Algèbre linéaire

Guglielmo Pasa

Notes prises durant le cours du
Pr. Boechat
section de Mathématique
Université de Lausanne
(1991–1992)

L'auteur du document ne répond pas d'un usage illicite de ce document qui est distribué uniquement dans l'espoir qu'il soit utile à quelqu'un.
Le présent cours se veut autant exempt d'erreur que possible, mais, malgré tout le soin que j'y apporte, des erreurs y sont sûrement encore présentes. Si vous en trouvez, veuillez me les indiquer à l'adresse e-mail ci-dessous.
Toute contribution peut être faite directement à l'auteur à l'adresse

guglielmo.pasa@gmail.com.

Toute aide financière peut être faite en envoyant votre part au moyen d'un bulletin de versement à :

Pasa Guglielmo
Rte des Cases 17A
CH-1890 **St-Maurice**.

Dans ce dernier cas veuillez noter une adresse e-mail ou postale où il me sera possible de vous communiquer de nouvelles versions de ce document.

Ce document a été écrit en LaTeX en utilisant MikTeX v. 1.08 et PDFLaTeX 0.11, avec les options de AMS-LaTeX.

Table des matières

Chapitre 0

Notions préliminaires

0.1 Quelques définitions

Definition 1

L'ensemble des parties d'un ensemble E, $\mathcal{P}(E)$, est l'ensemble de tous les sous-ensembles de E.

On a toujours $\emptyset \in \mathcal{P}(E)$, $E \in \mathcal{P}(E)$.

Definition 2

Une *partition* de E est un ensemble de parties de E deux à deux disjointes, telles que leurs réunion donne E.

Definition 3

Une *fonction* (ou *application*) $f : E \to F$ est une correspondance qui associe à tout élément x de E un unique élément $f(x)$ de F.

f est dite :

- surjective : si : $f(E) = F$.
- injective : si : $x \neq x' \Rightarrow f(x) \neq f(x')$.
- bijective : si : f est injective et surjective.

0.2 généralités

Si f est bijective il existe une fonction $f^{-1} : F \to E$ réciproque de f telle que $f(f^{-1}(y)) = y$ pour tout $y \in F$ et $f^{-1}(f(x)) = x$ pour tout $x \in E$.

L'ensemble des fonctions de E dans F se note $\mathcal{F}(E, F)$ ou F^E. $F \times \cdots \times F$ s'identifie avec $F^{\mathbb{N}_n}$ que l'on écrit F^n.

Soit A une partie de E et B une partie de F. Soit encore f une fonction de E vers F. On appelle l'*image* (directe) de A par f l'ensemble $f(A) = \{f(x)|x \in A\}$, et l'*image réciproque* de B par f l'ensemble $f^{-1}(B) = \{x \in E|f(x) \in B\}$.

Un ensemble E est dit fini s'il existe $n \in \mathbb{N}$ et une bijection $f : E \to \mathbb{N}_n$. Dans ce cas n est unique et est appelé le *cardinal* de E, que l'on note : $Card(E) = n$.

Si $f : E \to F$ est une fonction avec $Card(E) = Card(F) = n < \infty$, alors :

$$f \text{ est injective } \Leftrightarrow f \text{ est surjective } \Leftrightarrow f \text{ est bijective.}$$

Si E et F sont des ensembles finis, alors :
- $Card(E \times F) = Card(E) \cdot Card(F)$
- $Card(F^E) = Card(F)^{Card(E)}$
- $Card(E \cup F) + Card(E \cap F) = Card(E) + Card(F)$

Definition 4 (relation d'équivalence)

Une relation binaire $\mathcal{R}$ de $E \times E$ est une *relation d'équivalence* si :
- $\mathcal{R}$ est *réflexive* : $x\mathcal{R}x \quad \forall x \in E$,
- $\mathcal{R}$ est *symétrique* : $x\mathcal{R}y \Rightarrow y\mathcal{R}x \quad \forall x, y \in E$,
- $\mathcal{R}$ est *transitive* : $x\mathcal{R}y$ et $y\mathcal{R}z \Leftrightarrow x\mathcal{R}z$.

Dans ce cas l'ensemble $[x]_{\mathcal{R}} = \{y \in E | y\mathcal{R}x\}$ est appelé la *classe d'équivalence de $x \in E$ pour $\mathcal{R}$*. L'ensemble $\frac{E}{\mathcal{R}}$ des classes d'équivalence est une partition de E et s'appelle l'*ensemble quotient* de E par $\mathcal{R}$. La surjection canonique de E sur $\frac{E}{\mathcal{R}}$ est $x \mapsto [x]_{\mathcal{R}}$.

0.3 Notions et résultats divers

Soit $*$ une loi sur E. On dit qu'une partie $A \subset E$ est *stable* pour $*$ si $x * y \in A$ pour tout $x, y \in A$. La restriction de $*$ à A définit une *loi induite* par celle de E.

Si $*$ est une loi associative et si on a des éléments qui commutent alors la composition de ces éléments est indépendante de leur ordre et de celui des parenthèses.

On dit que $e \in E$ est *neutre* si $x * e = e * x = x \quad \forall x \in E$, e est unique.

On dit que $a \in E$ est *simplifiable* si pour tout $x, y \in E$:

$$x = y \Leftrightarrow a * x = a * y \Leftrightarrow x * a = y * a.$$

On dit que $y \in E$ est inverse de x si $x * y = y * x = e$.

Théorème 0.1

Soit $*$ une loi de composition associative sur E, admettant l'élément neutre e. Alors :

a) tout élément inversible est simplifiable,

b) pour chaque élément inversible il n'y a qu'un inverse.

Preuve. démonstration. □

Théorème 0.2

Soit $*$ une loi de composition associative sur E admettant l'élément neutre e. Si $x, y \in E$ sont inversibles, alors $x * y$ l'est également et on a : $(x * y)' = y' * x'$.

Preuve. démo. □

Chapitre 1

Groupes, Anneaux et Corps

1.1 Groupes

Definition 1 (Groupe)

Un groupe est un ensemble G muni d'une loi de composition :
- associative,
- admettant un élément neutre,
- telle que tout élément a un inverse.

Si de plus la loi est commutative, le groupe est dit *abélien* ou *commutatif*.

Remarque 1

On utilise essentiellement deux notations pour la loi d'un groupe :
1) *notation multiplicative :* $(x, y) \mapsto xy$, l'élément neutre se note alors 1 ou e, et l'inverse de x se note x^{-1}.
2) *notation additive :* $(x, y) \mapsto x + y$, l'élément neutre se note 0, l'inverse de x se note $-x$ et s'appelle l'opposé de x.

La notation additive ne s'utilisera que pour des groupes abéliens.

Théorème 1.1

Soit G un groupe. On a alors :
1) Tout élément $x \in G$ est simplifiable.
2) Si $a, b \in G$, alors :
   a) il existe un unique $x \in G$ tel que $ax = b$,
   b) il existe un unique $x \in G$ tel que $xa = b$.

Preuve. 1) Soit $x \in G$, x est inversible et on a, pour $a, b \in G$, si :

$$x * a = x * b,$$

par composition avec x', l'inverse de x :

$$a = e * a = (x' * x) * a = x' * (x * a) = x' * (x * b) = (x' * x) * b = e * b = b,$$

Ainsi :

$$x * a = x * b \Rightarrow a = b.$$

2) On a :

$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$

donc $x = a^{-1}b$ est une solution de $ax = b$.
Si x' est tel que $ax' = b$, alors $ax = ax'$, or a est simplifiable, donc :

$$x = x'.$$

□

Definition 2 (Sous-groupe)

Soit G un groupe. On appelle *sous-groupe* de G une partie H de G telle que :
1) $e \in H$,
2) $\forall x, y \in G : (x \in H \text{ et } y \in H) \Rightarrow xy \in H$,
3) $\forall x \in G : x \in H \Rightarrow x^{-1} \in H$.

Dans ce cas H est un groupe pour la même loi que G, i.e. pour la loi induite par celle de G.

Definition 3

Soient $\mathcal{G}, \mathcal{G}'$ deux groupes. On appelle *homomorphisme* (de groupe) de G dans G' toute application $f : \mathcal{G} \to \mathcal{G}'$ telle que :

$$f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

On utilise encore les terminologies suivantes :
— Un homomorphisme (de groupe) bijectif est appelé un *isomorphisme* (de groupe.)
— Dans ce cas $f^{-1} : \mathcal{G}' \to \mathcal{G}$ est aussi un homomorphisme.
— Un isomorphisme de $\mathcal{G}$ dans lui-même s'appelle un *automorphisme* de $\mathcal{G}$.
— Deux groupes $\mathcal{G}$ et $\mathcal{G}'$ sont dits *isomorphes* s'il existe un isomorphisme de l'un sur l'autre.

Exemple 1

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des groupes abéliens pour l'addition usuelle.
2. $\mathbb{R}^*, \mathbb{Q}^*, \{-1, +1\}$ sont des groupes abéliens pour la multiplication usuelle.
3. $\mathbb{Z}, \mathbb{Q}$ sont des sous-groupes de $\mathbb{R}$ pour l'addition.
4. $\{-1, +1\}, \mathbb{Q}^*$ sont des sous-groupes de $\mathbb{R}^*$ pour la multiplication.
5. $\log$ est un isomorphisme de $\mathbb{R}_+^*$ (muni de la multiplication) sur $\mathbb{R}$ (muni de l'addition.)
6. $\{e\}, \mathcal{G}$ sont des sous-groupes de G.
7. Soit $\mathcal{G}$ un groupe et $x \in \mathcal{G}$, l'application de $\mathbb{Z} \to \mathcal{G}$ définie par $n \mapsto x^n$ (pour tout $n \in \mathbb{Z}$) est un homomorphisme de groupe (de $(\mathbb{Z}, +)$.) C'est l'unique homomorphisme de $\mathbb{Z}$ vers G qui envoie 1 sur l'élément x.
8. Soit $\mathcal{G}$ un groupe abélien et $n \in \mathbb{Z}$. L'application de $\mathcal{G} \to \mathcal{G}$ définie par $x \mapsto x^n$ (pour tout $x \in \mathcal{G}$) est un homomorphisme de groupe.

9. Soit X un ensemble quelconque. L'ensemble $\mathrm{Perm}(X)$ de toutes les permutations (i. e. des bijections de X sur X) de X est un groupe pour la composition $(f, g) \mapsto f \circ g$ (où f et g sont des applications dans X.) L'élément neutre est l'application de X, id_X, définie par $\mathrm{id}_X(x) = x$ pour tout $x \in X$ et l'inverse de f est la permutation réciproque f^{-1}. Ce groupe $(\mathrm{Perm}(X), \circ)$ n'est pas abélien si $\mathrm{Card}(X) \geq 2$ ou si X est infini.

Théorème 1.2

Si $f : G \to G'$ et $g : G' \to G''$ sont des homomorphismes de groupes alors $g \circ f : G \to G''$ est encore un homomorphisme de groupe.

Théorème 1.3

Si $f : G \to G'$ est un isomorphisme de groupes alors Si $f^{-1} : G' \to G$ est aussi un isomorphisme de groupes.

Théorème 1.4

Soit $f : G \to G'$ un homomorphisme de groupes, alors :

1. $f(e) = e'$.
2. $f(x^{-1}) = f(x)^{-1}, \forall x \in G$.

où e et e' sont les éléments neutres de G et G'.

Preuve.

1. $f(e)f(e) = f(e \cdot e) = f(e) = f(e)e'$, d'où :
$$f(e) = e'.$$
2. Soit $x \in G$:
$$f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'.$$
Ainsi :
$$f(x^{-1}) = f(x)^{-1},$$
car dans un groupe : $xy = e \Leftrightarrow x = y^{-1}$.

$\square$

Théorème 1.5

Soit $f : G \to G'$ un homomorphisme de groupes.

a) Si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'.
b) Si H' est un sous-groupe de G', alors $f^{-1}(H')$ est un sous-groupe de G.

Definition 4

Si $f : G \to G'$ est un homomorhisme de groupes, le sous-groupe $f^{-1}(\{e'\})$ s'appelle le *noyau de* f et se note $\ker\ f$.

Théorème 1.6

Soit $f : G \to G'$ un homomorphisme de groupes, alors :

$$\ker f = \{e\} \Leftrightarrow f \text{ est injective.}$$

Théorème 1.7

Si H est un sous-groupe de $\mathbb{Z}$ alors il existe $n \in \mathbb{N}$ tel que : $H = n\mathbb{Z}$.

Definition 5

On appelle *congruence sur* G. un groupe, toute relation d'équivalence $\mathcal{R}$ sur G qui a les propriétés suivantes :

$$\forall x, x', y, y' \in G \ : \ \text{si } x\mathcal{R}y,\ x'\mathcal{R}y', \quad \text{alors : } xx'\mathcal{R}yy'.$$

Si $\mathcal{R}$ est une congruence, on définit alors sur $\frac{G}{\mathcal{R}}$ la loi de composition :

$$[x]_{\mathcal{R}}[y]_{\mathcal{R}} = [xy]_{\mathcal{R}}.$$

Alors $\frac{G}{\mathcal{R}}$ muni de cette loi est un groupe.

Definition 6

Soit G un groupe, $x \in G$ et $\phi : \mathbb{Z} \to G$ définie par $\phi(n) = x^n\ \forall n \in \mathbb{Z}$. Alors $\phi(\mathbb{Z}) = \{x^n | n \in \mathbb{Z}\} =< x >$ est un sous-groupe de G contenant x. On dit que $< x >$ est le *sous-engendré par* x.

G est dit cyclique s'il existe $x \in G$ tel que : $G =< x >$.

Definition 7

Si G est un groupe est $x \in G$, on appelle *ordre* de x le nombre d'éléments de $< x >$.

Exemple 2

1.2 Groupes symétriques

Definition 8

Soit $n \in \mathbb{N}$. On appelle *groupe symétrique de degré* n, et on notera $\mathcal{S}_n$, le groupe $Perm(\mathbb{N}_n)$. Pour $\sigma \in \mathcal{S}_n$, on désigne par :

— $\mathrm{Fix}(\sigma) = \{i \in \mathbb{N}_n | \sigma(i) = i\}$ l'ensemble des points fixes par σ,

— $\mathrm{supp}(\sigma) = \{i \in \mathbb{N}_n | \sigma(i) \neq i\}$ le *support* de σ.

La loi de composition de $\mathcal{S}_n$ est la composition des applications que l'on notera toujours multiplicativement.

Definition 9

Deux permutations $\sigma, \tau \in \mathcal{S}_n$ sont dites *disjointes* si :

$$\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$$

On a alors : $\sigma\tau = \tau\sigma$.

Théorème 1.8

Toute permutation peut s'écrire comme un produit de cycles deux à deux disjoints.

Definition 10

Le cardinal m du support d'une permutation est la longueur du cycle définissant la permutation, on appelle cette permutation un m-cycle, ou cycle de longueur m.

Les 2-cycles s'appellent aussi *transpositions*.

Théorème 1.9

Toute permutation $\sigma \in \mathcal{S}_n$, $n \geq 2$ est un produit de transpositions.

Definition 11

soit $\mathcal{P}_{k,n}$ $(0 \leq k \leq n)$, l'ensemble des parties à k éléments de $\mathbb{N}_n$. Si $\sigma \in \mathcal{S}_n$, $n \geq 2$, on définit la *signature de* σ par :

$$\mathrm{sign}(\sigma) = \prod_{\{i,j\} \in \mathcal{P}_{2,n}} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{\{i,j\} \in \mathcal{P}_{2,n}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}$$

Théorème 1.10

Si $n \geq 2$ et $\sigma, \tau \in \mathcal{S}_n$, alors $\text{sign}(\sigma\tau) = \text{sign}(\sigma)\sigma(\tau)$, i. e. : $\text{sign} : \mathcal{S}_n \to \mathbb{R}^*$ est un homomorphisme de groupes.

Lemme 1.11

Soit G un groupe fini et $\phi : G \to \mathbb{R}^*$ un homomorphisme de groupes, alors : $\phi(x) = \pm 1, \forall x \in \mathcal{G}$.

Corollaire 1.12

Si $n \geq 2$, la signature est un homomorphisme de $\mathcal{S}_n$ dans le groupe multiplicatif $\{-1, 1\}$.

Corollaire 1.13

Si $n \geq 2$ et $\sigma \in \mathcal{S}_n$, on a : $\text{sign}(\sigma) = (-1)^\nu$, où ν est le nombre de paires $\{i, j\} \in \mathcal{P}_{2,n}$ telles que $\frac{\sigma(i)-\sigma(j)}{i-j} < 0$, i. e. :

$$\nu = \text{Card}(\{(i, j) \in \mathbb{N}_n \times \mathbb{N}_n | i < j \text{ et } \sigma(i) > \sigma(j)\}).$$

Théorème 1.14

Si $\tau \in \mathcal{S}_n$ $(n \geq 2)$ est une transposition, alors : $\text{sign}(\tau) = -1$.

Corollaire 1.15

Si $\sigma \in \mathcal{S}_n$ $(n \geq 2)$ est le produit de m transpositions, alors : $\text{sign}(\sigma) = (-1)^m$.

Corollaire 1.16

Si $\tau_1, \ldots, \tau_m$ et $\tau'_1, \ldots, \tau'_l$ sont des transpositions telles que $\tau_1 \ldots \tau_m = \tau'_1 \ldots \tau'_l$, alors m et l ont même parité.

Definition 12

Si σ est un k-cycle, $\text{sign}(\sigma) = (-1)^{k-1}$. Les permutations de signature $+1$ (resp. -1) sont dites *paires (impaires)*.

L'ensemble des permutations paires forment le noyau de l'homomorphisme $\text{sign} : \mathcal{S}_n \to \{-1, 1\}$. C'est un sous-groupe de $\mathcal{S}_n$ qui est appelé le *groupe alterné de degré* n et est noté : $\mathcal{A}lt_{\ n}$.

On a :

$$\mathrm{Card}(\mathcal{A}lt_{\,n}) = \frac{1}{2}\mathrm{Card}(\mathcal{S}_n) = \frac{n!}{2}.$$

1.3 Anneaux et Corps

Definition 13

Un *anneau* est un ensemble $\mathbb{A}$ muni de deux lois $(+,\cdot)$ vérifiants les conditions suivantes :

1. $(\mathbb{A},+)$ est un groupe abélien ;
2. la multiplication est associative et admet un élément neutre : $1_{\mathbb{A}}$;
3. la multiplication est distributive. $\forall x,y \in \mathbb{A}$:
   a) $x(y+z) = xy + xz$,
   b) $(x+y)z = xz + yz$.

L'anneau est dit *commutatif* si la multiplication est commutative.

Proposition 1.17

1) $k(xy) = (kx)y = x(ky),\ \forall k \in \mathbb{Z},\ \forall x,y \in \mathbb{A}$;
2) $0x = x0 = 0,\ \forall x \in \mathbb{A}$,
   $(-1)x = -x = x(-1)$;
3) $x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n$,
   $$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j;$$
4) Si $xy = yx$, on a : $(x+y)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$, où $\dbinom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

Definition 14

vocabulaire $x \in \mathbb{A}$ est dit :

1. *nilpotent* s'il existe $n \geq 1$ tel que $x^n = 0$,
2. *idempotent* si $x^2 = x$,
3. *inversible* s'il est inversible pour la multiplication,
4. *simplifiable* s'il est simplifiable pour le multiplication.

Definition 15

Un anneau $\mathbb{A}$ est :

1. dit *intègre* si $\mathbb{A} \neq \{0\}$, $\mathbb{A}$ est commutatif et tout élément non nul est simplifiable,

2. un *corps* si $\mathbb{A} \neq \{0\}$, $\mathbb{A}$ est commutatif et tout élément non nul est inversible.

Tout corps est intègre.

Théorème 1.18

Soit $\mathbb{A}$ un anneau intègre. Il existe un corps $\mathbb{K}$, dit *corps des fractions de* $\mathbb{A}$, qui a les propriétés suivantes :

a) il existe un homomorphisme d'anneau $a \mapsto \tilde{a}$ de $\mathbb{A}$ dans $\mathbb{K}$,
b) tout $x \in \mathbb{K}$, $x \neq 0$, peut s'écrire $\tilde{a}\tilde{b}^{-1}$ pour certains $a, b \in \mathbb{A}$, avec $b \neq 0$.

