C) Espaces vectoriels.

1) Définition d'un espace vectoriel.

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ est le corps des *scalaires*.

E est un $\mathbb{K}$-espace vectoriel si et seulement si :

C'est un ensemble non vide muni de deux opérations, une loi interne notée : « + », et une loi externe notée : « . ».

Le couple (E, +) est un groupe commutatif[i].

La loi externe vérifie les quatre propriétés suivantes, pour tout couple de vecteurs (u, v) et tout couple de scalaires (α, β) :

(i) : $1.u = u$;
(ii) : $\alpha.(u + v) = \alpha.u + \alpha.v$;
(iii) : $(\alpha + \beta).u = \alpha.u + \beta.u$;
(iv) : $\alpha.(\beta.u) = (\alpha\beta).u$.

- *Propriétés*.

a) La commutativité de l'addition est une conséquence des autres axiomes[ii].

- *Preuve* : $(1 + 1).(u + v) = 1.(u + v) + 1.(u + v) = (u + v) + (u + v) = u + v + u + v$ (en appliquant (iii), puis l'associativité de l'addition).
Mais : $(1 + 1).(u + v) = (1 + 1).u + (1 + 1).v = u + u + v + v$ (en appliquant d'abord (ii), puis (iii)).
D'où : $u + v + u + v = u + u + v + v$; on additionne $(-u)$ à gauche et $(-v)$ à droite, il reste ainsi : $v + u = u + v$.

b) Intégrité : $\alpha.u = 0_E \Leftrightarrow \alpha = 0$ ou $u = 0_E$.

- *Preuves* : $u = 1.u = (1 + 0).u = 1.u + 0.u = u + 0.u$; d'où : $u = u + 0.u$; en additionnant $-u$ à gauche : $0_E = 0.u$. On peut écrire de même : $\alpha.0_E = \alpha.(0_E + 0_E) = \alpha.0_E + \alpha.0_E$, en additionnant $-(\alpha.0_E)$ à gauche : $0_E = \alpha.0_E$. Ainsi : $\alpha = 0$ ou $u = 0_E \Rightarrow \alpha.u = 0_E$. Supposons maintenant que : $\alpha.u = 0_E$. Si $\alpha = 0$ la propriété est vraie ; sinon il possède un inverse α^{-1} et on a ainsi :
$u = 1.u = (\alpha^{-1}\alpha).u = \alpha^{-1}.(\alpha.u) = \alpha^{-1}.0_E = 0_E$, d'où : $u = 0_E$. La réciproque est établie, ce qui achève de prouver la propriété.

c) Soustractions : $(-1).u = -u$; $(-\alpha).u = \alpha.(-u) = -(\alpha.u)$; $\alpha.(u - v) = \alpha.u - \alpha.v$; $(\alpha - \beta).u = \alpha.u - \beta.u$.

- *Preuves* : $u + (-1).u = 1.u + (-1).u = (1 + (-1)).u = 0.u = 0_E$; donc : $u + (-1).u = 0_E$, en additionnant $-u$ à gauche : $(-1).u = -u$. Par suite : $(-\alpha).u = (-1.\alpha).u = (\alpha(-1)).u = \alpha.((-1).u) = \alpha.(-u)$, et : $(-\alpha).u = (-1.\alpha).u = (-1).(\alpha.u) = -(\alpha.u)$; on note plus simplement : $-\alpha.u$. De même : $\alpha.(u - v) = \alpha.(u + (-v)) = \alpha.u + \alpha.(-v) = \alpha.u + (-\alpha.v) = \alpha.u - \alpha.v$.
Ou encore : $(\alpha - \beta).u = (\alpha + (-\beta)).u = \alpha.u + (-\beta).u = \alpha.u + (-\beta.u) = \alpha.u - \beta.u$.

- *Exemples* : $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel et un $\mathbb{R}$-espace vectoriel (ainsi qu'un $\mathbb{Q}$-espace vectoriel ; tout espace vectoriel sur un corps est aussi un espace vectoriel sur les corps plus petits) ; $\mathscr{F}(A, E)$ l'ensemble des applications de A dans E, où A est un ensemble quelconque non vide et E un $\mathbb{K}$-espace vectoriel, est un $\mathbb{K}$-espace vectoriel (si $A = \mathbb{N}$: suites à valeurs dans $\mathbb{K}$). De même : $\mathscr{C}^m(\mathbb{K}^n, \mathbb{K}^p)$ l'ensemble des applications de classe C^m de $\mathbb{K}^n$ dans $\mathbb{K}^p$ est un $\mathbb{K}$-espace vectoriel (si $m = 0$: continues, sinon si $p = 1$: dérivée m-ième continue, si $p > 1$: dérivées partielles d'ordre m continues). Ou encore : $\mathbb{K}[X]$ l'ensemble des polynômes d'indéterminée X à coefficients dans $\mathbb{K}$, l'ensemble des suites ou l'ensemble des fonctions définies par des séries entières à valeurs dans $\mathbb{K}^n$, sont aussi des $\mathbb{K}$-espaces vectoriels. Ainsi que les ensembles de matrices de $\mathscr{M}_{n,p}(\mathbb{K})$ à n lignes, p colonnes et à valeur dans $\mathbb{K}$.

2) Sous-espaces vectoriels.

- *Combinaison linéaire* : On appelle combinaison linéaire de la famille de vecteurs : $u_1, u_2, ..., u_n$, tout vecteur v de E tel qu'il existe des scalaires $\alpha_1, \alpha_2, ..., \alpha_n$, pour lesquels : $v = \alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n$.

F est un sous-espace vectoriel (sev) de E si et seulement si :

$$\boxed{F \neq \emptyset \text{ et } (\forall \alpha \in \mathbb{K} \text{ et } \forall (u, v) \in F^2,\ u + v \in F \text{ et } \alpha.u \in F)}.$$

- *Preuve* : La commutativité et l'associativité de l'addition se transmettent : *par hérédité* ; si l'opération externe est stable alors pour tout vecteur u de F : $0.u = 0_E \in F$, et $(-1).u = -u \in F$. Les quatre propriétés de l'opération externe sont tout aussi évidentes.

- *Remarque* : (F est un sev de E) $\Leftrightarrow$ $(F \neq \emptyset$ et $\forall (\alpha, \beta) \in \mathbb{K}^2$ et $\forall (u, v) \in F^2,\ \alpha.u + \beta.v \in F)$.

$\Leftrightarrow$ $(0_E \in F$ et $\forall \alpha \in \mathbb{K},\ \forall (u, v) \in F^2,\ \alpha.u + v \in F)$.

$\Leftrightarrow$ $(F \neq \emptyset$ et $\forall \alpha \in \mathbb{K},\ \forall (u, v) \in F^2,\ \alpha.u - v \in F)$.

- *Preuve* : On note (*i*) la définition, et respectivement (*ii*), (*iii*), (*iv*) les trois propositions de la remarque ci-dessus. (*ii*) $\Rightarrow$ (*i*) est une évidence car en posant dans (*ii*) $\beta = 0$ on retrouve la première condition de (*i*), et la seconde en posant $\alpha = \beta = 1$. L'implication réciproque est simple à établir car la première condition de (*i*) implique que αu et βv sont dans F, tandis que la seconde condition implique que leur somme $\alpha u + \beta v$ est aussi dans F.
Il est tout aussi évident que (*ii*) implique (*iii*) et (*iv*), moyennant la remarque que si F est non vide il contient au moins un vecteur u, donc aussi $0.u = 0_E$. Si on part de (*iii*), la première partie de la proposition prouve au passage que F est non vide ; en posant successivement $v = 0_E$ (raison pour laquelle il faut qu'il soit dans F), puis $\alpha = 1$, on obtient les deux conditions de (*i*). Enfin, en posant $\alpha = 1$ et $u = v$ dans (*iv*) on montre que 0_E est dans F, et la fin est triviale.

- *Proposition* : Étant donnée une famille A non vide de vecteurs de E, l'ensemble des combinaisons linéaires finies (d'un nombre fini) de vecteurs de A est un sous-espace vectoriel de E, noté : Vect(A). Par ailleurs Vect(A) est le plus petit sous-espace vectoriel de E contenant A. On pose par ailleurs : $\text{Vect}(\emptyset) = \{\vec{0}\}$.

- *Preuve* : $v + w = (\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n) + (\beta_1.u_1 + \beta_2.u_2 + ... + \beta_n.u_n) = (\alpha_1 + \beta_1)u_1 + (\alpha_2 + \beta_2).u_2 + ... + (\alpha_n + \beta_n).u_n$, et on procède de même pour la stabilité de la loi externe ; comme A n'est pas vide, c'est bien un sev. Il contient A car chaque vecteur de A est une combinaison linéaire où son propre coefficient vaut 1 et les autres 0. C'est aussi le plus petit car s'il y en avait un plus petit ça voudrait dire qu'il ne contiendrait pas au moins une des combinaisons linéaires, ce qui serait en contradiction avec les conditions de stabilité des deux lois.

3) Familles génératrices. Définition de la dimension infinie.

Une famille G de vecteurs de E est dite génératrice si et seulement si tout vecteur de E peut s'écrire comme combinaison linéaire **finie** de vecteurs de G.

Un sous-espace vectoriel F étant lui-même un espace vectoriel, on pourra parler de « famille génératrice de F » : A est une famille génératrice de F si et seulement si Vect(A) = F.

Si E possède une partie génératrice finie, on dit qu'il est de dimension finie ; dans le cas contraire on dit qu'il est de dimension infinie.

- *Théorème* : De toute famille génératrice d'un espace vectoriel de dimension finie, on peut extraire une partie génératrice finie.

- *Preuve* : Soit G une partie génératrice quelconque de E. Par définition il existe une partie génératrice finie G' de E ; il existe donc un entier naturel n tel que $G' = \{e_1, e_2, ..., e_n\}$. La famille G étant aussi génératrice, les vecteurs de G' sont des combinaisons linéaires finies d'éléments de G ; soit $\{u_{k,1}, u_{k,2}, ..., u_{k,n_k}\}$ les vecteurs de G dont e_k est combinaison linéaire. Alors : $G_0 = \bigcup_{k=1}^{n}\{u_{k,1}, u_{k,2}, ..., u_{k,n_k}\}$ est une partie finie de G tout en étant génératrice car, dans toute combinaison linéaire d'éléments de G', il suffit de remplacer e_k par son expression dans G_0.

- *Exemple des polynômes* : Toute famille de polynôme contenant au moins un polynôme de chaque degré est génératrice : A génératrice de $\mathbb{K}[X]$ $\Leftrightarrow$ $\forall n \in \mathbb{N},\ \exists P \in A,\ \deg(P) = n$. (On peut adapter à $\mathbb{K}_n[X]$).

4) Familles libres.

Une famille L de vecteurs de E est dite libre si et seulement si :

Pour toute famille $(u_1, u_2, ..., u_n)$ de L, le fait qu'il existe $(\alpha_1, ..., \alpha_n) \in \mathbb{K}^n$ tels que $\alpha_1.u_1 + ... + \alpha_n.u_n = 0_E$, implique nécessairement $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$.

Cela signifie que les seules combinaisons linéaires finies de $Vect(L)$ égales au vecteur nul sont celles dont tous les coefficients sont nuls. On dit que 0_E admet une décomposition unique dans L.

$$\boxed{\forall \{u_1, u_2, ..., u_n\} \subset L,\ (\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n = 0_E \Rightarrow \alpha_1 = \alpha_2 = ... = \alpha_n = 0)}.$$

- *Remarques* : En dimension finie il faut et il suffit que la condition soit vérifiée par toute la famille, tandis qu'en dimension infinie il faut que la condition s'applique à toutes les combinaisons linéaires finies. (*Autre remarque* : L'implication réciproque de cette définition correspond à la propriété d'intégrité).
Cette proposition signifie aussi que le vecteur nul possède une unique décomposition dans une famille libre (et réciproquement).

- Aucune famille libre ne peut contenir le vecteur nul, ni deux vecteurs colinéaires, ni aucun vecteur qui puisse être une combinaison linéaire finie d'autres vecteurs de la même famille.

- Les vecteurs d'une famille libre sont dits : linéairement indépendants. Une famille non libre est dite : liée ; et les vecteurs d'une famille liée sont dits : linéairement dépendants.

- On conviendra de noter les familles de vecteurs à l'aide de parenthèses pour y introduire un ordre ; ainsi, en notant $(u_1, u_2, ..., u_n)$ une famille de vecteurs, on dira que v est combinaison linéaire de cette famille affecté des coefficients : $(\alpha_1, \alpha_2, ..., \alpha_n)$, si on a dans l'ordre : $v = \alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n$.

- *Théorème* : Toute famille libre d'un espace vectoriel de dimension finie est finie.

- *Preuve* : Soit L une famille libre. Par définition, il existe une partie génératrice finie G. Soit $\mathscr{P}$ l'ensemble des parties G' de G telles que $G' \cup L$ soit libre ; $\mathscr{P}$ n'est pas vide car $\emptyset$ est un élément de $\mathscr{P}$. Par ailleurs G ayant un nombre fini de parties, $\mathscr{P}$ est finie. Il existe donc un élément G_0 de $\mathscr{P}$ de cardinal maximal. Dans ce cas $G_0 \cup L$ est génératrice car sinon il existerait au moins un vecteur u de G qui ne serait pas combinaison linéaire d'éléments de $G_0 \cup L$ et alors $G_0 \cup \{u\}$ serait dans $\mathscr{P}$ tout en ayant un cardinal supérieur à G_0. Par ailleurs, si on enlève un élément u de $G_0 \cup L$, alors $(G_0 \cup L) \setminus \{u\}$ n'est plus génératrice, sinon u est combinaison linéaire d'éléments de $(G_0 \cup L) \setminus \{u\}$ et alors $G_0 \cup L$ ne peut plus être libre. Si $G_0 \cup L$ était infinie, on pourrait en extraire une partie génératrice finie ; comme c'est impossible, $G_0 \cup L$ est finie. Il s'en suit que L est elle-même finie, ayant un cardinal inférieur à celui de $G_0 \cup L$.

- *Proposition* : Si un vecteur est combinaison linéaire d'une famille libre, les coefficients associés sont uniques. On dit aussi que ce vecteur possède une décomposition unique dans la famille libre, et les coefficients sont alors appelés : les *composantes* du vecteur dans cette famille. (La définition d'une famille signifie donc que L est libre si et seulement si le vecteur nul admet uniquement des composantes nulles dans L).

- *Preuve* : Soit $v = \alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n = \beta_1.u_1 + \beta_2.u_2 + ... + \beta_n.u_n \Rightarrow (\alpha_1 - \beta_1).u_1 + (\alpha_2 - \beta_2).u_2 + ... + (\alpha_n - \beta_n).u_n = 0_E$, on peut alors appliquer la définition et on a : $\alpha_1 - \beta_1 = \alpha_2 - \beta_2 = ... = \alpha_n - \beta_n = 0$, d'où l'unicité.

- *Cas particulier d'un espace de fonctions (dont les polynômes)* :

$$\alpha_1.f_1 + \alpha_2.f_2 + ... + \alpha_n.f_n = 0_E \Leftrightarrow (\forall x \in \mathbb{K},\ \alpha_1.f_1(x) + \alpha_2.f_2(x) + ... + \alpha_n.f_n(x) = 0).$$

Polynômes : • Toute famille de polynômes non nuls de degrés distincts deux à deux est libre.

• Toute famille de polynômes de degrés étagés est libre : $A = (P_n)_{n\in\mathbb{N}}$, où : $\forall n \in \mathbb{N},\ 0 \le d°(P_n) < d°(P_{n+1})$.

5) Bases. Théorème d'existence.

Une famille B de vecteurs de E est une base si et seulement si elle est libre et génératrice.

B est une base de E si et seulement si tout vecteur de E s'écrit de manière unique comme combinaison linéaire **finie** d'éléments de B.

- *Théorème d'échange* (sujet d'oral) : Soit A une partie de l'espace vectoriel E, ainsi que deux vecteurs u et v de E. Alors : $(u \in \mathrm{Vect}(A \cup \{v\}) \setminus \mathrm{Vect}(A)) \Leftrightarrow (v \in \mathrm{Vect}(A \cup \{u\}) \setminus \mathrm{Vect}(A))$.

- *Preuve* : $u \in \mathrm{Vect}(A \cup \{v\}) \Rightarrow u$ est combinaison linéaire finie des vecteurs de A et de v. Soit w la combinaison linéaire des vecteurs de A ; alors : $u = w + \beta.v$, avec $\beta \neq 0$ car $u \notin \mathrm{Vect}(A)$). Alors : $v = \beta^{-1}.u + (-\beta^{-1}).w$, ce qui prouve la première implication, la seconde étant obtenue par symétrie.

- *Corollaire* : Si la famille $(u_1, u_2, ..., u_n)$ est liée et que la famille $(u_1, u_2, ..., u_{n-1})$ est libre alors u_n est combinaison linéaire de $(u_1, u_2, ..., u_{n-1})$.

- *Preuve* : Si, pour $1 \leq i \leq n - 1$, $u_i \in \mathrm{Vect}(u_1, u_2, ..., u_{i-1}, u_{i+1}, ..., u_n)$ et $u_i \notin \mathrm{Vect}(u_1, ..., u_{i-1}, u_{i+1}, ..., u_{n-1})$ alors $u_n \in \mathrm{Vect}(u_1, u_2, ..., u_{n-1})$. Un tel vecteur u_i existe obligatoirement car $(u_1, u_2, ..., u_n)$ est liée, si $u_n \neq 0_E$ il y a forcément un coefficient non nul dans une combinaison linéaire nulle (et si $u_n = 0$ c'est trivial).

- *Proposition* : Si la famille $(u_1, ..., u_n)$ est libre et incluse dans $\mathrm{Vect}(e_1, ..., e_n)$, alors la famille $(e_1, e_2, ..., e_n)$ est libre et incluse dans $\mathrm{Vect}(u_1, u_2, ..., u_n)$.

