varphi(x, y) = 0$$

un sous espace vectoriel de $E$.

On peut prendre un supplémentaire $F$ de $N$, et la restriction de $\varphi$ à $F$ est alors non dégénérée (Sinon, $\exists y \in F$, tel que $\forall z \in F, \varphi(y,z) = 0$ et alors on a aussi $\forall z \in N, \varphi(y,z) = 0$, d'où $y \in N$ et $y = 0$.)

On procède par récurrence sur $\dim E = n$.

$n = 1$, clair.

$n \geq 2$, il existe dans $E$ un $x$ non isotrope (sinon, $\forall x, h(x) = \varphi(x,x) = 0$ et par polorisation, $\forall x, y,\ \varphi(x,y) = 0$.

Soit $e_1 \in E$, tel que $\varphi(e_1, e_1) \neq 0$, $V = \mathbb{C}e_1$ est nonisotrope et

$$E = \mathbb{C}e_1 \oplus (\mathbb{C}e_1)^{\perp}$$

On considère la restrictino de $\varphi$ à $(\mathbb{C}e_1)^{\perp}$ à qui on peut appliquer l'hypothèse de récurrence.

On trouve une base $(e_2, \ldots, e_n)$ dans laquelle la matrice de $\varphi$ est de la forme :

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \end{pmatrix}$$

On sait que $\varphi(e_1, e_1) \in \mathbb{R}$, on pose

$$e_1' = \begin{cases} \dfrac{1}{\sqrt{\varphi(e_1,e_1)}} e_1, \text{ si } \varphi(e_1,e_1) > 0 \\ -\dfrac{1}{\sqrt{\varphi(e_1,e_1)}} e_1, \text{ si } \varphi(e_1,e_1) < 0 \end{cases}$$

et dans la base $(e_1', e_2, \ldots, e_n)$, $\varphi$ est (à permutation près) de la forme voulue.

Ici, $r + s = \mathrm{rg}(\varphi)$.

De plus, $r$ et $s$ sont bien déterminés par $\varphi$.

Supposons $\varphi$ non dégénérée et qu'il existe 2 bases de $E$ $(e_1, \ldots, e_n)$, $(e_1', \ldots, e_n')$ dans lesquelles

$\varphi$ aurait pour matrice

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \end{pmatrix}$$
$$\underbrace{\qquad\qquad}_{r}\ \underbrace{\qquad\qquad}_{s}\qquad\qquad \underbrace{\qquad\qquad}_{r'}\ \underbrace{\qquad\qquad}_{s'}$$

et on a

$$r + s = r' + s' = n$$

Soit $F = \mathrm{Vect}(e_1, \dots, e_r)$ et $G = \mathrm{Vect}(e'_{r+1}, \dots, e'_n)$.

Si $x \in F \cap G$, $x \neq 0$, on a :

$\varphi(x, x) > 0$, vu dans $F$.

$\varphi(x, x) < 0$, vu dans $G$.

C'est impossible, alors,

$$F \cap G = \{0\}$$

Donc, on a

$$r + s' \leq n,\ r \leq n - s' = r'$$

par symétrie, $r' \leq r$, où

$$r = r'$$

□

**Définition 10.19.** Deux formes sesquilinéaires $\varphi, \psi$ à symétrie hermitienne sont dites équivalentes s'il existe $u \in GL(E)$, tel que

$$\forall x, y \in E,\ \psi(x, y) = \varphi(u(x), u(y))$$

En termes de matrices, si $A, B$ sont leurs matrices dans même base de $E$, $\exists P \in GL(E)$, tel que $B = P^* AP$ (i.e. dans la même orbite pour l'action de $GL(E)$).

**Théorème 10.20.** *Deux formes $\varphi$, $\psi$ sont équivalentes si et seulement si elles ont même signature.*

**Définition 10.21.** Une forme hermitienne est dite positive si $\forall x \in E$, $h(x) \geq 0$ ; est dite définie positive si $\forall x \in E$, $h(x) \geq 0$ et $h(x) = 0 \Rightarrow x = 0$ (i.e. $\forall x \neq 0$, $h(x) > 0$).

**Définition 10.22.** Une forme hermitienne définie positive est appelée produit scalaire hermitienne.

**Exemple.** Dans $M_n(\mathbb{C})$, on pose $\varphi(A, B) = \mathrm{Tr}(A^* B)$, alors

$$\begin{aligned} \varphi(B, A) &= \mathrm{Tr}(B^* A) \\ &= \mathrm{Tr}((A^* B)^*) \\ &= \overline{\mathrm{Tr}({}^t(A^* B))} \\ &= \overline{\mathrm{Tr}(A^* B)} \\ &= \overline{\varphi(A, B)} \end{aligned}$$

et

$$\varphi(A, A) = \sum_{1 \leq i,j \leq n} |a_{ij}|^2$$

**Inégalité de Cauchy-Schwarz**

**Théorème 10.23.** *Soit $h$ une forme hermitienne $\geq 0$, $\varphi$ une forme sesquilinéaire associée, alors, $\forall x, y \in E$, on a*

$$|\varphi(x, y)| \leq \sqrt{h(x) h(y)}$$

*De plus, si $h$ est définie positive, il y a égalité si et seulement si $x$ et $y$ sont liés.*

*Démonstration.* Soient $x, y \in E$, alors,

$$\forall \lambda \in \mathbb{C}, \ \varphi(x + \lambda y, x + \lambda y) \geq 0$$

c'est-à-dire que

$$h(x) + |\lambda|^2 h(y) + 2\,\mathrm{Re}(\lambda \varphi(x, y)) \geq 0$$

Posons $\varphi(x, y) = \rho e^{i\theta}$, $\rho \geq 0$.

Si $\rho = 0$, OK.

On suppose que $\rho > 0$, posons $\lambda = t\rho^{-i\theta}, t \in \mathbb{R}$.

On a

$$h(x) + t^2 h(y) + 2\rho t \geq 0$$

Ce polynôme réel en $t$ de degré 2 doit avoir un discriminant $\leq 0$ :

$$\rho^2 - h(x)h(y) \leq 0 \Rightarrow |\varphi(x, y)|^2 \leq h(x)h(y)$$

Si $h$ est définie positive et cas d'égalité, le polynôme a une racine double $t_0$ et $\varphi(x + \lambda y, x + \lambda y) = 0$, $\lambda = t_0 e^{-i\theta}$, alors,

$$x = -t_0 e^{-i\theta} y$$

□

**Norme associée à une forme hermitienne définie positive :**

On note $< x, y >= \varphi(x, y)$.

**Proposition 10.24.** *L'application*

$$x \mapsto \sqrt{h(x)} = \|x\|$$

*est une norme sur $E$.*

*Démonstration.* On a $\|x\| \geq 0$ et $\|x\| = 0 \Leftrightarrow x = 0$.

$\|\lambda x\| = |\lambda| \|x\|$ : clair.

Inégalité triangulaire :

On a

$$\begin{aligned}
\|x + y\|^2 &= h(x + y) \\
&= h(x) + h(y) + 2 \operatorname{Re} < x, y > \\
&\leq h(x) + h(y) + 2\sqrt{h(x)h(y)} \\
&= (\sqrt{h(x)} + \sqrt{h(y)})^2
\end{aligned}$$

alors, on a

$$\|x + y\|^2 \leq \|x\|^2 + \|y\|^2$$

Cas d'égalité : on doit avoir

$$\mathrm{Re} < x, y >= \sqrt{h(x)h(y)}$$

d'où déjà égalité dans Cauchy-Schwartz, d'où $y = \lambda x$ avec $\lambda \in \mathbb{C}$.

Alors,

$$\mathrm{Re} < x, \lambda x >= \sqrt{h(x)}\sqrt{|\lambda|^2 h(x)} = |\lambda| h(x)$$

alors, on a

$$h(x)\,\mathrm{Re}(\lambda) = |\lambda| h(x)$$

d'où $\mathrm{Re}(\lambda) = |\lambda|$, i.e. $\lambda \in \mathbb{R}^+$.

Conclusion : il y a égalité dans l'inégalité triangulaire si et seulement si $x$ et $y$ sont positivement liés. $\square$

## 10.2 Espace hermitien

**Définition 10.25.** On appelle espace préhilbertien un $\mathbb{C}$-espace vectoriel muni un produit scalaire hermitienne (pas nécessairement de dimension finie) si l'espace est de plus de dimension finie. On parle d'espace hermitien.

*Remarque.* On dispose ainsi d'une norme, donc d'une topologie.

*Remarque.* On a introduit, pour $M \in M_n(\mathbb{C}^*)$, $M^* =^t \overline{M}$, on l'appelle matrice adjointe.

Dorénavant, $(E, <>)$ est un espace hermitien.

**Proposition 10.26.** *(Adjoint d'un endomorphisme)*

*Soit $u \in \mathcal{L}(E)$, il existe un unique $u^* \in \mathcal{L}(E)$ tel que*

$$\forall x, y \in E,\ < u(x), y >=< x, u^*(y) >$$

*Cet endomorphisme $u^*$ est appelé adjoint de $u$.*

*Démonstration.* On utilise le fait que toute forme linéaire sur $E$ est de type $y \mapsto < x, y >$ pour un certaint $x \in E$.

Soit $u \in \mathcal{L}(E)$, $x \in E$, alors, l'application :

$$\begin{aligned} E &\to \mathbb{C} \\ y &\mapsto < x, u(y) > \end{aligned}$$

est forme linéaire.

Donc, $\exists x' \in E$, tel que $\forall y \in E$,

$$< x', y >=< x, u(y) >$$

Posons $x' = u * (x)$, on vérifie que $x \mapsto u^*(x)$ est linéaire.

$$\begin{aligned} < u^*(x + \lambda z), y > &=< x + \lambda z, u(y) > \\ &=< x, u(y) > +\overline{\lambda} < z, u(y) > \\ &=< u^*(x), y > +\overline{\lambda} < u^*(z), y > \\ &=< u^*(x) + \lambda u^*(z), y > \end{aligned}$$

d'où

$$u^*(x+\lambda z) = u^*(x) + \lambda u^*(z)$$

En suite, on a

$$\begin{aligned} < u(x), y > &= \overline{< y, u(x) >} \\ &= \overline{< u^*(y), x >} \\ &=< x, u^*(y) > \end{aligned}$$

□

**Proposition 10.27.** *(1)* $(u^*)^* = u$.

*(2)* $(u+\lambda v)^* = u^* + \overline{\lambda} v^*$.

*(3)* $(u \circ v)^* = v^* \circ u^*$.

*Démonstration.* (3) on a

$$\begin{aligned} < x, (u \circ y)^*(x) > &=< u \circ v(x), y > \\ &=< v(x), u^*(y) > \\ &=< x, v^* \circ u^*(y) > \end{aligned}$$

□

**Proposition 10.28.** $\ker u^* = (\operatorname{Im} u)^\perp$, $\operatorname{Im} u^* = (\ker u)^\perp$.

*Démonstration.* On a :

$$\begin{aligned} x \in \ker u^* &\Leftrightarrow u^*(x) = 0 \\ &\Leftrightarrow \forall y,\ < u^*(x), y >= 0 \\ &\Leftrightarrow \forall y,\ < x, u(y) >= 0 \\ &\Leftrightarrow x \in (\operatorname{Im} u)^\perp \end{aligned}$$

□

**Proposition 10.29.** *Soit $u \in \mathcal{L}(E)$, $e = (e_1, \dots, e_n)$ base orthonomale de $E$, i.e. une base telle que $< e_i, e_j >= \delta_{ij}$ et $M$ est la matrice de $u$ dans $e$. Alors, la matrice de $u^*$ dans $e$ est $M^*$.*

*Démonstration.* Notons $M = (m_{ij})$, alors,

$$u(e_j) = \sum_{i=1}^{n} m_{ij} e_i$$

et on a alors

$$\begin{aligned} m_{ij} &=< e_i, u(e_j) > \\ &=< u^*(e_i), e_j > \\ &= \overline{< e_j, u^*(e_i) >} \\ &= \overline{m'_{ji}} \end{aligned}$$

et

$$M' = (m'_{ij}) = \mathrm{Mat}(u^*)$$

□

**Endomorphisme normaux**

**Définition 10.30.** Soit $E$ un espace hermitien, $u \in \mathcal{L}(E)$ est dit normal, si

$$uu^* = u^*u$$

**Théorème 10.31.** *Les conditions suivantes sont équivalentes, pour $u \in \mathcal{L}(E)$.*

*(1) $u$ est normal.*

*(2) $\forall x \in E$, $\|u(x)\| = \|u^*(x)\|$.*

*(3) $\forall F$ sous-espace vectoriel par $u$, $F$ est stable par $u^*$.*

*(4) $\forall F$ sous-espace vectoriel par $u$, $F^\perp$ est stable par $u$.*

*(5) $u$ est diagonalisable en base orthonormée.*

*Démonstration.* (1) $\Rightarrow$ (2) On a

$$\begin{aligned}\|u(x)\|^2 &= (u(x), u(x))\\ &= (u^*u(x), x)\\ &= (uu^*(x), x)\\ &= (u^*(x), u^*(x))\\ &= \|u^*(x)\|^2\end{aligned}$$

(2) $\Rightarrow$ (1) On utilise un lemme : soit $f \in \mathcal{L}(E)$, tel que $\forall x, < f(x), x >= 0$, alors, $f = 0$.

*Remarque.* Ici, $E$ est un espace hermitien sur $\mathbb{C}$, le résultat est faux sur $\mathbb{R}$.

Posons :

$$g_1 = \frac{1}{2}(f + f^*),\ g_2 = \frac{1}{2i}(f - f^*)$$

alors, on a

$$g_1^* = g_1,\ g_2^* = g_2$$

et $f = g_1 + ig_2$.

On a

$$< f(x), x >=< g_1(x), x > -i < g_2(x), x >$$

mais $< g_1(x), x >= 0$, car

$$\begin{aligned}< g_1(x), x > &=< x, g_1(x) >\\ &= \overline{< g_1(x), x >}\end{aligned}$$

de même $< g_2(x), x >\in \mathbb{R}$.

Alors, $\forall x$, on a

$$< g_1(x), x >= 0,\ < g_2(x), x >= 0$$

Posons $\varphi(x, y) =< g_1(x), y >$, $\varphi$ est une forme sesquilinéaire à symétrie hermitienne.

On a

$$\forall x,\ \varphi(x, x) = 0$$

donc, par polorisation :

$$\forall x, y,\ \varphi(x, y) = 0$$

i.e. $< g_1(x), y >= 0$.

À $x$ fixé :

$$\forall y,\ < g_1(x), y >= 0 \Rightarrow g_1(x) = 0$$

De même $g_2(x) = 0$, alors $f = 0$.

Retour à (2) $\Rightarrow$ (1) On suppose $\forall x,\ \|u(x)\|^2 = \|u^*(x)\|^2$, alors

$$\begin{aligned} & < u(x), u(x) >=< u^*(x), u^*(x) > \\ \Rightarrow & < u^*u(x), x >=< uu^*(x), x > \\ \Rightarrow & < (uu^* - u^*u)(x), x >= 0,\ \forall x \end{aligned}$$

Prenant $f = u^*u - uu^*$ dans le lemme, on a

$$u^*u = uu^*$$

(1) $\Rightarrow$ (3) et (4) On a $E = F \oplus F^\perp$ et on choisit des bases orthonormées, elles forment alors une base orthonormée de $E$.

La matrice de $u$ et $u^*$ est :

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} et \begin{pmatrix} A^* & 0 \\ B^* & C^* \end{pmatrix}$$

car on a pris une base orthonormée de $E$.

On constate :

$F$ est stable par $u^* \Leftrightarrow B^* = 0$.