Definition 16

Soit $\mathbb{A}$ un anneau. Un *sous-anneau* de $\mathbb{A}$ est une partie $\mathbb{B} \subset \mathbb{A}$ telle que :

1. $\forall\, x, y \in \mathbb{B} \; : \; x + y \in \mathbb{B}$
2. $\forall\, x, y \in \mathbb{B} \; : \; xy \in \mathbb{B}$
3. $-1_{\mathbb{A}} \in \mathbb{B}$.

Definition 17

Soient $\mathbb{A}$ et $\mathbb{B}$ des anneaux. On appelle *homomorphisme d'anneaux* toute application $f : \mathbb{A} \to \mathbb{B}$ telle que :

1. $f(x+y) = f(x) + f(y) \; \forall\, x, y \in \mathbb{A}$,
2. $f(xy) = f(x)f(y) \; \forall\, x, y \in \mathbb{A}$,
3. $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$

Definition 18

Soit ϕ l'homomorphisme de $\mathbb{Z}$ vers $\mathbb{A}$ défini par $n \mapsto n \cdot 1_{\mathbb{A}}$. L'entier $n \geq 0$ déterminé par la condition :

$$\ker \phi = \{m \in \mathbb{Z} | \phi(m) = 0\} = n\mathbb{Z}$$

s'appelle la caractéristique de l'anneau $\mathbb{A}$. Si $1_{\mathbb{A}}$ est d'ordre infini, alors $n = 0$; si $1_{\mathbb{A}}$ est d'ordre fini, alors $n > 0$.

Théorème 1.19

Si $\mathbb{A}$ est un anneau intègre, sa caractéristique est un nombre premier ou nul.

1.4 Les nombres complexes

Definition 19

L'*ensemble de nombres complexes* $\mathbb{C}$ est l'ensemble $\mathbb{R} \times \mathbb{R}$ muni de l'addition et de la multiplication suivantes :

$$(a,b) + (a',b') = (a+a', b+b')$$
$$(a,b) \cdot (a',b') = (aa' - bb', ab' + a'b)$$

En identifiant $(a,0) = a \in \mathbb{R}$ et en posant $i = (0,1)$, on a :

i) $i^2 = -1$,

ii) $z = (a,b) \in \mathbb{C}$ s'écrit : $z = a + bi$, $a, b \in \mathbb{R}$.

On appelle :

$\Re(z) = a$ la *partie réelle* de z,
$\Im(z) = b$ la *partie imaginaire* de z,
bi avec $b \in \mathbb{R}$ un nombre *imaginaire pur*.

Definition 20

On appelle *module* d'un nombre complexe $z = a + bi$, le nombre réel positif ou nul

$$|z| = \sqrt{a^2 + b^2} \in \mathbb{R}_+$$

On vérifie sans peine que

$$|z + z'| \leq |z| + |z'|,$$
$$|zz'| = |z|\,|z'|.$$

Definition 21

On appelle *conjugué* d'un nombre complexe $z = a + bi$ le nombre complexe $\bar{z} = a - bi$.

Propriété 1.20

La conjugaison est un automorphisme de corps de $\mathbb{C}$ d'ordre 2. On a :

i) $\overline{z + z'} = \bar{z} + \bar{z}'$, $\forall z, z' \in \mathbb{C}$,

ii) $\overline{zz'} = \bar{z}\bar{z}'$, $\forall z, z' \in \mathbb{C}$,

iii) $\bar{z} = z \Leftrightarrow z \in \mathbb{R}$

iv) $\bar{z} = -z \Leftrightarrow z \in i\mathbb{R}$

v) $\bar{\bar{z}} = z$, $\forall z \in \mathbb{C}$

vi) $\bar{1} = 1$.

Definition 22

Soit le nombre complexe défini par $z = \rho(\cos(\theta) + i\sin(\theta)) = \rho \operatorname{cis} \theta$, avec $\rho = |z|$. θ est appelé l'*argument* de z.

Si $z = a + bi$ on a :

$$\cos\theta = \frac{a}{\sqrt{a^2+b^2}}$$
$$\sin\theta = \frac{b}{\sqrt{a^2+b^2}}$$

Propriété 1.21

$$zz' = \rho\rho'(\cos(\theta+\theta') + i\sin(\theta+\theta')) = \rho\rho' \operatorname{cis}(\theta+\theta').$$

Théorème 1.22

Soit $n \geq 1$ entier et $z = \rho(\cos(\theta) + i\sin(\theta)) \neq 0$. Alors z admet exactement n racines n-ièmes dans $\mathbb{C}$.

1.5 Suppléments

Definition 23

Si $f : X \to Y$, on appelle *support* de f l'ensemble :
$$\operatorname{supp} f = \{x \in X \mid f(x) \neq 0\}.$$

On note $\mathbb{K}^{(X)}$ l'ensemble des applications de X dans $\mathbb{K}$ à support fini. $\mathbb{K}^{(X)}$ est un sous espace de $\mathbb{K}^X$. Naturellement :
$$\mathbb{K}^{(X)} = \mathbb{K}^X \Leftrightarrow X \text{ est fini.}$$

Théorème 1.23

Tout anneau intègre fini est un corps.

Definition 24

Soit $\mathbb{A}$ un anneau et $S \subset \mathbb{A}$. On appelle *centraliseur de* S le sous-anneau de $\mathbb{A}$:
$$C(S) = \{a \in \mathbb{A} \,|\, as = sa\ \forall s \in \S\},$$
et on appelle *centre de* $\mathbb{A}$ le sous-anneau de $\mathbb{A}$:
$$Z(\mathbb{A}) = \{a \in \mathbb{A} \,|\, ab = ba\ \forall b \in \mathbb{A}\}.$$

Théorème 1.24

Soit $(G, +)$ un groupe abélien. $(\operatorname{End}(G), +, \circ)$ est un anneau.

Chapitre 2

Espaces Vectoriels

2.1 Définitions

Definition 1

Soit $\mathbb{K}$ un corps. Un *espace vectoriel sur* $\mathbb{K}$ ou $\mathbb{K}$-*espace vectoriel* est un groupe abélien V (que l'on notera additivement) muni d'une *action* de $\mathbb{K}$, i. e.d'une application $\mathbb{K} \times V \to V$ remplissant les conditions suivantes :

1. $\lambda(\mu x) = (\lambda\mu)x, \quad \forall \lambda, \mu \in \mathbb{K}$ et $\forall x \in V$.
2. $1_{\mathbb{K}} x = x, \quad \forall x \in V$.
3. $\lambda(x + y) = \lambda x + \lambda y, \quad \forall \lambda \in \mathbb{K}, \forall x, y \in V$
4. $(\lambda + \mu)x = \lambda x + \mu x, \quad \forall \lambda, \mu \in \mathbb{K}, \forall x \in V$.

Proposition 2.1

1. $k(\lambda x) = (k\lambda)x = \lambda(kx), \ \forall k \in \mathbb{Z}, \forall \lambda \in \mathbb{K}, \forall x \in V,$
2. $-(\lambda x) = (-\lambda)x = \lambda(-x), \ \forall \lambda \in \mathbb{K}, \forall x \in V,$
3. Si $\lambda \in \mathbb{K}$ et $x \in V$, on a : $\lambda x = 0_V \Leftrightarrow (\lambda = 0_{\mathbb{K}}$ ou $x = 0_V)$
4. Si $k \in \mathbb{Z}$ et $x \in V$, on a : $kx = 0_V \Leftrightarrow (x = 0_V$ ou k est un multiple de la caractéristique de $\mathbb{K})$

Notation et terminologie

1. Soit V un $\mathbb{K}$-espace vectoriel. On appelle les éléments de $\mathbb{K}$ des *scalaires* et les éléments de V des *vecteurs*.
2. Les $\mathbb{R}$-espaces vectoriels sont aussi appelés *espaces vectoriels réels* et les $\mathbb{C}$-espaces vectoriels *espaces vectoriels complexes*.

Exemple 1

1. Sur tout ensemble à un élément il existe une unique structure de $\mathbb{K}$-espace vectoriel.
2. Tout corps $\mathbb{K}$ peut être vu comme un espace vectoriel sur lui-même. L'action de $\mathbb{K}$ étant la multiplication.

3. Soit X un ensemble quelconque et $\mathbb{K}$ un corps. Alors l'ensemble K^X (ou $\mathcal{F}(X, \mathbb{K})$) des applications de X dans $\mathbb{K}$, est un $\mathbb{K}$-espace vectoriel pour l'addition et l'action de $\mathbb{K}$ définie par les formules suivantes :
   i) Si $f, g \in \mathbb{K}^X$, $f + g : X \to \mathbb{K}$ est définie par :
   $$(f+g)(x) = f(x) + g(x), \quad \forall x \in X$$
   ii) Si $\lambda \in \mathbb{K}$ et $f \in \mathbb{K}^X$, $\lambda f : X \to \mathbb{K}$ est définie par :
   $$(\lambda f)(x) = \lambda f(x) \quad \forall x \in X$$
4. Soit W un $\mathbb{K}$-espace vectoriel et X un ensemble. Alors l'ensemble W^X est un $\mathbb{K}$-espace vectoriel. L'addition et l'action de $\mathbb{K}$ étants définies comme ci-dessus, $\forall x \in X$:
   $$(f+g)(x) = f(x) + g(x)$$
   $$(\lambda f)(x) = \lambda f(x).$$
5. (Cas spécial de 3.) : On prend $X = \mathbb{N}_n$. $\mathbb{K}^X$ devient alors $\mathbb{K}^n = \mathbb{K} \times \cdots \times \mathbb{K}$. L'addition et l'action deviennent :
   i) $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$
   ii) $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$
6. Soient $V_1, \ldots, V_n$ des $\mathbb{K}$-espaces vectoriels. Sur le produit cartésien $V = V_1 \times \cdots \times V_n$ on peut définir une structure de $\mathbb{K}$-espace vectoriel à l'aide des opérations suivantes :
   i) $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$,
   ii) $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$,
   $\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in V$, $\forall \lambda \in \mathbb{K}$.
7. Soit $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps (par exemple $\mathbb{L} = \mathbb{C}$ et $\mathbb{K} = \mathbb{R}$). $\mathbb{L}$ peut être considéré comme un $\mathbb{K}$-espace vectoriel. L'addition étant celle de $\mathbb{L}$ et l'action de $\mathbb{K}$ sur $\mathbb{L}$ étant obtenue en restreignant à $\mathbb{K} \times \mathbb{L}$ la multiplication de $\mathbb{L} \times \mathbb{L} \to \mathbb{L}$.
8. Soit $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps. Tout $\mathbb{L}$-espace vectoriel V peut être vu comme un $\mathbb{K}$-espace vectoriel comme suit :
   — l'addition est celle de V,
   — l'action de $\mathbb{K}$ sur V étant obtenue en restreignant à $\mathbb{K} \times V$ l'action de $\mathbb{L}$ sur V.
9. Soit V un $\mathbb{C}$-espace vectoriel. On définit le conjugué de V, $\bar{V}$, de la façon suivante :
   — $\bar{V} = V$ comme ensemble.
   — l'addition de $\bar{V}$ est la même que celle de V.
   — l'action de $\mathbb{C}$ sur $\bar{V}$ est l'application $\mathbb{C} \times \bar{V} \to \bar{V}$ telle que $(\lambda, x) \mapsto \lambda \star x$ est définie par : $\lambda \star x = \bar{\lambda} x$ ($\lambda \in \mathbb{C}, x \in V$).
10. Soit V un groupe abélien, noté additivement. Supposons qu'il existe un nombre premier p tel que $px = \underbrace{x + x + \cdots + x}_{p \text{ fois}} = 0$ pour tout $x \in V$. Il s'en suit que si $k, l \in \mathbb{Z}$ sont tels que $k \equiv l \mod p$, alors $kx = lx \; \forall x \in V$. En effet
    $$kx - lx = (k - l)x = (mp)x = m(px) = m0 = 0.$$
    Cela permet de définir une action de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ sur V par la règle $(k)_p x = kx$. Comme p est premier, $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps. On a une action de $\mathbb{F}_p$ sur V qui vérifie tous les axiomes d'espace vectoriel sur $\mathbb{F}_p$.

11. Soit X un ensemble quelconque et soit $V = \mathcal{P}(X)$. On définit une addition sur V comme suit. Pour tout $A, B \in V$:

$$A + B = (A \backslash B) \cup (B \backslash A) = A \triangle B$$

la différence symétrique de A et B.

On vérifie que V est un groupe abélien pour cette addition. Clairement, pour tout $A \in V$, on a $2A = A + A = \emptyset$. Remarquons de plus que $\emptyset$ est l'élément neutre de V pour cette addition. V est donc un espace vectoriel sur le corps à deux éléments $\mathbb{F}_2$.

12. Les vecteurs de la géométrie euclidienne en dimension 2 ou 3. Si on introduit un système de coordonnées, ce qui donne une bijection du plan sur $\mathbb{R}^2$ ou de l'espace sur $\mathbb{R}^3$ cela permet de transporter les structures de $\mathbb{R}$-espace vectoriels de $\mathbb{R}^2$ (resp. $\mathbb{R}^3$) en une structure de $\mathbb{R}$-espace vectoriel du plan (resp. de l'espace).

On représente le vecteur correspondant à (x, y) par le segment orienté $\vec{OP}$, où O est le point correspondant à $(0, 0)$ et P à (x, y). Les opérations d'espace vectoriel correspondant aux constructions géométriques bien connues.

Definition 2

Soit V un $\mathbb{K}$-espace vectoriel. On dit qu'une partie $W \subset V$ est un sous-espace vectoriel si

i) $0_V \in W$

ii) Si $x, y \in W$ alors $x + y \in W$

iii) Si $x \in W$ et $\lambda \in \mathbb{K}$ alors $\lambda x \in W$.

Il est immédiat que W est alors lui-même un espace vectoriel pour les mêmes opérations.

Definition 3

Soit V et W deux $\mathbb{K}$-espaces vectoriels. Une application $f : V \to W$ est une application linéaire si :

i) $f(x + y) = f(x) + f(y), \forall x, y \in V$,

ii) $f(\lambda x) = \lambda f(x), \forall \lambda \in \mathbb{K}$ et $\forall x \in V$.

Théorème 2.2

a) Si $f : V \to W$ et $g : W \to U$ sont des applications linéaires, alors l'application $g \circ f : V \to U$ l'est aussi.

b) Si $f : V \to W$ est une application linéaire bijective, alors $f^{-1} : W \to V$ est aussi un *isomorphisme linéaire*.

Théorème 2.3

Soit $f : V \to W$ une application linéaire, alors :

a) Si U est un sous-espace vectoriel de V, alors $f(U)$ est un sous-espace vectoriel de W.

b) Si U est un sous-espace vectoriel de W, alors $f^{-1}(U)$ est un sous-espace vectoriel de V.

Théorème 2.4

L'ensemble des applications linéaires de V dans W est un sous-espace vectoriel de $\mathcal{F}(V, W)$, que l'on note $\mathcal{L}(V, W)$.

Definition 4

Soit $f : V \to W$ une application linéaire. On appelle respectivement la *noyau de* f et *l'image de* f les ensembles :

$$\ker f = \{x \in V | f(x) = 0_W\} = f^{-1}(\{0_W\}),$$

$$\mathrm{im} f = \{y \in W | \exists x \in V \text{ tq } f(x) = y\} = f(V).$$

Ce sont des sous-espaces vectoriels. Clairement f est surjective si et seulement si $\mathrm{im} f = W$.

Théorème 2.5

Soit $f : V \to W$ une application linéaire, alors :

$$f \text{ est injective } \Leftrightarrow \ker f = \{0\}.$$

Théorème 2.6

Si $(U_\alpha)_{\alpha \in A}$ est une famille de sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel V, alors $\bigcap_{\alpha \in A} U_\alpha$ est encore un sous-espace vectoriel de V

Par convention, si $A = \emptyset$ on pose : $\bigcap_{\alpha \in A} U_\alpha = V$.

Definition 5

Soit V un $\mathbb{K}$-espace vectoriel et $A, B \subset V$. On définit :

$$A + B = \{x + y | x \in A \text{ et } y \in B\}.$$

Théorème 2.7

Si V_1, V_2 sont des sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel V, alors $V_1 + v_2$ est aussi un sous-espace vectoriel de V.

Théorème 2.8 (modularité)

Soient W_1, W_2, F des sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel V. Si $W_1 \subset W_2$, alors :

$$W_2 \cap (W_1 + F) = W_1 + (W_2 \cap F).$$

Corollaire 2.9

Soient W_1, W_2, F des sous-espaces vectoriels d'un $\mathbb{K}$-espace V. On suppose que $W_1 \subset W_2$, $W_1 \cap F = W_2 \cap F$ et $W_1 + F = W_2 + F$, alors : $W_1 = W_2$.

Definition 6

Soient V un $\mathbb{K}$-espace vectoriel et $S \subset V$. L'intersection de tous les sous-espaces vectoriels qui contiennent S est un sous-espace vectoriel de V que l'on note $\mathrm{vect}(S)$, et que l'on appelle le *sous-espace vectoriel engendré par* S. Clairement $\mathrm{vect}(S)$ est le plus petit de tous les sous-espaces vectoriels de V qui contiennent S.

Definition 7

Soient V un $\mathbb{K}$-espace vectoriel et $S \subset V$.L'élément $x \in V$ est une *combinaison linéaire* des éléments de S, s'il existe $x_1, \ldots, x_n \in S$ et $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que :

$$x = \lambda_1 x_1 + \cdots + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i.$$

Par convention, si $n = 0$, $\sum_{i=1}^{n} \lambda_i x_i = 0$.

Théorème 2.10

Si V est un $\mathbb{K}$-espace vectoriel et $S \subset V$, alors $\mathrm{vect}(S)$ est l'ensemble de toutes les combinaisons linéaires des éléments de S.

2.2 Sommes directe et Projecteurs

Théorème 2.11

Soient $V_1, \ldots, V_n$ des sous-espaces d'un $\mathbb{K}$-espace vectoriel V. Les conditions suivantes sont équivalentes :

1. Pour tout choix de $x_1 \in V_1, \ldots, x_n \in V_n$, on a :

$$x_1 + \cdots + x_y = 0 \Leftrightarrow x_1 = \cdots = x_n = 0.$$

2. Pour chaque $x \in V_1 + \cdots + v_n$, les vecteurs $x_1 \in V_1, \ldots, x_n \in V_n$, tels que $x_1 + \cdots + x_n = x$

sont uniques.

3. Pour chaque $i = 1, \ldots, n$, on a : $V_i \cap (\sum_{j \neq i} V_j) = \{0\}$.
4. Popur chaque $i = 1, \ldots, n-1$, on a : $(V_1 + \cdots + V_i) \cap V_{i+1} = \{0\}$.

Definition 8

Si l'une (donc les autres aussi) des conditions du théorème est remplie, on dit que les sous-espaces $V_1, \ldots, V_n$ sont indépendants ou que la somme $V_1 + \cdots + V_n$ est une *somme directe*. On écrite alors :

$$V_1 \oplus \cdots \oplus V_n.$$

Definition 9

a) Soit V un $\mathbb{K}$-espace vectoriel. On appelle *projecteur* de V tout endomorphisme linéaire p de V tel que $p^2 = p \cdot p = p$.

b) Soient W_1, W_2 des sous-espaces vectoriels de V tels que : $V = W_1 \oplus W_2 = V$. L'application $p : V \to V$ définie par $p(x_1 + x_2) = x_1, \forall x_1 \in W_1, \forall x_2 \in W_2$ s'appelle la *projection de V sur W_1 le long de W_2*.

Théorème 2.12

Soit V un $\mathbb{K}$-espace vectoriel.

a) Si W_1 et W_2 sont des sous-espaces de V tels que $V = W_1 \oplus W_2$ et si p est la projection de V sur W_1 le long de W_2, alors :
   1. p est un projecteur de V,
   2. $\ker p = W_2$,
   3. $\mathrm{im} p = W_1$.

b) Soit p un projecteur de V. Posons $W_1 = \mathrm{im} p$ et $W_2 = \ker p$, alors :
   1. $V = W_1 \oplus W_2$,
   2. p est la projection sur W_1 le long de W_2.

