Algèbre Linéaire Avancée (1er Semestre)[1]

Philippe Michel

[1]Sunday 10$^{\text{th}}$ January, 2021, 18:30

Table des matieres

Introduction

Le terme "Algebre" est derive du mot arabe *al-jabr* qui est tire du titre d'un ouvrage du mathematicien persan *Al-Khwarizmi*, redige vers 825 (source wikipedia) et intitule

Kitab al-mukhtasar fi hisab al-jabr wa-l-muqabala

Abrege du calcul par la restauration et la comparaison.

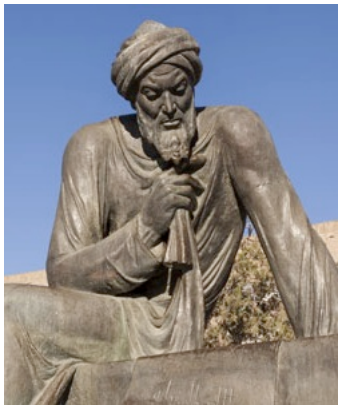
L'ouvrage fournissait des procedures generales de calcul pour resoudre des problemes pratiques lies aux actes legaux (partage lors d'un heritage, subdivision de terrains et calculs d'aires) qui conduisaient a resoudre des equations lineaires ou quadratiques. Le nom "Al-Khwarizmi" a d'ailleurs donne naissance au mot "Algorithme".

De nos jours le terme "Algebre" designe plutot l'etude et la classification de structures mathematiques formelles liees aux operations. l'*Algebre Lineaire* se concentre plus particulierement sur l'etude des "espaces vectoriels". Cependant avant d'arriver a cette notion, nous auront besoin d'introduire d'autre structures algebrique plus generales,

- Les "groupes",
- les "anneaux"
- et les "corps" (qui sont des anneaux particuliers) ainsi que
- les "modules" sur les anneaux, les espaces vectoriels sont des modules sur des corps.

L'etude des premiers releve de la "theorie des groupes" (qui sera developpee plus en details dans le cours MATH-113) et celle des trois au tres releve de "l'algebre commutative" (qui sera discutee en deuxieme annee) cependant, comme on va le voir, tous ces sujets sont intimement connectes et il est impossible de traiter l'un de ces sujets sans avoir recours aux autres.

Avant cela nous aurons besoin d' introduire le language des *ensembles*.



CHAPITRE 1

Le language des ensembles

Quelques abbreviations:

$\exists$: "il existe"; $\forall$: "quelque soit" ou bien "pour tout";

$\Longrightarrow$: "implique"; $\Longleftrightarrow$ ou ssi : "equivaut a, si et seulement si"; $|$ ou $t.q.$: "tel que"

$\wedge$: "et", $\vee$: "ou"

$A := B$: "l'objet A est defini par B", $A =: B$: "l'objet B est defini par A",

$spdg,\ wlog$: "sans perte de generalite " ou "without loss of generality"

ops, wma : "on peut supposer " ou "we may assume"

$spdgops,\ wlogwma : \cdots$

1.1. Ensembles

Une definition rigoureuse de la notion d'ensemble et des ensembles de base (comme les entiers naturels) necessiterait au prealable d'introduire de developper *le calcul des predicats du premier ordre* puis une *theorie des ensembles* munie d'une *axiomatique* convenable (la plupart du temps ZF ou ZFC). Comme il ne s'agit pas du sujet du cours, nous ne le ferons pas et nous en remettons a l'intuition du lecteur. Pour un traitement plus complet, nous referons le lecteur au debut du cours "Structures Algebriques" MATH-113 et plus tard au cours de "logique mathematique" MATH-381.

1.1.1. Un *ensemble* E est une collection d'objets appeles elements de E. Si e est un element de E (e appartient a E), on note cette relation

$$e \in E.$$

Exemple 1.1.1. Quelques ensembles

- Il existe un (unique) ensemble ne contenant aucun elements:*l'ensemble vide* que l'on notera
$$\emptyset.$$
- $\mathbb{N}$ est l'ensemble des entiers naturels:
$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$
- $\mathbb{Z}$ est l'ensemble des entiers relatifs:
$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}.$$
- $\mathbb{Q}$ est l'ensemble des nombres rationels:
$$\mathbb{Q} = \{\frac{p}{q},\ p, q \in \mathbb{Z},\ q \neq 0\}.$$
- $\mathbb{R}$ designera l'ensemble des nombres *reels*. Cet ensemble sera construit rigoureusement dans le cours d'analyse.

– $\mathbb{C}$ designera l'ensemble des nombres *complexes*. Cet ensemble sera construit rigoureusement dans le cours (en admettant l'existence de $\mathbb{R}$).

On designera un ensemble et les elements qu'il contient par la notation "crochets":

$$E = \{\cdots\}.$$

Entre ces crochets $\{\cdots\}$ on mettra soit

– La liste des elements de l'ensembles (si c'est possible) separes par des virgules: on enumere les elements de l'ensemble.
– une formule indiquant qu'on considere les element d'un autre ensemble (disons F) qui verifient une certaine propriete P codee par une formule logique:
  – $\{0,1,2,3\} = \{m \in \mathbb{N},\ m \leqslant 3\}$.
  – $\mathbb{N} = \mathbb{Z}_{\geqslant 0} = \{m \in \mathbb{Z},\ m \geqslant 0\}$.
  – $\mathcal{P} =$ Ensemble des nombres premiers $= \{p \in \mathbb{N},\ d|p \Longrightarrow d = 1 \text{ ou } p\}$.
  – Soit E-EPFL l'ensemble des etudiants de l'EPFL.

$$A := \{e \in \text{E-EPFL},\ 3|\text{SCIPER}(e)\},$$

$$B := \{e \in \text{E-EPFL},\ 3|\text{SCIPER}(e) - 1\},$$

$$C := \{e \in \text{E-EPFL},\ 3|\text{SCIPER}(e) - 2\}.$$

1.1.2. Sous-ensemble. Etant donne un ensemble E, un *sous-ensemble* de E est un ensemble A tel que tout element de A est contenu dans E: on note cette relation

$$A \subset E.$$

On dit egalement que A est *contenu* (*inclu*) dans E ou que A est une *partie* de E. Si $e \in E$ est un element de E, on note

$$\{e\} \subset E$$

le sous-ensemble de E dont l'unique element est e (le *singleton* e).

Par exemple, on a la chaine d'inclusions

$$\{1\} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Si A n'est pas contenu dans E, on le notera

$$A \not\subset E.$$

Notons que l'ensemble vide est un sous-ensemble de tout ensemble E:

$$\emptyset \subset E.$$

Deux ensemble sont *egaux* si ils ont les *memes* elements. On a donc l'equivalence

$$E = F \Longleftrightarrow E \subset F \text{ et } F \subset E.$$

En d'autre termes pour montrer que deux ensemble sont egaux il faut et il suffit de montrer que l'un est inclu dans l'autre et l'autre dans le premier: c'est la methode de la *double-inclusion*.

L'ensemble des sous-ensembles de E est note

$$\mathscr{P}(E) = \{A \text{ ensemble},\ A \subset E\}.$$

REMARQUE 1.1.1. *L'ensemble de tous les ensembles* ENS n'est PAS un ensemble: en effet si c'etait le cas, on pourrait considerer (Russell) l'ensemble de tous les ensembles *ne se contenant pas eux-meme*

$$\text{Ncont} = \{E \text{ ensemble},\ E \notin E\}$$

et se poser la question de savoir si

$$\text{Ncont} \in \text{Ncont ou bien Ncont} \notin \text{Ncont}.$$

Pour resoudre ce probleme, on est amene a introduire une notion plus souple que celle d'ensemble appelle *categorie*: l'ensemble de tous les ensembles ENS forme une categorie.

1.2. Operations sur les ensembles

1.2.1. Union, intersection. On defini les operations suivante sur l'ensemble $\mathscr{P}(E)$ des parties d'un ensemble: soient $A, B \subset E$

- la reunion de A et B,

$$A \cup B = \{e \in E | e \in A \text{ ou } e \in B\} \subset E.$$

- l'intersection de A et B,

$$A \cap B = \{e \in E | e \in A \text{ et } e \in B\} \subset E.$$

- la difference de A et B,

$$A - B = A \backslash B = \{a \in A | a \notin B\} \subset E.$$

  En particulier, la difference

$$E - A = \{e \in E,\ e \notin A\} := A^c$$

  s'appelle le complementaire de A dans E.
- la difference symetrique de A et B,

$$A \Delta B = A \backslash B \cup B \backslash A \subset E.$$

- Si $A \cap B = \emptyset$, on dit que A et B sont disjoints.

Plus generalement si on dispose de $n \geqslant 2$ sous-ensembles $E_1, \cdots, E_n \subset E$ on note

$$\bigcap_{i=1}^{n} E_i = E_1 \cup \cdots \cup E_n = E_1 \cup (E_2 \cup \cdots \cup E_n) = \{e \in E | \text{ il existe } i \leqslant n,\ e \in E_i\},$$

$$\bigcup_{i=1}^{n} E_i = E_1 \cap \cdots \cap E_n = E_1 \cap (E_2 \cap \cdots \cap E_n) = \{e \in E | \text{ pour tout } i \leqslant n,\ e \in E_i\}.$$

EXERCICE 1.1. Montrer que

$$A \Delta B = A \cup B - A \cap B.$$

1.2.2. Produit cartesien. Etant donne deux ensemble A, B leur *produit cartesien* $A \times B$ est l'ensemble des *couples ordonnes* (a, b) avec a un element de A et b un element de B:

$$A \times B = \{(a, b),\ a \in A, b \in B\}.$$

Si un des facteurs est l'ensemble vide le produit cartesien est vide: on a

$$\emptyset \times B = A \times \emptyset = \emptyset.$$

REMARQUE 1.2.1. Noter que les ensembles $A \times B$ et $B \times A$ sont distincts sauf si $A = B$ ou A ou B est l'ensemble vide. Si $A = B \neq \emptyset$ et $a \neq a'$, on a

$$(a, a') \neq (a', a).$$

Si on dispose de n ensembles $A_1, \cdots, A_n$ le produit

$$A_1 \times \cdots \times A_n$$

est l'ensemble des n-uples (ordonnes)

$$(a_1, \cdots, a_n),\ a_1 \in A_1, \cdots a_n \in A_n.$$

Si $A_1 = \cdots = A_n = A$ on note ce produit A^n.

1.2.2.1. *Relation binaire.* Une *relation* (binaire) $\mathcal{R}$ entre (les elements de) deux ensembles A, B est un sous-ensemble

$$\mathcal{R} \subset A \times B.$$

On dit alors que a, b sont *lies par la relation* $\mathcal{R}$ si

$$(a, b) \in \mathcal{R}$$

ce que l'on ecrit

$$a \sim_{\mathcal{R}} b \text{ ou bien } a\mathcal{R}b.$$

Si le sous-ensemble $\mathcal{R}$ a des proprietes supplementaires on dira que la relation a certaines proprietes.

Par exemple si $B = A$ on a les definitions suivantes: soit $\mathcal{R} \subset A \times A$ une relation de A sur lui-meme

- $\mathcal{R}$ est reflexive si
$$\forall a \in A, a\mathcal{R}a$$
(cad $(a, a) \in \mathcal{R}$). En d'autre termes $\Delta A \subset \mathcal{R}$ ou $\Delta A = \{(a, a),\ a \in A\}$ est la diagonale de A.
- $\mathcal{R}$ est symetrique si
$$\forall a, a' \in A,\ a\mathcal{R}a' \Longleftrightarrow a'\mathcal{R}a.$$
En d'autre termes $\mathcal{R}$ est invariant par la symetrie par rapport a la diagonale ΔA
$$s_\Delta : (a, a') \in A \times A \mapsto (a', a) \in A \times A$$
, c'est a dire
$$s_\Delta(\mathcal{R}) = \mathcal{R}.$$
- $\mathcal{R}$ est transitive si
$$\forall a, a', a'' \in A,\ a\mathcal{R}a' \text{ et } a'\mathcal{R}a'' \Longrightarrow a\mathcal{R}a''.$$
- $\mathcal{R}$ est une relation d'equivalence si elle est reflexive, symetrique et transitive.

1.3. Applications entre ensembles

Soient X et Y des ensembles. Une application (egalement fonction) f de X (l'espace de depart) vers Y (l'espace d'arrivee) est la donnee pour tout $x \in X$ d'un unique element $f(x) \in Y$; l'element $f(x)$ est *l'image* de x par f. Une application est notee

$$f : X \mapsto Y.$$

1.3.1. Graphe d'une application. On peut donner a la notion d'application une definition purement ensembliste a l'aide du produit cartesien. Se donner une application

$$f : X \mapsto Y$$

est equivalent a se donner un sous-ensemble

$$\Gamma \subset X \times Y$$

qu'on appelle un *graphe*:

DÉFINITION 1.1. *Un graphe $\Gamma \subset X \times Y$ est un sous-ensemble de $X \times Y$ tel que pour tout $x \in X$, l'ensemble des elements de Γ de la forme (x, y) (ie. dont la premiere coordonnee vaut x) possede exactement un element.*

Si $f : X \mapsto Y$ est une application, le graphe associe a f est le sous ensemble

$$\Gamma_f = \{(x, f(x)),\ x \in X\} \subset X \times Y.$$

Reciproquement si $\Gamma \subset X \times Y$ est un graphe, on lui associe l'application $f_\Gamma : X \mapsto Y$ qui a $x \in X$ associe $f(x) = y$ ou y est l'unique element de Y tel que

$$(x, y) \in \Gamma.$$

Cette realisation des ensembles en terme de graphes permet de dire que l'ensemble des applications entre X et Y est un ensemble et plus precisement un sous ensemble de $\mathscr{P}(X \times Y)$ (on l'identifie avec le sous-ensemble de tous les graphes dans $X \times Y$).

NOTATION 1.1. *On note*

$$\mathrm{Hom}_{ENS}(X, Y) \text{ ou encore } \mathcal{F}(X, Y) \text{ ou encore } Y^X$$

l'ensemble des applications de X vers Y (aussi les fonctions de X a valeurs dans Y).

1.3.1.1. *Exemples.* Soit $y \in Y$, application constante de valeur y est l'application

$$\underline{y} : x \in X \mapsto y \in Y.$$

Son graphe est

$$\Gamma(\underline{y}) = \{(x, y),\ x \in X\} \subset X \times Y.$$

Quand $X = Y$, une autre application importante est *l'identite* de X: c' est l'application

$$\mathrm{Id}_X : x \in X \mapsto x \in X.$$

Son graphe est

$$\Gamma(\mathrm{Id}_X) = \Delta(X) = \{(x, x),\ x \in X\} \subset X \times X$$

et s'appelle la diagonale de $X \times X$.

Soit $X = Y = \{1, 2, 3, 4\}$ et posont

$$f_1 : 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 2,\ 4 \mapsto 1$$
$$f_2 : 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 4,\ 4 \mapsto 1$$
$$f_3 : 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 4,\ 4 \mapsto 1.$$

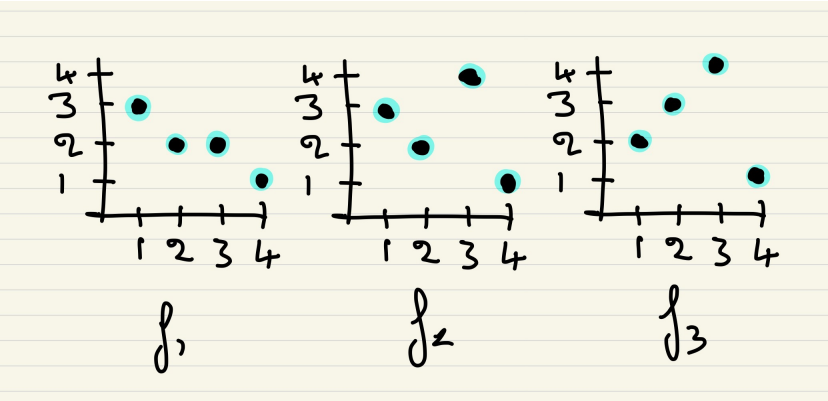


FIGURE 1. Graphes de f_1, f_2, f_3.

Les graphes de ces applications sont donnees par les dessins ci-dessus.

Projection. Soit $A_1, \cdots A_n$ des ensemble et

$$\prod_{i=1}^{n} A_i$$

leur produit cartesien. Pour $i = 1, \cdots, n$ la *projection sur le i-eme facteur* est l'application

$$\pi_i : \begin{array}{ccc} \prod_{i=1}^n A_i & \mapsto & A_i \\ (a_1, \cdots, a_n) & \mapsto & a_i \end{array}$$

qui a un n-uple associe la i-eme coordonnee.

1.3.2. Image, preimage. Une application

$$f : X \mapsto Y$$

induit naturellement deux applications entre les ensembles des parties de X et Y:

– L'image

$$\mathrm{Im}(f) : \mathscr{P}(X) \mapsto \mathscr{P}(Y)$$

qui a un sous-ensemble $A \subset X$ associe son image:

$$\mathrm{Im}(f)(A) = \{f(x),\ x \in A\} \subset Y.$$

On notera plus simplement l'image par

$$f(A) = \mathrm{Im}(f)(A).$$

On notera egalement

$$\mathrm{Im}(f) = \mathrm{Im}(f)(X)$$

l'image par f de tout l'ensemble de depart X qu'on appellera l'image de f.

– La preimage

$$\mathrm{preIm}(f) : \mathscr{P}(Y) \mapsto \mathscr{P}(X)$$

qui a un sous-ensemble $B \subset Y$ associe sa preimage:

$$\mathrm{preIm}(f)(B) = \{x \in X,\ f(x) \in B\} \subset X.$$

On notera plus simplement la preimage par

$$f^{-1}(B) = \mathrm{preIm}(f)(B).$$

DÉFINITION 1.2. *On dit quelquefois que la preimage de B est l'ensemble des* antecedents *des element de B par l'application f. Si $B = \{y\}$ ne possede qu'un element*

$$f^{-1}(\{y\}) = \{x \in X \mid f(x) = y\}$$

est l'ensemble des antecedent de y.

EXEMPLE 1.3.1. Pour $X = Y = \{1, 2, 3, 4\}$

$$\mathrm{Im}(f_1) = \{1, 2, 3\},\ \mathrm{Im}(f_2) = \{1, 2, 3, 4\},\ \mathrm{Im}(f_3) = \{1, 2, 3, 4\}$$
$$\mathrm{Im}(f_1)(\{2, 3\}) = \{2\},\ \mathrm{Im}(f_2)(\{2, 3\}) = \{2, 4\},\ \mathrm{Im}(f_3)(\{2, 3\}) = \{3, 4\}$$
$$f_1^{-1}(\{2, 4\}) = \{2, 3\},\ f_2^{-1}(\{2, 4\}) = \{2, 3\},\ f_3^{-1}(\{2, 4\}) = \{1, 3\}.$$

EXERCICE 1.2. Montrer que pour $A \subset X$, on a

$$A \subset f^{-1}(f(A)).$$

Montrer par un exemple qu'en general on n'a pas l'egalite

$$A = f^{-1}(f(A)).$$

Soit $B \subset Y$, existe-t-il des relations d'inclusion entre B et $f(f^{-1}(B))$?