$F^\perp$ est stable par $u \Leftrightarrow B = 0$.

De plus, on a

$$MM^* = \begin{pmatrix} AA^* + BB^* & BC^* \\ CB^* & CC^* \end{pmatrix},\ M^*M = \begin{pmatrix} A^*A & A^*B \\ B^*A & B^*B + C^*C \end{pmatrix}$$

Donc,

$$MM^* = M^*M \Rightarrow AA^* + BB^* = A^*A$$

et alors, on a

$$Tr(AA^* + BB^*) = Tr(AA^*) \Rightarrow Tr(BB^*) = 0$$

On pose $B = (b_{ij})_{1 \leq i \leq \dim F, 1 \leq j \leq \dim F^*}$, alors

$$Tr(BB^*) = \sum_{i,j} |b_{ij}|^2 = 0$$

d'où $\forall i, j,\ |b_{ij}| = 0$ et $B = 0$.

Inversement, si on a (3) ou (4), on a $B = 0$.

(4) $\Rightarrow$ (5) Sur $\mathbb{C}$, $u$ possède au moins une valeur propre.

On fait une démonstration par récurrence sur $\dim E$.

- $n = 1$, c'est clair.
- $n \geq 2$ Soit $\lambda \in \mathbb{C}$ un valeur propre et $x \neq 0$ un vecteur propre

$F = \mathbb{C}x$ est stable par $u$, donc $F^\perp$ l'est aussi.

Dans des bases adaptées, $u$ et $u*$ ont pour matrices :

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix} et \begin{pmatrix} \overline{\lambda} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C^* & \\ 0 & & & \end{pmatrix}$$

Alors,

$$uu^* = u^*u \Rightarrow CC^* = C^*C$$

Ainsi, les restrictions de $u$ et $u^*$ à $F^\perp$ commutent.

$u|_{F^\perp}$ est normal et on applique la récurrence :

Il existe une base orthonormée de $F^\perp$ formé de vecteur propres de $u$, d'où, avec $x$, une base orthonormée de $E$, dans laquelle $u$ est diagonal.

(5) $\Rightarrow$ (1) Si, dans une base orthonormée, $u$ et $u^*$ a pour matrice

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} et \begin{pmatrix} \overline{\lambda_1} & & \\ & \ddots & \\ & & \overline{\lambda_n} \end{pmatrix}$$

d'où

$$uu^* = u^*u$$

□

**Corollaire 10.32.** *$M \in M_n(\mathbb{C})$ avec $MM^* = M^*M$, alors $\exists u \in GL_n(\mathbb{C})$, $u^*u$ =Id, tel que $uMu^*$ est diagonale.*

**Définition 10.33.** Une matrice unitaire :

$u \in GL_n(\mathbb{C})$, tel que $u^*u = u^*u = I_n$.

*Remarque.* $u$ est unitaire $\Leftrightarrow$ ses vecteurs colonnes forment une base orthonomée de $\mathbb{C}^*$ muni du produit scalaire hermitien usuel.

(Exercice : le vérifier.)

Cas particulier du théorème

(1) Endomorphismes hermitiens :

$u \in \mathcal{L}(E)$, tel que $u = u^*$, $u$ est diagonalisable en base orthonomée et de plus, ses valeurs propres sont réelles.

Ceci caractérise les endomorphismes hermitiens.

(2) Endomorphismes antihermitiens :

$v \in \mathcal{L}(E)$, tel que $v^* = -v$, i.e. $v = iu$ avec $u$ hermitient, les endomorphisme antihermitiens sont diagonalisables en base orthonormée de valeurs propres imaginaires pure.

Ceci les caractérise.

(3) Endomorphismes unitaires :

$u \in \mathcal{L}(E)$, tel que $uu^* = u^*u = \text{Id}$, ceci signifie que $u$ préserve le produit scalaire hermitien :

$$\forall x, y, \ < u(x), u(y) >=< x, y >$$

Par polorisation, c'est aussi équivalent à

$$\forall u \in E, \ \|u(x)\| = \|x\|$$

Résultat :

$u \in \mathcal{L}(E)$ unitaire si et seulement si $u$ est diagonalisalbe en base orthonormée avec des valeurs propres de module 1 :

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \begin{pmatrix} \overline{\lambda_1} & & \\ & \ddots & \\ & & \overline{\lambda_n} \end{pmatrix} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

## 10.3 Projecteurs orthogonaux

$E$ hermitien, $F \subset E$, le projecteur orthogonal sur $F$ est le projecteur d'image $F$ et de noyau $F^\perp$.

**Proposition 10.34.** *Un projecteur $p$ est orthogonal si et seulement si $p = p^*$, i.e. les projecteurs orthogonaux sont caractérisés par :*

$$p^2 = p, \;\; p^* = p$$

*Démonstration.* Si $p$ est orthogonal, alors $\ker p = (\operatorname{Im} p)^\perp$ et dans une base orthonomée sa matrice

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

qui est hermitienne.

Inversement, si $p = p^*$, ses sous-espace propres sont orthogonaux, en effet, si $x$ et $y$ sont deux vecteurs propres de différents valeurs propres :

$$\begin{aligned} < x, y > &=< \frac{1}{\lambda_1} px, y > \\ &=< \frac{1}{\lambda_1} x, p^* y > \\ &=< \frac{1}{\lambda_1} x, py > \\ &= \frac{\lambda_2}{\lambda_1} < x, y > \end{aligned}$$

alors,

$$< x, y >= 0$$

et on a

$$(\operatorname{Im} p)^\perp = \ker p$$

$\square$

#### Symétries orthogonales

Ce sont des symétries, i.e. $s \in \mathcal{L}(E)$, tel que $s^2 = \mathrm{Id}$ et tels que les sous-espace propres, pour les valeurs propres 1 et -1 sont orthohonaux.

Une symétrie orthogonale est caractérisée par

$$s^2 = \mathrm{Id},\ \ s = s^*$$

*Remarque.* Si $F \subset E$, $(e_1, \ldots, e_n)$ une base orthonormée de $F$, alors le projecteur orthogonal sur $F$ est donnée par :

$$\forall x \in E,\ \ p(x) = \sum_{i=1}^{k} < e_i, x > e_i$$

Si $s$ est le symétrie orthogonale par rapport un sous-espace $F$ (i.e. $F = \ker(s - Id)$, on l'obtient à partir du projecteur orthogonal par :

$$s(x) = 2p(x) - x$$

<u>Orthonormalisation :</u> Procédé de Gram-Schmidt

Soit $(e_1, \ldots, e_n)$ une base quelconque de $E$, alors il existe une base orthonormée de $E$, $(v_1, \ldots, v_n)$, telle que, $\forall i \in \{1, \ldots, n\}$,

$$\mathrm{Vect}(e_1, \ldots, e_i) = \mathrm{Vect}(v_1, \ldots, v_i)$$

i.e. la matrice de changement de base est triangulaire supérieure.

Si on impose que les coefficients diagonaux sont $> 0$, elle est unique.

*Démonstration.* On procède pas à pas :

$$\begin{aligned} v_1 &= \frac{e_1}{\|e_1\|} \\ v_2' &= e_2 - < v_1, e_2 > v_1 \in \mathrm{Vect}(e_1, e_2) \end{aligned}$$

alors, $< v_1', v_2 >= 0$ et on pose

$$v_2 = \frac{v_2'}{\|v_2'\|}$$

À la $k^e$ étape : si on a déjà $v_1, \ldots, v_{k-1}$, on prend pour $v_k'$ :

$$v_k' = e_k - \sum_{j=1}^{k-1} < v_j, e_k > v_j \neq 0$$

car $e_k \notin \mathrm{Vect}(v_1, \ldots, v_{k-1}) = \mathrm{Vect}(e_1, \ldots, e_{k-1})$, on a

$$\forall j \in 1, \ldots, k-1, \; < v_j, v'_k >= 0$$

et on pose

$$v_k = \frac{v'_k}{\|v'_k\|}$$

$\square$

Interprètation :

Si $A \in GL_n(\mathbb{C})$, il existe $U$ unitaire et $T$ triangulaire supérieure à termes diagonaux $> 0$, tel que

$$A = U \cdot T$$

et ce couple est unique.

En effet, les vecteurs colonnes de $A$ forment une base de $E$, on applique à cette base le procédé de Gram-Schmidt et on obtient une base orthonormée, i.e. les vecteurs colonnes d'une matrice unitaire.

Notation :

$U_n(\mathbb{C}) = \{\text{matrices unitaire}\}$

*Remarque.* Si $u \in U_n(\mathbb{C})$, $\det u$ est de module 1.

**Définition 10.35.** $SU_n(\mathbb{C}) = \{u \in U_n(\mathbb{C}) \mid \det u = 1\}$

Dans $U_n(\mathbb{C})$, on dispose de matrice

$$\begin{array}{cc} & \begin{array}{ccccccc} \phantom{1} & \phantom{\ddots} & \phantom{1} & i & \phantom{1} & \phantom{\ddots} & \phantom{1} \end{array} \\ i & \begin{pmatrix} 1 &&&&&& \\ & \ddots &&&&& \\ && 1 &&&& \\ &&& \lambda &&& \\ &&&& 1 && \\ &&&&& \ddots & \\ &&&&&& 1 \end{pmatrix} \end{array} = D_i(\lambda)$$

avec $|\lambda| = 1$.

Leurs conjugées dans $U_n(\mathbb{C})$ sont appelées "pseudo réflextions".

Une pseudo réflextion est ainsi $u \in U(E)$ groupe unitaire telle que $\ker(u - Id)$ hyperplan et sur $\ker(u - Id)^{\perp}$, $u$ agit par multiplication par un nombre complexe de module 1.

**Proposition 10.36.** *Le centre est*

$$Z(U_n(\mathbb{C})) = \{\lambda Id \mid |\lambda| = 1\}$$

*Démonstration.* $A \in Z(U_n(\mathbb{C}))$, $A$ doit commuter avec toutes les pseudos réflexions, donc stabiliser toutes les droites vectionnelles, donc être une homothétie. □

**Proposition 10.37.** $U_n(\mathbb{C})$*,* $SU_n(\mathbb{C})$ *sont compacts.*

*Démonstration.* Prenons la norme sur $M_n(\mathbb{C})$, déduite de celle de $\mathbb{C}^n$ avec la norme hermitienne, i.e.

$$\|A\| = \sup_{x \in \mathbb{C}^n,\ \|x\|=1} \|Ax\|$$

Alors, $A \in U_n(\mathbb{C})$ (resp. $SU_n(\mathbb{C})$) si et seulement si

$$uu^* = I (\text{resp. } u^*u = I,\ \det u = 1)$$

Or les applications $u \mapsto u^*$ et le produit sont des applications continues, donc ces conditions définissent des sous espaces fermés, de plus, si $u \in U_n(\mathbb{C})$, $\|u\| = 1$, donc, ils sont bornés. □

**Racine carrée positive :**

**Définition 10.38.** Soit $u \in \mathcal{L}(E)$ hermitient, on dit que $u$ est positif si $\forall x \in E, < u(x), x > \geq 0$, ceci équivaux à $\forall \lambda$ valeur propre de $u$, $\lambda > 0$.

*Démonstration.* $\Rightarrow$ Immédiat.

$\Leftarrow$ On prend une base orthonormée de vecteurs propres $(e_1, \ldots, e_n)$ de valeurs propres $\geq 0$, $\lambda_1, \ldots, \lambda_n$.

Alors, $\forall x \in E$, $x = \sum_{i=1}^{n} x_i e_i$ et

$$< u(x), x >=< \sum_{i=1}^{n} x_i \lambda_i e_i, \sum_{i=1}^{n} x_i e_i >= \sum_{i=1}^{n} \lambda_i |x_i|^n$$

□

**Proposition 10.39.** *Soit $u \in \mathcal{L}(E)$, hermitien positif, alors $\exists v \in \mathcal{L}(E)$ hermitien positif, tel que $u = v^2$.*

*Démonstration.* On se place dans une base orthonormée de vecteurs propres $(e_1, \ldots, e_n)$, valeurs propres $\lambda_i \geq 0$, on dispose des $\sqrt{\lambda_i}$.

On prend l'endomorphisme ayant $e_1, \ldots, e_n$ pour vecteur propres et $\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n}$ comme valeurs propres associée. □

*Remarque.* $v$ est unique car si $v^2 = u$, $v$ commute avec $u$, donc stabilise les sous espaces propres de $u$.

Sa restriction à un sous espace propre est hermitienne car $v$ l'est et les sous espaces propres sont orthogonaux et $v^2 = \lambda \text{ Id}$, alors $v = \sqrt{\lambda}\text{Id}$ si $v$ est hermitien positif.

**Décomposition polaire :**

**Définition 10.40.** Une endomorphisme hermitienne est strictement positve si $\forall x \in E, x \neq 0$, $< u(x), x > \geq 0$, ceci équivaut à ce que toutes les valeurs propres de $u$ sont $> 0$.

**Définition 10.41.** Analogue d'une matrice hermitienne $> 0$.

**Théorème 10.42.** *Soit $A \in GL_n(\mathbb{C})$, alors il existe un unique couple $(U, H)$ avec $U \in U_n(\mathbb{C})$ et $H$ hermitienne $> 0$, tels que $A = U \cdot H$.*

*Remarque.* Ceci est l'analogue dans le cadre matriciel de l'écriture :

$$\forall z \neq 0, \exists \rho > 0, \theta \in \mathbb{R},\ z = \rho e^{i\theta}$$

*Démonstration.* Si $(U, H)$ exists, $A = UH$, $A^* = H^* U^*$, alors

$$A^* A = H^* H = H^2$$

Remarque important : si $A \in GL_n(\mathbb{C})$, $A^* A$ est hermitienne $> 0$, en effet, on a

$$< A^* Ax, x >= \|Ax\|^2$$

Ainsi, $H$ est nécessairement l'unique racine carrée strictement positive de $A^* A$.

Soit donc $H$ cette racine carrée. Comme on veut $A = UH$, on prend $U = AH^{-1}$ et on vérifie que $U \in U_n(\mathbb{C})$ :

$$U^* U = H^{-1} A^* A H^{-1} = Id$$

□

**Proposition 10.43.** *Soit $A \in M_n(\mathbb{C})$, alors $\exists U$ unitaire, $\exists H$ hermitienne $\geq 0$, tels que $A = UH$.*

*Démonstration.* On utilise le résultat précédent et la densité de $GL_n(\mathbb{C})$ dans $M_n(\mathbb{C})$ :

Si $A \in M_n(\mathbb{C})$, $\exists \rho > 0$, tel que

$$\forall z \in \mathbb{C}, 0 < |z| < \rho,\ A - zI \in GL_n(\mathbb{C})$$

ceci set vrai car $\det(A - zI) = \chi_A(z)$ n'a qu'un nombre fini de racine.

Retour au démonstration :

Soit $A \in M_n(\mathbb{C})$, $\exists$ une suite $(A_k)_{k\in\mathbb{N}}$, $A_k \in GL_n(K)$, telle que $A_k \to A$ dans $M_n(\mathbb{C})$.

Pour chaque $A_k$, on a $A_k = U_k H_k$, avec $U_k \in U_n(\mathbb{C})$, $H_k > 0$.

$U_n(\mathbb{C})$ est compact : il existe une sous-suite $(U_{\varphi(k)})$ qui converge vers $U \in U_n(\mathbb{C})$, $(A_{\varphi(k)})$ converge encore vers $A$.

Alors,

$$H_{\varphi(k)} = U^*_{\varphi(k)} A_{\varphi(k)}$$

converge vers une matrice $H$, avec $H^* = H$ et $H \geq 0$, d'où $H = U^* A$, $A = UH$. □

## 10.4 Matrice de Gram d'un système de vecteurs

$E$ hermitien, $(e_1, \ldots, e_n)$ des vecteurs de $E$.