Théorème 2.13

Soit V un $\mathbb{K}$-espace vectoriel et $n \geq 2$ un entier.

a) Soient $W_1, \ldots, W_n$ des sous-espaces de V tels que $V = W_1 \oplus \cdots \oplus W_n$. Pour chaque $i = 1, \ldots, n$, on a : $V = W_i \oplus (\sum_{j \neq i} W_j)$. On peut définir p_i la projection de V sur W_i le long de $\sum_{j \neq i} W_j)$. Alors les p_i sont des projecteurs tels que :
   1. $\sum_{i=1}^{n} p_i = \mathrm{id}_V$,
   2. pour tout choix de $i, j \in \mathbb{N}_n$ tel que $i \neq j$, on a : $p_i p_j = 0$.

b) Soient $p_1, \ldots, p_n$ des projecteurs de V tels que $\sum_{i=1}^{n} p_i = \mathrm{id}_V$ et $p_i p_j = 0$ toutes les fois que $i \neq j$. Pour chaque $i = 1, \dots, n$, posons $W_i = \mathrm{im} p_i$. On a alors :

1. $V = W_1 \oplus \cdots \oplus W_n$,
2. pour chaque $i = 1, \dots, n$, p_i est la projection de V sur W_i le long de $\sum_{j \neq i} W_j$.

Definition 10

Soient V un $\mathbb{K}$-espace vectoriel et W un sous-espace de V. On appelle *sous-espace supplémentaire* de W dans V tout sous-espace vectoriel E de V tel que $V = W \oplus E$. (i. e. $E \cap W = \{0\}$ et $W + E = V$.)

Théorème 2.14

Soient W, E_1, E_2 des sous-espaces vectoriels de V tels que $V = W \oplus E_1 = W \oplus E_2$, alors E_1 et E_2 sont isomorphes.

2.3 Dimension

Definition 11

Soit V un $\mathbb{K}$-espace vectoriel et W un sous-espace. On dit que W est un *hyperplan* de V si $W \neq V$ et si, pour tout sous-espace U de V tel que $W \subset U \subset V$, on a forcément $U = V$ ou $U = W$.

Théorème 2.15

Soit W un sous-espace d'un $\mathbb{K}$-espace vectoriel V tel que $W \neq V$. Les propriétés suivantes sont équivalentes :

1. W est un hyperplan de V.
2. $\forall x \in V \setminus W$, on a : $V = W + \mathbb{K}x$.
3. $\forall x \in V \setminus W$, on a : $V = W \oplus \mathbb{K}x$.
4. $\exists x \in V$, tel que : $V = W + \mathbb{K}x$.
5. $\exists x \in V$, tel que : $V = W \oplus \mathbb{K}x$.

Lemme 2.16

Soient W_1, W_2, F des sous-espaces d'un $\mathbb{K}$-espace vectoriel V tels que $W_1 \subset W_2$. On suppose que W_1 est un hyperplan de W_2. Alors on a une des deux propositions suivantes :

1. $W_1 \cap F$ est un hyperplan de $W_2 \cap F$ et $W_1 + F = W_2 + F$.
2. $W_1 + F$ est un hyperplan de $W_2 + F$ et $W_1 \cap F = W_2 \cap F$.

Definition 12

Soit W un sous-espace d'un $\mathbb{K}$-espace vectoriel de V. On appelle *drapeau (linéaire)* joignant W à V toute suite $W = W_0 \subset W_1 \subset \cdots \subset W_{n-1} \subset W_n = V$ de sous-espaces de V tels que pour chaque $i = 1, \ldots, n$ W_{i-1} soit un hyperplan de W_i. n est appelé la *longueur* du drapeau.

On dit que W est de *codimension finie dans* V s'il existe un drapeau joignant W à V.

Théorème 2.17 (Complétion des drapeaux)

Soit W un sous-espace de codimension finie dans V. Alors toute suit de sous-espaces $W = E_0 \subsetneq E_1 \subsetneq \cdots \subsetneq E_m = V$ peut être complétée en un drapeau joignant W à V en ajoutant des sous-espaces intermédiaires.

Théorème 2.18

Soit W un sous-espace d'un $\mathbb{K}$-espace vectoriel V. Deux drapeaux joignant W à V ont la même longueur.

Definition 13

Si W est un sous-espace de codimension finie dans V, la *codimension de W dans V* est la longueur de n'importe quel drapeau joignant W à V, on la note : $\operatorname{codim}(W, V)$.

W est dit de *dimension finie* si $\{0\}$ est de codimension finie dans W. Dans ce cas on appelle *dimension de w* la codimension de $\{0\}$ dans W ; on la note : $\dim(W)$.

S'il n'y a pas d'incertitude sur V, on écrit simplement $\operatorname{codim}(W)$ au lieu de $\operatorname{codim}(W, V)$.

Théorème 2.19

Soient $W_1 \subset W_2, E$ des sous-espaces vectoriels d'un espace vectoriel V. Alors W_1 est de codimension finie dans W_2 si et seulement si $W_1 + E$ est de codimension finie dans $W_2 + E$ et $W_1 \cap E$ est de codimension finie dans $W_2 \cap E$. Si c'est le cas on a :

$$\operatorname{codim}(W_1, W_2) = \operatorname{codim}(W_1 + E, W_2 + E) + \operatorname{codim}(W_1 \cap E, W_2 \cap E).$$

Corollaire 2.20

Soient $U_1 \subset U_2 \subset U_3$ des sous-espaces vectoriels de V. Alors U_1 est de codimension finie dans U_3 si et seulement si U_1 est de codimension finie dans U_2 et U_2 est de codimension finie dans U_3. Dans ce cas on a :

$$\operatorname{codim}(U_1, U_3) = \operatorname{codim}(U_1, U_2) + \operatorname{codim}(U_2, U_3).$$

Corollaire 2.21

Soit W un sous-espace vectoriel de V. Alors V est de dimension finie si et seulement si W est à la fois de dimension finie et de codimension finie et on a alors :

$$\dim V = \dim W + \mathrm{codim} W.$$

Théorème 2.22

Soient $W_1 \subset W_2$ et $V_1 \subset V_2$ des sous-espaces de V. Alors W_1 est de codimension finie dans W_2 et V_1 dans V_2 si et seulement si $W_1 \cap V_1$ est de codimension finie dans $W_2 \cap V_2$ et $W_1 + V_1$ dans $W_2 + V_2$ et alors :

$$\mathrm{codim}(W_1, W_2) + \mathrm{codim}(V_1, V_2) = \mathrm{codim}(W_1 \cap V_1, W_2 \cap V_2) + \mathrm{codim}(W_1 + V_1, W_2 + V_2).$$

Corollaire 2.23

Soient E, F des sous-espaces vectoriels d'un espace V. Si E et F sont de dimension finie, alors $E+F$ et $E \cap F$ sont de dimension finie et on a :

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

Corollaire 2.24

Soient E, F des sous-espaces vectoriels d'un espace V. Si E et F sont de codimension finie, alors $E + F$ et $E \cap F$ aussi et on a :

$$\mathrm{codim} E + \mathrm{codim} F = \mathrm{codim}(E + F) + \mathrm{codim}(E \cap F).$$

Corollaire 2.25

Soient E, F des sous-espace d'un espace V. Si E est de dimension finie et F de codimension finie alors $E \cap F$ est de dimension finie et $E + F$ de codimension finie et on a :

$$\dim E + \mathrm{codim}(E + F) = \dim(E \cap F) + \mathrm{codim} F.$$

Definition 14

Soit V un $\mathbb{K}$-espace vectoriel. On dit qu'une partie $A \subset V$, finie, est *libre,* ou *linéairement indépendante,* si l'unique famille $(\lambda_a)_{a \in A}$ de scalaires pour laquelle $\sum_{a \in A} \lambda_a a = 0$ est la famille nulle $(\lambda_a = 0, \forall a \in A.)$

Proposition 2.26

1. $\emptyset$ est libre.
2. Si A est libre, alors $B \subset A$ est libre aussi.
3. Si A est libre $0 \notin A$.
4. Si A est finie et non vide, dire que A est libre revient à dire que $0 \notin A$ et $\mathrm{vect}(A) = \bigoplus_{a \in A} \mathbb{K}a$.
5. Si A est finie et non vide, dire que A est libre revient à dire que si $x_1, \ldots, x_n$ est la liste des éléments de A et $V_i = \mathrm{vect}(x_1, \ldots, x_i)$ pour $i = 1, \ldots, n$, alors $V_1 \subset \cdots \subset V_n$ est un drapeau.

Corollaire 2.27

Si V est un espace de dimension finie n, alors toute partie libre a au plus n éléments et il existe au moins une partie libre à n éléments. Si V n'est pas de dimension finie, alors pour tout entier m il existe une partie libre à m éléments.

Definition 15

Soit V un $\mathbb{K}$-espace vectoriel. On dit que $A \subset V$ est *libre* si toute partie finie de A est libre.

Definition 16

Soit V un $\mathbb{K}$-espace vectoriel. On dit que $B \subset V$ est une *base* si B est libre et si $V = \mathrm{vect}(B)$.

Théorème 2.28

Dans un espace vectoriel V de dimension finie n, il existe des bases et toutes les bases de V ont exactement n éléments.

Théorème 2.29

Dans un espace vectoriel de dimension finie n, si S est une partie génératrice et si L est une partie libre, on peut compléter L en une base en lui adjoignant des éléments de S.

Théorème 2.30

Soi $B = \{x_1, \ldots, x_n\}$ une base de V, un $\mathbb{K}$-espace vectoriel. L'application $\phi : \mathbb{K}^n \to V$ définie par $(\lambda_1, \ldots, \lambda_n) \mapsto \sum_{i=1}^n \lambda_i x_i$, $\forall (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ est un isomorphisme.

En particulier, pour tout $x \in V$, il existe une unique suite $\lambda_1, \ldots, \lambda_n$ de scalaires telle que $x =$

$\lambda_1 x_1 + \cdots + \lambda_n x_n$. On dit que $\lambda_1, \ldots, \lambda_n$ sont les *composantes* ou les *coordonnées* de x relativement à la base B.

Théorème 2.31

Soit $B = \{x_1, \ldots, x_n\}$ une base de $\mathbb{K}$-espace vectoriel V. Soit W un $\mathbb{K}$-espace vectoriel et $y_1, \ldots, y_n \in W$.

Alors il existe une et une seule application linéaire $f : V \to W$ telle que $f(x_i) = y_i$ pour chaque $i = 1, \ldots, n$.

"En d'autres termes, l'application $\mathcal{L}(V, W) \to W^B$ définie par $f = f|_B$ est un isomorphisme linéaire.)

Corollaire 2.32

Soient V, W deux $\mathbb{K}$-espaces vectoriels. Supposons V de dimension finie n. Alors W est isomorphe à V si et seulement si $\dim W = n$.

Théorème 2.33

Soit W un sous-espace vectoriel d'un $\mathbb{K}$-espace vectoriel V. Les conditions suivantes sont équivalentes :

1. $\operatorname{codim}(W, V) < \infty$.
2. W admet un supplémentaire U de dimension finie et dans ce cas : $\dim U = \operatorname{codim}(W, V)$.

Corollaire 2.34

Si V est un espace vectoriel de dimension finie, alors tout sous-espace W de V admet un supplémentaire U et :

$$\dim U + \dim W = \dim V.$$

Definition 17

On dit qu'une application linéaire $f : V \to W$ est de *rang fini* si $\operatorname{im} f$ est de dimension finie et dans ce cas on appelle *rang de f* le nombre :

$$\operatorname{rang} f = \dim(\operatorname{im} f).$$

Théorème 2.35 (Théorème du rang)

Soit $f : V \to W$ une application linéaire. Les conditions suivantes sont équivalentes :

1. f est de rang fini.

2. $\ker f$ est de codimension finie dans V.

Si ces conditions sont remplies on a :

$$\text{rang} f = \text{codim}(\ker f).$$

Théorème 2.36 (Petit théorème du rang)

Soit $f : V \to W$ une application linéaire, on suppose $\dim V < \infty$. Alors f est de rang fini et :

$$\text{rang} f + \dim(\ker f) = \dim V.$$

Corollaire 2.37

Soient V, W deux espaces vectoriels tels que $\dim V = \dim W < \infty$ et $f : V \to W$ une application linéaire. Alors :

$$f \text{ injective} \Leftrightarrow f \text{ surjective.}$$

2.4 Dualité

Definition 18

Si V est un $\mathbb{K}$-espace vectoriel, on appelle *dual de V* l'espace vectoriel $V^{\#} = \mathcal{L}(V, \mathbb{K})$.

Definition 19

$e_1^{\#}, \ldots, e_n^{\#} \in V^{\#}$ définis par

$$e_i^{\#}(e_j) = \delta_{ij} = \begin{cases} 0 \ i \neq j \\ 1 \ i = j \end{cases},$$

est la *base duale* de la base $e_1, \ldots, e_n$ de V.

Théorème 2.38

Si V est de dimension finie, alors $V^{\#}$ aussi et :

$$\dim V^{\#} = \dim V.$$

Definition 20

Soit $S \subset V$. On appelle *espace des équations linéaires de S* ou *espace orthogonal absolu de S dans*

V le sous-espace S^0 de $V^\#$ défini par :

$$S^0 = \{\phi \in V^\# | \phi(x) = 0, \forall x \in S\}$$
$$= \{\phi \in V^\# | S \subset \ker \phi\}.$$

Proposition 2.39

1. $S^0 = \text{vect}(S)^0$.
2. $S_1 \subset S_2 \Rightarrow S_2^0 \subset S_1^0$.
3. $(S_1 \cup S_2)^0 = S_1^0 \cap S_2^0$.

Definition 21

Soit $S \subset V^\#$. On appelle *espace des solutions de S dans V* le sous-espace S_0 de V défini par :

$$S_0 = \{x \in V | \phi(x) = 0 \, \forall \phi \in S\}.$$

Proposition 2.40

1. $S_0 = \text{vect}(S)_0$.
2. $S_1 \subset S_2 \Rightarrow (S_2)_0 \subset (S_1)_0$.
3. $(S_1 \cup S_2)_0 = (S_1)_0 \cap (S_2)_0$.
4. Si $S \subset V$, alors $S \subset (S^0)_0$, et si $T \subset V^\#$, alors $T \subset (T_0)^0$.

Théorème 2.41

Soit V un $\mathbb{K}$-espace vectoriel, $\mathcal{E}'$ l'ensemble des sous-espace de codimension finie de V, $\mathcal{E}$ l'ensemble des sous-espaces de dimension finie de $V^\#$.

L'application $W \mapsto W^0$ est une bijection de $\mathcal{E}'$ sur $\mathcal{E}$ dont la réciproque est $W' \mapsto W'_0$. De plus, on a :

$$\dim W^0 = \text{codim} W, \quad \forall W \in \mathcal{E}'.$$

Definition 22

Soit $\alpha : V \to W$ une application linéaire. On définit l'*application duale de α* par : $\alpha^\# : W^\# \to V^\#$ où $\alpha^\#(\phi) = \phi \circ \alpha, \forall \phi \in W^\#$.

Clairement $\alpha^\#$ est linéaire.

Proposition 2.42

1. Si $\alpha : V \to W$ et $\beta : W \to U$, alors : $(\beta\alpha)^{\#} = \alpha^{\#}\beta^{\#}$.
2. $(\mathrm{id}_V)^{\#} = \mathrm{id}_{V^{\#}}$.
3. Si $\alpha : V \to W$ est un isomorphisme, alors $\alpha^{\#}$ aussi et on a : $(\alpha^{\#})^{-1} = (\alpha^{-1})^{\#}$.
4. $\ker \alpha^{\#} = \mathrm{im}(\alpha)^0$.

Théorème 2.43

Soit $\alpha : V \to W$ une application linéaire. On suppose $\dim W < \infty$. Alors :

$$\mathrm{rang}\,\alpha^{\#} = \mathrm{rang}\,\alpha.$$

Lemme 2.44

Soit V un $\mathbb{K}$-espace vectoriel de dimension finie n et soit $x \in V$ non nul. Alors il existe $\phi \in V^{\#}$ telle que :

$$\phi(x) \neq 0.$$

Théorème 2.45

Soit V un $\mathbb{K}$-espace vectoriel de dimension finie. Si $x \in V$ on lui associe $\hat{x} \in V^{\#\#}$ de la façon suivante $\hat{x} : V^{\#} \to \mathbb{K}$, où $\hat{x}(\phi) = \phi(x)$. Alors l'application $x \mapsto \hat{x}$ est un isomorphisme de V sur $V^{\#\#}$.

2.5 Algèbres

Definition 23

Une *algèbre sur un corps* $\mathbb{K}$ ou $\mathbb{K}$*-algèbre* est un $\mathbb{K}$-espace vectoriel $\mathbb{A}$ muni d'une deuxième loi de composition, notée multiplicativement, telle que $\mathbb{A}$ muni de l'addition et de la multiplication soit un anneau et vérifiant la condition :

$$\lambda(xy) = (\lambda x)y = x(\lambda y) \quad \forall \lambda \in \mathbb{K}, \forall x, y \in \mathbb{A}.$$

Definition 24

Un partie $\mathbb{B} \subset \mathbb{A}$ est une *sous-algèbre de* $\mathbb{A}$ si $\mathbb{B}$ est à la fois un sous-espace vectoriel et un sous-anneau de $\mathbb{A}$. $\mathbb{B}$ remplit alors les conditions suivantes :

1. Si $x, y \in \mathbb{B}$, alors : $x + y \in \mathbb{B}$.
2. Si $x, y \in \mathbb{B}$, alors : $xy \in \mathbb{B}$.

3. Si $\lambda \in \mathbb{K}$ et $x \in \mathbb{B}$, alors : $\lambda x \in \mathbb{B}$.
4. $1_{\mathbb{A}} \in \mathbb{B}$.

Definition 25

Si $\mathbb{A}$ et $\mathbb{B}$ sont des $\mathbb{K}$-algèbres, une application $f : \mathbb{A} \to \mathbb{B}$ est dite *homomorphisme de $\mathbb{K}$-algèbres* si f est à la fois une application linéaire et un homomorphisme d'anneau, soit si $\forall x, y \in \mathbb{A}$ et $\forall \lambda \in \mathbb{K}$:

1. $f(x+y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(\lambda x) = \lambda f(x)$
4. $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

Definition 26

On appelle *algèbre des polynômes à une variable à coefficients dans* $\mathbb{K}$ l'espace $\mathbb{K}^{(\mathbb{N})}$ vu comme $\mathbb{K}$-espace vectoriel, muni du produit suivant :

$$(a_n)_{n\geq 0}(b_n)_{n\geq 0} = (c_n)_{n\geq 0},$$

où : $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = \displaystyle\sum_{i+j=n} a_ib_j$.

Théorème 2.46

Soit $\mathbb{K}$ un corps. Il existe une $\mathbb{K}$-algèbre $\mathbb{A}$ contenant un élément t, telle que $1 = t^0, t, t^2, \ldots$ est une base (infinie.) Cette algèbre sera notée $\mathbb{K}[t]$ et appelée l'*algèbre des polynômes à une indéterminée sur le corps* $\mathbb{K}$. L'élément t s'appelle l'*indéterminée* et les éléments de $\mathbb{K}[t]$ s'appellent *polynômes.*

Proposition 2.47

1. Si $a_0, \ldots, a_n \in \mathbb{K}$, alors :
$$\sum_{i=0}^{n} a_it^i = 0 \Leftrightarrow a_0 = \cdots = a_n = 0.$$
2. Si $f \in \mathbb{K}[t]$, $f \neq 0$, alors il existe un entier $n \geq 0$ unique et des $a_0, \ldots, a_n \in \mathbb{K}$ uniques tels que : $f = \sum_{i=0}^{n} a_it^i$ et $a_n \neq 0$.
f est dit de *degré* n et a_n s'appelle le *coefficient dominant de* f :

$\mathrm{dom}(f) = a_n$	$\deg(f) = n$
$\mathrm{dom}(0) = 0$	$\deg(0) = -\infty$ (par convention).

Definition 27

Un polynôme $f \in \mathbb{K}[t]$ est dit *unitaire* si $\mathrm{dom}(f) = 1$.

Théorème 2.48

Soit $\mathbb{A}$ une $\mathbb{K}$-algèbre et $\alpha \in \mathbb{A}$. Il existe un unique homomorphisme d'algèbre $\mathbb{K}[t] \to \mathbb{A}$ qui envoie l'élément t de $\mathbb{K}[t]$ sur l'élément α de $\mathbb{K}$.

Definition 28

Soit $f \in \mathbb{K}[t]$ définie par $f = \sum_{i=0}^{n} a_i t^i$. On appelle *valeur de f en α* l'expression $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$ où $\alpha \in \mathbb{A}$, une $\mathbb{K}$-algèbre.