- *Preuve* : Par récurrence. Si $n = 1$ alors pour que (u_1) soit une famille libre, il est nécessaire que u_1 soit non nul. En outre, pour que u_1 soit dans $\mathrm{Vect}(e_1)$ il faut aussi que e_1 soit non nul. Par suite $u_1 = \alpha e_1$ où $\alpha \neq 0$, donc $e_1 = (1/\alpha)u_1$, ce qui est le résultat souhaité.
On suppose ensuite que la propriété est vraie jusqu'au rang $n - 1$; comme u_n n'est pas nul, $u_n = \alpha_1 e_1 + ... + \alpha_n e_n$, il existe au moins un coefficient α_i non nul. Quitte à réordonner la famille $(e_1, ..., e_n)$, on peut supposer qu'il s'agit de α_n. Alors $e_n \in \mathrm{Vect}(e_1, ..., e_{n-1}, u_n)$; soit, donc : $e_n = (u_n - \alpha_1 e_1 - ... - \alpha_{n-1}e_{n-1})/\alpha_n$.
On a ainsi, pour i quelconque, $1 \leq i \leq n - 1$: $u_i = \alpha_{1,i}e_1 + ... + \alpha_{n,i}e_n$, soit : $u_i - (\alpha_{n,i}/\alpha_n).u_n = (\alpha_{1,i} - (\alpha_{1,i}/\alpha_n).e_1 + ... + (\alpha_{1,i} - (\alpha_{n-1,i}/\alpha_n).e_{n-1}$.
On pose $v_i = u_i - (\alpha_{n,i}/\alpha_n).u_n$, et alors : $v_i \in \mathrm{Vect}(e_1, ..., e_{n-1})$. On remarque au passage que la famille $(v_1, ..., v_{n-1})$ est libre ; car, en effet : $a_1v_1 + ... + a_{n-1}v_{n-1} = a_1u_1 + ... + a_{n-1}u_{n-1} - ((a_1\alpha_{n,1} + ... + a_{n-1}\alpha_{n-1,1})/\alpha_n).u_n$. Donc, d'après l'hypothèse de récurrence, $(e_1, ..., e_{n-1})$ est libre.
Toujours selon l'hypothèse de récurrence : $(e_1, ..., e_{n-1}) \subset \mathrm{Vect}(v_1, ..., v_{n-1}) \subset \mathrm{Vect}(u_1, ..., u_n)$, et $e_n \in \mathrm{Vect}(e_1, ..., e_{n-1}, u_n) \subset \mathrm{Vect}(u_1, ..., u_n)$, et l'inclusion est établie. (L'indépendance linéaire n'est pas essentielle pour la suite, mais autant la démontrer quand même).
Si $(e_1, ... , e_{n-1}, e_n)$ est libre, la proposition est démontrée. Sinon $e_n \in \mathrm{Vect}(e_1, ..., e_{n-1})$; on peut donc remplacer e_n par son expression dans les combinaisons linéaires des u_i : $u_i = \alpha_{1,i}e_1 + ... + \alpha_{n,i}(\beta_1e_1 + ... + \beta_{n-1}e_{n-1}) \in \mathrm{Vect}(e_1, ..., e_{n-1})$.
Mais alors, comme $(u_1, ..., u_{n-1})$ est libre et incluse dans $\mathrm{Vect}(e_1, ..., e_{n-1})$, alors $(e_1, ..., e_{n-1})$ est libre et incluse dans $\mathrm{Vect}(u_1, ..., u_{n-1})$. En remplaçant chaque e_i par son expression dans $\mathrm{Vect}(u_1, ..., u_{n-1})$ dans la combinaison linéaire de u_n :
$u_n \in \alpha_1.\mathrm{Vect}(u_1, ..., u_{n-1}) + ... + \alpha_n.\mathrm{Vect}(u_1, ..., u_{n-1}) = \mathrm{Vect}(u_1, ..., u_{n-1})$. Il s'en suit que la famille $(u_1, ..., u_n)$ n'est pas libre, ce qui est exclu. Finalement, $(e_1, ..., e_n)$ est libre et la proposition est entièrement démontrée.

Théorème : Tout espace vectoriel possède une base ($\varnothing$ pour $\{\vec{0}\}$). En dimension finie elles ont toutes le même nombre d'éléments, c'est ainsi ce nombre qui est défini comme étant la dimension de l'espace concerné. Si E est de dimension infinie, toutes les bases ont une infinité d'éléments et on note : $\dim(E) = +\infty$.

- *Preuve en dimension finie*[iii] : $\{\vec{0}\}$ admet $\varnothing$ pour unique base, le théorème est donc trivialement vrai ; on suppose donc que $E \neq \{\vec{0}\}$.
Si E est de dimension finie, il existe une partie génératrice finie $G = (e_1, e_2, ..., e_n)$ de E. Si e_n s'exprime comme combinaison linéaire de $(e_1, e_2, ..., e_{n-1})$, on pose $G_{n-1} = (e_1, e_2, ..., e_{n-1})$, sinon $G_{n-1} = G$. On passe ensuite à e_{n-1} ; si e_{n-1} s'exprime comme combinaison linéaire des éléments de G_{n-1}, on pose $G_{n-2} = G_{n-1} \setminus \{e_{n-1}\}$, sinon $G_{n-2} = G_{n-1}$. Et ainsi de suite jusqu'à e, où l'on construit le dernier ensemble G_0. Il faut remarquer au passage que les familles ainsi construites sont toujours génératrices car on enlève uniquement des vecteurs qui peuvent être remplacés par ceux qui restent.
Si G_0 n'est pas libre, cela signifie qu'un de ses vecteurs s'exprime en fonction des autres, mais il aurait alors été retiré au cours du processus. La famille est donc libre et génératrice, c'est une base.

Il existe donc une base finie B de E, soit : $B = (e_1, e_2, ..., e_n)$. Soit C une autre base, elle aussi finie : $C = (u_1, u_2, ..., u_p)$. On suppose $p \geq n$ (sinon on échange les rôles de B et C). On applique alors la proposition précédente :
$(u_1, u_2, ..., u_n)$ est libre et incluse dans $\mathrm{Vect}(e_1, ..., e_n)$; il s'en suit que $(e_1, ..., e_n)$ est incluse dans $\mathrm{Vect}(u_1, ..., u_n)$, il s'en suit que, s'il existait, u_{n+1} serait combinaison linéaire des $(u_1, ..., u_n)$, ce qui est impossible. Donc $p = n$.

- *Remarque* : Il existe essentiellement deux sortes d'espaces de dimension infinie, ceux pour lesquels il est possible d'énumérer une base, comme dans l'espace des polynômes, et ceux dans lesquels ça n'est pas possible (dans ce dernier cas, la validité du théorème est liée à la validité de l'axiome du choix).

Proposition : De toute famille génératrice d'un espace vectoriel non réduit à $\{\vec{0}\}$ on peut extraire une base. (Cette base est évidemment finie en dimension finie, et infinie en dimension infinie ; en outre, la démonstration a déjà été faite à la proposition précédente dans le cas de la dimension finie).

- *Preuve en dimension finie* : Si la famille G finie, comportant n vecteurs, est liée alors il existe une combinaison linéaire nulle ayant des coefficients non nuls ; autrement dit, l'un des vecteurs u_0 de cette combinaison linéaire peut s'exprimer en fonction des autres ; soit alors $G_1 = G \setminus \{u_0\}$. Il faut remarquer que G_1 est toujours génératrice ; si G_1 n'est pas libre alors on construit G_2 de la même façon, etc... Si on devait arriver jusque là, G_{n-1} ne contiendrait plus qu'un vecteur non nul, ce serait une famille libre. Mais, si l'on s'arrête avant cela signifie qu'il y a un moment où il n'existe plus de combinaison linéaire nulle à coefficients non nuls ; autrement dit, on a construit une famille à la fois génératrice et libre : une base.

Théorème de la base incomplète : Toute famille libre peut être complétée par une autre famille libre (par exemple extraite d'une autre base) pour former une base de E. (La démonstration en dimension finie[iv] réutilise la fin de la démonstration du théorème du §4 : $G_0 \cup L$ est une base).

- *Remarque* : Si L est une famille libre et G une famille génératrice, il existe une base B telle qu'on ait :

$L \subset B \subset L \cup G$ (on peut donc compléter toute famille libre avec des vecteurs de la base canonique).

- *Exemple des polynômes* : La famille $(1, X, X^2, ..., X^n, ...)$ est une base de $\mathbb{K}[X]$, mais ce n'est pas une base de l'ensemble des séries formelles, de la forme : $f(X) = \sum_0^{\infty} a_n X^n$.

- Toute famille de polynômes non nuls de degrés distincts deux à deux est libre.
- Toute famille A de polynômes telle que : $[\forall n \in \mathbb{N},\ \exists P \in A$ tel que $d°(P) = n]$, est génératrice.
- Toute famille A de polynômes telle que : $[\forall n \in \mathbb{N},\ \exists! P \in A$ tel que $d°(P) = n]$, est une base.

(Donc : Toute famille de polynômes $(P_n)_{n \in \mathbb{N}}$ telle que : $[\forall n \in \mathbb{N},\ d°(P_n) = n]$, est une base ; c'est une famille à degrés échelonnés)[v].

- *Remarque* : Une famille $(P_n)_{n \in \mathbb{N}}$ de polynômes dont les degrés sont strictement croissants est dite : *Famille de polynômes de degrés étagés* ; si $\forall n \in \mathbb{N}$, $\deg(P_n) = n$, on dit qu'elle est à degrés échelonnés

Toute famille de polynômes de degrés étagés est libre.

Toute famille de $n+1$ polynômes de degrés étagés de $\mathbb{K}_n[X]$ est une base de $\mathbb{K}_n[X]$; elle est alors à degrés échelonnés.

6) <u>Cardinaux et nature des familles de vecteurs en comparaison avec la dimension de l'espace</u>.

La dimension du sous-espace vectoriel engendré par une famille A de vecteurs est appelé : le *rang* de cette famille. Le sous-espace vectoriel est noté $\mathrm{Vect}(A)$ et son rang $\mathrm{rg}(A)$. Un sous-espace vectoriel de dimension 1 est une *droite* ; s'il est de dimension 2, c'est un *plan* ; et si $\dim(E)$ finie et s'il est de dimension $(\dim(E) - 1)$ c'est un *hyperplan* (en dimension infinie un hyperplan est défini comme ayant un supplémentaire de dimension 1, cf. §7, ou bien : $\mathrm{Vect}(A)$ est un hyperplan si et seulement si $\mathrm{Vect}(A) \neq E$ et $\exists u \in E$ tel que $\mathrm{Vect}(A \cup \{u\}) = E$).

Proposition : A finie est libre si et seulement si $\mathrm{rg}(A) = \mathrm{Card}(A)$. En dimension finie, A est génératrice si et seulement si $\mathrm{rg}(A) = \dim(E)$.

- *Preuve* : Un sev est un espace vectoriel ; toutes ses bases ont le même cardinal, et c'est ce cardinal qui est sa dimension. La famille libre initiale est une base parmi les autres de ce sev ; son cardinal est donc égal à la dimension du sev.

Par ailleurs, d'après le théorème de la base incomplète, il est possible de compléter la famille libre pour obtenir une base dont le cardinal sera égal à la dimension de l'espace tout entier. Par suite, la famille libre initiale ayant moins de vecteurs avant d'être complétée, son cardinal est inférieur à la dimension de l'espace.

Dans le cas de la dimension finie, si son cardinal est égal à la dimension de l'espace, elle engendre donc un sev de même dimension que l'espace. Si c'est une base de l'espace la proposition est établie ; sinon, on peut la compléter pour faire une base de l'espace mais elle a alors plus de vecteurs que la dimension de l'espace, ce qui est impossible.

Conséquences : En dimension finie, soit $n = \dim(E)$.

A est une base de E si et seulement si $\mathrm{rg}(A) = \mathrm{Card}(A) = n$.

$\mathrm{Card}(A) < n \Rightarrow A$ n'est pas génératrice ; $\mathrm{Card}(A) > n \Rightarrow A$ n'est pas libre.

Une famille libre de n vecteurs est une base.
Une famille génératrice de n vecteurs est une base.
Une famille ayant moins (au sens strict) de n vecteurs n'est pas génératrice.
Une famille ayant plus (au sens strict) de n vecteurs n'est pas libre.

- *Corollaire* : La dimension d'un sous-espace vectoriel est inférieure ou égale à celle de l'espace. Et, en dimension finie, lorsqu'elle est égale, le sous-espace vectoriel est l'espace lui-même.

- *Notation* : Si $x_1, x_2, ..., x_n$ sont dans cet ordre les composantes de u dans la base $B = (e_1, e_2, ..., e_n)$, on note plus simplement $u:(x_1, x_2, ..., x_n)$, ou l'indice $_B$ est facultatif s'il n'y a pas d'ambiguïté, par exemple lorsqu'on convient que tous les vecteurs seront donnés initialement par leurs composantes dans une base fixée au départ ; une telle base s'appelle : *base canonique* .

$$u:(x_1, x_2, ..., x_n)_B \text{ ou } u:\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}_B \Leftrightarrow u = x_1.e_1 + x_2.e_2 + ... + x_n.e_n.$$

Par abus d'écriture, on peut mettre un signe égal à la place des deux points (:).

$(x_1, x_2, ..., x_n)$ sont les composantes, ou encore : *coordonnées*, du vecteur u dans la base B (dans la base canonique en l'absence de l'indice $_B$).

7) <u>Définition et existence des supplémentaires</u>.

- *Somme* : La somme de deux sous-espaces vectoriels F et F' d'un espace vectoriel E est notée $F + F'$ et définie de la façon suivante : $F + F' = \{u + u' ,\ u \in F \text{ et } u' \in F'\}$. C'est un sous-espace vectoriel ; c'est aussi le plus petit sous-espace vectoriel contenant $F \cup F'$ ($F + F' = \mathrm{Vect}(F \cup F')$) (Et réciproquement : si la décomposition est unique, la somme est directe).

- *Preuve* : Il contient F en faisant $u + 0_E$, il contient F' en faisant $0_E + u'$; il contient donc leur réunion. C'est le plus petit car il doit contenir toutes les combinaisons linéaires des vecteurs de F et de ceux de F'. Par ailleurs, c'est bien un sous-espace vectoriel car il est de façon évidente stable pour les deux lois.

- *Somme directe* : Si l'intersection de deux sous-espace vectoriels F et F' est égale à $\{0_E\}$, elle est alors minimale, leur somme est dite *directe* et notée : $F \oplus F'$. En conséquence de quoi, la décomposition d'un vecteur de $F + F'$ en un vecteur de F et un vecteur de F' est unique.

- *Preuve* : On suppose que deux décompositions sont égales : $u + u' = v + v' \Leftrightarrow u - v = v' - u'$. Comme $u - v$ est dans F et que $v' - u'$ est dans F', alors ils sont dans l'intersection ; c'est-à-dire : $u - v = v' - u' = 0_E$, ce qui prouve la proposition.

- *Intersection* : L'intersection de deux sous-espaces vectoriels est un sous-espace vectoriel.

- *Preuve* : Cette intersection est non vide car elle contient le vecteur nul. Par ailleurs, les deux lois sont stables dans cette intersection car, pour $u \in F \cap F'$: $\alpha.u$ appartient à F grâce à la stabilité dans F, et à F' grâce à la stabilité dans F' ; idem pour l'addition.

Deux sous-espaces vectoriels F et F' de E sont *supplémentaires* si et seulement si : $F \oplus F' = E$ (somme directe ; rappel : $F + F' = \{u + u',\ u \in F \text{ et } u' \in F'\}$).

$$\boxed{F \oplus F' = E \Leftrightarrow (F + F' = E \text{ et } F \cap F' = \{0_E\})}.$$

$$F \oplus F' = E \Leftrightarrow (\forall v \in E,\ \exists!\ u \in F \text{ et } \exists!\ u' \in F' \text{ tels que } v = u + u').$$

$$F \oplus F' = E \Leftrightarrow [(C \text{ base de } F \text{ et } C' \text{ base de } F' \Rightarrow C \cup C' \text{ base de } E) \text{ et } F \cap F' = \{0_E\}]$$

- *Preuve* : Tout vecteur de E se décompose de façon unique en un vecteur de F, lui-même étant combinaison linéaire unique dans C, et un vecteur de F', lui-même étant combinaison linéaire unique dans C'. Il s'en suit que tout vecteur de E se décompose de façon unique dans B ; c'est bien une base. Réciproquement, si tout vecteur de E se décompose en une combinaison linéaire de C et une combinaison linéaire de C' alors F + F' = E. Si en plus C et C' sont disjointes alors s'il y avait un vecteur non nul dans l'intersection de F et F', il serait à la fois une combinaison linéaire de C et de C' ; mais alors, en les soustrayant, il existerait une combinaison linéaire nulle de $C \cup C'$ avec des coefficients non nuls, ce qui est exclu.

- *Remarque* : Il y a d'autre équivalences en dimension finie, par exemple :

$$F \oplus F' = E \Leftrightarrow (F \cap F' = \{0_E\} \text{ et } \dim(F) + \dim(F') = \dim(E)).$$

$$F \oplus F' = E \Leftrightarrow (F + F' = E \text{ et } \dim(F) + \dim(F') = \dim(E)).$$

- *Preuve* : Si F et F' sont supplémentaires, les deux égalités sont vérifiées, l'une par définition et l'autre grâce à la proposition précédente. Il faut donc prouver la réciproque. Soit C une base de F et C' une base de F' ; elles sont nécessairement disjointes et leur réunion est une famille libre à cause de la condition : $F \cap F' = \{0_E\}$. En outre, d'après l'autre condition leur réunion est une famille de cardinal la dimension de E ; c'est donc une base de E, on est donc dans les conditions de la proposition sur la réunion des bases, et ce corollaire est vrai. Pour finir, si on suppose que F + F' = E alors $C \cup C'$ est génératrice ; et donc : $\dim(E) \le \mathrm{Card}(C \cup C') \le \mathrm{Card}(C) + \mathrm{Card}(C') = \dim(E)$ par hypothèse, alors $\mathrm{Card}(C \cup C') = \mathrm{Card}(C) + \mathrm{Card}(C')$ et elles sont disjointes. La proposition est donc vraie d'après la proposition sur la réunion des bases.

Proposition : Tout sous-espace vectoriel possède au moins un supplémentaire. Par ailleurs, en dimension finie, tous ses supplémentaires ont la même dimension.

- *Preuve* : Tout sous-espace vectoriel possède une base C qui est une famille l bre de l'espace vectoriel E ; il est donc possible de la compléter par une famille libre C' afin que $B = C \cup C'$ soit une base de E. Par suite : F et Vect(C') sont supplémentaires. En dimension finie, si dim E = n et Card(C) = p alors Card(C') = n - p ; toute famille libre complétant C devra avoir de même n - p vecteurs.

- *Proposition* (*hors programme*) : Soit f un automorphisme de E, si F et F' sont des sous-espaces supplémentaires alors il en est de même de f(F) et f(F').