**Définition 10.44.** La matrice de Gram de ce système est

$$G(e_1, \ldots, e_n) = (< e_i, e_j >)_{1 \leq i,j \leq k} \in M_k(\mathbb{C})$$

**Proposition 10.45.** *(1) $G(e_1, \ldots, e_n)$ est hermitienne $\geq 0$ et elle est $> 0$, si et seulement si $e_1, \ldots, e_n$ est famille libre.*

*(2) $rgG(e_1, \ldots, e_n) = \dim$ Vect$(e_1, \ldots, e_n)$.*

*Démonstration.* On note $G(e_1, \ldots, e_n) = (g_{ij})$ et $g_{ij} =< e_i, e_j >= \overline{< e_j, e_i >} = \overline{g_{ij}}$, d'où hermitienne.

Calculons, dans $\mathbb{C}^n$, pour $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$,

$$\begin{aligned} < G(x), x > &= \sum_{1 \leq i,j \leq n} \overline{x_i} < e_i, e_j > x_j \\ &= \sum_{1 \leq i,j \leq n} < x_i e_i, x_j e_j > \\ &=< \sum_{1 \leq i \leq n} x_i e_i, \sum_{1 \leq j \leq n} x_j e_j > \\ &= \| \sum_{1 \leq i \leq n} x_i e_i \|^2 \geq 0 \end{aligned}$$

On a écrit $< G(x), x >$ produit scalaire dans $\mathbb{C}^k$ pour $x =< x_1, \ldots, x_n >$ en terme du produit scalaire dans $E$ du vecteur $\sum_{i=1}^{x} x_i e_i \in E : < G(x), x >= \| \sum_{1 \leq i \leq n} x_i e_i \|^2$

On voit que

$$< G(x), x >= 0 \Leftrightarrow \sum_{i=1}^{n} x_i e_i = 0$$

Considérons donc l'application linéaire :

$$\begin{aligned} f : \mathbb{C}^n &\to E \\ (x_1, \ldots, x_n) &\mapsto \sum_{i=1}^{n} x_i e_i \end{aligned}$$

On a

$$\operatorname{Im} f = \operatorname{Vect}(e_1, \dots, e_n)$$
$$rgf = \dim \operatorname{Vect}(e_1, \dots, e_n)$$

Comme $G$ est hermitienne positive, on dispose de la forme sesquilinéaire à symétrie hermitienne :

$$\varphi : (x, y) \mapsto < G(x), y >$$

$\varphi$ est positive.

Alors, l'inégalité de Cauchy schiwarz dit que

$$G(x) = 0 \Leftrightarrow < G(x), x >= 0$$

$\Rightarrow$ clair.

$\Leftarrow < G(x), y > \leq \sqrt{< G(x), x >}\sqrt{< G(y), y >}$, si $< G(x), x >= 0$, alors $\forall y$, $< G(x), y >= 0$ dans $\mathbb{C}^n$, donc $G(x) = 0$.

Ainsi,

$$x \in \ker G \Leftrightarrow < G(x), x >= 0 \Leftrightarrow f(x) = 0$$

Ainsi,

$$rgf = \dim \operatorname{Vect}(e_1, \dots, e_n)$$

$\square$

Soit $V = (e_1, \dots, e_n)$ et notons $d$ la distance déduite de la norme.

**Théorème 10.46.** *Si $a \in E$, alors $d(a, V)^2 = \frac{|G(a_1, e_1, \dots, e_n)|}{|G(e_1, \dots, e_n)|}$.*

*Démonstration.* Si $p$ est la projection orthogonal $E \to V$, alors

$$d(a, V) = \|a - p(a)\|$$

Posons $p(a) = \sum_{i=1}^{n} \lambda_i e_i$, $\lambda_i \in \mathbb{C}$.

On a

$$G(a, e_1, \ldots, e_n) = \begin{pmatrix} < a, a > & < a, e_1 > & \cdots & < a, e_n > \\ < e_1, a > & < e_1, e_1 > & \cdots & < e_1, e_n > \\ \vdots & \vdots & \vdots & \vdots \\ < e_n, a > & < e_n, e_1 > & \cdots & < e_n, e_n > \end{pmatrix}$$

Appelons $C_0, C_1, \ldots, C_n$ les vecteurs colonnes, on remplace $C_0$ par $C_0 - \sum_{i=1}^n \lambda_i C_i$, ceci ne change pas le determinant et transforme $C_0$ en $\begin{pmatrix} < a, a - \sum_{i=1}^n \lambda_i e_i > \\ < e_1, a - \sum_{i=1}^n \lambda_i e_i > \\ \vdots \\ < e_n, a - \sum_{i=1}^n \lambda_i e_i > \end{pmatrix}$, alors

$$|G(a, e_1, \ldots, e_n)| = \begin{vmatrix} < a, a - p(a) > & < a, e_1 > & \cdots & < a, e_n > \\ < e_1, a - p(a) > & < e_1, e_1 > & \cdots & < e_1, e_n > \\ \vdots & \vdots & \vdots & \vdots \\ < e_n, a - p(a) > & < e_n, e_1 > & \cdots & < e_n, e_n > \end{vmatrix}$$

On a $< e_i, a - p(a) >= 0 >$ car $a - p(a) \perp V$.

Alors,

$$|G(a, e_1, \ldots, e_n)| = \begin{vmatrix} < a, a - p(a) > & \cdots \\ 0 & \\ \vdots & G(e_1, \ldots, e_n) \\ 0 & \end{vmatrix}$$

Comme $< a, a - p(a) >= \|a - p(a)\|^2$, on a

$$|G(a, e_1, \ldots, e_n)| = \|a - p(a)\|^2 |G(e_1, \ldots, e_n)|$$

$\square$

*Remarque.* On a utilisé plusieur fois, le théorème de Pythagore :

Si $x \perp y$, alors

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2$$

Ici, dans le cas hermitien, l'égalité de Pythagore n'implique pas l'orthogonalité.

## 10.5 Compléments et applications

**Réduction simultanée de 2 formes quadratiques hermitiens dont l'une est définie positive :**

**Théorème 10.47.** *Soit $A \in M_n(\mathbb{C})$, hermitienne définie positive, $B$ hermitienne, alors $\exists P \in GL_n(\mathbb{C})$ et $D$ diagonale, telles que $A = P^*P$, $B = P^*DP$.*

Interprétation : $P \in GL_n(\mathbb{C})$, matrice de changement de base, dans la nouvelle base, la forme hermitienne définie par $A$ a pour matrice Id, i.e. la nouvelle base est orthonormée pour cette forme hermitienne et cette base est orthogonale pour la forme hermitienne définie par $B$.

**Théorème 10.48.** *Soit $A$ matrice hermitienne $A > 0$, $C$ hermitienne, alors $AC$ est diagonalisable.*

*Démonstration.* Si $A$ est définie positive, elle définit un produit scalaire hermitien :

$$X, Y \in \mathbb{C}^n,\ < X, Y >=^t \overline{X} AY$$

$B$ est hermitienne, définit une forme sesquilinéaire hermitienne sur $\mathbb{C}^n$,

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

On travaille dans le structure hermitienne $<, >$, on sait alors que toute forme hermitienne est représentée par un endomorphisme autoadjoint alias hermitien pour cette structure, $\exists u \in \mathcal{L}(\mathbb{C}^n)$, tel que

$$\varphi(X, Y) =< u(X), Y >=< X, u(Y) >$$

Pour le théorème 1 :

On applique le théorème de réduction, il existe une base orthonormale pour $<, >$, dans laquelle $u$ est une matrice diagonale.

Soit $C$ la matrice de $u$ dans la base standard de $\mathbb{C}^n$, on a

$$\begin{aligned}\varphi(X, Y) &=^t \overline{X} BY \\ &=^t \overline{CX} AY \\ &=^t \overline{X}^t \overline{C} AY\end{aligned}$$

Alors, on a

$$B = C^* A = AC$$

et $A^{-1}B = C$, matrice de $u$ et on sait que $u$ diagonalisable en base orthonorée pour $<,>$.

C'est ce qui donne la matrice $p$.

Pour le théorème 2 :

$A > 0$, $C$ hermitienne, considérons $A^{-1}$ hermitienne définie positive, donc, d'après ci-dessus (en changeant les rôles de $B$ et de $C$), et en remplaçant $A$ par $A^{-1}$, on a $AC$ est diagonalisable. (Dans une base orthonormée pour la structure hermitienne définie par $A^{-1}$.) □

**Remarque sur les valeurs propres des endomorphismes hermitienns :**

Soit $u \in \mathcal{L}(E)$ hermitien, il est diagonalisable en base orthonormée à valeurs propres réelles, soient $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ ses valeurs propres, il y a une base orthonormée, telle que

$$\forall i,\ u(e_i) = \lambda_i e_i$$

**Proposition 10.49.** *On a*

$$\lambda_1 = \min_{\|x\|=1} < u(x), x >$$
$$\lambda_n = \max_{\|x\|=1} < u(x), x >$$

*Démonstration.* Soit $x \in E$, $x = \sum_{i=1}^n x_i e_i$, alors

$$< u(x), x >= \sum_{i=1}^n \lambda_i |x_i|^2$$

alors, comme $\lambda_1 \leq \lambda_i \lambda_n$, on a

$$\lambda_1 \sum_{i=1}^n |x_i|^2 \leq < u(x), x > \leq \lambda_n \sum_{i=1}^n |x_i|^2$$

d'où les égalités si $\|x\| = 1$ □

Pour aller plus loin :

Considérons, pour $1 \leq i \leq n$,

$$F_i = \text{Vect}(e_1, \dots, e_i)$$
$$G_i = \text{Vect}(e_i, \dots, e_n)$$

Alors, on sait que

$$\forall x \in F_i,\ \|x\| = 1,\ < u(x), x > \leq \lambda_i$$
$$\forall x \in G_i,\ \|x\| = 1,\ < u(x), x > \geq \lambda_i$$

Soit $F$ un sous espace vectoriel de dimension $i$, comme $\dim G_i = n - i + 1$, on sait que $G_i \cap F \neq \{0\}$ :

$$\exists x,\ \|x\| = 1,\ x \in G_i \cap F,\ < u(x), x > \geq \lambda_i$$

Alors $\sup_{\|x\|=1, x \in F} < u(x), x > \geq \lambda_i$.

De plus, pour $F_i$, il y a égalité, ainsi, on a le thérorème min-max :

$$\lambda_i = \min_{\dim F = i} \max_{x \in F, \|x\|=1} < u(x), x >$$

# 11 Algèbre tensoriel

## 11.1 produit tensoriel

**Cadre :** $k$ corps,on considère des $k$ espaces vectoriels E.

**Notation :** On a déjà vu des formes bilinéaires $\varphi : E \times E \to k$. Souvent, on peut écrire

$$\varphi(x,y) = \sum_{l_i, l'_i \in E^*} l_i(x) l'_i(y)$$

On voit apparaître un objet $\sum l_i \bigotimes l'_i$.

On recherche une structure permettant étant donnés deux espaces vectoriels E,F de représenter les applications bilinéaire de $E \times F$ vers un autre espaces vectoriel G pour des application bilinéaire d'un nouvel espace vectoriel construit à partir de E et F, à valeurs dans G.

**Notation :** E,F,G espaces vectoriels.

$$Bil(E \times F, G) = \{application\ bilinaire\ de E \times F \to G\}$$

On voudrait un espace vectoriel T t.q. $Bil(E \times F, G) = \mathscr{L}(T, G)$, ceci pour tout G.

De plus, il y aura une application bilinéaire $E \times F \to T$ et toutes les autres seront constructes à partir de celle-ci.

**Théorème 11.1.** *Soient E,F espaces vectoriels. Il existe un couple (T,t) avec T espace vectoriel, $t : E \times F \to T$ bilinéaire tel que :*

*pour tout espace vectoriel G et toute application bilinéiare $b : E \times F \to G$, il existe une unique application bilinéaire $b' : T \to G$ telle que $b = b' \circ t$*

$$\begin{tikzcd} E \times F \arrow[r, "b"] \arrow[d, "t"] & G \\ T \arrow[ur, dashed, "b'"'] & \end{tikzcd}$$

**Proposition 11.2.** *Si un tel (T,t)existe, il est unique à isomorphisme unique près, c-à d :*

*si (T',t') est un autre couple satisfaisant la propriété, alors il y a un unique isomorphisme $\phi : T \to T'$ t.q. :*

$$\begin{tikzcd} & E \times F \arrow[dl, "t"'] \arrow[dr, "t'"] & \\ T \arrow[rr, "\phi"] & & T' \end{tikzcd}$$

*Démonstration.* On part de (T,t) et on applique sa propriété pour les applications bilinéaire à $t' : E \times T \to T'$. On en déduit une application linéaire unique $\phi : T \to T'$ t.q. $t' = \phi \circ t$.

Il faut voir $\phi$ isomorphisme.Pour cela, on applique la propriété universelle à (T',t'),

$$\exists! \phi' : T' \to T \ t.q. \ t = \phi' \circ t'$$

Alors $t = (\phi' \circ \phi) \circ t$

$\phi' \circ \phi : T \to T$ linéaire qui résoud le problème de propriété universelle entre $t : E \times F \to T$ et $t : E \times F \to T$

Comme Id convient trivialement, pour le propriété d'unicité dans associée,

$$\phi' \circ \phi = Id_T$$

De même

$$\phi \circ \phi' = Id_{T'}$$

□

**Existence :** on considère l'espace vectoriel $\boldsymbol{k}^{(E\times F)}$ (on voit $E \times F$ comme un ensemble) : c'est un espace vectoriel de base indèxée par les éléments de $E \times F$

$$(E_{v,w})_{v \in E, w \in F}$$

C'est l'espace vectoriel des application de $E \times F \to \boldsymbol{k}$ , à support fini.

On dispose d'une application $f : E \times F \to \boldsymbol{k}$ ,$(v, w) \mapsto e_{v,w}$

Elle n'est pas bilinéaire. On quotiente $\boldsymbol{k}^{E\times F}$ pour un sous-espace pour les rendre bilinéaire.

Soit S le sous espae de $\boldsymbol{k}^{(E\times F)}$ engendré par :

$$e_{\lambda v + \mu v', w} - (\lambda e_{v,w} + \mu e_{v',w})$$

$$e_{v, \lambda w + \mu w'} - (\lambda e_{v,w} + \mu e_{v,w'})$$

On considère $T = \boldsymbol{k}^{E\times F}/S$

On dispose de

$$t : E \times F \to \boldsymbol{k}^{E\times F} \to T$$

la conposée est bilinéaire.

Notons $v \otimes w$ la classe de $e_{v,w}$ dans le quotient T.

$$t(v,w) = v \otimes w$$

T est engendré par les $v \otimes w$.

Montreons que (T,t) satisfait à la propriété universelle : Soit G es[ace vectoriel, $b : E\times F \to G$ bilinéaire, alors : $\exists! b' : T \to G$ t.q. $b = b' \circ t$.

À partir de b, on fabrique une application bilinéaire $\varphi \boldsymbol{k}^{E\times F} \to G$ , $\varphi(e_{v,w}) = b(v,w)$.

Comme b est biliéaire ,$\varphi$ s'annule sur S, et donc ppasse au quotient T en une application $b' : T \to G$ qui satisfait $b = b' \circ t$. L'unicité de b' est donc au fait que T est engendré par les $v \otimes w$, et $b'(v \otimes w) = b(v,w)$ imposée.