2.6 Matrices

Definition 29

Soit $\mathbb{K}$ un corps, $n \geq 1, m \geq 1$. Les éléments du $\mathbb{K}$-espace vectoriel $\mathbb{K}`\mathbb{N}_n \times \mathbb{N}_m$ s'appellent *matrices* $n \times m$ à coefficients dans $\mathbb{K}$.

Cet espace se notera $M_{n\times m}(\mathbb{K})$.

Si $A \in M_{n\times m}(\mathbb{K})$, par définition :

$$\begin{aligned} A :& \mathbb{N}_n \times \mathbb{N}_m \to \mathbb{K} \\ & (i,j) \mapsto A(i,j). \end{aligned}$$

$A(i,j)$ est le corfficient de la i-e ligne et j-e colonne de A.

La *j-e colonne de A* se note $c_j(A) \in M_{n\times 1}(\mathbb{K})$.

La *i-e ligne de A* se note $l_i(A) \in M_{1\times m}(\mathbb{K})$.

Si $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ on note :

$$\mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

On note $I_n \in M_n(\mathbb{K})$ la matrice-unité $\mathrm{diag}(\underbrace{1, \ldots, 1}_{n \text{ fois}})$.

Definition 30

Si $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$ et $B = (b_{ij}) \in M_{m\times p}(\mathbb{K})$ on définit le produit $AB = (c_{ij}) \in M_{n\times p}(\mathbb{K})$

par la règle :
$$c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj} \qquad (1 \leq i \leq n,\ 1 \leq j \leq p).$$

Proposition 2.49

Pour tout $\lambda \in \mathbb{K}$, $A, A_1, A_2 \in M_{n\times m}(\mathbb{K})$, $B, B_1, B_2 \in M_{m\times p}(\mathbb{K})$, $C \in M_{p\times q}(\mathbb{K})$ on a :

1. $(AB)C = A(BC)$
2. $(A_1 + A_2)B = A_1B + A_2B$
3. $A(B_1 + B_2) = AB_1 + AB_2$
4. $\lambda(AB) = (\lambda A)B = A(\lambda B)$
5. $I_nA = AI_m = A$

Si $n = m = p$, alors $M_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre.

Definition 31

Si $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$, on définit la *transposée de A* par la matrice $A^t = (b_{ij}) \in M_{m\times n}(\mathbb{K})$, où :
$$b_{ij} = a_{ji} \qquad (1 \leq j \leq n, 1 \leq i \leq m).$$

Proposition 2.50

Si $A, A' \in M_{n\times m}(\mathbb{K}), B \in M_{m\times p}(\mathbb{K}), \lambda \in \mathbb{K}$ on a :

1. $(A + A')^t = A^t + A'^t$
2. $(\lambda A)^t = \lambda A^t$
3. $(A^t)^t = A$
4. $(AB)^t = B^tA^t$

$A \mapsto A^t$ est un isomorphisme d'espace vectoriel de $M_{n\times m}(\mathbb{K}) \to M_{m\times n}(\mathbb{K})$.

Definition 32

Si $A = (a_{ij}) \in M_n(\mathbb{K})$, on définit la *trace de A* par :
$$\mathrm{tr}\ (A) = \sum_{i=1}^{n} a_{ii}.$$

$\mathrm{tr}\ (A) \in \mathbb{K}$.

Proposition 2.51

1. $\text{tr }(A+B) = \text{tr }(A) + \text{tr }(B), \forall A, B \in M_n(\mathbb{K})$.
2. $\text{tr }(\lambda A) = \lambda \text{tr }(A), \forall \lambda \in \mathbb{K}, \forall A \in M_n(\mathbb{K})$.
3. $\text{tr }(A^t) = \text{tr }(A), \forall A \in M_n(\mathbb{K})$.
4. $\text{tr }(AB) = \text{tr }(BA), \forall A \in M_{n\times m}(\mathbb{K}), \forall B \in M_{m\times n}(\mathbb{K})$.

$\text{tr } : M_n(\mathbb{K}) \to \mathbb{K}$ est linéaire.

Definition 33

On dit que $A \in M_n(\mathbb{K})$ est *inversible* s'il existe $B \in M_n(K)$ telle que $AB = BA = I_n$.
Si c'est le cas, B est unique, se note A^{-1} et s'appelle l'*inverse de* A.

Notation 1

On note $\text{GL}_n(\mathbb{K})$ l'ensemble des éléments inversibles de $M_n(\mathbb{K})$. $\text{GL}_n(\mathbb{K})$ est un groupe pour la multiplication matricielle. On l'appelle le *groupe linéaire général* (General Linear group.)

Théorème 2.52

Si $A \in \text{GL}_n(\mathbb{K})$, alors $A^t \in \text{GL}_n(\mathbb{K})$ et $(A^t)^{-1} = (A^{-1})^t$.

Théorème 2.53

Soit $A \in M_n(\mathbb{K})$. On suppose qu'il existe $B \in M_n(\mathbb{K})$ telle que $AB = I_n$. Alors $BA = I_n$. Donc $A \in \text{GL}_n(\mathbb{K})$ et $B = A^{-1}$.

2.7 Applications linéaires

Definition 34

Soit V un $\mathbb{K}$-espace vectoriel de dimension finie. Une *base ordonnée de* V est une base munie d'un ordre total. Cela revient à donner une numérotation des éléments de la base. On note $\mathcal{B} = (e_1, \dots, e_n)$, si $\dim V = n$.

Notation 2

Á la base ordonnée $\mathcal{B} = (e_1, \dots, e_n)$ de V correspond un isomorphisme $V \xrightarrow{\simeq} \mathbb{K}$ et on a $x = \sum_{i=1}^{n} x_i e_i$.

On notera :

$$M_{\mathcal{B}}(x) = (x_1, \ldots, x_n) \in M_{1\times n}(\mathbb{K})$$
$$M^{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n\times 1}(\mathbb{K}).$$

Clairement : $M^{\mathcal{B}}(x) = (M_{\mathcal{B}}(x))^t$.

Si $\alpha : V \to V'$ linéaire, on note $M_{\mathcal{B}}^{\mathcal{B}'}(\alpha)$ la matrice de α relative aux bases ordonnées $\mathcal{B}$ et $\mathcal{B}'$. On a $M_{\mathcal{B}}^{\mathcal{B}'}(\alpha) = (a_{ij}) \in M_{n\times m}(\mathbb{K})$, avec :

$$\alpha(e_j) = \sum_{i=1}^{m} a_{ij} e'_i \quad j = 1, \ldots, n.$$

Théorème 2.54

Si $\mathcal{B}$ (resp. $\mathcal{B}'$) est une base ordonnée de V (resp. V') l'application $\alpha \mapsto M_{\mathcal{B}}^{\mathcal{B}'}(\alpha)$ est un isomorphisme linéaire de $\mathcal{L}(V, V')$ sur $M_{n\times m}(\mathbb{K})$.

Théorème 2.55

Soient $\mathcal{B}, \mathcal{B}', \mathcal{B}''$ des bases ordonnées de V, V', V'' respectivement et soient $\alpha : V \to V'$ et $\beta : V' \to V''$ deux applications linéaires. On a :

$$M_{\mathcal{B}}^{\mathcal{B}''}(\beta \circ \alpha) = M_{\mathcal{B}'}^{\mathcal{B}''}(\beta) M_{\mathcal{B}}^{\mathcal{B}'}(\alpha).$$

Théorème 2.56

Soient $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_n)$ des bases ordonnées de V et V' respectivement. Soient $\mathcal{B}^\# = (e_1^\#, \ldots, e_n^\#)$ et $\mathcal{B}'^\# = (e_1'^\#, \ldots, e_n'^\#)$ les bases ordonnées duales de $V^\#$ et $V'^\#$.

Soit $\alpha : V \to V'$ une application linéaire. On a :

$$M_{\mathcal{B}'^\#}^{\mathcal{B}^\#}(\alpha^\#) = \left(M_{\mathcal{B}}^{\mathcal{B}'}(\alpha)\right)^t.$$

Propriété 2.57

Soient V, V' des $\mathbb{K}$-espaces vectoriels de dimension finie n. Soient $\mathcal{B}, \mathcal{B}'$ des bases ordonnées de V, V' et $\alpha : V \to V'$ linéaire.

Alors α est un isomorphisme si et seulement si $M_{\mathcal{B}}^{\mathcal{B}'}(\alpha) \in \mathrm{GL}_n(\mathbb{K})$ et dans ce cas on a :

$$M_{\mathcal{B}'}^{\mathcal{B}}(\alpha^{-1}) = M_{\mathcal{B}}^{\mathcal{B}'}(\alpha)^{-1}.$$

Propriété 2.58

Soit V un $\mathbb{K}$-espace vectoriel de dimension n. Soit $\mathcal{B}$ une base ordonnée de V.

a) La correspondance $\mathcal{B}' \mapsto M_{\mathcal{B}'}^{\mathcal{B}}(\mathrm{id}_V)$ est une bijection de l'ensemble de toutes les bases ordonnées de V sur $\mathrm{GL}_n(\mathbb{K})$.

b) La correspondance $\mathcal{B}' \mapsto M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ est une bijection de l'ensemble de toutes les bases ordonnées de V dans $\mathrm{GL}_n(\mathbb{K})$.

Definition 35

Soit $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$. Le *rang* de A, noté $\mathrm{rang}(A)$, est la dimension du sous-espace vectoriel de $M_{n\times 1}(\mathbb{K})$ engendré par les colonnes $c_1(A), \ldots, c_m(A)$ de A.

En d'autres termes $\mathrm{rang}(A)$ est le nombre maximum de colonnes linéairement indépendantes.

Propriété 2.59

Soit V, V' des $\mathbb{K}$-espaces vectoriels de dimension finie n et m et $\mathcal{B}, \mathcal{B}'$ des bases ordonnées de V, V' respectivement et $A = M_{\mathcal{B}}^{\mathcal{B}'}(\alpha)$. Alors :

$$\mathrm{rang}\, A = \mathrm{rang}\, \alpha.$$

Théorème 2.60

Soit $A \in M_{n\times m}(\mathbb{K})$. Alors $\mathrm{rang}(A)$ est :

— la dimension du sous-espace vectoriel de $M_{1\times m}(\mathbb{K})$ engendré par les lignes de A.

— le nombre maximum de lignes linéairement indépendantes.

Théorème 2.61

Toute matrice $A \in M_{n\times m}(\mathbb{K})$ peut être transformée en une matrice échelonnée réduite par une suite (finie) d'opérations élémentaires sur les lignes.

Definition 36

Deux matrices $A, B \in M_{n\times m}(\mathbb{K})$ sont dites *équivalentes* (ou *associées*) s'il existe des matrices $P \in \mathrm{GL}_n(\mathbb{K})$ et $Q \in \mathrm{GL}_m(\mathbb{K})$ telles que $B = PAQ$.

On écrit alors $A \sim B$. $\sim$ est une relation d'équivalence.

Théorème 2.62

Soit V, V' deux $\mathbb{K}$-espaces vectoriels de dimension finie m, n respectivement et $\mathcal{B}_1, \mathcal{B}_1'$ des bases ordonnées de V, V' repsectivement. Soit encore $\alpha : V \to V'$ linéaire et $A = M_{\mathcal{B}_1}^{\mathcal{B}_1'}(\alpha) \in M_{n\times m}(\mathbb{K})$. Enfin soit $B \in M_{n\times m}(\mathbb{K})$. Il y a équivalence entre les deux propriétés suivantes :

1. $A \sim B$.
2. il existe des bases ordonnées $\mathcal{B}_2, \mathcal{B}_2'$ de V, V' respectivement telles que $B = M_{\mathcal{B}_2}^{\mathcal{B}_2'}(\alpha)$.

Théorème 2.63

Soit $A \in M_{n\times m}(\mathbb{K})$ de rang r. Alors :

$$A \sim \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right).$$

Corollaire 2.64

Soient $A, B \in M_{n\times m}(\mathbb{K})$. Alors :

$$A \sim B \Leftrightarrow \text{rang}\, A = \text{rang}\, B.$$

2.8 Complément

2.8.1 Partition des matrices

Notation

On note $\mathcal{P}_{r,n}$ l'ensemble de toutes les parties à r éléments de $\mathbb{N}_n$. Si $\alpha \in \mathcal{P}_{r,n}$, on note $\alpha(1) < \cdots < \alpha(r)$ les r éléments de α, par ordre croissant.

Soit $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$, $\alpha \in \mathcal{P}_{r,n}$, $\beta \in \mathcal{P}_{s,m}$. On note $A[\alpha, \beta] \in M_{r\times s}(\mathbb{K})$ la matrice dont le coefficient d'indice (kl) est $a_{\alpha(k),\beta(l)}$ $(1 \leq k \leq r, 1 \leq l \leq s)$.

On note aussi $A(\alpha, \beta)$ la matrice $A[\alpha', \beta']$ où α' (resp. β') désigne le complémentaire de α (resp. β) dans $\mathbb{N}_n$ (resp. $\mathbb{N}_m$).

Les matrices de la forme $A[\alpha, \beta]$ sont des *sous- matrices* de A.

Soit des partitions ordonnées $\underline{\alpha} = (\alpha_1, \ldots, \alpha_r)$ de $\mathbb{N}_n$ et $\underline{\beta} = (\beta_1, \ldots, \beta_s)$ de $\mathbb{N}_m$. On a alors la partition, en sous-matrices, en matrices blocs :

$$A = (A[\alpha_i, \beta_j])_{\substack{1\leq i\leq r \\ 1\leq j\leq s}}.$$

Multiplication

Soient $A \in M_{n\times m}(\mathbb{K})$, $B \in M_{m\times p}(\mathbb{K})$, $C = AB \in M_{n\times p}(\mathbb{K})$ et $\underline{\alpha} = (\alpha_1, \ldots, \alpha_r)$, $\underline{\beta} = (\beta_1, \ldots, \beta_s)$, et $\underline{\gamma} = (\gamma_1, \ldots, \gamma_t)$ des partitions de $\mathbb{N}_n$, $\mathbb{N}_m$ et $\mathbb{N}_p$, et soit :

$$A = (A[\alpha_i, \beta_j])_{\substack{1\leq i\leq r \\ 1\leq j\leq s}}, \quad B = (B[\beta_j, \gamma_k])_{\substack{1\leq j\leq s \\ 1\leq k\leq t}}, \quad C = (C[\alpha_i, \gamma_k])_{\substack{1\leq i\leq r \\ 1\leq k\leq t}},$$

alors :

$$C[\alpha_i, \gamma_k] = \sum_{j=1}^{s} A[\alpha_i, \beta_j] B[\beta_j, \gamma_k].$$

2.9 Supplément

Théorème 2.65

Soient V_1, V_2 des espaces vectoriels $f \in \mathcal{L}(V_1, V_2)$ et W un sous-espace de V_1. Alors :

$$f^{-1}(f(W)) = W + \ker f$$

Théorème 2.66

Soient V, W des espaces vectoriels, $S, T \subset V$ et $f \in \mathcal{L}(V, W)$, alors :

1. $\mathrm{vect}(S \cup T) = \mathrm{vect}\, S + \mathrm{vect}\, T$.
2. Si V_1, V_2 sont des sous-espaces de V : $\mathrm{vect}(V_1 \cup V_2) = V_1 + V_2$.
3. $\mathrm{vect}\, f(S) = f(\mathrm{vect}\, S)$.

Théorème 2.67

Soient V, W deux espaces vectoriels et $f \in \mathcal{L}(V, W)$, alors :

a) Si $V_1 \subset V_2$ sont des sous-espaces de V :

$$\mathrm{codim}(V_1 + \ker f, V_2 + \ker f) = \mathrm{codim}(f(V_1), f(V_2)).$$

b) Si $W_1 \subset W_2$ sont des sous-espaces de W, alors :

$$\mathrm{codim}(W_1 \cap \mathrm{im}\, f, W_2 \cap \mathrm{im}\, f) = \mathrm{codim}(f^{-1}(W_1), f^{-1}(W_2)).$$

Definition 37

Soient V, W deux espaces vectoriels et $f \in \mathcal{L}(V, W)$. On dit que f est *de Fredholm* si $\ker f$ est de dimension finie et $\mathrm{im}\, f$ de codimension finie. On définit alors l'*indice de Fredholm de f* par :

$$\mathrm{ind}\, f = \dim(\ker f) - \mathrm{codim}(\mathrm{im}\, f).$$

Théorème 2.68

Soient V et W deux espaces vectoriels de dimension finie et $f \in \mathcal{L}(V, W)$ de Fredholm, alors :

a) $\mathrm{ind}\, f = \dim V - \dim W$.

b) Si f, g sont de Fredholm, alors $g \circ f$ aussi et :

$$\operatorname{ind} g \circ f = \operatorname{ind} f + \in\ g.$$

Théorème 2.69

Soient V, W deux espaces vectoriels et $f \in \mathcal{L}(V, W)$ de Fredholm. Soit $f^{\#} \in \mathcal{L}(W^{\#}, V^{\#})$, alors :

a) $\operatorname{im} f^{\#} = (\ker\ f)^0$.

b) $f^{\#}$ est de Fredholm.

Chapitre 3

Déterminants

3.1 Formes multilinéaires alternées

Definition 1

Soient $V_1, \dots, V_n$ et W des $\mathbb{K}$-espaces vectoriels. Une application $f : V_1 \times \cdots \times V_n \to W$ est dite *multilinéaire* si pour tout choix d'un $i \in \mathbb{N}_n$ et tout chois d'éléments $a_j \in V_j$ pour chaque $j \in \mathbb{N}_n$, sauf $j = i$, l'application $V_i \to W$ définie par $x \mapsto f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ est linéaire.

On désigne par $\mathcal{L}(V_1, \dots, V_n; W)$ l'ensemble des applications multilinéaires de $V_1 \times \cdots \times V_n$ dans W. On vérifie que $\mathcal{L}(V_1, \dots, V_n; W)$ est un sous-espace vectoriel de l'espace vectoriel $\mathcal{F}(V_1 \times \cdots \times V_n; W) = W^{V_1 \times \cdots \times V_n}$.

Lorsque $n = 2$ on dit que f est *bilinéaire*, si $n = 2$ on dit que f est *trilinéaire*, etc. .

Remarque 1

Il ne faut pas confondre $f : V_1 \times V_2 \to W$ multilinéaire (i. e. telle que $f(x_1 + y_1, x_2 + y_2) = f(x_1, x_2) + f(x_1, y_2) + f(y_1, x_2) + f(y_1, y_2)$) avec linéaire (i. e. telle que $f(x_1 + y_1, x_2 + y_2) = f(x_1, x_2) + f(y_1, y_2)$.)

Exemple 1

Si V est un espace vectoriel sur $\mathbb{K}$, l'application $V \times V^{\#} \to \mathbb{K}$ définie par $(x, \phi) \mapsto \phi(x)$ est bilinéaire.

Exemple 2

L'application $M_{n\times m}(\mathbb{K}) \times M_{m\times p}(\mathbb{K}) \to M_{n\times p}(\mathbb{K})$ définie par $(A, B) \mapsto AB$ est multilinéaire.

Exemple 3

On peut définir une $\mathbb{K}$-algèbre $\mathbb{A}$ de la manière (équivallente à celle donnée dans le cours) suivante : c'est un $\mathbb{K}$-espace vectoriel $\mathbb{A}$ muni d'une multiplication $\mathbb{A} \times \mathbb{A} \to \mathbb{A}$, $(x, y) \mapsto xy$, associative, admettant un élément neutre et bilinéaire.

Exemple 4 (Le produit vectoriel)

Si $\mathbb{K}$ est un corps, alors l'application $\mathbb{K}^3 \times \mathbb{K}^3 \to \mathbb{K}^3$ définie par :

$$((x_1, y_1, z_1), (x_2, y_2, z_2)) \mapsto (y_1 z_2 - y_2 z_1, z_1 x_2 - z_2 x_1, x_1 y_2 - x_2 y_1),$$

est bilinéaire. Lorsque $\mathbb{K} = \mathbb{R}$ et $\mathbb{R}^3$ sont les coordonnées de l'espace euclidien de dimension 3 relativement à une base orthonormée orientée positivement, alors on retrouve le *produit vectoriel* de la géométrie élémentaire.