- *Preuve* : Soit $v \in f(F) \cap f(F')$ alors $\exists\, u \in F$ et $\exists\, u' \in F'$ tels que $v = f(u) = f(u')$, mais comme f est injective alors u = u', ils sont donc nuls et alors v aussi. Par suite $f(F) \cap f(F') = \{0_E\}$; en outre f étant linéaire et surjective : $f(E) = f(F + F') = f(F) + f(F') = E$.

- *Cardinal de la somme* : Si F et F' sont deux sous-espaces vectoriels de E de dimension finie, alors : $\dim(F + F') = \dim F + \dim F' - \dim(F \cap F')$ (formule de Grassman[1]). En outre : $\dim(F \oplus F') = \dim F + \dim F'$.

- *Preuve* : Soit D une base de $F \cap F'$. Comme c'est une famille libre de F, on peut la compléter par une famille libre C de vecteurs de F pour que $C \cup D$ soit une base de F ; comme c'est aussi une famille libre de F', on peut la compléter par une famille libre C' de F' pour que $C' \cup D$ soit une base de F'. Alors $C \cup C' \cup D$ est une base de F + F' où elle est libre par construction et génératrice car tous les vecteur de F et de F' sont respectivement des combinaisons linéaires de $C \cup D$ et $C' \cup D$. Il suffit ensuite de les additionner, et alors : $\dim(F + F') = \mathrm{Card}(C \cup C' \cup D) = \mathrm{Card}(C) + \mathrm{Card}(C') + \mathrm{Card}(D)$ car elles sont disjointes. De même : $\dim F = \mathrm{Card}(C) + \mathrm{Card}(D)$, et puis : $\dim F' = \mathrm{Card}(C') + \mathrm{Card}(D)$; donc : $\dim(F + F') = (\mathrm{Card}(C) + \mathrm{Card}(D)) + (\mathrm{Card}(C') + \mathrm{Card}(D)) - \mathrm{Card}(D)$, la proposition est donc vraie.

- *Proposition* : Dans un espace vectoriel E, l'intersection des sous-espaces vectoriels est distributive par rapport à l'addition des sous-espaces vectoriels[vi].

[1] Hermann Günther Grassman : 1809-1877. La formule de Grassman est voisine du principe d'exclusion-inclusion, encore appelé formule de Poincaré[(*)] (*ou du crible*), pour deux ensembles : $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$ (*qu'on peut étendre aux probabilités*).
[(*)] Henri Jules Poincaré : 1854-1912.

8) Applications linéaires.

Étant donnés deux espaces vectoriels E et F, $f : E \to F$ est une application linéaire si et seulement si :

$$\forall (\alpha, \beta) \in \mathbb{K}^2 \text{ et } \forall (u, v) \in E^2,\ f(\alpha.u + \beta.v) = \alpha.f(u) + \beta.f(v).$$

- *Ou bien* : $\forall \alpha \in \mathbb{K}$ et $\forall (u, v) \in E^2$, $f(\alpha.u) = \alpha.f(u)$ et $f(u + v) = f(u) + f(v)$.

- *Remarques* : $f(0_E) = 0_F$, et : $f(\alpha.u - \beta.v) = \alpha.f(u) - \beta.f(v)$.

L'ensemble des applications linéaires de E dans F est noté $\mathscr{L}(E, F)$; l'ensemble des applications de E dans lui-même (endomorphismes) est noté plus simplement $\mathscr{L}(E)$. On distingue entre les différents types d'applications linéaires, selon que l'ensemble d'arrivée est E ou non, et selon qu'elles sont bijectives[vii] ou non :

	E et F quelconques	E = F
f quelconque	homomorphisme	endomorphisme
f bijective	isomorphisme	automorphisme

- *Remarque* : Les termes contenus dans ce tableau doivent en réalité êtres complétés par « *d'espace vectoriel* » qui dans ce chapitre est sous-entendu. Par exemple « *isomorphisme* » signifie ici : « *isomorphisme d'espace vectoriel* » car il en existe d'autres types, par exemple l'application $\mathcal{M}$ qui à une application linéaire f associe sa matrice $\mathcal{M}(f)$ dans la base canonique est en réalité un *isomorphisme d'algèbre* car une opération supplémentaire est conservée : $\mathcal{M}(f + g) = \mathcal{M}(f) + \mathcal{M}(g)$, $\mathcal{M}(\alpha.f) = \alpha.\mathcal{M}(f)$ (où α est un scalaire), et en plus : $\mathcal{M}(f\circ g) = \mathcal{M}(f)\times\mathcal{M}(g)$.

- *Remarque* : $\mathscr{L}(E, F)$ et $\mathscr{L}(E)$ sont des $\mathbb{K}$-espaces vectoriels, sous-espaces vectoriels respectifs de $\mathscr{F}(E, F)$ et de $\mathscr{F}(E, E)$.

• *Proposition* : La composée de deux applications linéaires est une application linéaire. L'inverse de toute application linéaire bijective (isomorphisme) est une application linéaire. L'ensemble des applications linéaires bijectives de $\mathscr{L}(E)$ (automorphismes) est un groupe noté $GL(E)$ et appelé : *groupe linéaire* de E.

- *Preuve* : f et g étant des applications linéaires quelconques, pour tout couple de scalaires (α, β) et tout couple de vecteurs (u, v), $f\circ g(\alpha.u + \beta.v) = f(g(\alpha.u + \beta.v)) = f(\alpha.g(u) + \beta.g(v)) = \alpha.f(g(u)) + \beta.f(g(v)) = \alpha.(f\circ g)(u) + \beta.(f\circ g)(v)$. La composée de f et g est donc encore linéaire.
Si f est bijective, soit $u' = f(u)$ et $v' = f(v)$; alors $f^{-1}(\alpha.u' + \beta.v') = f^{-1}(\alpha.f(u) + \beta.f(v)) = f^{-1}(f(\alpha.u + \beta.v)) = \alpha.u + \beta.v = \alpha.f^{-1}(u') + \beta.f^{-1}(v')$. La réciproque de f est donc aussi une application linéaire.

- *Cas particuliers* : Si l'ensemble d'arrivée est $\mathbb{K}$, l'application linéaire est appelée : *forme linéaire*. S'il s'agit d'un endomorphisme qui à tout vecteur associe lui-même, on l'appelle : *application identique*, ou : *identité*, et on la note : id_E ; $\forall u \in E$, $id_E(u) = u$.

- *Exemples* : L'application qui à tout vecteur de E associe le vecteur nul de F est appelée : application nulle. L'endomorphisme qui à tout vecteur u de E associe $k.u$, où $k \in \mathbb{K}$, est appelée : homothétie de rapport k. Étant donnés deux sous-espaces vectoriels supplémentaires F_1 et F_2 de E, l'endomorphisme qui à tout vecteur u de E associe sa composante dans F_1 est appelée : projection sur F_1 de direction F_2 (ou parallèlement à F_2) ; l'endomorphisme qui à u associe la différence des composantes dans F_1 et F_2 est la symétrie par rapport à F_1 de direction F_2 :

$F_1 \oplus F_2 = E \Rightarrow \forall u \in E, \exists! (u_1, u_2) \in F_1 \times F_2, u = u_1 + u_2$;
$p(u) = u_1 \Rightarrow p$ est un projecteur $\in \mathscr{L}(E)$; $s(u) = u_1 - u_2 \Rightarrow s$ est une symétrie $\in \mathscr{L}(E)$.

- *Contre-exemple* : Une translation de vecteur non nul, $t_v(u) = u + v$, n'est pas une application linéaire (car $t_v(0_E) \neq 0_E$).

- *Exemple de forme linéaire* : Si f est une fonction numérique définie et dérivable sur un intervalle $[a, b]$, l'application ϕ qui à f associe : $\phi(f) = \int_a^b(\int_a^x f(t)dt)dx + \int_a^b f(x)dx + f(b) - f(a) + f'(b) - f'(a)$, est une forme linéaire, etc.

9) Image et image réciproque d'un sous-espace vectoriel.

L'image d'un sous-espace vectoriel par une application linéaire est un sous-espace vectoriel.

L'image réciproque d'un sous-espace vectoriel par une application linéaire est un sous-espace vectoriel.

- *Preuves* : Soit $f \in \mathscr{L}(E, F)$, E' un sev de E et F' un sev de F. Alors : $f(E')$ n'est pas vide car il contient au moins $f(0_E) = 0_F$; de même $f^{-1}(F')$ n'est pas vide car il contient au moins 0_E pour la même raison. Étant donnés un scalaire quelconque α, et deux vecteurs u et v de E' tels que $f(u) = u'$ et $f(v) = v'$, on a : $f(\alpha.u) = \alpha.f(u) = \alpha.u'$ et comme $\alpha.u$ est dans E' alors $\alpha.u'$ est dans $f(E')$. On a de même : $f(u + v) = f(u) + f(v) = u' + v'$ et comme $u + v$ est dans E', alors $u' + v'$ est dans $f(E')$. Il s'en suit que $f(E')$ est un sev. (On peut aussi utiliser l'existence du supplémentaire au lieu du théorème de la base incomplète).
Étant donnés deux vecteurs u' et v' de F', il peut se présenter plusieurs cas selon qu'ils ont ou non des antécédents. Si u' admet un antécédent u, alors $f(\alpha.u) = \alpha.u'$ donc $\alpha.u$ est l'antécédent d'un vecteur de F' et il est dans $f^{-1}(F')$; si u' n'admet pas d'antécédent le problème ne se pose pas. Pour l'addition : si u' et v' admettent des antécédents respectifs u et v, alors $f(u + v) = f(u) + f(v) = u' + v'$. Il s'en suit que $u' + v'$, qui est un élément de F', admet l'antécédent $u + v$ qui est donc dans $f^{-1}(F')$. Si u' et v' n'ont pas d'antécédents, le problème ne se pose pas. Si un seul des deux a un antécédent alors nécessairement leur somme n'a pas d'antécédent et le problème ne se pose pas ; en effet : $f(u) = u'$ et $f(w) = u' + v' \Rightarrow f(w - u) = f(w) - f(u) = v'$ ce qui contredit l'hypothèse.

En particulier l'image de E notée $f(E)$ ou plus souvent : **Im(f)**. On appelle rang de f : **rg(f)** = dim(Im(f)).

De même, l'image réciproque du vecteur nul notée $f^{-1}(0_F)$ ou plus souvent **Ker(f)** et appelée : Noyau de f.

Théorème du rang (ou de la dimension) : $\boxed{\mathbf{rg(f) + dim(Ker(f)) = dim(E)}}$.

- *Preuve* : Soit $B = (e_1, e_2, ..., e_p)$ une base de Ker(f) ; c'est une famille libre de E, on peut donc la compléter par $C = (u_1, u_2, ..., u_q)$ de façon à ce que $B \cup C$ soit une base de E, donc $\dim(E) = p + q$. Tout vecteur v de E s'écrit alors de manière unique dans cette base : $v = x_1.e_1 + x_2.e_2 + ... + x_p.e_p + \alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_q.u_q$, et ainsi : $f(v) = \alpha_1.f(u_1) + \alpha_2.f(u_2) + ... + \alpha_q.f(u_q)$ car la première partie étant dans le noyau, son image est nulle ; il s'en suit que $f(C)$ est une partie génératrice de Im(f).
Ensuite, étant donnée une combinaison linéaire nulle de $f(C)$: $\alpha_1.f(u_1) + \alpha_2.f(u_2) + ... + \alpha_q.f(u_q) = 0_F \Rightarrow f(\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_q.u_q) = 0_F$, d'où $\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_q.u_q \in \mathrm{Ker}(f)$ et possède une combinaison linéaire dans B : $\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_q.u_q = x_1.e_1 + x_2.e_2 + ... + x_p.e_p$. Alors : $-x_1.e_1 - ... - x_p.e_p + \alpha_1.u_1 + ... + \alpha_q.u_q = 0_E$, et comme $B \cup C$ est une base, les coefficients sont tous nuls, ce qui a pour conséquence le fait que $f(C)$ est libre. Finalement : $\dim(E) = \mathrm{Card}(B \cup C) = \mathrm{Card}(B) + \mathrm{Card}(C) = \dim(\mathrm{Ker}(f)) + \dim(f(C)) = \dim(\mathrm{Ker}(f)) + \mathrm{rg}(f)$ car $\dim(\mathrm{Im}(f)) = \dim(f(C))$. (*En dimension infinie, cette égalité est sans intérêt, elle se ramène à : $+\infty = +\infty$*).

- *Corollaire* : Si E est de dimension finie et $f \in \mathscr{L}(E, F)$, alors : Im(f) est isomorphe à tout supplémentaire de Ker(f). (Preuve immédiate avec des considérations sur les dimensions).

De l'autre côté : Soit $\dim(E) = \dim(F)$ finie, et V un supplémentaire de Im(f) dans F. Alors, d'après le théorème du rang : $\dim(V) = \dim(\mathrm{Ker}(f))$; il existe donc bien un isomorphisme de Kerf(f) dans V, mais ce n'est pas f car le seul élément de V à avoir un antécédent par f est 0_F, tandis que tous les éléments de $\mathrm{Ker}(f)$ ont pour image 0_F (on peut par exemple en construire un, en envoyant une base de $\mathrm{Ker}(f)$ sur une base de V).

10) Injections, surjections, caractérisations[viii].

$\boxed{f \text{ est injective si et seulement si : } \mathrm{Ker}(f) = \{0_E\}}$.

f est injective si et seulement si l'image d'une base de E est une famille libre de F (une base de E si f est un endomorphisme). (Ou si elle transforme toute famille libre en famille libre).

f est surjective si et seulement si : $\mathrm{Im}(f) = F$.

f est surjective si et seulement si l'image d'une base de E est une partie génératrice de F.

- *Preuves* : ① Définition d'une injection : Tout élément de l'ensemble d'arrivée admet au plus un antécédent dans l'ensemble de départ. On suppose donc qu'un certain vecteur v en a deux : u et u' ; alors : $f(u) = f(u') \Rightarrow f(u - u') = 0_F$, donc $u - u' \in \mathrm{Ker}(f)$, c'est-à-dire $u - u' = 0_E$, ce qui prouve bien $u = u'$ et l'injectivité de f.

Réciproquement, si f est injective, alors 0_F admet un unique antécédent, à savoir 0_E.

② Soit $B = (e_1, e_2, ..., e_n, ...)$ une base de E ; son image est $f(B) = (f(e_1), f(e_2), ..., f(e_n), ...)$. Si f est injective, soit $(\alpha_1, , \alpha_2, ..., \alpha_n) \in \mathbb{K}^n$ tels que : $\alpha_1.f(e_1) + \alpha_2.f(e_2) + ... + \alpha_n.f(e_n) = 0_F$; alors : $f(\alpha_1.e_1 + \alpha_2.e_2 + ... + \alpha_n.e_n) = 0_F$, donc, comme l'unique antécédent de 0_F est 0_E : $\alpha_1.e_1 + \alpha_2.e_2 + ... + \alpha_n.e_n = 0_E$, d'où, comme B est une base : $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$, ce qui prouve que $f(B)$ est libre.

Réciproquement : Si $f(B)$ est libre, soit un vecteur $u = \alpha_1.e_1 + \alpha_2.e_2 + ... + \alpha_n.e_n \in \mathrm{Ker}(f)$; on a donc : $f(\alpha_1.e_1 + \alpha_2.e_2 + ... + \alpha_n.e_n) = 0_F$, c'est-à-dire : $\alpha_1.f(e_1) + \alpha_2.f(e_2) + ... + \alpha_n.f(e_n) = 0_F$. Et comme $f(B)$ est libre alors : $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$, ce qui prouve que $\mathrm{Ker}(f) = \{0_E\}$, donc f injective.

③ C'est la définition : Si f est surjective, tout élément de f admet un antécédent dans E donc $\mathrm{Im}(f) = F$, et réciproquement.

④ Si f est surjective, tout élément v de F, étant dans $\mathrm{Im}(f)$, admet un antécédent u dans E ; u se décompose dans B, donc :

$u = \alpha_1.e_1 + \alpha_2.e_2 + ... + \alpha_n.e_n \Rightarrow v = f(u) = \alpha_1.f(e_1) + \alpha_2.f(e_2) + ... + \alpha_n.f(e_n)$, ce qui implique que $f(B)$ est une partie génératrice de F.

Réciproquement : Si $f(B)$ est une famille génératrice de F, alors tout élément v de F admet une décomposition dans cette famille, donc : $v = \alpha_1.f(e_1) + \alpha_2.f(e_2) + ... + \alpha_n.f(e_n)$, ce qui implique $v = f(\alpha_1.e_1 + \alpha_2.e_2 + ... + \alpha_n.e_n)$, et prouve que $v \in \mathrm{Im}(f)$, donc $\mathrm{Im}(f) = F$.

$\boxed{\text{Si } \dim(E) = \dim(F) \text{ (finie) alors : } f \text{ injective} \Leftrightarrow f \text{ surjective} \Leftrightarrow f \text{ bijective}}$.

- *Preuve* : Toute la démonstration repose sur le théorème du rang : f injective $\Rightarrow \dim(\mathrm{Ker}(f)) = 0$ donc $\dim(\mathrm{Im}(f)) = \dim(E)$, et tout sous-espace vectoriel de E ayant la dimension de E est E lui-même, ce qui prouve la surjectivité.

Réciproquement, si f est surjective alors $\dim(\mathrm{Im}(f)) = \dim(E)$ donc $\dim(\mathrm{Ker}(f)) = 0$, c'est-à-dire $\mathrm{Ker}(f) = \{0_E\}$.

- *Proposition* : Si $f \in \mathscr{L}(E, F)$ et si C est une famille libre de E alors $f(C)$ est une famille génératrice de $f(\mathrm{Vect}(C))$, donc : $\mathrm{Vect}(f(C)) = f(\mathrm{Vect}(C))$. Si en outre f est injective alors $f(C)$ est une famille libre. Si C est finie et f injective, alors $\dim(\mathrm{Vect}(C)) = \dim(f(\mathrm{Vect}(C)) = \mathrm{Card}(C)$.