**Notation** : $E \otimes F = T$

**Attention** : Tout élément de $E \otimes F$ n'est pas nécessairement de la forme $v \otimes w$. Un élément de $E \otimes F$ est une somme finie d'éléments $v \otimes w$. Ces éléments sont appelé s tenseurs décomposables, ou tenseurs simples ouu tenseurs purs.

**Rem :**

$$(\lambda v + \mu v') \otimes w = \lambda v \otimes w + \mu v' \otimes w$$

et vice versa.

**Conclusion :** $Bil(E \times F, G) = \mathscr{L}(E \times F, G)$

En particulier, les formes bilinéaires sur $E \times F$ forment l'espace vectoriel dual $(E \times F)^*$.

**Proposition 11.3.** $E_1,\ E_2,\ F_1,\ F_2$ *espaces vectoriels,* $f : E_1 \to E_2$, $g : F_1 \to F_2$ *linéaires.*

*Alors il existe une unique application linéaire* $E_1 \otimes F_1 \to E_2 \otimes F_2$ *qui envoie* $v \otimes w \mapsto f(v) \otimes g(w)$. *On la note* $f \otimes g$. *Ainsi :*

$$\begin{aligned} f \otimes g : E_1 \otimes F_2 &\to E_2 \otimes F_2 \\ v \otimes w &\mapsto f(v) \otimes g(w) \end{aligned} \tag{11.1}$$

*De plus si* $E_1 \xrightarrow{f} E_2 \xrightarrow{f'} E_3, F_1 \xrightarrow{g} F_2 \xrightarrow{g'} F_3$

*Alors* $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$

$$\begin{array}{ccc} E_1 \times F_1 & \xrightarrow{f\times g} & E_2 \times F_2 \\ \downarrow{\scriptstyle t_1} & & \downarrow{\scriptstyle t_2} \\ E_1 \otimes F_1 & \xrightarrow{f\otimes g} & E_2 \otimes F_2 \end{array}$$

*Démonstration.* On fabrique une application $f \times g : E_1 \times F_2 \to E_2 \times F_2$, $(v, w) \mapsto (f(v), g(w))$.

L'application $t_0' : (f \times g) : E_1 \times F_2 \to E_2 \otimes F_2$ est bilinéaire. Par la propriété de $E_1 \otimes F_1$, il y a une unique application $f \otimes g$ t.q.

$$\begin{aligned} (f \otimes g)(v \otimes w) &= t_2 \circ (f \times g)(v, w) \\ &= t_2(f(v), g(w)) \\ &= f(v) \otimes g(w) \end{aligned} \tag{11.2}$$

Propriété par la composée unicité appliquée à $(f' \circ f) \otimes (g' \circ g) : E_2 \otimes F_2 \to E_3 \otimes F_3$, $v \otimes w \mapsto (f' \circ f)(v) \otimes g' \circ g(w)$.

Mais

$$\begin{aligned} (f' \circ f)(v) \otimes g' \circ g(w) &= f'(f(v)) \otimes g'(g(w)) \\ &= (f' \otimes g')(f(v) \otimes g(w) \\ &= (f' \otimes g')((f \otimes g)(v \otimes w)) \\ &= (f' \otimes g') \circ (f \otimes g)(v \otimes w) \end{aligned} \tag{11.3}$$

□

**Propriété de $\otimes$ :** Soit $\boldsymbol{k}$ corps

(1).

$$\begin{aligned} \boldsymbol{k} \otimes E \simeq &\quad E \\ \lambda \otimes v \mapsto &\quad \lambda v \end{aligned} \tag{11.4}$$

(2)E, $E_i,\ i \in I$ espaces vectoriels.

$$\begin{aligned} (\bigoplus_{i\in I} E_i) \otimes E \simeq &\quad \bigoplus_{i\in I} E_i \otimes E \\ (\sum v_i) \otimes w \mapsto &\quad \sum v_i \otimes w \end{aligned} \tag{11.5}$$

(3) E, F espaces vectoriels

$$\begin{aligned} E \otimes F &\simeq F \otimes E \\ v \otimes w &\mapsto w \otimes v \end{aligned} \tag{11.6}$$

(4) E, F ,G espaces vectoriels

$$\begin{aligned} (E \otimes F) \otimes G &\simeq E \otimes (F \otimes G) \\ v \otimes w &\mapsto w \otimes v \end{aligned} \tag{11.7}$$

*Démonstration.* :

(1)

$$\boldsymbol{k} \times E \to E$$

$$(\lambda, v) \mapsto \lambda v$$

est bilinéaire d'où

$$\boldsymbol{k} \otimes E \to E$$

$$\lambda \otimes v \mapsto \lambda v$$

linéaire bijective, de réciproque

$$E \to \boldsymbol{k} \otimes E$$

$$v \mapsto 1 \otimes v$$

(2)On construit une application bilinéaire

$$(\bigoplus_{i \in I} E_i) \times E \to \bigoplus_{i \in I} E_i \otimes E$$

$$((\sum v_i), w) \mapsto \sum v_i \otimes w$$

d'où une application linéaire

$$(\bigoplus_{i \in I} E_i) \otimes E \to \bigoplus_{i \in I} E_i \otimes E$$

Inversement :

On dispose des injections

$$\varphi_i : E_i \to \bigoplus E_i$$

d'où une application linéaire

$$\varphi_i \otimes Id : E_i \otimes E \to (\sum E_i) \otimes E$$

et par propriété des $\sum$, ou oblient une application linéaire

$$\sum(\varphi_i \otimes Id) : \sum(E_i \otimes E) \to (\sum E_i) \otimes E$$

ces deux application linéaire sont inverses l'une de l'autre.

(3) L'application

$$E \times F \to F \otimes E$$

$$(v, w) \mapsto w \otimes v$$

est bilinéaire.d'où une unique application linéaire

$$E \otimes F \to F \otimes E$$

$$v \otimes w \mapsto w \otimes v$$

La réciproque se construit de la même façon

(4)Exercice. □

**Bases :** Soit $(e_i)_{i\in I}$ base de E. $E \simeq \bigoplus_{j\in I} \boldsymbol{k} e_j$.

Ainsi $E \otimes F \simeq \bigoplus_{i\in I}(\boldsymbol{k} e_i \otimes F)$

Tout élément de $E \otimes F$ s'écrit de moins de unique : $\sum_{t\in I} e_i \otimes w_i$, avec $w_i \in F$ et les $w_i$ presque tous nuls.

Soit $(f_j)_{j\in J}$ base de F. $E \otimes F \simeq \bigoplus_{j\in J} E \otimes \boldsymbol{k} f_j$.

On obtient un isomorphisme d'espaces vetoriels.

$$E \otimes F \simeq \bigoplus_{i\in I, j\in J} \boldsymbol{k}(e_i \otimes f_j)$$

Ainsi $(e_i \otimes f_j)_{(i,j)\in I\times J}$forment une base de $E \otimes F$.

**Proposition 11.4.** *Si $dimE,\ dimF < \infty$, alors $dim(E \otimes F) = dimE \cdot dimF$.*

*Démonstration.* Matrices d'applications linéaires

Si $E_1$, $E_2$, $F_1$, $F_2$ espaces vectoriels, $(e_{1,i})_{i\in I_1}$, $(e_{2,i})_{i\in I_2}$, $(e_{1,j})_{j\in J_1}$, $(e_{2,j})_{j\in J_1}$, des bases respectives.

$\varphi : E_1 \to E_2$ de matrice $(a_{ik})$, et $\psi : F_1 \to F_2$ de matrice $(b_{jl})$.

$$(\varphi \otimes \psi)(e_{2,i} \otimes f_{1,l} = \sum a_{ik} b_{jl} e_{2,i} \otimes f_{2,j}$$

Prenons $E_1 = E_2 = E$ de base $(e_1, ...e_n)$, $F_1 = F_2 = F$ de base $(f_1, ..., f_p)$, allors les $(e_i \otimes f_j)$ base de $E \otimes F$. □

Plusieurs possibilités pour écrire des matrices selon l'ordre total mix sur$\{1, ..., n\} \times \{1, ..., p\}$

(1) Ordre lexicographique : $(i, j) < (i', j')$ si $i < i'$ ou $i = i'\ etj < j'$. On considère le base

$$(e_1 \otimes f_1, e_1 \otimes f_2, ..., e_1 \otimes f_p, e_2 \otimes f_1, ..., e_2 \otimes f_p, ..., e_n \otimes f_1, ..., e_n \otimes f_p)$$

La matrice de $\varphi \otimes \psi$ dans cette base s'écrit en fonction des matrices $A = (a_{ij})\ de\ \varphi, B = (b_{kl})\ de\ \psi$.

Ainsi : $\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \ddots & & \vdots \\ a_{n1}B & \cdots & & a_{nn}B \end{pmatrix}$

(2) Ordre lexicographique inverse : $(i, j) < (i', j')$ si $i' < j'$ ou $i' = j'\ et\ i < j$.

Alors la matrice :

$\begin{pmatrix} Ab_{11} & Ab_{12} & \cdots & Ab_{1n} \\ \vdots & \ddots & & \vdots \\ Ab_{n1} & \cdots & & Ab_{nn} \end{pmatrix}$

**Propriétés :**

(1) $Tr(\varphi \otimes \psi) = Tr(\varphi)tr(\psi)$

(2) $det(\varphi \otimes \psi) = det(\varphi)^{dimF} \cdot det(\psi)^{dimE}$

*Démonstration.* (1) On regarde la matrice dans la première base.

$$a_{11}Tr(B) + a_{22}Tr(B) + \cdots + a_{nn}Tr(B) = Tr(A)Tr(B)$$

(2) On a :$\varphi \otimes \psi = (\varphi \otimes Id_F)(Id_E \otimes \psi)$ dans la première base, on calcule $det(Id_F \otimes \psi) = (det\psi)^{dimE}$.

Dans la deuxième base, on voit : $det(\varphi \otimes Id_F) = (det\varphi)^{dimF}$

$\square$

*Remarque* 11.5. A,B matrices

$A \otimes B : (a_{ij}B)$ (lexicographie)

(antilexicographique $(b_{kl}A)$)

Permutation entre bases de $\boldsymbol{k}^n \otimes \boldsymbol{k}^m$

$$(e_1 \otimes f_1, e_1 \otimes f_2, ..., e_1 \otimes f_m, e_2 \otimes f_1, ..., e_2 \otimes f_m, ..., e_n \otimes f_1, ..., e_n \otimes f_m)$$

$$(e_1 \otimes f_1, e_2 \otimes f_1, ..., e_n \otimes f_1, e_1 \otimes f_2, ..., e_n \otimes f_2, ..., e_1 \otimes f_m, ..., e_n \otimes f_m)$$

Pour permuter , si n=m,

$$p = \sum_{1 \leq i,j \ \leq n} E_{ij} \otimes E_{ji}$$

$$p(v \otimes w) = w \otimes v$$

**Proposition 11.6.** *E,F espaces vectoriels.*

*Alors*

$$\varphi : E^* \otimes F \to Hom(E, F)$$

$$l \otimes v \mapsto [x \mapsto l(x)v]$$

*est bien définie, injective d'image l'espace des applications linéaire de rang fini.*

*En particulier, si E ou F est de dim finie,*

$$E^* \otimes F \simeq Hom(E, F)$$

*Démonstration.*

$$E^* \times F \to Hom(E, F)$$

$$l \otimes v \mapsto [x \mapsto l(x)v]$$

est bilinéaire , d'où l'existence de $\varphi$ linéaire , $\varphi$ injective.

Soit $\xi \in E^* \otimes F$, $\varphi(\xi) = 0$.

Soit $(f_i)$ base de F, alors $\xi$ s'écit

$$\xi = \sum_{finie} l_i \otimes f_i, \ l_i \in E^*$$

$$\varphi(\xi) = 0 \iff \forall x \in F,\ \sum l_i(x) f_i = 0$$

$(f_i)$ base $\rightarrow \forall i,\ l_i(x) = 0$ d'où $l_i = 0$ *et* $\xi = 0$.

En suite, si E de dim finie ou E de dim finie, cette application linéaire est de rang finie

*Remarque* 11.7. Si $u : E \rightarrow F$ est de rang fini, on prend une base de son image, sont $f_1, \cdots, f_p$ et alors :

$$\forall x \in E, u(x) \in Vect(f_1, \cdots, f_p)$$

$$u(x) = \sum \alpha_i(x) f_i, \alpha_i \in E^*$$

*Remarque* 11.8. Pour $E = F,\ dim < \infty,\ E^* \otimes E \simeq Hom(E, E)$.

Si $(E_i)$ base de E, $(E_i^*)$ base duale.

$$e_j^* \otimes e_i \longleftrightarrow E_{ij}$$

$E = F$ de dim finie, $\forall u \in (L)(E) = Hom(E, E)$, $u = \sum e_i^* \otimes u(e_i)$

$$Id = \sum e_i^* \otimes e_i$$

*Remarque* 11.9. On dispose sur $E^* \otimes E$ d'une forme linéaire :

$$l \otimes x \mapsto l(x)$$

$$E^* \otimes E \xrightarrow{ev} \boldsymbol{k}$$

Elle s'interprète sur $\mathscr{L}(E)$, comme la trace.

En effet : $u \in \mathscr{L}(E)$, on fixe une base $(e_i)$, $u = \sum e_i^* \otimes u(e_i)$, $ev(u) = \sum e_i^*(u(e_i))$.

Si $u(e_i) = \sum a_{ji} e_j$, $ev(u) = \sum_i a_{ii} = Tr(u)$

□

**Exemple :**

$$\boldsymbol{k}[X] \otimes \boldsymbol{k}[Y] \simeq \boldsymbol{k}[X, Y]$$

$$X^i \otimes Y^j \mapsto X^i Y^j$$

**Produit tensoriel d'applications linéaires**

$$u \in Hom(E_1, E_2),\ v \in Hom(F_1, F_2),\ u \otimes v \in Hom(E_1 \otimes F_1, E_2 \otimes F_2)$$

**Proposition 11.10.**

$$Keru \otimes F_1 + E_1 \otimes Kerv$$

$$Im(u \otimes v) = Im(u) \otimes Im(v)$$

*Démonstration.* Prenons des supplémentaires $E_1'$ de $Keru$ et $E_2'$ de $Kerv$.

$$E_1 \otimes E_2 = E_1' \otimes E_2' \bigoplus (Keru \otimes E_2 + E_1 \otimes Kerv)$$

Alors $u \otimes v$ s'annule sur la deuxième facteur et enduit un isomorphisme de $E_1' \otimes E_2'$ sur $Imu \otimes Imv$ (prendre des bases) □

**Quotients :**

E,F espaces vectoriels, $E' \subset E,\ F' \subset F$ des sous espace vectoriel. On considère $E/E'$ et $F/F'$

**Proposition 11.11.**

$$E/E' \otimes F/F' \simeq E \otimes F/(E' \otimes F + E \otimes F')$$

*Démonstration.* On dispose des applications $\pi_E : E \to E/E'$ et $\pi_F : F \to F/F'$ surjectives d'où une application linéaire surjective

$$\pi_E \otimes \pi_F : E \otimes F \to E/E' \otimes F/F'$$

Son noyau est

$$Ker\pi_E \otimes F + E \otimes Ker\pi_F = E' \otimes F + E \otimes F'$$

□

## 11.2 Algèbre tensorielle

**Notions d'algèbre** sur le est un $\boldsymbol{k}-$espace vectoriel A, $(A,+,\cdot)$, qui est aussi un anneau $(A,+,\times)$ tel que

$$A \times A \to A$$

$$(a,b) \mapsto a \times b$$

est bilinéaire

*Remarque* 11.12. Le produit dans A détermine une application linéaire

$$A \otimes A \to A,\ a \otimes b \mapsto a \times b$$

Souvent, on note ab le produit .

