# Université de Savoie Année 10/11

**Mathématiques générales : algèbre (MATH303 – 6 ECTS)**

## Table des matières

# 1 Anneaux

## 1.1 Abrégé de théorie des groupes

**Définition 1.1.1** Un *groupe* est un couple $(G, \cdot)$ où $G$ désigne un ensemble *non vide* et $\cdot$ une *loi de composition interne* (l.c.i.) *associative* telle que :

1. il existe un *élément neutre* $e \in G$ (souvent noté 1) pour $\cdot$ *i.e.* $\forall x \in G : ex = xe = x$
2. tout élément $x$ admet un *inverse* $y \in G$ pour $\cdot$ *i.e.* $(\forall x \in G)(\exists y \in G) : xy = yx = e$. On note $y = x^{-1}$.

**Remarque 1.1.1**

1. L'élément neutre, s'il existe pour une l.c.i, est unique.
2. L'inverse d'un élément, s'il existe pour une l.c.i. associative, est unique.
3. Quand la l.c.i. $\cdot$ est commutative, on la note en général $+$ et l'élément neutre 0 et on dit que $(G, +)$, ou plus simplement $G$ par abus de langage, est *commutatif* ou *abélien*.

**Définition 1.1.2** L'*ordre* d'un groupe $G$, noté $|G|$, est le cardinal de $G$. Un groupe est *fini* si son ordre est fini.

**Définition 1.1.3** Un *sous-groupe* $H$ de $(G, .)$ est un sous-ensemble non vide $H$ de $G$ tel que $\forall x, y \in H : xy^{-1} \in H$. Un sous-groupe $H$ est *distingué* ou *normal* (dans $G$) si $(\forall x \in G)(\forall h \in H) : xhx^{-1} \in H$ ; on note $H \lhd G$.

**Exemple 1.1.1** Si $g \in G$ alors $< g >= \{g^n : n \in \mathbb{Z}\}$ est un sous-groupe de $G$ appelé *sous-groupe engendré par* $g$ ; il est *monogène*. Un groupe monogène et fini est *cyclique*.

**Définition 1.1.4** L'*ordre* d'un élément $g \in G$ est l'ordre du sous-groupe $< g >$.

**Rappel 1.1.1** Une *relation d'équivalence* sur un ensemble $E$ est une relation binaire réflexive, symétrique et transitive sur $E$.

**Proposition 1.1.1** Soit $H$ un sous-groupe de $G$. Alors la relation définie par $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence sur $G$.

**Définition 1.1.5** Les classes d'équivalence de $\mathcal{R}$ sont les *classes à gauche*. L'*ensemble des classes d'équivalence* ou *ensemble quotient* est noté $G/\mathcal{R}$ ou $G/H$.

**Remarque 1.1.2**

1. On définirait de même les classes à droite par $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$.
2. Si $H \lhd G$ alors les classes à gauche et les classes à droite coïncident.

**Corollaire 1.1.1** Si $G$ est fini alors $|H|$ divise $|G|$.

**Proposition 1.1.2** Soit $\mathcal{R}$ une relation d'équivalence sur un groupe $G$. Alors, $\mathcal{R}$ est compatible avec $\cdot$ ssi il existe un sous-groupe $H$ distingué dans $G$ définissant $\mathcal{R}$.

**Proposition 1.1.3** Si $H \lhd G$ alors $G/H$ est muni d'une structure de groupe.

## 1.2 Généralités

**Définition 1.2.1** Un ensemble $(A, +, \cdot)$ muni de 2 lois de composition internes est un *anneau* si :

1. $(A, +)$ est un groupe commutatif (ou *abélien*)
2. $$\forall (a,b,c) \in A^3 : \quad \begin{array}{ll} (ab)c = a(bc) & (\textit{associativité}) \\ \left.\begin{array}{l} a(b+c) = ab + ac \\ (a+b)c = ac + bc \end{array}\right\} & (\textit{distributivité}) \end{array}$$

**Remarque 1.2.1**

1. Si la multiplication est commutative alors $A$ est *commutatif*.
2. Si la multiplication admet un élément neutre (noté $1_A$ ou 1) alors $A$ est *unitaire*.
   **Exercice** : Si $1_A = 0_A$ alors $A = \{0\}$.
3. Si $A$ est unitaire, $1 \neq 0$ et que pour tout $x \neq 0$, $x$ est inversible (pour la multiplication) alors $A$ est un *corps*.

**Exemple 1.2.1**

1. $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif et unitaire.
2. Si $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ alors $\mathbb{K}[X]$ *l'algèbre des polynômes en une indéterminée et à coefficients dans (le corps)* $\mathbb{K}$ est une anneau unitaire commutatif. C'est aussi un ($\mathbb{K}-$)espace vectoriel de dimension infinie.
3. Si $n \geq 2$ alors $\mathcal{M}_n(\mathbb{K})$ est un anneau unitaire *non* commutatif. Par exemple,
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0.$$
4. Si $n \geq 2$ alors $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau unitaire commutatif.
5. Soient $E$ un ensemble et $A$ un anneau. Alors $\mathcal{A}(E, A)$ est (canoniquement) muni d'une structure d'anneau induite par celle de $A$.

**Règles de calcul :**

1. $a0 = 0a = 0$ car $a0 = a(0+0) = a0 + a0$ donc $a0 = 0$ ; on permute 0 et $a$ pour démontrer la 2ième égalité.
2. $a(-x) = (-a)x = -ax$ car $a(x-x) = 0 = ax + a(-x)$ d'où $a(-x) = -ax$ ; preuve similaire pour la 2ième égalité.
3. $a(x-y) = ax - ay$
4. $(a-b)x = ax - bx$
5. $(-a)(-b) = ab$

**Exemple 1.2.2**

1. Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs.
2. Les ensembles $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}[X]$ ne sont pas des corps (munis des opérations usuelles).

**Proposition 1.2.1** Soient $A$ un anneau, $a, b \in A$ qui commutent et $n \in \mathbb{N}$. Alors
$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

**Définition 1.2.2** Soient $A$ et $B$ deux anneaux. Une application $f : A \to B$ est un *homomorphisme* d'anneaux si $\forall x, y \in A$ :

$$f(x+y) = f(x) + f(y)$$

et

$$f(xy) = f(x)f(y).$$

Le *noyau* de $f$ est $\ker f = \{x \in A : f(x) = 0\}$.

**Exercice** : $\ker f = \{0\} \Leftrightarrow f$ injective.

**Remarque 1.2.2**

1. $f(x+0) = f(x) + f(0) = f(x)$ donc $f(0_A) = 0_B$.
2. Mais on n'a pas nécessairement $f(1_A) = 1_B$ ; par exemple, en considérant

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & 0 \end{array}.$$

**Exemple 1.2.3**

1. Soit $a \in \mathbb{K}$.

$$\begin{array}{rccc} f: & \mathbb{K}[X] & \to & \mathbb{K} \\ & P & \mapsto & P(a) \end{array}$$

   est un homomorphisme d'anneaux.

2. Soit $A$ un anneau unitaire. L'application :

$$\begin{array}{rccl} f: & \mathbb{Z} & \to & A \\ & n & \mapsto & \begin{cases} 1_A + \cdots + 1_A & n \text{ fois si } n \geq 0 \\ -1_A - \cdots - 1_A & (-n) \text{ fois sinon.} \end{cases} \end{array}$$

   est un homomorphisme d'anneaux. Par exemple pour $n, n' \geq 0$, on a $f(nn') = (nn')1_A = nf(n') = 1_A f(n') + \cdots + 1_A f(n') = (1_A + \cdots + 1_A)f(n') = f(n)f(n')$.

3. Soient $\mathbb{K}, \mathbb{K}'$ deux corps et $f : \mathbb{K} \to \mathbb{K}'$ un homomorphisme d'anneaux. Deux cas se présentent :
   - $\ker f = \mathbb{K}$ et $f$ est l'application nulle.
   - $\ker f \neq \mathbb{K}$ : soit $x \notin \ker f$ alors $f(x1_{\mathbb{K}}) = f(x) = f(x)f(1_{\mathbb{K}})$ donc $f(1_{\mathbb{K}}) = 1_{\mathbb{K}'}$. Par suite, si $a \neq 0$ alors $a$ est inversible donc $f(aa^{-1}) = f(1_{\mathbb{K}}) = 1_{\mathbb{K}'} = f(a)f(a^{-1})$. Dès lors, si $a \neq 0$ alors $f(a)$ est inversible et $(f(a))^{-1} = f(a^{-1})$. Ainsi, $f(a) = 0$ ssi $a = 0$. D'où $\ker f = \{0\}$ et $f$ est injective.

**Définition 1.2.3** Un sous-ensemble $I$ d'un anneau $A$ est un *idéal* (*bilatère*) de $A$ si :

1. $I \neq \varnothing$
2. $\forall x, y \in I : x - y \in I$
3. $(\forall a \in A)(\forall x \in I) : ax \in I$ et $xa \in I$.

**Exemple 1.2.4**

1. Si $A$ est commutatif, on note $(a) = \{ax : x \in A\} = aA$, *l'idéal engendré* par $a$. Si $A$ est unitaire alors $a \in (a)$. Si $a \in I$ alors $(a) \subseteq I$.
2. Si $\mathbb{K}$ est un corps, ses seuls idéaux sont $\{0\}$ et $\mathbb{K}$.
3. Les idéaux de $\mathbb{Z}$ sont les $(n) = n\mathbb{Z}$ pour $n \in \mathbb{N}$.
4. Les idéaux de $\mathbb{K}[X]$ sont les $(P)$ pour $P \in \mathbb{K}[X]$.

**Proposition 1.2.2** Soient $A, B$ deux anneaux et $f : A \to B$ un homomorphisme. Alors $\ker f = f^{-1}(\{0\})$ est un idéal de $A$.

**Dém.** : $\ker f \neq \varnothing$ car $0 \in \ker f$. Soient $x, y \in \ker f$, alors $f(x-y) = 0$ *i.e.* $x - y \in \ker f$. Enfin, soient $x \in \ker f$ et $a \in A$ alors $f(ax) = f(a)f(x) = 0$ donc $ax \in \ker f$ et $\ker f$ est un idéal de $A$.

**Définition 1.2.4** Une relation d'équivalence $\mathcal{R}$ sur un anneau $(A, +, \cdot)$ est *compatible* avec $+$ et $\cdot$ si

$$\forall (a, a', b, b') \in A^4 : a\mathcal{R}a' \text{ et } b\mathcal{R}b' \Rightarrow (a+b)\mathcal{R}(a'+b') \text{ et } ab\mathcal{R}a'b'.$$

**Exemple 1.2.5** Soit $n \in \mathbb{N}$. Pour $a, b \in \mathbb{Z}$, on définit :

$$a\mathcal{R}b \Leftrightarrow b - a \text{ est un multiple de } n.$$

On note $a \equiv b[n]$ que l'on lit *a est congru à b modulo n*. C'est une relation d'équivalence sur $\mathbb{Z}$ compatible avec $+$ et $\times$.

**Dém.** : soient $a' \equiv a[n]$ et $b' \equiv b[n]$ *i.e.* $a' = a + kn$ et $b' = b + ln$. Alors $a' + b' = a + b + (k+l)n$ et $a'b' = ab + (al + bk + kln)n$. Ainsi, $\equiv [n]$ est compatible avec l'addition et la multiplication dans $\mathbb{Z}$.

**Proposition 1.2.3** Soient $A$ un anneau et $\mathcal{R}$ une relation d'équivalence sur $A$. Alors $\mathcal{R}$ est compatible avec $+$ et $\cdot$ si et seulement si il existe un idéal $I$ de $A$ tel que :

$$\forall (x, y) \in A^2 : x\mathcal{R}y \Leftrightarrow x - y \in I.$$

**Dém.** :

($\Rightarrow$) Notons $I = \dot{0} = \{x \in A : x\mathcal{R}0\}$. Alors $I \neq \varnothing$. Par ailleurs, soient $x, y \in A$ tels que $x\mathcal{R}y$. On a $(-y)\mathcal{R}(-y)$ donc $(x-y)\mathcal{R}0$ ou encore $x - y \in I$. Il s'ensuit, d'une part que si $x, y \in I$ alors $x - y \in I$ (par symétrie et transitivité de $\mathcal{R}$), et d'autre part que, $x\mathcal{R}y \Leftrightarrow x - y \in I$. Enfin, si $x \in I$ et $a \in A$ alors $x\mathcal{R}0$ entraîne $ax\mathcal{R}a0$ *i.e.* $ax\mathcal{R}0$ ou encore $ax \in I$. On montrerait de même $xa \in I$. On conclut que $I$ est l'idéal répondant à la question.

($\Leftarrow$) Il est facile de vérifier que $\mathcal{R}$ est une relation d'équivalence. Soit $(x, y, x', y') \in A^4$ tel que $x\mathcal{R}y$ et $x'\mathcal{R}y'$. Alors, $x - y \in I$ et $x' - y' \in I$ *i.e.* il existe $p, p' \in I$ tels que $x = y + p$ et $x' = y' + p'$. Par suite, $x + x' = y + y' + (p + p')$ et $xx' = yy' + (yp' + py' + pp')$. Autrement dit, $\mathcal{R}$ est compatible avec $+$ et $\cdot$.

**Théorème 1.2.1** Soient $A$ un anneau et $I$ un idéal de $A$. Alors la relation $\mathcal{R}$ définie par :

$$\forall x, y \in A : x\mathcal{R}y \Leftrightarrow x - y \in I$$

est une relation d'équivalence compatible avec les lois de $A$. Le quotient $A/\mathcal{R}$, noté $A/I$, possède une structure d'anneau munie des opérations :

$$\dot{x}\dot{+}\dot{y} := \dot{\widehat{x + y}} \text{ et } \dot{x}\dot{y} := \dot{\widehat{xy}}.$$

La projection canonique $\pi : A \to A/I$ définie par $\pi(x) = \dot{x}$ est un homomorphisme surjectif d'anneaux et son noyau est $I = \dot{0}$.

**Dém.** : la relation d'équivance $\mathcal{R}$ est compatible avec $+$ et $\cdot$ d'après la proposition précédente. Par conséquent, les opérations $+$ et $\cdot$ *passent au quotient* et définissent une structure d'anneau sur $A/I$. L'application $\pi$, surjective par définition, est un homomorphisme d'anneau compte-tenu de la définition des lois $\dot{+}$ et $\dot{\times}$. Enfin, $\pi(x) = \dot{0} \Leftrightarrow x \in I$.

**Exemple 1.2.6** Pour $n = 6$, on note $\mathbb{Z}/6\mathbb{Z}$ le *quotient* de $\mathbb{Z}$ par (l'idéal) $6\mathbb{Z}$ (*i.e.* $x\mathcal{R}y \Leftrightarrow$ 6 divise $x - y$ ou encore $x - y \in 6\mathbb{Z}$). C'est l'anneau commutatif unitaire à 6 éléments :

$$(\{\dot{0}, \dot{1}, \ldots, \dot{5}\}, +, \cdot)$$

dont les tables sont :

| $+$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ |
|---|---|---|---|---|---|---|
| $\dot{0}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ |
| $\dot{1}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ |
| $\dot{2}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ | $\dot{1}$ |
| $\dot{3}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ |
| $\dot{4}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ |
| $\dot{5}$ | $\dot{5}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ |

| $\times$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ |
|---|---|---|---|---|---|---|
| $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ |
| $\dot{1}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ |
| $\dot{2}$ | $\dot{0}$ | $\dot{2}$ | $\dot{4}$ | $\dot{0}$ | $\dot{2}$ | $\dot{4}$ |
| $\dot{3}$ | $\dot{0}$ | $\dot{3}$ | $\dot{0}$ | $\dot{3}$ | $\dot{0}$ | $\dot{3}$ |
| $\dot{4}$ | $\dot{0}$ | $\dot{4}$ | $\dot{2}$ | $\dot{0}$ | $\dot{4}$ | $\dot{2}$ |
| $\dot{5}$ | $\dot{0}$ | $\dot{5}$ | $\dot{4}$ | $\dot{3}$ | $\dot{2}$ | $\dot{1}$ |

**Remarque 1.2.3**

1. $A$ commutatif $\Rightarrow A/I$ commutatif.
2. $A$ unitaire $\Rightarrow A/I$ unitaire (cas intéressant : $(0) \subsetneq I \subsetneq A$).

**Définition 1.2.5** Un sous-ensemble $A'$ de l'anneau $A$ est un *sous-anneau* de $A$ si :

1. $A'$ est un sous-groupe de $A$
2. la loi $\cdot$ resteinte à $A'$ est interne.

**Lemme 1.2.1**

1. Un sous-anneau $A'$ d'un anneau $A$ est un anneau.
2. Si $f : A \to B$ est un homomorphisme alors $f(A)$ est un sous-anneau de $B$.

**Théorème 1.2.2** Soient $A, B$ deux anneaux et $f : A \to B$ un homomorphisme. Alors

$$A/\ker f \cong f(A).$$

**Dém.** : le sous-ensemble $\ker f$ est un idéal de $A$, donc $A/\ker f$ est un anneau. Considérons le diagramme :

$$\begin{array}{ccc} A & \xrightarrow{\tilde{f}} & f(A) \hookrightarrow B \\ \pi \downarrow & \circlearrowleft & \nearrow \\ A/\ker f & & \bar{f} \end{array}$$

L'application $\tilde{f}$ se déduit de $f$ en changeant le *but*. Elle est surjective par définition. L'application $\bar{f}$ est bien définie par $\bar{f}(\dot{x}) = \tilde{f}(x) = f(x)$. En effet, si $\dot{x} \in A/\ker f$ et si $x, x'$ sont 2 représentants de $\dot{x}$ alors $x - x' \in \ker f$ donc $f(x - x') = 0$ ou encore $f(x) = f(x')$. Comme $f$ est un homomorphisme d'anneaux, $\bar{f}$ l'est aussi. Enfin, $\bar{f}(\dot{x}) = 0 \Leftrightarrow f(x) = 0 \Leftrightarrow x \in \ker f \Leftrightarrow \dot{x} = \dot{0}$, ainsi $\bar{f}$ est injective et surjective (car $\tilde{f} = \bar{f} \circ \pi$ est surjective) *i.e.* bijective.

**Remarque 1.2.4** Le diagramme suivant est *la factorisation canonique* de l'application $f$ :

$$f : A \xrightarrow{\pi} A/\ker f \xrightarrow{\bar{f}} f(A) \xhookrightarrow{i} B$$

(cette factorisation a encore lieu dans un cadre sensiblement plus général).

**Définition 1.2.6** Soient $A$ un anneau commutatif et $a, b \in A$. On dit que $a$ *divise* $b$, noté $a|b$, s'il existe $x \in A$ tel que $b = ax$. Ainsi $b$ est un *multiple* de $a$.

**Exemple 1.2.7** Dans $\mathbb{Z}$ et $\mathbb{K}[X]$ on retrouve la notion usuelle.

**Définition 1.2.7** Un élément $a \neq 0$ d'un anneau commutatif $A$ est *diviseur de* 0 s'il existe $b \neq 0$ tel que $ab = 0$.

**Exemple 1.2.8**

1. Déterminer dans $\mathbb{Z}/6\mathbb{Z}$ les diviseurs de 0.
2. Dans $\mathcal{A}(\mathbb{R}, \mathbb{R})$, on considère $f = 1_{\mathbb{R}^*_-}$ et $g = 1_{\mathbb{R}_+}$. Alors, $f$ et $g$ sont diviseurs de 0 (il existe aussi des diviseurs de 0 dans $\mathcal{A}(\mathbb{R}, \mathbb{R})$ de classe $C^\infty$).

**Définition 1.2.8** Un anneau $A$ est *intègre* si :

1. $A$ est commutatif
2. $A$ n'a pas de diviseur de 0.

**Exemple 1.2.9**

1. $\mathbb{Z}$ est intègre.
2. $\mathbb{Z}/6\mathbb{Z}$ ne l'est pas.

**Exercice** : $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ $n = 0$ ou $n = 1$ ou $n$ premier.

**Dém.** : ($\Rightarrow$) on peut supposer $n \geq 2$. Soit $a \in \mathbb{Z}$ divisant $n$. Alors il existe $b \in \mathbb{Z}$ tel que $ab = n$. Par conséquent, $\dot{a}\dot{b} = \dot{0}$. Comme $\mathbb{Z}/n\mathbb{Z}$ est intègre, $\dot{a} = \dot{0}$ ou $\dot{b} = \dot{0}$ *i.e.* $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$. Deux cas se présentent :

- $a \notin n\mathbb{Z}$ : alors $a = \pm 1$ et $b = \pm n$
- $a \in n\mathbb{Z}$ : alors $a = \pm n$ et $b = \pm 1$.