1.3.3. Injectivite, surjectivite, application reciproque.

- Une application $f : X \mapsto Y$ est *injective* (f est une injection) si pour tout $y \in Y$, $f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) ne possede pas plus d'un element. On note l'injectivite par
$$f : X \hookrightarrow Y.$$
- Une application $f : X \mapsto Y$ est *surjective* (f est une surjection) si pour tout $y \in Y$, $f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) possede au moins un element. On note l'injectivite par
$$f : X \twoheadrightarrow Y.$$
- Une application $f : X \mapsto Y$ est *bijective* (f est une bijection) si elle est *injective* et *surjective* : cad si pour tout $y \in Y$, $f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) possede exactement un element. On note la bijectivite par
$$f : X \xrightarrow{\sim} Y \text{ ou } f : X \simeq Y.$$

REMARQUE 1.3.1. Notons qu'une application $f : X \mapsto Y$ est tautologiquement surjective sur son image $\mathrm{Im}(f)$:

$$f : X \twoheadrightarrow \mathrm{Im}(f) \subset Y.$$

En particulier une application injective $f : X \hookrightarrow Y$ defini une bijection

$$f : X \simeq \mathrm{Im}(f).$$

On peut alors identifier les element de X a certains elements de Y via cette bijection.

NOTATION 1.2. *On note*

$$\mathrm{Inj}(X, Y),\ \mathrm{Surj}(X, Y),\ \mathrm{Bij}(X, Y) \subset \mathrm{Hom}_{ENS}(X, Y)$$

les ensemble d'applications, injective, surjectives et bijectives de X vers Y.

EXEMPLE 1.3.2. On a:

(1) f_1 n'est ni injective ($f_1^{-1}(\{2\}) = \{2, 3\}$) ni surjective ($4 \notin \mathrm{Im}(f_1)$). f_2 et f_3 sont bijectives.

(2) L'application $n \in \mathbb{Z} \mapsto 2n \in \mathbb{Z}$ est injective mais pas surjective.
(3) L'application $n \in \mathbb{N} \mapsto [n/2] \in \mathbb{N}$ est surjective mais pas injective ($[x]$ designe la partie entiere d'un nombre rationnel x, cad le plus grand entier $\leqslant x$).
(4) L'application polynomiale

$$C : (m, n) \mapsto ((m + n)^2 + m + 3n)/2$$

et une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$ (Cantor).
(5) L'application

$$(m, n) \mapsto m + (n + [(m + 1)/2])^2$$

et une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$.

Exercice 1.3. Demontrer (4). Pour cela

(1) Commencer a verifier qu'on a bien une application de $\mathbb{N}^2$ vers $\mathbb{N}$.
(2) Calculer les valeurs $C(m, n)$ pour $(m, n) \leqslant 5$ et les reporter sur le plan (m, n).
(3) Pour montrer l'injectivite et la surjectivite on pourra etudier l'application $(m, n) \mapsto C(m, n)$ quand on la restreint au sous-ensemble

$$D_k = \{(m, n) \in \mathbb{N}^2,\ m + n = k\}$$

pour $k \geqslant 0$ un entier et regarder les valeurs que prend cette fonction sur ces ensembles.

Dans le cas des ensembles finis dont on connait le nombre d'element on a les proprietes suivantes liant injectivite, surjectivite, bijectivite au nombres d'elements, tres utilie pour demontrer la bijectivite.

Proposition 1.1. *Soient X et Y des ensembles finis possedant respectivement $|X|$ et $|Y|$ elements et $f : X \mapsto Y$ une application entre ces ensembles. On a les proprietes suivantes*

- *Si $f : X \hookrightarrow Y$ est injective alors $|X| \leqslant |Y|$.*
- *Si $f : X \twoheadrightarrow Y$ est surjective alors $|X| \geqslant |Y|$.*
- *Si $f : X \hookrightarrow Y$ est injective et $|X| \geqslant |Y|$ alors $|X| = |Y|$ et f est bijective.*
-
- *Si $f : X \twoheadrightarrow Y$ est surjective et $|X| \leqslant |Y|$ alors $|X| = |Y|$ et f est bijective.*

1.3.3.1. *Application reciproque d'une bijection.* Soit $f : X \xrightarrow{\sim} Y$ une bijection, alors pour tout $y \in Y$, $f^{-1}(\{y\}) \subset X$ est un element a un seul element

$$f^{-1}(\{y\}) = \{x\},$$

a savoir l'unique element x de X tel que $f(x) = y$, ie. l'unique solution de l'equation dont l'inconnue est a valeur dans X

$$f(X) = y.$$

On peut donc definir une application (l'application *reciproque* de f)

$$f^{-1} : Y \to X$$

definie par

$$f^{-1}(y) = x.$$

REMARQUE 1.3.2. On prendra garde que l'on utilise la meme notation pour l'application reciproque d'une application bijective $f^{-1} : Y \xrightarrow{\sim} X$ (qui n'existe que si f est bijective) et l'application *preimage* (qui existe tout le temps)

$$\mathrm{preIm}(f) = f^{-1} : \mathscr{P}(Y) \mapsto \mathscr{P}(X).$$

Meme si les notations sont les memes (par commodite) le contexte devrait etre suffisant pour identifie la signification de la notation.

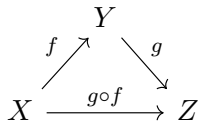
EXEMPLE 1.3.3. On a

$$\mathrm{Id}_X^{-1} = \mathrm{Id}_X.$$

1.3.4. Composition d'applications. Soit X, Y, Z des ensembles et $f : X \mapsto Y$ et $g : Y \mapsto Z$ des applications, a f et g on associe la *composee* de f et g

$$g \circ f : X \mapsto Z$$

est l'application qui va de X a Y via f et de Y a Z via g:



Elle est definie par

$$x \in X \mapsto g \circ f(x) := g(f(x)) \in Z.$$

En d'autre termes ona une application (dite de composition)

$$\circ : \begin{array}{ccc} \mathrm{Hom}_{ENS}(X,Y) \times \mathrm{Hom}_{ENS}(Y,Z) & \mapsto & \mathrm{Hom}_{ENS}(X,Z) \\ (f,g) & \mapsto & g \circ f \end{array} \tag{1.3.1}$$

La composition a les proprietes suivantes:

– Associativite: soient $f : X \mapsto Y$, $g : Y \mapsto Z$, $h : Z \mapsto W$,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

de sorte que la composee des trois applications s'ecrit simplement

$$h \circ g \circ f.$$

– Simplification: soit $f : X \xrightarrow{\sim} Y$ une bijection,

$$f \circ f^{-1} = \mathrm{Id}_X, \ f^{-1} \circ f = \mathrm{Id}_Y.$$

En particulier

$$\mathrm{Id}_X \circ \mathrm{Id}_X = \mathrm{Id}_X.$$

LEMME 1.1. *Soient des applications $f : X \mapsto Y$ et $g : Y \mapsto Z$. Si*

(1) Si f et g sont injectives, $g \circ f$ est injective.
(2) Si f et g sont surjectives, $g \circ f$ est surjective.
(3) Si f et g sont bijectives, $g \circ f$ est bijective et

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Preuve: Pour le (1), il s'agit de montrer que pour tout $z \in Z$, l'image reciproque $(g \circ f)^{-1}(\{z\})$ a au plus un element. On a

$$(g \circ f)^{-1}(\{z\}) = \{x \in X,\ g(f(x)) = z\}$$

Si $(g \circ f)^{-1}(\{z\}) = \emptyset$ on a fini. Sinon supposons que $x \in (g \circ f)^{-1}(\{z\})$, on veut montrer que x est unique. Comme g est injective $g^{-1}(\{z\})$ possede au plus un element et comme

$$z = g \circ f(x) = g(f(x))$$

on voit que $f(x)$ appartient a $g^{-1}(\{z\})$; en particulier $g^{-1}(\{z\})$ est non-vide et s'ecrit

$$g^{-1}(\{z\}) = \{y\}$$

pour un certain $y \in Y$ (qui ne depend que de z); on a donc $f(x) = y$ et donc $x \in f^{-1}(\{y\})$. Comme f est injective, $f^{-1}(\{y\})$ possede au plus un element et x est celui-ci donc x est l'unique element de $f^{-1}(\{y\})$ ou y est l'unique element de $g^{-1}(\{z\})$ et x est donc unique.

Pour (2): comme f est surjective on a $f(X) = Y$ et comme g est surjective on a $g(Y) = Z$ donc

$$g \circ f(X) = g(f(X)) = g(Y) = Z$$

et donc $g \circ f$ est surjective.

Pour (3), $g \circ f$ est injective et surjective par les point (1) et (2) (car f et g le sont) et est donc bijective. Pour montrer que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (on parle cette fois-ci de reciproques d'applications bijectives) il s'agit de montrer que pour tout $z \in Z$ on a

$$x := (g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z) = f^{-1}(g^{-1}(z)) =: x'.$$

Posons $x := (g \circ f)^{-1}(z)$ et $x' := f^{-1}(g^{-1}(z))$. On a

$$g \circ f(x) = z$$

(par definition de la reciproque $(g \circ f)^{-1}$ et on a

$$g \circ f(x') = g(f(f^{-1}(g^{-1}(z))))$$

mais

$$f(f^{-1}(g^{-1}(z))) = g(g^{-1}(z)) = z$$

(car pour tout $u \in X$, $f^{-1}(f(u)) = u$) et $g(g^{-1}(z)) = z$) et donc

$$g \circ f(x') = z = g \circ f(x)$$

et comme $g \circ f$ est injective cela implique que $x' = x$. □

Exercice 1.4. Soient des applications $f : X \mapsto Y$ et $g : Y \mapsto Z$. Montrer que si

(1) Si $g \circ f$ est injective alors f est injective.
(2) Si $g \circ f$ est surjective alors g est surjective.

Montrer par des exemples que dans le premier cas g n'est pas forcement injective et que dans le second cas f n'est pas forcement surjective.

On suppose que $g \circ f$ est bijective, que peut on dire (ou ne pas dire) de f et de g ?

Exercice 1.5. Soit $f : X \mapsto Y$ une application.

- Qu'il existe $g : Y \mapsto X$ telle que $g \circ f = \mathrm{Id}_X$ et $f \circ g = \mathrm{Id}_Y$. Montrer qu'alors f est bijective et que g est sa reciproque.
- Montrer que ce n'est pas forcement vrai si on a seulement que $g \circ f = \mathrm{Id}_X$.

1.3.5. Unions et intersections generalises. On peut generaliser maintenant l'intersection et l'union de sous-ensembles: soit X un ensemble, I un autre ensemble (qu'on suppose non vide) et

$$f : I \mapsto \mathscr{P}(X)$$

une application de I a valeurs dans l'ensemble des sous-ensemble de X. On notera alors pour tout $i \in I$

$$f(i) =: X_i$$

et on notera l'application f sous la forme

$$(X_i)_{i\in I}$$

et on dira que $(X_i)_{i\in I}$ est une *collection* ou un *famille* de sous-ensembles de X indexee par I. On peut alors former les sous-ensembles "union" et "intersection" des $(X_i)_{i\in I}$

$$\bigcup_{i\in I} X_i = \{x \in X, \text{ il existe } i \in I,\ x \in X_i\} \subset X$$

$$\bigcap_{i\in I} X_i = \{x \in X, \text{ pour tout } i \in I,\ x \in X_i\} \subset X.$$

1.3.6. Produits cartesiens generalises. De meme on definit le produit cartesien associes a une famille d'ensembles $(X_i)_{i\in I}$ (ou l'on suppose que les X_i sont contenus dans un ensemble d'ensemble:

$$\prod_{i\in I} X_i = \{(x_i)_{i\in I},\ \forall i \in I, x_i \in X_i\}.$$

Si l'un des $X_i = \emptyset$ alors $\prod_{i\in I} X_i = \emptyset$.

Supposons que tous les X_i soient non-vides. Si I est un ensemble fini (I est en bijection alrs un ensemble de la forme $\{1, \cdots, n\},\ n \geqslant 1$) alors le produit est non-vide. En revanche si I n'est pas fini, le fait que le produit est *toujours* non-vide est ce qu'on appelle *l'axiome du choix* que l'on peut decider (ou pas) d'inclure dans la theorie axiomatique que l'on se donne au depart.

1.4. Cardinal d'un ensemble

DÉFINITION 1.3. *Soient X et Y deux ensembles. Si il existe une bijection $f : X \xrightarrow{\sim} Y$, on dit que X et Y ont le meme cardinal et on le note*

$$|X| = |Y|.$$

PROPOSITION 1.2. *La relation "avoir le meme cardinal" a la proprietes suivantes*

(1) Reflexivite: $|X| = |X|$
(2) Symetrie: $|X| = |Y| \Longrightarrow |Y| = |X|$,
(3) Transitivite: $|X| = |Y|$ et $|Y| = |Z| \Longrightarrow |X| = |Z|$.

Preuve: Pour la reflexivite, il suffit de prendre Id_X. Pour la Symetrie, si $f : X \simeq Y$ est une bijection, sa reciproque $f^{-1} : Y \simeq X$ est une bijection. Pour la Transitivite, si $f : X \simeq Y$ et $g : Y \simeq Z$ sont des bijections alors $g \circ f : X \mapsto Z$ est encore une bijection. □

DÉFINITION 1.4. *Un ensemble X est fini si il est soit vide, soit en bijection avec un ensemble de la forme $\{1, \cdots, n\}$ pour $n \in \mathbb{N}$ un entier $\geqslant 1$. On ecrit alors*

$$|\emptyset| = 0,\ |X| = n.$$

Un ensemble est infini sinon.

Définition 1.5. *Un ensemble X est denombrable si il est fini ou a meme cardinal que $\mathbb{N}$. Un ensemble est indenombrable sinon.*

Exemple 1.4.1.
(1) Pour tout ensemble X, $|\mathscr{P}(X)| = |\{0,1\}^X|$.
(2) Si $|X| = n \in \mathbb{N}$, $|\mathscr{P}(X)| = 2^n$.
(3) $|\mathbb{Z}|$ est denombrable.
(4) $\mathbb{Q}$ est denombrable.
(5) $|X| = |Y| = |\mathbb{N}| \Longrightarrow |X| \times |Y| = |\mathbb{N}|$.
(6) (Cantor) Si X est denombrable et infini alors $\mathscr{P}(X)$ n'est pas denombrable.
(7) $\mathbb{R}$ nest pas denombrable (c'est un corollaire du point precedent).

On va demontrer (6) qui est du a G. Cantor.

Preuve: Si X denombrable infini alors on a une identification $X \xrightarrow{\sim} \mathbb{N}$ et donc

$$\mathscr{P}(X) \xrightarrow{\sim} \mathscr{P}(\mathbb{N}) \xrightarrow{\sim} \{0,1\}^{\mathbb{N}}.$$

Il suffit donc de montrer que ce dernier ensemble n'est pas denombrable.

Une application $f : n \in \mathbb{N} \mapsto f(n) \in \{0,1\}$ est simplement une *suite* a valeurs dans $\{0,1\}$. Supposons que l'on ait une bijection

$$\mathbb{N} \xrightarrow{\sim} \{0,1\}^{\mathbb{N}}.$$

Ainsi, a tout entier k on associe la suite $f_k = (f_k(n))_{n \geqslant 0}$ et par hypothese, toute suite f est de la forme f_k pour un certain k. Soit f_C la suite definie par

$$f_C(n) = \begin{cases} 0 & \text{si } f_n(n) = 1 \\ 1 & \text{si } f_n(n) = 0. \end{cases}$$

Alors $f_C = f_{k_0}$ pour un certain $k_0 \geqslant 0$. quelle est la valeur de $f_C(k_0)$? Il y a deux possibilites 0 ou 1:

- Si $f_C(k_0) = 0$ alors $f_{k_0}(k_0) = 1$ par definition de f_C mais alors $0 = f_C(k_0) = f_{k_0}(k_0) = 1$, contradiction.
- Si $f_C(k_0) = 1$ alors $f_C(k_0) = 0$ par definition de f_C mais alors $1 = f_C(k_0) = f_{k_0}(k_0) = 0$, contradiction.

Donc $\{0,1\}^{\mathbb{N}}$ n'est pas denombrable. Cet argument s'appelle l'argument de *la diagonale de Cantor*. □

Exercice 1.6. Deduire (7) de (6) (utiliser le developpement binaire d'un nombre reel dans $[0,1[$ masi faire attention que par convention un developpement binaire ne se termine pas par une suite constante de 1 (heureusement l'ensemble des suites a valeurs dans $\{0,1\}$ qui sont ultimement constantes egales a 1 est "petit".

1.4.1. Le Theoreme de Cantor-Bernstein-Schroeder. On peut raffiner la notion d'egalite des cardinaux:

Définition 1.6. *Soient X et Y deux ensembles. Si il existe une application injective entre X et Y, $\phi : X \hookrightarrow Y$, on dit que le cardinal de X est plus petit que celui de Y et on note cette relation $|X| \leqslant |Y|$. Si de plus $|X| \neq |Y|$, on le note $|X| < |Y|$.*

Bien evidemment si les ensembles sont finis cette definition correspond a la notion habituelle de cardinal comme etant le nombre d'elements.

Exercice 1.7. Montrer la transittivite de cette relation:

$$|X| \leqslant |Y| \text{ et } |Y| \leqslant |Z| \Longrightarrow |X| \leqslant |Z|.$$

En pensant au cas des ensembles finis il est tres tentant de penser que

$$|X| \leqslant |Y| \text{ et } |Y| \leqslant |X| \Longrightarrow |X| = |Y|.$$

Eh bien c'est vrai et c'est le theoreme suivant dont la preuve est donnee en exercice du cours "Structures Algebriques":

THÉORÈME (Cantor-Bernstein-Schroeder). *Soit X et Y deux ensembles (pas necessairement finis). Si il existe une injection $\phi : X \hookrightarrow Y$ et une injection $\psi : Y \hookrightarrow X$ alors il existe une bijection $\varphi : X \simeq Y$. En d'autre termes*

$$|X| \leqslant |Y| \text{ et } |Y| \leqslant |X| \Longleftrightarrow |X| = |Y|.$$

CHAPITRE 2

Groupes

2.1. Le cas du groupe symetrique

Soit X un ensemble, on note

$$\mathrm{Bij}(X) = \mathfrak{S}(X) = \mathrm{Aut}_{ENS}(X) = \mathrm{Bij}(X,X) \subset \mathrm{Hom}_{ENS}(X,X)$$

l'ensemble des bijections de X vers lui-meme.

Si X est fini non-vide (on peut alors supposer que $X = \{1, \cdots n\}$) pour $n \geqslant 1$ une tell bijection s'appelle alors une *permutation* de X sur lui-meme.