Formule générale

Si $f : V_1 \times \cdots \times V_n \to W$ est multilinéaire, alors on a, pour tout choix d'éléments $x_1^{(i)}, \ldots, x_{m(i)}^{(i)} \in V_i$ $(1 \leq i \leq n)$ et de scalaires $\lambda_{i,j} \in \mathbb{K}$ $(1 \leq j \leq m(i)$ et $1 \leq i \leq n)$, la formule :

$$f(\sum_{j_1=1}^{m(1)} \lambda_{1,j_1} x_{j_1}^{(i)}, \ldots, \sum_{j_n=1}^{m(n)} \lambda_{n,j_n} x_{j_n}^{(n)}) = \sum_{j_1=1}^{m(1)} \cdots \sum_{j_n=1}^{m(n)} \lambda_{1,j_1} \ldots \lambda_{n,j_n} f(x_{j_1}^{(1)}, \ldots, x_{j_n}^{(n)}).$$

Si $V_1 = \cdots = V_n$ et $W = \mathbb{K}$ on obtient les *formes n-multilinéaires sur V*.

Definition 2

Soit V un $\mathbb{K}$-espace vectoriel. Une forme n-multilinéaire $f : \underbrace{V \times \cdots \times V}_{n} \to \mathbb{K}$ est dite *alternée* si toutes les fois que deux (au moins) des éléments $x_1, \ldots, x_n$ de V sont égaux, alors $f(x_1, \ldots, x_n) = 0$.

Exemple 5

Si $V = \mathbb{K}^3$, les applications :

$$\begin{aligned}
\phi_1((x_1, y_1, z_1), (x_2, y_2, z_2)) &= y_1 z_2 - y_2 z_1 \\
\phi_2((x_1, y_1, z_1), (x_2, y_2, z_2)) &= z_1 x_2 - z_2 x_1 \\
\phi_3((x_1, y_1, z_1), (x_2, y_2, z_2)) &= x_1 y_2 - x_2 y_1,
\end{aligned}$$

de $\mathbb{K}^3 \times \mathbb{K}^3 \to \mathbb{K}$ sont bilinéaires alternées.

L'ensemble des formes n-multilinéaires alternées sur V se note $\mathcal{A}lt_{\,n}(V)$, c'est un sous-espace vectoriel de $\mathcal{L}(\underbrace{V, \ldots, V}_{n}; \mathbb{K})$.

Propriété 3.1 (Propriétés des formes n-multilinéaires alternées)

Soit $f : V \times \cdots \times V \to \mathbb{K}$ n-multilinéaire alternée.

1. Si on échange deux des variables $x_1, \ldots, x_n \in V$, f change de signe.
2. Soit $\sigma \in \mathcal{S}_n$, alors : $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \operatorname{sign}(\sigma) f(x_1, \ldots, x_n)$.
3. Si on ajoute à l'un des x_i une combinaison linéaire des autres x_j, alors la valeur de f ne change pas.
4. Si $x_1, \ldots, x_n$ sont linéairement dépendants, alors : $f(x_1, \ldots, x_n) = 0$.

Preuve.

1. Supposons $i < j$. Fixons x_k pour $k \neq i$ et $k \neq j$ et posons :

$$g(x, y) = f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{j-1}, y, x_{j+1}, \ldots, x_n).$$

g étant bilinéaire alternée on a :

$$0 = g(x+y, x+y) = g(x, x+y) + g(y, x+y) = g(x, x) + g(x, y) + g(y, x) + g(y, y),$$

donc :

$$g(x, y) = -g(y, x).$$

2. On peut passer de la suite $(x_1, \ldots, x_n)$ à la suite $(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ par une succession de m transpositions. Par le point 1, on a ainsi :

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = (-1)^m f(x_1, \ldots, x_n).$$

Or : $(-1)^m = \operatorname{sign}(\sigma)$.

3. Revenons à $g(x, y)$ comme plus haut. Il suffit de vérifier que, $\forall \lambda \in \mathbb{K}$, $g(x + \lambda y) = g(x, y)$, ce qui est clair :

$$g(x + \lambda y, y) = g(x, y) + \lambda g(y, y) = g(x, y).$$

4. Supposons $x_1 = \sum_{i=2}^{n} \lambda_i x_i$, alors :

$$f(x_1, \ldots, x_n) = f(x_1 - \sum_{i=2}^{n} \lambda_i x_i, x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n) = 0.$$

□

En corollaire on obtient :

Proposition 3.2

Si V est un $\mathbb{K}$-espace vectoriel de dimension finie, on a $\mathcal{A}lt_n(V) = \{0\}$ pour $n > \dim V$.

Théorème 3.3

Soit V un $\mathbb{K}$-espace vectoriel de dimension n. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base ordonnée de V. Alors il existe une unique forme n-multilinéaire alternée sur V, $\Delta_{\mathcal{B}}$, pour laquelle $\Delta_{\mathcal{B}}(e_1, \ldots, e_n) = 1$. Si $\phi \in \mathcal{A}lt_n(V)$, alors $\phi = \phi(e_1, \ldots, e_n)\Delta_{\mathcal{B}}$.

Remarque 2

Ce théorème montre en particulier que dim $\mathcal{A}lt_n(v) = 1$.

Preuve. 1. Supposons que $\Delta_{\mathcal{B}}$ existe. Soit $x_1, \ldots, x_n \in V$. Pour chaque $i = 1, \ldots, n$ on a $x_i = \sum_{j=1}^{n} x_{ij} e_j$. Alors :

$$\begin{aligned}
\Delta_{\mathcal{B}}(x_1, \ldots, x_n) &= \Delta_{\mathcal{B}}(\sum_{j=1}^{n} x_{1j_1} e_{j_1}, \ldots, \sum_{j=1}^{n} x_{nj_n} e_{j_n}) \\
&= \sum_{(j_1, \ldots, j_n) \in \mathbb{N}_n^n} x_{1j_1} \ldots x_{nj_n} \Delta_{\mathcal{B}}(e_{j_1}, \ldots, e_{j_n}) \\
&= \sum_{\sigma \in \mathcal{S}_n} x_{1\sigma(1)} \ldots x_{n\sigma(n)} \Delta_{\mathcal{B}}(e_{\sigma(1)}, \ldots, e_{\sigma(n)}) \\
&= \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) x_{1\sigma(1)} \ldots x_{n\sigma(n)} \Delta_{\mathcal{B}}(e_1, \ldots, e_n) \\
&= \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) x_{1\sigma(1)} \ldots x_{n\sigma(n)},
\end{aligned}$$

d'où l'unicité de $\Delta_{\mathcal{B}}$ si elle existe.

2. Montrons que $\phi = \phi(e_1, \ldots, e_n)\Delta_{\mathcal{B}}$, $\forall \phi \in \mathcal{A}lt_n(V)$. On fait les mêmes déductions avec ϕ au lieu de $\Delta_{\mathcal{B}}$ (elles sont valables, sauf la dernière étape), on obtient :

$$\begin{aligned}
\phi(x_1, \ldots, x_n) &= \underbrace{\sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) x_{1\sigma(1)} \ldots x_{n\sigma(n)}}_{\Delta_{\mathcal{B}}(x_1, \ldots, x_n)} \phi(e_1, \ldots, e_n) \\
&= \phi(e_1, \ldots, e_n)\Delta_{\mathcal{B}}(x_1, \ldots, x_n),
\end{aligned}$$

$\forall x_1, \ldots, x_n \in V$, d'où la conclusion.

3. Définissons $\Delta_{\mathcal{B}}$ par l'expression trouvée dans la première partie :

$$\Delta_{\mathcal{B}}(x_1, \ldots, x_n) = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) x_{1\sigma(1)} \ldots x_{n\sigma(n)} \quad \forall x_1, \ldots, x_n \in V.$$

Il est clair que

$$\Delta_{\mathcal{B}}(e_1, \ldots, e_n) = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) \delta_{1\sigma(1)} \ldots \delta_{n\sigma(n)} = 1.$$

Il est aussi clair que $\Delta_{\mathcal{B}}$ est n-multilinéaire. Pour chaque $\sigma \in \mathcal{S}_n$ l'application

$$(x_1, \ldots, x_n) \mapsto x_{1\sigma(1)} \ldots x_{n\sigma(n)}$$

est n-multilinéaire et $\Delta_{\mathcal{B}}$ est une combinaison linéaire de ces formes n-multilinéaires particuliaires.
Il n'y a plus qu'à vérifier que $\Delta_{\mathcal{B}}$ est alternée. Supposons $x_i = x_j$ avec $i < j$ et calculons $\Delta_{\mathcal{B}}(x_1, \ldots, x_n)$.
Posons :

$$\begin{aligned}
\Sigma_+ &= \{\sigma \in \mathcal{S}_n | \sigma(i) < \sigma(j)\} \\
\Sigma_- &= \{\sigma \in \mathcal{S}_n | \sigma(i) > \sigma(j)\}.
\end{aligned}$$

Soit τ la transposition qui échange i et j. Clairement l'application de $\mathcal{S}_n$ dans lui-même définie par $\sigma \mapsto \sigma\tau$ est une bijection, de $\mathcal{S}_n$ sur lui-même, qui échange Σ_+ et Σ_-.
Alors :

$$\begin{aligned}\Delta_{\mathcal{B}}(x_1,\ldots,x_n) &= \sum_{\sigma\in\Sigma_+} \text{sign}(\sigma)x_{1\sigma(1)}\ldots x_{n\sigma(n)} + \sum_{\sigma\in\Sigma_-} \text{idem} \\ &= \sum_{\sigma\in\Sigma_+} \text{sign}(\sigma)x_{1\sigma(1)}\ldots x_{n\sigma(n)} + \sum_{\sigma\in\Sigma_+} \text{sign}(\sigma\tau)x_{1\sigma\tau(1)}\ldots x_{n\sigma\tau(n)}\end{aligned}$$

Or :

$$\begin{array}{llll} \text{si } k\neq i \text{ et } k\neq j, & \text{alors } \tau(k)=k, & \text{et :} & x_{k\sigma\tau(k)} = x_{k\sigma(k)} \\ \text{si } k=i, & \text{alors } \tau(i)=j, & \text{et :} & x_{i\sigma\tau(i)} = x_{i\sigma(j)} = x_{j\sigma(j)} \\ \text{si } k=j, & \text{alors } \tau(j)=i, & \text{et :} & x_{j\sigma\tau(j)} = x_{j\sigma(i)} = x_{i\sigma(i)}, \end{array}$$

d'où :

$$x_{1\sigma\tau(1)}\ldots x_{n\sigma\tau(n)} = x_{1\sigma(1)}\ldots x_{n\sigma(n)},$$

et donc :

$$\Delta_{\mathcal{B}}(x_1,\ldots,x_n) = \sum_{\sigma\in\Sigma_+} (\text{sign}(\sigma)+\text{sign}(\sigma\tau))x_{1\sigma(1)}\ldots x_{n\sigma(n)}.$$

Enfin $\forall\sigma\in\mathcal{S}_n$:

$$\text{sign}(\sigma)+\text{sign}(\sigma\tau) = \text{sign}(\sigma)+\text{sign}(\sigma)\text{sign}(\tau) = \text{sign}(\sigma)-\text{sign}(\sigma) = 0,$$

ce qui implique :

$$\Delta_{\mathcal{B}}(x_1,\ldots,x_n) = 0.$$

□

3.2 Déterminant

Definition 3

Choisissons $V = M_{1\times n}(\mathbb{K})$, $\mathcal{B} = (e_1,\ldots,e_n)$ la base canonique avec $e_1 = (1,0,\ldots,0)$,…,$e_n = (0,\ldots,0,1)$ etc. et $\Delta_{\mathcal{B}} \in \mathcal{A}lt_{\,n}(V)$ la n-forme multilinéaire alternée définie au théorème (3.3).

Si $A\in M_n(\mathbb{K})$ on définit le *déterminant de A* par :

$$\det(A) = \Delta_{\mathcal{B}}(l_1(A),\ldots,l_n(A)) = \sum_{\sigma\in\mathcal{S}_n} \text{sign}(\sigma)a_{1\sigma(1)}\ldots a_{n\sigma(n)}.$$

Ainsi $\det : M_n(\mathbb{K}) \to \mathbb{K}$ est l'unique forme multilinéaire alternée en fonction des lignes des matrices de $M_n(\mathbb{K})$ telle que $\det(I_n) = 1$.

Propriété 3.4

Si $A\in M_n(\mathbb{K})$, alors $\det(A^t) = \det(A)$.

Preuve. Pour $A = (a_{ij})$, il faut prouver l'égalité :

$$\sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} = \sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

$a_{1\sigma(1)} \dots a_{n\sigma(n)}$ est le produit de tous les coefficients a_{ij} de A pour lesquels $j = \sigma(i)$. C'est donc aussi le produit de tous les a_{ij} tels que $i = \sigma^{-1}(j)$, i. e. $a_{\sigma(1)1} \dots a_{\sigma(n)n}$. On a aussi pour toute permutation $\sigma \in \mathcal{S}_n$ $\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma^{-1})$, d'où :

$$\begin{aligned}\sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} &= \sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma^{-1}) a_{\sigma^{-1}(1)1} \dots a_{\sigma^{-1}(n)n} \\ &= \sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n},\end{aligned}$$

car lorsque σ parcours $\mathcal{S}_n$, alors σ^{-1} aussi. □

Théorème 3.5

Si $A, B \in M_n(\mathbb{K})$, alors :
$$\det(AB) = \det(A)\det(B).$$

Preuve. Soit $\mathcal{B} = (e_1, \dots, e_n)$ la base ordonnée canonique de l'espace vectoriel $M_{1\times n}(\mathbb{K})$ et $\Delta_{\mathcal{B}}$ la forme n-multilinéaire alternée sur $M_{1\times n}(\mathbb{K})$ telle que $\Delta_{\mathcal{B}}(e_1, \dots, e_n) = 1$. Observons que si $M, N \in M_n(\mathbb{K})$, on a $l_i(MN) = l_i(M)N$ pour $i = 1, \dots, n$.

On définit une application $\phi : M_{1\times n}(\mathbb{K}) \times \dots \times M_{1\times n}(\mathbb{K}) \to \mathbb{K}$ par

$$\phi(x_1, \dots, x_n) = \Delta_{\mathcal{B}}(x_1 B, \dots, x_n B).$$

Il est immédiat que ϕ est une forme n-multilinéaire alternée sur $M_{1\times n}(\mathbb{K})$. On a :

$$\phi = \phi(e_1, \dots, e_n)\Delta_{\mathcal{B}}.$$

Comme $e_i = l_i(I_n)$, :

$$\begin{aligned}\phi(e_1, \dots, e_n) &= \Delta_{\mathcal{B}}(l_1(I_n)B, \dots, l_n(I_n)B) \\ &= \Delta_{\mathcal{B}}(l_1(I_nB), \dots, l_n(I_nB)) \\ &= \Delta_{\mathcal{B}}(l_1(B), \dots, l_n(B)) = \det(B).\end{aligned}$$

De même :

$$\begin{aligned}\phi(l_1(A), \dots, l_n(A)) &= \Delta_{\mathcal{B}}(l_1(A)B, \dots, l_n(A)B) \\ &= \Delta_{\mathcal{B}}(l_1(AB), \dots, l_n(AB)) = \det(AB).\end{aligned}$$

Ainsi :

$$\underbrace{\phi(l_1(A), \dots, l_n(A))}_{\det(AB)} = \underbrace{\phi(e_1, \dots, e_n)}_{\det(B)} \underbrace{\Delta_{\mathcal{B}}(l_1(A), \dots, l_n(A))}_{\det(A)}.$$

□

Théorème 3.6

Soit $A = (a_{ij}) \in M_n(\mathbb{K})$ et $i \in \mathbb{N}_n$.

1. $\det(A) = \sum_{k=1}^{n} (-1)^{k+i} a_{ik} \det A(\{i\}, \{k\})$.
2. $\det(A) = \sum_{k=1}^{n} (-1)^{k+i} a_{ki} \det A(\{k\}, \{i\})$.

Notation 1

Si $A \in M_n(\mathbb{K})$, on écrit $A(i, j)$ au lieu de $A(\{i\}, \{j\})$ $\forall i, j \in \mathbb{N}_n$.

Démonstration. On peut énoncer ce théorème par les formules suivantes :

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

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

a) (resp. b)) s'appelle le *développement de* $\det A$ *selon les éléments de la* i^e *ligne* (i^e colonne.) Prouvons a). Soient $e_1, \dots, e_n$ les éléments de la base canonique de $M_{1\times n}(\mathbb{K})$. On a donc : $l_i(A) = \sum_{j=1}^{n} a_{ij} e_i$.

Si on fait passer la i^e ligne de A à la 1^{re} place, alors A devient $\begin{pmatrix} l_i(A) \\ \hline A(\{i\}; \emptyset) \end{pmatrix}$.

On obtient cette modification en échangeant la i^e ligne avec chacune des $i - 1$ lignes qui précèdent. On a donc :

$$\det A = (-1)^{i-1} \det \begin{pmatrix} l_i(A) \\ \hline A(\{i\}; \emptyset) \end{pmatrix} = (-1)^{i-1} \sum_{j=1}^{n} a_{ij} \det \begin{pmatrix} e_j \\ \hline A(\{i\}; \emptyset) \end{pmatrix}.$$

Si on fait passer la j^e colonne de $\begin{pmatrix} e_j \\ \hline A(\{i\}; \emptyset) \end{pmatrix}$ à la 1^{re} place, on obtient la matrice :

$$\left(\begin{array}{c|c} 1 & 0 \\ * & A(i, j) \end{array}\right).$$

Comme précédemment cela s'obtient en échangeant la j^e colonne avec chacune des $j - 1$ colonnes qui la précèdent. Donc :

$$\det \begin{pmatrix} e_j \\ \hline A(\{i\}; \emptyset) \end{pmatrix} = (-1)^{j-1} \det \left(\begin{array}{c|c} 1 & 0 \\ * & A(i, j) \end{array}\right).$$

De plus, en ajoutant à chacune des lignes d'indice 2 à n un multiple scalaire convenable de la 1^{re} ligne, on peut transformer la matrice $\left(\begin{array}{c|c} 1 & 0 \\ * & A(i, j) \end{array}\right)$ en $\left(\begin{array}{c|c} 1 & 0 \\ 0 & A(i, j) \end{array}\right)$, ce qui ne change pas le déterminant. On trouve ainsi :

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \left(\begin{array}{c|c} 1 & 0 \\ 0 & A(i, j) \end{array}\right),$$

d'où la formule a) via le lemme suivant.

La formule b) s'obtient en appliquant la formule a) à la matrice transposée A^t et en observant que $A^t(i, j) = A(j, i)^t$ et en utilisant l'invariance du déterminant par transposition. □

Lemme 3.7

Soit $n \geq 2$. Si $A \in M_{n-1}(\mathbb{K})$, on a :

$$\det \left(\begin{array}{c|c} 1 & 0 \\ 0 & A(i,j) \end{array}\right) = \det A.$$

Preuve. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ la base ordonnée canonique de $M_{1\times n}(\mathbb{K})$ et $\Delta_{\mathcal{B}}$ la forme n-multilinéaire alternée sur $M_{1\times n}(\mathbb{K})$ pour laquelle $\Delta_{\mathcal{B}}(e_1, \ldots, e_n) = 1$. Soit pour $X = (x_1, \ldots, x_{n-1}) \in M_{1\times n-1}(\mathbb{K})$, $\check{x} = (0, x_1, \ldots, x_{n-1}) \in M_{1\times n}(\mathbb{K})$.

Ainsi, si $\mathcal{B}' = (e'_1, \ldots, e'_n)$ est la base ordonnée canonique de $M_{1\times(n-1)}(\mathbb{K})$, on a $\check{e}'_i = e_{i+1}$ pour $i = 1, \ldots, n-1$.

Posons $\phi : M_{1\times(n-1)}(\mathbb{K}) \times \cdots \times M_{1\times(n-1)}(\mathbb{K}) \to \mathbb{K}$ définie par :

$$\phi(X_1, \ldots, X_{n-1}) = \Delta_{\mathcal{B}}(e_1, \check{X}_1, \ldots, \check{X}_{n-1}).$$

Il est clair que l'application $X \mapsto \check{X}$ est une application linéaire de $M_{1\times(n-1)}(\mathbb{K})$ dans $M_{1\times n}(\mathbb{K})$ et que ϕ est une forme $(n-1)$-multilinéaire alternée sur $M_{1\times(n-1)}(\mathbb{K})$. De plus :

$$\phi(e'_1, \ldots, e'_{n-1}) = \Delta_{\mathcal{B}}(e_1, \check{e}'_1, \ldots, \check{e}'_{n-1}) = \Delta_{\mathcal{B}}(e_1, \ldots, e_n) = 1,$$

donc : $\phi = \Delta_{\mathcal{B}'}$.