Ainsi, les diviseurs de $n$ sont $\pm 1$ et $\pm n$ et $n$ est premier.

**Proposition 1.2.4** Soient $A$ un anneau intègre et $a, b, x \in A$. Si $ax = bx$ et $x \neq 0$ alors $a = b$.
**Dém.** : comme $A$ est intègre, $a - b$ n'est pas un diviseur de 0 donc $a - b = 0$.

## 1.3 Anneaux principaux

### 1.3.1 Généralités

**Lemme 1.3.1** Soient $A$ un anneau commutatif unitaire et $a, b \in A$. C.S.S.E. :

1. $(a) \subseteq (b)$
2. $a \in (b)$
3. $b|a$

**Dém.** :
1) $\Rightarrow$ 2) facile car $1 \in A$.
2) $\Rightarrow$ 3) par définition de $(b)$.
3) $\Rightarrow$ 1) Comme $b|a$, il existe $q \in A$ tel que $a = bq$. Par suite, $a \in (b)$. Or $(b)$ est un idéal donc $(a) \subseteq (b)$.

**Définition 1.3.1** Un idéal $I$ d'un anneau *commutatif unitaire* $A$ est *principal* s'il existe $a \in A$ tel que

$$I = (a) = \{ax : x \in A\}.$$

**Définition 1.3.2** Un anneau $A$ est *principal* si

1. $A$ est commutatif, unitaire et intègre ;
2. tout idéal de $A$ est principal.

**Exemple 1.3.1** Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

**Dém.** : on va le démontrer pour $\mathbb{Z}$. L'anneau $\mathbb{Z}$ est commutatif, unitaire et intègre. Soit $I$ un idéal de $\mathbb{Z}$. Deux cas se présentent :

1. $I = \{0\}$ *i.e.* $I = (0)$ qui est principal ;
2. $(0) \subsetneq I$. Alors $I_+^* = I \cap \mathbb{N} - \{0\}$ est une partie non vide de $\mathbb{N}^*$. Il existe donc $p = \min I_+^*$ ($\in I_+^*$ !). Soit $n \in I$. Alors $n = pq + r$ avec $0 \leqslant r < p$. Donc $r = n - pq \in I \cap \mathbb{N}$. Comme $r < p$, il s'ensuit que $r = 0$ donc $I \subseteq (p)$. Par ailleurs, $p \in I$ donc $I = (p)$ et $I$ est principal. Il est facile de voir qu'un tel générateur $p$ est unique au signe près.

**Proposition 1.3.1** Soient $A$ un anneau commutatif unitaire intègre et $a, b \in A$. Alors :

$$(a) = (b) \Leftrightarrow \text{ il existe un élément inversible } u \text{ de } A \text{ tel que } a = bu.$$

**Dém.** :
($\Rightarrow$) $(a) = (b) \Rightarrow a \in (b)$ et $b \in (a)$. Il existe donc $p \in A$ (resp. $q \in A$) tel que $a = bp$ (resp. $b = aq$). Dès lors, $a = apq$ d'où $a(1 - pq) = 0$. Deux cas se présentent :

1. $a = 0$, alors $(b) = (0)$ ; en particulier $u = 1$ convient.
2. $a \neq 0$, alors, comme $A$ est intègre, $pq = 1$ et $u = p$ est inversible.

($\Leftarrow$) On a $a \in (b)$ donc $(a) \subseteq (b)$. De plus, il existe $v \in A$ tel que $uv = 1$. Donc $av = b$ et $b \in (a)$ d'où $(b) \subseteq (a)$. On conclut que $(a) = (b)$

**Proposition 1.3.2** Soient $I, J$ deux idéaux de $A$. Alors

$$I \cap J$$

et

$$I + J = \{u + v : u \in I, v \in J\}$$

sont des idéaux de $A$.

**Remarque 1.3.1** En fait, une intersection quelconque d'idéaux est encore un idéal.

### 1.3.2 pgcd et ppcm

**Définition 1.3.3** Soient $a$ et $b \in A$, un anneau principal.
- *Un ppcm* de $(a, b)$ est un élément $m \in A$ tel que $(a) \cap (b) = (m)$.
- *Un pgcd* de $(a, b)$ est un élément $\delta \in A$ tel que $(a) + (b) = (\delta)$ ; on note $a \wedge b = \delta$.
- Les éléments $a$ et $b$ sont *premiers* entre eux si 1 est pgcd de $(a, b)$.
- Un élément $a$ est *irréductible* ou *premier* si $a \neq 0$, non inversible et si ses seuls diviseurs sont les inversibles de $A$ et les $au$ pour $u$ inversible.

**Exemple 1.3.2** Dans $\mathbb{Z}$, si $a = 4$ et $b = 6$ alors $ppcm(a, b) = \pm 12$ et $pgcd(a, b) = \pm 2$.

**Remarque 1.3.2**

1. $a \wedge b = 1 \Leftrightarrow (a) + (b) = A$ !
2. Cette définition se généralise à un nombre fini d'éléments de $A$.
3. *Le* pgcd et *le* ppcm sont définis à un inversible près.

**Lemme 1.3.2** Soient $a$ et $b \in A$, un anneau principal.

1. Si $d$ est un pgcd de $(a, b)$ alors il existe $u, v \in A$ tels que $d = au + bv$.
2. S'il existe $u, v \in A$ tels que $d = au + bv$ et si $d$ divise $a$ et $b$ alors $d$ est un pgcd de $(a, b)$.

**Dém.** :
1. résulte de la définition d'un pgcd.
Pour démontrer 2., on constate que $d \in (a) + (b)$ donc $(d) \subseteq (a) + (b)$. Par ailleurs, si $d|a$ (resp. $d|b$) alors $(a) \subseteq (d)$ (resp. $(b) \subseteq (d)$). Dès lors, $(a) + (b) \subseteq (d)$. D'où l'égalité.

**Proposition 1.3.3 [Minimalité du ppcm et maximalité du pgcd]** Soient $a, b \in A$ principal, $m$ un ppcm de $(a, b)$ et $\delta$ un pgcd de $(a, b)$.

1. Si $m'$ est un multiple de $a$ et de $b$ alors $m'$ est un multiple de $m$.
2. Si $d$ divise $a$ et $b$ alors $d|\delta$.

**Dém.** :

1. Si $a$ et $b$ divisent $m'$ alors $m' \in (a)$ et $m' \in (b)$. Donc $m' \in (a) \cap (b) = (m)$ et $m|m'$.
2. Si $d|a$ et $d|b$ alors $a, b \in (d)$. Il s'ensuit que $(\delta) = (a) + (b) \subseteq (d)$. Donc $d|\delta$.

**Corollaire 1.3.1** **[Caractérisation]** Soient $(a, b) \in A^2$ (avec $A$ principal) et $m', d' \in A$.

1. Si $m'$ est un multiple de $a$ et $b$ qui divise tout multiple de $a$ et $b$ alors $m'$ est un ppcm de $(a, b)$.
2. Si $d'$ divise $a$ et $b$ et si tout diviseur de $a$ et $b$ divise $d'$ alors $d'$ est un pgcd de $(a, b)$.

**Dém.** :

1. Soit $m$ un ppcm de $(a, b)$. Alors $m'|m$. En vertu de la proposition précédente, $m|m'$. On obtient $(m) = (m')$ et $m'$ est un ppcm de $(a, b)$.
2. Soit $\delta$ un pgcd de $(a, b)$. On déduit de la proposition précédente que $d'|\delta$. De plus, $\delta$ est un diviseur de $a$ et $b$ donc $\delta|d'$ par hypothèse. Il s'ensuit que $d'$ est un pgcd de $(a, b)$.

**Corollaire 1.3.2** Deux éléments $a, b \in A$ (principal) sont premiers entre eux ssi les seuls diviseurs communs à $a$ et $b$ sont les éléments inversibles.

**Dém.** :
($\Rightarrow$) Soit $d$ un diviseur de $a$ et $b$. Alors le 2. de la proposition précédente assure que $d|1$. Autrement dit, $d$ est inversible.
($\Leftarrow$) 1 est évidemment un diviseur de $a$ et $b$. Comme les seuls diviseurs de $a$ et $b$ sont les inversibles, ils divisent 1. En vertu du 2. du corollaire précédent, 1 est un pgcd de $(a, b)$.

**Théorème 1.3.1** **[de Bezout]** Soient $a, b \in A$ un anneau principal. Alors

$$a \text{ et } b \text{ sont premiers entre eux} \Leftrightarrow \exists u, v \in A : au + bv = 1$$

**Dém.** :
($\Rightarrow$) résulte de la définition.
($\Leftarrow$) résulte du 2. du lemme précédent.

**Remarque 1.3.3** On n'a pas unicité du couple $(u, v)$ ($1 = 2.(-1) + 3.1 = 2.2 + 3.(-1)$ sauf si l'on impose de surcroît $0 < \delta u < b$ ou $0 < \delta v < a$ par exemple).

**Théorème 1.3.2** **[de Gauss]** Soient $a, b, c \in A$, un anneau principal. Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

**Dém.** : comme $a \wedge b = 1$, il existe par définition, $u, v \in A$ tels que $au + bv = 1$. Par suite, $c = acu + bcv$. Comme, $a|bc$, il existe $q \in A$ tel que $bc = aq$. Il s'ensuit que $c = a(cu + qv)$ *i.e.* $a|c$.

**Lemme 1.3.3** Un corps est un anneau intègre.

**Proposition 1.3.4** Soit $n \in \mathbb{N}$. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $n$ est premier.

**Dém.** :
($\Rightarrow$) Comme $\mathbb{Z}/n\mathbb{Z}$ est un corps, $n \geq 2$. Soit $k \in \mathbb{Z}$ un diviseur de $n$. Deux cas se présentent :

1. $\dot{k} = \dot{0}$ *i.e.* $k \in n\mathbb{Z}$ mais alors $k = \pm n$.
2. $\dot{k} \neq \dot{0}$ donc $\dot{k}$ est inversible dans le corps $\mathbb{Z}/n\mathbb{Z}$. Il existe donc $k' \in \mathbb{Z}$ tel que $kk' \equiv 1[n] \Leftrightarrow kk' = 1 + nl$. Or $k|n$. Dès lors, $k(k' - n'l) = 1$. Cette égalité ne peut avoir lieu que si $\begin{cases} k = 1 \\ k' - n'l = 1 \end{cases}$ ou $\begin{cases} k = -1 \\ k' - n'l = -1 \end{cases}$. On conclut que $n$ est premier.

($\Leftarrow$) Comme $n$ est premier, $n \geq 2$. Soit $k \in \mathbb{Z}$ tel que $\dot{k} \neq \dot{0}$ (*i.e.* $k$ non multiple de $n$) et $\dot{k} \neq \dot{1}$. Comme $k$ est premier avec $n$, il existe $u, v \in \mathbb{Z}$ tels que $ku + nv = 1$. Par suite, $\dot{k}\dot{u} = \dot{1}$ et $\dot{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

# 2 Déterminant

## 2.1 Le groupe symétrique $\mathfrak{S}_n$

### 2.1.1 Généralités

**Définition 2.1.1** Soit $n \in \mathbb{N}^*$. Le *groupe symétrique de degré* $n$, noté $\mathfrak{S}_n$, est l'ensemble des bijections de $\{1, \ldots, n\}$ muni de la composition ($\circ$) des applications. Une *permutation* $\sigma$ est un élément de $\mathfrak{S}_n$ ; on notera :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

et $\sigma\tau$ au lieu de $\sigma \circ \tau$.

**Remarque 2.1.1** On aurait pu définir le groupe symétrique d'un ensemble $E$ de cardinal $n$. Les résultats sont rigoureusement les mêmes que ceux qui suivent.

**Exemple 2.1.1** On a :

1. $\mathfrak{S}_1 = \{id\}$.
2. $\mathfrak{S}_2 = \{id, (1\ 2)\}$ où $(1\ 2) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

**Proposition 2.1.1** Le groupe symétrique $\mathfrak{S}_n$ est un groupe (non commutatif si $n \geq 3$) d'ordre $n!$.

**Définition 2.1.2** Le *support* d'une permutation $\sigma$ est le sous-ensemble de $\{1, \ldots, n\}$ $supp\ \sigma := \{x \in \{1, \ldots, n\} : \sigma(x) \neq x\}$.

**Lemme 2.1.1** Le support d'une permutation $\sigma$ est stable par $\sigma$ et $\sigma_{|\complement supp\ \sigma} = id_{|\complement supp\ \sigma}$.

**Dém.** : soit $x \in supp\ \sigma$. On a : $\sigma(x) \neq x \Leftrightarrow \sigma(\sigma(x)) \neq \sigma(x)$ (car $\sigma$ est injective). Ainsi, $\sigma(supp\ \sigma) \subseteq supp\ \sigma$. Comme $\sigma$ est injective, $\sigma(supp\ \sigma)$ et $supp\ \sigma$ ont même cardinal fini donc sont égaux.

D'autre part : $x \notin supp\ \sigma \Leftrightarrow \sigma(x) = x \Leftrightarrow \sigma(x) = id(x)$ *i.e.* $\sigma_{|\complement supp\ \sigma} = id_{|\complement supp\ \sigma}$.

**Lemme 2.1.2** Si $\sigma$ et $\tau$ commutent alors le support de l'une est stable par l'autre. Si $supp\ \sigma \cap supp\ \tau = \varnothing$ alors $\sigma\tau = \tau\sigma$.

**Dém.** : soit $x \in supp\ \tau$ *i.e.* $\tau(x) \neq x$. Alors $\sigma\tau(x) \neq \sigma(x)$. Or $\sigma$ et $\tau$ commutent donc $\tau\sigma(x) \neq \sigma(x)$ d'où $\sigma(supp\ \tau) \subseteq supp\ \tau$. Comme $supp\ \tau$ et $\sigma(supp\ \tau)$ ont même cardinal fini, ils sont égaux.

Soit $x \in supp\ \tau$. Comme $\tau(x) \in supp\ \tau$ et que $supp\ \sigma \cap supp\ \tau = \varnothing$, on obtient $\sigma\tau(x) = \tau(x) = \tau\sigma(x)$. En inversant les rôles de $\tau$ et $\sigma$, on constate que si $x \in supp\ \sigma$ alors $\tau\sigma(x) = \sigma\tau(x)$. Enfin si $F = supp\ \sigma \cup supp\ \tau$ alors $\sigma_{|\complement F} = \tau_{|\complement F} = id_{|\complement F}$ d'où le résultat.

**Proposition 2.1.2** Soit $\sigma \in \mathfrak{S}_n$. La relation $x\mathcal{R}_\sigma y$ définie par

$$\exists k \in \mathbb{Z} : y = \sigma^k(x)$$

est une relation d'équivalence sur $\{1, \ldots, n\}$.

**Définition 2.1.3** L'*orbite* de $x \in \{1, \ldots, n\}$ suivant $\sigma \in \mathfrak{S}_n$ est la classe d'équivalence de $x$ modulo $\mathcal{R}_\sigma$. Autrement dit, $O_x = \{\sigma^k(x) : k \in \mathbb{Z}\}$.

**Remarque 2.1.2** Les orbites suivant $\sigma$ déterminent une partition de $\{1, \ldots, n\}$.

**Proposition 2.1.3** Soient $O$ une orbite non triviale (*i.e.* de cardinal $c \geq 2$) suivant $\sigma$ et $x \in O$. Alors $O = \{x, \sigma(x), \ldots, \sigma^{c-1}(x)\}$ avec $\sigma^c(x) = x$.

**Dém.** : comme $O$ est finie, il existe $i, j \in \mathbb{N}, i > j$ tels que $\sigma^i(x) = \sigma^j(x)$. Autrement dit, $\sigma^{i-j}(x) = x$ avec $i - j > 0$. Par suite, $\{k \in \mathbb{N}^* : \sigma^k(x) = x\}$ admet un plus petit élément $s > 1$ (sinon $O$ serait triviale). Pour $k \in \mathbb{Z}$, on a : $k = sq + r$ avec $0 \leqslant r < s$. Donc, $\sigma^k(x) = \sigma^{sq+r}(x) = \sigma^r(\sigma^{qs}(x)) = \sigma^r(x)$. Considérons la séquence $x, \sigma(x), \ldots, \sigma^{s-1}(x)$. On constate que $\sigma^k(x) \neq \sigma^{k'}(x)$ pour $0 \leqslant k, k' < s$ et $k \neq k'$, sinon $s$ ne serait pas minimal. Il vient $O = \{x, \sigma(x), \ldots, \sigma^{s-1}(x)\}$ ce qui exige $s = c$.

### 2.1.2 Décompositions en produit de cycles

**Définition 2.1.4** Un *cycle* est une permutation possèdant une unique orbite non réduite à 1 point. La *longueur* d'un cycle est le cardinal de son orbite non triviale.

**Exemple 2.1.2**

1. Dans $\mathfrak{S}_3$ :
   (a) le cycle (1 2) est de longueur 2 ; son orbite est $\{1, 2\}$ ;
   (b) les cycles (1 2 3) $= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et (1 3 2) $= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ sont de longueur 3 ; leur orbite est $\{1, 2, 3\}$ ;
   (c) en fait, $\mathfrak{S}_3 - \{id\}$ est constitué de cycles de longueur 2 ou 3.
2. Dans $\mathfrak{S}_4$, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$ n'est pas un cycle car elle possède 2 orbites : $\{1, 2\}$ et $\{3, 4\}$.

**Remarque 2.1.3** Le support d'un cycle coïncide avec son orbite non triviale.

**Définition 2.1.5** Un cycle de longueur 2 est une *transposition.*

**Exemple 2.1.3**

1. Une transposition permute exactement 2 éléments de $\{1, \ldots, n\}$.
2. La permutation (1 2) est une transposition.
3. Si $\tau$ est une transposition alors $\tau^{-1} = \tau$ ou encore $\tau^2 = id$ ; $\tau$ est une *involution.*

**Proposition 2.1.4** Une permutation $\neq id$ se décompose (de manière unique à l'ordre près) en un produit commutatif de cycle(s) de support 2 à 2 disjoint.

**Dém.** : soient $O_1, \ldots, O_p$ les orbites non réduites à 1 point d'une permutation $\sigma$. Notons $\sigma_i$ la permutation définie par $\sigma_{i|O_i} = \sigma_{|O_i}$ et $\sigma_{i|\complement O_i} = id_{|\complement O_i}$ pour $1 \leqslant i \leqslant p$. Comme les supports $O_i$ des $\sigma_i$ sont 2 à 2 disjoints, les *cycles* $\sigma_i$ commutent 2 à 2. De plus, pour $x \in \bigsqcup_{i=1}^{p} O_i$, on a $\sigma(x) = \sigma_{i_x}(x)$ par définition d'où $\sigma = \sigma_1 \cdots \sigma_p$. En outre, si $\sigma = \sigma'_1 \cdots \sigma'_{p'}$ (avec $\sigma'_i$ cycle) alors $p' = p$ (car $p'$ est le nombre d'orbites non triviales suivant $\sigma$) et l'orbite (non triviale) suivant $\sigma'_i$ est l'une des orbites non triviales de $\sigma$ *i.e.* de l'un des $\sigma_j$.

**Exemple 2.1.4** On a : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 1 & 7 & 3 & 6 & 4 & 10 & 8 & 9 \end{pmatrix} = (1\ 2\ 5\ 3)(4\ 7)(8\ 10\ 9)$.

**Proposition 2.1.5** Soit $n \geq 2$. L'ensemble des transpositions engendre $\mathfrak{S}_n$.

**Dém.** : soit $\sigma \in \mathfrak{S}_n$. Deux cas se présentent :

1. $\sigma = id$ alors $id = \tau^2$ pour toute transposition $\tau$.
2. $\sigma \neq id$ alors il (faut et il) suffit de traiter le cas d'un cycle. Soient $O$ l'orbite non triviale suivant $\sigma$ et $x \in O$. Alors $\sigma = (x\ \sigma(x)\ \cdots\ \sigma^{c-1}(x))$ avec $c \geqslant 2$.
   (a) Si la longueur $c = 2$ alors $\sigma$ est un transposition.
   (b) Sinon, supposons le résultat vrai pour un certain $c \geqslant 2$ et soit $\sigma$ un cycle de longueur $c+1$. Posons $\tau = (x\ \sigma^c(x))$. Il vient $\tau\sigma = (x\ \sigma(x)\ \cdots\ \sigma^{c-1}(x))$. Ainsi, $\tau\sigma$ est un cycle de longueur $c$ qui se décompose, par récurrence, en produit de $(c-1)$ transpositions.

**Remarque 2.1.4** Cette écriture n'est pas unique.

### 2.1.3 Signature

**Définition 2.1.6** La *signature* d'une permutation $\sigma \in \mathfrak{S}_n$ est l'entier $\epsilon(\sigma) = (-1)^{n-m}$ où $m$ est le nombre d'orbites suivant $\sigma$.