Cet ensemble admet des structures supplementaires

(1) $\mathrm{Bij}(X)$ est non-vide: $\mathrm{Id}_X \in \mathrm{Bij}(X)$,

(2) $\mathrm{Bij}(X)$ est stable par composition des applications (1.3.1): soient $f : X \xrightarrow{\sim} X$, $g : X \xrightarrow{\sim} X$ des bijections alors l'application composee, $f \circ g : X \to X$ est encore une bijection (la composee d'applications injectives est injective et la composee d'applications surjectives est surjective). On dispose donc d'une application (de composition):

$$\circ : \begin{array}{ccc} \mathrm{Bij}(X) \times \mathrm{Bij}(X) & \mapsto & \mathrm{Bij}(X) \\ (f,g) & \mapsto & f \circ g \end{array}.$$

(3) La composition est associative:

$$\forall f,g,h \in \mathrm{Bij}(X),\ (f \circ g) \circ h = f \circ (g \circ h) =: f \circ g \circ h.$$

(4) L'identite Id_X a la propriete de *neutralite*:

$$\forall f \in \mathrm{Bij}(X),\ f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f.$$

(5) L'application reciproque $f \mapsto f^{-1}$ envoie $\mathrm{Bij}(X)$ sur $\mathrm{Bij}(X)$

$$\bullet^{-1} : \begin{array}{ccc} \mathrm{Bij}(X) & \mapsto & \mathrm{Bij}(X) \\ f & \mapsto & f^{-1} \end{array}$$

et on a

$$\forall f \in \mathrm{Bij}(X),\ f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X.$$

Ces proprietes font de l'ensemble $\mathrm{Bij}(X)$ un *groupe* qu'on appelle le *groupe symetrique de* X.

2.1.1. Exemple: les permutations d'un ensemble fini. Considerons le cas ou X est un ensemble fini, non-vide de cardinal $n \geqslant 1$; on peut alors supposer que $X = \{1, \cdots n\}$. On note souvent ce groupe Σ_n.

On rappelle qu'alors $\mathrm{Bij}(X)$ est fini de cardinal

$$|\mathrm{Bij}(X)| = n!$$

avec

$$n! = 1.2. \cdots .n,\ n \geqslant 1,\ 0! = 1.$$

Preuve: En effet pour definir une bijection $\sigma : \{1, \cdots n\} \xrightarrow{\sim} \{1, \cdots n\}$. On choist $\sigma(1)$ parmi n elements, puis $\sigma(2)$ parmi les $n-1$ element restants,... Le mieux est de demontrer cette egalite une recurrence sur n. □

On peut representer une permutation par un tableau a deux lignes et n colonnes

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

Ainsi l'identite est ainsi codee par

$$\mathrm{Id}_X = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Par exemple, pour $n = 4$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

est la permutation qui envoie

$$1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 4,\ 4 \mapsto 1$$

et si on compose σ avec elle-meme on obtient

$$\sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix},$$

qui envoie

$$1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 1;$$

iterant une fois de plus, on a

$$\sigma \circ \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{Id}_X.$$

2.1.1.1. *Cycles.* Un autre exemple est la permutation cyclique

$$\sigma_{+1} = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

qui envoie

$$1 \mapsto 2,\ 2 \mapsto 3, \cdots,\ k \mapsto k+1, \cdots, n \mapsto 1.$$

Pour les permutations cycliques telle que celle ci-dessus, une autre notation (plus compacte) est tres utile: pour $1 \leqslant k \leqslant n$, on se donne

$$\{a_1, \cdots, a_k\} \subset \{1, \cdots n\}$$

des elements *distincts* et on pose

$$(a_1 a_2 \cdots a_k)$$

la permutation qui envoie

$$a_1 \mapsto a_2,\ a_2 \mapsto a_2, \cdots, a_k \mapsto a_1$$

et qui envoie chacun des $n-k$ elements de $\{1, \cdots n\} - \{a_1, \cdots, a_k\}$ sur lui meme: la permutation $(a_1 a_2 \cdots a_k)$ est appellee *cycle de longueur* k.

Par exemple

$$\sigma_{+1} = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} = (12 \cdots n)$$

est un cycle de longueur n et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (134)$$

est un cycle de longueur 3.

Transpositions. Un classe particulierement importante de cycle sont ceux de longueur 2, $(a_1 a_2)$, $a_1 \neq a_2$ qu'on les appelle *transpositions*: explicitement $(a_1 a_2)$ echange a_1 et a_2 et envoie tous les autres elements sur eux-meme.

Dans le cours MATH-113 vous demontrerez le theorem de decomposition suivant

THÉORÈME 2.1. *Soit $\mathfrak{S}_n = \mathrm{Bij}(\{1, \cdots, n\})$ le groupe de permutations de n elements alors*

(1) Toute permutation s'ecrit comme une composee de cycles,
(2) tout cycle s'ecrit comme compose de tranpositions,
(3) et donc toute permutation s'ecrit comme compose de tranpositions.

Par exemple

$$\sigma = (134) = (34) \circ (14)$$

et (le demontrer)

$$(12 \cdots n) = (2n) \circ (23) \circ \cdots \circ (k-1, k) \circ \cdots \circ (n-2, n-1) \circ (1n)$$

2.2. Groupes abstraits

DÉFINITION 2.1. *Un groupe $(G, \star, e_G, \cdot^{-1})$ est la donnee d'un quadruple forme de*

- *d'un ensemble G non-vide,*
- *d'une application (appelee loi de composition interne)*

$$\star : \begin{array}{ccc} G \times G & \mapsto & G \\ (g, g') & \mapsto & \star(g, g') =: g \star g' \end{array}$$

- *d'un element $e_G \in G$ (appele element neutre),*
- *d'une application (appele inversion)*

$$\bullet^{-1} : \begin{array}{ccc} G & \mapsto & G \\ g & \mapsto & g^{-1} \end{array}$$

ayant les proprietes suivantes:

- *Associativite: $\forall g, g', g'' \in G,\ (g \star g') \star g'' = g \star (g' \star g'')$.*
- *Neutralite de e_G: $\forall g \in G,\ g \star e_G = e_G \star g = g$.*
- *Inversibilite: $\forall g \in G,\ g^{-1} \star g = g \star g^{-1} = e_G$.*

REMARQUE 2.2.1. Par soucis de concision on omettra l'element neutre et l'inversion (voire de la loi de groupe) dans les donnees: notera souvent un groupe par G ou $(G, \star)$.

REMARQUE 2.2.2. La propriete d'associativite est indispensable et par ailleurs extremement utile: si l'on se donne 3 elements

$$g_1, g_2, g_3 \in G$$

dont on veut former le produit (dans cet ordre): pour cela on calcule $g_{12} = g_1 \star g_2$ puis le produit $g_{12} \star g_3 = (g_1 \star g_2) \star g_3$ et l'associativite nous dit qu'au lieu de cela on aurait pu commencer par calculer $g_{23} = g_2 \star g_3$ et faire le produit

$$g_1 \star g_{23} = g_1 \star (g_2 \star g_3)$$

et l'associativite nous dit que cela de depend pas de la maniere dont on s'y prend:

$$(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$$

et on peut ecrire sans ambiguite ce produit sans parantheses

$$g_1 \star g_2 \star g_3 = g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3.$$

De meme si on dispose de n elements $g_1, \cdots, g_n \in G$, on defini sans ambiguite leur produit

$$g_1 \star \cdots \star g_n = \star_{i=1}^{n} g_i.$$

PROPOSITION 2.1. *(Proprietes de base de la loi de groupe) Soit G un groupe. On a*

(1) Involutivite de l'inversion:

$$\forall g,\ (g^{-1})^{-1} = g,\ g^{-1} \star g = e_G.$$

(2) Unicite de l'element neutre: soit $e'_G \in G$ tel qu'il existe $g \in G$ verifiant $g \star e'_G = g$ alors $e'_G = e_G$. On a la meme conclusion si il existe g' tel que $e'_G \star g' = e'_G$.

(3) Unicite de l'inverse: si $g' \in G$ verifie $g \star g' = e_G$ alors $g' = g^{-1}$ et on a donc egalement $g' \star g = e_G$. De meme si $g' \in G$ verifie $g' \star g = e_G$ alors $g' = g^{-1}$ et on a donc egalement $g \star g' = e_G$.

(4) Inverse d'un produit: on a

$$(g \star g')^{-1} = g'^{-1} \star g^{-1}.$$

Preuve: (2) Unicite de l'element neutre: dans l'equation

$$g \star e'_G = g$$

on multiple a gauche par g^{-1} ce qui donne

$$g^{-1} \star g \star e'_G = e_G \star e'_G = e'_G = g^{-1} \star g = e_G.$$

Pour le deuxieme cas, on multiplie a droite par g'^{-1}.

(3) Unicite de l'inverse: en multipliant l'egalite $g \star g' = e_G$ a gauche par g^{-1} et en utilisant l'associativite on a

$$g \star g' = e_G \Longrightarrow g^{-1} \star g \star g' = g^{-1} \star e_G$$

et $g^{-1} \star g \star g' = g'$ tandis que $g^{-1} \star e_G = g^{-1}$.

On traite de la meme maniere le cas $g' \star g = e_G$.

(1) Involutivite de l'inversion: en particulier, appliquant ce raisonnement a g^{-1} avec $g' = g$, comme $g \star g^{-1} = e_G$ on obtient que $(g^{-1})^{-1} = g$.

(4) Inverse d'un produit:

$$(g'^{-1} \star g^{-1}) \star (g \star g') = g'^{-1} \star (g^{-1}) \star g) \star g' = g'^{-1} \star e_G \star g' = g'^{-1} \star g' = e_G$$

et donc (par unicite de l'inverse)

$$(g \star g')^{-1} = g'^{-1} \star g^{-1}.$$

2.2.1. Exemples de groupes.

(1) Comme on l'a vu $(\mathrm{Bij}(X), \circ, \mathrm{Id}_X, \bullet^{-1})$ muni de la composition des applications , de l'identite Id_X et de la reciproque forme un groupe: le *groupe symetrique de* X ou le groupe des *permutations* de X.
(2) L'ensemble $(\mathbb{Z}, +, 0, -\bullet)$des entiers relatifs $\mathbb{Z}$ muni de l'addition, du zero 0 et de l'oppose $n \mapsto -n$ forme un groupe.
(3) En revanche $(\mathbb{Z} - \{0\}, +, 0, -\bullet)$ forme des entiers non-nuls muni des memes structures ne forme pas un groupe (il manque un element neutre et d'ailleurs il n'est pas stable par addition).
(4) L'ensemble $(\mathbb{Q}, +, 0, -\bullet)$ des entiers relatifs $\mathbb{Z}$ muni de l'addition, du zero 0 et de l'oppose $n \mapsto -n$ forme un groupe.
(5) L'ensemble $(\mathbb{Q}^\times, \times, 1, 1/\bullet)$ avec $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ est l'ensemble des nombres rationels non-nuls muni de la multiplication, de l'unite 1 et de l'inversion $\lambda \mapsto 1/\lambda$ forme un groupe,
(6) de meme que le sous-ensemble $\mathbb{Z}^\times := \{\pm 1\}$ muni des memes structures.
(7) Groupe produit: soient $(G, \star)$ et $(H, *)$ deux groupes. Le groupe produit $(G \times H, \boxtimes)$ est le groupe associe au produit cartesien

$$G \times H = \{(g, h),\ g \in G,\ h \in H\}$$

muni de la loi de composition interne $\boxtimes$ definie par

$$(g, h) \boxtimes (g', h') := (g \star g', h * h').$$

On peut le munir d'un element neutre et d'une inversion pour en faire un groupe (exercice).

2.2.1.1. *Notation exponentielle.* Soit $g \in G$ un element d'un groupe. Pour tout entier $n \geqslant 1$, on forme le produit de g avec lui-meme n fois et on le note

$$g \star g \star \cdots \star g = g^n.$$

On a donc

$$g^{n+1} = g^n \star g = g \star g^n.$$

On pose ensuite

$$g^0 = e_G \tag{2.2.1}$$

et si $n < 0$ est un entier negatif, on pose

$$g^n = (g^{-1})^{-n} = g^{-1} \star \cdots \star g^{-1} (-n = |n| \text{ fois}).$$

cela defini g^n pour $n \in \mathbb{Z}$ On a alors pour tout $m, n \in \mathbb{Z}$

$$g^{m+n} = g^m \star g^n. \tag{2.2.2}$$

On a alors defini une fonction

$$\exp_g : \begin{array}{ccc} \mathbb{Z} & \mapsto & G \\ n & \mapsto & \exp_g(n) = g^n \end{array} \tag{2.2.3}$$

qu'on appelle *exponentielle* de n dans la base g. On dira alors que l'image

$$\mathrm{Im}(\exp_g) = \exp_g(\mathbb{Z}) = \{g^n,\ n \in \mathbb{Z}\}$$

est l'ensemble des puissances de g.

2.2.2. Groupes commutatifs. A l'exception du tout premier exemple, les autres groupes ont une propriete supplementaire: la *commutativite*

DÉFINITION 2.2. *Soit $(G,\star)$ un groupe. Deux elements g,h commutent si*

$$g\star h=h\star g.$$

Un groupe G est abelien (ou commutatif) si toutes les paires d'elements de G commutent:

$$g,h\in G,\ g\star h=h\star g.$$

EXERCICE 2.1. Montrer que si X possede 2 elements ou moins alors $\mathrm{Bij}(X)$ est commutatif. Montrer que si X possede au moins 3 element il ne l'est pas (pour cela choisir trois elements distincts $x_1,x_2,x_3\in X$ et trouver des bijections σ,τ qui verifient

$$\forall x\in X-\{x_1,x_2,x_3\},\sigma(x)=x,\ \tau(x)=x$$

et telles que $\sigma\circ\tau=\tau\circ\sigma$.

2.2.2.1. *Notation additive.* Si le groupe G est commutatif, sa loi de groupe sera souvent notee (mais pas toujours) par une addition (par exemple $+_G$), l'element neutre par le signe "0" (par exemple 0_G) et l'inversion par $-\bullet$.

L'inverse de g, $-g$ sera alors appele *l'oppose de g*. De plus, on ecrira

$$g+_G g',g+_G 0_G=0_G+_G g=g,g+_G(-g)=0_G$$

et l'exponentielle d'un entier $n\in\mathbb{Z}$ dans la base un element g sera notee sous forme de multiple: pour $n\geqslant 1$,

$$n.g=g+_G\cdots+_G g,\ (-n).g=(-Gg)+_G\cdots+_G(-_Gg)(n\text{ fois}),\ 0.g=0_G,$$

de sorte que (2.2.2) devient

$$\forall m,n\in\mathbb{Z},\ (m+n).g=m.g+_G n.g.$$

On dispose alors d'une application (de multiplication par g) de $\mathbb{Z}$ a valeurs dans G:

$$\cdot.g:\begin{array}{ccc}\mathbb{Z}&\mapsto&G\\ n&\mapsto&n.g\end{array}$$

On dira alors que son image

$$\mathbb{Z}.g=\{n.g,\ n\in\mathbb{Z}\}\subset G$$

est l'ensemble des multiples de g.

2.3. Sous-groupes

Avec la notion d'ensemble vient la notion de sous-ensemble. De meme avec la notion de *groupe* vient la notion de *sous-groupe* d'un groupe G: un sous-groupe est un sous-ensemble de G qui herite naturellement des structures additionelles $\star,e_G,\bullet^{-1}$ venant avec la structure de groupe de l'ensemble G.

DÉFINITION 2.3. *Soit $(G,\star,e_G,\bullet^{-1})$ un groupe. Un sous-groupe $H\subset G$ est un sous-ensemble de G tel que*

(1) $e_G\in H$.
(2) H est stable pour la loi de composition interne $\star$:

$$\forall h,h'\in H,\ h\star h'\in H.$$

(3) H est stable par l'inversion:

$$\forall h \in H,\ h^{-1} \in H.$$

Alors si on note $\star_H$ et $\bullet_H^{-1}$ les restrictions de la loi de composition $\star$ et de l'inversion $\bullet^{-1}$ aux sous-ensembles $H \times H$ et H on a

$$\star_H : \begin{array}{ccc} H \times H & \mapsto & H \\ (h,h') & \mapsto & h \star h', \end{array} \quad \bullet_H^{-1} : \begin{array}{ccc} H & \mapsto & H \\ h & \mapsto & h^{-1} \end{array}$$

et $(H, \star_H, e_G, \bullet_H^{-1})$ forme un groupe.

Remarque 2.3.1. Distinguer les restrictions a H de la loi de composition et de l'inversion est formellement correct mais un peu pedant. La convention universelle est d'omettre cette restriction dans les notations et d'ecrire $(H, \star, e_H = e_G, \bullet^{-1})$ ou plus simplement $(, \star)$.

En fait il n'est pas necessaire de verifer les trois conditions de la definition d'un sous-groupe.

Proposition 2.2 (Critere de sous-groupe). *Pour montrer qu'un sous-ensemble non-vide $\emptyset \neq H \subset G$ est un sous-groupe il suffit de verifier l'un ou l'autre des groupes de proprietes (1) ou (2) ci-dessous:*

(1) (a) $\forall h, h' \in H,\ h \star h' \in H$,
(b) $\forall h \in H,\ h^{-1} \in H$.
(2) $\forall h, h' \in H,\ h \star h'^{-1} \in H$.

Preuve: On va montrer que si (2) est verifiee alors H est un sous-groupe (le cas (1) est encore plus simple):

- En prenant $h' = h$, on a $h \star h^{-1} = e_G \in H$ donc H contient l'element neutre.
- En applicant $h \star h'^{-1} \in H$ avec $h = e_G$ on a que si $h' \in H$ alors $h'^{-1} \in H$.
- En applicant $h \star h'^{-1} \in H$ avec $h \in H$ et $h'' = h'^{-1}$ et en utilisant que $(h'^{-1})^{-1} = h'$, on a que si $h, h' \in H$ alors $h \star h' \in H$.

□

Exemple 2.3.1. Voici quelques exemples de sous-groupes:

(1) $\{e_G\} \subset G$ est un sous.-groupe: le sous-groupe trivial.
(2) $G \subset G$ est egalement un sous-groupe.
(3) l'ensemble vide $\emptyset \subset G$ n'est pas un sous-groupe (il lui manque l'element neutre).
(4) $2\mathbb{Z} \subset \mathbb{Z}$ (l'ensemble des entiers pairs) est un sous-groupe.
(5) $1 + 2\mathbb{Z} \subset \mathbb{Z}$ (l'ensemble des entiers impairs) n'est pas un sous-groupe.
(6) Pour tout entier $q \in \mathbb{Z}$,

$$q.\mathbb{Z} = \{q.n, n \in \mathbb{Z}\} \subset \mathbb{Z},$$

l'ensemble des multiples de q est un sous-groupe. Reciproquement, tout sous-groupe de $\mathbb{Z}$ est de la forme $q.\mathbb{Z}$ pour $q \in \mathbb{Z}$. En effet, soit $H \subset \mathbb{Z}$ un sous-groupe. Si $H = \{0\}$ on a termine car $H = 0.\mathbb{Z}$. Sinon soit $q \in H - \{0\}$; quitte a remplacer q par $-q$ (qui est encore dans H car H est un sous-groupe) ops $q > 0$. On peut egalement supposer que q est le plus petit entier > 0 contenu dans H. On va montrer qu'alors $H = q.\mathbb{Z}$.