En particulier :

$$\phi(l_1(A), \ldots, l_{n-1}(A)) = \det A,$$

et d'autre part, par définition :

$$\phi(l_1(A), \ldots, l_{n-1}(A)) = \Delta_{\mathcal{B}}(e_1, l_1(\check{A}), \ldots, l_n(\check{A})) = \det \left(\begin{array}{c|c} 1 & 0 \\ 0 & A \end{array}\right),$$

d'où le lemme. $\square$

Les théorèmes 3.5 et 3.6 sont des cas particuliers des résultats suivants :

Théorème 3.8 (Binet, Cauchy)

Soient $A \in M_{n\times m}(\mathbb{K})$, $B \in M_{m\times p}(\mathbb{K})$, $C = AB$, $1 \leq r \leq \min(n,p)$. Alors, si $\alpha \in \mathcal{P}_{r,n}$ et $\beta \in \mathcal{P}_{r,p}$:

$$\det C([\alpha, \beta]) = \begin{cases} 0 & \text{si } r > m \\ \displaystyle\sum_{\gamma \in \mathcal{P}_{r,m}} \det A([\alpha, \gamma]) \det B([\gamma, \beta]) & \text{si } r \leq m. \end{cases}$$

Théorème 3.9 (Laplace)

Soit $A \in M_n(\mathbb{K})$ et $\alpha \in \mathcal{P}_{r,n}$. On a les formules :

1. $\det A = \displaystyle\sum_{\beta \in \mathcal{P}_{r,n}} (-1)^{\|\alpha\|+\|\beta\|} \det A([\alpha, \beta]) \det A((\alpha, \beta))$,
2. $\det A = \displaystyle\sum_{\beta \in \mathcal{P}_{r,n}} (-1)^{\|\alpha\|+\|\beta\|} \det A([\beta, \alpha]) \det A((\beta, \alpha))$.

(Si $\gamma \in \mathcal{P}_{r,n}$, $\|\gamma\|$ = somme des éléments de γ.)

3.3 Applications

3.3.1 Inversion

On a vu que si $A = (a_{ij}) \in M_n(\mathbb{K})$, on a la formule :

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

Cette formule isole les éléments $a_{i1}, \dots, a_{in}$ de la i^{e} ligne. D'une manière un peu plus explicite on peut écrire :

$$\sum_{j=1}^{n} (-1)^{i+j} x_j \det A(i,j) = \det \begin{pmatrix} l_1(A) \\ \vdots \\ l_{i-1}(A) \\ x_1 \cdots x_n \\ l_{i+1}(A) \\ \vdots \\ l_n(A) \end{pmatrix}.$$

Si $(x_1, \dots, x_n) = l_k(A)$, avec $k \neq i$:

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

est le déterminant d'une matrice qui a deux lignes égales, donc c'est 0. Ainsi :

$$\sum_{j=1}^{n} (-1)^{i+j} a_{kj} \det A(i,j) = \delta_{ki} \det A \quad (1 \leq i, k \leq n). \tag{3.1}$$

Definition 4

Soit $A = (a_{ij}) \in M_n(\mathbb{K})$. On appelle *co-matrice* de A la matrice $\tilde{A} = (\tilde{a}_{ij}) \in M_n(\mathbb{K})$ dont les coefficients sont

$$\tilde{a}_{ij} = (-1)^{i+j} \det A(i,j) \quad (1 \leq i, j \leq n).$$

La relation (3.1) s'écrit simplement :

$$A\tilde{A} = \det(A) I_n.$$

De la même manière, la formule de développement du déterminant par rapport à la j^{e} colonne donne la formule :

$$\sum_{i=1}^{n} (-1)^{i+j} a_{ik} \det A(i,j) = \delta_{jk} \det A \quad (1 \leq j, k \leq n),$$

qui s'écrit simplement :

$$\tilde{A}A = \det(A) I_n.$$

On a donc montré :

Théorème 3.10 (Cramer 1750)

Si $A \in M_n(\mathbb{K})$, alors :
$$\tilde{A}A = A\tilde{A} = \det(A)I_n.$$

Corollaire 3.11

Si $A \in M_n(\mathbb{K})$, alors
$$A \in \mathrm{GL}_n(\mathbb{K}) \Leftrightarrow \det A \neq 0.$$
De plus, si $A \in \mathrm{GL}_n(\mathbb{K})$, alors :
$$A^{-1} = \frac{1}{\det A}\tilde{A}.$$

Preuve. Si $A \in \mathrm{GL}_n(\mathbb{K})$, alors $AA^{-1} = I_n$. Prenons le déterminant :
$$\det A \det(A^{-1}) = \det(AA^{-1}) = \det(I_n) = 1,$$
alors : $\det A \neq 0$. Inversement, supposons que $\det A \neq 0$. Alors le théorème précédent donne :
$$\left(\frac{1}{\det A}\tilde{A}\right) A = A\left(\frac{1}{\det A}\tilde{A}\right) = I_n,$$
donc $A \in \mathrm{GL}_n(\mathbb{K})$ et $A^{-1} = \frac{1}{\det A}\tilde{A}$. □

En particulier, le déterminant donne un homomorphisme de groupes $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ surjectif.[1] On note $\mathrm{SL}_n(\mathbb{K})$ le noyau de cet homomorphisme. Ainsi :
$$\mathrm{SL}_n(\mathbb{K}) = \{A \in \mathrm{GL}_n(\mathbb{K}) | \det A = 1\}.$$
C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$, (en anglais Special Linear group.)

3.3.2 Rang

Théorème 3.12

Soit $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$ et soit $r = \mathrm{rang}(A)$ ($r \leq \min(n, m)$), alors :

a) Il existe $\alpha \in \mathcal{P}_{r,n}$ et $\beta \in \mathcal{P}_{r,m}$, tel que : $\det A[\alpha, \beta] \neq 0$.

b) Si $r < s < \min(n, m)$, alors $\det A[\gamma, \delta] = 0 \ \forall \gamma \in \mathcal{P}_{s,n}, \forall \delta \in \mathcal{P}_{s,m}$.

Preuve. b) Soit $r < s < \min(n, m)$, $\gamma \in \mathcal{P}_{s,n}$ et $\delta \in \mathcal{P}_{s,n}$.
Les lignes $l_{\gamma(1)}(A), \dots, l_{\gamma(s)}(A)$ de A sont linéairement dépendantes. Á fortiori, les lignews de $A[\gamma, \delta]$ sont linéairement dépendantes donc $\det A[\gamma, \delta] = 0$, ce qui prouve b).

a) Puisque A est de rang r, il existe un choix de r lignes linéairement indépendantes $l_{\alpha(1)}(A), \dots, l_{\alpha(r)}(A)$, avec $\alpha \in \mathcal{P}_{r,n}$.
La matrice $A[\alpha, \mathbb{N}_n] \in M_{r\times m}(\mathbb{K})$ est de rang r, elle admet donc r colonnes inépendantes, disons les colonnes d'indice $\beta(1) < \cdots < \beta(r)$ avec $\beta \in \mathcal{P}_{r,m}$ convenable. Alors la matrice $A[\alpha, \beta] \in M_n(\mathbb{K})$ est de rang r et $\det A[\alpha, \beta] \neq 0$.

□

1. $\det \begin{pmatrix} a & 0 \\ 0 & 1_{n-1} \end{pmatrix} = a \ \forall a \in \mathbb{K}^*$

Théorème 3.13

Soit $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$. Supposons que $1 \leq r \leq \min(n, m)$ a les propriétés suivantes :
Il existe $\alpha \in \mathcal{P}_{r,n}$ et $\beta \in \mathcal{P}_{r,m}$ telles que :

1. $\det A[\alpha, \beta] \neq 0$.
2. On a $\det A[\gamma, \delta] = 0$, $\forall \gamma \in \mathcal{P}_{r+1,n}$, $\forall \delta \in \mathcal{P}_{r+1,m}$ telles que $\alpha < \gamma$ et $\beta < \delta$.

Alors : $r = \mathrm{rang} A$.

Preuve. Par a) on a $r \leq \mathrm{rang} A$. Pour démontrer le théorème, on suppose que $\mathrm{rang} A > r$ et on cherche une contradiction.

Puisque $A[\alpha, \beta]$ est inversible, ses lignes sont linéairement indépendantes et à fortiori les lignes $l_{\alpha(1)}(A), \ldots, l_{\alpha(r)}(A)$ sont linéairement indépendantes. Puisque $\mathrm{rang} A > r$ on peut trouver $\gamma \in \mathcal{P}_{r+1,n}$ telle que $\alpha < \gamma$ et $l_{\gamma(1)}(A), \ldots, l_{\gamma(r+1)}(A)$ sont linéairement indépendantes. Les colonnes de $A[\alpha, \beta]$ sont aussi linéairement indépendantes, donc à fortiori aussi les colonnes de $A[\gamma, \beta]$ (qui est donc de rang r.)

$A[\alpha, \beta]$ étant de rang r, ses colonnes sont linéairement indépendantes, donc à fortiori les colonnes de $A[\gamma, \mathbb{N}_m]$ d'indice $\beta(1), \ldots, \beta(\gamma)$ sont linéairement indépendantes, donc il existe $\delta \in \mathcal{P}_{r+1,m}$ tel que $\beta < \delta$ et telle que les colonnes de $A[\gamma, \mathbb{N}_m]$ d'indice $\delta(1), \ldots, \delta(r+1)$ soient linéairement indépendantes.

Ainsi la matrice $A[\gamma, \delta] \in M_{r+1}(\mathbb{K})$ est de rang $r+1$ et donc $\det A[\gamma, \delta] \neq 0$ contredisant la condition b). $\square$

3.3.3 Orientation

L'ensemble $\mathrm{GL}_n^+(\mathbb{R})$ des éléments de $\mathrm{GL}_n(\mathbb{R})$ de déterminant positif est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

Soit V un espace vectoriel réel de dimension finie n. Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases ordonnées de V, on dit qu'elles ont la même orientation (notation : $\mathcal{B} \sim \mathcal{B}'$,) si $M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V) \in \mathrm{GL}_n^+(\mathbb{R})$. C'est une relation d'équivalence sur l'ensemble de toutes les bases ordonnées de V.

Il y a exactement deux classes d'équivalence. Se donner une orientation, c'est choisir l'une de ces deux classes d'équivalence. On dit alors que V est un espace vectoriel réel orienté.

Chapitre 4

Endomorphismes

4.1 Généralités

Rappels

Si V est un $\mathbb{K}$-espace vectoriel, un endomorphismede V est une application linéaire de V dans lui-même. On note $\mathcal{L}(V)$ l'ensemble des endomorphismes de V. $\mathcal{L}(V)$ est une $\mathbb{K}$-algèbre pour les opérations suivantes :

1. Si $\lambda \in \mathbb{K}$ et $\alpha \in \mathcal{L}(V)$: $(\lambda\alpha)(x) = \lambda\,\alpha(x),\ \forall x \in V$.
2. Si $\alpha, \beta \in \mathcal{L}(V)$: $(\alpha+\beta)(x) = \alpha(x) + \beta(x),\ \forall x \in V$.
3. Si $\alpha, \beta \in \mathcal{L}(V)$: $(\alpha\beta)(x) = \alpha(\beta(x)),\ \forall x \in V$.

Si $f = \sum_{i=0}^{n} a_i t^i \in \mathbb{K}[t]$ et si $\alpha \in \mathcal{L}(V)$, on note $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$. Donc $f(\alpha) \in \mathcal{L}(V)$. On observe que :

1. Si $f, g \in \mathbb{K}[t]$, alors : $f(\alpha)g(\alpha) = g(\alpha)f(\alpha)\ \forall \alpha \in \mathcal{L}(V)$.
2. L'ensemble de tous les $f(\alpha)$ pour $f \in \mathbb{K}[t]$ est une sous-algèbre de $\mathcal{L}(V)$. C'est la plus petite qui contienne α. On la note $\mathbb{K}[\alpha]$.

Definition 1

Soit $\alpha \in \mathcal{L}(V)$. Un sous-espace W de V est dit *invariant par* α si $\alpha(W) \subset W$.

Remarque 1

1. Si W est invariant par α, alors, par restriction à W, α donne un endomorphisme de W $\alpha|_W$: $W \to W$, l'endomorphisme *induit* par α.
2. Parmi les sous-espaces de V invariants par α, il y a $\{0\}$, V, $\ker(\alpha)$ et $\mathrm{im}(\alpha)$.
3. Si $\beta\alpha = \alpha\beta$ et si W est invariant par α, alors $\beta(W)$ et $\beta^{-1}(W)$ sont invariants par α.
   Par exemple $\ker(\beta)$ et $\mathrm{im}(\beta)$ sont invariants par α. Plus particulièrement, si $f \in \mathbb{K}[t]$, alors $\ker\ f(\alpha)$ et $\mathrm{im}\,f(\alpha)$ sont invariants par α.
4. Si $\lambda \in \mathbb{K}$, alors tout sous-espace vectoriel de V est invariant par $\lambda\mathrm{id}_V$.
   Si $\alpha \in \mathcal{L}(V)$ est tel que tout sous-espace de V est invariant par α, alors $\exists\lambda \in \mathbb{K}$ tel que $\alpha = \lambda\mathrm{id}_V$.

5. Toute somme et toute intersection de sous-espaces invariants par α est encore un sous-espace invariant par α.
6. Si W est un sous-espace de V invariant par $\alpha \in \mathcal{L}(V)$, il n'existe pas toujours un sous-espace invariant par α supplémentaire de W dans V.

Exemple 1

$V = \mathbb{R}[t]$ et $\alpha : V \to V$ définie par $\alpha(f) = f'$ (la dérivée de f) où :

$$\left(\sum_{i=0}^{n} a_i t^i\right)' = \sum_{i=1}^{n} i a_i t^{i-1}.$$

Les sous-espaces invariants par α sont exactement les sous-espaces $\mathbb{R}[t]_n$ pour $n = 0, 1, \ldots$, où :

$$\mathbb{R}[t]_n = \{f \in \mathbb{R}[t] | \deg\, f \leq n\},$$

$\{0\}$ et $\mathbb{R}[t]$.

Ainsi aucun des sous-espaces invariants $\mathbb{R}[t]_n$ pour $n = 0, 1, \ldots$ n'a de supplémentaire invariant.

Definition 2

On dit que $\alpha \in \mathcal{L}(V)$ est *semi-simple* si tout sous-espace invariant admet un supplémentaire invariant.

Remarque 2

Si W est un sous-espace invariant par $\alpha \in \mathcal{L}(V)$, alors c'est aussi un sous-espace invariant par $f(\alpha)$, $\forall f \in \mathbb{K}[t]$.

4.2 Polynômes

4.3 Passage aux matrices

Chapitre 5

Formes bilinéaires et sesquilinéaires

5.1 Formes bilinéaires

Definition 1 (Rappel)

Soit V un $\mathbb{K}$-espace vectoriel. On appelle *forme bilinéaire sur V* toute application $\phi : V \times V \to \mathbb{K}$ telle que :

1. $\phi(x_1 + x_2, y) = \phi(x_1, y) + \phi(x_2, y), \forall x_y, x_2, y \in V$
   $\phi(\lambda x, y) = \lambda\phi(x, y), \forall \lambda \in \mathbb{K}, \forall x, y \in V.$
2. $\phi(x, y_1 + y_2) = \phi(x, y_1) + \phi(x, y_2), \forall x, y_1, y_2 \in V,$
   $\phi(x, \lambda y) = \lambda\phi(x, y), \forall \lambda \in \mathbb{K}, \forall x, y \in V.$

Exemple 1

1. $V = M_{n\times m}(\mathbb{K})$, $\phi : V \times V \to \mathbb{K}$, définie par :
$$\phi(\mathbf{A}, \mathbf{B}) = \mathrm{tr}\,(\mathbf{A}^t\mathbf{B}).$$
2. $\xi, \psi \in V^\#$ permettent de définir $\phi : V \times V \to \mathbb{K}$ telle que :
$$\phi(x, y) = \xi(x)\psi(y), \quad \forall x, y \in V.$$
3. Si $\xi_1, \ldots, \xi_n, \psi_1, \ldots, \psi_n \in V^\#$, on peut définir :
$$\phi(x, y) = \sum_{i,j} a_{ij}\xi_i(x)\psi_j(y),$$
   où $A = (a_{ij}) \in M_{n\times m}(\mathbb{K})$.
4. Soit V un espace vecoriel de la géométrie euclidienne de dimension 3.
   $\phi(x, y) = |x|\,|y| \cos(\angle(x, y))$ (le produit scalaire usuel) où $|x|$ est la longueur de x.

Si $V \equiv \mathbb{R}^3$ via une base orthonormée (e_1, e_2, e_3) de V, on sait que :

$$\phi(x, y) = \phi((x_1, x_2, x_3), (y_1, y_2, y_3)) = \sum_{i=1}^{3} x_i y_i.$$

Definition 2

Soit $\phi : V \times V \to \mathbb{K}$ une forme bilinéaire sur V. On définit $\tilde{\phi} : V \to V^\#$ par $\tilde{\phi}(y)(x) = \phi(x, y)$, $\forall x, y \in V$. On vérifie que $\tilde{\phi}$ est l'*application linéaire associée* à ϕ.

L'application $\phi \mapsto \tilde{\phi}$ est une bijection de l'ensemble des formes bilinéaires sur V sur $\mathcal{L}(V, V^\#)$.

Si V est de dimension finie n et si $\mathcal{B} = (e_1, \dots, e_n)$ est une base ordonnée de V, alors à toute forme bilinéaire $\phi : V \times V \to \mathbb{K}$ on peut associer la matrice relative à $\mathcal{B}$: $M_{\mathcal{B}}(\phi) = (\phi(e_i, e_j))$ (élément de la i^e^ ligne et j^e^ colonne).

Posant $a_{ij} = \phi(e_i, e_j)$, on voit que :

$$\phi(\sum_{i=1}^{n} x^i e_i, \sum_{j=1}^{n} y^j e_j) = \sum_{i=1}^{n} \sum_{j=1}^{n} x^i y^j a_{ij}. \tag{5.1}$$

On vérifie facilement que pour une base ordonnée $\mathcal{B}$ fixée, l'application $\phi \mapsto M_{\mathcal{B}}(\phi)$ est une bijectionde l'ensemble des formes bilinéaires sur V sur $M_n(\mathbb{K})$.

Remarque 1

Si $A = (a_{ij})$, $X = \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix}$ et $Y = \begin{pmatrix} y^1 \\ \vdots \\ y^n \end{pmatrix}$, alors (5.1) s'écrit :

$$\phi(\sum_{i=1}^{n} x^i e_i, \sum_{j=1}^{n} y^j e_j) = X^t A Y.$$

Lorsque l'on change de base ordonnée, supposons $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{B}' = (e'_1, \dots, e'_n)$ des bases ordonnées et $T = M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$, et soit $\phi : V \times V \to \mathbb{K}$ bilinéaire, $A = M_{\mathcal{B}}(\phi)$ $A' = M_{\mathcal{B}'}(\phi)$. Alors :

$$\phi(x, y) = X^t A Y = X'^t A' Y',$$

où $x = \sum x^i e_i = \sum x^{i\prime} e_i{}'$ et $X = \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix}$, $X' = \begin{pmatrix} x^{1\prime} \\ \vdots \\ x^{n\prime} \end{pmatrix}$ et idem pour Y et Y'. On a alors :

$$X = TX' \quad \text{et} \quad Y = TY',$$

donc :

$$X^t A Y = X'^t T^t A T Y' = X'^t A' Y'.$$

Comme ceci est valable pour tout X', Y', on obtient :

$$\boxed{A' = T^t A T}$$

Definition 3

On dit que $A, B \in M_n(\mathbb{K})$ sont *congruents* s'il existe $T \in GL_n(\mathbb{K})$ telle que $B = T^t A T$. On notera $A \cong B$. C'est une relation d'équivalence sur $M_n(\mathbb{K})$.

On a donc :

Théorème 5.1

Soient $\phi : V \times V \to \mathbb{K}$ une forme bilinéaire, $A, B \in M_n(\mathbb{K})$ et $\mathcal{B}$ une base ordonnée de V telle que $A = M_{\mathcal{B}}(\phi)$, alors :

$$A \cong B \Leftrightarrow \exists \text{ une base ordonnée } \mathcal{B}' \text{ telle que } B = M_{\mathcal{B}'}(\phi).$$

Remarque 2

Si $\phi : V \times V \to \mathbb{K}$ est une forme bilinéaire sur V et si $\tilde{\phi} : V \to V^{\#}$ est l'application linéaire associée et si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base ordonnée de V, alors on a :

$$M_{\mathcal{B}}(\phi) = M_{\mathcal{B}}^{\mathcal{B}^{\#}}(\tilde{\phi}).$$

5.2 Formes bilinéaires symétriques

Definition 4

Une forme bilinéaire $\phi : V \times V \to \mathbb{K}$ est dite *symétrique* si : $\phi(x, y) = \phi(y, x)$ $\forall x, y \in V$.