**Exemple 2.1.5**

1. La signature de l'identité est 1.
2. Si $\tau$ est une transposition alors $\epsilon(\tau) = (-1)^{n-(n-2+1)} = -1$.
3. Plus généralement, si $\sigma$ est un cycle de longueur $q$ alors $\epsilon(\sigma) = (-1)^{n-(n-q+1)} = (-1)^{q-1}$.

**Lemme 2.1.3** Soient $\sigma \in \mathfrak{S}_n$ et $\tau = (a\ b)$ une transposition. Alors $\epsilon(\sigma\tau) = -\epsilon(\sigma)$.

**Dém.** : la transposition $\tau$ agit uniquement sur les orbites suivant $\sigma$ contenant $a$ ou $b$. Posons $\sigma' = \sigma\tau$ et distinguons 2 cas :

1. $a$ et $b$ appartiennent à la même orbite $O = \{a, \sigma(a), \ldots, b = \sigma^q(a), \ldots, \sigma^{p-1}(a)\}$ suivant $\sigma$ avec $\sigma^p(a) = a$ et $0 < q \leqslant p-1$. Les itérées de $a$ par $\sigma'$ sont :

$$\begin{aligned} \sigma'^0(a) &= a \\ \sigma'(a) &= \sigma\tau(a) = \sigma(b) = \sigma^{q+1}(a) \\ \sigma'^2(a) &= \sigma\tau(\sigma^{q+1}(a)) = \sigma^{q+2}(a) \\ \vdots &= \vdots \\ \sigma'^{p-q}(a) &= \sigma^p(a) = a \end{aligned}$$

   De même les itérées de $b$ sont :

$$\begin{aligned} \sigma'^0(b) &= b \\ \sigma'(b) &= \sigma\tau(b) = \sigma(a) \\ \sigma'^2(b) &= \sigma^2(a) \\ \vdots &= \vdots \\ \sigma'^q(b) &= b \end{aligned}$$

   Ainsi, l'orbite $O$ se scinde en 2 orbites distinctes suivant $\sigma'$ donc $\epsilon(\sigma') = (-1)^{n-(m_\sigma+1)} = -\epsilon(\sigma)$.

2. $a, b$ appartiennent à des orbites distinctes suivant $\sigma$ *i.e.* $O_a = \{a, \sigma(a), \ldots, \sigma^{p-1}(a)\}$ et $O_b = \{b, \sigma(b), \ldots, \sigma^{q-1}(b)\}$, $q \leqslant p$. Les itérées de $a$ sont :

$$\begin{aligned} \sigma'^0(a) &= a \\ \sigma'(a) &= \sigma(b) \end{aligned}$$

$$\begin{aligned}
\vdots &= \vdots \\
\sigma'^{q-1}(a) &= \sigma^{q-1}(b) \\
\sigma'^{q}(a) &= b \\
\sigma'^{q+1}(a) &= \sigma(a) \\
\vdots &= \vdots \\
\sigma'^{q+p-1}(a) &= \sigma^{p-1}(a) \\
\sigma'^{q+p}(a) &= a
\end{aligned}$$

Et $O_a, O_b$ fusionnent en une même orbite suivant $\sigma'$ d'où $\epsilon(\sigma') = (-1)^{n-(m_\sigma-1)} = -\epsilon(\sigma)$.

**Proposition 2.1.6** Soient $\sigma \in \mathfrak{S}_n$ et $\sigma = \tau_1 \cdots \tau_p$ une écriture de $\sigma$ en un produit de transposition(s). Alors $\epsilon(\sigma) = (-1)^p$ *i.e.* la signature ne dépend que de la parité de $p$ (donc la parité de $p$ est invariante pour $\sigma$ donnée).

**Dém.** : récurrence à l'aide du lemme précédent.

**Définition 2.1.7** Une permutation $\sigma$ est *paire* (resp. *impaire*) si $\epsilon(\sigma) = 1$ (resp. $\epsilon(\sigma) = -1$).

**Corollaire 2.1.1** La signature $\epsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un homomorphisme (surjectif si $n \geq 2$) de groupes.

**Dém.** : il suffit de vérifier que le produit de 2 permutations de même parité (resp. de parité différente) est pair (resp. impair). Ce qui est immédiat.

**Proposition 2.1.7** Le sous-ensemble de(s) permutation(s) paire(s) est un sous-groupe distingué $\mathfrak{A}_n$ dans $\mathfrak{S}_n$ appelé *sous-groupe alterné* de $\mathfrak{S}_n$.

**Dém.** conséquence du fait que $\epsilon$ est un morphisme de groupes.

## 2.2 Déterminant d'un endomorphisme

### 2.2.1 Rappels et compléments d'algèbre linéaire

**Définition 2.2.1** Soient $E$ un $\mathbb{K}-$espace vectoriel ($ev$) et $\mathcal{F} = (a_i)_{i\in I}$ une famille de vecteurs de $E$.

1. La famille $\mathcal{F}$ est *génératrice* si pour tout $x \in E$, il existe un *nombre fini* d'indices $i_1, \ldots, i_n$ et $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que $x = \sum_{k=1}^{n} \lambda_k a_{i_k}$. Si $I$ est fini, la condition de finitude est toujours satisfaite.
2. Si $E$ admet une famille génératrice finie, il est de *dimension finie*.
3. La famille $\mathcal{F}$ est *libre* si toute sous-famille *finie* est *libre* :

$$(a_{i_1}, \ldots, a_{i_n}) \text{ libre } \Leftrightarrow (\forall \lambda_1, \ldots, \lambda_n \in \mathbb{K} : \sum_{k=1}^{n} \lambda_k a_{i_k} = 0 \Rightarrow \forall k \in \{1, \ldots, n\} : \lambda_k = 0).$$

   Si $I$ est fini il suffit de vérifier la condition pour $n = card(I)$.
   Si une famille n'est pas libre alors elle est *liée*.
4. La famille $\mathcal{F}$ est une *base* de $E$ si elle est libre et génératrice.

**Exemple 2.2.1**

1. Le $\mathbb{R}-$ev $\mathbb{R}^n$ est de dimension finie $n$ (sur $\mathbb{R}$). La *base canonique* est la famille $\mathcal{C}_n = (e_i)_{1 \leqslant i \leqslant n}$ avec $e_i = (0, \ldots, 0, \underbrace{1}_{ième}, 0, \ldots, 0)$.
2. Le $\mathbb{K}-$ev $\mathbb{K}[X]$ est de dimension infinie (sur $\mathbb{K}$). Sa base canonique est la famille $(1, X, X^2, \ldots, X^n, \ldots)$

**Remarque 2.2.1**

1. Une sous-famille d'une famille libre est libre.
2. La famille vide est libre.
3. Une sur-famille d'une famille génératrice est génératrice.

**Définition 2.2.2** Un *sous-espace vectoriel* (*sev*) est un sous-ensemble *non vide* $F$ d'un ev $E$ tel que :

1. $\forall x, y \in F : x + y \in F$
2. $(\forall x \in F)(\forall \lambda \in \mathbb{K}) : \lambda x \in F$

**Remarque 2.2.2**

1. Une intersection de sevs est un sev. Une somme finie de sevs est un sev.
2. Une réunion de sevs n'est pas un sev.
3. Le plus petit sev d'un ev est $\{0\}$. Le plus grand est $E$.

**Définition 2.2.3** Soit $A$ une partie de $E$. Le *sev engendré* par $A$, noté $< A >$ est l'ensemble des combinaisons linéaires $\{\sum_{i=1}^{k} \lambda_i a_i : \lambda_i \in \mathbb{K}, a_i \in A, 1 \leqslant i \leqslant k, k \in \mathbb{N}^*\}$.

**Proposition 2.2.1** Le sev $< A >$ est le plus petit sev contenant $A$.

**Théorème 2.2.1 (de la base incomplète)** Soient $E$ un ev et $L$ (resp. $G$) une famille libre (resp. génératrice) de $E$ telle que $L \subseteq G$. Alors, il existe une famille $B$ de vecteurs de $E$ avec $L \subseteq B \subseteq G$, qui est une base de $E$.

**Proposition 2.2.2** Toutes les bases ont le même cardinal.

**Définition 2.2.4** Le cardinal d'une base de $E$ est la *dimension* de $E$.

**Remarque 2.2.3**

1. La dimension d'un sev $F$ est inférieure ou égale à la dimension de $E$.
2. Si $F$ est un sev de $E$ et si $\dim F = \dim E$ est finie alors $F = E$.
3. Si $\dim(F + G)$ est finie alors $\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$.

**Proposition 2.2.3** Soit $E$ un ev de dimension finie $n$.

1. Si $\mathcal{F}$ est une famille libre alors $card(\mathcal{F}) \leqslant n$. Si $card(\mathcal{F}) = n$ alors $\mathcal{F}$ est une base.
2. Si $\mathcal{F}$ est une famille génératrice alors $card(\mathcal{F}) \geqslant n$. Si $card(\mathcal{F}) = n$ alors $\mathcal{F}$ est une base.

**Définition 2.2.5** Soient $E$ un ev et $F_1, \ldots, F_p$ des sevs de $E$. L'ev $E$ est *somme directe* de $F_1, \ldots, F_p$, noté $E = \bigoplus_{i=1}^{p} F_i$, si tout $x$ de $E$ s'écrit de manière unique $x = x_1 + \cdots + x_p$ avec $x_i \in F_i$ pour $1 \leqslant i \leqslant p$.

**Proposition 2.2.4**

1. $E$ somme directe de $F_1, \ldots, F_p$ ssi $\left\{ \begin{array}{l} E = F_1 + \cdots + F_p \\ F_{i+1} \cap (F_1 + \cdots + F_i) = \{0\},\ 1 \leqslant i \leqslant p-1 \end{array} \right.$.
2. Si $p = 2$ et $\dim E = \dim F_1 + \dim F_2$ est finie alors C.S.S.E. :
   (a) $E = F_1 \oplus F_2$
   (b) $E = F_1 + F_2$
   (c) $F_1 \cap F_2 = \{0\}$

   Dans ce cas, la concaténation d'une base de $F_1$ et d'une base de $F_2$ produit une base de $E$.

**Définition 2.2.6** Soit $f \in L(E, F)$ (le $\mathbb{K}-$ev des *applications linéaires* de $E$ dans $F$).
- $\ker f = \{x \in E : f(x) = 0\} = f^{-1}(\{0\})$ est le *noyau* de $f$.
- $\operatorname{Im} f = \{y \in F : \exists x \in E, y = f(x)\} = f(E)$ est l'*image* de $f$.

**Remarque 2.2.4**

1. Si $f$ est une application linéaire alors $\ker f$ (resp. $\operatorname{Im} f$) est un sev de $E$ (resp. $F$). Le *rang* de $f$ noté $\operatorname{rg} f$ est $\dim \operatorname{Im} f$.
2. Si $F = \mathbb{K}$ alors $f$ est une *forme linéaire* et si $\dim E = n > 0$ alors

$$\left\{ \begin{array}{l} \dim \ker f = n-1 \text{ (hyperplan)} \\ \operatorname{Im} f = \mathbb{K} \end{array} \right. \text{ si } f \neq 0 \text{ ou bien } \left\{ \begin{array}{l} \ker f = E \\ \operatorname{Im} f = \{0\} \end{array} \right. \text{ si } f = 0.$$

**Théorème 2.2.2 (du rang)** Soient $E$ un ev de dimension finie et $f \in L(E, F)$. Alors

$$\dim E = \dim \ker f + \operatorname{rg} f.$$

**Exemple 2.2.2** Soit $p \in L(E)$ tel que $p \circ p = p$. On a $\dim E = \dim \ker p + \operatorname{rg} p$. Soit $x \in \ker p \cap \operatorname{Im} p$. Alors $p(x) = 0$ et $\exists x' \in E : p(x') = x$. Donc $p(p(x')) = 0 = p(x')$ *i.e.* $x = 0$. Par suite, $E = \ker p \oplus \operatorname{Im} p$. L'*endomorphisme* $p$ est le *projecteur* sur $\operatorname{Im} p$ parallèlement à $\ker p$.

**Proposition 2.2.5** Soient $E, F$ deux evs de *même* dimension *finie* et $f \in L(E, F)$. C.S.S.E. :

1. $f$ est injective ($\Leftrightarrow \ker f = \{0\}$)
2. $f$ est bijective
3. $f$ est surjective ($\Leftrightarrow \operatorname{rg} f = \dim F$).

**Remarque 2.2.5**

1. C'est faux si $\dim E$ est infinie.
2. Si $E$ et $F$ sont de même dimension finie et $f \in L(E, F)$, $g \in L(F, E)$ tels que $g \circ f = id_E$ alors $f$ est bijective et $g = f^{-1}$.

### 2.2.2 Définitions

Dans le reste du chapitre, $\mathbb{K}$ désigne un corps dans lequel $1 + 1 \neq 0$ (*i.e.* $\mathbb{K}$ n'est pas de *caractéristique* 2).

**Définition 2.2.7** Soient $E_1, \ldots, E_n, F$ des evs et $f : E_1 \times \cdots \times E_n \to F$. L'application $f$ est $n-$*linéaire* (ou *multilinéaire*) si $f$ est linéaire par rapport à la variable $i, 1 \leqslant i \leqslant n$ lorsque les $(n-1)$ restantes sont fixées *i.e.*
$(\forall i \in \{1, \ldots, n\})(\forall (x_1, \ldots, \widehat{x_i}, \ldots, x_n) \in E_1 \times \cdots \times \widehat{E_i} \times \cdots \times E_n)$ :

1. $\forall x, x' \in E_i : f(x_1, \ldots, x_{i-1}, x + x', x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n)$
$+f(x_1, \ldots, x_{i-1}, x', x_{i+1}, \ldots, x_n)$
2. $(\forall x \in E_i)(\forall \lambda \in \mathbb{K}) : f(x_1, \ldots, x_{i-1}, \lambda x, \ldots, x_n) = \lambda f(x_1, \ldots, x_{i-1}, x, \ldots, x_n)$.

Si $F = \mathbb{K}$ alors $f$ est une *forme $n-$linéaire*.

On note $L(E_1, \ldots, E_n; F)$ (resp. $L_n(E; F)$) l'ev des applications $n-$linéaires de $E_1 \times \cdots \times E_n$ (resp. $E^n$) dans $F$.

**Exemple 2.2.3**

1. Le *produit scalaire* $\begin{array}{ccc} \mathbb{R}^3 \times \mathbb{R}^3 & \to & \mathbb{R} \\ (x, y) & \mapsto & x \cdot y \end{array}$ est une forme bilinéaire.
2. Le *produit vectoriel* $\begin{array}{ccc} \mathbb{R}^3 \times \mathbb{R}^3 & \to & \mathbb{R}^3 \\ (x, y) & \mapsto & x \wedge y \end{array}$ est une application bilinéaire.
3. Le *produit mixte* $\begin{array}{ccc} \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 & \to & \mathbb{R} \\ (x, y, z) & \mapsto & x \cdot (y \wedge z) \end{array}$ est une forme trilinéaire.
4. Calculer $f(\sum_{i=1}^{n} \lambda_i x_i, \sum_{j=1}^{n} \mu_j x_j)$.

**Définition 2.2.8** Une application $f \in L_n(E; F)$ est *alternée* si

$$(\forall (x_1, \ldots, x_n) \in E^n)(\exists i \neq j : x_i = x_j) \Rightarrow f(x_1, \ldots, x_n) = 0.$$

**Lemme 2.2.1** Soit $f \in L_n(E; F)$. Alors $f$ est alternée ssi $(\forall x_1, \ldots, x_n \in E)(\forall 1 \leq i < j \leq n)$ :

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = -f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n). \quad (1)$$

**Dém.** :

($\Rightarrow$) Comme $f$ est alternée $f(x_1, \ldots, x_i + x_j, \ldots, x_j + x_i, \ldots, x_n) = 0$. Par suite,

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) + f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = 0.$$

($\Leftarrow$) Si $x_i = x_j$ alors $2f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = 0$. Comme $\mathbb{K}$ n'est pas de caractéristique 2, $f$ est alternée.

**Remarque 2.2.6** Quand la condition (1) est satisfaite, on dit aussi que $f$ est *antisymétrique*.

**Proposition 2.2.6** Soient $E, F$ deux evs et $f \in L_n(E; F)$. Alors $f$ est alternée ssi

$$\forall \sigma \in \mathfrak{S}_n : f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \epsilon(\sigma) f(x_1, \ldots, x_n).$$

**Dém.** :

($\Rightarrow$) Si $\sigma = \tau = (i\ j), i < j$ est une transposition alors

$$f(x_{\tau(1)}, \ldots, x_{\tau(n)}) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = \epsilon(\tau) f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n).$$

En décomposant, $\sigma$ en produit de transpositions et en raisonnant par récurrence sur le nombre de transpositions on obtient :

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \epsilon(\tau_1) f(x_{\tau_2 \cdots \tau_p(1)}, \ldots, x_{\tau_2 \cdots \tau_p(n)}) = \epsilon(\sigma) f(x_1, \ldots, x_n).$$

($\Leftarrow$) L'antisymétrie de $f$ est immédiate.

**Proposition 2.2.7** Soit $f \in L_n(E;F)$. Alors $f$ est alternée ssi

$$(\forall (x_1,\dots,x_n)\in E^n)(\forall(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n) : f(x_1,\dots,\overbrace{\sum_{j=1}^{n}\lambda_j x_j}^{iéme},\dots,x_n) = \lambda_i f(x_1,\dots,x_n).$$

**Dém.** :
($\Rightarrow$) immédiat.
($\Leftarrow$) $f(x_1,\dots,x_i,\dots,x_i,\dots,x_n) = f(x_1,\dots,x_i - x_i,\dots,x_i,\dots,x_n) = 0$ de sorte que $f$ est alternée.

**Corollaire 2.2.1** La valeur d'une application $n-$linéaire alternée en un $n-$uplet est inchangée lorsque l'on remplace un vecteur du $n-$uplet par la somme de ce vecteur et d'une combinaison linéaire des vecteurs restants du $n-$uplet.

**Corollaire 2.2.2** Soient $f \in L_n(E;F)$ alternée et $x_1,\dots,x_n \in E$. Alors

$$f(x_1,\dots,x_n) \neq 0 \Rightarrow (x_1,\dots,x_n) \text{ libre.}$$

**Dém.** : par contraposée.

**Proposition 2.2.8** Soient $(e_1,\dots,e_n)$ une base d'un ev $E$, $x_1,\dots,x_n \in E$ tels que $x_j = \sum_{i=1}^{n} x_{ij}e_i$ et $f \in L_n(E;F)$ alternée. Alors

$$f(x_1,\dots,x_n) = \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) x_{1\sigma(1)}\cdots x_{n\sigma(n)} f(e_1,\dots,e_n).$$

**Dém.** :

$$\begin{aligned} f(x_1,\dots,x_n) &= f(\sum_{i_1=1}^{n} x_{i_1 1}e_{i_1},\dots,\sum_{i_n=1}^{n} x_{i_n n}e_{i_n}) \\ &= \sum_{1\leqslant i_1,\dots,i_n\leqslant n} x_{i_1 1}\cdots x_{i_n n} f(e_{i_1},\dots,e_{i_n}) \\ &= \sum_{1\leqslant i_1\neq\cdots\neq i_n\leqslant n} x_{i_1 1}\cdots x_{i_n n} f(e_{i_1},\dots,e_{i_n}). \end{aligned}$$

car $f$ est alternée donc les seuls termes qui subsistent sont tels que $(i_1,\dots,i_n)$ est une permutation de $\{1,\dots,n\}$. Et dans ce cas, $f(e_{\sigma(1)},\dots,e_{\sigma(n)}) = \epsilon(\sigma) f(e_1,\dots,e_n)$. Ainsi,

$$f(x_1,\dots,x_n) = \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) x_{\sigma(1)1}\cdots x_{\sigma(n)n} f(e_1,\dots,e_n). \tag{2}$$

Cette dernière somme peut se réécrire :

$$f(x_1,\dots,x_n) = \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma^{-1}) x_{\sigma^{-1}(1)1}\cdots x_{\sigma^{-1}(n)n} f(e_1,\dots,e_n).$$

Maintenant, si $a_{\sigma^{-1}} := x_{\sigma^{-1}(1)1}\cdots x_{\sigma^{-1}(n)n}$ alors $a_{\sigma^{-1}} = x_{\sigma^{-1}(1)\sigma\sigma^{-1}(1)}\cdots x_{\sigma^{-1}(n)\sigma\sigma^{-1}(n)}$ et lorsque $j$ décrit $\{1,\dots,n\}$, $\sigma^{-1}(j)$ décrit « bijectivement » $\{1,\dots,n\}$. D'où $a_{\sigma^{-1}} = x_{1\sigma(1)}\cdots x_{n\sigma(n)}$. Finalement (2) se réécrit :

$$f(x_1,\dots,x_n) = \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) x_{1\sigma(1)}\cdots x_{n\sigma(n)} f(e_1,\dots,e_n).$$

**Définition 2.2.9** Le *déterminant de la famille* $(x_1, \ldots, x_n)$ *dans la base* $\mathcal{B} = (e_1, \ldots, e_n)$ est

$$\det_{\mathcal{B}}(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) x_{1\sigma(1)} \cdots x_{n\sigma(n)}.$$

**Remarque 2.2.7**

1. Le $\det_{\mathcal{B}}$ dépend de la base $\mathcal{B}$.
2. On a : $\det_{\mathcal{B}}(e_1, \ldots, e_n) = 1$.

**Théorème 2.2.3** Soient $E, F$ deux evs, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de $E$ et $f \in L_n(E; F)$ alternée. Alors $f$ est entièrement déterminée par sa valeur sur $(e_1, \ldots, e_n)$ et on a

$$f(x_1, \ldots, x_n) = \det_{\mathcal{B}}(x_1, \ldots, x_n) f(e_1, \ldots, e_n).$$

**Remarque 2.2.8** En particulier, on constate que si $F = \mathbb{K}$ alors toute forme $n-$linéaire alternée $f$ est un multiple de $\det_{\mathcal{B}}$.