Comme $q \in H$ on a $q.\mathbb{Z} \subset H$

Soit $h \in H$ alors par division euclidienne, h peut s'ecrire

$$h = q.k + r$$

avec $k \in \mathbb{Z}$ et $0 \leqslant r < q$. Mais comme H est un sous-groupe et que h et $q.k = \pm(q + \cdots + q)$ ($|k|$ fois) sont dans H,

$$r = h - q.k \in H.$$

Comme $0 \leqslant r < q$ on a necessairement $r = 0$ (par definition de q comme plus petit element positif non-nul de H) et donc $h = q.k \in q.\mathbb{Z}$.

(7) Pour $g \in G$, l'ensemble des puissance de g

$$\exp_g(\mathbb{Z}) = \{g^n,\ n \in \mathbb{Z}\} \subset G$$

est un sous-groupe commutatif de G.

(8) Si G est commutatif et que la loi de groupe est notee additivement, l'ensemble des multiples de g,

$$\mathbb{Z}.g = \{n.g,\ n \in \mathbb{Z}\} \subset G$$

est un sous-groupe commutatif de G.

(9) Soit X un ensemble $G = \mathrm{Bij}(X)$ et $x \in X$ un element, alors le sous-ensemble

$$\mathrm{Bij}(X)_x = \{\sigma \in \mathrm{Bij}(X),\ \sigma(x) = x\}$$

est un sous-groupe: on l'appelle *le stabilisateur* de x dans $\mathrm{Bij}(X)$.

Le resultat suivant qu'on demontrera plus tard nous dit que le cas du groupe symetrique est fondamental (voir Exercice 2.6 pour la preuve) :

THÉORÈME 2.2. *Soit G un groupe alors G s'identifie canoniquement a un sous-groupe du groupe* $\mathrm{Bij}(G)$ *des bijections de G sur lui-meme.*

2.3.1. Groupe engendre par un ensemble.

PROPOSITION 2.3. *(Invariance par intersection) Soit G un groupe et $H_1, H_2 \subset G$ deux sous-groupes alors $H_1 \cap H_2$ est un sous-groupe. Plus generalement soit $H_i, i \in I,\ H_i \in G$ une collection de sous-groupes de G indexes par I alors*

$$\bigcap_{i \in I} H_i \subset G$$

est un sous-groupe de G.

Preuve: On utilise le critere de sous-groupe: d'abord $\bigcap_{i\in I} H_i$ est non-vide car il contient l'element neutre e_G. Soient $h, h' \in \bigcap_{i\in I} H_i$ montrons que $h \star h'^{-1} \in \bigcap_{i\in I} H_i$. Il s'agit de montrer que pour tout $i \in I$, $h \star h'^{-1} \in H_i$ mais c'est vrai car H_i est un sous-groupe de G. □

DÉFINITION 2.4. *Soit*

$$\mathcal{G}_A = \{H \subset G \text{ sous-groupe } | A \subset H\}$$

l'ensemble de tous les sous-groupes de G contenant A (cet ensemble est non-vide car G est dedans). Alors l'intersection de ses sous-groupes

$$\bigcap_{H \in \mathcal{G}_A} H \subset G$$

est un sous-groupe contenant A et c'est le plus petit (si H est un sous-groupe contenant A alors $\langle A \rangle \subset H$.) Ce sous-groupe

$$\langle A \rangle := \bigcap_{H \in \mathcal{G}_A} H$$

s' appelle le sous-groupe engendre par A.

Voici une caracterisation plus constructive de $\langle A\rangle$ (qui justifie la terminologie):

THÉORÈME 2.3 (Caracterisation linguistique du groupe engendre par un ensemble). *Soit $A \subset G$ un ensemble, si $A = \emptyset$ alors $\langle A\rangle = \{e_G\}$, sinon on pose*

$$A^{-1} = \{g^{-1},\ g \in A\} \subset G$$

l'image de A par l'inversion, alors

$$\langle A\rangle = \{g_1 \star \cdots \star g_n,\ n \geqslant 1,\ g_i \in A \cup A^{-1}\}.$$

En d'autres termes, $\langle A\rangle$ est l'ensemble des elements de G qu'on peut former en multipliant ensemble des elements de A et de son inverse A^{-1} de toutes les manieres possibles.

Preuve: Si $A = \emptyset$, il est clair que le groupe trivial a les bonnes proprietes. Supposons A non-vide. Il s'agit de montrer que l'ensemble

$$\langle A\rangle' = \{g_1 \star \cdots \star g_n,\ n \geqslant 1,\ g_i \in A \cup A^{-1}\}$$

est un sous-groupe contenant A et qu'il est contenu dans tout sous-groupe $H \supset A$.

Considerant les mots de longueur 1, $g_1,\ g_1 \in A$ on voit que $A \subset \langle A\rangle'$. Soient

$$g_1 \star \cdots \star g_n, g_1' \star \cdots \star g_{n'}' \in \langle A\rangle'$$

deux tels mots alors

$$g_1 \star \cdots \star g_n \star (g_1' \star \cdots \star g_{n'}')^{-1} = g_1 \star \cdots \star g_n \star g_{n'}'^{-1} \star \cdots \star g_1'^{-1} \in \langle A\rangle'.$$

ainsi $\langle A\rangle'$ est un sous-groupe de G contenant A par consequent

$$\langle A\rangle \subset \langle A\rangle'.$$

Enfin, si $A \subset H$ est un autre sous-groupe alors $A^{-1} \in H$ (car H est stable par inversion) et pour tout $n \geqslant 1$ et tout $g_1, \cdots, g_n \in A \cup A^{-1} \subset H$ on a $g_1 \star \cdots \star g_n \in H$ car H est stable par $\star$ et donc $\langle A\rangle' \subset H$ et donc

$$\langle A\rangle' \subset \bigcap_{H \in \mathcal{G}_A} H = \langle A\rangle \subset \langle A\rangle'.$$

□

EXEMPLE 2.3.2. Soit $g \in G$ alors le sous-groupe engendre par g, $\langle\{g\}\rangle$ vaut

$$\langle\{g\}\rangle = g^{\mathbb{Z}}.$$

2.4. Morphismes de groupes

Les sous-groupes d'une groupe son les sous-ensemble qui preservent la structur de groupe; les *morphismes* de groupes sont les applications entre deux groupes qui preservent les structures respectives de ces groupes.

DÉFINITION 2.5. *Soient $(G, \star)$ et $(H, *)$ deux groupes, un morphisme de groupes $\varphi : G \mapsto H$ est une application telle que*

$$\forall g, g' \in G,\ \varphi(g \star g') = \varphi(g) * \varphi(g').$$

THÉORÈME 2.4 (Propriete fonctionnelle d'un morphisme). *Soit $\varphi : G \mapsto H$ un morphisme de groupes alors*

(1) $\varphi(e_G) = e_H$,

(2) $\forall g \in G,\ \varphi(g^{-1}) = \varphi(g)^{-1}$,
(3) $\forall g, g' \in G,\ \varphi(g \star g') = \varphi(g) * \varphi(g')$.

Preuve: La troisieme identite est juste une repetition de la definition.

Pour la premiere identite, on a

$$\varphi(g) = \varphi(g \star e_G) = \varphi(g) * \varphi(e_G)$$

et donc $\varphi(e_G) = e_H$ par unicite de l'element neutre dans H.

Pour la deuxieme on a pour tout $g \in G$

$$\varphi(g \star g^{-1}) = \varphi(e_G) = e_H = \varphi(g) * \varphi(g^{-1})$$

et donc $\varphi(g^{-1}) = \varphi(g)^{-1}$ par unicite de l'inverse dans H. □

EXEMPLE 2.4.1. Les applications suivantes sont des morphismes de groupes

- Soit G un groupe (note multiplicativement) et $g \in G$. Montrer que l'application
$$\exp_g : n \in \mathbb{Z} \mapsto g^n \in G$$
est un morphisme de groupe.
- En particulier pour
$$q \in \mathbb{Z},\ [\times q] : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathbb{Z} \\ n & \mapsto & qn \end{array}$$
est un morphisme de groupes.
- Les fonctions exponentielles et logarithme
$$\exp : \begin{array}{ccc} (\mathbb{R},+) & \mapsto & (\mathbb{R}_{>0},\times) \\ x & \mapsto & \exp(x) \end{array},\ \log : \begin{array}{ccc} (\mathbb{R}_{>0},\times) & \mapsto & (\mathbb{R},+) \\ x & \mapsto & \log(x) \end{array}.$$

Ensembles de morphismes. On peut egalement construire des morphismes de groupes a partir d'autres morphismes de groupes:

PROPOSITION 2.4. *(Invariance par composition) Soient $(G,\star),(H,*),(K,\otimes)$ des groupes et $\varphi : G \mapsto H$ et $\psi : H \mapsto K$ des morphismes de groupes alors la composee $\psi \circ \varphi : G \mapsto K$ est un morphisme de groupes.*

Preuve: Soit $g, g' \in G$ alors

$$\psi \circ \varphi(g \star g') = \psi(\varphi(g \star g')) = \psi(\varphi(g) * \varphi(g')) = \psi(\varphi(g)) \otimes \psi(\varphi(g')) = \psi \circ \varphi(g) \otimes \psi \circ \varphi(g').$$

□

Ensuite les morphismes de groupes bijectifs sont stable par l'application reciproque:

PROPOSITION 2.5. *(Invariance par reciproque) Soit $\varphi : G \mapsto$ un morphisme de groupe bijectif alors l'application reciproque $\varphi^{-1} \in \mathrm{Hom}_{ENS}(H,G)$ est un morphisme de groupe bijectif.*

Preuve: Il faut montrer que pour $h, h' \in H$

$$\varphi^{-1}(h * h') = \varphi^{-1}(h) \star \varphi^{-1}(h').$$

Soit $g = \varphi^{-1}(h),\ g' = \varphi^{-1}(h')$ alors

$$\varphi(g \star g') = \varphi(g) * \varphi(g') = \varphi(\varphi^{-1}(h)) * \varphi(\varphi^{-1}(h')) = h * h'.$$

Ainsi $g \star g' \in \varphi^{-1}(\{h * h'\})$ mais comme φ est bijective $\varphi^{-1}(\{h * h'\})$ ne possede qu'un seul element et comme $\varphi^{-1}(h * h')$ en fait partie (puisque $\varphi(\varphi^{-1}(h * h')) = h * h'$) on a

$$\varphi^{-1}(h) \star \varphi^{-1}(h') = g \star g' = \varphi^{-1}(h * h')$$

□

On en deduit le

COROLLAIRE 2.1. *L'ensemble* $\mathrm{Aut}_{Gr}(G) \subset \mathrm{Bij}_{ENS}(G)$ *est un sous-groupe pour la composition* $\circ$.

Preuve: En effet l'ensemble $\mathrm{Aut}_{Gr}(G) \subset \mathrm{Bij}_{ENS}(G)$ est stable par composition et par reciproque. On applique le critere de sous-groupe. □

Notation. On notera

- $\mathrm{Hom}_{Gr}(G,H)$ l'ensemble des morphismes de groupes de G vers H,
- $\mathrm{Inj}_{Gr}(G,H)$ l'ensemble des morphisme injectifs (qu'on appelle egalement monomorphismes de groupes),
- $\mathrm{Surj}_{Gr}(G,H)$ l'ensemble des morphisme surjectifs (qu'on appelle egalement epimorphismes de groupes), et
- $\mathrm{Iso}_{Gr}(G,H)$, l'ensemble des morphisme de groupes bijectifs (qu'on appelle egalement isomorphismes de groupes).
- Si $H = G$, on ecrit notera ces ensembles

$$\mathrm{Hom}_{Gr}(G),\ \mathrm{Inj}_{Gr}(G),\ \mathrm{Surj}_{Gr}(G),\ \mathrm{Iso}_{Gr}(G)$$

et par ailleurs on ecrira egalement

$$\mathrm{Hom}_{Gr}(G) = \mathrm{End}_{Gr}(G)$$

(qu'on appelle egalement endomorphismes de groupe) et

$$\mathrm{Iso}_{Gr}(G) = \mathrm{Aut}_{Gr}(G)$$

(qu'on appelle egalement automorphismes de groupe).

Groupes isomorphes. Soient G, H deux groupes tels que $\mathrm{Iso}_{Gr}(G,H) \neq \emptyset$ et il existe donc un isomorphisme de groupes

$$\varphi : G \xrightarrow{\sim} H.$$

On dit alors que G et H sont *isomorphes* et one le note

$$G \simeq_{Gr} H.$$

Si c'est le cas, – pour autant que l'on soit interesse par les structures de groupes – G et H ont exactement les meme proprietes et peuvent etre identifies l'un a l'autre comme groupes via les morphismes φ et φ^{-1}.

EXERCICE 2.2. montrer que la relation pour deux groupes d'etre isomorphes est une relation d'equivalence sur la categorie des groupes (qui n'est pas un ensemble): soient G, H, K des groupes,

(1) on a $G \simeq_{Gr} G$.
(2) Si $G \simeq_{Gr} H$ alors $H \simeq_{Gr} G$,
(3) si $G \simeq_{Gr} H$ et $H \simeq_{Gr} K$ alors $G \simeq_{Gr} K$.

EXERCICE 2.3. Soient G et H deux groupes isomorphes (de sorte que $\mathrm{Iso}_{Gr}(G,H) \neq \emptyset$). Montrer que pour tout $\varphi \in \mathrm{Iso}_{Gr}(G,H)$,

$$\mathrm{Iso}_{Gr}(G,H) = \varphi \circ \mathrm{Aut}_{Gr}(G) = \mathrm{Aut}_{Gr}(H) \circ \varphi$$

avec

$$\varphi \circ \mathrm{Aut}_{Gr}(G) = \{\varphi \circ \psi,\ \psi \in \mathrm{Aut}_{Gr}(G)\}$$

et

$$\mathrm{Aut}_{Gr}(H) \circ \varphi = \{\psi \circ \varphi,\ \phi \in \mathrm{Aut}_{Gr}(H)\}.$$

2.4.1. Noyau, Image. Les morphismes preserve la structure de sous-groupe:

PROPOSITION 2.6. *(Invariance des sous-groupes par morphismes) Soit $\varphi \in \mathrm{Hom}_{Gr}(G,H)$ un morphisme de groupes.*

(1) Soit $K \subset G$ un sous-groupe alors $\varphi(K) \subset H$ est un sous-groupe. En particulier l'image de φ,

$$\mathrm{Im}(\varphi) = \varphi(G)$$

est un sous-groupe de H.

(2) Soit $L \subset H$ un sous-groupe de H, alors l'image inverse

$$\varphi^{-1}(L) = \{g \in G,\ \varphi(g) \in L\} \in G$$

est un sous-groupe de G. En particulier $\varphi^{-1}(\{e_H\})$ est un sous-groupe de G.

Preuve: Soit $h, h' \in \varphi(K)$, on veut montrer que $h * h'^{-1} \in \varphi(K)$. Par definition il existe $k, k' \in K$ tels que $\varphi(k) = h, \varphi(k') = h'$ et

$$h * h'^{-1} = \varphi(k) * \varphi(k')^{-1} = \varphi(k \star k'^{-1}) \in \varphi(K)$$

car $k \star k'^{-1} \in K$ puisque K est un sous-groupe.

Soit $g, g' \in \varphi^{-1}(L)$ alors montrons que $\varphi(g \star g'^{-1}) \in L$. On a

$$\varphi(g \star g'^{-1}) = \varphi(g) * \varphi(g')^{-1} \in L$$

car $\varphi(g), \varphi(g') \in L$ par definition et L est un sous-groupe. □

DÉFINITION 2.6. *Le sous-groupe $\varphi^{-1}(\{e_H\})$ s'appele le noyau de φ et est note*

$$\ker(\varphi) = \varphi^{-1}(\{e_H\}) = \{g \in G,\ \varphi(g) = e_H\}.$$

L'importance du noyan vient du fait qu'il permet de tester facilement si un morphisme est injectif.

THÉORÈME 2.5 (Critere d'injectivite). *Soit $\varphi \in \mathrm{Hom}_{Gr}(G,H)$ un morphisme de groupes alors les proprietes suivantes sont equivalentes*

(1) φ est injectif,

(2) $\ker(\varphi) = \{e_G\}$.

Preuve: Supposons φ injectif alors $\ker(\varphi) = \{g \in G,\ \varphi(g) = e_H\}$ possede au plus un element. Mais comme $\varphi(e_G) = e_H$ on a $\ker(\varphi) = \{e_G\}$.

Supposons que $\ker(\varphi) = \{e_G\}$; on veut montrer que pour tout $h \in H$,

$$\varphi^{-1}(h) = \{g \in G,\ \varphi(g) = h\}$$

possede au plus un element. Soient $g, g' \in \varphi^{-1}(h)$ (si l'ensemble est vide on a fini) alors

$$\varphi(g) = \varphi(g') = h$$

et

$$\varphi(g) * \varphi(g')^{-1} = h * h^{-1} = e_H$$

mais

$$e_H = \varphi(g) * \varphi(g')^{-1} = \varphi(g \star g'^{-1})$$

donc $g \star g'^{-1} \in \ker(\varphi) = \{e_G\}$ et

$$g \star g'^{-1} = e_G \Longrightarrow g = g'$$

et donc $\varphi^{-1}(h)$ possede au plus un element. □

EXERCICE 2.4 (Equations dans les groupes). Soit G, H des groupes et $\varphi : G \mapsto H$ un morphisme. Etant donne $h \in H$, on cherche a resoudre l'equation d'inconnue $g \in G$:

$$Eq(\varphi, h) : \qquad \varphi(g) = h.$$

L'ensemble des solutions de cette equation n'est autre que la preimage $\varphi^{-1}(\{h\})$...

(1) Montrer que
$$\varphi^{-1}(\{h\})$$
est soit vide soit qu'il existe $g_0 \in G$ tel que
$$\varphi^{-1}(\{h\}) = g_0 \star \ker(\varphi)$$
ou
$$g_0 \star \ker(\varphi) = \{g_0 \star k,\ k \in \ker(\varphi)\}.$$

(2) Montrer que
$$\varphi^{-1}(\{h\}) = \ker(\varphi) \star g_0$$
avec
$$\ker(\varphi) \star g_0 = \{k \star g_0,\ k \in \ker(\varphi)\}.$$

Quel est l'ensemble de tous les $g_0 \in G$ ayant cette propriete ? Cela vous rappelle t il quelque chose ? (pensez a "equation avec" et "sans second membre", "solution particuliere", "solution generale" ...)

2.4.2. Exemple: ordre d'un element. Soit $g \in G$ un element d'un groupe. On a le morphisme puissances

$$\exp_g : n \in \mathbb{Z} \mapsto g^n \in G$$

et $\ker(\exp_g)$ est un sous-groupe de $\mathbb{Z}$ et donc de la forme

$$\ker(\exp_g) = q.\mathbb{Z}$$

avec $q = q(g) \in \mathbb{N}$ (car tous les sous-groupes de $\mathbb{Z}$ sont de cette forme).