- *Preuve* : Soit $C = (u_1, u_2, ..., u_n)$ une famille libre de E, $E' = \mathrm{Vect}(C)$ et $F' = f(E')$, qui est donc un sev d'après un théorème précédent. Tout vecteur v de E' est combinaison linéaire de C : $v = \alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n$; d'où $f(v) = \alpha_1.f(u_1) + \alpha_2.f(u_2) + ... + \alpha_n.f(u_n)$ et il s'en suit que la famille $C' = (f(u_1), f(u_2), ..., f(u_n))$ est une famille génératrice de F'. On considère ensuite une combinaison linéaire nulle de C' : $\alpha_1.f(u_1) + \alpha_2.f(u_2) + ... + \alpha_n.f(u_n) = 0_F$; on a ainsi : $f(\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n) = 0_F$. Si f est injective alors $\alpha_1.u_1 + \alpha_2.u_2 + ... + \alpha_n.u_n = 0_E$ d'où l'on déduit que $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$, en conséquence de quoi C' est une famille libre. La démonstration serait la même en dimension infinie.

- *Remarque* : Deux espaces vectoriels de même dimension finie sont isomorphes (ce qui signifie qu'il existe un isomorphisme de l'un vers l'autre). Réciproquement, s'il existe un isomorphisme de l'un vers l'autre, ils ont nécessairement même dimension. (On peut étendre cette proposition aux espaces vectoriels de dimension infinie qui possèdent une base dénombrable, c'est-à-dire énumérable, comme c'est le cas de l'espace des polynômes).

- *Preuve* : Il suffit de connaître deux bases $B = (e_1, e_2, ..., e_n)$ de E et $B' = (e'_1, e'_2, ..., e'_n)$ de F , et de poser :
$f(x_1.e_1 + x_2.e_2 + ... + x_n.e_n) = x_1.e'_1 + x_2.e'_2 + ... + x_n.e'_n$; c'est de façon évidente un isomorphisme.

- *Cas particulier* : • Si $\dim(E) = n$ alors E et $\mathbb{K}^n$ sont isomorphes. Cela permet, une fois une base canonique fixée, d'assimiler un vecteur à un n-uplet de $\mathbb{K}^n$, correspondant à ses composantes dans la base canonique. On peut alors faire toutes les opérations souhaitées sur les n-uplets à la place des vecteurs, l'isomorphisme assurant la totale compatibilité entre les uns et les autres. Il est possible d'écrire, au choix, ces n-uplets sous forme de lignes ou de colonnes ; toutefois les colonnes seront préférables en deux circonstances : lorsqu'il risque d'y avoir confusion avec des coordonnées de points dans un repère, ou encore lorsqu'on pratiquera des opérations matricielles pour chercher des images de vecteurs par une application linéaire.

Si $B = (e_1, e_2, ..., e_n)$ est la base canonique, $u:\begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{pmatrix} \Leftrightarrow u = x_1.e_1 + x_2.e_2 + ... + x_n.e_n$.

Il reste possible d'utiliser cette notation en colonne dans une autre base, à condition d'indiquer le nom de la base en indice, comme pour les lignes ; toutefois cela reste assez rare et n'est utilisé pratiquement que dans les formules de changement de base.

On note : u_B, la matrice colonne correspondant aux composantes de u dans la base B. Lorsqu'il n'y a pas d'ambiguïté, par exemple dans la base canonique, on peut écrire simplement u, ce qui revient à assimiler un vecteur à ses composantes ; c'est vrai dans $\mathbb{K}^n$, et cela consiste sinon à utiliser l'isomorphisme de E dans $\mathbb{K}^n$.

En particulier, chaque vecteur de la base canonique peut-être associée à ses composantes dans $\mathbb{K}^n$, et on écrira :

$$B = (\begin{pmatrix} 1 \\ 0 \\ ... \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ ... \\ 0 \end{pmatrix}, ..., \begin{pmatrix} 0 \\ 0 \\ ... \\ 1 \end{pmatrix})$$ (qui, sous cette forme, est aussi la base canonique de $\mathbb{K}^n$).

• *Autre cas particulier* : Il existe un isomorphisme de l'espace des polynômes dans l'ensemble des fonctions polynomiales, qui permet la plupart du temps de les assimiler l'un à l'autre.

- *De même* : On peut connaître une application linéaire simplement par la donnée des images des vecteurs d'une base de E. Soit $B = (e_1, e_2, ..., e_n)$, et $B' = (f(e_1), f(e_2), ..., f(e_n))$ qui n'est pas forcément libre ; alors : $f(x_1.e_1 + x_2.e_2 + ... + x_n.e_n) = x_1.f(e_1) + x_2.f(e_2) + ... + x_n.f(e_n)$.

- *Complément* (*hors programme*) :

• Le rang d'une injection de $\mathscr{L}(E, F)$ est $\dim(E)$; le rang d'une surjection est $\dim(F)$, le rang d'une bijection est donc $\dim(E) = \dim(F)$.

- *Preuve* : Si B est une base de E et f une injection alors $f(B)$ est une base de $\mathrm{Im}(f)$ et on a bien $\mathrm{rg}(f) = \dim(E)$. Si f est une surjection alors $f(B)$ est une famille génératrice de F ; on peut en extraire une base de F d'où $\mathrm{rg}(f) = \dim(F)$. Pour une bijection on peut appliquer les deux principes précédents simultanément.

• Si f est une bijection et qu'il est possible de composer $f \circ g$ alors $\mathrm{rg}(f \circ g) = \mathrm{rg}(g)$; et s'il est possible de composer $g \circ f$ alors $\mathrm{rg}(g \circ f) = \mathrm{rg}(g)$.
Si f est une injection et qu'il est possible de composer $f \circ g$ alors $\mathrm{rg}(f \circ g) = \mathrm{rg}(g)$.
Si f est une surjection et qu'il est possible de composer $g \circ f$ alors $\mathrm{rg}(g \circ f) = \mathrm{rg}(g)$.
Dans tous les cas, s'il est possible de composer $g \circ f$ alors $\mathrm{rg}(g \circ f) \leq \inf\{\mathrm{rg}(f), \mathrm{rg}(g)\}$. Et s'il est possible de composer $f \circ g$ alors $\mathrm{rg}(f \circ g) \leq \inf\{\mathrm{rg}(f), \mathrm{rg}(g)\}$.[ix]

11) Valeurs propres et vecteurs propres, sous-espace propres.

f étant un endomorphisme de E, λ est une valeur propre de f si et seulement s'il existe un vecteur non nul u tel que $f(u) = \lambda.u$. L'ensemble des valeurs propres d'un endomorphisme s'appelle : son *spectre*.

Étant donnée une valeur propre λ, u est un vecteur propre de f associé à la valeur propre λ si et seulement si $f(u) = \lambda.u$. Par convention, on décide que le vecteur nul n'est pas un vecteur propre.

Proposition : L'ensemble des vecteurs propres associé à une valeur propre λ donnée, auquel on adjoint 0_E, est un sous-espace vectoriel appelé sous-espace propre associé à λ, et noté lorsqu'il n'y a pas d'ambiguïté possible : E_λ.

- *Preuve* : $E_\lambda \neq \emptyset$ car $0_E \in E_\lambda$; si $(\alpha, \beta) \in \mathbb{K}^2$ et $(u, v) \in E_\lambda^2$ alors $f(\alpha.u + \beta.v) = \alpha.f(u) + \beta.f(v) = \lambda.(\alpha.u + \beta.v)$, d'où $\alpha.u + \beta.v \in E_\lambda$.

- *Proposition importante* : Toute famille de vecteurs propres (donc non nuls) associés à des valeurs propres distinctes est libre.

- *Preuve* : Par récurrence sur p, la propriété est évidente pour $p = 1$; on suppose que la famille $(u_1, u_2, ..., u_p)$ de vecteurs propres associée aux valeurs propres respectives : $\lambda_1, \lambda_2, ..., \lambda_p$, est libre. S'il existe un autre vecteur propre u_{p+1} associé à la valeur propre λ_{p+1}, la famille $(u_1, u_2, ..., u_{p+1})$ ne peut être liée que si u_{p+1} est combinaison linéaire des précédents : $u_{p+1} = \alpha 1.u1 + \alpha_2.u_2 + ... + \alpha_p.u_p$. On fait ensuite l'image par f de cette égalité d'une part, et on la multiplie par λ_{p+1}, d'autre part :
$\lambda_{p+1}.u_{p+1} = \lambda_1\alpha 1.u1 + \lambda_2\alpha_2.u_2 + ... + \lambda_p\alpha_p.u_p = \lambda_{p+1}\alpha 1.u1 + ... + \lambda_{p+1}\alpha_p.u_p$; il ne reste plus qu'à soustraire les deux formes obtenues :
$(\lambda_1 - \lambda_{p+1})\alpha 1.u1 + (\lambda_2 - \lambda_{p+1})\alpha_2.u_2 + ... + (\lambda_p - \lambda_{p+1})\alpha_p.u_p = 0_E$. D'où, comme c'est une combinaison linéaire nulle d'une famille libre :
Soit $\lambda_1 = \lambda_2 = ... = \lambda_{p+1}$, ce qui est impossible par hypothèse, soit $u_{p+1} = 0_E$, ce qui aussi exclu, d'où la validité de la proposition.

- *Exemple* : Dans $E = \mathbb{R}^4$ muni d'une base $B = (e_1, e_2, e_3, e_4)$, soit l'endomorphisme f tel que :

$f(e_1) = e_3$, $f(e_2) = -e_4$, $f(e_3) = e_1$, $f(e_4) = -e_2$.

On arrive à : $E_1 = Vect(e_1 + e_3, e_2 - e_4)$ et $E_{-1} = Vect(e_1 - e_3, e_2 + e_4)$, avec $E_1 \oplus E_{-1} = E$.

- *Application* : S'il existe une base de vecteurs propres, l'application linéaire s'exprime très simplement dans cette base : Soit $B = (e_1, e_2, ..., e_n)$ une telle base, chaque e_i étant associé à la valeur propre λ_i (pas forcément distinctes) ; alors : $f(x_1.e_1 + x_2.e_2 + ... + x_n.e_n) = \lambda_1 x_1.e_1 + \lambda_2 x_2.e_2 + ... + \lambda_n x_n.e_n$.

- *Exemple* : Dans l'espace des fonctions numériques, soit la famille ; $(e^{a_1x}, e^{a_2x}, ..., e^{a_nx})$ où les a_i sont des réels distincts deux à deux. Ces fonctions sont des vecteurs propres de l'application linéaire qui à toute fonction associe sa dérivée, associées à des valeurs propres distinctes. Autrement dit, c'est une famille libre.

- *Remarque* : $E_0 = Ker(f)$ et $E_1 = Inv(f)$.

12) <u>Cas particuliers des homothéties, projecteurs et symétries</u>.

L'endomorphisme h est une homothétie si et seulement s'il existe un scalaire k appelé son rapport tel que pour tout vecteur u : $h(u) = k.u$. Il s'en suit que k est son unique valeur propre et que le sous-espace propre associé est E lui-même.

• *Proposition* (*hors programme*) : L'ensemble des homothéties de rapport non nul sur E est un sous-groupe[x] de GL(E).

- *Preuve* : Il est non vide car l'identité est une homothétie de rapport 1 ; par ailleurs une homothétie de rapport non nul est bijective, l'inverse de l'homothétie de rapport k est l'homothétie de rapport $1/k$. Enfin, la composée de deux homothéties de rapports respectifs k et k' est une homothétie de rapport kk'. C'est donc bien un sous-groupe.

- *Exercice* : Si $f \in \mathscr{L}(E)$ vérifie : Pour tout vecteur u de E, u et $f(u)$ sont colinéaires, montrer que c'est une homothétie (on distinguera les cas où $\dim(E) = 1$ et où $\dim(E) \geq 2$)[xi].

L'endomorphisme p est un projection, ou un projecteur, si et seulement si $p \circ p = p$. Ou encore : si et seulement si les sous-espaces propres E_1 et E_0 sont supplémentaires (alors p est la projection sur E_1 parallèlement à E_0. On peut aussi remarquer que $E_1 = Inv(p)$ et $E_0 = Ker(p)$).

- *Preuve* : ① Si E_0 et E_1 sont supplémentaires, il est simple d'établir que p est un projecteur en utilisant la définition. Réciproquement, si p est un projecteur, alors E_0 et E_1 sont naturellement supplémentaires.

② Soit $F = Im(p)$ et $F' = Ker(p)$; si p est un projecteur alors $F = E_1$ et $F' = E_0$, d'où tout vecteur v se décompose de manière unique dans $F{\times}F'$: $v = u + u'$, avec $p(v) = p(u) + p(u') = u \Rightarrow p{\circ}p(v) = p(u) = u = p(v)$, ce qui implique $p{\circ}p = p$.

Réciproquement, si $p{\circ}p = p$, alors : $u = p(v) \in F$ et $u' = v - u$ est tel que $p(v - u) = p(v) - p(u) = p{\circ}p(v) - p(u) = p(u) - p(u) = 0_E$, d'où : $u' \in F'$. Ainsi, comme $v = p(v) + (v - p(v)) = u + u'$ possède donc une décomposition unique dans $F{\times}F'$, ce qui implique qu'ils sont supplémentaires. En outre : $u = p(v) = p{\circ}p(v) = p(u)$ donc $F \subset Inv(p) = E_1$. Comme $F \oplus E_0 = E$ et $E_1 \cap E_0 = \{0_E\}$, alors $E_1 = F$, donc p est un projecteur.

- *Corollaire* : L'endomorphisme p est un projecteur si et seulement si $Im(p) = Inv(p)$.

- *Preuve* : On sait déjà que si p est un projecteur alors $Im(p) = Inv(p)$; il faut donc prouver la réciproque. On suppose donc qu'on sait que $Im(p) = Inv(p)$; alors pour tout vecteur u de E, $p(u)$ est dans $Im(p)$, il est donc invariant. Par suite : $p(p(u)) = p(u)$, d'où $p{\circ}p = p$ qui est bien un projecteur.

• Étant donnée une base canonique : $B = (e_1, e_2, ..., e_n)$, il existe des projecteurs particuliers appelés : *projecteurs canoniques*. Le i-ème projecteur canonique, noté e_i^*, vérifie : $e_i^*(x_1.e_1 + x_2.e_2 + ... + x_n.e_n) = x_i.e_i$. La définition est la même en dimension infinie. Il ne faut pas le confondre avec la i-ème application coordonnée, notée x_i^*, qui est une forme linéaire : $x_i^*(x_1.e_1 + x_2.e_2 + ... + x_n.e_n) = x_i$.

- *Proposition* : La composée de deux projecteurs est un projecteur[xii].

- *Proposition* : s est une symétrie si et seulement si $p = (s + id_E)/2$ est un projecteur. De même p est un projecteur si et seulement si $\boxed{s = 2p - id_E}$ est une symétrie. (Avec en outre égalités respectives des sous-espace propres : $E_1(s) = E_1(p)$ et $E_{-1}(s) = E_0(p)$).

- *Preuve* : Si s est la symétrie par rapport à U de direction V, où U et V sont supplémentaires, alors tout vecteur w de E se décompose de manière unique en une somme d'un vecteur u de U et d'un vecteur v de V, avec $w = u + v$ et $s(w) = u - v$. Alors :
$p(w) = \frac{1}{2}.(s + id_E)(u + v) = \frac{1}{2}.(u - v) + \frac{1}{2}.(u + v) = u$; il s'agit bien de la projection sur U de direction V.
Si p est un projecteur, on a encore $w = u + v$, et comme $p(w) = u$, alors $(2p - id_E)(w) = 2u - (u + v) = u - v$, ce qui prouve que s est bien une symétrie (en n'oubliant pas que $p = \frac{1}{2}.(s + id_E) \Leftrightarrow s = 2p - id_E$).

- *Proposition* : L'endomorphisme s est une symétrie si et seulement si $s{\circ}s = id_E$. Ou encore : si et seulement si les sous-espaces propres E_1 et E_{-1} sont supplémentaires (alors s est la symétrie par rapport à E_1 parallèlement à E_{-1}).

- *Preuve* : En posant $p = \frac{1}{2}.(s + id_E)$, on a : s symétrie $\Leftrightarrow$ p projecteur $\Leftrightarrow$ $p^2 = p$ $\Leftrightarrow$ $(\frac{1}{2}.(s + id_E))^2 = \frac{1}{2}.(s + id_E)$ $\Leftrightarrow$ $s^2 = id_E$.

• *Corollaire* : Les automorphismes involutifs[xiii] de $GL(E)$ sont les symétries.

13) <u>Matrice d'une application linéaire</u>.

Soit $f \in \mathscr{L}(E, F)$, E et F étant de dimensions finies : $\dim(E) = p$ et $\dim(F) = n$, ainsi que $B = (e_1, e_2, ..., e_p)$ une base de E et $C = (i_1, i_2, ..., i_n)$ une base de F ; soit enfin la matrice $M \in \mathscr{M}_{n,p}(\mathbb{K})$ ayant n lignes et p colonnes à coefficients dans $\mathbb{K}$, sa j-ième colonne étant la donnée de $f(e_j)$ dans la base C. Alors (en notant u_B le vecteur colonne des composantes de u dans la base B) :

$$\forall\, u \in E,\quad \boxed{f(u)_C = M.u_B}.$$

Cela signifie que le vecteur colonne des composantes de $f(u)$ dans la base C est égal au produit de la matrice M par le vecteur colonne des composantes de u dans la base B ; on dit que M est la matrice de f relativement aux bases B et C. (On rappelle que le produit de deux matrices n'est possible que si la première matrice a autant de colonnes que la seconde a de lignes. On multiplie alors terme à terme, en additionnant au fur et à mesure, chaque ligne i de la première matrice par une colonne j de la seconde matrice, ce qui aboutit au terme situé à la i-ème ligne et j-ième colonne de la matrice produit.

Ainsi : $\mathcal{M}_{n,q}(\mathbb{K}).\mathcal{M}_{q,p}(\mathbb{K}) = \mathcal{M}_{n,p}(\mathbb{K})$.

- *Preuve* : $f(x_1.e_1 + x_2.e_2 + ... + x_p.e_p) = \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + ... + a_{1,p}x_p \\ a_{2,1}x_1 + a_{2,2}x_2 + ... + a_{2,p}x_p \\ ... \\ a_{n,1}x_1 + a_{n,2}x_2 + ... + a_{n,p}x_p \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & ... & a_{1,p} \\ a_{2,1} & a_{2,2} & ... & a_{2,p} \\ ... & ... & ... & ... \\ a_{n,1} & a_{n,2} & ... & a_{n,p} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_p \end{pmatrix}$.

On écrira plus simplement : $(a_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le p}} = \begin{pmatrix} a_{1,1} & a_{1,2} & ... & a_{1,p} \\ a_{2,1} & a_{2,2} & ... & a_{2,p} \\ ... & ... & ... & ... \\ a_{n,1} & a_{n,2} & ... & a_{n,p} \end{pmatrix}$.