**Proposition 2.2.9** Soient $E$ un $\mathbb{K}-$ev et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de $E$. Alors $\det_{\mathcal{B}}$ est une forme $n-$linéaire alternée.

**Dém.** : la multilinéarité est conséquence de la multilinéarité du produit dans $\mathbb{K}$ d'après (2).
On a :

$$\begin{aligned} \det_{\mathcal{B}}(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) &= \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) x_{1\sigma(1)} \cdots x_{j\sigma(i)} \cdots x_{i\sigma(j)} \cdots x_{n\sigma(n)} \\ &= \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) x_{1\sigma\tau(1)} \cdots x_{j\sigma\tau(j)} \cdots x_{i\sigma\tau(i)} \cdots x_{n\sigma\tau(n)} \end{aligned}$$

avec $\tau = (i\ j)$. Or, lorsque $\sigma$ décrit $\mathfrak{S}_n$, $\sigma\tau$ décrit (bijectivement) $\mathfrak{S}_n$. On peut ainsi remplacer $\sigma$ par $\sigma\tau$ dans la somme précedente. Comme $\tau^2 = Id$, on obtient :

$$\det_{\mathcal{B}}(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = -\det_{\mathcal{B}}(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)$$

car $\epsilon(\sigma\tau) = -\epsilon(\sigma)$.

**Remarque 2.2.9** Ainsi, il existe *bien* des formes (donc des applications) multilinéaires alternées (non triviales !). L'espace vectoriel de telles formes (resp. applications) est donc de dimension 1 (resp. $\dim F$).

**Théorème 2.2.4** La fonction $\det_{\mathcal{B}}$ est l'unique forme $n-$linéaire alternée qui prend la valeur 1 sur $(e_1, \ldots, e_n)$.

**Dém.** : le seul point à démontrer est l'unicité. Elle résulte du fait qu'une application $n-$linéaire alternée est entièrement déterminée par sa valeur sur $(e_1, \ldots, e_n)$.

### 2.2.3 Propriétés générales

**Proposition 2.2.10** Soient $E$ un $\mathbb{K}-$ev, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de $E$ et $(x_1, \ldots, x_n) \in E^n$. Alors $\det_{\mathcal{B}}(x_1, \ldots, x_n) \neq 0 \Leftrightarrow (x_1, \ldots, x_n)$ libre (*i.e.* $(x_1, \ldots, x_n)$ base de $E$).

**Dém.** :

($\Rightarrow$) déjà vu.

($\Leftarrow$) Notons $\mathcal{B}' = (x_1, \ldots, x_n)$. Alors $\det_{\mathcal{B}'}$ est une forme $n-$linéaire alternée multiple de $\det_{\mathcal{B}}$, plus précisément $\det_{\mathcal{B}'}(x_1, \ldots, x_n) = \det_{\mathcal{B}}(x_1, \ldots, x_n) \det_{\mathcal{B}'}(e_1, \ldots, e_n)$. En particulier, $\det_{\mathcal{B}}(x_1, \ldots, x_n) \neq 0$.

**Définition 2.2.10** Soit $A = (a_{ij})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$. Le *déterminant* de $A$ est

$$\det(A) = \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

**Proposition 2.2.11** Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors

$$\det(A) = \det(A^t).$$

**Dém.** : déjà vu sur les vecteurs.

**Proposition 2.2.12** Soient $A = (a_{ij})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de $\mathbb{K}^n$ et $x_j = \sum_{i=1}^{n} a_{ij} e_i$. Alors $\det(A) = \det_{\mathcal{B}}(x_1, \ldots, x_n)$.

**Remarque 2.2.10** $\det_{\mathcal{B}}(x_1, \ldots, x_n)$ est le déterminant dans la base $\mathcal{B}$ de la famille des vecteurs colonnes de $A$.

**Corollaire 2.2.3** Si $f$ est un endomorphisme de $E$ et si $A = mat(f, \mathcal{B})$ alors

$$\det(A) = \det_{\mathcal{B}}(f(e_1), \ldots, f(e_n)).$$

**Théorème 2.2.5** Soient $A, B \in \mathcal{M}_n(\mathbb{K})$. Alors

$$\det(AB) = \det(A)\det(B).$$

**Dém.** : fixons une base $\mathcal{B} = (e_1, \ldots, e_n)$ de $\mathbb{K}^n$. Soit $f$ (resp. $g$) l'endomorphisme de $\mathbb{K}^n$ tel que $A = mat(f, \mathcal{B})$ (resp. $B = mat(g, \mathcal{B})$). Alors $AB = mat(f \circ g, \mathcal{B})$. Considérons $\varphi : (\mathbb{K}^n)^n \to \mathbb{K}$ défini par

$$\varphi(x_1, \ldots, x_n) = \det_{\mathcal{B}}(f(x_1), \ldots, f(x_n)).$$

Alors $\varphi$ est $n-$linéaire alternée donc $\varphi(x_1, \ldots, x_n) = \det_{\mathcal{B}}(x_1, \ldots, x_n)\varphi(e_1, \ldots, e_n)$. Or $\varphi(e_1, \ldots, e_n) = \det_{\mathcal{B}}(f(e_1), \ldots, f(e_n)) = \det(A)$. Évaluons maintenant $\varphi$ en $(g(e_1), \ldots, g(e_n))$, il vient :

$$\varphi(g(e_1), \ldots, g(e_n)) = \det_{\mathcal{B}}(f \circ g(e_1), \ldots f \circ g(e_n)) = \det(AB) = \det(B)\det(A).$$

**Corollaire 2.2.4** Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors

$$A \text{ inversible ssi } \det(A) \neq 0 \text{ et dans ce cas } \det(A^{-1}) = \frac{1}{\det(A)}.$$

**Dém.** :

($\Rightarrow$) Comme $A$ est inversible, il existe une matrice $B$ telle que $AB = I_n$. Mais alors, $\det(A)\det(B) = 1$. D'où $\det(A) \neq 0$ et $\det(B) = \det(A^{-1}) = \frac{1}{\det(A)}$.

($\Leftarrow$) Notons $f$ l'endomorphisme de $\mathbb{K}^n$ tel que $A = mat(f, \mathcal{C}_n)$. Alors $\det(A) = \det_{\mathcal{C}_n}(f(e_1), \ldots, f(e_n))$. Par suite, $(f(e_1), \ldots, f(e_n))$ est libre donc c'est une base de $\mathbb{K}^n$. Dès lors, $f$ est inversible et il existe $g \in L(\mathbb{K}^n)$ tel que $f \circ g = id_{\mathbb{K}^n}$. On conclut que $A$ est inversible.

**Proposition 2.2.13** Soient $f$ un endomorphisme d'un ev $E$ et $\mathcal{B}, \mathcal{B}'$ deux bases de $E$. Alors $\det(mat(f, \mathcal{B})) = \det(mat(f, \mathcal{B}'))$.

**Dém.** : en effet, $A' = P^{-1}AP$ où $P = mat(id_E, \mathcal{B}', \mathcal{B})$ est la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Donc $\det(A') = \det(A)$.

**Définition 2.2.11** Le *déterminant* d'un endomorphisme $f$ est $\det(A)$ où $A$ désigne la matrice de $f$ dans une base de $E$. On note

$$\det(f) = \det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

**Proposition 2.2.14 (définition intrinsèque du déterminant)** Soit $f \in L(E)$ avec $\dim E = n$. Alors, pour tout $\varphi \in L_n(E;\mathbb{K})$ alternée on a :

$$\varphi(f(x_1), \ldots, f(x_n)) = \det(f)\varphi(x_1, \ldots, x_n).$$

**Dém.** : on a déjà vu que l'espace des *formes* linéaires alternées $\mathcal{A}_n(E;\mathbb{K})$ est de dimension 1. Si $\psi$ désigne l'endomorphisme $\varphi \mapsto \psi(\varphi) = \varphi(f, \ldots, f)$ alors $\psi$ est une homothétie de $\mathcal{A}_n(E;\mathbb{K})$ *i.e.* $(\exists \alpha \in \mathbb{K})(\forall \varphi \in \mathcal{A}_n(E;\mathbb{K})) : \psi(\varphi) = \alpha\varphi$. Maintenant, soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de $E$. Si $\varphi = \det_{\mathcal{B}}$ alors $\det_{\mathcal{B}}(f(e_1), \ldots, f(e_n)) = \alpha \det_{\mathcal{B}}(e_1, \ldots, e_n)$ *i.e.* $\alpha = \det(f)$.

### 2.2.4 Calculs pratiques

**Lemme 2.2.2** Soit $A \in \mathcal{M}_n(\mathbb{K})$. On a :

$$\det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1i} + \sum_{j=1, j\neq i}^{n} \lambda_j a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{ni} + \sum_{j=1, j\neq i}^{n} \lambda_j a_{nj} & \cdots & a_{nn} \end{vmatrix}.$$

De plus :

$$\begin{vmatrix} a_{11} & \cdots & a_{1j-1} & 0 & a_{1j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i-11} & \cdots & a_{i-1j-1} & 0 & a_{i-1j+1} & \cdots & a_{i-1n} \\ a_{i1} & \cdots & a_{ij-1} & 1 & a_{ij+1} & \cdots & a_{in} \\ a_{i+11} & \cdots & a_{i+1j-1} & 0 & a_{i+1j+1} & \cdots & a_{i+1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj-1} & 0 & a_{nj+1} & \cdots & a_{nn} \end{vmatrix}$$

$$= (-1)^{i+j} \begin{vmatrix} a_{11} & \cdots & a_{1j-1} & a_{1j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-11} & \cdots & a_{i-1j-1} & a_{i-1j+1} & \cdots & a_{i-1n} \\ a_{i+11} & \cdots & a_{i+1j-1} & a_{i+1j+1} & \cdots & a_{i+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj-1} & a_{nj+1} & \cdots & a_{nn} \end{vmatrix}.$$

On a des propriétés analogues en permutant lignes et colonnes.

Soient $A \in \mathcal{M}_n(\mathbb{K})$ et $1 \leqslant i, j \leqslant n$. Notons $A_{i,j}$ la matrice d'ordre $n-1$ obtenue en supprimant la $i-$ème ligne et la $j-$ème colonne de $A$.

**Proposition 2.2.15 (Développement suivant une colonne)** Soit $1 \leqslant j \leqslant n$. Alors

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{i,j}).$$

**Dém.** : on va traiter le cas $j = 1$. Notons $x_k$ le vecteur associé à la $k-$ième colonne de $A$. Alors $x_1 = \sum_{i=1}^{n} a_{i1} e_i$ où $(e_1, \ldots, e_n)$ désigne la base canonique $\mathcal{C}_n$ de $\mathbb{K}^n$. On a :

$$\det(A) = \det_{\mathcal{C}_n}(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_{i1} \det_{\mathcal{C}_n}(e_i, x_2, \ldots, x_n)$$

Or, $\det_{\mathcal{C}_n}(e_i, x_2, \ldots, x_n) = (-1)^{i+1} \det(A_{i,1})$ d'après le lemme.

**Corollaire 2.2.5 (Développement suivant une ligne)** Soit $1 \leqslant i \leqslant n$. Alors

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{i,j}).$$

**Dém.** : comme $\det(A) = \det({}^tA)$, il suffit d'appliquer la proposition précédente à ${}^tA$.

**Exemple 2.2.4**

1. $$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

2. $$\begin{vmatrix} 2 & 1 & -1 \\ -1 & 0 & 1 \\ 5 & -3 & -2 \end{vmatrix} = \begin{vmatrix} 2 & 1 & -1 \\ 0 & 0 & 1 \\ 0 & -3 & -2 \end{vmatrix} = 2 \begin{vmatrix} 0 & 1 \\ -3 & -2 \end{vmatrix} = 6.$$

**Proposition 2.2.16** Soit $A \in \mathcal{M}_n(\mathbb{K})$ triangulaire. Alors

$$\det(A) = \prod_{i=1}^{n} a_{ii}.$$

**Dém.** : on peut supposer $A$ triangulaire supérieure. En développant le déterminant suivant la 1ère colonne, on obtient $\det(A) = a_{11} \det(A_{11})$. Or, $A_{11}$ est une matrice triangulaire supérieure d'ordre $n - 1$. D'où le résultat par récurrence.

**Remarque 2.2.11** La formule s'applique en particulier si $A$ est diagonale.

**Exemple 2.2.5**

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{vmatrix} = \begin{vmatrix} 4 & 0 & 0 \\ 5 & 1 & 0 \\ 2 & -3 & 6 \end{vmatrix} = 24.$$

# 3 Dualité

## 3.1 Espace dual

Soit $E$ un $\mathbb{K}-$ev.

**Définition 3.1.1** Le *dual* (*algébrique*) de $E$ noté $E^*$ est l'espace vectoriel $L_{\mathbb{K}}(E, \mathbb{K})$ des formes linéaires sur $E$.

**Rappel** :

$$(\forall x \in E)(\forall(\lambda_i)_{1\leqslant i\leqslant n} \subset \mathbb{K})(\forall(f_i)_{1\leqslant i\leqslant n} \subset E^*) : (\sum_{i=1}^{n} \lambda_i f_i)(x) = \sum_{i=1}^{n} \lambda_i f_i(x).$$

**Exemple 3.1.1**

1. Soient $(e_1, \ldots, e_n)$ une base de $E$ de dimension $n$ et $1 \leqslant i \leqslant n$. Considérons
$$\begin{array}{rccc} e_i^* : & E & \to & \mathbb{K} \\ & x & \mapsto & x_i \end{array}.$$
Cette application est bien définie car l'écriture d'un vecteur $x$ suivant une base de $E$ est unique : $x = \sum_{j=1}^{n} x_j e_j$.
La fonction $e_i^*$ est linéaire. En effet, soient $x, y \in E$ alors $x+y = \sum_{j=1}^{n}(x_j+y_j)e_j$ par unicité de la décomposition sur une base. Par suite, $e_i^*(x+y) = e_i^*(x) + e_i^*(y)$.
Pour la même raison, $e_i^*(\lambda x) = \lambda e_i^*(x)$. Par ailleurs, $e_i^*(e_j) = \delta_{ij}$.
2. Soient $E = \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors
$$\begin{array}{rccc} \varphi_a : & E & \to & \mathbb{K} \\ & P & \mapsto & P(a) \end{array}$$
est une forme linéaire. C'est aussi un morphisme d'anneaux. Son noyau est un idéal *maximal* $\mathcal{M}_a$ de $\mathbb{K}[X]$, $\mathcal{M}_a = (X-a)$.
Par ailleurs, si $a \neq b$ alors $(\varphi_a, \varphi_b)$ est libre. En effet, soient $\alpha, \beta \in \mathbb{K}$ tels que $\alpha\varphi_a + \beta\varphi_b = 0$. Posons $P = X - a$, on obtient $\alpha(a-a) + \beta(a-b) = 0$. Donc $\beta = 0$. Mais alors $\alpha = 0$. On montre plus généralement que $(\varphi_a)_{a\in\mathbb{K}}$ est libre.
3. Soit $E = C([a,b], \mathbb{R})$. Alors
$$\begin{array}{rccc} I_{a,b} : & E & \to & \mathbb{R} \\ & f & \mapsto & \int_a^b f(t)dt \end{array}$$
est une forme linéaire sur $E$.

**Théorème 3.1.1** Soient $E$ un ev de dimension $n$ et $(e_1, \ldots, e_n)$ une base de $E$. Alors $(e_1^*, \ldots, e_n^*)$ est une base de $E^*$ et toute forme linéaire $f \in E^*$ s'écrit de manière unique dans cette base :

$$f = \sum_{i=1}^{n} f(e_i) e_i^*.$$

**Dém.** : soit $x \in E$ alors $x = \sum_{i=1}^{n} x_i e_i$. Donc $f(x) = \sum_{i=1}^{n} x_i f(e_i) = \sum_{i=1}^{n} f(e_i) e_i^*(x)$. Ainsi,

$$f = \sum_{i=1}^{n} f(e_i) e_i^* \tag{3}$$

D'autre part, si $\sum_{i=1}^{n} \lambda_i e_i^* = 0$ alors pour $1 \leqslant j \leqslant n$, $\sum_{i=1}^{n} \lambda_i e_i^*(e_j) = \sum_{i=1}^{n} \lambda_i \delta_{ij} = \lambda_j = 0$. Donc $(e_i^*)_{1\leqslant i\leqslant n}$ est libre et la décomposition (3) est unique.

**Corollaire 3.1.1** Si $\dim E = n$ alors $\dim E^* = n$.

**Définition 3.1.2** Soit $(e_1, \ldots, e_n)$ (resp. $(f_1, \ldots, f_n)$) une base de $E$ (resp. $E^*$). Ces bases sont *duales* si $f_i(e_j) = \delta_{ij}$.

**Remarque 3.1.1** Si $\dim E = +\infty$ alors $E$ et $E^*$ *ne* sont *pas* isomorphes. Par exemple, on peut poser $E = \mathbb{R}[X]$ ; on a notamment $(\varphi_a)_{a\in\mathbb{R}}$ libre mais non dénombrable.

## 3.2 Transposée

**Rappel** : soient $E, F, G$ trois $\mathbb{K}-$evs. Soient $f_1, f_2 \in L(E,F)$, $g_1, g_2 \in L(F,G)$ et $\lambda \in \mathbb{K}$. Alors

$$\begin{aligned} g_1 \circ (f_1 + f_2) &= g_1 \circ f_1 + g_1 \circ f_2 \quad (4) \\ (g_1 + g_2) \circ f_1 &= g_1 \circ f_1 + g_2 \circ f_1 \quad (5) \\ \lambda(g_1 \circ f_1) &= (\lambda g_1) \circ f_1 = g_1 \circ (\lambda f_1) \quad (6) \end{aligned}$$

**Remarque 3.2.1** Ces propriétés sont bien connues en dimension finie en calcul matriciel et traduisent la bilinéarité du produit matriciel.

**Définition 3.2.1** Soient $E, F$ deux evs et $f \in L(E,F)$. La *transposée* de $f$, notée ${}^t f$, est l'application de $F^*$ dans $E^*$ définie par ${}^t f(y^*) = y^* \circ f$.