- Si $q = 0$ alors $\ker(\exp_g) = \{0\}$ et $\exp_g$ est injectif et $\mathbb{Z} \simeq g^{\mathbb{Z}}$ (c'est meme un isomorphisme de groupes). On dit que g est 'd'ordre infini et on le note
$$\mathrm{ord}(g) = \infty.$$
- Si $q > 0$, alors q est le plus petit entier strictement positif tel que
$$g^q = e_G$$
et $g^{\mathbb{Z}}$ est un groupe fini de cardinal q. On dit alors que g est d'ordre q et on le note
$$\mathrm{ord}(g) = q.$$

EXERCICE 2.5. Demontrer les affirmations precedentes et en particulier que

$$g^{\mathbb{Z}} = \{g^0 = e_G, g, \cdots, g^{q-1}\}$$

est fini de

2.4.3. Exemple: la conjugaison dans un groupe. Soit $(G,.)$ un groupe et $g \in G$ un element. La conjugaison par g est l'application

$$\mathrm{Ad}_g : \begin{array}{ccc} G & \mapsto & G \\ h & \mapsto & g.h.g^{-1}. \end{array}$$

PROPOSITION 2.7. *Pour tout g, l'application Ad_g est un morphisme de groupe bijectif et dont l'application reciproque vaut*

$$\mathrm{Ad}_g^{-1} = \mathrm{Ad}_{g^{-1}} : G \xrightarrow{\sim} G.$$

De plus l'application

$$\mathrm{Ad} : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{Ad}_g \end{array}$$

est un morphisme de groupes.

Preuve: Calculons (comme $g.g^{-1} = e_G$)

$$\mathrm{Ad}_g(h.h') = g.h.h'.g^{-1} = g.h.e_G.h'.g^{-1} = g.h.g.g^{-1}.h'.g^{-1} = \mathrm{Ad}_g(h).\mathrm{Ad}_g(h').$$

Verifions que Ad_g est injective en calculant son noyau:

$$\ker(\mathrm{Ad}_g) = \{h \in G, g.h.g^{-1} = e_G\}$$

mais

$$g.h.g^{-1} = e_G \Longrightarrow g.h = g \Longrightarrow h = e_G$$

(en multipliant a droite par g et a gauche par g^{-1}. Notons ensuite que pour tout $h' \in G$

$$\mathrm{Ad}_g(g^{-1}.h'.g) = g.g^{-1}.h'.g.g^{-1} = h'$$

donc $h' \in \mathrm{Im}(\mathrm{Ad}_g)$ et l'application est surjective. En fait on a pour tout $h \in G$

$$\mathrm{Ad}_{g^{-1}}(\mathrm{Ad}_g(h)) = h,\ \mathrm{Ad}_g(\mathrm{Ad}_{g^{-1}}(h)) = h$$

de sorte que $\mathrm{Ad}_{g^{-1}}$ est la reciproque de Ad_g. Ainsi $\mathrm{Ad}_g \in \mathrm{Bij}(G)$.

On a pour tout $g, g' \in G$, $h \in G$

$$\mathrm{Ad}_g \circ \mathrm{Ad}_{g'}(h) = g.g'.h.g'^{-1}.g^{-1} = \mathrm{Ad}_{g.g'}(h)$$

de sorte que

$$\mathrm{Ad}_g \circ \mathrm{Ad}_{g'} = \mathrm{Ad}_{g.g'}$$

et l'application $\mathrm{Ad} : G \mapsto \mathrm{Bij}(G)$ est bien un morphisme de groupes (dont l'image est contenue dans $\mathrm{Aut}_{Gr}(G)$). □

REMARQUE 2.4.1. Le noyau de Ad est le sous-groupe

$$\ker(\mathrm{Ad}) = \{g \in G,\ \mathrm{Ad}_g = \mathrm{Id}_G\} = \{g \in G,\ \forall h \in G,\ g.h.g^{-1} = h\}$$

$$= \{g \in G,\ \forall h \in G,\ g.h = h.g\}$$

est l'ensemble des elements de G qui commutent avec tous les elements de G, on appelle ce sous-groupe le *centre de G* et on le note

$$Z(G).$$

2.4.4. Translations dans un groupe. Soit $(G,.)$ un groupe et $g \in G$, l'application de translation a gauche par g est l'application

$$t_g : \begin{array}{ccc} G & \mapsto & G \\ g' & \mapsto & g.g'. \end{array}$$

Cette application n'est PAS un morphisme de groupe en general: elle ne l'est que si $g = e_G$. En effet si $g = e_G$, on a $t_g(g') = e_g.g' = g'$ et $t_{e_G} = \mathrm{Id}_G$. Sinon on a

$$t_g(e_G) = g.e_G = g \neq e_G$$

donc t_g, 'est pas un morphisme de groupes.

En revanche $t_g \in \mathrm{Bij}(G)$. En effet, t_g admet $t_{g^{-1}}$ comme application reciproque:

$$t_{g^{-1}} \circ t_g(g') = g^{-1}.g.g' = g'$$

et donc $t_{g^{-1}} \circ t_g = \mathrm{Id}_G$ et de meme $t_g \circ t_{g^{-1}} = \mathrm{Id}_G$.

Exercice 2.6. Montrer que l'application translation a gauche

$$t_\bullet : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & t_g \end{array}$$

est un morphisme de groupes de $(G,.)$ vers $(\mathrm{Bij}(G), \circ)$ qui est injectif. Ainsi

$$G \xrightarrow{\sim} t_G \subset \mathrm{Bij}(G)$$

et donc G est isomorphe a un sous-groupe de $\mathrm{Bij}(G)$: le groupe des translations a gauche sur l'ensemble G.

CHAPITRE 3

Anneaux et Modules

"Un Anneau pour les gouverner tous,
Un Anneau pour les trouver,
Un Anneau pour les amener tous,
Et dans les ténèbres les lier"

3.1. Anneaux

DÉFINITION 3.1. *Un anneau $(A, +, ., 0_A, 1_A)$ est la donnee, d'un groupe commutatif $(A, +)$ (note additivement) d'element neutre note 0_A, d'une loi de composition interne (dite de multiplication)*

$$\bullet.\bullet : \begin{array}{ccc} A \times A & \mapsto & A \\ (a, b) & \mapsto & a.b \end{array}$$

et d'un element unite $1_A \in A$ ayant les proprietes suivantes

(1) Associativite de la multiplication:

$$\forall a, b, c \in A,\ (a.b).c = a.(b.c) = a.b.c.$$

(2) distributivite:

$$\forall a, b, c \in A,\ (a + b).c = a.c + b.c,\ c.(a + b) = c.a + c.b.$$

(3) Neutralite de l'unite:

$$\forall a \in A,\ a.1_A = 1_A.a = a.$$

Un anneau est dit commutatif si de plus la multiplication est commutative:

$$\forall a, b \in A,\ a.b = b.a.$$

LEMME 3.1. *Pour tout $a, b \in A$, on a*

$$0_A.a = a.0_A = 0_A,$$

(on dit que l'element neutre de l'addition 0_A est absorbant*). Pour l'oppose, on a*

$$(-a).b = -(a.b) = a.(-b).$$

Preuve: Pour tout a on a

$$a = 1_A.a = (1_A + 0_A).a = a + 0_A.a$$

et donc $0_A.a = 0_A$. □

EXERCICE 3.1. Montrer que si $1'_A$ a la propriete de neutralite: $\forall a \in A,\ a.1'_A = 1'_A.a = a.$ alors $1'_A = 1_A$.

EXEMPLE 3.1.1.

(1) Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de leurs lois usuelles sont des anneaux commutatifs.

(2) L'anneau nul: Soit Nul $= \{\mathbf{0}\}$ un ensemble non-vide forme d'un seul element. On muni cet ensemble de l'addition et de la multiplication definies par

$$\mathbf{0} + \mathbf{0} := \mathbf{0},\ \mathbf{0}.\mathbf{0} := \mathbf{0}$$

alors

$$(\text{Nul}, +, ., \mathbf{0}, \mathbf{0})$$

est un anneau commutatif qu'on appelle l'anneau nul.

(3) Soit X un ensemble et $\mathcal{F}(X;\mathbb{R})$ l'ensemble des fonctions sur X a valeurs dans $\mathbb{R}$: on definit l'addition et la multiplication de deux fonctions $f, g \in \mathcal{F}(X;\mathbb{R})$ par

$$f+g : x \mapsto (f+g)(x) = f(x)+g(x),\ f.g : x \mapsto (f.g)(x) := f(x).g(x).$$

Alors si $\underline{0}$ et $\underline{1}$ sont les fonctions constantes egales a 0 et 1, $(\mathcal{F}(X;\mathbb{R}), +, ., \underline{0}, \underline{1})$ est un anneau commutatif.

Plus generalement si A est un anneau, et que

$$\underline{0_A}, \underline{1_A} : X \begin{matrix} \mapsto \\ \mapsto \end{matrix} \begin{matrix} \\ \end{matrix} {}^s_t oA$$

designent les fonctions de X vers A qui sont constantes egales respectivement a 0_A et 1_A alors

$$(\mathcal{F}(X;A), +, ., \underline{0_A}, \underline{1_A})$$

est un anneau.

(4) Soit

$$\mathbb{R}[X] = \{P(X) = a_0 + a_1.X + a_2X^2 + \cdots + a_d.X^d,\ d \geqslant 1,\ a_0, a_1, \cdots, a_d \in \mathbb{R}\}$$

l'ensemble des fonctions polynomiales a coefficients dans $\mathbb{R}$. Alors $\mathbb{R}[X]$ muni de l'addition des polynomes et de la multiplication des polynomes est un anneau dont le neutre est le polynome constant nul 0 et l'element unite est le polynome constant 1.

(5) Plus generalement pour tout anneau commutatif A on peut former l'anneau des polynomes a coefficients dans A, $A[X]$:

$$A[X] = \{P(X) = a_0 + a_1.X + a_2X^2 + \cdots + a_d.X^d,\ d \geqslant 1,\ a_0, a_1, \cdots, a_d \in A\}$$

qui est un anneau commutatif muni des lois d'addition et de multiplication des polynomes usuelles. Formellement, on ne le definit par comme l'ensemble des fonctions polynomiales de A a valeurs dans A (ce dernier anneau est en general plus petit) mais comme l'ensemble des symboles $a_0 + a_1.X + a_2X^2 + \cdots + a_d.X^d$ munis des regles usuelles d'addition et de multiplications des polynomes (voir la feuille d'exercices).

(6) L'ensemble

$$M_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in \mathbb{R}\}$$

des matrices 2×2 a coefficients dans $\mathbb{R}$ et muni des lois d'addition et de multiplication des matrices est un anneau (non-commutatif) d'element nul la matrice nulle

$$0_{M_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

et d'unite la matrice identite

$$1_{M_2(\mathbb{R})} = \mathrm{Id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(7) Soit A un anneau commutatif, l'ensemble

$$M_2(A) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in A\}$$

des matrices 2×2 a coefficients dans A et muni des lois d'addition et de multiplication des matrices est un anneau (non-commutatif) d'element nul la matrice nulle

$$0_{M_2(A)} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix}$$

et d'unite la matrice identite

$$1_{M_2(A)} = \mathrm{Id}_2 = \begin{pmatrix} 1_A & 0 \\ 0 & 1_A \end{pmatrix}.$$

(8) (Produits d'anneaux) Soient A et B des anneaux alors le produit $A \times B$ muni de l'addition et de la multiplication "coordonnee par coordonnee"

$$(a,b) + (a',b') = (a +_A a', b +_B b'),\ (a,b).(a',b') = (a._A a', b._B b')$$

est un anneau avec $(0_A, 0_B)$ comme element neutre et $(1_A, 1_B)$ comme element unite.

Exemple: l'anneau des endomorphismes d'un groupe commutatif. Soit $(M,+)$ un groupe commutatif note additivement et $\mathrm{End}(M) := \mathrm{End}_{Gr}(M)$ l'ensemble des endomorphismes de M (les morphismes de groupe de M vers M). Alors, on peut munir $\mathrm{End}(M)$ d'une structure d'anneau (non-commutatif en general):

(1) L'addition est definie comme suit (cf. Serie 2): soient $\varphi, \psi \in \mathrm{End}(M)$, on pose

$$\varphi + \psi : \begin{array}{ccc} M & \mapsto & M \\ m & \mapsto & (\varphi+\psi)(m) := \varphi(m) + \psi(m) \end{array}.$$

alors $\varphi + \psi \in \mathrm{End}(M)$ est bien un morphisme de groupes;

(2) On definit l'oppose pour l'addition par

$$-\varphi : \begin{array}{ccc} M & \mapsto & M \\ m & \mapsto & (-\varphi)(m) := -\varphi(m) \end{array}$$

et on verifie que $-\varphi$ est encore un morphisme de groupes.

(3) Ainsi $(\mathrm{End}(M), +)$ forme un groupe commutatif dont l'element neutre est le morphisme nul:

$$\underline{0}_M : m \in M \mapsto 0_M.$$

(4) La multiplication des endomorphismes est definie par la composition des applications:

$$\varphi \circ \psi : m \in M \mapsto \varphi \circ \psi(m) = \varphi(\psi(m)).$$

qui est encore un morphisme de groupes par le chapitre precedent.

On verifie alors en prenant comme element unite l'application identite de M:

$$\mathrm{Id}_M : m \in M \mapsto m \in M$$

que

$$(\mathrm{End}(M), +, \circ, \underline{0}_M, \mathrm{Id}_M)$$

forme un anneau.

3.1.1. Elements inversibles.

Définition 3.2. *Soit A un anneau. Un element $a \in A$ est inversible si il existe $b \in A$ tel que*

$$a.b = b.a = 1_A.$$

On dit alors que b est un inverse (a gauche et a droite) de a (pour la multiplication).

Proposition 3.1. *(Unicite de l'inverse) Soit A un anneau et $a \in A$ un element inversible et soit b tel que $a.b = b.a = 1_A$.*

Soit b' verifiant

$$a.b' = 1_A$$

alors $b' = b$; de meme si b' verifie

$$b'.a = 1_A$$

alors $b' = b$

Preuve: Supposons que a est inversible avec $a.b = b.a = 1_A$ et soit $b' \in A$ tel que

$$a.b' = 1_A$$

alors

$$a.b' = 1_A \Longrightarrow b.a.b' = b = 1_A.b' = b'.$$

□

NOTATION 3.1. *Par la Proposition precedente si un element $a \in A$ est inversible son inverse est unique. On notera cet inverse*

$$a^{-1}.$$

Notons que a^{-1} est egalement inversible et on a

$$(a^{-1})^{-1} = a.$$

On deduit de cette discussion que

PROPOSITION 3.2. *Soit $A^\times$ l'ensemble des elements inversibles d'un anneau A, alors*

$$(A^\times, ., 1_A, \bullet^{-1})$$

forme un groupe: le groupe des elements inversibles de A.

REMARQUE 3.1.1. Rappelons que l'on utilise la notations additive pour le groupe commutatif $(A, +)$. En particulier pour tout $a \in A$, l'element $-a$ ("l'inverse" de a pour la loi $+$) sera appele l'oppose de a:

$$a + (-a) = (-a) + a = 0_A.$$

On reservera le terme "inverse" a la multiplication.

REMARQUE 3.1.2. Par une perversite du vocabulaire, le groupe $A^\times$ est egalement appele le groupe des *unites* de A et ses elements sont des *unites* de A. Quand on voudra parler d'un element a inversible on parlera d'une "unite" de A et on reservera le terme "l'unite de A" a l'element 1_A.

EXEMPLE 3.1.2.

(1) On a

$$\mathbb{Z}^\times = \{+1, -1\},\ \mathbb{Q}^\times = \mathbb{Q} - \{0\}, \mathbb{R}^\times = \mathbb{R} - \{0\}, \mathbb{C}^\times = \mathbb{C} - \{0\}.$$

par exemple 2 n'est pas inversible dans $\mathbb{Z}$ car son inverse $1/2$ n'est pas entier mais il est inversible dans $\mathbb{Q}$.

(2) On a

$$\mathrm{Nul}(A)^\times = \{0_A\}.$$

(3) Les matrices inversibles de $\mathbb{R}$ sont celles dont le determinant est inversible:

(4) $M_2(\mathbb{R})^\times = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in \mathbb{R},\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in \mathbb{R}^\times = \mathbb{R} - \{0\}\}$.

(5) Si $(M, +)$ est un groupe commutatif et $\mathrm{End}(M) = \mathrm{End}_{Gr}(M)$ est son anneau d'endomorphismes, le groupe des unites de $\mathrm{End}(M)$ est

$$\mathrm{End}(M)^\times = \mathrm{Aut}_{Gr}(M)$$

le groupe des automorphismes du groupe $(M, +)$.

(6) Si A et B sont des anneaux, le groupe des elements inversibles du produit $A \times B$ est

$$(A \times B)^\times = A^\times \times B^\times.$$

EXERCICE 3.2. Soit A un anneau commutatif et $M_2(A)$ l'anneau des matrices a coefficients dans A. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$, une matrice des cofacteurs de M est la matrice definie par

$$\mathrm{cof}(M) := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(1) Montrer que

$$M.\mathrm{cof}(M) = \mathrm{cof}(M).M = \det(M).\mathrm{Id}_2 = \begin{pmatrix} \det(M) & 0 \\ 0 & \det(M) \end{pmatrix}$$

ou $\det(M)$ (le determinant de M) est defini par

$$\det(M) := ad - bc \in A.$$

(2) En deduire que

$$M_2(A)^\times = \mathrm{GL}_2(A) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a,b,c,d \in A,\ \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in A^\times\}.$$

3.1.2. Sous-anneau.

DÉFINITION 3.3. *Soit $(A,+,.)$ un anneau. Un sous-anneau $B \subset A$ est un sous-groupe de $(A,+)$ qui est*

- *soit le sous-groupe trivial $\{0_A\}$,*
- *soit qui contient l'unite 1_A et qui est stable par multiplication:*

$$\forall b, b' \in B,\ b.b' \in B.$$

Ainsi $(B,+,.,0_A,1_A)$ est un anneau.

PROPOSITION 3.3. *(Critere de sous-anneau) Soit $(A,+,.)$ un anneau et $B \subset A$ un sous-ensemble non-vide; alors B est un sous-anneau ssi $B = \{0_B\}$, ou bien $1_A \in B$ et*

$$\forall b, b', b'' \in B,\ b.b' - b'' \in B \tag{3.1.1}$$

Preuve: Exercice. □

EXEMPLE 3.1.3. (1) La chaine d'inclusions

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

est une chaine de sous-anneaux de $\mathbb{C}$.

(2) L'ensemble des matrices scalaires

$$\mathbb{R}.\mathrm{Id}_2 = \{\lambda.\mathrm{Id}_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},\ \lambda \in \mathbb{R}\}$$

est un sous-anneau de $M_2(\mathbb{R})$.