**Exemples :**

(1)algèbres de polynômes

(2) algèbres de matrices

**Produit tensoriel d'algèbres** Toutes les algèbres considérées seront unitère (on dit aussi unitaire) i.e. passèdent une unité, notée 1, pour le produit, $\forall a \in A, 1 \cdot a = a \cdot 1 = a$.

Les morphismes d'algèbres i.e. $\varphi : A \to B$ linéaires , $\varphi : A \to B$ linéaires, $\varphi(ab) = \varphi(a)\varphi(b)$, $\forall a, b \in A$, et $\varphi(1_A) = 1_B$

**Proposition 11.13.** *Soient A,B alèbres. Alors il eiste sur $A \otimes B$ une unique atructure d'algèbre telle que, $\forall a, a' \in A,\ \forall b, b' \in B,\ a \otimes b\ a' \otimes b' = aa' \otimes bb'$*

*Démonstration.* unicité claire car $A \otimes B$ engendréré comme esp. vect. par les $a \otimes b$

**Existence :**

*Remarque* 11.14. la structure d'algèbre de A est connue, si on connait, $\forall a \in A$, l'application linéaire

$$L_a : A' \to A$$

$$b \mapsto ab$$

On a $L_a \circ L_{a'} = L_{aa'}$. (Traduit l'assocaitivité)

Fixons$(a, b) \in A \times B$

$$A \times B \to A \otimes B$$

$$(a', b') \mapsto aa' \otimes bb'$$

est bilinéaire,d'où une application linéaire

$$\mathscr{L}_{(a,b)} : A \otimes B \to A \otimes B$$

$$a' \otimes b' \mapsto aa' \otimes bb'$$

On a aussi une application

$$\mathscr{L} : A \times B \to \mathscr{L}(A \otimes B)$$

$$(a, b) \mapsto \mathscr{L}_{(a,b)}$$

$\mathscr{L}$ est bilinéaire, d'où une application linéaire

$$L : A \otimes B \to \mathscr{L}(A \otimes B)$$

$$a \otimes b \mapsto [a' \otimes b' \mapsto aa' \otimes bb']$$

Ainsi $\forall x = \sum a_i \otimes b_i$ dans $A \otimes B$, on dispose de $L_x : A \otimes B \to A \otimes B$ d'où une application $A \otimes B \times A \otimes B \to A \otimes B$ bilinéaire t.q. $(a \otimes b, a' \otimes b') \mapsto aa' \otimes bb'$

On vérifie que c'est assocaitif (car de A et B ça l'est) et $1_A \otimes 1_B$ unité. □

*Remarque* 11.15. On dispose de morphismes injectifs

$$i_A : A \to A \otimes B$$

$$a \mapsto a \otimes 1_B$$

et

$$i_B : B \to A \otimes B$$

$$b \mapsto 1_A \otimes b$$

avec $\forall a \in A, b \in B$, $i_A(a)i_B(b) = i_B(b)i_A(a) = a \otimes b$

i.e. A et B se voient comme des sous-algèbres de A et B, et $i_A(A)$, $i_B(B)$ commutent.

Si $\varphi : A \otimes B \to C$ morphisme d'algèbres, alors $\varphi$ détermine des morphismes $\varphi_A : A \to C$, $\varphi_A(a) = \varphi(a \otimes 1)$ et $\varphi_B : B \to C$, $\varphi_B(b) = \varphi(1 \otimes b)$, et $\forall a \in A$, $\forall b \in B$, $\varphi_A(a)\ \varphi_B(b) = \varphi_B(b)\ \varphi_A(a)$

**Inversement** :

**Propriété universelle de $A \otimes B$ :** Soient A,B,C algèbres, $\varphi_A : A \to C,\ \varphi_B : B \to C$ morphismes d'algèbres dont les images commutent :

$$\forall a \in A,\ \forall b \in B,\ \varphi_A(a)\ \varphi_B(b) = \varphi_B(b)\ \varphi_A(a)$$

Alors il existe un unique morphisme d'algèbre $\varphi : A \otimes B \to C$ t.q. $\varphi(a \otimes b) = \varphi_A(a)\varphi_B(b)$

*Démonstration.* <u>Unicité :</u> claire car les $a \otimes b$ engendrent $A \otimes B$ comme espace vectoriel.

<u>Existence :</u> nécessairement

$$\varphi(a \otimes 1) = \varphi_A(a),\ \varphi(1 \otimes b) = \varphi_B(b)$$

$$A \times B \to C$$

$$(a, b) \mapsto \varphi_A(a)\varphi_B(b)$$

bilinéiare, d'où une unique applicaiton linéaire $\varphi : A \otimes B \to C$ t.q. $\varphi(a \otimes b) = \varphi_A(a)\varphi_B(b)$

On a $\varphi(1_A \otimes 1_B) = 1_c \cdot 1_C = 1_C$

Vérifions la multiplicalivité de $\varphi$ . Par linéarité de $\varphi$ et bilinéarité du produit dans $A \otimes B$, il suffit de voir $\varphi(a \otimes b, a' \otimes b') = \varphi(a \otimes b)\varphi(a' \otimes b')$

$$\begin{aligned}
\varphi(a \otimes b, a' \otimes b') &= \varphi(aa' \otimes bb') \\
&= \varphi_A(aa')\varphi_B(bb') \\
&= \varphi_A(a)\varphi_A(a')\varphi_B(b)\varphi_B(b') \\
&= \varphi_A(a)\varphi_B(b)\varphi_A(a')\varphi_B(b') \\
&= \varphi(a \otimes b)\varphi(a' \otimes b')
\end{aligned} \tag{11.8}$$

□

**Exemple :** E,F espaces vectoriels de dimension finie. On a vu que ai $u \in \mathscr{L}(E),\ v \in \mathscr{L}(F)$, on dispose de $u \otimes v \in \mathscr{L}(E \otimes F)$. On a donc une application bilinéaire,

$$\mathscr{L}(E) \times \mathscr{L}(F) \to \mathscr{L}(E \otimes F)$$

$$(u, v) \mapsto u \otimes v$$

d'où une unique application linéaire $\mathscr{L}(E) \otimes \mathscr{L}(F) \to \mathscr{L}(E \otimes F)$ et on a vu que c'est en fait un morphisme d'algèbres.

**Proposition 11.16.** *C'est un isomorphisme d'algèbres*

*Démonstration.* On vérifie l'injectivité et on a aussi égalité des dimensions (détails en exercice) □

**Extension des scalaires $\boldsymbol{k}$,** $K$ corps, $\boldsymbol{k} \subset K$ (tipiquement $\mathbb{R} \subset \mathbb{C}$), donc telle inclusion de corps de K un $\boldsymbol{k}$ espace vectoriel.

Soit E un $\boldsymbol{k}$ espaces vectoriel. Soit $E^K = K \otimes E$, c'est un $\boldsymbol{k}$ espace vectoriel. On le munit d'une structure de K-espace vectoriel aussi :

· même structure de groupe abélien

· si $\alpha \in K$, on dispose de $m_\alpha : K \to K$ $(x \mapsto \alpha x)$ linéaire et on fait agir $\alpha$ sur $E^K$ par $m_\alpha \otimes id_E$

$$\alpha \cdot (\sum x_i \otimes e_i) = \sum \alpha x_i \otimes e_i$$

**Propriétés :** (1) Si $(e_i)$ base de E sur $\boldsymbol{k}$, alors $(1_K \otimes e_i)_{i \in I}$ base de $E^K$ sur K.

(2) Si $u \in \mathscr{L}(E)$, alors elle détermine une application K-linéaire sur $E^K$ via : $id_K \otimes u = u^K$

i.e. $u^K(\alpha \otimes e) = \alpha \otimes u^K(e)$

De plus si $(e_i)$ base de E, la matrice de $u^K$ dans la base $(1 \otimes e_i)_{i \in I}$ est la matrice de u dans la base $(e_i)$

*Remarque* 11.17. (1) dit que $dim_K(E^K) = dim_{\boldsymbol{k}}(E)$

**Quelques généralités sur les algèbres**

On s'intéresse à des algèbres sur un $\boldsymbol{k}$ corps, unitères, par nécessairement commutatures.

**Définition 11.18.** Soit A une algèbre. Un idéal bilatère I de A est un sous espace vectoriel t.q.

$$\forall x \in I, \forall a \in A, ax \in I,\ xa \in I$$

**exemple :**$\{0\}, A$

Exemple type : Si A,B sont 2 algèbres , $\varphi : A \to B$ morphisme d'algèbres, alors $Ker\varphi$ est un idéal bilatère.

**Structure quotient.** Soit A une algébre, $I \subset A$ idéal bilatère. Alors il y a sur l'espace vectoriel quotient une unique structure d'algèbre telle que :

$$\pi : A \to A/I,\ a \mapsto \bar{a} = a + I$$

est un morphisme d'algèbre, i.e. $\bar{a} \cdot \bar{b} = \bar{ab}$

**Vérification :** analogue au ces commutatif :

$$(a+I)(b+I) = ab + aI + Ib + I \cdot I \equiv ab\ modI$$

**Construction d'idéaux**

**Proposition 11.19.** *Une intersection d'idéaux bilatères est un idéal bilatère.*

**Définition 11.20.** Soit A algèbre, $X \subset A$ une partie de A. L'idéal engendré par X est le plus petit idéal de A contenant, qui est l'intersection de tous les idéaux de A contenant X.

**Exercice 11.21.** Prenons $A = M_n(\boldsymbol{k})$ algèbre des matrices. Ses seuls idéaux bilatères sont $\{\ 0\ \}$ et A, on dit que c'est une algèbre simple

### 11.2.1 Algèbre graduée

**Définition 11.22.** Une algèbre graduée est une alg'ebre A munie d'une suitede sous-espaces vectoriels $A_n,\ n \in \mathbb{N}$t.q. :

$(1) A = \sum_{n\in\mathbb{N}} A_n$ comme espace vectoriel.

$(2) A_n \cdot A_m \subset A_{n+m}$ i.e. $(\forall n \in A_n,\ y \in A_m) \Rightarrow xy \in A_{n+m}$

**Terminologie :** Les $A_n$ sont appelées composantes homogènes. Un élément $x \in A$ est dit homogène si $\exists n \in \mathbb{N}, x \in A_n$. Ce n est appelé son degré, et noté $\partial(x)$ , ou $deg(x)$, ou $d(x)$.

**Exemple :** (1) $\boldsymbol{k}[X] = A$, $A_n = \boldsymbol{k} \cdot X^n$

(2) $\boldsymbol{k}[X_1, \cdots, X_p]$ degré total d'un monôme $\partial(X_1^{a_1} \cdots X_n^{a_n}) = a_1 + \cdots + a_n$

**Idéal gradué d'une algèbre graduée**

$A = \bigoplus A_n$, I idéal bilatère

**Définition 11.23.** On dit que I est gradué si $I = \bigoplus_{n=0}^{\infty}(I \cap A_n)$,

i.e. si $x \in I,\ x = \sum x_n,\ x_n \in A_n$, alors $\forall n, x_n \in I$.

Soit I un idéal, $I_n = I \cap A_n$. On dispose des espaces vectoriels quotients $A_n/I_n$ et on forme :

$$\bigoplus_{n\in\mathbb{N}} A_n/I_n = \bar{A}$$

On dispose d'une structure d'algèbre graduée sur $\bar{A}$.

Si $\alpha_n = \bar{a_n} \in A_n/I_n,\ \beta_m = \bar{b_m} \in A_m/I_m,\ a_n \in A_n,\ b_m \in A_m$, alors $\alpha_n \cdot \alpha_m = \overline{a_n b_m}$ est bien défini dans $A_{n+m}/I_{n+m}$.

On dispose d'un morphisme d'algèbres$\bigoplus A_n = A \to \bigoplus A_n/I_n$, le noyau est I, car I est gradué.

Conclusion : On a un isomorphisme d'algèbres $A/I \simeq \bigoplus A_n/I_n$. $\underline{A/I \text{ algèbre graduée}}$

**Produit tensoriel gradué d'algèbres** $A = \bigoplus A_n,\ B = \bigoplus B_n$ des algèbres graduée. Alors on peut munir $A \bigoplus B$ d'une structure d'algèbre graduée :

$$(A \otimes B)_n = \bigoplus_{p+q=n,\ p,q\in\mathbb{N}} (A_p \otimes B_q)$$

$A_p \subset A, B_q \subset B, A_p \otimes B_q \subset A \otimes B,$

$$\begin{aligned} A \otimes B &= (\bigoplus_n A_n) \otimes (\bigoplus_m B_m) \\ &= \bigoplus_{n,m} (A_n \otimes B_m) \\ &= \bigoplus_{n\in\mathbb{N}} (\bigoplus_{p+q=n} A_p \otimes B_q) \end{aligned} \tag{11.9}$$

*Remarque* 11.24. Le cas des polynômes en plusieurs variables, avec le degré total, est un cas particulier.

On a muni $A \otimes B$ d'une structure d'algèbre.

**Proposition 11.25.** *Si A et B sont graduée, alors, avec la graduation ci-dessus, $A \otimes B$ est aussi une algèbre graduée.*

*Démonstration.* Exercice. □

**Produit tensoriel tordu d'algèbres graduées**

*Remarque* 11.26. Quand on a défini le produit tensoriel d'algèbres A et B, on a imposé :

$$(a \otimes 1)(1 \otimes b) = a \otimes b$$

$$(1 \otimes b)(a \otimes 1) = a \otimes b$$

Dans le cas où A et B sont des algèbres graduées, on peut imposer une autre règle : si $a \in A_n,\ b \in B_m$

$\cdot(1 \otimes b)(a \otimes 1) = (-1)^{nm} a \otimes b$

$\cdot(1 \otimes b)(a \otimes 1) = a \otimes b$

**Proposition 11.27.** *Soient $A$ et $B$ des algèbres graduées. Alors il existe sur l'espace vectoriel $A \otimes B$ une unique structure d'algèbre graduée t.q. : si $a, a' \in A$, $b, b' \in B$ avec a'homogène, $b$ homogène*

$$(a \otimes a')(b \otimes b') = (-1)^{\partial a' \partial b}(ab \otimes a'b')$$

*Cette structure est notée $A \otimes^g B$, produit tensoriel tendu (ou gradué).*

*Démonstration.* Essentiellement la même que pour le cas non gradué. Prendre soin aux signes pour l'associativité, en utilisant si $\partial(xy) = \partial(x) + \partial(y)$. □

**Question :** à partir d'un espace vectoriel V construire une algèbre $T(V) \supset V$ t.q. (propriété universelle) pour toute algèbre A, touote application linéaire $F : V \to A$ , alors il existe un unique morphisme d'algèbre $T(f)$ t.q.

$$\begin{tikzcd} T(V) \arrow[r, "T(f)"] & A \\ V \arrow[u, hook] \arrow[ur, "f"'] & \end{tikzcd}$$

**Produit tensoriel d'algèbres graduées**

$A = \bigoplus_{n\in\mathbb{N}} A_n$, $B = \bigoplus_{m\in\mathbb{N}} B_m$, $(A \otimes B)_n = \bigoplus_{p+q=n} A_p \otimes B_q$.