**Remarque 3.2.2** La transposée est définie en dimension quelconque.

**Proposition 3.2.1**

1. Si $f \in L(E,F)$ alors ${}^t f \in L(F^*, E^*)$.
2. ${}^t \in L(L(E,F), L(F^*,E^*))$.

**Proposition 3.2.2** Si $\dim F = m$ est finie et si $f \in L(E,F)$ alors $\mathrm{rg}\,({}^t f) = \mathrm{rg}\,(f)$.

**Dém.** : comme ${}^t f$ est linéaire et que $F^*$ est de dimension finie, on a :

$$\mathrm{rg}\,({}^t f) = \dim(F^*) - \dim(\ker({}^t f)).$$

Soit $y^* \in F^*$. Alors

$$\begin{aligned} y^* \in \ker({}^t f) &\Leftrightarrow {}^t f(y^*) = 0 \\ &\Leftrightarrow \mathrm{Im}\,(f) \subseteq \ker(y^*). \end{aligned}$$

Ainsi, $\ker({}^t f) = \{y^* \in F^* : \mathrm{Im}\,(f) \subseteq \ker(y^*)\}$. Soit $(f_1, \ldots, f_r)$ une base de $\mathrm{Im}\, f$ avec $r = \mathrm{rg}\,(f)$. Complètons cette famille *libre* en une base $(f_1, \ldots, f_r, f_{r+1}, \ldots, f_m)$ de $F$. Alors $(f_1^*, \ldots, f_m^*)$ est une base de $F^*$ (duale de $(f_1, \ldots, f_m)$). Par conséquent, tout $y^* \in F^*$ se décompose de manière unique dans cette base : $y^* = \sum_{i=1}^{m} \alpha_i f_i^*$ (en fait, $\alpha_i = y^*(f_i)$). Il vient :

$$\begin{aligned} y^* \in \ker({}^t f) &\Leftrightarrow \mathrm{Im}\,(f) \subseteq \ker(y^*) \\ &\Leftrightarrow < f_1, \ldots, f_r > \subseteq \ker(y^*) \\ &\Leftrightarrow y^*(f_i) = 0 \text{ pour } 1 \leq i \leq r \\ &\Leftrightarrow y^* = \sum_{i=r+1}^{m} y^*(f_i) f_i^* \\ &\Leftrightarrow y^* \in < f_{r+1}^*, \ldots, f_m^* > . \end{aligned}$$

Ainsi $\dim(\ker({}^t f)) = m - (r+1) + 1 = m - \mathrm{rg}\,(f)$ et finalement $\mathrm{rg}\,({}^t f) = m - (m - \mathrm{rg}\,(f))$.

**Proposition 3.2.3** On suppose $\dim E = n$ et $\dim F = m$. Soit $A = mat(f, (e_i), (f_j))$ et $B = mat({}^t f, (f_j^*), (e_i^*))$. Alors

$$B = {}^t A.$$

**Dém.** : calculons la $j-$ième colonne de $B$. C'est le vecteur colonne ${}^t f(f_j^*)$ décomposé dans la base $(e_i^*)$. Si ${}^t f(f_j^*) = \sum_{k=1}^{n} b_{kj} e_k^*$ alors $b_{kj}$ est le coefficient sur la $k-$ième ligne de la $j-$ième colonne de $B$. Comme $(e_i^*)$ est duale de $(e_i)$, on a $b_{ij} = {}^t f(f_j^*)(e_i)$. Autrement dit, $b_{ij} = f_j^*(f(e_i))$. Maintenant, $f(e_i) = \sum_{l=1}^{m} a_{li} f_l$ de sorte que $b_{ij} = \sum_{l=1}^{m} a_{li} f_j^*(f_l) = \sum_{l=1}^{m} a_{li} \delta_{jl} = a_{ji}$. D'où le résultat.

**Corollaire 3.2.1** Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$. Alors $\mathrm{rg}\,(A) = \mathrm{rg}\,({}^tA)$.

**Proposition 3.2.4** La transposée vérifie :

$$\begin{aligned} {}^t(g \circ f) &= {}^tf \circ {}^tg & (7)\\ \text{si } f \text{ est un isomorphisme alors } ({}^tf)^{-1} &= {}^t(f^{-1}). & (8) \end{aligned}$$

**Dém.** : Soit $z^* \in G^*$. Alors ${}^t(g\circ f)(z^*) = z^*(g\circ f) = z^*\circ g\circ f = (z^*\circ g)\circ f = {}^tg(z^*)\circ f = {}^tf\circ {}^tg(z^*)$.

Soit $g$ l'isomorphisme réciproque de $f$. Alors ${}^t(g\circ f) = {}^tid_E = id_{E^*}$. Or, d'après (7), ${}^t(g\circ f) = {}^tf\circ {}^tg$. On montrerait de même que ${}^tg\circ {}^tf = id_{F^*}$. D'où l'on tire ${}^tg = {}^t(f^{-1}) = ({}^tf)^{-1}$.

**Remarque 3.2.3** ${}^t({}^tf) : E^{**} \to F^{**}$ ($E^{**}$ *bidual* de $E$), donc en général ${}^t({}^tf) \neq f$ sauf en dimension finie pour laquelle ces applications s'identifient. En effet, l'application

$$\begin{array}{ccc} E & \to & E^{**} \\ x & \mapsto & x^{**} = \left\{ \begin{array}{ccc} E^* & \to & \mathbb{K} \\ y^* & \mapsto & y^*(x) \end{array} \right\} \end{array}$$

est injective. Donc surjective en dimension finie. Ainsi, on identifie $x$ et $x^{**}$. Maintenant, soit $f \in L(E,F)$ avec $\dim E$, $\dim F$ finis et $x^{**} \in E^{**}$. Alors

$${}^t({}^tf)(x) \equiv x^{**}\circ {}^tf = \{y^* \mapsto x^{**}({}^tf(y^*)) = x^{**}(y^*\circ f)\} = \{y^* \mapsto y^*(f(x))\} = f(x)^{**} \equiv f(x).$$

**Corollaire 3.2.2** Soient $A, B \in \mathcal{M}_n(\mathbb{K})$. Alors :

1. ${}^t(A+B) = {}^tA + {}^tB$
2. ${}^t(\lambda A) = \lambda {}^tA$
3. ${}^t(AB) = {}^tB\,{}^tA$
4. ${}^t({}^tA) = A$
5. ${}^t(A^{-1}) = ({}^tA)^{-1}$ si $A$ est inversible.

## 3.3 Orthogonalité

Soient $E$ un $\mathbb{K}-$ev et $E^*$ son dual.

**Définition 3.3.1** Les vecteurs $x \in E$ et $y^* \in E^*$ sont *orthogonaux* si $y^*(x) = 0$.

**Exemple 3.3.1** $e_i$ et $e_j^*$ sont orthogonaux ssi $i \neq j$.

**Définition 3.3.2** Soit $F \subseteq E$ (resp. $F^* \subseteq E^*$). L'*orthogonal* de $F$ (resp. $F^*$), noté $F^\perp$ (resp. $F^{*\circ}$) est l'ensemble des $y^* \in E^*$ (resp. $x \in E$) orthogonaux à tous les vecteurs de $F$ (resp. $F^*$) :

$$\begin{aligned} F^\perp &= \{y^* \in E^* : \forall x \in F, y^*(x) = 0\} \\ F^{*\circ} &= \{x \in E : \forall y^* \in F^*, y^*(x) = 0\} \end{aligned}$$

**Exemple 3.3.2** $\{0\}^\perp = E^*$ et $\{0^*\}^\circ = E$.

**Proposition 3.3.1** Si $\dim E = n$ et si $F$ (resp. $G$) est un sev de $E$ (resp. $E^*$). Alors :

$$\begin{aligned} \dim F + \dim F^\perp &= n \\ \dim G + \dim G^\circ &= n. \end{aligned}$$

**Dém.** : soit $(e_1, \ldots, e_p)$ une base de $F$. Complètons cette famille en une base $(e_1, \ldots, e_p, e_{p+1}, \ldots, e_n)$ de $E$. Maintenant :

$$\begin{aligned} y^* \in F^\perp &\Leftrightarrow F \subseteq \ker(y^*) \\ &\Leftrightarrow y^*(e_i) = 0 \text{ pour } 1 \leq i \leq p \\ &\Leftrightarrow y^* = \sum_{i=p+1}^{n} \alpha_i e_i^*, (\alpha_i)_{p+1 \leq i \leq n} \subset \mathbb{K} \\ &\Leftrightarrow y^* \in < e_{p+1}^*, \ldots, e_n^* > . \end{aligned}$$

D'où $\dim(F^\perp) = n - (p+1) + 1 = n - p$.

On démontre la seconde égalité de manière analogue.

**Corollaire 3.3.1** Si $F$ est un sev de $E$ de dimension $n$ alors $(F^\perp)^\circ = F$.

**Dém.** : soit $x \in F$. Alors, $\forall y^* \in F^\perp$, $y^*(x) = 0$. Donc $x \in (F^\perp)^\perp$. Ainsi, $F \subseteq (F^\perp)^\circ$. Comme $\dim((F^\perp)^\circ) = \dim(F)$, on conclut que $(F^\perp)^\circ = F$.

**Proposition 3.3.2** Soit $f \in L(E, F)$. Alors

$$(\operatorname{Im} f)^\perp = \ker({}^t f).$$

**Dém.** : soit $y^* \in \operatorname{Im}(f)^\perp$ *i.e.* $\forall x \in E : y^*(f(x)) = 0$.

$$\begin{aligned} \forall x \in E : y^*(f(x)) = 0 &\Leftrightarrow \forall x \in E : (y^* \circ f)(x) = 0 \\ &\Leftrightarrow \forall x \in E :^t f(y^*)(x) = 0 \\ &\Leftrightarrow {}^t f(y^*) = 0 \\ &\Leftrightarrow y^* \in \ker({}^t f). \end{aligned}$$

**Proposition 3.3.3** $\operatorname{Im}({}^t f) \subseteq \ker(f)^\perp$.

**Dém.** : soit $x^* \in \operatorname{Im}({}^t f)$ *i.e.* $\exists y^* \in F^* :^t f(y^*) = x^*$. Soit $x' \in \ker(f)$. Alors :

$$x^*(x') =^t f(y^*)(x') = y^* \circ f(x') = y^*(f(x')) = 0.$$

Et $x^* \in \ker(f)^\perp$.

**Remarque 3.3.1** Si $\dim E = n$ et $\dim F$ sont finis alors

$$\operatorname{rg}({}^t f) = \operatorname{rg}(f) = n - \dim(\ker(f)) = \dim(\ker(f)^\perp).$$

# 4 Espaces euclidiens et hermitiens

## 4.1 Formes bilinéaires et sesquilinéaires

**Définition 4.1.1** Soient $E, F, G$ trois $\mathbb{K}-$evs et $f : E \times F \to G$. L'application $f$ est *bilinéaire* si $(\forall x, x' \in E)(\forall y, y' \in F)(\forall \lambda, \in \mathbb{K})$ :

$$f(x + x', y) = f(x, y) + f(x', y) \quad (9)$$
$$f(x, y + y') = f(x, y) + f(x, y') \quad (10)$$
$$f(\lambda x, y) = \lambda f(x, y) \quad (11)$$
$$f(x, \lambda y) = \lambda f(x, y) \quad (12)$$

Si $\mathbb{K} = \mathbb{C}$ alors $f$ est *sesquilinéaire* si $f$ vérifie (9)-(11) et

$$f(x, \lambda y) = \bar{\lambda} f(x, y) \quad (13)$$

Si $G = \mathbb{K}$ alors $f$ est une *forme* bilinéaire (ou sesquilinéaire).

Dans la suite, on se limitera à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

**Exemple 4.1.1**

1. $E = F = G = \mathbb{K}$, $\begin{array}{ccc} \mathbb{K}\times\mathbb{K} & \to & \mathbb{K} \\ (x,y) & \mapsto & xy \end{array}$ est bilinéaire.
2. $E = F = G = L(V)$ avec $V$ un $\mathbb{K}-$ev., $\begin{array}{ccc} L(V)^2 & \to & L(V) \\ (f,g) & \mapsto & f\circ g \end{array}$ est bilinéaire.
3. $E = F = C([a,b],\mathbb{C})$, $\begin{array}{ccc} C([a,b],\mathbb{C})^2 & \to & \mathbb{C} \\ (f,g) & \mapsto & \int_a^b f(t)g(t)dt \end{array}$ est bilinéaire tandis que

$$\begin{array}{ccc} C([a,b],\mathbb{C})^2 & \to & \mathbb{C} \\ (f,g) & \mapsto & \int_a^b f(t)\bar{g}(t)dt \end{array}$$

est sesquilinéaire.

4. $E = F = \mathbb{K}^n \cong \mathcal{M}_{n,1}(\mathbb{K})$, $\begin{array}{ccc} \mathbb{K}^n\times\mathbb{K}^n & \to & \mathbb{K} \\ (x,y) & \mapsto & {}^tXY = {}^tYX \end{array}$ est bilinéaire tandis que

$$\begin{array}{ccc} \mathbb{C}^n\times\mathbb{C}^n & \to & \mathbb{C} \\ (x,y) & \mapsto & {}^tX\bar{Y} = Y^*X \end{array}$$

est sesquilinéaire (on a noté $Y^* = {}^t\bar{Y}$).

**Proposition 4.1.1** Soient $E, F$ deux evs sur $\mathbb{R}$ (resp. $\mathbb{C}$), $(a_1,\dots,a_n)$ une base de $E$, $(b_1,\dots,b_m)$ une base de $F$ et $f$ une forme bilinéaire (resp. sesquilinéaire) sur $E\times F$. On pose

$$A = (f(a_i,b_j))_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m}.$$

Si $x = \sum_{i=1}^n x_i a_i \in E$ et $y = \sum_{j=1}^m y_j b_j$ alors

$$f(x,y) = {}^tXAY$$

avec $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ (resp.

$$f(x,y) = {}^tXA\bar{Y} = Y^{*t}AX$$

avec $Y^* = (\bar{y}_1 \ \cdots \ \bar{y}_m)$).

**Dém.** : on va démontrer le cas sesquilinéaire. On a :

$$\begin{aligned} f(x,y) &= f(\sum_{i=1}^n x_i a_i, \sum_{j=1}^m y_j b_j) \\ &= \sum_{j=1}^m \bar{y}_j f(\sum_{i=1}^n x_i a_i, b_j) \\ &= \sum_{j=1}^m \bar{y}_j (\sum_{i=1}^n x_i f(a_i,b_j)) \\ &= \sum_{j=1}^m \bar{y}_j (\sum_{i=1}^n f(a_i,b_j)x_i) \\ &= Y^{*t}AX. \end{aligned}$$

**Remarque 4.1.1** Dans la cas réel, on a aussi $f(x,y) = {}^tY^tAX$ qui est l'expression analogue du cas sesquilinéaire.

**Définition 4.1.2** La matrice $A$ ci-dessus est la *matrice* de $f$ (dans les bases $(a_i)_{1\leqslant i\leqslant n}$ de $E$ et $(b_j)_{1\leqslant j\leqslant m}$ de $F$). On notera $A = mat_{(a_i)_{1\leqslant i\leqslant n},(b_j)_{1\leqslant j\leqslant m}}(f)$.

**Corollaire 4.1.1** Si $M \in \mathcal{M}_{n,m}(\mathbb{K})$ est telle que

$$\forall (x,y) \in E\times F : f(x,y) = {}^tXMY \text{ (resp. } {}^tXM\bar{Y} = Y^{*t}MX)$$

alors $M$ est la matrice de $f$ où $X$ (resp. $Y$) désigne la matrice colonne des compasantes de $x$ (resp. $y$) décomposé dans la base $(a_i)$ (resp. $(b_j)$).

**Dém.** : en effet, dans le cas complexe :

$$f(a_i,b_j) = \underbrace{\begin{pmatrix} 0 & \cdots & 0 & \overbrace{1}^{j} & 0 & \cdots & 0 \end{pmatrix}}_{b_j} {}^tM \left.\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1\}i \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right\} a_i = ({}^tM)_{ji} = M_{ij}$$

**Proposition 4.1.2** Soient $E, F$ deux evs de dimension finie sur $\mathbb{R}$ (resp. $\mathbb{C}$), $f$ une forme bilinéaire (resp. sesquilinéaire) sur $E\times F$, $A$ la matrice de $f$ relativement à des bases de $E$ et $F$ respectivement et $P$ (resp. $Q$) une matrice de changement de base dans $E$ (resp. $F$). Alors la matrice de $f$ dans les nouvelles bases est :

$$A' = {}^tPAQ \text{ (resp. } {}^tA' = Q^{*t}AP \text{ ou } A' = {}^tPA\bar{Q}).$$

**Dém.** : On a : $X = PX'$ et $Y = QY'$. Donc

$$f(x,y) = Y^{*t}AX = (QY')^{*t}A(PX') = Y'^{*}Q^{*t}APX' = Y'^{*t}A'X'.$$

**Définition 4.1.3** Soit $f : E\times E \to \mathbb{K}$. L'application $f$ est :
- *bilinéaire symétrique* si $f$ est bilinéaire et si $\forall x,y \in E : f(y,x) = f(x,y)$
- *hermitienne* si $f$ est sesquilinéaire et si $\forall x,y \in E : f(y,x) = \overline{f(x,y)}$.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ (resp. $\mathcal{M}_n(\mathbb{C})$). La matrice $A$ est *symétrique* (resp. *hermitienne*) si ${}^tA = A$ (resp. $A^* := {}^t\bar{A} = A$).

**Proposition 4.1.3**

$$f \text{ est symétrique} \Leftrightarrow A \text{ est symétrique}$$
$$f \text{ est hermitienne} \Leftrightarrow A \text{ est hermitienne.}$$

**Dém.** :

($\Rightarrow$) facile.

($\Leftarrow$) On le démontre dans le cas complexe. Soient $x,y \in E$. On a :

$$\begin{aligned} f(y,x) &= X^{*t}AY \\ &= X^*\bar{A}Y \\ &= ({}^tAX)^*Y \\ &= {}^tY\overline{{}^tAX} \\ &= \overline{Y^{*t}AX} \\ &= \overline{f(x,y)}. \end{aligned}$$

**Proposition 4.1.4** Soit $f : E \times E \to \mathbb{K}$ bilinéaire. Pour $x \in E$ fixé, notons $f(x,\cdot)$ (resp. $f(\cdot,x)$) l'application *partielle* de $E$ dans $\mathbb{K}$ définie par $f(x,\cdot)(y) = f(x,y)$ (resp. $f(\cdot,x)(y) = f(y,x)$). Alors $f(x,\cdot), f(\cdot,x) \in E^*$ et $x \mapsto f(x,\cdot)$ et $x \mapsto f(\cdot,x)$ sont linéaires de $E$ dans $E^*$.

**Remarque 4.1.2** Si $f$ est hermitienne alors $f(\cdot,x) \in E^*$ mais $f(x,\cdot)$ n'est plus linéaire ; elle est *semi-linéaire i.e.* $f(x,\lambda y) = \bar{\lambda} f(x,y)$.

**Lemme 4.1.1** Soient $E$ un $\mathbb{K}-$ev (resp. $\mathbb{C}-$ev) et $f$ une forme bilinéaire symétrique (resp. hermitienne). Alors $A = \{x \in E : f(x,\cdot) = 0\}$ et $B = \{x \in E : f(\cdot,x) = 0\}$ sont égaux et forment un sev de $E$.

**Dém.** : si $f$ est symétrique (resp. hermitienne) alors $f(x,y) = f(y,x)$ (resp. $f(x,y) = \overline{f(y,x)}$). Dès lors, $f(x,y) = 0 \Leftrightarrow f(y,x) = 0$.

**Définition 4.1.4** Soit $f$ une forme bilinéaire symétrique (resp. hermitienne). Le *noyau* de $f$ est l'ensemble $\{x \in E : f(x,\cdot) = 0\}$. Si le noyau est réduit à $\{0\}$ alors $f$ est *non dégénérée*.

**Remarque 4.1.3** $x \in$ noyau de $f \Leftrightarrow \forall y \in E : f(x,y) = 0$.

**Exemple 4.1.2**

1. Le produit scalaire euclidien et le produit scalaire hermitien sont non dégénérés.
2. Soit $f((x_1,y_1),(x_2,y_2)) = x_1x_2 - y_1y_2$. Alors $f$ est non dégénérée.

**Théorème 4.1.1** Soient $E$ un ev sur $\mathbb{R}$ ou $\mathbb{C}$, $\mathcal{B} = (e_1,\ldots,e_n)$ une base de $E$ et $f : E \times E \to \mathbb{K}$ une forme bilinéaire symétrique (resp. hermitienne). CSSE :

1. $f$ est non dégénérée
2. $\varphi : x \mapsto f(\cdot,x)$ de $E$ dans $E^*$ est un isomorphisme (resp. semi-isomorphisme)
3. le déterminant de la matrice de $f$ dans $\mathcal{B}$ est non nul.

**Dém.** :

1. $\Rightarrow$ 2. L'application $\varphi$ est linéaire car $f$ est linéaire (resp semi-linéaire) par rapport à la seconde variable. Comme $E$ est de dimension finie, $E^* \cong E$. Il suffit donc de montrer que $\varphi$ est injective. Soit $x \in E$ tel que $\varphi(x) = f(\cdot,x) = 0$. Alors, $x$ appartient au noyau de $f$ *i.e.* $x = 0$ et $\varphi$ est injectif donc c'est un isomorphisme (resp. semi-isomorphisme).

2. $\Rightarrow$ 3. Comme $\varphi$ est un isomorphisme, sa matrice $A$ dans $(\mathcal{B},\mathcal{B}^*)$ est inversible donc son déterminant est non nul. Or $A = (f(e_i,e_j))$ *i.e.* $\det(mat_{\mathcal{B}}(f)) \neq 0$.