(3) Plus generalement pour tout anneau commutatif,

$$A.\mathrm{Id}_2 = \{a.\mathrm{Id}_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},\ a \in A\} \subset M_2(A)$$

est un sous-anneau.

(4) La chaine d'inclusions

$$M_2(\mathbb{Z}) \subset M_2(\mathbb{Q}) \subset M_2(\mathbb{R}) \subset M_2(\mathbb{C})$$

est une chaine de sous-anneaux.

3.1.3. Morphismes d'anneaux.

DÉFINITION 3.4. *Soient $(A,+,.)$, $(B,+,.)$ des anneaux. Un morphisme d'anneaux $\varphi : A \mapsto B$ est un morphisme de groupes commutatif $\varphi : (A,+) \mapsto (B,+)$ tel que*

$$\varphi(1_A) = 1_B \text{ ou bien } \varphi(1_A) = 0_B,$$
$$\forall a, a' \in A,\ \varphi(a.a') = \varphi(a).\varphi(a').$$

REMARQUE 3.1.3. Si $\varphi(1_A) = 0_B$ alors φ est l'application constante nulle $\underline{0}_B$:

$$\forall a \in A,\ \varphi(a) = \varphi(a).\varphi(1_A) = 0_B.$$

NOTATION 3.2. *L'ensemble des morphismes d'anneaux de A vers B est note*

$$\mathrm{Hom}_{Ann}(A,B).$$

L'ensemble des morphismes d'anneaux de A vers lui-meme est note

$$\mathrm{End}_{Ann}(A)=\mathrm{Hom}_{Ann}(A,A)$$

est est appelle l'ensemble des endomorphismes *de A.*

Le morphisme canonique. Le morphisme canonique associe a un anneau A est l'application

$$\mathrm{Can}_A:\begin{array}{ccc}\mathbb{Z}&\mapsto&A\\ n&\mapsto&n.1_A\end{array}$$

ou

$$n.1_A=\begin{cases}0 & \text{si } n=0\\ 1_A+\cdots+1_A(n \text{ fois}) & \text{si } n>0\\ -(1_A+\cdots+1_A)(|n| \text{ fois}) & \text{si } n<0.\end{cases}$$

EXERCICE 3.3. On a deja vu que Can_Aest un morphisme de groupes commutatifs (pour l'addition). Verifier que c'est un morphisme d'anneaux.

3.1.4. Noyau, Image.

PROPOSITION 3.4. *(Stabilite par morphismes) Soient $\varphi\in\mathrm{Hom}_{Ann}(A,B)$ un morphisme alors $\varphi(A)\subset B$ est un sous-anneau. Par ailleurs le sous-groupe* $\ker(\varphi)$ *est stable par multiplication par A:*

$$\forall a\in A, k\in\ker(\varphi),\ a.k\in\ker(\varphi).$$

Preuve: On sait deja que $\varphi(A)$ est un sous-groupe de $(B,+)$. Si $\varphi(A)$ n'est pas l'anneau nul alors $1_B=\varphi(1_A)\in\varphi(A)$ et pour tout $b,b'\in\varphi(A)$, on a $b=\varphi(a),\ b'=\varphi(a')$ pour $a,a'\in A$ et

$$b.b'=\varphi(a).\varphi(a')=\varphi(a.a')\in\varphi(A)$$

ainsi $\varphi(A)$ est stable par produit.

On a $\forall, a\in A,\ k\in\ker(\varphi)$,

$$\varphi(a.k)=\varphi(a).\varphi(k)=\varphi(a).0_B=0_B$$

donc $a.k\in\ker(\varphi)$. □

REMARQUE 3.1.4. Notez que $\ker(\varphi)$ est PAS un sous-anneau en general : il ne contient pas 1_A sauf si $1_B=0_B$ (c'est a dire sauf si B est l'anneau nul).

Comme φ est un morphisme de groupes additifs on a

PROPOSITION 3.5. *Un morphisme d'anneaux $\varphi\in\mathrm{Hom}_{Ann}(A,B)$ est injectif ssi* $\ker(\varphi)=\{0_A\}$.

PROPOSITION 3.6. *Soient $\varphi:A\mapsto B$ et $\psi:B\mapsto C$ des morphismes d'anneaux alors*

- *$\psi\circ\varphi:A\mapsto C$ est un morphisme d'anneaux.*
- *Soit $\varphi\in\mathrm{Hom}_{Ann}(A,B)$ un morphisme d'anneaux bijectif, l'application reciproque $\varphi^{-1}:B\mapsto A$ est un morphisme d'anneaux. On dit que φ un isomorphisme d'anneaux et on dit que A et B sont des anneaux isomorphes.*

Preuve: Exercice. □

NOTATION 3.3. *On note*

$$\mathrm{Hom}_{Ann}(A,B),\mathrm{End}_{Ann}(A)=\mathrm{Hom}_{Ann}(A,A)$$

$$\mathrm{Isom}_{Ann}(A,B),\ \mathrm{Aut}_{Ann}(A)=\mathrm{Isom}_{Ann}(A,A)$$

l'ensemble des morphismes, endomorphismes, isomorphismes et automorphismes d'anneaux.

EXERCICE 3.4. L'ensemble des automorphismes $\mathrm{Aut}_{Ann}(A)$ muni de la composition forme un sous-groupe de $\mathrm{Bij}(A)$.

3.2. Modules sur un anneau

DÉFINITION 3.5. *Soit $(A,+,.)$ un anneau, un A-module (a gauche) est un groupe commutatif $(M,+)$ muni d'une loi de multiplication externe*

$$\bullet * \bullet : \begin{array}{ccc} A \times M & \mapsto & M \\ (a,m) & \mapsto & a*m \end{array}$$

(appellee multiplication par les scalaires) ayant les proprietes suivantes:

(1) Associativite: $\forall a, a' \in A,\ m \in M,$

$$(a.a') * m = a * (a' * m).$$

(2) Distributivite: $\forall a, a' \in A,\ m, m' \in M,$

$$(a+a') * m = a*m + a'*m,\ a*(m+m') = a*m + a*m'.$$

(3) Neutralite de 1_A*:* $\forall m \in M,$

$$1_A * m = m.$$

EXERCICE 3.5. Soit M un A-module. Montrer que

$$0_A * m = 0_M,\ (-1_A) * m = -m \text{ (ie. l'oppose de } m \text{ dans } (M,+).$$

EXEMPLE 3.2.1. Quelques exemples de modules sur des anneaux:

(1) Un anneau A est un A-module sur lui-meme pour la multiplication.
(2) Le singleton element neutre $\{0_A\}$ est un A-module: le module nul.
(3) Soit M un groupe abelien alors M est naturellement un $\mathbb{Z}$-module pour la loi de multiplication par les scalaires donnee par

$$n.m = \begin{cases} m+m+\cdots+m \ (n \text{ fois si } n \geqslant 0), \\ (-m)+(-m)+\cdots+(-m) \ (-n \text{ fois si } n \leqslant 0) \end{cases}$$

(4) Soit $d \geqslant 1$, le produit cartesien

$$A^d = A \times \cdots \times A = \{(a_1, \cdots, a_d),\ a_i \in A,\ i = 1, \cdots d\}$$

est un A-module avec la loi de groupes

$$(a_1, \cdots, a_d) + (a'_1, \cdots, a'_d) = (a_1 + a'_1, \cdots, a_d + a'_d)$$

et la multiplication par les scalaires

$$a.(a_1, \cdots, a_d) = (a.a_1, \cdots, a.a_d).$$

On dit que A^d est un A-module libre de rang d.
(5) Soit $\varphi : A \mapsto B$ un morphisme d'anneaux alors $\ker(\varphi) \subset A$ est un A-module pour la multiplication dans A.
(6) Soit A un anneau, X un ensemble et $\mathcal{F}(X;A)$ l'ensemble des fonction de X a valeurs dans A . On a vu que $\mathcal{F}(X;A)$ a une structure d'anneau; il a egalement une structure de A-module: on definit la multiplication externe d'un element $a \in A$ et d'une fonction $f : X \mapsto A$ par

$$a.f : x \mapsto (a.f)(x) = a.(f(x)).$$

(7) Soit A un anneau et $A[X]$ l 'anneau des polynomes alors $A[X]$ est naturellement un A-module pour la multiplications d'un polynome par un scalaire: si $P(X) = a_0 + \cdots + a_d.X^d$ alors la multiplication par les scalaires est donnee par

$$a.P(X) = a.a_0 + a.a_1.X + \cdots + a.a_d.X^d.$$

(8) Soit A un anneau et

$$A[X]_{\leqslant d} = \{a_0 + \cdots + a_d.X^d,\ a_0, \cdots, a_d \in A\}$$

l 'anneau des polynomes de degre $\leqslant d$ alors $A[X]_{\leqslant d}$ est naturellement un A-module (par contre ce n'est pas un anneau –sauf si $d = 0$: les polynomes constants c'est adire l'anneau A– car il n'est pas stable par produit en general).

Les exemples (6) et (7) sont des cas particulier de ce qu'on appelle une A-algebre:

DÉFINITION 3.6. *Une A-algebre est anneau $(B, +_B, .B)$ possedant une structure de A-module qui verifie la propriete d'associativite suivante pour les multiplications:*

$$\forall a \in A,\ b, b' \in B\ a * (b._B b') = (a * b)._B b'.$$

3.2.1. Sous-module.

DÉFINITION 3.7. *Soit M un A -module. Un sous-module $N \subset M$ d'un A-module M est un sous-groupe de $(M, +)$ qui est stable pour la multiplication par les scalaires:*

$$\forall a \in A,\ n \in N,\ a * n \in N.$$

On a donc $\forall n, n' \in N$, $a, a' \in A$

$$a * n + a' * n' \in N$$

On a le critere suivant

PROPOSITION 3.7. *(Critere de sous-module) Soit $N \subset M$ un sous-ensemble d'un A-module M alors N est un sous-module de M ssi*

$$\forall a \in A,\ n, n' \in N,\ a * n + n' \in N. \tag{3.2.1}$$

Preuve: Pour tout $n, n' \in N$, et applicant la condition (3.2.1) a n, n' et $a = -1_A$ on a

$$n + (-1_A) * n' = n - n' \in N$$

donc N verifie le critere de sous-groupe et est donc un sous-groupe de $(M, +)$. Il contient en particulier 0_M et alors pour tout $a \in A$, on a par (3.2.1)

$$a * n + 0_M = a * n \in N.$$

□

EXEMPLE 3.2.2. Exemples de sous-modules

(1) L'element nul $\{0_M\}$ forme un sous-module de M: le sous-module nul.
(2) Soit A^d le module libre de rank d et

$$\Delta A = \{(a, a \cdots, a) = a.(1, 1, \cdots, 1),\ a \in A\} \subset A^d$$

est un sous-module de A^d. Plus generalement pour tout $\vec{a} = (a_1, \cdots, a_d) \in A^d$ le sous-ensemble des multiples de $\vec{a}$

$$A.\vec{a} = \{a.\vec{a} = (a.a_1, \cdots, a.a_d),\ a \in A\}$$

est un sous-module de A^d.
(3) Soit $1 \leqslant d \leqslant d'$ alors

$$A[X]_{\leqslant d} \subset A[X]_{\leqslant d'} \subset A[X]$$

est un chaine de sous A-modules.

3.2.2. Ideal. Un exemple important de sous-module sont ceux contenus dans A, on les appelle des *ideaux* de A:

DÉFINITION 3.8. *Un ideal de A est un sous-ensemble $I \subset A$ qui est un sous-module du A module A (pour la multiplication dans A). De maniere equivalente, un ideal de A est un sous-groupe additif $(I,+) \subset (A,+)$ qui est stable par multiplication par les elements de A:*

$$\forall a \in A,\ b \in I,\ a.b \in I.$$

EXEMPLE 3.2.3. Soit $\varphi : A \mapsto B$ un morphisme d'anneaux montrer que $\ker(\varphi)$ est un ideal de A.

3.2.3. Module engendre par un ensemble.

PROPOSITION 3.8. *Soit $(M,+,*)$ un A-module et M_1, M_2 des sous-modules alors*

$$M_1 \cap M_2 \subset M$$

est un sous-module et plus generalement soit $(M_i)_{i\in I}$ une collection de sous-modules alors

$$\bigcap_{i\in I} M_i \subset M$$

est un sous-module.

DÉFINITION 3.9. *Soit $X \subset M$ un sous-ensemble d'un A-module, le module engendre par X est le plus petit sous-module de M contenant X (l'intersection de tous les sous-modules contenant X):*

$$\langle X \rangle := \bigcap_{X\subset N\subset M} N.$$

PROPOSITION 3.9. *Soit $X \subset M$ un ensemble alors $\langle X\rangle$ est soit le module nul $\{0_M\}$ si X est vide, soit l'ensemble des combinaisons lineaires d'elements de X a coefficients dans A:*

$$\langle X\rangle = \mathrm{CL}_A(X) := \{\sum_{i=1}^{n} a_i * x_i,\ n \geqslant 1,\ a_1,\cdots,a_n \in A,\ x_1,\cdots,x_n \in X\}.$$

Preuve: On suppose X non-vide. Soit $X \subset N$ un sous-module contenant X alors pour tout $n \geqslant 1$, tous $a_1,\cdots,a_n \in A$ et tout $x_1,\cdots,x_n \in X$ on a

$$a_1 * x_1 + \cdots + a_n * x_n \in N$$

par stabilite de N par $+$ et $*$. Donc tout sous-module N contenant X contient $\mathrm{CL}_A(X)$.

Il reste a montrer que $\mathrm{CL}_A(X)$ est un sous-module: soient u et u' des combinaison lineaires d'elements de X:

$$u = a_1 * x_1 + \cdots + a_n * x_n,\ u' = a'_1 * x'_1 + \cdots + a'_{n'} * x'_{n'}$$

alors

$$u + u' = a_1 * x_1 + \cdots + a_n * x_n + a'_1 * x'_1 + \cdots + a'_{n'} * x'_{n'}$$

est bien une combinaison lineaire. De plus $\mathrm{CL}_A(X)$ est stable par multiplication par A: pour tout $a \in A$ on a par distributivite et associativite

$$a * u = a * (a_1 * x_1 + \cdots + a_n * x_n) = (a.a_1) * x_1 + \cdots + (a.a_n) * x_n$$

est bien une combinaison lineaire. □

DÉFINITION 3.10. *Si $\langle X\rangle = M$, on dit que X est une famille generatrice de M.*

DÉFINITION 3.11. *Un A-module M est de type fini si il possede une famille generatrice qui est finie.*

EXEMPLE 3.2.4. (1) Soit A^d le A-module libre de rang d. La famille suivante est generatrice de A^d (on pose $1 = 1_A, 0 = 0_A$)

$$\mathscr{B}^0 := \{\mathbf{e}_1^0 = (1, 0, \cdots, 0),\ \mathbf{e}_2^0 = (0, 1, 0, \cdots, 0), \cdots, \mathbf{e}_d^0 = (0, 0, \cdots, 1)\}$$

($\mathbf{e}_i^0$ est le d-uple dont toutes les coordonnees sont nulles sauf la i-ieme qui vaut 1). En effet si

$$m = (a_1, \cdots, a_d) \in A^d$$

alors

$$m = a_1.\mathbf{e}_1^0 + \cdots + a_d.\mathbf{e}_d^0.$$

On appelle la famille $\mathscr{B}^0$ *la base canonique* de A^d.

(2) La famille des monomes

$$\{1, X, \cdots, X^d, \cdots X^{d+1}, \cdots\}$$

est une famille generatrice (infinie) de $A[X]$.

(3) La famille des monomes de degre $\leqslant d$

$$\{1, X, \cdots, X^d\}$$

est une famille generatrice de $A[X]_{\leqslant d}$ (qui est donc un module de type fini)

EXERCICE 3.6. Soient $u_1, \cdots, u_d \in A^\times$ des elements inversibles. Montrer que la famille suivante est generatrice de A^d

$$\mathscr{B} := \{\mathbf{e}_1 = (u_1, 0, \cdots, 0),\ \mathbf{e}_2 = (0, u_2, 0, \cdots, 0), \cdots, \mathbf{e}_d = (0, 0, \cdots, u_d)\}$$

EXERCICE 3.7. Soient $a, b, c, d \in \mathbb{Z}$ tels que $ad - bc = \pm 1$. Montrer que $\{(a, b), (c, d)\}$ engendre le $\mathbb{Z}$-module $\mathbb{Z}^2$. Pour cela on montrera que pour tout $(m, n) \in \mathbb{Z}^2$ le systeme lineaire

$$\begin{cases} ax + cy = m \\ bx + dy = n \end{cases}$$

admet une (unique) solution $(x, y) \in \mathbb{Z}^2$ et on montrera que (m, n) s'exprime en fonction de (a, b) et (c, d).

3.2.4. Morphismes de modules.

DÉFINITION 3.12. *Soit A un anneau et M, N des A-modules, un morphisme de A-modules entre M et N est un morphisme de groupes*

$$\varphi : M \mapsto N$$

qui est compatible avec les lois de multiplications externes $*_M$ et $*_N$:

$$\forall a \in A,\ m \in M,\ \varphi(a *_M m) = a *_N \varphi(m).$$

REMARQUE 3.2.1. Cette definition implique que pour tout $a, a' \in A$, $m, m' \in M$, on a

$$\varphi(a *_M m + a' *_M m') = a *_N \varphi(m) + a' *_N \varphi(m').$$

On dit que φ est une *application A-lineaire.*

LEMME 3.2. *(Critere d'application lineaire) Soit $\varphi : M \mapsto N$ une application entre deux sous-modules alors φ est un morphisme (ie. est A-lineaire) si et seulement si*

$$\forall a \in A,\ m, m' \in M,\ \varphi(a *_M m + m') = a *_N \varphi(m) + \varphi(m'). \tag{3.2.2}$$

Preuve: On applique (3.2.2) avec $a = 1_A$. On a donc

$$\forall m, m' \in M,\ \varphi(m + m') = \varphi(m) + \varphi(m')$$

donc φ est un morphisme de groupes. On a donc $\varphi(0_M) = 0_N$ et

$$\varphi(a *_M m) = \varphi(a *_M m + 0_M) = a *_N \varphi(m) + 0_N = a *_N \varphi(m).$$

□

3.2.5. Noyau, Image.

PROPOSITION 3.10. *Soit $\varphi : M \mapsto N$ un morphisme de A-modules et $M' \subset M$ et $N' \subset N$ des sous-modules alors*

$$\varphi(M') \subset N \text{ et } \varphi^{-1}(N') \subset M$$

sont des sous-modules de M et N respectivement. En particulier

$$\ker(\varphi) = \varphi^{-1}(\{0_N\}) \subset M \text{ et } \mathrm{Im}(\varphi) = \varphi(M) \subset N$$

sont des sous A-modules.

Preuve: Exercice. □

Comme un morphisme de A-module est un morphisme de groupes additifs on a

COROLLAIRE 3.1. *L'application A-lineaire $\varphi : M \mapsto M'$ est injective ssi* $\ker(\varphi) = \{0_M\}$.