- *Exemples* : Les matrices des applications linéaires de $\mathcal{L}(E)$ sont des matrices carrées ; en particulier la matrice de l'identité est appelée la matrice identique et notée I, ou I_n lorsqu'il est nécessaire de préciser qu'elle possède n lignes et n colonnes. La matrice I est composée de 1 dans sa diagonale principale et de 0 sinon :

$$I = \begin{pmatrix} 1\ 0 ... 0 \\ 0\ 1 ... 0 \\ .... \\ 0\ 0 ... 1 \end{pmatrix}.$$

- *Remarque* : $\mathcal{M}_{n,p}(\mathbb{K})$ est un $\mathbb{K}$-espace vectoriel, isomorphe à $\mathcal{L}(E, F)$ (quand : $\dim(E) = p$ et $\dim(F) = n$). (*Si $E = F$: isomorphisme d'algèbre*)

- *Conséquences* : $M(f \circ g) = M(f).M(g)$.

Si $\dim(E) = \dim(F)$: f bijective $\Leftrightarrow$ M inversible. Alors : $M(f^{-1}) = (M(f))^{-1}$.

Et aussi, $(\forall (f, g) \in \mathcal{L}(E, F)^2$ et $\forall (\alpha, \beta) \in \mathbb{K}^2)$: $M(\alpha f + \beta g) = \alpha.M(f) + \beta.M(g)$.

- *Preuve* : On assimile un vecteur à ses composantes dans la base canonique, alors $M(f \circ g).u = f \circ g(u) = f(g(u)) = M(f).g(u) = M(f).M(g).u$. Cette égalité étant vraie pour tous les vecteurs u, on obtient finalement l'égalité matricielle souhaitée.

Formules de changement de base :

Soit P la matrice de passage (de B à B') dont les colonnes sont les composantes dans la base B de E des vecteurs de la base B'. Alors :

$$\boxed{u_{B'} = P^{-1}.u_B}.$$

- *Preuve* : Soit $B = (e_1, e_2, ..., e_n)$ et $u = x_1.i_1 + x_2.i_2 + ... + x_n.i_n$ dans $B' = (i_1, i_2, ..., i_n)$, avec $i_k = a_{k,1}.e_1 + a_{k,2}.e_2 + ... + a_{k,n}.e_n$ pour tout k. Ainsi, si l'on veut exprimer u dans B il faut remplacer chaque i_k par ses composantes dans B, et on obtient à la fin le produit de matrices :

$$u_B = \begin{pmatrix} a_{1,1} & a_{1,2} & ... & a_{1,n} \\ a_{2,1} & a_{2,2} & ... & a_{2,n} \\ ... & ... & ... & ... \\ a_{n,1} & a_{n,2} & ... & a_{n,n} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{pmatrix} = P.u_{B'}, \text{ d'où le résultat.}$$

À noter que P est inversible car elle est aussi la matrice d'un endomorphisme transformant une base en une autre base.

Par suite, si $v = f(u)$ alors : $v_C = M.u_B$ et $v_{C'} = M'.u_{B'}$, d'où : $Q.v_{C'} = M.P.u_{B'}$, c'est-à-dire : $v_{C'} = Q^{-1}.M.P.u_{B'}$. Cette dernière égalité étant vérifiée pour tous les vecteurs u et v, elle est vraie pour les matrices et ainsi : $M' = Q^{-1}.M.P$.

Si f est une application linéaire de E dans F où Q est la matrice de passage de la base C' de F donnée dans C, alors :

$$M(f)_{B'C'} = Q^{-1}M(f)_{BC}P.$$

Deux matrices qui représentent la même application linéaire sont dites équivalentes.

Si f est un endomorphisme de E : $M(f)_{B'} = P^{-1}M(f)_BP$.

Deux matrices qui représentent le même endomorphisme dans des bases différentes sont **semblables** : M et M' semblables $\Leftrightarrow$ $\exists\, P$ inversible telle que $\boxed{M' = P^{-1}MP}$.

- *Conséquences* : Pour tout entier naturel n, $M'^n = P^{-1}M^nP$. Et si M est inversible cette égalité reste vraie pour tout entier relatif.

- *Exemple d'une matrice diagonale* : $\forall p \in \mathbb{N}$, $\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix}^p = \begin{pmatrix} a_1^p & 0 & \dots & 0 \\ 0 & a_2^p & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n^p \end{pmatrix}$, et si $a_i \neq 0$ pour tout i, c'est vrai pour $p \in \mathbb{Z}$.

• Plus généralement : le rang d'une matrice est le rang de la famille de ses vecteurs colonnes, c'est aussi le rang de ses vecteurs lignes, ou encore le rang de l'application linéaire qu'elle représente dans n'importe quelles bases. On notera $rg(M)$ le rang de la matrice M. Donc : **rg(M) ≤ inf{*nombre de lignes, nombre de colonnes*}**[xiv]. Ceci est une conséquence de $rg({}^tM) = rg(M)$.

- *Corollaire 1* : Si P est inversible, pour toute matrice M, si le produit $P.M$ existe alors $rg(P.M) = rg(M)$, et si on peut faire le produit $M.P$ alors $rg(M.P) = rg(M)$. Dans le cas général : $\mathbf{rg(AB) \leq inf\{rg(A), rg(B)\}}$.

- *Corollaire 2* : Deux matrices équivalentes ou deux matrices semblables ont même rang. (Immédiat avec le corollaire précédent). Deux matrices M et M' sont équivalentes s'il existe deux matrices inversibles P et Q telles que : $M' = Q^{-1}.M.P$ (la puissance $^{-1}$ est facultative) ; deux matrices M et M' sont semblables s'il existe une matrice inversible P telle que : $M' = P^{-1}.M.P$ (immédiat avec les formules de changement de base).

- *Exemples* : La matrice d'une homothétie de rapport k est : $k.I$.

Dans l'espace vectoriel E de dimension finie, soit les deux sous-espaces vectoriel supplémentaires F_1 et F_2, de bases respectives C_1 et C_2 ; alors $B = C_1 \cup C_2$ est une base de E. Soit p la projection sur F_1 de direction F_2, et s la symétrie par rapport à F_1 de direction F_2. Alors, si $M(p)$ et $M(s)$ sont les matrices respectives de p et s dans B, on a :

$$M(p) = \begin{pmatrix} 1\,0 \dots 0\,0 \dots 0 \\ 0\,1 \dots 0\,0 \dots 0 \\ \dots\dots\dots\dots \\ 0\,0 \dots 1\,0 \dots 0 \\ 0\,0 \dots 0\,0 \dots 0 \\ \dots\dots\dots\dots \\ 0\,0 \dots 0\,0 \dots 0 \end{pmatrix}, \text{ et } M(s) = \begin{pmatrix} 1\,0 \dots 0\,0 \dots 0 \\ 0\,1 \dots 0\,0 \dots 0 \\ \dots\dots\dots\dots \\ 0\,0 \dots 1\,0 \dots 0 \\ 0\,0 \dots 0\,{-1} \dots 0 \\ \dots\dots\dots\dots \\ 0\,0 \dots 0\,0 \dots {-1} \end{pmatrix}$$ (il y a exactement $\dim(F_1)$ « +1 » dans chacune).

- *Preuve* : Pour $\dim(F_1) = p$ et $\dim(F_2) = q$, et deux bases $C_1 = (e_1, e_2, ..., e_p)$ et $C_2 = (i_1, i_2, ..., i_q)$, alors
$p(x_1.e_1 + x_2.e_2 + ... + x_p.e_p + x_{p+1}.i_1 + x_{p+2}.i_2 + ... + x_{p+q}.i_q) = x_1.e_1 + x_2.e_2 + ... + x_p.e_p$, et
$s(x_1.e_1 + x_2.e_2 + ... + x_p.e_p + x_{p+1}.i_1 + x_{p+2}.i_2 + ... + x_{p+q}.i_q) = x_1.e_1 + x_2.e_2 + ... + x_p.e_p - x_{p+1}.i_1 - x_{p+2}.i_2 - ... - x_{p+q}.i_q$, d'où les matrices.

- *Remarques* : Plus généralement, si f possède une base de vecteurs propres, sa matrice sera diagonale dans cette base, la diagonale étant composée des différentes valeurs propres. Le spectre de f est aussi le spectre de la matrice.

• **rg(p) = tr(M(p))** (et ceci reste donc valable si la matrice est donnée dans une autre base comme en atteste le paragraphe 18)).

- *Complément.*

• Formule du produit de deux matrices : $(a_{i,k})_{\substack{1 \leq i \leq n \\ 1 \leq k \leq m}}.(b_{k,j})_{\substack{1 \leq k \leq m \\ 1 \leq j \leq p}} = (\sum_{k=1}^{m} a_{i,k}b_{k,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$.

Avec la forme ligne×colonne : Les L_i sont des matrices lignes de dimension m, les C_i sont des matrices colonnes de dimension m :

$$\begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{pmatrix}.(C_1\ \ C_2\ \ ...\ \ C_p) = \begin{pmatrix} L_1C_1 & L_1C_2 & ... & L_1C_p \\ L_2C_1 & L_2C_2 & ... & L_2C_p \\ \vdots & \vdots & \vdots & \vdots \\ L_nC_1 & L_nC_2 & ... & L_nC_p \end{pmatrix}.$$

• Inversion de matrices : Si $ad - bc \neq 0$, $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}.\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

$$M = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \Rightarrow Co(M) = \begin{pmatrix} b_2c_3 - c_2b_3 & -(a_2c_3 - c_2a_3) & a_2b_3 - b_2a_3 \\ -(b_1c_3 - c_1b_3) & a_1c_3 - c_1a_3 & -(a_1b_3 - b_1a_3) \\ b_1c_2 - c_1b_2 & -(a_1c_2 - c_1a_2) & a_1b_2 - b_1a_2 \end{pmatrix}, \text{ et :}$$

$$M.{}^tCo(M) = {}^tCo(M).M = \begin{pmatrix} \det(M) & 0 & 0 \\ 0 & \det(M) & 0 \\ 0 & 0 & \det(M) \end{pmatrix}. \text{ Si } \det(M) \neq 0,\ M^{-1} = \frac{1}{\det(M)}.{}^tCo(M).$$

- *Remarques* :

En dimension 2 : $M^2 = tr(M).M - \det(M).I$; en dimension 3 : $M^2 = tr(M).M + {}^tCo(M) - tr({}^tCo(M)).I$.

En dimension 3 : Soit C_1, C_2, C_3 les colonnes de $M = (C_1, C_2, C_3)$, alors $Co(M) = (C_2 \wedge C_3, C_3 \wedge C_1, C_1 \wedge C_2)$,

donc : $(C_1, C_2, C_3)^{-1} = \frac{1}{\det(C_1, C_2, C_3)}.{}^t(C_2 \wedge C_3, C_3 \wedge C_1, C_1 \wedge C_2)$.

En outre : $\det(M) = {}^tC_1 \times (C_2 \wedge C_3) = {}^tC_2 \times (C_3 \wedge C_1) = {}^tC_3 \times (C_1 \wedge C_2) = \ = {}^t(C_2 \wedge C_3) \times C_1 = {}^t(C_3 \wedge C_1) \times C_2 = {}^t(C_1 \wedge C_2) \times C_3$.

• *Cas particulier* : Si (C_1, C_2, C_3) est une base orthonormale directe, $C_1 = C_2 \wedge C_3$, $C_2 = C_3 \wedge C_1)$, $C_3 = C_1 \wedge C_2$, d'où l'on déduit : $\det(M) = {}^tC_1 \times C_1 = 1$ (c'est le carré de la norme de C_1). Ainsi : $(C_1, C_2, C_3)^{-1} = {}^t(C_1, C_2, C_3)$. (Cf. ch. I). On appelle matrice orthogonale une matrice de ce type (cf. ch. I).

- *Propriétés de la transposition et de l'inversion* : La transposée de $M = {}^tM$ (échange des lignes et des colonnes). Alors, $(\forall\ (M, N) \in \mathcal{M}_{n,p}(\mathbb{K})^2$ et $\forall\ (\alpha, \beta) \in \mathbb{K}^2)$: ${}^t(\alpha M + \beta N) = \alpha.{}^tM + \beta.{}^tN$; ${}^t(MN) = {}^tN{}^tM$. À noter que si M et N sont inversibles alors : $(MN)^{-1} = N^{-1}M^{-1}$.

En particulier, en notant L_i les lignes et C_i les colonnes : ${}^t(C_1\ C_2\ ...\ C_p) = \begin{pmatrix} {}^tC_1 \\ {}^tC_2 \\ ... \\ {}^tC_p \end{pmatrix}$ et ${}^t\begin{pmatrix} L_1 \\ L_2 \\ ... \\ L_n \end{pmatrix} = ({}^tL_1\ {}^tL_2\ ...\ {}^tL_n)$

14) <u>Méthode du pivot de Gauss</u>.

• On appelle **transformation élémentaire** d'une matrice le fait d'opérer l'une des six modifications suivantes :

(1.1) Échanger deux colonnes.

(1.2) Échanger deux lignes.

(2.1) Multiplier une colonne par un scalaire non nul.

(2.2) Multiplier une ligne par un scalaire non nul.

(3.1) Additionner à une colonne une autre colonne préalablement multipliée par un scalaire.

(3.2) Additionner à une ligne une autre ligne préalablement multipliée par un scalaire.

Chacune de ces transformations correspond à un produit de matrices : Soit $T_{i,j}$ (*<u>transposition</u>*) la matrice correspondant à la matrice identité dans laquelle on a échangé la i-ème et la j-ième ligne (ou colonne) ; soit $K_{i,\alpha}$ (*<u>dilatation</u>*) la matrice correspondant à la matrice identité dans laquelle on a multiplié la i-ème ligne (ou colonne) par le scalaire non nul α ; soit enfin $E_{i,j,\alpha}$ (*<u>transvection</u>*) une matrice correspondant à la matrice identité dans laquelle on a additionné à la ième ligne le produit de la j-ième par le scalaire α (ou à la j-ème colonne le produit de la i-ème par α, qui vient : i-ème ligne, j-ième colonne). Alors :

- En supposant que ce produit existe : $M.T_{i,j}$ est une matrice correspondant à M dans laquelle on a échangé la i-ème et la j-ième colonne.

- En supposant que ce produit existe : $T_{i,j}.M$ est une matrice correspondant à M dans laquelle on a échangé la i-ème et la j-ième ligne.

- En supposant que ce produit existe : $M.K_{i,\alpha}$ est une matrice correspondant à M dans laquelle on a multiplié la i-ème colonne par α .

- En supposant que ce produit existe : $K_{i,\alpha}.M$ est une matrice correspondant à M dans laquelle on a multiplié la i-ème ligne par α .

- En supposant que ce produit existe : $M.E_{i,j,\alpha}$ est une matrice correspondant à M dans laquelle on a additionné à la j-ème colonne le produit de la i-ième par α .

- En supposant que ce produit existe : ${}^tE_{i,j,\alpha}.M$ est une matrice correspondant à M dans laquelle on a additionné à la i-ème ligne le produit de la j-ième par α .

- *Proposition* : Les matrices des transformations élémentaires sont inversibles (pour les dilatations il faut que α soit non nul). Il s'en suit que la transformation élémentaire d'une matrice laisse son rang invariant. (Comme elles sont carrées, il suffit de montrer que leurs colonnes sont linéairement indépendantes).

$$T^{-1}_{i,j} = T_{i,j},\ K^{-1}_{i,\alpha} = K_{i,1/\alpha}\ (\alpha \neq 0),\ E^{-1}_{i,j,\alpha} = E_{i,j,-\alpha}.$$

- *Remarques* : On peut donc appliquer les transformations élémentaires en cascade ; autrement dit, on peut appliquer n'importe quelle permutation des colonnes ou des lignes, on peut remplacer n'importe quelle colonne ou ligne par une combinaison linéaire respectivement de toutes les colonnes ou toutes les lignes, à condition que le coefficient concernant la colonne ou la ligne initiale ne soit pas nul. Cela sans changer le rang de la matrice.

- *Méthode du pivot* : Soit M une matrice carrée et I l'identité de même dimension : n. On construit avec ces deux matrices une nouvelle matrice G telle que ses n premières colonnes soit celles de M et ses n dernières colonnes soient celles de I : $G = ((M)(I))$; il suffit ensuite, si c'est possible, d'appliquer à G les transformations élémentaires sur les lignes jusqu'à ce que ses n premières colonnes soient celles de I. Alors, si on a réussi à mener le procédé à terme, les n dernières colonnes de la nouvelle matrice sont celles de l'inverse de M : $((I)(M^{-1}))$.

On peut aussi construire une matrice G' telle que ses n premières lignes soient celles de M et ses n dernières lignes celles de I : $\begin{pmatrix}(M)\\(I)\end{pmatrix}$, et d'appliquer les transformations élémentaires sur les colonnes jusqu'à obtenir, si c'est possible, les lignes de I sur les n premières lignes ; alors les n dernières lignes sont celles de l'inverse de M : $\begin{pmatrix}(I)\\(M^{-1})\end{pmatrix}$.

- *Exemple* : Appliquer les deux procédés aux matrices $\begin{pmatrix}1&3&6\\1&4&7\\2&5&8\end{pmatrix}$ et $\begin{pmatrix}1&4&7\\2&5&8\\3&6&9\end{pmatrix}$. (L'une est inversible, pas l'autre).

- *Exemple de système* : Soit $M = \begin{pmatrix}1&3&6\\1&4&7\end{pmatrix}$, ce qu'on traduit par : $\begin{cases}x+3y=6\\x+4y=7\end{cases}$, ou : $\left|\begin{array}{cc|c}x&y&z\\\hline 1&3&6\\1&4&7\end{array}\right|$

On applique la transformation : $\{L_2 - L_1 \to L_2\}$, ce qui revient à multiplier M à gauche par $E_{2,1,-1}$.

$$E_{1,2,-1}\times M = \begin{pmatrix}1&3&6\\0&1&1\end{pmatrix} \text{ ou } \left|\begin{array}{cc|c}x&y&z\\\hline 1&3&6\\0&1&1\end{array}\right|.$$

On applique la transformation : $\{L_1 - 3.L_2 \to L_1\}$, ce qui revient à multiplier M à gauche par $E_{1,2,-3}$.

$$E_{1,2,-3}\times E_{2,1,-1}\times M = \begin{pmatrix}1&0&3\\0&1&1\end{pmatrix} \text{ ou } \left|\begin{array}{cc|c}x&y&z\\\hline 1&0&3\\0&1&1\end{array}\right|.$$

• Dans le cas où M n'est pas inversible, on peut pousser le processus jusqu'à obtenir une matrice de projecteur exprimée dans sa base et de rang le même rang que M, ce qui veut dire qu'on a le début de l'identité jusqu'à $rg(M)$ lignes, les lignes suivantes étant nulles. Une matrice non inversible est donc équivalente à la matrice d'un projecteur de même rang. On appelle ce procédé : mise sous forme canonique ; il en ressort que toute matrice inversible est un produit de transformations élémentaires et équivalente à l'identité, tandis que toute matrice non inversible est équivalente à une matrice de projecteur.