**Deux structures d'algèbres** :

(1) produit tensoriel usuel

$a \in A,\ b \in B$

$$(a \otimes 1)(1 \otimes b) = (1 \otimes b)(a \otimes 1) = a \otimes b$$

Propriété universelle pour les morphismes $\varphi_A : A \to C$, $\varphi_B : B \to C$ t.q. $\forall a \in A,\ b \in B$, $\varphi_A(a)\varphi_B(b) = \varphi_B(b)\varphi_A(a)$

(2) produit tensoriel gradué : $a \in A_n,\ b \in B_m$

$\cdot(a \otimes 1)(1 \otimes b) = a \otimes b$

$\cdot(1 \otimes b)(a \otimes 1) = (-1)^{nm} a \otimes b$

Propriété universelle pour les morphismes $\varphi_A : A \to C$, $\varphi_B : B \to C$ t.q. $\forall a \in A_n,\ b \in B_m$, $\varphi_A(a)\varphi_B(b) = (-1)^{nm}\varphi_B(b)\varphi_A(a)$

Alors il existe un unique morphisme d'algèbre $\varphi : A \otimes^g B \to C$ t.q.$\varphi(a \otimes b) = \varphi_A(a)\varphi_B(b)$

*Démonstration.* L'existence de $\varphi$ comme application linéaire provient de la bilinéarité du produit. Il faut vérifier que $\varphi$ morphisme d'algèbres : il suffit de voir sur tenseurs décomposables

$$\begin{aligned}
\varphi(a \otimes b \cdot a' \otimes b') &= \varphi((-1)^{\partial b \cdot \partial a'} aa' \otimes bb') \\
&= (-1)^{\partial b \partial a'} \varphi_A(aa')\varphi_B(bb') \\
&= (-1)^{\partial b \partial a'} \varphi_A(a)\varphi_A(a')\varphi_B(b)\varphi_B(b') \\
&= (-1)^{\partial b \partial a'} \varphi_A(a)[(-1)^{\partial b \partial a'} \varphi_B(b)\varphi_A(a')]\varphi_B(b') \\
&= \varphi_A(a)\varphi_B(b)\varphi_A(a')\varphi_B(b') \\
&= \varphi(a \otimes b)\varphi(a' \otimes b')
\end{aligned} \tag{11.10}$$

□

**Définition 11.28.** Une algèbre graduée A est dite :

· anticommutative si :

$$\forall a, a' homognes : aa' = (-1)^{\partial a \partial a'} a'a$$

· alternée si : elle est anticommutative et de plus : $\forall a$ de degré impair $a^2 = 0$

*Remarque* 11.29. si 2 est inversible dans $\boldsymbol{k}$ alors alternée $\Leftrightarrow$ anticommutative

**Proposition 11.30.** *(1) Le produit tensoriel usuel de 2 algèbres commutatives est une algèbre commutatuve.*

*(2) Le produit tensoriel gradué de 2 algèbres anticommutatives est une algèbre anticommutative.*

*(3)Le produit tensoriel gradué d'algèbres alternées est une algèbre alternée.*

*Démonstration.* prendre en compte le fait que le degré d'un produit tensoriel est donne par le degré total.

Exercice : Vérifier ces propriétés. □

### 11.2.2 Algèbre tensorielle

$\boldsymbol{k}$ corps, V un $\boldsymbol{k}$-espcaces vectoriel.

*Remarque* 11.31. produit tensoriel itéré $V_1, V_2, \cdots, V_p$ esp. vect., on a vu $(V_1 \otimes V_2) \otimes V_3 = V_1 \otimes (V_2 \otimes V_3)$

On peut ainsi construire $V_1 \otimes V_2 \cdots \otimes V_p$ itérativement, et l'espace obtenu ne dépend par du parenthésage.

Il peut aussi être caractérisé via les applications multilinéaires sur $V_1 \times V_2 \times \cdots \times V_p$ à valeurs dans un e.v. quelconque :

Soit E esp. vect. Une applicaiton linéaire $\varphi : V_1 \times \cdots \times V_p \to E$ est une application qui est linéaire en chaque terme.

Pour toute telle application p-linéaire, il existe une unique application linéaire $\bar{\varphi} : V_1 \otimes \cdots \otimes V_p \to E$ t.q.

$$\begin{tikzcd}
V_1 \times \cdots \times V_p \arrow[rr] \arrow[dr, "\varphi"] & & V_1 \otimes \cdots \otimes V_p \\
& E \arrow[ur, "\bar{\varphi}"] &
\end{tikzcd}$$

(On pourait aussi construire $V_1 \otimes \cdots \otimes V_p$directement  par quotient comme pour p=2. La propriété universelle indique qu'on obtient un espace isomorphe )

**Définition 11.32.** $T(V) = \bigoplus_{n \in \mathbb{N}} V^{\otimes n}$

$\cdot n = 0,\ V^{\otimes 0} = \boldsymbol{k}$

$\cdot V^{\otimes(n+1)} = (V^{\otimes n}) \otimes V$

On munit T(V) d'une structure d'algèbre graduée :

$$V^{\otimes p} \times V^{\otimes q} \to V^{\otimes(p+q)}$$

$$(v_1 \otimes \cdots \otimes v_p, w_1 \otimes \cdots \otimes w_q) \mapsto v_1 \otimes \cdots \otimes v_p \otimes w_1 \otimes \cdots \otimes w_q$$

"juxtaposition sur les tenseurs simples"

· Les propriétés du produit tensoriel indiquent que c'est bien défini

$$\begin{tikzcd}
\underbrace{V \times \cdots \times V}_{p+q} \arrow[r] \arrow[d] & V^{\otimes(p+q)} \\
V^{\otimes p} \times V^{\otimes q} \arrow[ur] &
\end{tikzcd}$$

pour p=0 ou q=0 : on utilise l'action de le sur l'espace vectoriel considéré.

Cette application est associative comme on le voit sur les tenseurs décomposables.

Ceci munit T(V) d'une structure d'algèbre unitère, avec une injection linéaire $V \overset{i}{\hookrightarrow} T(V)$

<u>Notation</u>

$$T^p(V) = v^{\otimes p}$$

$$V \hookrightarrow T^p(V) \subset T(V)$$

Si $(e_i)_{i\in I}$ base de V, les $(e_{i_1} \otimes \cdots \otimes e_{i_p}),\ p \in \mathbb{N},\ i_1, \cdots, i_p \in I$ forment une base de T(V).

La définition du produit dit que c'est une algèbre graduée, qui est engendrée par $V = T^p(V)$

**Propriété universelle :** $T(V)$ possède la propriété universelle . Si A algèbre, $f : V \to A$ application linéaire, alors $\exists! \bar{f} : T(V) \to A$ morphisme d'algèbres t.q. : $f = \bar{f} \circ i$

$$\begin{tikzcd} V \arrow[r, hook, "i"] \arrow[d, "f"] & T(V) \arrow[dl, "\bar{f}"] \\ A & \end{tikzcd}$$

Ainsi pour toute alèbre A

$$\begin{aligned} \mathscr{L}(V, A) &\simeq Hom_{alg}(T(V), A) \\ f &\mapsto \bar{f} \\ \varphi|_V(= \varphi \circ i) &\longleftarrow \varphi \end{aligned} \tag{11.11}$$

*Démonstration.* prolongeons f à T(V) en la prolongeant à chaque $V^{\otimes p}$

$$V^p \longrightarrow A$$

$$(v_1, \cdots, v_p) \mapsto f(v_1)f(v_2)\cdots f(v_p)$$

est une application p-linéaire, donc elle se factorise à trouver $V^{\otimes p}$ en une application linéaire

$$\bar{f} : V^{\otimes p} \longrightarrow A$$

$$v_1 \otimes \cdots \otimes v_p \mapsto f(v_1)f(v_2)\cdots f(v_p)$$

Ceci définit $\bar{f} : T(V) \to A$ comme application linéaire.

(Rem :Sur $T^\circ(V) = \boldsymbol{k}$, on pose $\bar{f}(\lambda) = \lambda 1_A$)

On vérifie que $\bar{f}$ est un morphisme d'algèbres : il suffit de le faire sur les tenseurs décomposables.

$$\begin{aligned}\bar{f}((v_1 \otimes \cdots \otimes v_p) \cdot (w_1 \otimes \cdots \otimes w_q)) &= \bar{f}(v_1 \otimes \cdots \otimes v_p \otimes w_1 \otimes \cdots \otimes w_q) \\ &= f(v_1) \cdots f(v_p) f(w_1) \cdots f(w_q) \\ &= \bar{f}(v_1 \otimes \cdots \otimes v_p) \cdot \bar{f}(w_1 \otimes \cdots \otimes w_q)\end{aligned} \tag{11.12}$$

□

**Fonctionalité** Soient V,W espaces vectoriels et $u \in \mathscr{L}(V, W)$

**Proposition 11.33.** *$\exists! \bar{u}, T(V) \to T(W)$ morphisme d'algèbres t.q. :*

$$\begin{tikzcd} V \arrow[r, "u"] \arrow[d, hook] & W \arrow[d, hook] \\ T(V) \arrow[r, "\bar{u}"] & T(W) \end{tikzcd}$$

*$\bar{u} = \bigoplus u^{\otimes p}$ où $u^{\otimes p} : V^{\otimes p} \to W^{\otimes p}$ est l'application linéaire donnée par :$u^{\otimes p}(v_1 \otimes \cdots \otimes v_p) = u(v_1) \otimes u(v_2) \cdots \otimes u(v_p)$*

*Démonstration.* On doit avoir $\bar{u}(v_1 \otimes \cdots \otimes v_p) = \bar{u}(v_1 \cdots v_p) = \bar{u}(v_1) \cdots \bar{u}(v_p) = u(v_1) \cdots u(v_p)$ d'où l'unicité.

Notation $T(u) : T(V) \to T(W)$ □

**Proposition 11.34.** *Si $V \xrightarrow{f} W \xrightarrow{g} R$, f,g applications linéaires. Alors $T(g \circ f)(= T(g) \circ T(f)) : T(V) \to T(R)$*

*Démonstration.* Ceci provient de l'unicité dans la prop précédente $T(g \circ f)$ et $T(g) \circ T(f)$ satisfant à même propriété de prolongement de $g \circ f$ en un morphisme d'algèbre. □

*Remarque* 11.35. T(V) n'est pas commutative si v et w non proportionnels, $v \otimes w \neq w \otimes v$.

Si $f : V \to A$ algèbre commutative, alors $T(f) : T(V) \to A$ va satisfaire

$$T(f)(v \otimes w) = f(v)f(w) = f(w)f(v) = T(f)(w \otimes v)$$

$v \otimes w - w \otimes v \in KerT(f)$

**Définition 11.36.** Soit I l'idéal bilatère de T(V) engendrée par les $v \otimes w - w \otimes v, \ v, w \in V$.

On remarque que I est engendré par des éléments homogènes (de degré 2), donc I est un idéal gradué : $I = \bigoplus_n I_n$, où $I_n = I \bigcap T^n(V)$, $x \in I$ est somme d'éléments $a(v \otimes w - w \otimes v)b$, $a, b \in T(V)$ et en décomposant a et b en composant homogènes, on ait que les composantes homogènes de x sont dans I.

On a $I_1 = \{0\}$, $I_0 = \{0\}$

**Définition 11.37.** L'algèbre symétrique $S(V) = T(V)/I$. C'est une algèbre graduée. $S(V) = \bigoplus_{n\in\mathbb{N}} S^n(V)$, où $S^n(V) = T^n(V)/I_n$. NB. $S^1(V) = V$. S(V) commutative.

**Proposition 11.38.** *(Propriété universelle de S(V))*

*Soit A algèbre commutative et $f : V \to A$ linéaire. Alors il existe un unique morphisme d'algèbre $\bar{f} : S(V) \to A$ t.q.*

$$\begin{tikzcd}
V \arrow[r, hook, "\iota"] \arrow[d, "f"] & S(V) \arrow[dl, "\bar{f}"] \\
A &
\end{tikzcd}$$

*Démonstration.* Comme f morphisme d'algèbre, $\exists ! \widetilde{f} : T(V) \to A$

(propriété universelle de T(V) : $\begin{tikzcd}
T(V) \arrow[r, "\widetilde{f}"] \arrow[d, hook, "i"] & A \\
V \arrow[ur, hook, "f"] &
\end{tikzcd}$ )

Comme A commutative, on a $\widetilde{f}(v \otimes w - w \otimes v) = 0$. Donc $I \subset Ker\widetilde{f}$.

Ainsi $\widetilde{f}$ passe au quotient

$$\begin{tikzcd}
T(V) \arrow[rr, "\widetilde{f}"] \arrow[d, "p"] & & A \\
S(V) \arrow[urr, "\bar{f}"] & & \\
& V \arrow[uul, hook, "i"] \arrow[ul, hook, "i'"] \arrow[uur, "f"] &
\end{tikzcd}$$

$p \circ i = i'$, d'où $\bar{f} \circ i' = f$ $\square$

*Remarque* 11.39. De même que T(V), S(V) est engendrée par V comme algèbre. On note le produit dans S(V) sans mettre de signe particulier $vw \in S(V)$.

Ainsi $\bar{f}$ ci dessus est donnée par $\bar{f}(v_1 \cdots v_p) = f(v_1) \cdots f(v_p)$.

**Fonctorialité** Soient V,W esp. vect, $f \in \mathscr{L}(V, W)$.

**Proposition 11.40.** $\exists!$ *morphisme d'algèbres (graduée)* $S(f) : S(V) \to S(W)$ *qui prolonge* $f$*, et il est donnée par* $S(f)(v_1 \cdots v_p) = f(v_1) \cdots f(v_p)$

*Démonstration.* On utilise le propriété universelle avec l'alèbre commutative S(W). □

**Proposition 11.41.** *Si* $V \xrightarrow{f} W \xrightarrow{g} R$ *applications linéaires, alors* $S(g \circ f) = S(g) \circ S(f)$

*Démonstration.* $S(g) \circ S(f) : S(V) \to S(R)$ morphisme d'algèbre qui prolonge $g \circ f$. $S(g) \circ S(f) = S(g \circ f)$ par unicité

□

**Algèbre symétrique d'une somme directe finie** Soient $V_1, \cdots V_n$ espaces vectoriels.

**Théorème 11.42.** *On a un isomorphisme d'al'ebres*

$$S(\bigoplus_{i=1}^{n} V_i \simeq \otimes_{i=1}^{n} S(V_i)$$

*(produit tensoriel usuel d'algèbres)*

Application : Soit V espace vectoriel de dimension n, $(e_1, \cdots, e_n)$ base de V. Alors $V = \bigoplus_{i=1}^{n} \boldsymbol{k} e_i$,

$$S(V) = \otimes_{i=1}^{n} S(\boldsymbol{k} e_i)$$

Or, pour un espace vectoriel de dimension 1 de base e, $T(\boldsymbol{k}e) = \bigoplus_{i=1}^{\infty} \boldsymbol{k} e^{\otimes n}$. $T^n(\boldsymbol{k}e) = \boldsymbol{k} e^{\otimes n}$ de dimension 1 et la loi d'al'ebre $e^{\otimes n} \cdot e^{\otimes m} = e^{\otimes(n+m)}$.

On a donc un isomorphisme d'algèbres graduée

$$T(\boldsymbol{k}e) \simeq \boldsymbol{k}[X]$$

$$e^{\otimes n} \mapsto X^n$$

Comme ici I={ 0 }. On a $T(\boldsymbol{k}e) = S(\boldsymbol{k}e) = \boldsymbol{k}[X]$.

Alors le thm dit que, pour $V = \boldsymbol{k} e_1 \bigoplus \cdots \bigoplus \boldsymbol{k} e_n$.

$$\begin{aligned} S(V) &\simeq S(\boldsymbol{k} e_1) \otimes \cdots \otimes S(\boldsymbol{k} e_n) \\ &= \boldsymbol{k}[X_1] \otimes \cdots \otimes \boldsymbol{k}[X_n] \\ &= \boldsymbol{k}[X_1, \cdots, X_n] \end{aligned} \tag{11.13}$$

*Démonstration.* du thm

$S(V_1 \otimes \cdots \otimes V_n)$, $S(V_1) \otimes \cdots \otimes S(V_n)$

On a vu : chaque $S(V_i)$ est une algèbre commutative et que le produit tensoriel usuel $S(V_1) \otimes \cdots \otimes S(V_n)$ est une algèbre commutative.