3. $\Rightarrow$ 1. Soit $x \in E$ tel que $\forall y \in E : f(y,x) = 0$. Comme $A$ est inversible, il existe $Z \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $X = {}^tAZ$. Donc $f(z,x) = {}^tZA\bar{X} = {}^tX\bar{X} = 0$. Mais alors $x = 0$ et $f$ est non dégénérée.

**Corollaire 4.1.2** Soit $f : E \times E \to \mathbb{K}$ une forme bilinéaire symétrique (resp. hermitienne) non dégénérée. Pour tout $y^* \in E^*$, il existe un unique $x$ de $E$ tel que $y^* = f(\cdot,x)$.

**Dém.** : si $f$ est symétrique (resp. hermitienne) alors $\varphi$ est un isomorphisme (resp. semi-isomorphisme).

## 4.2 Orthogonalité

Soit $f$ une forme bilinéaire symétrique ou hermitienne sur $E \times E$.

**Définition 4.2.1** Les vecteurs $x, y \in E$ sont *orthogonaux (relativement à $f$)* si $f(x,y) = 0$ (ou $f(y,x) = 0$). Soit $A$ une partie de $E$. L'*orthogonal* de $A$, noté $A^\perp$, est $\{x \in E : \forall a \in A, f(x,a) = 0\}$.

**Remarque 4.2.1**

1. Le noyau de $f$ est $E^\perp$.
2. $A^\perp$ est un sev de $E$.
3. Si $f$ est un produit scalaire alors on retrouve la notion usuelle.

**Théorème 4.2.1** Soit $F$ un sev de $E$ de dimension $n$. Alors $F^\perp$ est un sev de $E$ et $F \subseteq (F^\perp)^\perp$. De plus si $f$ est non dégénérée alors $\dim(F^\perp) = codim(F)$ et $F = (F^\perp)^\perp$.

**Dém.** : soit $x \in F$. Pour $t \in F^\perp$ on a $f(t,x) = 0$. Comme $f$ est symétrique ou hermitienne, $f(x,t) = 0$. Mais alors $x$ est orthogonal à tous les vecteurs de $F^\perp$.

Si $f$ est non dégénérée alors $\varphi$ est un (semi-)isomorphisme. Soit $(e_1, \ldots, e_p)$ une base de $F$ que l'on complète en une base de $E$. Soit $H = \{y^* \in E^* : y^*(F) = \{0\}\}$. Alors $H =< e^*_{p+1}, \ldots, e^*_n >$. Donc $\dim(H) = codim F$. Montrons que $\varphi^{-1}(H) = F^\perp$. On a :

$$\begin{aligned} y \in \varphi^{-1}(H) &\Leftrightarrow \varphi(y) \in H \\ &\Leftrightarrow \forall x \in F : \varphi(y)(x) = 0 \\ &\Leftrightarrow \forall x \in F : f(x,y) = 0 \\ &\Leftrightarrow y \in F^\perp. \end{aligned}$$

Comme $\varphi$ est un (semi-)isomorphisme, il conserve la dimension de $H$ donc $\dim(F^\perp) = n - p$. D'où le résultat.

**Définition 4.2.2** Un vecteur $x \in E$ est *isotrope* si $f(x,x) = 0$. Un sev $F$ de $E$ est *isotrope* si $F \cap F^\perp \neq \{0\}$. On note souvent $I$ l'ensemble des vecteurs isotropes. Ce n'est pas un sev en général mais $I$ est *conique i.e.* $(\forall x \in I)(\forall \lambda \in \mathbb{K}) : \lambda x \in I$.

**Exemple 4.2.1** Dans l'exemple 2. précédent, $I =< (1,1) > \cup < (-1,1) >$.

**Proposition 4.2.1** Soient $E$ un $\mathbb{K}-$ev de dimension finie et $F$ un sev de $E$. C.S.S.E. :

1. $f_{|F \times F}$ est non dégénérée
2. $F \cap F^\perp = \{0\}$
3. $E = F \oplus F^\perp$.

**Dém.** :

1. $\Leftrightarrow$ 2. $f_{|F\times F}$ est non dégénérée $\Leftrightarrow \{x \in F : \forall y \in F, f(y,x) = 0\} = \{0\} \Leftrightarrow F \cap F^\perp = \{0\}$.

1. $\Rightarrow$ 3. Soit $x \in E$. Alors $f(\cdot, x)_{|F} \in F^*$. Comme $f_{|F\times F}$ est non dégénérée, il existe un unique $x_1 \in F$ tel que $f(\cdot,x)_{|F} = f(\cdot,x_1)_{|F}$. Mais alors $x - x_1 \in F^\perp$ et $E = F \oplus F^\perp$.

3. $\Rightarrow$ 2. par définition.

**Remarque 4.2.2** Ne pas chercher à comparer $f_{|F\times F}$ non dégénérée et $f$ non dégénérée.

**Définition 4.2.3** Une base $(e_i)$ de $E$ est *orthogonale* (resp. *orthonormale*) si

$$f(e_i, e_j) = 0 \text{ si } i \neq j \text{ (resp. } f(e_i,e_j) = \delta_{ij} \text{ pour tout } i,j).$$

**Exemple 4.2.2** La base canonique $\mathcal{C}_n$ de $\mathbb{K}^n$ est orthonormée pour le produit scalaire usuel.

**Théorème 4.2.2 (fondamental)** Soit $E$ un $\mathbb{K}-$ev de dimension finie. Alors $E$ admet une base orthogonale pour $f$.

**Lemme 4.2.1** $f = 0 \Leftrightarrow \forall x \in E : f(x,x) = 0$.

**Dém.** :

($\Rightarrow$) évident.

($\Leftarrow$) soient $x, y \in E$.

- Dans le cas réel : $f(x+y, x+y) = f(x,x) + 2f(x,y) + f(y,y) = 2f(x,y) = 0$.
- Dans le cas complexe : $2Re(f(x,y)) = 0$. De même, $f(x-iy, x-iy) = f(x,x) - if(y,x) + if(x,y) + f(y,y) = 0$. D'où $Im(f(x,y)) = 0$.

**Dém.** (du théorème) :
- immédiat si $f = 0$.
- Sinon, on raisonne par récurrence sur la dimension de $E$.
  - Si $\dim E = 1$ alors c'est évident.
  - On suppose le résultat vrai pour la dimension $n-1$. Comme $f \neq 0$, il existe un vecteur $x$ non isotrope *i.e.* $f(\cdot, x) \neq 0$. Posons $H = \{f(\cdot, x) = 0\}$ : c'est un hyperplan de $E$ qui ne contient pas $x$. Appliquons l'hypothèse de récurrence à $f_{|H\times H}$. Il existe une base $(e_2, \ldots, e_n)$ de $H$ orthogonale pour $f$. Mais alors $(x, e_2, \ldots, e_n)$ est une base de $E$ orthogonale pour $f$.

**Remarque 4.2.3**

1. La matrice de $f$ dans cette base est diagonale.
2. Cette preuve n'est pas constructive.
3. Si $f$ est hermitienne alors $\forall x \in E : f(x, x) \in \mathbb{R}$.

**Proposition 4.2.2** Soit $(e_1, \ldots, e_n)$ une base orthogonale. Alors $\{e_i : f(e_i, e_i) = 0\}$ est une base du noyau de $f$.

**Dém.** : notons $K = \{k \in \{1, \ldots, n\} : f(e_k, e_k) = 0\}$.

Comme $(e_1, \ldots, e_n)$ est orthogonale, pour $k \in K$, $e_k$ appartient au noyau de $f$. Ainsi $(e_k)_{k\in K}$ est une famille libre de vecteurs du noyau de $f$.

Soit $x = \sum_{i=1}^{n} \lambda_i e_i$ appartenant au noyau de $f$. Si $j \notin K$ alors $f(x, e_j) = \lambda_j f(e_j, e_j)$. Or, $f(e_j, e_j) \neq 0$. Par suite $\lambda_j = 0$. Donc $(e_k)_{k\in K}$ est une famille génératrice du noyau de $f$.

**Théorème 4.2.3 (d'inertie de Sylvester)** Soient $E$ un $\mathbb{R}-$ev (resp. $\mathbb{C}-$ev) et $(e_1, \ldots, e_n)$ une base orthogonale telle que :

$$\begin{aligned} f(e_i, e_i) &> 0, \quad && 1 \leq i \leq r \\ f(e_i, e_i) &< 0, \quad && r+1 \leq i \leq r+s \\ f(e_i, e_i) &= 0, \quad && r+s+1 \leq i \leq n. \end{aligned}$$

Alors $r$ et $s$ ne dépendent que de $f$ ; autrement dit, si $(e'_1, \ldots, e'_n)$ est une autre base orthogonale telle que :

$$\begin{aligned} f(e'_i, e'_i) &> 0, \quad && 1 \leq i \leq r' \\ f(e'_i, e'_i) &< 0, \quad && r'+1 \leq i \leq r'+s' \\ f(e'_i, e'_i) &= 0, \quad && r'+s'+1 \leq i \leq n \end{aligned}$$

alors $r' = r$ et $s' = s$.

**Dém.** : notons $F =< e_1, \ldots, e_r >$ et $G =< e'_{r'+1}, \ldots, e'_n >$. Soit $x \in F \cap G$. Alors $f(x, x) = \sum_{i=1}^{r} |\lambda_i|^2 f(e_i, e_i) \geq 0$ mais on a aussi $f(x, x) = \sum_{i=r'+1}^{n} |\lambda'_i|^2 f(e'_i, e'_i) \leq 0$. Par suite $f(x, x) = 0$. Mais alors $\lambda_i = 0$ pour $1 \leq i \leq r$ donc $x = 0$. Il s'ensuit que :

$$\dim(F + G) = \dim F + \dim G \leq n.$$

Ou encore $r + n - r' \leq n$ *i.e.* $r \leq r'$. En inversant le rôle de $r$ et $r'$ on obtient que $r = r'$. Comme la dimension du noyau est $n - (r+s) = n - (r'+s')$ d'après la proposition précédente, on conclut que $s = s'$.

**Remarque 4.2.4** Ainsi, $r$ (resp. $s$) est la dimension maximale d'un sev sur lequel $f(x, x) > 0$ (resp. $f(x, x) < 0$) si $x \neq 0$.

## 4.3 Adjoint d'un endomorphisme

**Proposition 4.3.1** Soient $E$ un ev de dimension $n$ et $u$ un endomorphisme de $E$. Si $f$ est non dégénérée alors il existe un unique endomorphisme $u^*$ de $E$ tel que :

$$\forall x, y \in E : f(u(x), y) = f(x, u^*(y)).$$

**Dém.** : soit $y \in E$. Alors $\alpha_y : x \mapsto f(u(x), y) \in E^*$. Comme $f$ est non dégénéré, il existe un unique $z \in E$ tel que $\alpha_y = f(\cdot, z)$. On pose $u^*(y) = z$. Ainsi :

$$\forall x, y \in E : f(u(x), y) = f(x, u^*(y)).$$

De plus, soient $y, y' \in E$. On a :

$$\forall x \in E : f(x, u^*(y + y')) = f(u(x), y + y') = f(x, u^*(y) + u^*(y'))$$

Or $f$ est non dégénéré donc $u^*(y+y') = u^*(y)+u^*(y')$. De même, soient $\lambda \in \mathbb{K}$ et $y \in E$. On a :

$$\forall x \in E : f(x, u^*(\lambda y)) = f(u(x), \lambda y) = f(x, \lambda u^*(y))$$

Donc $u^*(\lambda y) = \lambda u^*(y)$.

On conclut que $u^*$ est bien défini, de manière unique et appartient à $L(E)$.

**Définition 4.3.1** Soient $f$ non dégénérée et $u \in L(E)$. L'*adjoint* de $u$ noté $u^*$ est l'unique endomorphisme de $E$ tel que :

$$\forall x, y \in E : f(u(x), y) = f(x, u^*(y)).$$

**Proposition 4.3.2** On a les propriétés suivantes :

$$(u+v)^* = u^* + v^* \text{ et } \begin{cases} (\lambda u)^* = \lambda u^* & \text{si } f \text{ est bilinéaire symétrique} \\ (\lambda u)^* = \bar{\lambda} u^* & \text{si } f \text{ est hermitienne} \end{cases}$$

$$(u \circ v)^* = v^* \circ u^* \text{ et } (u^*)^* = u$$

$$\operatorname{rg} u^* = \operatorname{rg} u \text{ et } \begin{cases} \det\ u^* = \det\ u & \text{si } f \text{ est bilinéaire symétrique} \\ \det\ u^* = \overline{\det\ u} & \text{si } f \text{ est hermitienne} \end{cases}$$

**Dém.** : on va démontrer les 2 dernières propriétés. On a :

$$\begin{aligned} x \in \ker u &\Leftrightarrow \forall y \in E : f(u(x), y) = 0 \\ &\Leftrightarrow \forall y \in E : f(x, u^*(y)) = 0 \\ &\Leftrightarrow x \in (\operatorname{Im} u^*)^\perp. \end{aligned}$$

*i.e.* $\ker u = (\operatorname{Im} u^*)^\perp$. Or, $f$ est non dégénérée donc $\dim \ker u = n - \operatorname{rg} u^*$ *i.e.* $\operatorname{rg} u = \operatorname{rg} u^*$.

Soit $(e'_i)_{1 \le i \le n}$ une base orthogonale. Comme $f$ est non dégénérée, on peut poser :

$$e_i = \begin{cases} \dfrac{e'_i}{\sqrt{f(e'_i, e'_i)}} & \text{si } f(e'_i, e'_i) > 0 \\ \dfrac{e'_i}{\sqrt{-f(e'_i, e'_i)}} & \text{si } f(e'_i, e'_i) < 0 \end{cases}$$

Notons $\mathcal{B} = (e_1, \ldots, e_n)$ et traitons le cas hermitien.

Pour $1 \le j \le n : u(e_j) = \sum_{i=1}^{n} \alpha_{ij} e_i$ et $u^*(e_j) = \sum_{i=1}^{n} \beta_{ij} e_i$.

On a donc $\forall i, j : f(u(e_i), e_j) = \epsilon \alpha_{ji} = f(e_i, u^*(e_j)) = \epsilon \bar{\beta}_{ij}$ *i.e.* $mat(u^*, \mathcal{B}) = mat(u, \mathcal{B})^*$. Par suite, $\det u^* = \det mat(u^*, \mathcal{B}) = \overline{\det mat(u, \mathcal{B})} = \overline{\det u}$.

**Définition 4.3.2** Soient $f$ non dégénérée et $u \in L(E)$ tel que

$$\forall x, y \in E : f(u(x), u(y)) = f(x, y).$$

Si $f$ est bilinéaire symétrique alors $u$ est *orthogonal*.
Si $f$ est hermitienne alors $u$ est *unitaire*.

**Proposition 4.3.3** L'endomorphisme $u$ est orthogonal ou unitaire ssi $u^* \circ u = id_E$.

**Exemple 4.3.1**

1. $E = \mathbb{R}^n$, $f(x, y) = \sum_{i=1}^{n} x_i y_i = {}^tXY$.

   $u$ orthogonal $\Leftrightarrow \forall x, y \in E : f(u(x), u(y)) = f(x, y)$.

   Notons $U$ la matrice de $u$ alors :

   $$\begin{aligned} {}^t(UX)(UY) &= {}^tXY \\ &= {}^tX({}^tUU)Y \end{aligned}$$

   Dés lors,

   $$u \text{ orthogonal} \Leftrightarrow U \text{ orthogonale} \Leftrightarrow {}^tU = U^{-1}.$$

2. $E = \mathbb{C}^n$, $f(x, y) = \sum_{i=1}^{n} x_i \bar{y_i}$. Alors :

   $$u \text{ unitaire} \Leftrightarrow U \text{ unitaire} \Leftrightarrow U^* = U^{-1}.$$

## 4.4 Formes quadratiques et formes quadratiques hermitiennes

**Définition 4.4.1** Soient $E$ un $\mathbb{K}-$ev et $q : E \to \mathbb{K}$. L'application $q$ est une *forme quadratique* (resp. *quadratique hermitienne*) si il existe une forme bilinéaire (resp. hermitienne) $f$ telle que :

$$\forall x \in E : q(x) = f(x, x).$$

**Proposition 4.4.1** Si $q : E \to \mathbb{K}$ est une forme quadratique (resp. quadratique hermitienne) alors il existe une unique forme bilinéaire symétrique (resp. hermitienne) $f$ telle que $q(x) = f(x, x)$ et

$$f(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y)) = \frac{1}{4}(q(x + y) - q(x - y)) \tag{14}$$

(resp.

$$f(x, y) = \frac{1}{2}(q(x + y) - iq(x + iy) - (1 - i)(q(x) + q(y))) \tag{15}$$

).

**Définition 4.4.2** La forme bilinéaire symétrique ou hermitienne $f$ telle que $q(x) = f(x, x)$ est la *forme polaire* de $q$.

**Remarque 4.4.1**

1. On a en fait un isomorphisme entre $S_2(E, \mathbb{K})$ et $Q(E, \mathbb{K})$. Toute notion définie sur une forme bilinéaire symétrique se transporte sur $Q(E, \mathbb{K})$ via cet isomorphisme. De même, le $\mathbb{R}-$ev des formes (sesquilinéaires) hermitiennes est isomorphe au $\mathbb{R}-$ev des formes quadratiques hermitiennes.

2. Soient $\mathcal{B}$ une base de $E$ et $A = mat_{\mathcal{B}}(q)$ (*i.e.* $mat_{\mathcal{B}}(f)$). Alors
$$q(x) = {}^tXAX = {}^tX{}^tAX.$$
3. De même, si $q$ est une forme quadratique hermitienne alors
$$q(x) = {}^tXA\bar{X} = X^{*t}AX$$
4. Deux formes bilinéaires satisfaisant à (14) diffèrent d'une forme antisymétrique.
5. Les égalités (14) et (15) sont les *identités de polarisation*.

**Exemple 4.4.1** Ecrire la matrice $A$ des formes quadratiques :
1. $q(x) = 2x_1^2 + 2x_1x_2 + x_3^2 - 2x_1x_3$
2. $q(x) = x_1\bar{x}_1 - 2ix_1\bar{x}_3 + 2i\bar{x}_1x_3 + 2x_3\bar{x}_3 + x_1\bar{x}_2 + \bar{x}_1x_2$.

**Théorème 4.4.1 (Décomposition de Gauss)** Soit $q$ une forme quadratique sur $E$ de dimension $n$. Alors il existe $p \leqslant n$ formes linéaires indépendantes $l_1, \ldots, l_p$ telles que
$$q(x) = \sum_{i=1}^{p} \alpha_i l_i^2(x).$$

**Dém.** : il s'agit d'épuiser les variables une par une. On raisonne par récurrence sur le nombre de variables restantes. On pose $q_1 = q$. Deux cas se présentent.
1. Il existe $1 \leqslant i \leqslant n$ : $a_{ii} \neq 0$. Quitte à renuméroter les variables, on peut supposer $i = 1$. Ainsi
$$q_1(x) = a_{11}x_1^2 + x_1 l(x_2, \ldots, x_n) + q'(x_2, \ldots, x_n)$$
En écrivant le début d'un carré, il vient :
$$q_1(x) = a_{11}(x_1 + \frac{1}{2a_{11}}l)^2 - \frac{1}{4a_{11}}l^2 + q'(x_2, \ldots, x_n).$$
On pose $\alpha_1 = a_{11}$, $l_1 = x_1 + \dfrac{l}{2a_{11}}$ et $q_2(x_2, \ldots, x_n) = q'(x_2, \ldots, x_n) - \dfrac{l^2}{4a_{11}}$.
2. Pour tout $1 \leqslant i \leqslant n$ : $a_{ii} = 0$. Si $q \neq 0$ alors il existe $i < j$ tels que $a_{ij} \neq 0$. Sans perte de généralité, on peut supposer que $i = 1 < 2 = j$. Alors
$$q_1(x) = a_{12}(x_1x_2 + x_1l_1'(x_3, \ldots, x_n) + x_2l_2'(x_3, \ldots, x_n)) + q'(x_3, \ldots, x_n).$$
On peut écrire :
$$\begin{aligned} q_1 &= a_{12}(x_1 + l_2')(x_2 + l_1') - a_{12}l_1'l_2' + q' \\ &= \frac{a_{12}}{4}\left((x_1 + l_1' + x_2 + l_2')^2 - (x_1 + l_1' - (x_2 + l_2'))^2\right) + q_1 - a_{12}l_1'l_2' \end{aligned}$$
On pose $\alpha_1 = \dfrac{a_{12}}{4}$, $\alpha_2 = -\dfrac{a_{12}}{4}$, $l_1 = x_1 + l_1' + x_2 + l_2'$, $l_2 = x_1 + l_1' - x_2 - l_2'$ et $q_2(x_3, \ldots, x_n) = q_1(x_3, \ldots, x_n) - a_{12}l_1'(x_3, \ldots, x_n)l_2'(x_3, \ldots, x_n)$.