3.2.6. Structure des espaces de morphismes.

NOTATION 3.4. *On note*

$$\mathrm{Hom}_{A-mod}(M,N),\ \mathrm{Isom}_{A-mod}(M,N),$$
$$\mathrm{End}_{A-mod}(M) = \mathrm{Hom}_{A-mod}(M,M),$$
$$\mathrm{Aut}_{A-mod}(M) = \mathrm{GL}_{A-mod}(M) = \mathrm{Isom}_{A-mod}(M,M)$$

les ensemble de morphismes, morphismes bijectifs (ou isomorphismes), d'endomorphismes et d'automorphismes des A-modules M et N.

On a les proprietes de stabilites usuelles pour la composition (similaires a celles pour les morphismes de groupes)

PROPOSITION 3.11. *Soient $\varphi : L \mapsto M$ et $\psi : M \mapsto N$ des morphismes de A-modules alors*

- *$\psi \circ \varphi : L \mapsto N$ est un morphisme de A-modules.*
- *Si $\varphi : L \mapsto M$ est bijectif alors $\varphi^{-1} : M \mapsto L$ est un morphisme de A-modules.*

Preuve: Exercice. □

En particulier on a

COROLLAIRE 3.2. *L'ensemble* $\mathrm{Aut}_{A-mod}(M) \subset \mathrm{Bij}(M)$ *est un sous-groupe de* $\mathrm{Bij}(M)$. *Plus precisement* $\mathrm{Aut}_{A-mod}(M)$ *est un sous-groupe de* $Aut_{Gr}(M)$.

On a un propriete supplementaire de stabilite par somme:

PROPOSITION 3.12. *Soient M et N des A-modules alors* $\mathrm{Hom}_{A-mod}(M,N)$ *a une structure naturelle de groupe commutatif. Si de plus A est commutatif alors* $\mathrm{Hom}_{A-mod}(M,N)$ *a une structure naturelle de A-module.*

Preuve: Soient $\varphi, \psi \in \mathrm{Hom}_{A-mod}(M,N)$, on definit l'addition par

$$\varphi + \psi : m \mapsto (\varphi + \psi)(m) = \varphi(m) + \psi(m) \in N.$$

C'est un morphisme de A-module car N est un A-module:

$$\begin{aligned}(\varphi+\psi)(a*m+m') &= \varphi(a*m+m') + \psi(a*m+m') \\ &= a*\varphi(m) + \varphi(m') + a*\psi(m) + \psi(m') = a*(\varphi+\psi)(m) + (\varphi+\psi)(m').\end{aligned}$$

et on definit l'oppose $-\varphi$ en posant

$$-\varphi(m) = -(\varphi(m)) \in N$$

et on verifie a nouveau que $-\varphi$ est A-lineaire. L'element neutre est le morphisme nul:

$$\underline{0}_N : m \in M \mapsto 0_N$$

et c'est une application A-lineaire:

$$\forall a \in a, m \in M, \underline{0}_N(a * m) = 0_N = a * \underline{0}_N(m).$$

Supposons que A soit commutatif: on definit la multiplication par les scalaires en posant pour $a \in A$

$$a * \varphi : m \mapsto (a * \varphi)(m) := a *_N (\varphi(m)).$$

C'est un morphisme de A-modules: pour $a' \in A$, on a

$$a * \varphi(a' *_M m + m') = a *_N (\varphi(a' *_M m + m')) = a *_N (a'_N * \varphi(m) + \varphi(m'))$$

$$= (a.a')_N * \varphi(m)) + a_N * \varphi(m') = (a'.a)_N * \varphi(m)) + a * \varphi(m') = a'_N * (a * \varphi)(m) + (a * \varphi)(m').$$

Ici on a utilise le fait que A est commutatif et donc $a.a' = a'.a$. □

3.2.7. L'algebre des endomorphismes d'un module. On a vu que l'ensemble des endomorphisme du groupe additif $\mathrm{End}_{Gr}(M)$ muni de la composition et de l'addition est un anneau. Pour les morphismes de A-modules on a

THÉORÈME 3.1. *Soit M un A-module. L'ensemble $\mathrm{End}_{A-mod}(M)$ des endomorphismes de M comme A-module est un sous-anneau de $(\mathrm{End}_{Gr}(M), +, \circ)$ dont le groupe des unites est $\mathrm{Aut}_{A-mod}(M)$. C'est l'anneau des endomorphismes de (du A-module) M.*

De plus, si A est commutatif, $\mathrm{End}_{A-mod}(M)$ possede une structure naturelle de A-module qui en fait une A-algebre et $\mathrm{End}_{A-mod}(M)$ est appellee

algebre des endomorphismes de (du A-module) M.

Preuve: D'abord Id_M et l'application constante nulle $\underline{0}_M$ qui sont des morphismes de groupes sont egalement des morphismes de A-module:

$$\forall a \in a, m \in M,\ \mathrm{Id}_M(a * m) = a * m = a * \mathrm{Id}_M(m),\ \underline{0}_M(a * m) = 0_M = a * \underline{0}_M(m).$$

On a vu que $\mathrm{End}_{A-mod}(M)$ est stable par composition et on a vu que la somme de deux endomorphismes est encore un endomorphisme de A-module. Ainsi $\mathrm{End}_{A-mod}(M)$ est un sous-anneau de $\mathrm{End}_{Gr}(M)$.

Si A est commutatif on a vu que $\mathrm{End}_{A-mod}(M) = \mathrm{Hom}_{A-mod}(M, M)$ possede une multiplication par les scalaires qui en fait un A-module ce qui fait de cet anneau une A-algebre: en effet pour tout $\varphi, \psi \in \mathrm{End}_{A-mod}(M)$ et $a \in A$, on a pour $m \in M$

$$a.(\varphi \circ \psi)(m) = a.\varphi(\psi(m)) = (a.\varphi)(\psi(m)) = (a.\varphi) \circ \psi(m)$$

de sorte que

$$a.(\varphi \circ \psi) = (a.\varphi) \circ \psi.$$

□

CHAPITRE 4

Corps

"Le corps conditionnne le raisonnement."

4.1. Corps

DÉFINITION 4.1. *Un corps K est un anneau commutatif possedant au moins deux elements $0_K \neq 1_K$ et tel que tout element non-nul est inversible:*

$$K^\times = K - \{0_K\}.$$

REMARQUE 4.1.1. Dans cette definition, on demande que K soit commutatif. Il existe des anneaux non-commutatifs dont l'ensemble des elements inversibles sont exactement les elements non-nuls. On les appelle *corps gauche* ou *algebres a divisions*.

EXEMPLE 4.1.1. On a

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps; $\mathbb{Z}$ n'en est pas un (par exemple 2 n'est pas inversible dans $\mathbb{Z}$).
(2) $M_2(\mathbb{R})$ n'est pas un corps (gauche): la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est non-nulle mais pas inversible.

Comme on va le voir, le fait, dans un corps, de pouvoir inverser tous les elements non-nuls simplifie considerablement la theorie. Par exemple on a

PROPOSITION 4.1. *Soit K un corps, B un anneau et $\varphi \in \mathrm{Hom}_{Ann}(K, B)$ un morphisme. Alors si φ n'est pas nul ($\varphi \neq \underline{0}_B$) φ est injectif:*

$$\varphi : K \hookrightarrow B.$$

Preuve: Supposons que φ n'est pas nul. Il s'agit de montrer que $\ker \varphi = \{0_K\}$. Soit $x \in K - \{0\}$, alors x est inversible et soit x^{-1} son inverse. On a

$$\varphi(x.x^{-1}) = \varphi(1_K) = \varphi(x).\varphi(x^{-1})$$

et comme $\varphi \not\equiv 0_B$, $\varphi(1_K) = 1_B \neq 0_B$ et $\varphi(x) \neq 0$ et donc $x \notin \ker(\varphi)$. □

REMARQUE 4.1.2. On a meme mieux: si $x \in K - \{0\}$ alors $\varphi(x)$ est inversible dans B, d'inverse

$$\varphi(x)^{-1} = \varphi(x^{-1}).$$

4.2. Corps des fractions

Etant donne un anneau A, sous certaines hypotheses, on peut construire un corps K (le plus petit possible) dont A est peut etre considere comme un sous-anneau. En particulier si $a \in A - \{0\}$ alors il existe $a^{-1} \in K$ tel que $a.a^{-1} = 1_A = 1_K$. Pour cela il faut que A satisfasse une propriete particuliere: etre *integre*.

LEMME 4.1. *Soit $\{0\} \neq A \subset K$ un sous anneau non-nul d'un corps K alors A est commutatif et*

$$\forall a, b \in A,\ a.b = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0. \tag{4.2.1}$$

Preuve: A est commutatif car K est commutatif. Pour (4.2.1) seule la direction $\Longrightarrow$ est non evidente: supposons que $a, b \neq 0$ alors il existe $a^{-1} \in K$ tel que $a^{-1}.a = 1_K$ mais alors on a

$$a.b = 0 \Longrightarrow a^{-1}.a.b = 0_K = b,$$

contradiction. □

DÉFINITION 4.2. *Un anneau A non-nul, commutatif, tel que $\forall a, b \in A$ on ait*

$$a.b = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0$$

est dit integre.

REMARQUE 4.2.1. En particulier un corps est integre: appliquer le lemme precedent a $A = K$.

PROPOSITION 4.2. *Soit A un anneau integre (en particulier commutatif) , alors il existe un corps K et un morphisme d'anneau injectif*

$$\iota_K : A \hookrightarrow K$$

(de sorte qu'on peut considerer A comme un sous-anneau de K en identifiant A a $\iota(A) \subset K$) et tel que K a la propriete de minimalite suivante: pour tout corps K' et tout morphisme injectif

$$\iota_{K'} : A \hookrightarrow K'$$

(de sorte que A peut etre identifie a un sous-corps de K'), il existe un morphisme (necessairement injectif)

$$\iota' : K \hookrightarrow K'$$

prolongeant le morphisme $\iota_{K'}$ (ainsi A et K peuvent etre vus comme des sous-anneaux de K').

REMARQUE 4.2.2. "Prolonge" signifie que

$$\iota_{K'} = \iota' \circ \iota_K :$$

pour tout $a \in A$, on a

$$\iota_{K'}(a) = \iota'(\iota_K(a)).$$

Preuve: Soit A un anneau integre. On considere le produit cartesien

$$A \times (A - \{0\}) = \{(a, b),\ a, b \in A,\ b \neq 0\}.$$

On definit sur $A \times (A - \{0\})$ une relation $\sim$ en posant

$$(a, b) \sim (a', b') \Longleftrightarrow a.b' = a'.b.$$

Cette relation est une relation d'equivalence (reflexive, symetrique, transitive). En effet

- reflexive: $(a, b) \sim (a, b)$ car $ab = ab$.
- symetrique: $(a, b) \sim (a', b') \Longleftrightarrow a'b = ab' \Longleftrightarrow (a', b') \sim (a, b)$
- transitive: si $(a, b) \sim (a', b')$ et $(a', b') \sim (a'', b'')$, alors on a

  $$a.b' = a'.b,\ a'.b'' = a''.b'$$

  et comme A est commutatif

  $$a.b''.b' = a.b'.b'' = a'.b.b'' = a''.b'.b = a''.b.b'.$$

  On a donc

  $$0_A = a.b''.b' - a''.b.b' = (a.b'' - a''.b).b'$$

  et comme A est integre et $b' \neq 0$ on a

  $$a.b'' - a''.b = 0_A \Longleftrightarrow a.b'' = a''.b \Longleftrightarrow (a, b) \sim (a'', b'').$$

On note

$$K = \mathrm{Frac}(A) = A \times (A - \{0\})/\sim$$

l'ensemble des classes d'equivalence et on note

$$\frac{a}{b} \in K$$

la classe d'equivalence de la paire (a, b). On l'appelle la fraction $\frac{a}{b}$ de numerateur a et de denominateur b.

On munit $\mathrm{Frac}(A)$ d'une structure d'anneau en posant

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd},\ \frac{a}{b}.\frac{c}{d} = \frac{ac}{bd},\ -\frac{a}{b} = \frac{-a}{b}$$

$$0_K = \frac{0}{1},\ 1_K = \frac{1}{1}.$$

Notons que comme A est integre, si b et d sont non-nuls et produit $b.d$ est non-nul et

$$(a.d + b.c, b.d), (a.c, b.d) \in A \times (A - \{0\}).$$

On verifie premierement que ces definitions ne dependent pas du choix des representants de chaque classe d'equivalence: si $\frac{a}{b} = \frac{a'}{b'}$ et $\frac{c}{d} = \frac{c'}{d'}$ cad si

$$(a, b) \sim (a', b'),\ (c, d) \sim (c', d')$$

alors

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'}$$

et

$$\frac{a}{b}.\frac{c}{d} = \frac{a.c}{b.d} = \frac{a'.c'}{b'.d'} = \frac{a'}{b'}.\frac{c'}{d'}$$

c'est a dire que

$$(ad + bc, bd) \sim (a'd' + b'c', b'd'),\ (a.c, b.d) \simeq (a'.c', b'.d').$$

On doit verifier ensuite que $(K, +, ., 0_K, 1_K)$ forme un anneau (exercice)

Soit $\frac{a}{b} \neq 0_K = \frac{0}{1}$, cela signifie que

$$a.1 \neq b.0 = 0$$

et donc la paire $(b, a) \in A \times (A - \{0\})$ et on a

$$\frac{a}{b}.\frac{b}{a} = \frac{a.b}{a.b} = \frac{1_A}{1_A} = 1_K$$

donc $\frac{a}{b}$ est inversible dans K et K est un corps.

Soit

$$\iota_K : \begin{array}{ccc} A & \mapsto & K \\ a & \mapsto & \frac{a}{1}. \end{array}$$

On verifie que ι est un morphisme d'anneau injectif: en effet

$$\frac{a}{1} = 0_K = \frac{0}{1} \Longleftrightarrow a = a.1 = 0.1 = 0.$$

On peut donc identifier a a la fraction $\frac{a}{1}$ et voir A comme un sous-anneau de K.

Soit $\iota_{K'} : A \mapsto K'$ un morphisme injectif dans un corps K'. Comme $\iota_{K'}$ est injectif, pour tout $b \in A - \{0\}$, $\iota_{K'}(b) \neq 0_{K'}$ et l'inverse $\iota_{K'}(b)^{-1} \in K' - \{0_{K'}\}$ existe.

On definit alors pour toute fraction $\frac{a}{b} \in \mathrm{Frac}(A)$,

$$\iota'(\frac{a}{b}) := \iota_{K'}(a).\iota_{K'}(b)^{-1}.$$

On verifie alors que l'application

$$\iota' : \begin{array}{ccc} \mathrm{Frac}(A) & \mapsto & K' \\ \frac{a}{b} & \mapsto & \iota_{K'}(a).\iota_{K'}(b)^{-1} \end{array}$$

est bien definie et est un morphisme non-nul de K vers K' et qu'il prolonge $\iota_{K'} : A \mapsto K'$. □

DÉFINITION 4.3. *Le corps K s'appelle le corps des fractions K et se note* $\mathrm{Frac}(A)$.

REMARQUE 4.2.3. La condition que $\iota_{K'}$ soit injective est vraiment necessaire (merci a Estelle de l'avoir remarque)

EXERCICE 4.1. Donner un exemple d'un anneau integre A et d'un morphisme d'anneau $\iota : A \mapsto K'$ non-nul et a valeurs dans un corps K' qui n'est pas injectif.

Preuve: (Estelle) L'anneau $\mathbb{Z}$ est intègre et si p est premier l'anneau $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps fini. L'application de reduction modulo p (qui n'est autre que l'application canonique)

$$n \in \mathbb{Z} \mapsto n \,(\mathrm{mod}\, p) = n.1_{\mathbb{F}_p} \in \mathbb{F}_p$$

n'est pas nulle (elle est surjective) et n'est pas injective puisque son noyau est $p\mathbb{Z}$. □

4.3. Caracteristique d'un corps, Sous-corps premier

Soit K un corps alors on a vu qu'il existe un morphisme d'anneaux canonique

$$\mathrm{Can}_K : \begin{array}{ccc} \mathbb{Z} & \mapsto & K \\ n & \mapsto & n.1_K = n_K \end{array}.$$

Le noyau de ce morphisme est de la forme

$$\ker(\mathrm{Can}_K) = p.\mathbb{Z},\ p \geqslant 0.$$

DÉFINITION 4.4. *L'entier p s'appelle la caracteristique du corps K et se note*

$$\mathrm{car}(K).$$

4.3.0.1. *Caracteristique nulle.* Si $\mathrm{car}(K) = p = 0$ alors Can_K est injectif et K contient l'anneau $\mathbb{Z}$ et donc le corps des fractions de $\mathbb{Z}$ qui est le corps des nombres rationels $\mathbb{Q}$.

4.3.0.2. *Caracteristique strictement positive.* Si $p > 0$ alors $p \neq 1$ car $1_K = 1.1_K \neq 0_K$. On a en fait

LEMME 4.2. *Si* $\mathrm{car}(K) > 0$ *alors* $\mathrm{car}(K) = p$ *est un nombre premier.*

Preuve: Supposons que p n'est pas premier alors $p = q_1.q_2$ avec $2 \leqslant q_1, q_2 < p$ et on a

$$p_K = 0_K = q_{1K}.q_{2K}$$

et donc ou bien $q_{1K} = 0$ ou bien $q_{2K} = 0$. Cela signifie que q_1 ou bien q_2 appartient a $\ker(\mathrm{Can}_K) = p.\mathbb{Z}$ mais cela contredit le fait que p est le plus petit entier strictement positif contenu dans $\ker(\mathrm{Can}_K)$. □

Considerons alors l'image $\mathrm{Can}_K(\mathbb{Z}) = \mathbb{Z}.1_K$, c'est un sous-anneau de K qui est donc integre. On notera cet anneau

$$\mathbb{F}_p := \mathrm{Can}_K(\mathbb{Z}) = \mathbb{Z}.1_K.$$

LEMME 4.3. *L'anneau $\mathbb{F}_p$ est un corps fini de cardinal p.*

Preuve: Notons que pour tout $n, k \in \mathbb{Z}$ on a

$$\mathrm{Can}_K(n + p.k) = \mathrm{Can}_K(n) + \mathrm{Can}_K(p.k) = \mathrm{Can}_K(n)$$

car $p.k \in \ker(\mathrm{Can}_K)$ donc si $r \in \{0, \cdots, p-1\}$ est le reste de la division euclidienne de n par p:

$$n = p.k + r,\ r \in \{0, \cdots, p-1\}$$

on a $n_K = r_K$ et ainsi

$$\mathbb{Z}.1_K = \{0_K, 1_K, \cdots, (p-1).1_K\}$$

est donc fini. De plus pour deux element distincts $i \neq j \in \{0, \cdots, p-1\}$, les valeurs i_K et j_K sont distinctes: sinon on aurait

$$(i-j)_K = i_K - j_K = 0_K$$

et donc $i - j \in p.\mathbb{Z}$ (serait un multiple de p) ce qui est impossible car $0 \leqslant i, j < p$ et $|j - i| < p$.