Pour construire un morphisme d'algèbre $S(V_1 \bigoplus \cdots \bigoplus V_m) \to S(V_1) \otimes \cdots \otimes S(V_n)$, il suffit, par la prop. universelle de l'algèbre symétrique, de construire une application linéaire $V_1 \bigoplus \cdots \bigoplus V_n \to S(V_1) \otimes \cdots \otimes S(V_n)$ , $\forall j$, on dispose de l'inclusion $V_j \hookrightarrow S(V_j)$ , puis d'un morphisme d'algèbre

$$S(V_j) \to S(V_1) \otimes \cdots \otimes S(V_j) \otimes \cdots \otimes S(V_n)$$

$$m_j \mapsto 1 \otimes a \cdots \otimes m_j \otimes 1 \cdots \otimes 1$$

On a aussi $V_j \to \otimes_{i=1}^n S(V_i)$ d'où une application linéaire $\bigoplus V_j \to \bigotimes S(V_i)$ dont on déduit un morphisme d'algèbre

$$\varphi : S(\bigoplus V_i) \to \bigotimes S(V_i)$$

<u>Inversement :</u> pour construire un morphisme de $\bigotimes S(V_i) \to S(\bigoplus V_j)$ il suffit de construire des morphisme d'algèbres $\psi_i : S(V_i) \to S(\bigoplus V_j)$ . ensuite, comme $S(\bigoplus V_j)$ est commutative, les images des $\psi_i$ commutant, et pour les propriété du $\otimes$ usuel d'algèbres, il y a un unique morphisme d'algèbre $\psi : \bigotimes S(V_i) \to S(\bigoplus V_j)$, $\psi(m_1 \otimes \cdots \otimes m_n = \psi_1(m_1) \cdots \psi_n(m_n)$.

On vérifie que $\psi \circ \varphi = Id$, $\varphi \circ \psi = Id$ (il suffit de le faire sur les générateurs, i.e. pour $m_i \in V_i$ où c'est aisé) $\square$

**Lien avec les tenseurs symétriques** :

On a construire S(V) comme un quotient de T(V).

Lorsque $car(\boldsymbol{k}) = 0$, il existe dans $T^n(V)$ un sous espace vectoriel isomorphe à $S^n(V)$.

**Proposition 11.43.** *$\forall n \geq 1$ , le groupe symétrique $\mathfrak{S}_n$ agit dans $T^n(V) = V^{\otimes n}$ par : $\sigma \in \mathfrak{S}_n, v_i \in V$,*

$$\sigma \cdot (v_1 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)}$$

*(on permute les positions des $v_i$)*

*Démonstration.* Ceci est bien défini car $(v_1, \cdots, v_n) \mapsto v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)}$ est n linéaire.

On vérifie : $\sigma, \tau \in \mathfrak{S}_n$

$$\begin{aligned}(\sigma\tau)(v_1 \otimes \cdots \otimes v_n) &= \sigma(\tau)(v_1 \otimes \cdots \otimes v_n)\\ &= \sigma(v_{\tau^{-1}(1)} \otimes \cdots \otimes v_{\tau^{-1}(n)})\\ &(Posons w_i = v_{\tau^{-1}(i)})\\ &= \sigma(w_1 \otimes \cdots \otimes w_n)\\ &= w_{\sigma^{-1}(1)} \otimes \cdots \otimes w_{\sigma^{-1}(n)}\\ &= v_{\tau^{-1}\sigma^{-1}(1)} \otimes \cdots \otimes v_{\tau^{-1}\sigma^{-1}(n)}\\ &= v_{(\tau\sigma)^{-1}(1)} \otimes \cdots \otimes v_{(\tau\sigma)^{-1}(n)}\end{aligned} \tag{11.14}$$

d'où une application $\mathfrak{S}_n \to GL(V^{\otimes n})$ qui est un morphisme de groupes.

□

**Définition 11.44.** -DEF :

Un élément $\xi \in V^{\otimes n}$ est dit :

a) symétrique : si $\forall \sigma \in \mathfrak{S}_n$, $\sigma(\xi) = \xi$

b) antisymétrique si : $\forall \sigma \in \mathfrak{S}_n, \sigma(\xi) = \varepsilon(\sigma)\xi,\ \varepsilon$ signative.

**Proposition 11.45.** *Soit $P_n : V^{\otimes n} \to V^{\otimes n}$, $\xi \mapsto \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \sigma(\xi)$*

*Alors $P_n$ est un projecteur d'image les tenseurs symétriques et son noyau est $KerP_n = I_n$. Ainsi, après factorisation*

$$S^n(V) \simeq \{tenseurssymtriquesdedegrn\}$$

*Démonstration.* Montrons, $\forall \tau \in \mathfrak{S}_n$, $\tau P_n = P_n\tau = P_n$

$\forall \xi \in V^{\otimes n}$, $\tau(\frac{1}{n!}\sum\sigma) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \tau\cdot\sigma$.

Or, l'application $\mathfrak{S}_n \to \mathfrak{S}_n$, $\sigma \mapsto \tau\sigma$ est bijective. Alors

$$\sum_{\sigma\in\mathfrak{S}_n} \tau\sigma = \sum_{\sigma'\in\mathfrak{S}_n} \sigma'$$

Ainsi $\tau P_n = P_n$.

De même $P_n\tau = P_n$

Ensuite

$$\begin{aligned} P_n^2 &= (\frac{1}{n!}\sum \sigma)P_n \\ &= \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \sigma P_n \\ &= \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} P_n \\ &= P_n \end{aligned} \tag{11.15}$$

La formule $\tau P_n = P_n$ indique que $Im(P_n) \subset \{$ tenseurs symétrique $\}$. L'autre inclusion est évédente.

Etude de $KerP_n$ :

$I_n = T^n(V) \cap I$ appelons $s_i = (i\ i+1)$ la transposition échangement i et i+1.

On sait que ces transpositons engenfrent $\mathfrak{S}_n$.

De plus I est engendré linéairement par les tenseurs de la forme : $\xi - \sigma(\xi)$, $\sigma \in \mathfrak{S}_n$.

On a, pour $I_2$

$$v \otimes w - w \otimes v = v \otimes w - s_1(v \otimes w)$$

Ensuite un élément de $I_n$ sera une somme de termes $a \otimes (v \otimes w - w \otimes v) \otimes b$ avec a,b homogènes, de degrés, par ex, r et s. Alors cet élément s'écrit $a \otimes v \otimes w \otimes b - s_2(a \otimes u \otimes w \otimes b)$ donc dans l'espace voulu, et aussi $I_n = T^n(V) \cap I$ est dans l'espace décrit ci-dessus.

Inversement : montrons que les $\xi - \sigma(\xi) \in I_n$, on décompose $\sigma = s_{i_1} \cdots s_{i_p}$,

$$\xi - \sigma(\xi) = \xi - s_{i_p}(\xi) + \underbrace{s_{i_p} - \sigma(\xi)}_{\xi' - \sigma'(\psi'), \sigma' = s_{i_1} \cdots s_{i_p}}$$

Ensuite, il est clair que $I_n \subset Kerp_n$. Si $\xi \in Kerp_n$,

$$\xi = \xi - p_n(\xi) = \xi - \frac{1}{n!}\sum \sigma(\xi) = \frac{1}{n!}\sum(\xi - \sigma(\xi))$$

□

## 11.3 Algèbre extérieure

Soit V un espace vectoriel. On s'intésse aux application linéaires $f : V \to A$, A algèbre t.q. $f(v)^2 = 0$ (ex typique : A algèbre altennée et $\forall v,\ f(v)$ de degré impaire)

**Définition 11.46.** Soit J l'idéal bilatère de T(V) engendré par les $v \otimes v,\ v \in V$

**Proposition 11.47.** *J est un idéal homogène,* $J_0 = \{0\},\ J_1 = \{0\}$

**Définition 11.48.** L'algèbre extérieure $\Lambda(V)$ est l'algèbre quotient :

$$\Lambda(V) = T(V)/J$$

$\Lambda(V)$ est une algèbre graduée $\Lambda(V) = \bigoplus_{n=0}^{\infty} \Lambda^n(V)$, avec $\Lambda^0(V) = \boldsymbol{k}$, $\Lambda^1(V) = V$, $n \geq 2$, $\Lambda^n(V) = T^n(V)/J_n$.

Comme T(V), c'est une algèbre engendrée par V.

**Notation** :

Si $v_1, \cdots, v_p \in V$, on note $v_1 \wedge \cdots \wedge v_p$ l'image de $v_1 \otimes \cdots v_p$ dans le quotient $\Lambda(V)$.

Comme le projection $\pi : T(V) \to T(V)/J$ est un morphisme d'algèbre, cette notation sous entend que le produit dans $\Lambda(V)$ est aussi noté $\Lambda$.

$$\pi(v_1 \otimes \cdots \otimes v_p) = \pi(v_1) \otimes \cdots \otimes \pi(v_p) = v_1 \wedge \cdots \wedge v_p$$

**Proposition 11.49.** *Soient $v, w \in V$. Alors, dans $\Lambda(V)$, $v \wedge w = -w \wedge v$*

*Démonstration.* On a : $\forall x \in V,\ x \wedge x = 0$ car $x \otimes x \in J$

On applique à $x = v + w$

$$(v + w) \wedge (v + w) = v \wedge v + w \wedge v + v \wedge w + w \wedge w = 0$$

□

**Propriété universelle :**

**Théorème 11.50.** *Soit A algèbre, $f : V \to A$ linéaire t.q. : $\forall v \in V, f(v)^2 = 0$.*

*Alors $\exists!$ morphisme d'algèbre $\bar{f} : \Lambda(V) \to A$ t.q. $f = \bar{f} \circ i$*

$$\begin{tikzcd} \Lambda(V) \arrow[rr, "\bar{f}"] & & A \\ & V \arrow[ul, hook', "i"] \arrow[ur, "f"'] & \end{tikzcd}$$

*Démonstration.* Par propriété universelle de T(V), on sait $\exists! \widetilde{f}$ morpfisme d'algèbre

$$\begin{tikzcd} T(V) \arrow[rr, "\widetilde{f}"] & & A \\ & V \arrow[ul, hook', "i"] \arrow[ur, "f"'] & \end{tikzcd}$$

On a : $\widetilde{f}(v \otimes v) = \widetilde{f}(v)^2 = f(v)^2 = 0$.

Donc $\widetilde{f}$ s'annulle sur J et donne par passage au quotient un morphisme $\bar{f} : \Lambda(V) \to A$ qui convient.

Unicité claire car $\Lambda(V)$ engendrée par V. □

**Propriété** :

On a vu : $\forall v, w \in V,\, v \wedge w + w \wedge v = 0$

**Proposition 11.51.** $\Lambda(V)$ *est une algèbre alternée.*

*Démonstration.*

**Lemme 11.52.** *Soient* $v_1, \cdots, v_p \in V,\ \sigma \in \mathfrak{S}_p$*. Alors*

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(p)} = \varepsilon(\sigma) v_1 \wedge \cdots \wedge v_p$$

*Démonstration.* de lemme :

· vrai si $\sigma = s_i$ car $v_i \wedge v_{i+1} = -v_{i+1} \wedge v_i$

· On utilise que $s_1, \cdots, s_{p-1}$ engendrent $\mathfrak{S}_p$

· Si la propriété est vraie pour $\sigma\ \tau \in \mathfrak{S}_p$, alors elle l'est pour $\sigma \cdot \tau$

$$\begin{aligned} v_{\sigma\tau(1)} \wedge \cdots \wedge v_{\sigma\tau(p)} &= \varepsilon(\sigma) v_{\tau(1)} \wedge \cdots \wedge v_{\tau(p)} \\ &= \varepsilon(\sigma)\varepsilon(\tau) v_1 \wedge \cdots \wedge v_p \\ &= \varepsilon(\sigma\tau) v_1 \wedge \cdots \wedge v_p \end{aligned} \tag{11.16}$$

□

Montrons $\Lambda(V)$ anticommutative : x,y homogènes de degrés r et s, alors $x \wedge y = (-1)^{-s} y \wedge x$.

On sait que x et y sont sommes de termes $v_1 \wedge \cdots \wedge v_r$ ou $w_1 \wedge \cdots \wedge w_s$.

Mais : $v_1 \wedge \cdots \wedge v_r \wedge w_1 \wedge \cdots \wedge w_s = (-1)^r w_1 \wedge v_1 \wedge \cdots \wedge v_r \wedge \cdots \wedge w_s$.

On poursuit :$(-1)^{r \cdot s} w_1 \wedge \cdots \wedge w_s \wedge v_1 \wedge \cdots \wedge v_r$

· Si $x \in \Lambda(V)$, degré impair $\Rightarrow x^2 = 0$.

C'est vrai si $x = v_1 \wedge \cdots \wedge v_r$ car $v_i \wedge v_i = 0$. ensuite on écrit $x = \sum \xi_j$, $\xi_j$ tenseur décomposable $v_1 \wedge \cdots \wedge v_p$.

$$x^2 = \sum \xi_j^2 + \sum_{i<j} (\xi_i \wedge \xi_j + \xi_j \wedge \xi_i) = 0$$

□

**Fonctorialité :** V,W espaces vectoriels $f : V \to W$ linéaire. Alors $\exists!$ morphisme d'algèbres $\Lambda f : \Lambda(V) \to \Lambda(W)$ t.q.

$$\begin{tikzcd} \Lambda(V) \arrow[r, "\Lambda(f)"] & \Lambda(W) \\ V \arrow[u, hook] \arrow[r, "f"] & W \arrow[u, hook] \end{tikzcd}$$

De plus , si $g : W \to U$ linéaire, alors $\Lambda(g \circ f) = \Lambda(g) \circ \Lambda(f)$.

On a : $\forall v_1, \cdots, v_p \in V$ $\Lambda(f)(v_1 \wedge \cdots \wedge v_p) = f(v_1) \wedge \cdots \wedge f(v_p)$. (Ceci donne l'unicité).

*Démonstration.* On sait $\exists! T(f) : T(V) \to T(W)$, $v_1 \otimes \cdots \otimes v_p \mapsto f(v_1) \otimes \cdots \otimes f(v_p)$. On compose par $T(W) \to \Lambda(W)$ et on obtient une application linéaire : $T(V) \to \Lambda(W)$, $v_1 \otimes \cdots \otimes v_p \mapsto f(v_1) \wedge \cdots \wedge f(v_p)$ qui s'annule sur les générateurs de J. Elle passe au quotient en une applicaiton linéaire $\Lambda(f) : \Lambda(V) \to \Lambda(W)$ qui convient, et qui est donnée par la formule annoncée.