On recommence avec $q_2$ en remarquant qu'elle ne dépend plus que de $n-1$ ou $n-2$ variables.

**Exemple 4.4.2** Soit $q(x) = 2x_1x_2 + x_2x_3 + x_3x_1 + x_3x_4$. Alors
$$\begin{aligned} q(x) &= 2x_1x_2 + x_1x_3 + x_2x_3 + x_3x_4 \\ &= 2\left(x_1x_2 + x_1(\frac{1}{2}x_3) + x_2(\frac{1}{2}x_3)\right) + x_3x_4 \\ &= \frac{1}{2}(x_1 + \frac{1}{2}x_3 + x_2 + \frac{1}{2}x_3)^2 - \frac{1}{2}(x_1 + \frac{1}{2}x_3 - x_2 - \frac{1}{2}x_3)^2 - \frac{1}{2}x_3^2 + x_3x_4 \\ &= \frac{1}{2}(x_1 + x_2 + x_3)^2 - \frac{1}{2}(x_1 - x_2)^2 - \frac{1}{2}(x_3 - x_4)^2 + \frac{1}{2}x_4^2 \end{aligned}$$

**Remarque 4.4.2** Soit $f$ sesquilinéaire hermitienne. Si $a_{ij}x_i\bar{y}_j$ apparaît dans l'écriture de $f(x,y)$ (dans une base) alors $\bar{a}_{ij}x_j\bar{y}_i$ aussi. En particulier, dans une base orthogonale, $f(x,y) = \sum_{i=1}^{n} \alpha_i x_i \bar{y}_i$ donc $\alpha_i \in \mathbb{R}$.

**Proposition 4.4.2** Soient $E$ un $\mathbb{C}-$ev de dimension $n$ et $q$ une forme quadratique hermitienne. Alors il existe $p \leqslant n$ formes linéaires linéairement indépendantes $l_1, \ldots, l_p$ telles que

$$q(x) = \sum_{i=1}^{p} \alpha_i |l_i(x)|^2.$$

**Corollaire 4.4.1 (*aussi* du théorème de Sylvester)** Soient $q$ une forme quadratique (resp. quadratique hermitienne). Alors il existe une base orthogonale $(e_i)_{1\leqslant i\leqslant n}$ de $E$ telle que :

$$q(e_i) = \begin{cases} 1 & \text{si } 1 \leqslant i \leqslant r \\ -1 & \text{si } r+1 \leqslant i \leqslant r+s \\ 0 & \text{si } r+s+1 \leqslant i \leqslant n \end{cases}$$

où les entiers $r$ et $s$ ne dépendent que de $q$.

**Définition 4.4.3** La *signature* de $q$ est $\sigma(q) = (r,s)$. Le *rang* de $q$ est $r+s$.

**Définition 4.4.4** Soient $E$ un $\mathbb{R}-$ev (resp. $\mathbb{C}-$ev) et $f$ une forme bilinéaire symétrique (resp. hermitienne). La forme $f$ est :

- *positive* (resp. *négative*) si $\forall x \in E : f(x,x) \geqslant 0$ (resp. $f(x,x) \leqslant 0$)
- *définie positive* (resp. *définie négative*) si $\forall x \in E - \{0\} : f(x,x) > 0$ (resp. $f(x,x) < 0$).

Un *produit scalaire euclidien* (resp. *hermitien*) sur $E$ est une forme bilinéaire symétrique (resp. hermitienne) définie positive sur $E$.

**Remarque 4.4.3** Si $f$ est positive alors

$$f \text{ définie positive} \Leftrightarrow \text{le seul vecteur isotrope est } 0.$$

**Théorème 4.4.2 (Inégalité de Cauchy-Schwartz)** Soit $f$ une forme bilinéaire symétrique (sur un $\mathbb{R}-$ev) ou hermitienne (sur un $\mathbb{C}-$ev) positive . Alors

$$|f(x,y)|^2 \leqslant f(x,x)f(y,y). \tag{16}$$

**Dém.** : on va démontrer le cas bilinéaire symétrique. Soient $x, y \in E$. Pour tout $\lambda \in \mathbb{R}$, on a :

$$0 \leqslant f(x+\lambda y, x+\lambda y) = f(x,x) + 2\lambda f(x,y) + \lambda^2 f(y,y).$$

Deux cas se présentent :

1. $f(y,y) = 0$. Alors $\forall \lambda \in \mathbb{R} : 2\lambda f(x,y) + f(x,x) \geqslant 0$. Mais alors $f(x,y) = 0$ et (16) s'en suit.
2. $f(y,y) \neq 0$. Alors $f(x,x) + 2\lambda f(x,y) + \lambda^2 f(y,y)$ est un trinôme du second degré en $\lambda$ qui n'a pas de racine ou une racine double sur $\mathbb{R}$. Celà signifie que son discriminant est négatif ou nul. Ainsi, $\Delta' = f(x,y)^2 - f(x,x)f(y,y) \leqslant 0$. D'où (16).

**Corollaire 4.4.2** Soit $f$ une forme bilinéaire symétrique ou hermitienne positive. Alors le noyau de $f$ est l'ensemble des vecteurs isotropes. De plus,

$$f \text{ définie positive} \Leftrightarrow f \text{ non dégénérée.}$$

**Dém.** : par définition, le noyau est inclus dans l'ensemble des vecteurs isotropes. Réciproquement, soit $x$ un vecteur isotrope. Alors $\forall y \in E : f(x,y) = 0$ d'après Cauchy-Schwartz. Donc $x$ est élément du noyau de $f$.

($\Rightarrow$) Comme $f > 0$, elle ne possède aucun vecteur isotrope donc $f$ est non dégénéré.

($\Leftarrow$) Comme $f \geqslant 0$, l'ensemble des vecteurs isotropes coïncide avec le noyau de $f$. Or $f$ est non dégénéré donc $f > 0$.

**Théorème 4.4.3** Soient $E$ un $\mathbb{R}-$ev (resp. $\mathbb{C}-$ev) de dimension $n$ et $f$ une forme bilinéaire symétrique (resp. sesquilinéaire hermitienne) définie positive. Alors $E$ admet une base orthonormale et relativement à cette base :

$$f(x,y) = \sum_{i=1}^{n} x_i y_i \quad (\text{resp.} \quad f(x,y) = \sum_{i=1}^{n} x_i \bar{y_i})$$
$$q(x) = \sum_{i=1}^{n} x_i^2 \quad (\text{resp.} \quad q(x) = \sum_{i=1}^{n} |x_i|^2).$$

**Remarque 4.4.4**

1. L'expression de $f$ dans une base orthonormale est celle du produit scalaire usuel.
2. Cette preuve n'est pas constructive. Pour construire une base orthonormale pour une telle $f$ on peut utiliser le procédé d'orthonormalisation de Gram-Schmidt (cf TD).

**Proposition 4.4.3** Soient $E$ un $\mathbb{R}-$ev (resp. $\mathbb{C}-$ev) et $q$ une forme quadratique (resp. quadratique hermitienne) définie positive sur $E$. Alors l'application $N : E \to \mathbb{R}_+$ définie par $N(x) = \sqrt{q(x)}$ est une norme sur $E$.

**Théorème 4.4.4** Soient $E$ un ev de dimension finie, $(\cdot|\cdot\,\cdot)$ un produit scalaire euclidien (resp. hermitien) sur $E$ et $q$ une forme quadratique (resp. hermitienne). Alors il existe une base $((\cdot|\cdot\,\cdot)$-$)$orthonormée de $E$, orthogonale pour $q$.

# 5 Réduction des matrices et des endomorphismes

Dans ce chapitre, $f$ désigne un endomorphisme du $\mathbb{K}-$ev $E$ ($\mathbb{K}$ corps commutatif).

## 5.1 Valeurs propres et vecteurs propres

### 5.1.1 Généralités

**Définition 5.1.1**

- un scalaire $\lambda \in \mathbb{K}$ est *valeur propre* de $f$ si il existe $x \in E, x \neq 0$ tel que

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

- Si $\lambda$ est valeur propre de $f$ et $f(x) = \lambda x$ alors $x$ est un *vecteur propre* de $f$ *associé* à $\lambda$. L'ensemble $E_\lambda$ des vecteurs propres associés à la valeur propre $\lambda$ auquel on adjoint 0, est le *sous-espace propre* associé à $\lambda$.
- Le *spectre* de $f$, noté $Sp(f)$, est l'ensemble des valeurs propres de $f$.

**Remarque 5.1.1**

1. Si $A$ est une matrice $n \times n$ alors on peut définir les mêmes notions.
2. On a $E_\lambda = \ker(f - \lambda id_E)$. En particulier, $E_\lambda$ est un sev de $E$.

**Exemple 5.1.1**

1. $\begin{array}{rccc} f: & \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (x_1,x_2) & \mapsto & (2x_2,2x_1). \end{array}$

   Soient $(x_1,x_2)\in\mathbb{R}^2$ et $\lambda\in\mathbb{R}$.

$$\begin{aligned} f(x_1,x_2)=\lambda(x_1,x_2) &\Leftrightarrow \left\{\begin{array}{rcl} \lambda x_1-2x_2 &=& 0\\ 2x_1-\lambda x_2 &=& 0\end{array}\right.\\ &\Leftrightarrow \left\{\begin{array}{rcl} 2x_1-\lambda x_2 &=& 0\\ \lambda x_1-2x_2 &=& 0\end{array}\right.\\ &\Leftrightarrow \left\{\begin{array}{rcl} x_1-\frac{\lambda}{2}x_2 &=& 0\\ (\frac{\lambda^2}{2}-2)x_2 &=& 0\end{array}\right.\\ &\Leftrightarrow \left\{\begin{array}{rcl} x_1-\frac{\lambda}{2}x_2 &=& 0\\ (\lambda^2-4)x_2 &=& 0\end{array}\right. . \end{aligned}$$

   Donc $Sp(f)=\{-2,2\}$, $E_{-2}=\{(-x_2,x_2):x_2\in\mathbb{R}\}$ et $E_2=\{(x_2,x_2):x_2\in\mathbb{R}\}$.

2. $\begin{array}{rccc} D: & C^\infty(\mathbb{R},\mathbb{R}) & \to & C^\infty(\mathbb{R},\mathbb{R}) \\ & \varphi & \mapsto & \varphi'. \end{array}$

   Soit $\lambda\in\mathbb{R}$. Alors $\varphi'=\lambda\varphi\Leftrightarrow\varphi(t)=Ce^{\lambda t}$ avec $C\in\mathbb{R}$, pour tout $t\in\mathbb{R}$. Ainsi $Sp(D)=\mathbb{R}$ et pour tout $\lambda\in\mathbb{R}$, $E_\lambda=<e^{\lambda t}>$.

**Proposition 5.1.1** Une somme finie de sous-espaces propres du type $\sum_{k=1}^{m}E_{\lambda_k}$ (avec $\lambda_k\neq\lambda_{k'}$ si $k\neq k'$) est directe.

**Dém.** : montrons le par récurrence sur $m$.

- Si $m=2$ alors il s'agit de montrer que $F=E_{\lambda_1}\cap E_{\lambda_2}=\{0\}$. Mais si $x\in F$ alors $f(x)=\lambda_1 x=\lambda_2 x$ Comme $\lambda_1\neq\lambda_2$, il vient $x=0$.
- Sinon, supposons que la somme de $m$ tels sevs soit directe. Soit $x\in\sum_{k=1}^{m}E_{\lambda_k}\cap E_{\lambda_{m+1}}$. Alors $x=\sum_{k=1}^{m}x_k\in E_{\lambda_{m+1}}$. D'où $f(x)=\sum_{k=1}^{m}\lambda_k x_k=\lambda_{m+1}x$. On obtient donc $\sum_{k=1}^{m}(\lambda_k-\lambda_{m+1})x_k=0$. Comme les $\lambda_k$ sont 2 à 2 distincts il vient $x=0$.

**Remarque 5.1.2** En particulier $(e^{\lambda t})_{\lambda\in\mathbb{R}}$ est libre.

Si $\dim E=n$, on fixe une base $(e_i)_{1\leqslant i\leqslant n}$ de $E$ et $A=mat(f,(e_i))$.

**Proposition 5.1.2**

$$\lambda\in Sp(f)\Leftrightarrow\det(f-\lambda id_E)=0\Leftrightarrow\det(A-\lambda I_n)=0.$$

**Dém.** : $\lambda$ valeur propre de $f$ ssi $f-\lambda id_E$ est non injective ssi $\det(f-\lambda id_E)=0$.

**Définition 5.1.2** Le *polynôme caractéristique* de $f$ (ou $A$) est le déterminant

$$\chi_f(X)=\det(f-Xid_E)=\det(A-XI_n).$$

La multiplicité (*algébrique*) d'une racine $\lambda$ est notée $m_\lambda$.

**Remarque 5.1.3** Soit $E$ un $\mathbb{K}-$ev de dimension $n$.

1. Le déterminant d'une matrice ne dépend que de sa *classe de similitude*.
2. Le polynôme $\chi_f$ n'est pas (identiquement) nul. Plus précisément,
$$\chi_f(X) = (-1)^n X^n + (-1)^{n-1} tr(A) X^{n-1} + \cdots + \det(A).$$
3. Les valeurs propres de $f$ (ou $A$) sont les racines de $\chi_f$.
4. Le degré $deg(\chi_f) = n$ donc $f$ admet au plus $n$ valeurs propres distinctes (exactement $n$ comptées avec multiplicité si le corps est algébriquement clos –$\mathbb{K} = \mathbb{C}$ notamment).
5. Si $f$ a $p$ valeurs propres alors $\dim E \geqslant p$.

**Exemple 5.1.2** Si $A$ est triangulaire alors $\chi_A(X) = \prod_{k=1}^{n} (a_{kk} - X)$.

**Proposition 5.1.3** Les endomorphismes $f$ et ${}^t f$ ont même polynôme caractéristique.

**Proposition 5.1.4** Soient $E'$ un sev (de $E$) non réduit à $\{0\}$, stable par $f$ (*i.e.* $f(E') \subseteq E'$) et $g = f_{|E'} : E' \to E'$ (avec un abus de notation inoffensif). Alors $\chi_g$ divise $\chi_f$.
**Dém.** : soit $\mathcal{B}' = (e'_1, \ldots, e'_p)$ une base de $E'$. Complétons-la en une base $\mathcal{B} = (e'_1, \ldots, e'_p, e_{p+1}, \ldots, e_n)$ de $E$. Notons $A = mat(f, \mathcal{B})$ et $A' = mat(g, \mathcal{B}')$. Alors

$$A = \begin{pmatrix} A' & B \\ 0 & C \end{pmatrix}.$$

Donc $\chi_f = \det(A - XI_n) = \begin{vmatrix} A' - XI_p & B \\ 0 & C - XI_{n-p} \end{vmatrix}$. D'où :

$$\chi_f = \chi_g \det(C - XI_{n-p}).$$

Et $\chi_g$ divise $\chi_f$.

**Remarque 5.1.4**

1. La formule du déterminant par bloc s'obtient facilement à l'aide d'une récurrence sur la taille du bloc carré supérieur gauche.
2. $E_\lambda$ est stable par $f$ !

### 5.1.2 Détermination pratique des valeurs propres et vecteurs propres

Les valeurs propres sont exactement les racines du polynôme caractéristique. Ce sont exactement les scalaires $\lambda$ tel que le système linéaire homogène (17) admette une solution non triviale (une infinité si $\mathbb{K}$ est infini).

Pour identifier le sous-espace propre associé à une valeur propre $\lambda$, on détermine le sev $\ker(f - \lambda id_E)$ en résolvant l'équation matricielle :

$$\begin{pmatrix} a_{11} - \lambda & a_{22} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{17}$$

Le corang $q_\lambda = n - r_\lambda$ de ce système linéaire est la dimension de $E_\lambda$.

**Proposition 5.1.5** Soit $\lambda \in Sp(f)$. Alors :

$$1 \leqslant q_\lambda \leqslant m_\lambda.$$

**Dém.** : en effet, soit $g = f_{|E_\lambda} : E_\lambda \to E_\lambda$. Alors $g \in L(E_\lambda)$ ; en fait, $g = \lambda id_{E_\lambda}$. De sorte que $\chi_g = (\lambda - X)^{q_\lambda}$. En vertu de 5.1.4, $\chi_g \mid \chi_f$. En particulier, $0 < q_\lambda \leqslant m_\lambda$.

**Remarque 5.1.5** L'entier $q_\lambda$ est la *multiplicité géométrique* de $\lambda$.

**Corollaire 5.1.1** Si $\lambda \in Sp(f)$ est racine simple de $\chi_f$ alors $\dim E_\lambda = 1$.

**Exemple 5.1.3** Le polynôme caractéristique de (5.1.1) est $\lambda^2 - 4 = (\lambda - 2)(\lambda + 2)$. Donc $Sp(f) = \{-2, 2\}$. En particulier ici, $E_{-2} \oplus E_2 = \mathbb{R}^2$. Les sous-espaces propres sont donnés par :

- $E_{-2} = \ker(f + 2id_E) = \ker(A + 2I) = \ker(\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}) =< (-1, 1) >$.
- $E_2 = \ker(\begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix}) =< (1, 1) >$.

## 5.2 Diagonalisation et trigonalisation

**Définition 5.2.1** Un endomorphisme $f$ est *diagonalisable* si il existe une base $(e_k)$ de vecteurs propres. En particulier, si $\dim E$ est finie alors $mat(f, (e_k))$ est diagonale.

**Définition 5.2.2** Un polynôme $P \in \mathbb{K}[X]$ de degré $> 0$ est *scindé* sur $\mathbb{K}$ si il peut s'écrire comme produit de polynômes de degré 1. Ou, de manière équivalente, si toutes les racines de $P$ appartiennent à $\mathbb{K}$.

**Exemple 5.2.1**

1. $X^2 - 1$ est scindé sur $\mathbb{R}$.
2. $X^2 + 1$ n'est pas scindé sur $\mathbb{R}$ mais l'est sur $\mathbb{C}$.
3. Plus généralement, tout polynôme de $\mathbb{R}[X]$ de degré $\geqslant 1$ se factorise en produit de polynômes de degré 1 ou, de degré 2 à discriminant $< 0$. Tout polynôme de $\mathbb{C}[X]$ de degré $\geqslant 1$ est scindé sur $\mathbb{C}$ ; le corps $\mathbb{C}$ est *algébriquement clos*.

**Théorème 5.2.1** Soient $E$ un $\mathbb{K}-$ev de dimension finie $n$ et $f \in L(E)$. C.S.S.E. :

1. $f$ est diagonalisable
2. $\chi_f$ est scindé sur $\mathbb{K}$ et $\forall \lambda \in Sp(f) : \dim E_\lambda = m_\lambda$
3. $E = \bigoplus_{\lambda \in Sp(f)} \ker(f - \lambda id_E)$.

**Dém.** :

1. $\Rightarrow$ 2. Soit $\mathcal{B}$ une base de $E$ qui diagonalise $f$. Alors, $A = mat(f, \mathcal{B})$ est diagonale. En particulier, $\chi_f(X) = \det(A - XI_n) = \prod_{\lambda \in Sp(f)} (\lambda - X)^{m_\lambda}$. Soit $\lambda \in Sp(f)$. On a $\dim(\ker(f - \lambda id_E)) = m_\lambda$ car la valeur propre $\lambda$ se retrouve $m_\lambda$ fois sur la diagonale de $A$.

2. $\Rightarrow$ 3. Comme, pour tout $\lambda \in Sp(f)$, $\ker(f - \lambda id_E)$ est de dimension $m_\lambda$, $\sum_{\lambda \in Sp(f)} m_\lambda = n$, et les sous-espaces propres sont en somme directe, il vient $E = \bigoplus_{\lambda \in Sp(f)} \ker(f - \lambda id_E)$.

3. $\Rightarrow$ 1. Pour tout $\lambda \in Sp(f)$, soit $(e_1^\lambda, \ldots, e_{q_\lambda}^\lambda)$ une base de $E_\lambda$. Alors la réunion de ces bases forme une base de $E$ d'après 3. et $f_{|E_\lambda} = \lambda j_{E_\lambda}$. Donc $f$ est diagonalisable.

**Corollaire 5.2.1** Si $f$ admet $n$ valeurs propres distinctes alors $f$ est diagonalisable.

**Remarque 5.2.1**

1. La réciproque de ce corollaire est fausse. Considérer $0_{L(E)}$ ou $id_E$.
2. Sous l'une des conditions du théorème 5.2.1, il existe $P \in GL_n(\mathbb{K})$ tel que
$$\Delta = P^{-1}AP \text{ est diagonale.}$$

**Définition 5.2.3** Soit $E$ un $\mathbb{K}-$ev de dimension finie $n$ et $f \in L(E)$. L'endomorphisme $f$ est *trigonalisable* si il existe une base de $E$ dans laquelle la matrice de $f$ est triangulaire.