- *Preuve* : C'est immédiat avec le lemme 2 car, en notant K la matrice produit des différentes transformations élémentaires permettant de passer de $((M)(I))$ à $((I)(N))$, en supposant que la matrice soit inversible, alors : $K.((M)(I)) = ((K.M)(K)) = ((I)(N)) \Rightarrow K.M = I$ et $N = K$ d'où $N = K = M^{-1}$.

Si M n'est pas inversible, on considère M comme la matrice, donnée dans les bases canoniques, d'une application linéaire $f : E \to F$. Soit alors $E_2 = Ker(f)$ et E_1 un supplémentaire de $Ker(f)$ dont on sait qu'il est isomorphe à $Im(f)$; on peut choisir pour cet isomorphisme la restriction de f à F_1 car u se décompose de manière unique dans $F_1{\times}F_2$: $u = u_1 + u_2$, avec $f(u) = f(u_1) + f(u_2) = f(u_1)$. On note ϕ cette restriction ; $\phi : F \to Im(f)$ a donc pour matrice une matrice carrée inversible. La matrice M est équivalente à la matrice M' de f donnée dans la réunion des bases de F_1 et F_2, d'où : $M' = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right)$, où A est la matrice de ϕ donnée dans la base F_1. Il s'en suit que A est semblable à l'identité, d'où le résultat.

C'est la même démonstration pour les opérations sur les colonnes.

Résumé :

On applique des transformations élémentaires à $\boxed{M|I}$ jusqu'à arriver à $\boxed{I|M^{-1}}$.

(On appelle *transformations élémentaires* : Échanger deux lignes, multiplier une ligne par un scalaire non nul, additionner à une ligne une autre ligne préalablement multipliée par un scalaire (ou une combinaison linéaire des autres lignes)).

S'il est impossible de terminer le processus alors la matrice n'est pas inversible ; le nombre de lignes non nulles de la matrice finale est ainsi égal au rang de la matrice initiale.

- *Remarque* : On peut aussi utiliser la méthode du pivot de Gauss pour résoudre des systèmes, ou pour trouver le noyau et l'image d'une application linéaire.

• Si la dimension de la matrice n est paire, il est possible d'obtenir $-I$ comme le carré d'une composée de transformations élémentaires. Il suffit de l'établir pour $n = 2$ et de traiter ensuite les éléments de la diagonale de I deux par deux :

$$-I_2 = (E_{2,1,1}.E_{1,2,-1}.E_{2,1,1})^2 = (E_{1,2,1}.E_{2,1,-1}.E_{1,2,1})^2.$$

- *Produit partiel* : Soit $M = (a_{i,k})_{\substack{1 \le i \le n \\ 1 \le k \le m}}$, $N = (b_{k,j})_{\substack{1 \le k \le m \\ 1 \le j \le p}}$ et $M.N = (c_{i,j})_{\substack{1 \le i \le n, \\ 1 \le j \le p}}$ avec pour tout couple (i, j) convenable : $c_{i,j} = \sum_{k=1}^{m} a_{i,k}.b_{k,j}$. Alors, les lignes h à h' de M multipliée par les colonnes q à q' de N donnent la sous-matrice de $M.N$: $(a_{i,k})_{\substack{h \le i \le h' \\ 1 \le k \le m}}.(b_{k,j})_{\substack{1 \le k \le m \\ q \le j \le q'}} = (c_{i,j})_{\substack{h \le i \le h' \\ q \le j \le q'}}$ (en remarquant qu'on est obligé de multiplier des lignes complètes de M par des colonnes complètes de N).

$$\begin{pmatrix} a_{11} & \cdots & \cdots & \cdots & \cdots & \cdots & a_{1m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{a_{h1}} & \cdots & \cdots & \cdots & \cdots & \cdots & \mathbf{a_{hm}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{a_{h'1}} & \cdots & \cdots & \cdots & \cdots & \cdots & \mathbf{a_{h'm}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & \cdots & \cdots & \cdots & \cdots & a_{nm} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & \mathbf{b_{1q}} & \cdots & \mathbf{b_{1q'}} & \cdots & b_{1p} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{m1} & \cdots & \mathbf{b_{mq}} & \cdots & \mathbf{b_{mq'}} & \cdots & b_{mp} \end{pmatrix} = \begin{pmatrix} c_{11} & \cdots & c_{1q} & \cdots & c_{1q'} & \cdots & c_{1p} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{h1} & \cdots & \mathbf{c_{hq}} & \cdots & \mathbf{c_{hq'}} & \cdots & c_{hp} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{h'1} & \cdots & \mathbf{c_{h'q}} & \cdots & \mathbf{c_{h'q'}} & \cdots & c_{h'p} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{n1} & \cdots & c_{nq} & \cdots & c_{nq'} & \cdots & c_{np} \end{pmatrix}.$$

- *Produit par blocs* : Lorsque les produits de matrices $M.N$ et $M.N'$ sont possibles et que N et N' ont le même nombre de lignes, en notant $((N)(N'))$ la matrice formée de deux sous-matrices contiguës dont l'une vaut N et l'autre N', alors : $M.((N)(N')) = ((M.N)(M.N'))$.

De même dans l'autre sens : si les produit M.N et M'.N sont possibles et que M et M' ont le même nombre de colonnes, en notant $\begin{pmatrix}(M)\\(M')\end{pmatrix}$ la matrice formée de deux sous-matrices verticalement contiguës dont l'une vaut M et l'autre vaut M', alors : $\begin{pmatrix}(M)\\(M')\end{pmatrix}.N = \begin{pmatrix}(M.N)\\(M'.N)\end{pmatrix}$. (Corollaire du produit partiel).

De même : $\begin{pmatrix}(M)\\(M')\end{pmatrix}.((N)(N')) = \begin{pmatrix}(MN) & (MN')\\(M'N) & (M'N')\end{pmatrix}$; $\begin{pmatrix}(A) & (C)\\(B) & (D)\end{pmatrix}\begin{pmatrix}(A') & (C')\\(B') & (D')\end{pmatrix} = \begin{pmatrix}(AA' + CB') & (AC' + CD')\\(BA' + DB') & (BC' + DD')\end{pmatrix}$.

(Les matrice A, B, C, D sont des matrices carrées de même ordre. En pratique on peut se passer d'écrire les parenthèses internes).

• Dans chacun des cas, les dimensions des matrices doivent vérifier certaines contraintes. Par exemple le dernier produit :

	m_1 m_2	p_1 p_2			p_1 p_2	
n_1 n_2	$\begin{pmatrix}(A) & (C)\\(B) & (D)\end{pmatrix}$	$\begin{pmatrix}(A') & (C')\\(B') & (D')\end{pmatrix}$	m_1 m_2	=	$\begin{pmatrix}(AA' + CB') & (AC' + CD')\\(BA' + DB') & (BC' + DD')\end{pmatrix}$	n_1 n_2

15) <u>Résolution de (f(u) = v), application aux équations de sous-espaces vectoriels et aux systèmes linéaires</u>.

Soit $f \in \mathscr{L}(E, F)$.

- *Résolution* : Si $v \notin Im(f)$ il n'y a pas de solution. Si $v \in Im(f)$, soit u_p une solution particulière de cette équation. Alors $f(u - u_p) = 0_F$, et alors $u = u_0 + u_p$ où u_0 décrit Ker(f). L'ensemble des solutions peut être noté : $u_p + Ker(f)$. On peut aussi dire que :

La [***solution générale avec second membre***] est [***égale***] à la somme de la [***solution générale sans second membre***] [***plus***] une [***solution particulière avec second membre***].

- Équations cartésiennes des sous-espaces vectoriels.

- *Cas des hyperplans* : L'image d'une forme linéaire non nulle est le corps des scalaire, de dimension 1 ; il s'en suit que le noyau d'une forme linéaire non nulle est un hyperplan. Réciproquement, tout hyperplan peut être donné comme le noyau d'une forme linéaire.

Étant donnée une base canonique $B = (e_1, e_2, ..., e_n)$ et $u = x_1.e_1 + x_2.e_2 + ... + x_n.e_n$, soit alors $a_i = f(e_i)$ pour tout i ; l'image de u est donnée par : $f(u) = a_1.x_1 + a_2.x_2 + ... + a_n.x_n \in \mathbb{K}$. Le noyau est alors l'ensemble des vecteurs $u \in E$ tels que : $a_1.x_1 + a_2.x_2 + ... + a_n.x_n = 0$.

On peut à partir de cette équation trouver une base de l'hyperplan car au moins l'un des a_n n'est pas nul. On suppose que c'est a_n, mais le principe serait le même avec n'importe quel autre coefficient :

$(e_1 - (a_1/a_n).e_n, e_2 - (a_2/a_n).e_n, ..., e_{n-1} - (a_{n-1}/a_n).e_n)$ est une base de H.

Réciproquement, tout hyperplan H possède un supplémentaire D : une droite dirigée par n'importe quel vecteur non nul n'appartenant pas à H ; soit w un tel vecteur. Tous les vecteurs, en particuliers ceux de B, possèdent une décomposition unique dans H et D : $\forall e_i \in B$, $\exists! (e_i', e_i'') \in H\times D$ tels que $e_i = e_i' + e_i''$. Soit alors f définie, pour tout i, par $f(e_i') = 0$ et $f(e_i'') = f(a_i.w) = a_i.f(w)$; son noyau est H, et on a bien :

$u \in H \Leftrightarrow a_1.x_1 + a_2.x_2 + ... + a_n.x_n = 0$ (en divisant par f(w) qui n'est pas nul).
$u \in H \Leftrightarrow {}^t a.u = 0$, pour $a = a_1.e_1 + a_2.e_2 + ... + a_n.e_n$.

- *Généralisation* : Étant donné un espace vectoriel E de dimension finie : n, et F un sous-espace vectoriel tel que dim(F) = p, il existe une application linéaire $f \in \mathscr{L}(E, \mathbb{K}^{n-p})$ telle que : F = Ker(f).

- *Preuve* : Il existe un supplémentaire F' de dimension (n - p) de F et un isomorphisme ϕ de F' dans $\mathbb{K}^{n-p}$. Tout vecteur possède une décomposition unique dans F et F' ; il suffit alors, pour $v = u + u'$ où $u \in F$ et $u' \in F'$, de poser : $f(u) = 0$ et $f(v) = f(u') = \phi(u') \in \mathbb{K}^{n-p}$.

• On en conclut que tout sous-espace vectoriel de E peut être donné par un système de (n - p) équations linéaires dans la base canonique. Soit $B = (e_1, e_2, ..., e_n)$ la base canonique et $C = (u_1, u_2, ..., u_{n-p})$ une base de F' ; alors :

$\forall\ e_i \in B$, $\exists!\ (e_i', e_i'') \in F\times F'$ tels que $e_i = e_i' + e_i''$, où $e_i'' = a_{i,1}.u_1 + a_{i,2}.u_2 + ... + a_{i,n-p}.u_{n-p}$. On choisit ensuite l'application linéaire f, nulle sur F, telle que $f(u_j)$ soit le j-ième vecteur de la base canonique de $\mathbb{K}^{n-p}$. Ainsi :

$$f(e_i) = \begin{pmatrix} a_{i,1} \\ a_{i,2} \\ ... \\ a_{i,n-p} \end{pmatrix}, \text{ et } f(x_1.e_1 + x_2.e_2 + ... + x_n.e_n) = x_1.\begin{pmatrix} a_{1,1} \\ a_{1,2} \\ ... \\ a_{1,n-p} \end{pmatrix} + x_2.\begin{pmatrix} a_{2,1} \\ a_{2,2} \\ ... \\ a_{2,n-p} \end{pmatrix} + ... + x_n.\begin{pmatrix} a_{n,1} \\ a_{n,2} \\ ... \\ a_{n,n-p} \end{pmatrix} = \begin{pmatrix} a_{1,1}x_1 + a_{2,1}x_2 + ... + a_{n,1}x_n \\ a_{1,2}x_1 + a_{2,2}x_2 + ... + a_{n,2}x_n \\ ... \\ a_{1,n-p}x_1 + a_{2,n-p}x_2 + ... + a_{n,n-p}x_n \end{pmatrix}.$$

$$\text{Alors : } f(u) = \vec{0} \Leftrightarrow u \in F \Leftrightarrow \begin{cases} a_{1,1}x_1 + a_{2,1}x_2 + ... + a_{n,1}x_n = 0 \\ a_{1,2}x_1 + a_{2,2}x_2 + ... + a_{n,2}x_n = 0 \\ ... \\ a_{1,n-p}x_1 + a_{2,n-p}x_2 + ... + a_{n,n-p}x_n = 0 \end{cases}$$

Ce système d'équations est appelé la représentation cartésienne de F dans la base B. Et on remarque que, dans le cas général d'un sous-espace vectoriel F de E : **[Nombre d'équations indépendantes] = dim(E) - dim(F)**.

Soit M la matrice de l'endomorphisme f dans la base canonique, U et V les matrices colonnes des vecteurs u et v dans cette même base. On peut alors résoudre $f(u) = v$ par la méthode du pivot de Gauss.

Si M est inversible, on applique des transformations élémentaires à $\boxed{M|V}$ jusqu'à arriver à $\boxed{I|M^{-1}V}$. Si c'est impossible on arrive à $\boxed{u = u_0 + \mathrm{Ker}(f)}$ où u_0 est une solution particulière de l'équation.

- *Remarques* : L'application f ainsi construite admet pour applications coordonnées des formes linéaires f_i,

$$f = \begin{pmatrix} f_1 \\ f_2 \\ ... \\ f_{n-p} \end{pmatrix}, \text{ avec : } F = \mathrm{Ker}(f) = \mathrm{Ker}(f_1)\cap\mathrm{Ker}(f_2)\cap...\cap\mathrm{Ker}(f_{n-p}).$$

Mais on peut aussi construire f comme un projecteur de $\mathscr{L}(E)$ admettant F pour noyau et un supplémentaire quelconque de F pour image.

- <u>Application aux équations linéaires</u>.

a) *Définition* : E et F étant des espaces vectoriels de dimensions finies, munis des bases respectives B et C, ainsi que $f \in \mathscr{L}(E, F)$ de matrice M dans les bases respectives B et C, un système d'équation linéaire est donné par : $f(u) = v$ où v est une vecteur donné de F et où u est l'inconnue à déterminer. Cette équation se ramène donc effectivement à un système de $\dim(F)$ équations à $\dim(E)$ inconnues (les composantes de u) donné par :

$$M.u_B = v_C.$$

b) *Cas particulier* : On appelle *équation homogène*, l'équation $f(u) = 0_F$; il est donc clair que son ensemble de solution est $\mathrm{Ker}(f)$.

c) *Équation avec second membre* : Si u_0 est une solution particulière, soit u' tel que $u = u_0 + u'$; alors : $f(u_0 + u') = v \Leftrightarrow f(u_0) + f(u') = v \Leftrightarrow f(u') = 0_F \Leftrightarrow u = u_0 + u'$ avec $u' \in \mathrm{Ker}(f)$ quelconque.

- *Remarque* : Il ne peut y avoir de solution particulière que dans le cas où $v \in \mathrm{Im}(f)$; dans le cas contraire l'équation n'admet pas de solution.

d) *Linéarité* : Si α est un scalaire non nul et que u_1 est la solution générale de l'équation : $f(u) = v$, alors $\alpha.u_1$ est la solution générale de l'équation : $f(u) = \alpha.v$. Dans le cas particulier $\alpha = 0$, on se réfère à une proposition précédente ; dans le cas contraire on retrouve la solution à $\mathrm{Ker}(f)$ près car : Si $\alpha \neq 0$, on obtient ainsi $u \in \mathrm{Ker}(f) \Leftrightarrow \alpha.u \in \mathrm{Ker}(f)$.

- *Somme* : Si u_1 est la solution générale de l'équation : $f(u) = v_1$, et que u_2 est la solution générale de l'équation : $f(u) = v_2$, alors $u_1 + u_2$ est la solution générale de l'équation : $f(u) = v_1 + v_2$.

- *Preuve* : Il est évident que $u_1 + u_2$ est solution de cette équation ; comme u_1 est de la forme $u_{1,0} + u_1'$ où $u_{1,0}$ est une solution particulière de l'équation : $f(u) = v_1$, et u_1' un vecteur quelconque de Ker(f), et que u_2 est de la forme $u_{2,0} + u_2'$ où $u_{2,0}$ est une solution particulière de l'équation : $f(u) = v_2$, et u_2' un vecteur quelconque de Ker(f), alors $u_1 + u_2 = (u_{1,0} + u_{2,0}) + (u_1' + u_2')$. Il est ensuite clair que $(u_{1,0} + u_{2,0})$ est une solution particulière de l'équation : $f(u) = v_1 + v_2$, et que $(u_1' + u_2')$ décrit tout l'ensemble Ker(f), d'où la proposition.

- *Conclusion* : Soit α et β des scalaires, v_1 et v_2 des vecteurs tels que $\alpha.v_1 + \beta.v_2 \neq 0_F$; si u_1 est la solution générale de l'équation : $f(u) = v_1$, et que u_2 est la solution générale de l'équation : $f(u) = v_2$, alors : $\alpha.u_1 + \beta.u_2$ est la solution générale de l'équation : $f(u) = \alpha.v_1 + \beta.v_2$.

e) *Proposition* : Lorsqu'on multiplie un système linéaire d'équations par une matrice inversible, on obtient un système équivalent (admettant les mêmes solutions).

- *Preuve* : Si u est tel que $M.u = v$ (en assimilant les vecteurs et leurs composantes dans la base canonique), et P une matrice inversible, il est alors évident que $P.M.u = P.v$; à l'inverse, si u est tel que $P.M.u = P.V$ alors, en multipliant par P^{-1} : $M.u = v$, d'où la proposition.

f) *Méthode du pivot de Gauss* : On peut donc appliquer au système des transformations élémentaires, mais uniquement sur les lignes. Autrement dit on ne pourra réaliser la mise sous forme canonique jusqu'au bout que si M est inversible. Dans le cas où M n'est pas inversible, on peut obtenir une forme *minimale* équivalente à la matrice M :

$$M' = \left(\begin{array}{c|c} I_p & B \\ \hline 0 & 0 \end{array}\right),$$ où I_p est la matrice identité d'ordre : rg(M) (le rang de la matrice est aussi le rang du système).