On remarque que : $\forall p \geq 1$, $\Lambda(f)$ envoie $\Lambda^p(V) \to \Lambda^p(W)$ : $\Lambda^p(f) : \Lambda^p(V) \to \Lambda^p(W)$

La propriété $\Lambda(g \circ f) = \Lambda(g) \circ \Lambda(f)$ provient de l'unicité car $\Lambda(g) \circ \Lambda(f) : \Lambda(V) \to \Lambda(U)$ satisfait à la propriété qui caractérise $\Lambda(g \circ f)$ □

**Exemple 11.53.** : $dim V = 1$

Soit $e \neq 0$ dans V. ALors $\Lambda(V)$ engendré par e, et $e \wedge e = e^2 = 0$. Ainsi : $\Lambda(V) = \boldsymbol{k} \oplus V$

**Théorème 11.54.** *Soient* $(V_i)_{i\in I}$ *des espaces vectoriels,* $V = \bigoplus_{i\in I} V_i$. $I = \{1, \cdots, n\}$.
*Alors :*

$$\Lambda(V) \simeq \Lambda(V_1) \otimes^g \Lambda(V_2) \cdots \otimes^g \Lambda(V_n)$$

*isomorphisme d'algèbres.*

*Démonstration.* On construit des morphismes inverses l'un de l'autre.

$$\psi : \Lambda(V) \to \Lambda(V_1) \otimes^g \Lambda(V_2) \cdots \otimes^g \Lambda(V_n)$$

on utilise la prop. universelle de $\Lambda(V)$ : on construit d'abord une application linéaire $f : V \to \Lambda(V_1) \otimes^g \Lambda(V_2) \cdots \otimes^g \Lambda(V_n)$ t.q. $\forall v, f(v)^2 = 0$.

Comme $V = \bigoplus V_i$, on le fait sur chaque $V_i$. On dispose des inclusions

$$i_j : V_j \to \Lambda(V_j)$$

puis

$$\Lambda(V_j) \to \Lambda(V_1) \otimes^g \Lambda(V_2) \cdots \otimes^g \Lambda(V_n)$$

$$m_j \mapsto 1 \otimes \cdots \otimes 1 \otimes m_j \otimes 1 \cdots$$

la composée :

$$f_j : V_j \to \Lambda(V_1) \otimes^g \Lambda(V_2) \cdots \otimes^g \Lambda(V_n)$$

Vérifie : $\forall v \in V_j \ , \ f_j(v)^2 = 0$ .

On pose, pour $v_1 \in V_1, \cdots, v_n \in V_n$.

$$f(v_1 + \cdots + v_n) = \sum f_j(v_j)$$

$$f(v_1 + \cdots + v_n)^2 = \sum f_j(v_j)^2 + \sum_{i<j} (f_i(v_i) f_j(v_j) + f_j(v_j) f_i(v_i)) = 0$$

car produit tensoriel gradué d'algèbres.

Morphisme inverse :

On utilise la propriété universelle de $\otimes^g$.

Si on a des morphismes d'algèbres $\varphi_j : \Lambda(V_j) \to \Lambda(V)$ t.q. $\forall m_j \in \varphi_j$, homogènes, $\varphi_i(m_i)\varphi_j(m_j) = (-1)^{\partial m_j \partial m_i} \varphi_j(m_j)\varphi_i(m_i)$, alors $\exists!$ morphisme

$$\varphi : \Lambda(V_1) \otimes^g \cdots \otimes^g \Lambda(V_n) \to \Lambda(V)$$

$$\varphi(m_1 \otimes \cdots \otimes m_n) = \varphi_1(m_1) \cdots \varphi_n(m_n)$$

or, on dispose de l'inclusion $i_j : V_j \to V$ d'où le morphisme $\Lambda(i_j)(= \varphi_j) : \Lambda(V_j) \to \Lambda(V)$

et la propriété requise provient de ce que $\Lambda(V)$ est anticommutative, $\psi \circ \varphi = id, \ \varphi \circ \psi = id$

Je vérifient sur les générateurs. □

**Conséquence** :

Si V esp. vect. de dimension n, $\Lambda^k(V)$ est de dimension $\binom{n}{k}$.

<u>En particulier :</u> $\Lambda^k(V) = \{0\}$ si $k \geq n+1$, $dim\Lambda^n(V) = 1$

Si $(e_1, \cdots, e_n)$ base de V, alors pour $1 \leq k \leq n$ les $e_{i_1} \wedge \cdots \wedge e_{i_k}$ avec $1 \leq i_1 < i_2 < \cdots < i_k < n$ forment une base de $\Lambda^k(V)$.

Si $\mathscr{P}_k = \{partiesklmentsde\{1, \cdots, n\}\}$ une base de $\Lambda^k(V)$ est indexée par $\mathscr{P}_k$.

**Notation :** $I \in \mathscr{P}_k, I = \{i_1 < i_2 < \cdots < i_k\}$, $e_I = e_{i_1} \wedge \cdots \wedge e_{i_k}$

*Démonstration.*

$$V = \bigoplus_{i=1}^{n} \boldsymbol{k} e_i$$

$$\Lambda(V) = \Lambda(\boldsymbol{k} e_1) \otimes^g \cdots \otimes^g \Lambda(\boldsymbol{k} e_n)$$

$$\Lambda(\boldsymbol{k} e_j) = \boldsymbol{k} \oplus \boldsymbol{k} e_j$$

$\Lambda^k(V)$ est obtenu en prenant la partie homogène de degré k, i.e. en choisissant les k indices $i_1 < \cdots < i_k$ où on prend $\boldsymbol{k} e_{i_k}$.

On utilise que si W espace vectoriel $\boldsymbol{k} \otimes W \simeq W$

□

**Propriétés de** $\Lambda(V)$

On a vu, pour T(V) :

$d \geq 1, \ V^d \to V^{\otimes d}$, $(v_1, \cdots, v_d) \mapsto v_1 \otimes \cdots \otimes v_d$ est d-linéaire et toute applications d-linéaire $f : V^d \to W$, se factorise à travers elle :

$$f(v_1, \cdots, v_d) = \bar{f}(v_1 \otimes \cdots \otimes v_d)$$

**Proposition 11.55.** *L'application*

$$V^d \to \Lambda^d V$$

$$(v_1, \cdots, v_d) \mapsto v_1 \wedge \cdots \wedge v_d$$

*est d-linéaire alternée et si W espace vectoriel et* $g : V^d \to W$ *d-linéaire alternée, alors* $\exists! \bar{g} : \Lambda^d V \to W$ *linéaire t.q.* $g(v_1, \cdots, v_d) = \bar{g}(v_1 \wedge \cdots \wedge v_d)$

*Démonstration.* Par d-linéaritŕ, on sait que g se factorise à travers $V^{\otimes d}$, et comme elle est alternée, l'application obtenue s'annulle sur $V^{\otimes d} \cap J$, donc se factorise à travers $\Lambda 6 dV$.

Unicité claire sur la formule. □

**Proposition 11.56.** *Supposons* $dim V = n$ *finie. Alors pour* $0 \leq k \leq n$*, la forme bilinéaire*

$$\Lambda^k V \times \Lambda^{n-k} V \to \lambda^n \simeq \boldsymbol{k}$$

$$(x, y) \mapsto x \wedge y$$

*est non dégénésée. On a un isomorphisme*

$$\Lambda^{n-k} V \simeq (\Lambda^k V)^*$$

*(Il dépend du choix d'une base.)*

*Démonstration.* Fixons une base $(e_1, \cdots, e_n)$ de V.

Les $(e_I)_{I \in \mathscr{P}_K}$ base de $\Lambda^k V$.

Pour $I \in \mathscr{P}_k, J \in \mathscr{P}_{n-k}$, $e_I \wedge e_J = 0$ si $I \cap J \neq \varnothing$ et $e_I \wedge E_{I^c} = \pm e_1 \wedge \cdots \wedge e_n$. ($I^c$= comlémentaire de I).

La base duale de $(e_I)_{I \in \mathscr{P}_k}$ vis à vis de cette forme bilinéaire, est , au signe près $(e_{I^c})$ base de $\Lambda^{n-k}(V)$ □

**Proposition 11.57.** *Il existe une application bilinéaire* $\Lambda^p(V^*) \times \Lambda^p(V) \to \boldsymbol{k}$, $0 \leq p \leq n$, *donnée par* $(l_1 \wedge \cdots \wedge l_p, v_1 \wedge \cdots \wedge v_p) \mapsto det(l_i(v_j))_{1 \leq i,j \leq p}$ *qui est non dégénérée. d'où un isomorphisme*

$$\Lambda^p(V^*) \simeq (\Lambda^p(V))^*$$

*Remarque* 11.58. On a vu $dim \Lambda^n(V) = 1$ , ce qui ne démontre le fait que l'espace des formes n-linéaires alternées est de dim 1, puis que cela en est le duel.

Ceci donne l'existence du déterminant de n vecteurs.

Fixons $(e_1, \cdots, e_n)$ base, $x^1, \cdots, x^n \in V$, $x^1 = \sum x^i_j e_j$,

$$
\begin{aligned}
x^1 \wedge \cdots \wedge x^n &= (\sum_{j_1=1}^{n} x^1_{j_1} e_{j_1}) \wedge (\sum_{j_2=1}^{n} x^i_{j_2} e_{j_2}) \wedge \cdots \\
&= \sum_{j_1,\cdots,j_n} x^1_{j_1} \cdots x^n_{j_n} \quad \underbrace{e_{j_1} \wedge \cdots \wedge e_{j_n}}_{\neq 0 quesi \{j_1,\cdots,j_n\}=\{1,\cdots,n\}} \\
&(i.e.\ \ e_{j_1} \wedge \cdots \wedge e_{j_n} \neq 0 \iff j : K \mapsto j(k) \ \ bijection) \\
&= \sum_{j\in\mathfrak{S}_n} x^1_{j(1)} \cdots x^n_{j(n)} e_{j(1)} \wedge \cdots \wedge e_{j(n)} \\
&= \sum_{j\in\mathfrak{S}_n} x^1_{j(1)} \cdots x^n_{j(n)} \varepsilon(j) e_1 \wedge \cdots \wedge e_n \\
&= (\sum_{j\in\mathfrak{S}_n} \varepsilon(j) x^1_{j(1)} \cdots x^n_{j(n)}) e_1 \wedge \cdots \wedge e_n \\
&= det(x^1, \cdots, x^n)
\end{aligned}
\tag{11.17}
$$

*Démonstration.* de la proposition :

On sait que le déterminant d'une matrice est n-linéaire alterné en ses vecteurs lignes .

Ainsi $(l_1, \cdots, l_p) \mapsto det(l_i(x_j))$ est p-linéaire alternée, donc se factorise à travers $\Lambda^p(V^*)$.

De même $(x_1, \cdots, x_p) \mapsto det(l_i(x_j))$ se factorise à travers $\Lambda^p(V)$.

On dispose donc d'une application bilinaéaire $b : \Lambda^p(V^*) \times \Lambda^p(V) \to \boldsymbol{k}$.

Fixons $(e_1, \cdots, e_n)$ base de V.

Soit $(e^*_1, \cdots, e^*_n)$ base duale.

$(e_I)_{I\in\mathscr{P}_p}$ base de $\Lambda^p(V)$, $(e^*_J)_{J\in\mathscr{P}_p}$ base de $\Lambda^p(V^*)$.

$b(e^*_J, e_I) = 0$ si $I \neq J$, $b(e^*_J, e_I) = 1$ si $I = J$

$I = i_1 < \cdots < i_p$, $J = j_1 < \cdots < j_p$

$(e^*_{jk}(e_{il}))_{1\leq k,l\leq p}$ la première ligne non nulle $\Rightarrow\ \exists l,\ j_1 = i_l$. Si $l > 1$, alors $i_1 < j_1$ et lapremière colonne est nulle , d'où $j_1 = i_1$ si $det \neq 0$.

On poursuit avec $j_2$ et on obtient $det \neq 0 \iff I = J$.

□

*Remarque* 11.59. On a vu si $u \in \mathscr{L}(V)$, on a $\forall p = 0, \cdots n$, $\Lambda^p u : \Lambda^p V \to \Lambda^p V$. pour p=n, $\Lambda^n u$ est la multiplication par $detu$.

**Lien avec les déterminants mineurs d'une matrice**

$M \in M_n(\boldsymbol{k})$, $I, J \in \mathscr{P}_p$, $M_{I,J}$ la matrice extraite obtenue en prenant les lignes dont l'indice est dans I et les colonnes dont l'indice est dans J $det()M_{I,J}$ déterminant mineur d'indices I et J .

On considère M comme une application linéaire $u : \boldsymbol{k}^n \to \boldsymbol{k}^n$.

Pour $p \leq n$, on dispose de $\Lambda^p u : \Lambda^p(\boldsymbol{k}^n) \to \Lambda^p(\boldsymbol{k}^n)$. La matrice de $\Lambda^p u$ dans la base $(e_I)_{I \in \mathscr{P}_p}$, $(e_1, \cdots, e_n)$ base canomique de $\boldsymbol{k}^n$ est la matrice formée des déterminants mineurs de taille p.

*Démonstration.* $e_I = e_{i_1} \wedge \cdots \wedge e_{i_p}$

Le coefficient de matrice de $\Lambda^p u$ entre $e_I$ et $e_J$ est donnée par : $< e_I^*, \Lambda^p u(e_J) >$

$$\Lambda^p u(e_J) = u(e_{j_1}) \wedge \cdots \wedge u(e_{j_p})$$

On a vu ci-dessus $e_I^* = e_{i_1}^* \wedge \cdots \wedge e_{i_p}^*$ via la forme bilinéaire.

Il faut donc calculer

$$\begin{aligned} < e_{i_1}^* \wedge \cdots \wedge e_{i_p}^*, u(e_{j_1}) \wedge \cdots \wedge u(e_{j_p}) > &= det(e_{lk}^*(u(e_j l))) \\ &= det M_{I,J} \end{aligned} \tag{11.18}$$

$$m_{ij} =< e_i^*, u(e_j) >$$

□

**Conséquence** Déterminent mineur d'un produit de 2 matrices M,N

$$det((MN)_{I,J})$$

Soit $u \in \mathscr{L}(\boldsymbol{k}^n)$ de matrice M, $v \in \mathscr{L}(\boldsymbol{k}^n)$ de matrice N. Alors $u \circ v$ a pour matrice MN, $det((MN)_{I,J})$ = coefficient de la matrice de $\Lambda^p(uv)$ entre $e_I$ et $e_J$.

Mais $\Lambda^p(uv) = \Lambda^p(u)\Lambda^p(v)$. La matrice de $\Lambda^p(uv)$ est la produit des matrices de $\Lambda^p(u)$ et $\Lambda^p(v)$.

D'où

$$det(MN)_{I,J} = \sum_{K \in \mathscr{P}_p} (det M_{I,K})(det N_{K,J})$$

**Proposition 11.60.** *Soit $u \in \mathscr{L}(v)$*

$$det(\lambda Id + u) = \sum Tr(\Lambda^k u)\lambda^{n-k}$$

*Démonstration.* $det(\lambda Id + u)$

$$\Lambda^n(\lambda Id + u)(e_1 \wedge \cdots \wedge e_n) = (\lambda e_1 + u(e_1)) \wedge \cdots \wedge (\lambda e_n + u(e_n))$$

On développe ce polynôme en $\lambda$. Pour avoir le terme en $\lambda^{n-k}$, il faut prendre $(n-k)e_i$ et $ku(e_j)$.

$j_1 < \cdots < j_k$ d'où au signe près $\varepsilon(I)$

$$\begin{aligned} e_{I^c} \wedge \Lambda^k u(e_I) &= e_{I^c} \wedge \sum_{J \in \mathscr{P}_k} det(M_{II} e_J) \\ &= e_{I^c} \wedge det(M_{II}) e_I \end{aligned} \tag{11.19}$$

Qu'on somme

$$\begin{aligned} \sum_{I \in \mathscr{P}_k} \varepsilon(I) e_{I^c} \wedge e_I \cdot det(M_{II}) &= \sum_{I \in \mathscr{P}_k} e_1 \wedge \cdots \wedge e_n det(M_{II}) \\ &= (\sum_{I \in \mathscr{P}_k} det(M_{II})) e_1 \wedge \cdots \wedge e_n \\ &= Tr(\Lambda^k u) e_1 \wedge \cdots \wedge e_n \end{aligned} \tag{11.20}$$

□