**Théorème 5.2.2** Soient $E$ un $\mathbb{K}-$ev de dimension finie $n$ et $f \in L(E)$. Alors
$$f \text{ est trigonalisable} \Leftrightarrow \chi_f \text{ est scindé sur } \mathbb{K}.$$

**Dém.** :

($\Rightarrow$) Comme $f$ est trigonalisable, il existe une base de $E$ dans laquelle la matrice de $f$ est triangulaire. En particulier, $\chi_f$ est scindé sur $\mathbb{K}$.

($\Leftarrow$) on raisonne par récurrence sur la dimension de $E$.

– Si $n = 1$ alors c'est immédiat.

– Si $n \geqslant 2$ alors, comme $\chi_f$ est scindé sur $\mathbb{K}$, il existe une valeur propre $\lambda_1$ et un vecteur propre $e_1$. Soit $E'$ un supplémentaire de $< e_1 >$ dans $E$. Si $\pi : E \to E$ désigne le projecteur sur $E'$ parallèlement à $< e_1 >$ alors $E'$ est stable par $g = \pi \circ f$. Soit $(e'_2, \ldots, e'_n)$ une base de $E'$. Alors $\mathcal{B} = (e_1, e'_2, \ldots, e'_n)$ constitue une base de $E$ et
$$A = mat(f, \mathcal{B}) = \begin{pmatrix} \lambda_1 & L \\ 0 & A' \end{pmatrix}$$
où
$$A' = mat(g, (e'_i)_{2 \leqslant i \leqslant n}).$$
Par suite, $\chi_f = (\lambda_1 - X)\chi_g$. Or $\chi_f$ est scindé sur $\mathbb{K}$ donc $\chi_g$ l'est aussi. Par récurrence sur $\dim E'$, on peut ainsi supposer que $(e'_2, \ldots, e'_n)$ trigonalise $g_{|E'}$. De sorte que $A'$ est triangulaire (supérieure) et $A$ l'est aussi. On conclut que $f$ est trigonalisable.

**Corollaire 5.2.2** Soient $E$ un $\mathbb{K}-$ev de dimension finie $n$ et $f \in L(E)$. Si $\mathbb{K}$ est algébriquement clos (par exemple si $\mathbb{K} = \mathbb{C}$) alors $f$ est trigonalisable. En particulier, toute matrice carrée complexe est trigonalisable sur $\mathbb{C}$.

**Remarque 5.2.2**

1. $f$ diagonalisable sur $\mathbb{K} \Rightarrow f$ trigonalisable sur $\mathbb{K}$ mais la réciproque est fausse. En effet, si $f(x_1, x_2) = (x_2, 0)$ alors $f$ n'est pas diagonalisable.
2. $f$ trigonalisable sur $\mathbb{R} \Rightarrow f$ trigonalisable sur $\mathbb{C}$ mais la réciproque est fausse. En effet, soit $\theta \not\equiv 0[\pi]$ ; $f(x_1, x_2) = (\cos(\theta)x_1 - \sin(\theta)x_2, \sin(\theta)x_1 + \cos(\theta)x_2)$ est diagonalisable sur $\mathbb{C}$ ($Sp(f) = \{e^{i\theta}, e^{-i\theta}\}$) mais n'admet pas de valeur propre sur $\mathbb{R}$.

**Corollaire 5.2.3 (interprétation matricielle)** Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors il existe $P \in GL_n(\mathbb{C})$ tel que
$$T = P^{-1}AP \text{ est triangulaire.}$$

## 5.3 Polynôme d'endomorphisme

### 5.3.1 Généralités

**Définition 5.3.1** Si $Q(X) = \sum_{k=0}^{m} a_k X^k \in \mathbb{K}[X]$ alors

$$Q(f) := \sum_{k=0}^{m} a_k f^k \in L(E) \text{ où } f^k = \underbrace{f \circ \cdots \circ f}_{k \text{ fois}}.$$

**Remarque 5.3.1**

1. $f^0 = id_E$.
2. $mat(Q(f), (e_i)) = \sum_{k=0}^{m} a_k A^k$.
3. Si $\dim E$ est finie alors $\dim_{\mathbb{K}} L(E) = n^2$ donc pour tout $k \in \mathbb{N}$, $f^k$ s'écrit à l'aide d'au plus $n^2$ puissances de $f$ *i.e.* $(id_E, f, \ldots, f^{n^2-1}, f^k)$ est liée.

**Exemple 5.3.1**

1. Si $Q(X) = X^2 + 2X - 1$ alors $Q(f) = f^2 + 2f - id_E$.
2. De même, $Q(A) = A^2 + 2A - I_n$.

**Proposition 5.3.1** Soient $P, Q \in \mathbb{K}[X]$. Alors

$$(PQ)(f) = P(f) \circ Q(f) = Q(f) \circ P(f).$$

**Dém.** : il suffit de démontrer la première égalité. Elle résulte du fait que pour tout $k \in \mathbb{N}$, $f^k$ est linéaire.

**Exemple 5.3.2** On a $f^2 - 4id_E = (f - 2id_E)(f + 2id_E)$ pour l'exemple 5.1.1.

**Remarque 5.3.2**

1. L'application $\Phi : P \mapsto P(f)$ est un morphisme de la $\mathbb{K}-$algèbre $\mathbb{K}[X]$ dans la $\mathbb{K}-$algèbre $L(E)$.
2. En particulier, $\operatorname{Im}\Phi$ est une sous-algèbre commutative de $L(E)$ notée $\mathbb{K}[f]$.

**Lemme 5.3.1** Soient $P$ et $Q \in \mathbb{K}[X]$ premiers entre eux. Alors

$$\ker((PQ)(f)) = \ker P(f) \oplus \ker Q(f).$$

**Dém.** : soit $E'$ un supplémentaire de $\ker Q(f)$ dans $E$ *i.e.* $\ker Q(f) \oplus E' = E$. En particulier, $Q(f)_{|E'} : E' \to \operatorname{Im} Q(f) \hookrightarrow E$ réalise un isomorphisme $\psi$ sur $\operatorname{Im} Q(f)$.

Tout vecteur $x \in E$ se décompose de manière unique $x = x_q + x'$ avec $x_q \in \ker Q(f)$ et $x' \in E'$. On a :

$$x \in \ker(PQ)(f) \Leftrightarrow Q(f)(x') \in \ker P(f).$$

Autrement dit, $x \in \ker(PQ)(f) \Leftrightarrow x' \in \psi^{-1}(\operatorname{Im} Q(f) \cap \ker P(f))$.

En particulier,

$$\dim(\ker(PQ)(f)) \leqslant \dim\ker Q(f) + \dim\ker P(f).$$

D'autre part, comme $(PQ)(f) = P(f) \circ Q(f)$, $\ker Q(f) \subseteq \ker(PQ)(f)$. De même pour $\ker P(f)$ d'où $\ker P(f) + \ker Q(f) \subseteq \ker(PQ)(f)$.

Soit $x \in \ker P(f) \cap \ker Q(f)$. Comme $P$ et $Q$ sont premiers entre eux, d'après Bezout, il existe $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$. Alors, $x = 0$ *i.e.* $\ker P(f) \cap \ker Q(f) = \{0\}$. Par conséquent, $\ker P(f)$ et $\ker Q(f)$ sont en somme directe et $\dim(\ker P(f) + \ker Q(f)) = \dim \ker P(f) + \dim \ker Q(f)$. D'où le résultat.

**Théorème 5.3.1 (des noyaux)** Si $P_1, \ldots, P_m \in \mathbb{K}[X]$ sont premiers entre eux 2 à 2 alors

$$\ker(P_1 \cdots P_m)(f) = \bigoplus_{k=1}^{m} \ker P_k(f).$$

**Exemple 5.3.3** Les polynômes $X - 2$ et $X + 2$ de 5.1.1 sont premiers entre eux. Donc

$$\ker(f - 2id_E) \oplus \ker(f + 2id_E) = \ker(f^2 - 4id_E).$$

**Proposition 5.3.2** Soit $P \in \mathbb{K}[X]$. Alors $\ker P(f)$ et $\operatorname{Im} P(f)$ sont stables par $f$.

**Dém.** : l'endomorphisme $f$ commute avec $P(f)$ donc si $P(f)(x) = 0$ alors $f \circ P(f)(x) = P(f)(f(x)) = 0$ *i.e.* $f(x) \in \ker P(f)$. On raisonne de manière analogue pour $\operatorname{Im} P(f)$.

### 5.3.2 Théorème de Cayley-Hamilton

**Théorème 5.3.2 (de Cayley-Hamilton)** Soient $E$ un $\mathbb{K}-$ev de dimension $n$ et $f \in L(E)$. Alors $\chi_f(f) = 0$.

**Dém.** : considérons la matrice $A - XI_n \in \mathcal{M}_n(\mathbb{K}[X])$. Alors, la transposée de la matrice des cofacteurs de $A - XI_n$, $C$, vérifie :

$$(A - XI_n)C = \chi_f I_n.$$

D'autre part :

$$A^k - X^k I_n = (A - XI_n)(A^{k-1} + XA^{k-2} + \cdots + X^{k-1}I_n) \text{ pour } k \geqslant 1.$$

D'où $\chi_f(A) - \chi_f I_n = (A - XI_n)Q$. Mais alors

$$\chi_f(A) = (A - XI_n)(C + Q).$$

Or, $C + Q \in \mathcal{M}_n(\mathbb{K}[X])$ *i.e.* $C + Q = \sum_{k=0}^{n-1} X^k B_k$ avec $B_k \in \mathcal{M}_n(\mathbb{K})$. Supposons que l'un des $B_k$ soit non nul. Dés lors, il existe un indice $r$ maximal tel que $B_r \neq 0$. Ainsi, les coefficients de $\chi_f(A) \in \mathcal{M}_n(\mathbb{K})$ s'écriraient à l'aide d'un polynôme en $X$ de degré $r + 1$.

Tous les $B_k$ sont donc nuls et $\chi_f(f) = 0$.

**Remarque 5.3.3**

1. La démonstration ci-dessus est valable sur un $\mathbb{K}-$ev $E$ de dimension finie sur un corps commutatif $\mathbb{K}$.
2. Si $E$ est de dimension finie $n$ alors l'algèbre $\mathbb{K}[f]$ est qui est de *type fini* est engendrée par au plus $n$ éléments.

**Exemple 5.3.4** On a $f^2 = 4id_E$ donc $\mathbb{K}[f] =< id_E, f >$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$). En particulier, $f$ est inversible d'inverse $\frac{1}{4}f$.

### 5.3.3 Annulateur et polynôme minimal

Le noyau du morphisme de $\mathbb{K}-$algèbre $\Phi$ est un idéal de $\mathbb{K}[X]$.

**Définition 5.3.2** L'*idéal annulateur* de $f$ est $Ann(f) = \{P \in \mathbb{K}[X] \mid P(f) = 0\} = \ker \Phi$.

Comme $\mathbb{K}[X]$ est principal, il existe $P \in \mathbb{K}[X]$ tel que $(P) = Ann(f)$.

**Définition 5.3.3** L'unique polynôme unitaire $\mu_f$ tel que $(\mu_f) = Ann(f)$ est le *polynôme minimal* de $f$.

**Remarque 5.3.4** Un endomorphisme d'un $\mathbb{K}-$ev de dimension finie admet un polynôme minimal.

**Théorème 5.3.3** Le polynôme $\mu_f$ divise $\chi_f$.
**Dém.** : c'est facile d'après Cayley-Hamilton.

**Proposition 5.3.3** Soient $E'$ un sev stable par $f$ et $g = f_{|E'}$. Alors $\mu_g \mid \mu_f$.
**Dém.** : par définition de $\mu_f$, pour tout $x \in E$, $\mu_f(f)(x) = 0$. En particulier, $\forall x \in E' : \mu_f(f)(x) = 0$. Or $g$ coïncide avec $f$ sur $E'$. Donc $\mu_f \in Ann(g)$ et $\mu_g \mid \mu_f$.

**Proposition 5.3.4** Soit $Q$ un facteur irréductible de $\chi_f$. Alors $Q \mid \mu_f$.
**Dém.** : en effet, comme $\ker Q(f)$ est stable par $f$ et que $\mu_f(f_{|\ker Q(f)}) = 0$ on a $Q \mid \mu_f$ car $Q$ est irréductible.

**Corollaire 5.3.1** Soit $\lambda \in Sp(f)$. Alors $\lambda$ est racine de tout polynôme de l'annulateur de $f$.

**Théorème 5.3.4** Soit $f \in L(E)$ un endomorphisme d'un $\mathbb{K}-$ev $E$ de dimension $n$.

$f$ est diagonalisable sur $\mathbb{K}$ ssi $\mu_f$ est scindé sur $\mathbb{K}$ et ses racines sont simples.

**Dém.** :
($\Rightarrow$) Comme $f$ est diagonalisable, $\chi_f$ est scindé sur $\mathbb{K}$. En particulier, $\mu_f$ l'est. Comme $\bigoplus_{\lambda \in Sp(f)} \ker(f - \lambda id_E) = E$, il vient :

$$\forall x \in E : \prod_{\lambda \in Sp(f)} (f - \lambda id_E)(x) = 0.$$

Donc $\mu_f \mid \prod_{\lambda \in Sp(f)} (\lambda - X)$ et ses racines sont simples.

($\Leftarrow$) Notons $\lambda_1, \ldots, \lambda_m$ les racines 2 à 2 distinctes de $\mu_f$. Autrement dit, $\mu_f(X) = \prod_{k=1}^{m} (\lambda_k - X)$.
D'après le théorème des noyaux,

$$\bigoplus_{k=1}^{m} \ker(f - \lambda_k id_E) = E.$$

L'endomorphisme $f$ est donc diagonalisable.

## 5.4 Nilpotence et réduite de Jordan

### 5.4.1 Sous-espaces caractéristiques

**Proposition 5.4.1** Soient $f \in L(E)$ et $\lambda \in Sp(f)$. Alors la suite $(\ker(f-\lambda id_E)^k)_k$ est croissante. De plus, s'il existe $r \in \mathbb{N}$ tel que $\ker(f-\lambda id_E)^{r+1} = \ker(f-\lambda id_E)^r$ alors elle est stationnaire.

**Dém.** : en effet, notons $F_k = \ker(f-\lambda id_E)^k$. Si $x \in F_k$ alors $(f-\lambda id_E)^{k+1}(x) = 0$ donc la suite $(F_k)_k$ est croissante.

Soit $r \in \mathbb{N}$ tel que $F_{r+1} = F_r$. Soit $x \in F_{r+2}$ alors $(f-\lambda id_E)^{r+2}(x) = 0$. Autrement dit $(f-\lambda id_E)^{r+1}((f-\lambda id_E)(x)) = 0$ donc $(f-\lambda id_E)(x) \in F_{r+1} = F_r$ *i.e.* $(f-\lambda id_E)^{r+1}(x) = 0$ ou encore $x \in F_{r+1}$.

**Corollaire 5.4.1** Si $\dim E$ est finie alors $(\ker(f-\lambda id_E)^k)_k$ est stationnaire.

**Théorème 5.4.1 (de décomposition des noyaux)** Supposons que $\chi_f$ soit scindé sur $\mathbb{K}$ *i.e.* $\chi_f(X) = \prod_{k=1}^{p}(\lambda_k - X)^{m_k}$. Alors

$$E = \bigoplus_{k=1}^{p} \ker(f-\lambda_k id_E)^{m_k}.$$

**Dém.** : on applique le théorème des noyaux avec les facteurs $(\lambda - X)^{m_\lambda}$ de $\chi_f$ en remarquant que $\chi_f(f) = 0$.

**Définition 5.4.1** Soit $\lambda \in Sp(f)$ de multiplicité algébrique $m_\lambda$. Le sev $\ker(f-\lambda id_E)^{m_\lambda}$ est le *sous-espace caractéristique* $E_\lambda^c$ associé à $\lambda$.

**Corollaire 5.4.2** Supposons que $\chi_f$ soit scindé sur $\mathbb{K}$. Alors

$$\forall \lambda \in Sp(f) : \dim E_\lambda^c = m_\lambda.$$

**Dém.** : soit $\lambda \in Sp(f)$. Comme $\chi_{f_{|E_\lambda^c}}$ est scindé, $f_{|E_\lambda^c}$ est trigonalisable et les coefficients diagonaux d'une matrice représentative triangulaire sont tous égaux à $\lambda$. Donc $\dim E_\lambda^c \leq m_\lambda$. Comme $\sum_{\lambda' \in Sp(f)} m_{\lambda'} = \dim E$ et que $\chi_f$ est scindé sur $\mathbb{K}$, il s'ensuit que $\dim E_\lambda^c = m_\lambda$.

**Corollaire 5.4.3 (interprétation matricielle)** Si $\chi_f$ est scindé sur $\mathbb{K}$ alors la matrice $A$ de $f$ dans une base adaptée au théorème de décomposition des noyaux est diagonale par bloc du type :

$$A = \begin{pmatrix} A_{\lambda_1} & 0 & \cdots & 0 \\ 0 & A_{\lambda_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_{\lambda_p} \end{pmatrix}.$$

avec $A_{\lambda_i} \in \mathcal{M}_{m_i}(\mathbb{K})$ où $m_i$ est la multiplicité algébrique de la valeur propre $\lambda_i$ de $f$.

### 5.4.2 Nilpotence

**Définition 5.4.2** Un endomorphisme $f$ d'un $\mathbb{K}-$ev $E$ est *nilpotent* s'il existe $r \in \mathbb{N}$ tel que $f^r = 0$. Le plus petit des tel entiers $r$ est l'*indice* de nilpotence de $f$. Par convention, si un tel $r$ n'existe pas alors $r = +\infty$.

**Exemple 5.4.1**

1. On définit généralement la notion de nilpotence dans un anneau $A$. En particulier, si $A$ est intègre alors il n'a pas d'élément nilpotent. Un anneau sans élément nilpotent est un anneau *réduit*.
2. Un endomorphisme diagonalisable est nilpotent ssi il est nul. Plus généralement, si $f$ est nilpotent alors $Sp(f) = \{0\}$. Si $\mu_f$ est scindé sur $\mathbb{K}$ et $Sp(f) = \{0\}$ alors $f$ est nilpotente.

**Remarque 5.4.1** On constate ainsi que l'indice de nilpotence $r_\lambda$ de $(f - \lambda id_E)_{|E_\lambda^c}$ est inférieur ou égal à $m_\lambda$.

**Proposition 5.4.2** Soient $E$ un $\mathbb{K}-$ev de dimension $n$, $\lambda \in Sp(f)$ et $r_\lambda$ l'indice de $g_\lambda$. Alors $r_\lambda$ est la multiplicité algébrique $n_\lambda$ de $\lambda$ dans $\mu_f$.

**Dém.** : le polynôme minimal $\mu_{f_{|E_\lambda^c}} = (\lambda - X)^{r_\lambda}$ divise $\mu_f$. Donc il divise $(\lambda - X)^{n_\lambda}$. Posons $Q = \dfrac{\mu_f}{(\lambda - X)^{n_\lambda}}$. Si $r_\lambda < n_\lambda$ alors $P = (\lambda - X)^{r_\lambda} Q$ annule encore $f$ car $\dim \ker (f - \lambda id_E)^{r_\lambda} = m_\lambda = n - \dim \ker Q(f)$. Or $P$ est de degré strictement plus petit que $\mu_f$ $\rightarrow\leftarrow$.

**Proposition 5.4.3** Soient $\lambda \in Sp(f)$, $\Delta_\lambda = \lambda id_{E_\lambda^c}$ et $g_\lambda = (f - \lambda id_E)_{|E_\lambda^c}$. Alors

$$f_{|E_\lambda^c} = \Delta_\lambda + g_\lambda,$$

où $g_\lambda$ est nilpotente d'indice $r_\lambda$ et, $\Delta_\lambda$ et $g_\lambda$ commutent.

**Corollaire 5.4.4 (interprétation matricielle)** Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice dont le polynôme caractéristique est scindé sur $\mathbb{K}$. Alors il existe une matrice diagonale $D$ et une matrice nilpotente triangulaire supérieure stricte $N$ telles que :

$$A = D + N,\ DN = ND,\ N^r = 0 \text{ avec } r = \max_{\lambda \in Sp(A)} r_\lambda.$$

## 5.5 Applications

### 5.5.1 Suites linéaires

### 5.5.2 Puissance et exponentielle de matrice

### 5.5.3 Système différentiel linéaire à coefficients constants