- *Remarque* : Il n'y a pas toujours de lignes de zéros, par exemple s'il y a au départ plus d'inconnues que d'équations.

Soit K la matrice inversible des successions de transformations élémentaires permettant de passer de M à M' ; alors : $K.((M)(v)) = ((K.M)(K.v))$ permet de résoudre le système.

En particulier, si M inversible alors : $K = M^{-1}$, et : $u = M^{-1}.v = K.v$.

g) *Cas où M n'est pas inversible* : On peut dans ce cas, sous la forme finale, exprimer certaines des inconnues en fonction des autres qui servent alors de paramètres. En utilisant le principe de résolution sans second membre, s'il existe une solution particulière u_0 du système avec second membre, et U le sous-espace vectoriel défini par le système d'équations : $M.u = 0$, ou plutôt : $K.M.u = 0$, alors l'ensemble des solutions du système est : $u_0 + U$.

Il peut aussi apparaître de façon évidente que u_0 n'existe pas ; il n'y a dans ce cas pas de solution.

h) *Système linéaire sur-déterminé* (ou surdéterminé) : Se dit d'un système ayant plus d'équations que d'inconnues (on dit aussi que la matrice est *rectangulaire debout*). Pour la résolution analytique, il faut isoler un nombre d'équations égal au nombre d'inconnues, si possible linéairement indépendantes, et d'injecter la solution obtenue dans les dernières équations pour voir s'il y a compatibilité.

i) *Exemples* : Résoudre les systèmes $\begin{cases} x + 2y + 3z = 2 \\ 4x + 5y + 6z = 5 \\ 7x + 8y + 9z = 8 \end{cases}$, et $\begin{cases} x + 2y + 3z = 2 \\ 4x + 5y + 6z = 5 \\ 7x + 8y + 8z = 8 \end{cases}$.

En écrivant le premier système sous la forme $AX = B$, le premier tableau de pivot est (A B) et le dernier :

$$E_{1,2,-2}D_{2,-3}E_{3,2,-2}E_{2,1,-4}E_{3,1,-7}(A\ \ B).$$

16) Applications bilinéaires, formes bilinéaires.

E_1, E_2 et F étant des espaces vectoriels, $\phi : E_1 \times E_2 \to F$ est **bilinéaire** si pour tout vecteur u_1 de E_1 et tout vecteur u_2 de E_2, les applications $\phi_1 : E_1 \to F$ et $\phi_2 : E_2 \to F$ définies par $\phi_1(u) = \phi(u, u_2)$ et $\phi_2(u) = \phi(u_1, u)$ sont linéaires. Les applications ϕ_1 et ϕ_2 sont appelées applications *partielles* de f.

Ça signifie que : $\forall \alpha \in \mathbb{K}$ et $\forall (u_1, u'_1, u_2, u'_2) \in E_1^2 \times E_2^2$, alors :

$\phi(\alpha.u_1, u_2) = \phi(u_1, \alpha.u_2) = \alpha.\phi(u_1, u_2)$, $\phi(u_1 + u'_1, u_2) = \phi(u_1, u_2) + \phi(u'_1, u_2)$, $\phi(u_1, u_2 + u'_2) = \phi(u_1, u_2) + \phi(u_1, u'_2)$.

Lorsque $E_1 = E_2$, on note plus simplement E.

- *Remarque* : ϕ bilinéaire $\Rightarrow$ $\phi(0_{E_1}, u_2) = \phi(u_1, 0_{E_2}) = 0_F$.

ϕ est **symétrique** si $E = E_1 = E_2$ et pour tout couple (u, v) de vecteurs de E :

$\phi(v, u) = \phi(u, v)$.

ϕ est **antisymétrique** si $E = E_1 = E_2$ et pour tout couple (u, v) de vecteurs de E :

$\phi(v, u) = -\phi(u, v)$ (alors, pour tout vecteur u de E : $\phi(u, u) = 0_F$).

ϕ est **alternée** si $E = E_1 = E_2$ et pour tout vecteur u de E : $\phi(u, u) = 0$.

- *Proposition* : ϕ alternée $\Leftrightarrow$ ϕ antisymétrique.

- *Preuve* : Si ϕ est antisymétrique, alors $\phi(u, u) = -\phi(u, u) = 0$. Si ϕ est alternée, alors $\phi(u+v, u+v) = 0$; en développant : $\phi(u+v, u+v) = \phi(u, u) + \phi(u, v) + \phi(v, u) + \phi(v, v) = \phi(u, v) + \phi(v, u) = 0$.

- *Exemples* : Le produit vectoriel est une application bilinéaire antisymétrique, le produit externe est une application bilinéaire, pas la somme vectorielle.

- *Remarque* : Lorsque ϕ est symétrique ou antisymétrique, la linéarité à gauche (ou à droite) implique la bilinéarité.

Lorsque l'ensemble d'arrivée est $\mathbb{K}$, ϕ est une *forme bilinéaire*. Une forme bilinéaire antisymétrique est aussi appelée : forme bilinéaire *alternée*.

ϕ forme bilinéaire $\Leftrightarrow$ les applications ϕ_1 et ϕ_2 sont des formes linéaires.

Une forme bilinéaire symétrique est ***positive*** si pour tout vecteur u de E : $\phi(u, u) \geq 0$ (ce qui implique que c'est un réel, $\mathbb{K} = \mathbb{R}$) ; elle est ***définie*** si $(\phi(u, u) = 0 \Leftrightarrow u = 0_E)$.

Une forme bilinéaire est ***non dégénérée*** si les deux applications linéaires associées (partielles) sont injectives. Elle est *dégénérée* si :

$$(\exists\, u \in E,\ \forall\, v \in E,\ \phi(u, v) = 0) \text{ ou } (\exists\, w \in E,\ \forall\, v \in E,\ \phi(v, w) = 0).$$

ϕ est non dégénérée si et seulement si :

$$[(\forall\, u \in E,\ \phi(u, w) = 0) \Rightarrow w = 0_E] \text{ et } [(\forall\, u \in E,\ \phi(w, u) = 0) \Rightarrow w = 0_E]$$

En particulier, une forme bilinéaire symétrique *définie* est non dégénérée (car pour $u = w$ on obtient $w = 0_E$) ; réciproquement, une forme bilinéaire symétrique positive non dégénérée est définie (car si $\phi(w, w) = 0$, $[\forall \lambda \text{ et } u,\ \phi(\lambda.w + u, \lambda.w + u) \geq 0] \Rightarrow w = 0_E$).

Une forme bilinéaire symétrique définie positive est un produit scalaire.

- *Composition* : Pour les ensembles de départs et d'arrivées convenables, si ϕ est bilinéaire, f et g linéaires alors $f_o\phi$ est bilinéaire et $(u, v) \mapsto \phi(f(u), g(v))$ aussi.

Par contre, si $\psi: D \to E_1 \times E_2$ est linéaire, il n'en est pas de même de $\phi_o\psi$. Par exemple, soit $E = \mathbb{R}^3$, $\psi: \mathbb{R} \to E^2$ définie par $\psi(t) = (\begin{pmatrix} t \\ 2t \\ 3t \end{pmatrix}, \begin{pmatrix} -t \\ 0 \\ t \end{pmatrix})$, et ϕ le produit vectoriel ; alors : $\phi_o\psi(t) = \begin{pmatrix} t \\ 2t \\ 3t \end{pmatrix} \wedge \begin{pmatrix} -t \\ 0 \\ t \end{pmatrix} = \begin{pmatrix} 2t^2 \\ -4t^2 \\ 2t^2 \end{pmatrix}$.

17) Matrice d'une forme bilinéaire.

Soit B_1, B_2 les bases canoniques respectives de E_1, E_2, et ϕ une forme bilinéaire. Il existe alors une matrice M telle que, en assimilant u_1, u_2 et $v = \phi(u_1, u_2)$ à leurs composantes dans ces bases, on a : $\boxed{v = {}^t u_1.M.u_2}$.

Si $E = E_1 = E_2$ et $B = (e_1, e_2, ..., e_n)$: $M = \begin{pmatrix} \phi(e_1, e_1) & \phi(e_1, e_2) & ... & \phi(e_1, e_n) \\ \phi(e_2, e_1) & \phi(e_2, e_2) & ... & \phi(e_2, e_n) \\ ... & ... & ... & ... \\ \phi(e_n, e_1) & \phi(e_n, e_2) & ... & \phi(e_n, e_n) \end{pmatrix}$ (matrice de Gram).

Dans ce dernier cas, si ϕ est symétrique alors M est symétrique et si ϕ est antisymétrique (alternée) alors M est antisymétrique.

- *Preuve* : Comme, pour tout couple de vecteurs (u, v), on doit avoir $\phi(u, v) = \phi(v, u)$; alors, en assimilant les vecteurs à leurs composantes dans la base canonique, si ϕ est une forme bilinéaire symétrique on a : ${}^tu.M.v = {}^tv.M.u = {}^t({}^tu.{}^tM.v)$; d'où, comme un scalaire est égal à sa transposée : ${}^tu.M.v = {}^tu.{}^tM.v$. Cette égalité étant vraie pour tous les couples de vecteurs, elle implique ${}^tM = M$; et alors M est une matrice symétrique. En procédant de même pour une forme bilinéaire antisymétrique : ${}^tu.M.v = -{}^tv.M.u = -{}^t({}^tu.{}^tM.v) = {}^tu.{}^tM.v = -{}^tu.{}^tM.v$; d'où pour tout couple de vecteurs : ${}^tu.(-M).v = {}^tu.{}^tM.v$, ce qui implique : ${}^tM = -M$, et alors M est une matrice antisymétrique.

- *Exemple* : $(x_1\ x_2\ x_3).\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1y_1 + 4x_1y_2 + 2x_2y_1 + 5x_2y_2 + 3x_3y_1 + 6x_3y_2$.

- *Remarque* : M antisymétrique $\Leftrightarrow$ $(\forall X \in \mathbb{R}^n,\ {}^tXMX = \Theta)$ ($(E_1, ..., E_n)$ étant la base de $\mathbb{R}^n$, on pose $X = E_i + E_j$). (Ou bien il suffit de remarquer que c'est dû au fait que la forme bilinéaire associée est alternée).

- *Proposition* : (En dimension finie) ϕ est une forme bilinéaire si et seulement s'il existe une matrice carrée M et une base B telles que pour tout couple de vecteurs (u, v), $f(u, v) = {}^tu_BMv_B$. En outre, si M est antisymétrique alors f aussi, et si M est symétrique, alors f aussi.

- *Corollaire* : (En dimension finie) ϕ est une forme bilinéaire si et seulement s'il existe une base B et des coefficients $(a_{i,j})$ tels que pour tout couple de vecteurs (u, v), $u:(x_1, x_2, ..., x_n)_B$, $v:(y_1, y_2, ..., y_n)_B$, et :

$$\phi(u, v) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j}x_iy_j.$$

Si pour tout i, j : $a_{j,i} = a_{i,j}$ alors ϕ est symétrique, et si pour tout i, j : $a_{j,i} = -a_{i,j}$ alors ϕ est antisymétrique.

Si ϕ est symétrique, alors : $\phi(u, u) = \sum_{i=1}^{n} a_{i,i}x_i^2 + 2.\sum_{1\le i<j\le n} a_{i,j}x_ix_j$.

Formule de changement de base : Si P est la matrice de passage de la base B' donnée dans la base B, alors : $\boxed{M' = {}^tPMP}$ (où M et M' sont les matrices respectives de ϕ dans B et dans B').

- *Remarque* : Il existe des matrices appelées *matrices orthogonales* telles que ${}^tP = P^{-1}$; exclusivement dans ce cas la formule de changement de base de l'endomorphisme de matrice M et la formule de changement de base de la forme bilinéaire de matrice M coïncident. (Cf. §13).

- *Proposition* : Toute forme bilinéaire alternée du plan est égale au produit du déterminant par une constante non nulle. De même, soit E l'espace ordinaire muni de sa base canonique (e_1, e_2, e_3), toute application bilinéaire antisymétrique de E^2 sur E est complètement déterminée par : $\phi(e_1, e_2)$, $\phi(e_2, e_3)$ et $\phi(e_3, e_1)$. Cette détermination est unique si, en plus : $(\phi(e_1, e_2), \phi(e_2, e_3), \phi(e_3, e_1))$ est une famille libre. Il s'en suit que le produit vectoriel est la seule application bilinéaire antisymétrique de E^2 sur E telle que : $\phi(e_1, e_2) = e_3$, $\phi(e_2, e_3) = e_1$ et $\phi(e_3, e_1) = e_2$.

- *Preuve* : C'est immédiat pour le déterminant car : $\phi(u, v) = (x_1\ \ x_2)\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}.\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = a(x_1 y_2 - x_2y_1) = a.\det(u, v)$.

Soit ϕ une application bilinéaire antisymétrique de l'espace ordinaire ; en appliquant ses propriétés on arrive à :

$\phi(x_1.e_1 + x_2.e_2 + x_3.e_3, y_1.e_1 + y_2.e_2 + y_3.e_3) = (x_1y_2 - x_2y_1).\phi(e_1, e_2) - (x_1y_3 - x_3y_1).\phi(e_3, e_1) + (x_2y_3 - x_3y_2).\phi(e_2, e_3)$, d'où la proposition.

- *Proposition* : Soit ϕ une forme bilinéaire symétrique du plan de matrice M dans une base B donnée. Alors ϕ est positive si et seulement si $\det(M) \geq 0$, et ϕ est définie positive si et seulement si $\det(M) > 0$.

- *Preuve* : $\phi(u, u) = (x_1\ \ x_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}.\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = ax_1^2 + 2bx_1x_2 + cx_2^2$; or, le discriminant réduit vaut $-\det(M)$, la fin est donc immédiate.

18) <u>Propriétés de la trace d'une matrice</u>.

Si M est une matrice carrée, sa trace : $Tr(M)$ désigne la somme des coefficients de la diagonale principale de M. Alors :

Transposition : $Tr({}^tA) = Tr(A)$.

Linéarité : $Tr(A + B) = Tr(A) + Tr(B)$; $Tr(\alpha.A) = \alpha.Tr(A)$ (où α est un scalaire).

Produit : $Tr(AB) = Tr(BA)$. *Conséquence* : A et B semblables $\Rightarrow$ $Tr(A) = Tr(B)$.

$(A, B) \mapsto Tr({}^tA.B)$ est une forme bilinéaire symétrique définie positive (produit scalaire).

La trace d'un projecteur est égale à son rang.

Si A est une matrice de trace non nulle, alors $M \in Vect(A) \Leftrightarrow M = \frac{Tr(M)}{Tr(A)}.A$.

Si M est une matrice à coefficients complexes : $Tr(\overline{M}) = \overline{Tr(M)}$ ($\overline{M}$ est la matrice des conjugués).

- *Preuves* : *Linéarité*. Si $A = (a_{ij})$ et $B = (b_{ij})$, alors $\alpha.A = (\alpha a_{ij})$ et $A + B = (a_{ij} + b_{ij})$, ce qui rend la linéarité évidente.
Produit : $AB = (c_{ij})$ et $BA = (d_{ij})$, avec $c_{ij} = (\sum_k a_{ik}b_{kj})$ et $d = (\sum_k b_{ik}a_{kj})$. Il s'en suit que $tr(AB) = \sum_i\sum_k a_{ik}b_{ki}$, et $tr(BA) = \sum_i\sum_k b_{ik}a_{ki}$, expressions qui sont évidemment égales. Par conséquent, s'il existe P inversible telle que $B = P^{-1}AP$ alors : $tr((P^{-1}A)P) = tr(P(P^{-1}A)) = tr(A)$.
Paramétrage de droite : $M \in Vect(A) \Rightarrow \exists\, k \in \mathbb{K}$ tel que $M = k.A$, donc : $tr(M) = k.tr(A)$, d'où : $k = tr(M)/tr(A)$.
Conjugué : La propriété vient du fait que les conjugués d'une somme et d'un produit sont respectivement la somme et le produit des conjugués.

- *Exemple* : Montrer que $AB - BA = kI \Leftrightarrow k = 0$ ($AB - BA$ = crochet de Lie de A et B).

(*Réponse* : $Tr(AB - BA) = 0 = Tr(kI) = kn$).

• *Propriété de la transposée* : ${}^{tt}A = A$, ${}^t(A + B) = {}^tA + {}^tB$, ${}^t(\alpha.A) = \alpha.{}^tA$, ${}^t(AB) = {}^tB{}^tA$.

19) <u>Matrice d'un projecteur de $\mathbb{R}^3$</u> (*hors programme*) : Soit (u_1, u_2, u_3) une base dont les vecteurs sont donnés respectivement dans la base canonique par les vecteurs colonnes U_1, U_2, U_3. La matrice M dans la base canonique de la projection p_1 sur $\mathrm{Vect}(u_1)$ parallèlement à $\mathrm{Vect}(u_2, u_3)$ est :

$$M_1 = \frac{U_1\times{}^t(U_2\wedge U_3)}{{}^tU_1\times(U_2\wedge U_3)},$$ (en notant que le produit vectoriel peut être défini sans connaissance du produit scalaire),

avec en outre : ${}^t(U_2\wedge U_3)\times U_1 = \det(U_1, U_2, U_3)$.

Alors la matrice de p_2 la projection sur $\mathrm{Vect}(u_2)$ parallèlement à $\mathrm{Vect}(u_1, u_3)$ est : $M_2 = \frac{U_2\times{}^t(U_3\wedge U_1)}{{}^tU_2\times(U_3\wedge U_1)}$, et celle de p_3 la projection sur $\mathrm{Vect}(u_3)$ parallèlement à $\mathrm{Vect}(u_1, u_2)$ est : $M_3 = \frac{U_3\times{}^t(U_1\wedge U_2)}{{}^tU_3\times(U_1\wedge U_2)}$; avec : $M_1 + M_2 + M_3 = I$.