Lemme 5.2

Si $\phi : V \times V \to \mathbb{K}$ est une forme bilinéaire et si $\mathcal{B}$ est une base ordonnée de V et $A = M_{\mathcal{B}}(\phi)$, alors :

$$\phi \text{ est symétrique } \Leftrightarrow A \text{ est symétrique.}$$

(i. e. $A^t = A$.)

Definition 5

Une forme bilinéaire symétrique $\phi : V \times V \to \mathbb{K}$ est dite *non dégénérée* si la condition $\phi(x, y) = 0$ $\forall y \in V$ implique $x = 0$.

Lemme 5.3

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base ordonnée de V, $\phi : V \times V \to \mathbb{K}$ une forme bilinéaire symétrique et $A = M_{\mathcal{B}}(\phi)$. Alors :

$$\phi \text{ est non dégénérée } \Leftrightarrow A \in \mathrm{GL}_n(\mathbb{K}).$$

Preuve. La condition $\phi(x, y) = 0$, $\forall y \in V$, équivaut à :

$$X^t AY = 0, \quad \forall Y \in M_{n\times 1}(\mathbb{K}),$$

ce qui équivaut à $X^t A = 0$, ou encore à $AX = 0$.

Donc :

$$\begin{aligned} \phi \text{ non dégénérée } &\Leftrightarrow (AX = 0 \Rightarrow X = 0) \\ &\Leftrightarrow A \text{ est inversible.} \end{aligned}$$

□

Lemme 5.4

Soient $A \in \mathrm{GL}_n(\mathbb{K})$, $C \in M_m(\mathbb{K})$, $B \in M_{n\times m}(\mathbb{K})$, alors on a :

$$\left(\begin{array}{c|c} I_n & 0 \\ \hline -B^t A^{-1} & I_m \end{array}\right) \left(\begin{array}{c|c} A & B \\ \hline B^t & C \end{array}\right) \left(\begin{array}{c|c} I_n & -A^{-1}B \\ \hline 0 & I_m \end{array}\right) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & C - B^t A^{-1} B \end{array}\right).$$

Corollaire 5.5

Si $A = A^t \in \mathrm{GL}_n(\mathbb{K})$. $C = C^t \in M_n(\mathbb{K})$, $B \in M_{n\times m}(\mathbb{K})$. alors :

$$\left(\begin{array}{c|c} A & B \\ \hline B^t & 0 \end{array}\right) \cong \left(\begin{array}{c|c} A & 0 \\ \hline 0 & C - B^t A^{-1} B \end{array}\right),$$

et la matrice de passage peut être choisie *triangulaire unipotente.*

Théorème 5.6

Si $\mathbb{K}$ n'est pas de caractéristique 2, toute matrice symétrique $A \in M_n(\mathbb{K})$ est congruente à une matrice diagonale.

Definition 6

Soit V un $\mathbb{K}$-espace vectoriel. On appelle *forme quadratique* sur V une application q telle que :

1. $q(\lambda x) = \lambda^2 q(x)$, $\forall \lambda \in \mathbb{K}$, et $\forall x \in V$.
2. L'application de $V \times V \to \mathbb{K}$ définie par $(x, y) \mapsto q(x + y) - q(x) - q(y)$ est bilinéaire (év.

symétrique.)

Exemple 2

Soit $\phi : V \times V \to \mathbb{K}$ une forme bilinéaire. L'application $q : V \to \mathbb{K}$ définie par $q(x) = \phi(x, x)$, $\forall x \in V$ est une forme quadratique, dite *associée à* ϕ.

Si q est la forme quadratique associée à ϕ, alors :

$$\begin{aligned} q(x+y) - q(x) - q(y) &= \phi(x+y, x+y) - \phi(x, x) - \phi(y, y) \\ &= [\phi(x, x) + \phi(x, y) + \phi(y, x) + \phi(y, y)] - \phi(x, x) - \phi(y, y) \\ &= \phi(x, y) + \phi(y, x). \end{aligned}$$

Si ϕ est symétrique on obtient :

$$2\phi(x, y) = q(x+y) - q(x) - q(y).$$

On peut en tirer :

$$\phi(x, x) = \frac{1}{2}[q(x, y) - q(x) - q(y)],$$

et de même :

$$\phi(x, y) = \frac{1}{4}[q(x+y) - q(x-y)],$$

pour autant que $\mathbb{K}$ soit de caractéristique différente de 2.

Corollaire 5.7

Si $\phi : V \times V \to \mathbb{K}$ est une forme bilinéaire symétrique non nulle et si la caractéristique de $\mathbb{K}$ est différente de 2, alors il existe $x \in V$ tel que :

$$\phi(x, x) \neq 0.$$

Preuve du théorème. Soit $A = A^t \in M_n(\mathbb{K})$ et $\mathrm{Car}(\mathbb{K}) \neq 2$. Par récurrence sur n :

pour $n = 1$: C'est immédiat.

pour $n > 1$: Supposons $n > 1$ et le résultat vrai pour les matrices symétriques $(n-1) \times (n-1)$.

Si $A = 0$, elle est déjà diagonale.

Si $A \neq 0$, on utilise le corollaire. Il existe $X \in M_{n\times 1}(\mathbb{K})$, $X \neq 0$, tel que $X^t AX \neq 0$.

Soit $T \in \mathrm{GL}_n(\mathbb{K})$ admettant X pour première colonne. Alors $B = T^t AT = (b_{ij})$ est une matrice symétrique telle que :

$$b_{11} = X^t AX \neq 0.$$

Par le lemme B est congruente à une matrice de la forme :

$$C = \left(\begin{array}{c|c} b_{11} & 0 \\ 0 & B_0 \end{array}\right), \quad \text{avec : } B_0 = B_0^t \in M_{n-1}(\mathbb{K}).$$

Par hypothèse de récurrence, il existe $S_0 \in \mathrm{GL}_{n-1}(\mathbb{K})$, telle que $S_0^t B_0 S_0$ est diagonale. Alors :

$$\left(\begin{array}{c|c} 1 & 0 \\ 0 & S_0^t \end{array}\right) \left(\begin{array}{c|c} b_{11} & 0 \\ 0 & B_0 \end{array}\right) \left(\begin{array}{c|c} 1 & 0 \\ 0 & S_0 \end{array}\right) = \left(\begin{array}{c|c} b_{11} & 0 \\ 0 & S_0^t B_0 S_0 \end{array}\right),$$

qui est diagonale.

$\square$

Il reste encore à résoudre le problème de la congruence de deux matrices diagonales. L'ordre des éléments de la diagonale ne change pas la classe de congruence :

$$\mathrm{diag}(\lambda_{\alpha_1}, \ldots, \lambda_{\alpha_n}) = P^t \mathrm{diag}(\lambda_1, \ldots, \lambda_n) P,$$

où : $P = P(\alpha) = (P_{ij})$, avec :

$$P_{ij} = \begin{cases} 1 & \text{si } i = \sigma(j) \\ 0 & \text{sinon.} \end{cases}$$

On peut aussi multiplier les coefficients diagonaux par des carrés arbitraires :

$$\mathrm{diag}(\mu_1^2\lambda_1, \ldots, \mu_n^2\lambda_n) = \mathrm{diag}(\mu_1, \ldots, \mu_n)\mathrm{diag}(\lambda_1, \ldots, \lambda_n)\mathrm{diag}(\mu_1, \ldots, \mu_n),$$

où $\mu_1, \ldots, \mu_n \neq 0$.

Théorème 5.8

Soit $A = A^t \in M_n(\mathbb{C})$ de rang r, alors :

$$A \cong \mathrm{diag}(\underbrace{1, \ldots, 1}_{r \text{ fois}}, 0, \ldots, 0).$$

Preuve. On sait que $A \cong \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, où r éléments sont non nuls et $n - r$ sont nuls. On applique la formule ci dessus avec :

$$\begin{cases} \mu_i = \sqrt{\lambda_i^{-1}} & \text{si } \lambda_i \neq 0 \\ \mu_i = 1 & \text{si } \lambda_i = 0. \end{cases}$$

$\square$

Corollaire 5.9

Si $A = A^t$ et $B = B^t \in M_n(\mathbb{C})$, alors :

$$A \cong B \Leftrightarrow \mathrm{rang}\, A = \mathrm{rang}\, B.$$

Théorème 5.10 (Théorème d'inertie de Sylvester)

Soit $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n \in \mathbb{R}$, alors, en posant :

$$\begin{aligned} \nu_+ &= \text{nombre des } i \text{ tels que } \lambda_i > 0, \\ \nu_- &= \text{nombre des } i \text{ tels que } \lambda_i < 0, \\ \tau_+ &= \text{nombre des } i \text{ tels que } \mu_i > 0, \\ \tau_- &= \text{nombre des } i \text{ tels que } \mu_i < 0, \end{aligned}$$

on a :

$$\mathrm{diag}(\lambda_1, \dots, \lambda_n) \cong \mathrm{diag}(\mu_1, \dots, \mu_n) \Leftrightarrow \nu_+ = \tau_+ \text{ et } \nu_- = \tau_-.$$

Definition 7

Si $A = \mathrm{diag}(\lambda_1, \dots, \lambda_n) \in M_n(\mathbb{R})$, et $n_+(A)$ est le nombre d'éléments diagonaux positifs, $n_-(A)$ le nombre d'éléments diagonaux négatifs, on appelle *signature* de A l'entier :

$$\mathrm{sign}(A) = n_+(A) - n_-(A) \in \mathbb{Z}.$$

Théorème 5.11

Soient $A = A^t$, $B = B^t \in M_n(\mathbb{R})$, alors $A \cong B$ si et seulement si

$$\begin{aligned} \mathrm{rang}(A) &= \mathrm{rang}(B) \\ \mathrm{sign}(A) &= \mathrm{sign}(B). \end{aligned}$$

Théorème 5.12 (Sylvester)

Soient $A, B \in M_n(\mathbb{R})$ diagonales.

$$A \cong B \Leftrightarrow \mathrm{sign}(A) = \mathrm{sign}(B).$$

Preuve. Soit $\phi : V \times V \to \mathbb{R}$ une forme bilinéaire symétrique pour laquelle $A = M_{\mathcal{B}}(\phi)$ et $B = M_{\mathcal{B}'}(\phi)$ où $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{B}' = (e'_1, \dots, e'_n)$ sont des bases ordonnées de V. On peut supposer que $A = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ et $B = \mathrm{diag}(\mu_1, \dots, \mu_n)$ avec

$$\begin{aligned} &\lambda_i > 0 \text{ pour } 1 \leq i \leq r \\ &\lambda_i < 0 \text{ pour } r+1 \leq i \leq r+s \\ &\lambda_i = 0 \text{ si } i > r+s \\ &\mu_i > 0 \text{ pour } 1 \leq i \leq r' \\ &\mu_i < 0 \text{ pour } r'+1 \leq i \leq r'+s' \\ &\mu_i = 0 \text{ si } i > r'+s'. \end{aligned}$$

Alors $\mathrm{sign}(A) = r - s$ et $\mathrm{sign}(B) = r' - s'$. Évidemment $\mathrm{rang}(A) = r + s$ et $\mathrm{rang}(B) = r' + s'$. Comme $A \cong B$, à fortiori $A \sim B$, donc $\mathrm{rang}(A) = \mathrm{rang}(B)$, i. e. : $r + s = r' + s'$.

Pour prouver que $\mathrm{sign}(A) = \mathrm{sign}(B)$ il suffit de prouver que $r = r'$. Définissons $W = \mathrm{vect}(e_1, \dots, e_r)$ et $W' = \mathrm{vect}(e'_{r+1}, \dots, e'_n)$, alors :

$$\dim W = r \quad \text{et} \quad \dim W' = n - r'.$$

Soit $x \in W \cap W'$, alors $x = \sum_{i=1}^{r} x^i e_i = \sum_{j=r'+1}^{n} y^j$, et donc :

$$\phi(x, x) = \sum_{i=1}^{r} \underbrace{\lambda_i (x^i)^2}_{\geq 0, \text{ avec ``$=$'' ssi } x^i = 0} = \sum_{j=r'+1}^{n} \underbrace{\mu_j (y^j)^2}_{\leq 0, \text{ car } y^j \in \mathbb{R},\, \mu_j < 0}$$

donc $x = 0$. Et $W \cap W' = \{0\}$, ainsi $\dim W + \dim W' \leq \dim V$ i. e.

$$r + (n - r') \leq n.$$

D'où $r \leq r'$.

Par un raisonnement analogue, en échangeant r et r', dans les matrices on obtient $r' \leq r$, donc finalement :

$$r = r'$$

$\square$

Definition 8

Soit $A \in M_n(\mathbb{R})$, $A = A^t$. On appelle *signature de* A, $\operatorname{sign}(A)$, la signature de n'importe quelle matrice diagonale congruente à A.

Lemme 5.13

Soit $A = A^t \in M_n(\mathbb{R})$. Si $r = \frac{\operatorname{rang}(A)+\operatorname{sign}(A)}{2}$ et $s = \frac{\operatorname{rang}(A)-\operatorname{sign}(A)}{2}$, alors :

$$A \cong \operatorname{diag}(\underbrace{1,\ldots,1}_{r},\underbrace{-1,\ldots,-1}_{s},0,\ldots,0).$$

Preuve. Soit $D = \operatorname{diag}(\lambda_1,\ldots,\lambda_n)$ congruente à A. On a $\operatorname{rang}(A) = \operatorname{rang}(D)$ et $\operatorname{sign}(A) = \operatorname{sign}(D)$. On sait que r est le nombre des i tels que $\lambda_i > 0$ et s le nombre des i tels que $\lambda_i < 0$. On peut donc supposer que $\lambda_i > 0$ si $1 \leq i \leq r$, $\lambda_i < 0$ si $r+1 \leq i \leq r+s$ et $\lambda_i = 0$ si $i > r+s$.

Alors :

$$\operatorname{diag}(\mu_1,\ldots,\mu_n)D\operatorname{diag}(\mu_1,\ldots,\mu_n) = \operatorname{diag}(\underbrace{1,\ldots,1}_{r},\underbrace{-1,\ldots,-1}_{s},0,\ldots,0),$$

où :

$$\begin{aligned}
&\mu_i = \sqrt{\lambda_i} \quad \text{si } 1 \leq i \leq r\\
&\mu_i = \sqrt{-\lambda_i} \quad \text{si } r+1 \leq i \leq r+s\\
&\mu_i = 1 \quad sii > r+s.
\end{aligned}$$

$\square$

Théorème 5.14

Soient $A, B \in M_n(\mathbb{R})$ symétriques.

$$A \cong B \Leftrightarrow (\operatorname{rang}(A) = \operatorname{rang}(B) \ \underline{\text{et}}\ \operatorname{sign}(A) = \operatorname{sign}(B)).$$

Preuve. $\Rightarrow$ est clair.

$\Leftarrow$ par le Lemme. $\square$

5.2.1 Méthode de Jacobi

Théorème 5.15

Soit $A = A^t \in M_n(\mathbb{K})$. Posons $A_r = A[1, \ldots, r; 1, \ldots, r] \in M_r(\mathbb{K})$ et $\delta_r = \det A_r$. Si $\delta_1, \ldots, \delta_n$ sont tous non nuls, alors il existe une matrice $T \in M_n(\mathbb{K})$ triangulaire unipotente telle que :

$$T^t AT = \operatorname{diag}(\delta_1, \frac{\delta_2}{\delta_1}, \ldots, \frac{\delta_n}{\delta_{n-1}}).$$

Preuve. Par récurrence sur n. Pour $n = 1$ c'est clair. On suppose $n > 1$ et le théorème prouvé pour $n - 1$. On a :

$$A = \left(\begin{array}{c|c} A_{n-1} & * \\ \hline * & a_{nn} \end{array}\right)$$

et A_{n-1} inversible.

On a vu qu'il existe T_0 triangulaire unipotente telle que :

$$T_0^t AT_0 = \left(\begin{array}{c|c} A_{n-1} & 0 \\ \hline * & c \end{array}\right).$$

Comme $\det T_0 = 1$, alors :

$$\delta_n = \det A = \det(T_0^t AT_0) = c \det A_{n-1} = c\delta_{n-1},$$

donc :

$$c = \frac{\delta_n}{\delta_{n-1}}.$$

Par hypothèse de réurrence, il existe $U \in M_{n-1}(\mathbb{K})$ triangulaire unipotente telle que :

$$U^t A_{n-1} U = \operatorname{diag}(\delta_1, \frac{\delta_2}{\delta_1}, \ldots, \frac{\delta_{n-1}}{\delta_{n-2}}).$$

Si on pose $T = T_0 \left(\begin{array}{c|c} U & 0 \\ \hline 0 & 1 \end{array}\right)$, alors :

$$\begin{aligned} T^t AT &= \left(\begin{array}{c|c} U^t A_{n-1} U & 0 \\ \hline 0 & c \end{array}\right) \\ &= \operatorname{diag}(\delta_1, \frac{\delta_2}{\delta_1}, \ldots, \frac{\delta_{n-1}}{\delta_{n-2}}, c) \\ &= \operatorname{diag}(\delta_1, \ldots, \frac{\delta_n}{\delta_{n-1}}). \end{aligned}$$

□

5.2.2 Méthode de Lagrange-Gauss

On travaille sur les formes quadratiques associée ($\mathbb{K}$ un corps de caractéristique différente de 2.)
Soit $Q(x_1, \ldots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j$, $A = A^t = (a_{ij}) \in M_n(\mathbb{K})$.

1[er] cas : On suppose que l'un au moins des a_{ij} est non nul. Disons $a_{11} \neq 0$.

$$\begin{aligned} Q(x_1, \ldots, x_n) &= a_{11}x_1^2 + 2\sum_{i=2}^{n} a_{1i}x_1x_i + \sum_{i,j=2}^{n} a_{ij}x_ix_j \\ &= a_{11}(x_1 + \sum_{i=2}^{n} a_{11}^{-1}a_{1i}x_i)^2 + \underbrace{\sum_{i,j=2}^{n} a_{ij}x_ix_j - a_{11}^{-1}(\sum_{i=2}^{n} a_{1i}x_i)^2}_{Q'(x_2,\ldots,x_n)} \end{aligned}$$

Si on change de variable :

$$\begin{cases} y_1 = x_1 + \sum_{i=2}^{n} a_{11}^{-1}a_{ij}x_i, \\ y_i = x_i \quad \text{si } i = 2, \ldots, n. \end{cases}$$

Alors :

$$Q(x_1, \ldots, x_n) = a_{11}y_1^2 + Q'(y_2, \ldots, y_n).$$

Ensuite on travaille sur Q'.

2[e] cas : $a_{ii} = 0, \ \forall i \in \mathbb{N}_n$.

On choisit un $a_{ij} \neq 0$. Disons $a_{12} \neq 0$ et on fait le changement de variable suivant :

$$\begin{cases} y_1 &= \frac{x_1+x_2}{2} \\ y_2 &= \frac{x_1-x_2}{2} \\ y_i &= x_i \quad \text{pour } i > 2. \end{cases}$$

Alors :

$$Q(x_1, \ldots, x_n) = Q(y_1 + y_2, y_1 - y_2, y_3, \ldots, y_n) = \sum_{i,j=1}^{n} b_{ij}y_iy_j,$$

avec $b_{11} \neq 0$. On est alors ramené au 1[er] cas.

Definition 9

Soit $\phi : V \times V \to \mathbb{R}$ une forme bilinéaire symétrique sur un $\mathbb{R}$-espace vectoriel V. On dit que :

1. ϕ est *(semi-définie positive) non négative* si $\phi(x, x) \geq 0, \forall x \in V \setminus \{0\}$.
2. ϕ est *définie positive* si $\phi(x, x) > 0 \ \forall x \in V \setminus \{0\}$.
3. ϕ est définie *non positive* si $-\phi$ est définie non négative.
4. ϕ est définie *négative* si $-\phi$ est définie positive.