($M_2 + M_3$ est donc, par exemple, la matrice de la projection sur $\mathrm{Vect}(u_2, u_3)$ parallèlement à $\mathrm{Vect}(u_1)$). On retrouve aussi la formule d'inversion des matrices 3×3 (avec ${}^tU_1\times(U_2\wedge U_3) = {}^tU_2\times(U_3\wedge U_1) = {}^tU_3\times(U_1\wedge U_2) = \det(U_1, U_2, U_3)$) :

$$U_1\times{}^t(U_2\wedge U_3) + U_2\times{}^t(U_3\wedge U_1) + U_3\times{}^t(U_1\wedge U_2) = (U_1\ \ U_2\ \ U_3)\times{}^t(U_2\wedge U_3\ \ \ U_3\wedge U_1\ \ \ U_1\wedge U_2) = \det(U_1, U_2, U_3).I.$$

On peut généraliser ces formules à la dimension n, en notant $\mathrm{Co}(U_1)$ la matrice colonne des cofacteurs de U_1 (dans la matrice $(U_1\ \ U_2\ \ldots\ U_n)$), la matrice de p_1 est : $M_1 = \frac{U_1\times{}^t\mathrm{Co}(U_1)}{{}^tU_1\times\mathrm{Co}(U_1)}$, avec : ${}^tU_1\times\mathrm{Co}(U_1) = \det(U_1, U_2, \ldots, U_n)$. Etc..[xv]

20) <u>Matrices involutives réelles d'ordre trois</u> (*hors programme*).

Ce sont des matrices de symétries, pas forcément orthogonales. Donc, à part I et $-I$, il y a les symétries de direction une droite ou un plan qui se déduisent l'une de l'autre. Si $u:(a_1, a_2, a_3)$, $v:(b_1, b_2, b_3)$, $w:(c_1, c_2, c_3)$, tels que (u, v, w) soit une base, s la symétrie de direction u par rapport à $\mathrm{Vect}(v, w)$ et σ la symétrie de direction $\mathrm{Vect}(v, w)$ par rapport à $\mathrm{Vect}(u)$, alors, pour tout vecteur x : $x = s(x) + \sigma(x)$. Donc, si M est la matrice de S, la matrice de σ est $I - M$. Et si P est la matrice de la base (u, v, w), alors :

$M = P\begin{pmatrix}-1&0&0\\0&1&0\\0&0&1\end{pmatrix}P^{-1}$. On obtient ainsi : $M = I - 2U.{}^t(V\wedge W)$, où U, V, W sont les matrices colonnes des vecteurs u, v, w.

Et : $I - M = 2U.{}^t(V\wedge W)$.

Toutes les solutions sont de la forme $\pm P\begin{pmatrix}-1&0&0\\0&1&0\\0&0&1\end{pmatrix}P^{-1}$, ou $\pm I$.

- ***Proposition***. Toutes les matrices involutives réelles d'ordre 3 sont dans cette liste :

$$\pm\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad \pm\begin{pmatrix}1-ab&0&(2-ab)b\\abc&1&(ab-2)bc\\a&0&ab-1\end{pmatrix},\quad \pm\begin{pmatrix}1&0&0\\ad&abc-1&-ab\\acd&(abc-2)c&1-abc\end{pmatrix},\quad \pm\begin{pmatrix}a&1/d&b\\(1-a)(a+bcd+1)d&-a-bcd&-(a+bcd+1)bd\\(a-1)cd&c&bcd+1\end{pmatrix},$$

$$\pm\begin{pmatrix}1&0&0\\0&1&0\\a&b&-1\end{pmatrix},\quad \pm\begin{pmatrix}-1&0&b\\-2a&1&ab\\0&0&1\end{pmatrix}.$$

- *Preuve* : À part $\pm I$, on se limite aux matrices de trace 1 (l'autre cas est résolu en multipliant tous les résultats par -1).

En notant $P = \begin{pmatrix}a_1&b_1&c_1\\a_2&b_2&c_2\\a_3&b_3&c_3\end{pmatrix}$, alors : $\det(P) = \Delta = a_1(b_2c_3 - b_3c_2) + a_2(b_3c_1 - b_1c_3) + a_3(b_1c_2 - b_2c_1)$. On pose ensuite $a = 1 + 2a_1(b_3c_2 - b_2c_3)/\Delta$, $b = 2a_1(b_2c_1 - b_1c_2)/\Delta$, $c = 2a_3(b_1c_3 - b_3c_1)/\Delta$, et $e = 2a_1(b_1c_3 - b_3c_1)/\Delta$.

1. Si $e \neq 0$, en posant $d = 1/e$: $\begin{pmatrix}a&1/d&b\\(1-a)(a+bcd+1)d&-a-bcd&-(a+bcd+1)bd\\(a-1)cd&c&bcd+1\end{pmatrix} = P\begin{pmatrix}-1&0&0\\0&1&0\\0&0&1\end{pmatrix}P^{-1}$.

2. Si $e = 0$ alors $a_1 = 0$, ou $b_1c_3 - b_3c_1 = 0$, et d n'existe pas.

2.1. Si $a_1 = 0$: Alors $a = 1$, $b = 0$.

2.1.1. Si $a_2 = 0$: Alors $P\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2a_3(b_3c_2 - b_2c_3)/\Delta & c & -1 \end{pmatrix}$, qui du type de l'avant-dernière de la liste.

2.1.2. Si $a_2 \neq 0$: On pose $u = a_3/a_2$, $v = 2(b_2c_1 - b_1c_2)/\Delta$, $w = 2(b_3c_2 - b_2c_3)/\Delta$; alors :

$P\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ wa_2 & -1-uva_2 & va_2 \\ uwa_2 & (-2-uva_2)u & 1+uva_2 \end{pmatrix}$, qui est du type de la troisième matrice de la liste.

2.2. Si $a_1 \neq 0$: Alors $b_1c_3 - b_3c_1 = 0$, $c = 0$.

2.2.1. Si $a_3 = 0$: $P\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1} = \begin{pmatrix} -1 & 0 & b \\ -2a_2/a_1 & 1 & ba_2/a_1 \\ 0 & 0 & 1 \end{pmatrix}$, qui du type de la dernière de la liste.

2.2.2. Si $a_3 \neq 0$: $P\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1} = \begin{pmatrix} a & 0 & -(a+1)a_1/a_3 \\ (a-1)a_2/a_1 & 1 & -(a+1)a_2/a_3 \\ (a-1)a_3/a_1 & 0 & -a \end{pmatrix}$; en notant $a' = (a - 1)a_3/a_1$, $b' = -a_1/a_3$, $c' = -a_2/a_1$, on obtient la deuxième matrice de la liste.

---

[i] L'addition doit être commutative, associative, posséder un élément neutre noté 0, et tout élément de l'ensemble doit posséder un opposé.

[ii] Un axiome est un énoncé dont on décide arbitrairement qu'il est vrai.

[iii] La démonstration de ce théorème en dimension infinie utilise l'axiome du choix qui, comme son nom l'indique, est supposé vrai sans qu'il soit possible de le démontrer (certains mathématiciens n'acceptent pas cet axiome). Une conséquence, entre autres, de ce théorème concernant le fait que $\mathbb{R}$ est un $\mathbb{Q}$-espace vectoriel, implique qu'il existe une famille de réels tel que tout réel s'exprime de manière unique comme combinaison linéaire finie (à coefficients rationnels) d'éléments de cette famille. Il est impossible de donner explicitement une telle famille. (On peut aussi se demander à quoi ressemblerait une base de l'ensemble des séries entières ? On affirme que ça existe, mais il est impossible d'en donner une explicitement).

[iv] En dimension infinie on utilise un équivalent de l'axiome du choix qui s'appelle : le lemme de Zorn, et qui permet d'affirmer l'existence de la partie maximale G_0 de G ; le reste de la démonstration est identique.

[v] Soit $(P_n)_{n\in\mathbb{N}}$ une famille de polynômes non nuls de degrés deux à deux distincts ; on l'ordonne par degrés croissants, pour tout entier naturel n : $d°(P_n) < d°(P_{n+1})$. On démontre ensuite par récurrence que $(P_k)_{0 \le k \le n}$ est libre :

> Initialisation : $P_0 \neq \Theta$ donc (P_0) est libre.
>
> On suppose la propriété vraie jusqu'au rang n.
>
> Au rang $n + 1$: Comme $(P_k)_{0 \le k \le n}$ est libre, si on suppose que $(P_k)_{0 \le k \le n+1}$ est liée, alors $P_{n+1} \in \mathrm{Vect}((P_k)_{0 \le k \le n})$ d'après le corollaire du théorème d'échange. Or, il est impossible d'obtenir ainsi le terme de plus haut degré de P_{n+1}.

Il en résulte que la famille $(P_k)_{0 \le k \le n}$ est effectivement libre pour tout entier naturel n. Par suite, comme toute famille finie extraite de $(P_n)_{n\in\mathbb{N}}$ est libre, on en déduit que $(P_n)_{n\in\mathbb{N}}$ est libre.

Soit A une famille de polynômes telle que : $[\forall\, n \in \mathbb{N},\ \exists\, P \in A$ tel que $d°(P) = n]$, et $(P_n)_{n\in\mathbb{N}}$ la sous-famille de A vérifiant $d°(P_n) = n$. D'après la démonstration précédente c'est une famille libre. En outre, pour n fixé, $(P_k)_{0 \le k \le n}$ est génératrice de $\mathbb{K}_n[X]$, c'en est donc une base. Par suite : $(P_n)_{n\in\mathbb{N}} = (P_k)_{0 \le k \le n}$ est une base de $\mathbb{K}_n[X] = \bigcup_{n\in\mathbb{N}} \mathbb{K}[X]$. Les deux dernières propositions sont donc démontrées.

[vi] Soit U, V et W trois sous-espaces vectoriels de E, et $x \in (U\cap V) + (U\cap W)$; il existe alors $y \in U\cap V$ et $z \in U\cap W$ tels que $x = y + z$; mais comme $y \in U$ et $z \in U$, alors $x \in U$; en outre $y \in V$ et $z \in W$, donc $x \in V + W$ ce dont on déduit $x \in U\cap(V + W)$ et ainsi : $(U\cap V) + (U\cap W) \subset U\cap(V + W)$.

Réciproquement, soit $x \in U\cap(V + W)$, donc il existe $y \in V$ et $z \in W$ tels que $x = y + z$. Soit V' un supplémentaire de $U\cap V$ dans V, et W' un supplémentaire de $U\cap W$ dans W ; alors $y = y_1 + y_2$ avec $y_1 \in U\cap V$ et $y_2 \in V'$, tandis que $z = z_1 + z_2$ avec $z_1 \in U\cap W$ et $z_2 \in W'$. Ainsi : $x - y_1 - z_1 \in U$ et $x - y_1 - z_1 = y_2 + z_2 \in V' + W'$; mais comme il n'y a aucun vecteur non nul de U dans $V' + W'$, alors $y_2 + z_2 = 0_E$, d'où : $x = y_1 + z_1 \in (U\cap V) + (U\cap W)$. L'inclusion réciproque étant établie, on a bien : $(U\cap V) + (U\cap W) = U\cap(V + W)$. (L'autre côté est obtenu par commutativité de l'intersection).

[vii] Une application f d'un ensemble E dans un ensemble F est une bijection si et seulement si tout élément de F admet un unique antécédent dans E.

[viii] Une application f de E dans F est une injection si et seulement si tout élément de F admet au plus un antécédent dans E. Une application f de E dans F est une surjection si et seulement si tout élément de F admet au moins un antécédent dans E. On démontre qu'une application est injective en supposant que deux éléments ont la même image et en prouvant leur égalité : $f(x) = f(x') \Rightarrow x = x'$. On démontre qu'une application est surjective en exprimant l'antécédent d'un élément quelconque de F en fonction de lui-même.

[ix] Soit $f : F \to G$, $g : E \to F$, et B une base de $g(E)$; on a : $\mathrm{Card}(B) = \mathrm{rg}(g)$. Si f est injective alors $f(B)$ est une famille libre de G ayant le même nombre de vecteurs que B, et c'est une base de $\mathrm{Im}(f\circ g)$. Ainsi : $\mathrm{rg}(g) = \mathrm{Card}(B) = \mathrm{Card}(f(B)) = \mathrm{rg}(f\circ g)$.

Si f n'est pas injective, alors : $\mathrm{rg}(g) = \mathrm{Card}(B) \ge \mathrm{Card}(f(B)) = \mathrm{rg}(f\circ g)$. En outre : $\mathrm{rg}(f) = \dim(f(F)) \ge \dim(f(g(E)))$, d'où :

$\mathrm{rg}(f\circ g) \le \inf\{\mathrm{rg}(f), \mathrm{rg}(g)\}$.

Dans l'autre sens : Soit $g : F \to G$, $f : E \to F$; si f surjective alors $f(E) = F$ d'où $g(f(E)) = g(F)$, et ainsi : $\mathrm{rg}(g\circ f) = \mathrm{rg}(g)$. Si f n'est pas surjective on reproduit la démonstration précédente pour arriver à : $\mathrm{rg}(g\circ f) \le \inf\{\mathrm{rg}(f), \mathrm{rg}(g)\}$.

Pour une bijection, on applique la règle de l'injection d'un côté et celle de la surjection de l'autre.

[x] $(F, *)$ est un sous-groupe de $(E, *)$ si et seulement si : F est non vide, stable par $*$, et tous les symétriques (inverses pour un produit, opposés pour une addition) des éléments de F sont aussi des éléments de F.

[xi] Si $\dim(E) = 0$, la question ne se pose pas. Si $\dim(E) = 1$, alors E est isomorphe à $\mathbb{K}$, ce qui revient à chercher tous les endomorphismes de $\mathbb{K}$. Mais : $\forall\, x \in \mathbb{K}$, $f(x) = f(x.1) = x.f(1)$, qui est bien une homothétie.

Si $\dim(E) \geq 2$: Soit u et v deux vecteurs colinéaires ; on note k_u, k_v et k_{u+v} tels que $f(u) = k_u.u$, $f(v) = k_v.v$ et $f(u + v) = k_{u+v}.(u + v)$. Alors, comme $f(u + v) = f(u) + f(v)$: $(k_{u+v} - k_u).u + (k_{u+v} - k_v).v = 0_E$; et comme ils sont linéairement indépendants : $k_{u+v} - k_u = k_{u+v} - k_v = 0$, d'où : $k_{u+v} = k_u = k_v$. Comme u et v sont quelconques, si on applique ce procédé à $\alpha.u$ avec $\alpha \neq 0$, alors : $k_{\alpha u} = k_u$. Finalement, le coefficient est constant sur chaque direction, et de même sur toutes les autres directions ; ceci prouve que f est une homothétie.

[xii] Soit les sous-espaces vectoriels supplémentaires $U \oplus V = E$ et $U' \oplus V' = E$, ainsi que p la projection sur U de direction V et q la projection sur U' de direction V'. On a alors : $(U \cap U') + (U \cap V') + (V \cap U') + (V \cap V') = (U \cap (U' + V')) + (V \cap (U' + V')) = U + V = E$. En outre, ces sommes sont directes de façon évidente.

Soit $x \in E$; il existe $x_1 \in U \cap U'$, $x_2 \in U \cap V'$, $x_3 \in V \cap U'$ et $x_4 \in V \cap V'$ tels que $x = x_1 + x_2 + x_3 + x_4$; on a donc :

$p \circ q(x) = p \circ q(x_1) + p \circ q(x_2) + p \circ q(x_3) + p \circ q(x_4) = p(q(x_1)) + p(q(x_2)) + p(q(x_3)) + p(q(x_4)) = p(x_1) + p(0_E) + p(x_3) + p(0_E)$ car x_1 et x_3 sont dans U', tandis que x_2 et x_4 sont dans V'. Par suite, comme $p(x_1) = x_1$ car $x_1 \in U$, et $p(x_3) = 0_E$ car $x_3 \in V$: $p \circ q(x) = x_1 \in U \cap U'$.

Soit $F = U \cap U'$ et $G = (U \cap V') + (V \cap U') + (V \cap V') = (U \cap V') + V = (V \cap U') + V'$; alors $F \oplus G = E$, $\mathrm{Im}(p \circ q) \subset F$ et $G \subset \mathrm{Ker}(p \circ q)$.

Soit $x \in F$, alors $x = x_1$ et $x_2 = x_3 = x_4 = 0$, donc $p \circ q(x) = x_1 = x$, d'où $x \in \mathrm{Im}(p \circ q)$. Comme il y a la double inclusion, alors : $F = \mathrm{Im}(p \circ q)$.

Soit $x \in \mathrm{Ker}(p \circ q)$, alors $p \circ q(x) = x_1 = 0$, donc $x \in G$. Comme il y a la double inclusion, alors : $G = \mathrm{Ker}(p \circ q)$.

Il s'en suit que $p \circ q$ est bien un projecteur.

[xiii] Une involution est une bijection égale à sa réciproque.

[xiv] Soit $u' = f(u)$; alors $u' = M.u$, et comme $u = f^{-1}(u')$, alors f^{-1} admet une matrice N telle que $u = N.u'$. Par suite : $f^{-1} \circ f(u) = u$ et $f \circ f^{-1}(u') = u'$; d'où : $M.N = N.M = I$, en remarquant que E et F ont même dimension car f est un isomorphisme, et il s'agit donc bien d'une unique matrice identité. Ces dernières égalités signifient que M est inversible d'inverse N.

Pour la seconde partie de la proposition, il suffit de faire la preuve dans des bases judicieusement choisies, et d'appliquer ensuite les formules de changement de base. Soit f ayant pour matrice M dans les bases canoniques ;on pose $F_2 = \mathrm{Ker}(f)$, et soit F_1 un supplémentaire de $\mathrm{Ker}(f)$ dont on a vu qu'il était isomorphe à $\mathrm{Im}(f)$. On considère alors la nouvelle base $C_1 \cup C_2$ réunion des bases respectives de F_1 et F_2. Dans cette nouvelle base, la matrice de f est de la forme : $\left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right)$, où A est une matrice carrée inversible ayant $\dim(F_1)$ lignes et colonnes. Pour cette matrice, le théorème est évident. Il ne reste plus qu'à montrer que le fait de multiplier par une matrice inversible ne modifie pas le rang, ce qui est une conséquence directe d'une proposition précédente.

[xv] À noter que ce vecteur formé des cofacteurs s'appelle toujours le produit vectoriel de $(U_2, U_3, \dots, U_n)$. Dans un espace euclidien de dimension n, le produit vectoriel des $n - 1$ vecteurs $v_1, v_2, \dots, v_{n-1}$ est l'unique vecteur w tel que pour tout vecteur x on ait l'égalité : $\det(v_1, v_2, \dots, v_{n-1}, x) = (w|x)$.