Théorème 5.16

Soit $A = (a_{ij}) = A^t \in M_n(\mathbb{R})$. $A_r = A[1, \ldots, r; 1, \ldots, r]$, $r = 1, \ldots, n$. Alors A est définie positive si et seulement si $\det A_r > 0 \ \forall r = 1, \ldots, n$.

Preuve. $\Leftarrow$: Par la méthode de Jacobi, $A \cong \operatorname{diag}(\delta_1, \frac{\delta_2}{\delta_1}, \ldots, \frac{\delta_n}{\delta_{n-1}})$, avec $\delta_i > 0$, pour $i = 1, \ldots, n$. Ainsi $\operatorname{sign}(A) = \operatorname{rang}(A) = n$ et donc A est définie positive.

$\Rightarrow$: Si A est définie positive, on a $\sum_{i,j=1}^{r} a_{ij}x_ix_j > 0$, $\forall (x_1,\ldots,x_n) \neq (0,\ldots,0)$, pour chaque $r = 1,\ldots,n$.
Ainsi A_r est définie positive pour chaque $r = 1,\ldots,n$, i. e. $\operatorname{sign}(A_r) = r$, ou encore $A_r \cong I_r$.
Pour chaque $r = 1,\ldots,n$ il y a donc $T_r \in \mathrm{GL}_r(\mathbb{R})$ telle que $A_r = T_r^t I_r T_r$. D'où :

$$\det A_r = \det(T_r^t)\det(T_r) = (\det T_r)^2 > 0.$$

□

Definition 10

Soit $A = A^t = (a_{ij}) \in M_n(\mathbb{R})$. On dit que A est définie *non négative* (resp. positive, non positive, négative) si la forme bilinéaire symétrique $\phi : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ définie par $\phi((x_1,\ldots,x_n);(y_1,\ldots,y_n)) = \sum_{i,j=1}^{n} a_{ij}x_iy_j$ a cette propriété.

Remarque 3

Si $\phi : V \times V \to \mathbb{R}$ est une forme bilinéaire symétrique su un $\mathbb{R}$-espace vectoriel V de dimension finie n, si $\mathcal{B}$ est une base ordonnée de V et si $A = M_{\mathcal{B}}(\phi)$, il est clair que ϕ est définie on négative (resp. positive, non positive, négative) si et seulement si A l'est.

Remarque 4

Si $A = A^t \in M_n(\mathbb{R})$, on a :

$$\begin{aligned}
&A \text{ est définie non négative} \Leftrightarrow \operatorname{sign}(A) = \operatorname{rang}(A)\\
&A \text{ est définie positive} \Leftrightarrow \operatorname{sign}(A) = n\\
&A \text{ est définie non positive} \Leftrightarrow \operatorname{sign}(A) = -\operatorname{rang}(A)\\
&A \text{ est définie négative} \Leftrightarrow \operatorname{sign}(A) = -n.
\end{aligned}$$

Théorème 5.17

Soit $A = A^t \in M_n(\mathbb{R})$. Alors A est définie non négative si et seulement si on a :

$$\det A[i_1,\ldots,i_r; i_1,\ldots,i_r] \geq 0,$$

pour toutes les suites $1 \leq i_1 < i_2 < \cdots < i_r \leq n$.

Preuve. cf. ex. 9 série 23–24. □

5.3 Formes sesquilinéaires et hermitiennes

Definition 11

Soit V un $\mathbb{C}$-espace vectoriel. On appelle *forme sesquilinéaire sur V* toute application $\phi : V \times V \to \mathbb{C}$ telle que :

1. $\phi(x_1 + x_2, y) = \phi(x_1, y) + \phi(x_2, y) \quad \forall x_y, x_2, y \in V$,
2. $\phi(x, y_1 + y_2) = \phi(x, y_1) + \phi(x, y_2) \quad \forall x, y_1, y_2 \in V$,
3. $\phi(x, \lambda y) = \lambda\phi(x, y) \quad \forall x, y \in V, \forall \lambda \in \mathbb{C}$,
4. $\phi(\lambda x, y) = \bar{\lambda}\phi(x, y) \quad \forall x, y \in V, \forall \lambda \in \mathbb{C}$.

Soit $\phi : V \times V \to \mathbb{C}$ une forme sesquilinéaire, alors si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base ordonnée de V, on appelle *matrice de ϕ relativement à $\mathcal{B}$* la matrice $M_{\mathcal{B}} = (\phi(e_i, e_j))$.

Si $A = (a_{ij}) = M_{\mathcal{B}}(\phi)$, on a :

$$\begin{aligned} \phi(\sum_{i=1}^{n} x^i e_i, \sum_{j=1}^{n} y^j e_i) &= \sum_{i,j=1}^{n} a_{ij} \bar{x}^i y^j \\ &= \bar{X}^t A Y = X^* A Y, \end{aligned}$$

où on a utilisé la notation $M^* = \bar{M}^t$, si $M \in M_{p\times q}(\mathbb{C})$ et avec :

$$X = \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix}, \quad Y = \begin{pmatrix} y^1 \\ \vdots \\ y^n \end{pmatrix}.$$

L'application $\phi \mapsto M_{\mathcal{B}}(\phi)$ est une bijection de l'ensemble des formes sesquilinéaires sur V sur $M_n(\mathbb{C})$.

Definition 12

$A, B \in M_n(\mathbb{C})$, sont dites *semi-congruentes* s'il existe $T \in \mathrm{GL}_n(\mathbb{C})$ telle que :

$$B = T^* A T.$$

Théorème 5.18

$A, B \in M_n(\mathbb{C})$ représentent une même forme sesquilinéaire si et seulement si elles sont semi-congruentes.

Definition 13

Une forme sesquilinéaire $\phi : V \times V \to \mathbb{C}$ est dite *hermitienne* si elle a la propriété de symétrie suivante :

$$\phi(x, y) = \overline{\phi(y, x)}.$$

Si $\mathcal{B}$ est une base ordonnée de V et $A = M_{\mathcal{B}}(\phi)$, alors ϕ est hermitienne si et seulement si $A = A^*$, on dit que A est une matrice *hermitienne*.

Théorème 5.19

Toute matrice hermitienne $A = A^* \in M_n(\mathbb{C})$ est semi-congruente à une matrice diagonale réelle.

On définit alors la signature d'une matrice hermitienne de manière analogue au cas des matrices symétriques réelles et on démontre :

Théorème 5.20

Soit $A, B \in M_n(\mathbb{C})$ hermitienne. Alors A et B sont semi-congruentes si et seulement si :

$$\mathrm{rang}(A) = \mathrm{rang}(B) \quad \underline{\text{et}} \quad \mathrm{sign}(A) = \mathrm{sign}(B).$$

Chapitre 6

Espaces Unitaires

6.1 Orthogonalité

Notations $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Si $\lambda \in \mathbb{K}$, on pose :

$$|\lambda| = \begin{cases} \text{valeur absolue de } \lambda \text{ si } \mathbb{K} = \mathbb{R} \\ \text{module de } \lambda \text{ si } \mathbb{K} = \mathbb{C} \end{cases}$$

$$\bar{\lambda} = \begin{cases} \lambda \text{ si } \mathbb{K} = \mathbb{R} \\ \bar{\lambda} \text{ si } \mathbb{K} = \mathbb{C}. \end{cases}$$

Si $A \in M_{n\times m}(\mathbb{K})$:

$$\bar{A} = \begin{cases} A \text{ si } \mathbb{K} = \mathbb{R} \\ \bar{A} \text{ si } \mathbb{K} = \mathbb{C} \end{cases}$$

$$A *^{=} \bar{A}^t = \begin{cases} A^t \text{ si } \mathbb{K} = \mathbb{R} \\ \bar{A}^t = A* \text{ si } \mathbb{K} = \mathbb{C}. \end{cases}$$

Definition 1

On appelle *espace unitaire réel (resp. complexe)* un espace vectoriel réel (resp. complexe) V muni d'une forme bilinéaire symétrique (resp. hermitienne) définie positive. Cette forme sera notée $(x, y) \mapsto (x|y)$ et baptisée *la produit scalaire* de l'espace unitaire considéré.

Rappel

Dire que $(\cdot|\cdot) : V \times V \to \mathbb{K}$ est une forme bilinéaire symétrique (resp. hermitienne) définie positive signifie que

1. $(x|y_1 + y_2) = (x|y_1) + (x|y_2)$ $\forall x, y_1, y_2 \in V$.
2. $(x|\lambda y) = \lambda(x|y)$ $\forall x, y \in V$, $\forall \lambda \in \mathbb{K}$
3. $(x|y) = \overline{(y|x)}$ $\forall x, y \in V$
4. $(x|x) > 0$ $\forall x \in V$, $x \neq 0$.

Exemple 1

Dans $V = \mathbb{K}^n$ si $x = (x_1, \ldots, x_n) \in V$ et $y = (y_1, \ldots, y_n) \in V$, alors on peut définir :

$$(x|y) = \sum_{i=1}^{n} \bar{x}_i y_i.$$

Exemple 2

Dans $V = \mathcal{C}(I, \mathbb{K})$, l'ensemble de toutes les applications continues d'un intervalle I fermé borné dans $\mathbb{K}$, on peut définir :

$$(f|g) = \int_I \bar{f}(x) g(x)\, dx, \qquad \text{pour } f, g \in V.$$

Remarques terminologiques On trouve aussi les appelations suivantes :

— espace préhilbertien, pour les espaces unitaires,
— espace euclidien, pour les espaces unitaires réels de dimension finie,
— espace hermitien, pour les espaces unitaires complexes de dimension finie.

Definition 2

Si V est un espace unitaire, on appelle *norme de* $x \in V$ et on note $\|x\|$ la racine carré réelle positive de $(x|x)$.

C'est à dire $\|x\| \geq 0$ et $\|x\|^2 = (x|x)$.

Clairement on a :

$$\|x\| = 0 \Leftrightarrow x = 0$$
$$\|\lambda x\| = |\lambda| \|x\| \quad \forall \lambda \in \mathbb{K} \text{ et } \forall x \in V.$$

Remarque 1

$x \mapsto \|x\|^2$ est simplement la forme quadratique associée au produit scalaire. En particulier, on a les *identités de polarisation* :

$$(x|y) = \frac{1}{4}(\|x+y\|^2 - \|x-y\|^2) \quad \text{si } \mathbb{K} = \mathbb{R}$$
$$(x|y) = \frac{1}{4}(\|x+y\|^2 - \|x-y\|^2) + i\frac{1}{4}(\|ix+y\|^2 - \|ix-y\|^2) \quad \text{si } \mathbb{K} = \mathbb{C}.$$

Théorème 6.1 (Inégalité de Cauchy-Schwarz)

Si V est un espace unitaire, alors pour tout $x, y \in V$ on a :

$$|(x|y)| \leq \|x\|\|y\|.$$

Il y a égalité si et seulement si x et y sont linéairement dépendants.

Preuve. Si x et y sont dépendants, alors :

— si $x = 0$, alors : $(x|y) = 0$ et $\|x\|\|y\| = 0$, donc $(x|y) = \|x\|\|y\|$.

— si $x \neq 0$, alors $\exists \lambda \in \mathbb{K}$ tel que $y = \lambda x$. On a alors $(x|y) = (x|\lambda x) = \lambda(x,x) = \lambda\|x\|^2$. Ainsi :

$$\begin{aligned} |(x|y)| &= |\lambda|\|x\|^2 = \|x\|(|\lambda|\|x\|) \\ &= \|x\|\|\lambda x\| = \|x\|\|y\|. \end{aligned}$$

Si x et y sont linéairement indépendants, en particulier $y \neq 0$, donc on peut définir

$$\lambda_0 = \frac{\overline{(x|y)}}{\|y\|^2}.$$

Comme $x - \lambda_0 y \neq 0$, on a $0 < \|x - \lambda_0 y\|^2$, ainsi :

$$\begin{aligned} 0 < \|x - \lambda_o y\|^2 &= (x - \lambda_0 y | x - \lambda_0 y) = (x|x) - \bar{\lambda}_0 (y|x) - \lambda_0 (x|y) + \lambda_0 \bar{\lambda}_0 (y|y) \\ &= \|x\|^2 - \bar{\lambda}_0 \overline{(x|y)} - \lambda_0 (x|y) + |\lambda_0|^2 \|y\|^2 \\ &= \|x\|^2 - \frac{(x|y)\overline{(x|y)}}{\|y\|^2} - \frac{(x|y)\overline{(x|y)}}{\|y\|^2} + \frac{(x|y)\overline{(x|y)}}{\|y\|^2} \\ &= \|x\|^2 - \frac{|(x|y)|^2}{\|y\|^2}. \end{aligned}$$

Multipliant par $\|y\|^2$, il vient :

$$0 < \|x\|^2\|y\|^2 - |(x|y)|^2,$$

i. e. :

$$|(x|y)|^2 < \|x\|^2\|y\|^2,$$

d'où (puisque $|\cdot| > 0$ et $\|\cdot\| > 0$) :

$$|(x|y)| < \|x\|\|y\|.$$

$\square$

Corollaire 6.2 (Inégalité triangulaire)

Si V est un espace unitaire, alors $\forall x, y \in V$:

$$\|x + y\| \leq \|x\| + \|y\|.$$

Preuve.

$$\begin{aligned} \|x+y\|^2 &= (x+y|x+y) = (x|x) + (x|y) + (y|x) + (y|y) \\ &= \|x\|^2 + 2\Re(x|y) + \|y\|^2 \quad (*) \\ &\leq \|x\|^2 + 2|(x|y)| + \|y\|^2 \\ &\leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2. \end{aligned}$$

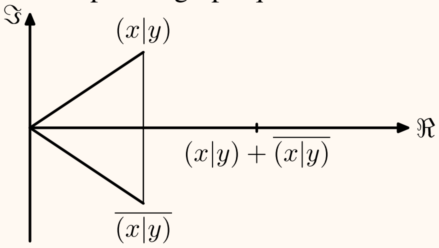
$\square$

Remarque 2

Dans $(*)$ on a utilisé le fait que

$$(x|y) + \overline{(x|y)} = 2\Re(x|y) + i[\Im(x|y) - \Im(x|y)] = 2\Re(x|y).$$

Cette égalité se comprend aisément d'après le graphique suivant



Definition 3

Si V est un espace unitaire et $x, y \in V$, on définit la *distance de x à y* par :

$$d(x, y) = \|x - y\|.$$

Proposition 6.3

1. $d(x, y) \geq 0$ et $d(x, y) = 0 \Leftrightarrow x = y$.
2. $d(x, y) = d(y, x), \ \forall x, y \in V$.
3. $d(x, y) \leq d(x, z) + d(z, y), \ \forall x, y, z \in V$.
4. $d(x, y) = d(x + z, y + z), \ \forall x, y, z \in V$.
5. $d(\lambda x, \lambda y) = |\lambda| d(x, y)$.

Definition 4

Soit V un espace unitaire.

— Si $x \in V$ et $A \subset V$, $A \neq \emptyset$, alors :

$$d(x, A) = \inf\{d(x, y) | y \in A\}.$$

— Si $A, B \subset V$, non vides :

$$d(A, B) = \inf\{d(x, y) | x \in A, \ y \in B\}.$$

Si V est un espace unitaire et $x, y \in V$ non nuls, par Cauchy-Schwarz :

$$0 \leq \frac{|(x|y)|}{\|x\|\|y\|} \leq 1.$$

On peut donc définir :

Definition 5

Soit V un espace unitaire et $x, y \in V$, non nuls. On définit *l'angle entre* $\mathbb{K}x$ *et* $\mathbb{K}y$ comme l'unique α tel que :

$$\cos\alpha = \frac{|(x|y)|}{\|x\|\|y\|}, \quad \text{et } 0 \leq \alpha \leq \frac{\pi}{2}.$$

Lorsque $\mathbb{K} = \mathbb{R}$ on peut faire mieux et définir l'angle entre $\mathbb{R}_+x$ et $\mathbb{R}_+y$ comme étant l'unique α tel que :

$$\cos\alpha = \frac{(x|y)}{\|x\|\,\|y\|}, \quad \text{et : } 0 \leq \alpha \leq \pi.$$

Remarque 3

Si toute suite de Cauchy converge dans un espace vectoriel V, alors V est dit *complet* et si V est un espace vectoriel unitaire complet, on l'appelle *espace de Hilbert*.

Definition 6

Soit V un espace unitaire. On dit que $x, y \in V$ sont *orthogonaux*, $x \perp y$, si $(x|y) = 0$.

Si W est un sous-espace de V, on définit $W^\perp$ par :

$$W^\perp = \{x \in V | x \perp y, \ \forall\, y \in W\}.$$

Proposition 6.4

1. $\{0\}^\perp = V$, et $V^\perp = \{0\}$.
2. $W^\perp$ est un sous-espace vectoriel de V et $W \cap W^\perp = \{0\}$.
3. $W \subset (W^\perp)^\perp$.
4. $(W_1 + W_2)^\perp = W_1^\perp + W_2^\perp$.
5. $W_1 \subset W_2 \Rightarrow W_2^\perp \subset W_1^\perp$.
6. Si $W = \mathrm{vect}(S)$, $W^\perp = \{x \in V | x \perp s, \ \forall\, s \in S\}$.

Lemme 6.5

Soit V un espace unitaire et $x_1, x_2, \ldots$ une suite finie ou non de vecteurs non nuls tels que $(x_i|x_j) = 0$ toutes les fois que $i \neq j$.

Alors $x_1, x_2, \ldots$ sont linéairement indépendants.

Preuve. Si $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ sont tels que :

$$\sum_{i=1}^{n} \lambda_i x_i = 0,$$

on a pour $j = 1, \ldots, n$:

$$0 = (x_j | \sum_{i=1}^{n} \lambda_i x_i) = \sum_{i=1}^{n} \lambda_i (x_i | x_j) = \lambda_j \|x_j\|^2$$

d'où, puisque $x_j \neq 0$: $\lambda_j = 0$. □

Definition 7

Une suite $x_1, x_2, \ldots$, finie ou non, est dite *orthonormée* si $(x_i|x_j) = 0$ toutes les fois que $i \neq j$ et si $\|x_i\| = 1$ pour tout i.

Théorème 6.6 (Procédé d'orthonormalisation de Gram-Schmidt)

Soit V un espace unitaire, $x_1, x_2, \ldots$, une suite finie ou non de vecteurs linéairement indépendants. Alors il existe une unique suite orthonormée $y_1, y_2, \ldots$ telle que :

1. $\text{vect}(x_1, \ldots, x_k) = \text{vect}(y_1, \ldots, y_k)$ pour tout k,
2. $(x_i, y_i) \in \mathbb{R}_+^*$ pour tout i.

Preuve. On construit les y_i par récurrence sur i. D'abord :

$$y_1 = \frac{x_1}{\|x_1\|}.$$

Supposons les y_i déjà construits pour $i = 1, 2, \ldots, k$. On construit le vecteur y_{k+1} de la façon suivante. On définit :

$$y'_{k+1} = x_{k+1} - \sum_{i=1}^{k} (y_i | x_{k+1}) y_i,$$

et on pose :

$$y_{k+1} = \frac{y'_{k+1}}{\|y'_{k+1}\|}.$$

Le fait que les y_i ainsi construits satisfont l'énoncé du théorème est une vérification facile laissée en exercice. □

Corollaire 6.7

Tout espace unitaire V de dimension finie admet une base orthonormée.

Preuve. Soit $x_1, \ldots, x_n$ une base ordonnée de V. Le procédé de Gram-Schmidt appliqué à cette suite fournit des vecteurs $y_1, \ldots, y_n$ orthonormés qui constituent donc une base orthonormée de V. □

Théorème 6.8 (Pythagore)

Soit V un espace unitaire et $x, y \in V$. Alors :

$$(x|y) = 0 \Rightarrow \|x - y\|^2 = \|x\|^2 + \|y\|^2.$$

Preuve. En effet :

$$\|x - y\|^2 = (x - y|x - y) = \|x\|^2 + \|y\|^2 - (x|y) - \overline{(x|y)} = \|x\|^2 + \|y\|^2.$$

□

Remarque 4

Si le corps de base est $\mathbb{R}$ on a $\Leftrightarrow$ au lieu de $\Rightarrow$.

Théorème 6.9

Soit W un sous-espace d'un espace unitaire V et $x \in V$. Pour $y \in W$ les deux conditions suivantes sont équivalentes :

1. $x - y \in W^{\perp}$.
2. $d(x, y) = d(x, W)$.

En outre, pour x donné, il existe au plus un seul $y \in W$ ayant ces propriétés.

6.2 Adjonction

6.3 Endomorphismes unitaires, autoadjoints, normaux