On a donc montre que $\mathbb{Z}.1_K$ est un anneau de cardinal p qui est integre (car sous-anneau d'un corps). Le fait que $\mathbb{F}_p$ soit un corps resulte du lemme suivant. □

LEMME 4.4. *Un anneau commutatif integre et fini est un corps.*

Preuve: Exercice. □

DÉFINITION 4.5. *Le corps $\mathbb{Q} \subset K$ (si $\mathrm{car}(K) = 0$) ou bien $\mathbb{F}_p \subset K$ (si $\mathrm{car}(K) = p > 0$) s'appelle le sous-corps premier de K.*

REMARQUE 4.3.1. Vous avez vu en cours "Structure algebrique" que si p est premier l'anneau fini des classes de congruences modulo $p(\mathbb{Z}/p\mathbb{Z}, +, .)$ est integre et donc un corps. En fait on a un isomorphisme de corps

$$\mathbb{Z}/p.\mathbb{Z} \simeq \mathbb{F}_p.$$

Ainsi pour une caracteristique fixe, tous les corps ayant cette caracteristique ont leurs sous-corps premiers isomorphes (soit a $\mathbb{Q}$ soit a $\mathbb{Z}/p\mathbb{Z}$ pour p premier).

NOTATION 4.1. *Soit K un corps et $n \in \mathbb{Z}$ un entier. On notera*

$$n_K = \mathrm{Can}_K(n) = n.1_K$$

l'image de n par le morphisme canonique.

4.3.1. Arithmetique des corps de caracteristique positive: le Frobenius.

PROPOSITION 4.3. *Soit K un corps de caracteristique $p > 0$ alors l'application*

$$\bullet^p : \begin{array}{ccc} K & \mapsto & K \\ x & \mapsto & x^p \end{array}$$

est un morphisme d'anneaux non-nul (donc necessairement injectif).

Preuve: Comme K est un anneau commutatif, on a pour tout $x, y \in K$

$$(x.y)^p = (x.y).\cdots.(x.y) = x^p.y^p.$$

Montrons que

$$(x + y)^p = x^p + y^p.$$

Par la formula du binome de Newton, on a (a nouveau parce que K est commutatif)

$$(x + y)^p = \sum_{k=0}^{p} C_p^k x^k.y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} C_p^k x^k.y^{p-k}$$

avec

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{p.(p-1).\cdots.(p-k+1)}{k.(k-1).\cdots.2.1} \in \mathbb{N}$$

(on rappelle que C_p^k est le nombre de sous-ensembles de k elements dans un ensemble de p elements).

LEMME 4.5. *Soit p un nombre premier et $1 \leqslant k \leqslant p-1$ alors C_p^k est divisible par p: il existe $c_{p,k} \in \mathbb{N}$ tel que $C_p^k = p.c_{p,k}$. En particulier $C_{p\,K}^k = 0_K$.*

Preuve: On a

$$C_p^k = p.\frac{(p-1).\cdots.(p-k+1)}{k.(k-1).\cdots.2.1} = p.c_{p,k}$$

avec $c_{p,k}$ a priori un nombre rationel. On sait que $1.2.\cdots.k$ divise $p.(p-1).\cdots.(p-k+1)$ (car C_p^k est un entier). Comme p est un nombre premier $k! = k.(k-1).\cdots.2.1$ est premier avec p (car tout diviseur premier de $k!$ est $< p$) et comme $k!$ divise $p.(p-1).\cdots.(p-k+1)$, il doit diviser $(p-1).\cdots.(p-k+1)$ et $c_{p,k}$ est premier. □

On a alors

$$(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} C_p^k.1_K.x^k.y^{p-k} = x^p + y^p$$

car pour $1 \leqslant k \leqslant p-1$, $C_p^k.1_K = 0_K$.

Ainsi $x \mapsto x^p$ est un morphisme d'anneau et comme $1_K^p = 1_K \neq 0_K$ il est non-nul.

□

DÉFINITION 4.6. *Soit K un corps de caracteristique p, le morphisme d'anneau precedent s'appelle le morphisme de Frobenius (ou simplement le Frobenius) de K se note*

$$\mathrm{frob}_p : x \in K \mapsto x^p \in K.$$

THÉORÈME 4.1 (Petit Theoreme de Fermat). *Soit K un corps de caracteristique positive p et $\mathrm{frob}_p : K \mapsto K$ le Frobenius. Pour tout $x \in \mathbb{F}_p = \mathbb{Z}.1_K$ on a*

$$\mathrm{frob}_p(x) = x^p = x.$$

Preuve: **Preuve**: Soit $x \in \mathbb{F}_p \subset K$, montrons que $x^p = x$; x est de la forme $x = n_K = n.1_K$ avec $n \in \mathbb{Z}$; montrons donc que

$$n_K^p = n_K.$$

Notons que c'est vrai pour -1: si $p = 2$, on a $(-1_K)^2 = 1_K = -1_K$ car $2_K = 2.1_K = 0_K$. Si $p > 2$ alors p est impair et $(-1)^p = -1$.

On peut donc supposer que $n \geqslant 1$: on a alors (par recurrence sur n)

$$(n.1_K)^p = ((n-1+1).1_K)^p = ((n-1)_K)^p + 1_K^p = (n-1)_K + 1_K = n_K.$$

□

CHAPITRE 5

Espaces Vectoriels

"An attempt at visualizing the Fourth Dimension:
Take a point, stretch it into a line,
curl it into a circle, twist it into a sphere,
and punch through the sphere."

5.1. Un changement de terminologie

Tout comme les corps sont des cas particuliers d'anneaux, les espace vectoriels sont des cas particuliers de modules: ce sont les modules dont l'anneau associe est un corps:

DÉFINITION 5.1. *Soit K un corps, un K-espace vectoriel (K-ev) V est simplement un K-module. Les elements de V sont appeles vecteurs de V.*

EXEMPLE 5.1.1. Exemples d'espaces vectoriels:

(1) L'espace vectoriel nul $\{0_K\}$.
(2) K est un espace vectoriel sur lui-meme.
(3) Si V et W sont des K-ev leur produit

$$V \times W = \{(v, w),\ v \in V,\ w \in W\}$$

muni de l'addition (composante par composante)

$$(v, w) + (v', w') := (v +_V v', w +_W w')$$

et de la mutliplication externe (composante par composante)

$$x.(v, w) := (x.v, x.w)$$

a une structure d'ev dont le vecteur nul est

$$0_{V\times W} = (0_V, 0_W).$$

(4) En particulier, pour $d \geqslant 1$, en iterant la construction precedente pour $W = K$ on forme le K-module libre de rank d,

$$K^d = \{(x_1, \cdots, x_d),\ x_i \in K\}$$

dont l'element neutre est le vecteur nul

$$0_d = (0, \cdots, 0).$$

(5) Si X est un ensemble,

$$\mathcal{F}(X; K) = K^X = \{f : X \mapsto K\}$$

a une structure de K-espace vectoriel.
(6) Plus generalement si V est un K-espace vectoriel et X est un ensemble,

$$\mathcal{F}(X; V) = V^X = \{f : X \mapsto V\}$$

a une structure de K-espace vectoriel.

NOTATION 5.1. *Pour alleger les notation on notera la multiplication par les scalaires sous la forme d'un point . (le meme point . que pour la multiplication dans le corps K) : pour $\lambda \in K,\ \vec{v} \in V$ on ecrira $\lambda.\vec{v}$.*

Les differentes structures associees aux modules sur un anneau ont un nouveau nom quand l'anneau est un corps.

5.1.1. Sous-espace vectoriel.

DÉFINITION 5.2. *Soit V un K-espace vectoriel, un sous-espace vectoriel (SEV) de V est un sous-K module $W \subset V$.*

PROPOSITION 5.1 (Critere de SEV). *Un sous-ensemble $U \subset V$ d'un K-EV est un SEV ssi*

$$\forall \lambda \in K,\ \vec{v}, \vec{v}' \in U,\ \lambda.\vec{v} + \vec{v}' \in U.$$

Preuve: C'est un cas particulier du critere de sous-module. □

EXEMPLE 5.1.2. Exemples de SEV:

- $\{0_V\}, V \subset V$.
- Pour $\mathbf{e} \in V$, $K.\mathbf{e} = \{x.\mathbf{e}, x \in K\}$.
- Si $V' \subset V$ et $W' \subset W$ sont des SEV, $V' \times W'$ en est un.
- $\{(x_1, \cdots, x_d) \in K^d,\ x_1 + \cdots + x_d = 0\} \subset K^d$.
- $\{(x_1, \cdots, x_d) \in K^d,\ x_1 + \cdots + x_d = 1\} \subset K^d$ n'est pas un SEV.
- Soit $x_0 \in X$, dans $\mathcal{F}(X, V)$ le sous-espaces des fonctions f telles que $f(x_0) = 0_V$.
- Dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$ l'ensemble des fonctions paires (resp. impaires).

  $$f : \mathbb{R} \mapsto \mathbb{R},\ \forall x \in \mathbb{R},\ f(x) = f(-x)\ (resp.\ f(x) = -f(-x))$$

  sont des SEV.

5.1.2. Applications lineaires.

DÉFINITION 5.3. *Soient V et W deux K-espaces vectoriel, un morphisme $\varphi : V \mapsto W$ de K-modules est appele une application K-lineaire.*

PROPOSITION 5.2 (Critere d'application lineaire). *Une application entre espaces vectoriels $\varphi : V \mapsto W$ est lineaire ssi*

$$\forall \lambda \in K,\ \vec{v}, \vec{v}' \in V,\ \varphi(\lambda.\vec{v} + \vec{v}') = \lambda.\varphi(\vec{v}) + \varphi(\vec{v}').$$

Preuve: C'est un cas particulier du critere de morphisme de modules. □

PROPOSITION 5.3. *Si $\varphi : V \mapsto W$ est une application lineaire, le noyau*

$$\ker \varphi = \{\vec{v} \in V,\ \varphi(\vec{v}) = 0_W\} \subset V$$

et l'image

$$\mathrm{Im}\, \varphi := \{\varphi(\vec{v}),\ \vec{v} \in V\} \subset W$$

sont des sous-espaces vectoriels de V et de W respectivement.

Preuve: C'est un cas particulier du cas des morphismes de modules sur un anneau. □

PROPOSITION 5.4. *Soit $\varphi : V \mapsto W$ est une application lineaire, alors φ est injective ssi*

$$\ker \varphi = \{0_V\}.$$

EXEMPLE 5.1.3. Dans K^d:

$$\mathbf{e}_i^* : \begin{array}{ccc} K^d & \mapsto & K \\ (x_1, \cdots, x_d) & \mapsto & x_i \end{array}.$$

$$\ker(\mathbf{e}_i^*) = \{(x_1, \cdots, 0, \cdots, x_d),\ x_j \in K,\ j \neq i\},\ \mathrm{Im}(\mathbf{e}_i^*) = K.$$

$$S : \begin{array}{ccc} K^d & \mapsto & K \\ (x_1, \cdots, x_d) & \mapsto & x_1 + \cdots + x_d \end{array}.$$
$$\ker(S) = \{(x_1, \cdots, x_d) \in K^d,\ x_1 + \cdots + x_d = 0\},\ \mathrm{Im}(S) = K.$$
$$\varphi : \begin{array}{ccc} K^2 & \mapsto & K^2 \\ (x_1, x_2) & \mapsto & (2x_1 + x_2, x_1 + x_2) \end{array}$$
$$\ker(\varphi) = \{0_2\},\ \mathrm{Im}(\varphi) = K^2.$$

NOTATION 5.2. *On notera*

$$\mathrm{Hom}_{K-ev}(V, W),\ \mathrm{Isom}_{K-ev}(V, W),$$
$$\mathrm{End}_{K-ev}(V) = \mathrm{Hom}_{K-ev}(V, V),\ \mathrm{Aut}_{K-ev}(V) = \mathrm{GL}(V) = \mathrm{Isom}_{K-ev}(V, V)$$

les ensembles des applications lineaires, applications lineaires bijectives (ou isomorphismes), d' endomorphismes et d'automorphismes des K-espaces vectoriels V et W.

Comme K est commutatif on a

THÉORÈME 5.1 (Les endomorphismes forment une algebre). *L'ensemble des endomorphismes de V, $\mathrm{End}_{K-ev}(V)$ muni de l'addition et de la composition a une structure canonique de K-algebre. Son groupe des unites est de groupe $\mathrm{End}_{K-ev}(V)^\times = \mathrm{Aut}_{K-ev}(V)$ des applications K-lineaires bijectives.*

5.1.3. Sous-espace engendre par un sous-ensemble. On rappelle egalement que

PROPOSITION 5.5 (Les SEV sont stables par intersection). *Soit $W_i,\ i \in I$ une famille de sev de V indexes par un ensemble I alors leur intersection*

$$\bigcap_{i \in I} W_i \subset V$$

est un SEV de V.

DÉFINITION 5.4. *Soit $\mathscr{F} \subset V$ un sous-ensemble, on note*

$$\langle \mathscr{F} \rangle = \mathrm{Vect}(\mathscr{F}) = CL_K(\mathscr{F}) \subset V$$

le sous-espace vectoriel (le sous-K module) engendre par $\mathscr{F}$.

On rappelle qu'il s'agit de maniere equivalente

- *de l'intersection de tous les sev contenant $\mathscr{F}$,*
- *de l'ensemble des combinaisons lineaires d'elements de $\mathscr{F}$ a coefficients dans K*

$$CL_K(\mathscr{F}) := \{\sum_{i=1}^{n} \lambda_i.x_i,\ n \geqslant 1,\ \lambda_1, \cdots, \lambda_n \in K,\ x_1, \cdots, x_n \in \mathscr{F}\}.$$

Cette notion admet des cas particuliers.

5.1.3.1. *Sommes d'espaces et sommes directes.*

DÉFINITION 5.5. *Soient $X, Y \subset V$ des sous-espaces d'un espace vectoriels. Leur somme $X+Y \subset V$ est*

$$X + Y = \langle X \cup Y \rangle \subset V$$

est le sous-espace vectoriel engendre par les vecteurs de X et de Y.

LEMME 5.1. *On a*

$$X + Y = \{x + y,\ x \in X,\ y \in Y\}.$$

Preuve: Soit $W \subset V$ un sev contenant X et Y alors W contient $X+Y$ car W est stable par somme. Il reste a montrer que $X + Y$ est un sev car ce sera necessairement le plus petit contenant X et Y.

Soit $\lambda \in K, x, x' \in X,\ y, y' \in Y$ alors

$$\lambda(x + y) + (x' + y') = (\lambda.x + x') + (\lambda.y + y') \in X + Y$$

car X et Y sont des sev. □

NOTATION 5.3. *Si $X \cap Y = \{0_V\}$, on dit que X et Y sont en somme directe et on ecrit*

$$X \oplus Y \subset V$$

pour leur somme. Si

$$X \oplus Y = V$$

on dit que V est somme directe de X et Y.

PROPOSITION 5.6. *Si X et Y sont en somme directe et $V = X \oplus Y$ est leur somme alors l'ecriture de $v \in V$ sous la forme*

$$v = x + y,\ x \in X,\ y \in Y$$

est unique.

Preuve: Si $x + y = x' + y'$ alors $x - x' = y' - y$ et donc $x - x' \in X \cap Y = \{0_V\}$ cad que

$$x = x',\ \text{et}\ y = y'.$$

□

EXERCICE 5.1. Montrer que si $V = X \oplus Y$ est somme directe de X et Y alors V est isomorphe a l'espace vectoriel produit $X \times Y$.

5.2. Famille generatrice, libre, base

5.2.1. Famille generatrice. On rappelle la definition qu'on a vu pour les modules:

DÉFINITION 5.6. *Soit V un K-e.v. Un sous-ensemble $\mathscr{G} \subset V$ est une famillle generatrice si*

$$\mathrm{Vect}(\mathscr{G}) = V,$$

ie. tout element $v \in V$ peut s'ecrire sous la forme d'une combinaison lineaire

$$v = \sum_{i=1}^{n} x_i \mathbf{e}_i, \tag{5.2.1}$$

pour $n \geqslant 1,\ x_1, \cdots, x_n \in K,\ \mathbf{e}_1, \cdots, \mathbf{e}_n \in \mathscr{F}$.

DÉFINITION 5.7. *Un K-espace vectoriel non-nul est dit de dimension finie si il est de type fini comme K-module: si il existe un ensemble $\mathscr{G}$ fini tel que*

$$V = \mathrm{Vect}(\mathscr{G}).$$

La dimension de V est definie comme le minimum du cardinal de toutes les familles generatrices finies de V:

$$\dim(V) = \min_{\mathscr{G}\ \text{generatrice}} |\mathscr{G}|.$$

Par convention, la dimension de l'espace vectoriel nul $\{0_V\}$ est

$$\dim(\{0_V\}) = 0$$

(on peux prendre la famille vide comme famille generatrice).

On va maintenant se restreindre au cas des espaces vectoriels de dimension finie. A la fin du chapitre, on decrira ce qui ce passe pour les espaces vectoriel qui ne sont pas de dimension finie.

Le resultat principal de cette section est le theoreme suivant:

THÉORÈME. *Tout K-espace vectoriel de dimension finie est libre de rang $d = \dim(V)$, c'est a dire isomorphe a K^d ($K^0 = \{0_K\}$).*

Avant de demontrer ce theoreme qui nous prendra un peu de temps, examinons sa signification concrete: supposons que $\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \subset V$ soit une famille generatrice de V. Tout element $v \in V$ peut se representer sous la forme d'une combinaison lineaire des $\mathbf{e}_i$

$$v = \sum_{i=1}^{d} x_i.\mathbf{e}_i,\ x_i \in K.$$

En d'autre termes, on dispose d'une application "combinaison lineaire" qui est surjective:

$$CL := CL_{\mathscr{G}} : \begin{array}{ccc} K^d & \mapsto & V \\ (x_1, \cdots, x_d) & \mapsto & CL_{\mathcal{G}}(x_1, \cdots, x_d) = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d \end{array}.$$

Remarque 5.2.1. Cette application *depend* de l'ordre dans lequel on enumere les elements de la famille $\mathscr{G}$: en general

$$x_1.\mathbf{e}_1 + x_2.\mathbf{e}_2 \neq x_1.\mathbf{e}_2 + x_2.\mathbf{e}_1.$$

Lemme 5.2. *L'application $CL_{\mathscr{G}}$ est lineaire.*

Preuve: Soit

$$\vec{x} = (x_1, \cdots, x_d),\ \vec{y} = (y_1, \cdots, y_d)$$

et $\lambda \in K$ alors on veut verifier que

$$CL(\lambda.\vec{x} + \vec{y}) = \lambda.CL(\vec{x}) + CL(\vec{y}).$$

C'est une consequence de la commutativite et de l'associativite des lois d'addition et de multiplication: on a

$$\begin{array}{rcl} CL(\lambda.\vec{x} + \vec{y}) & = & CL(\lambda.x_1 + y_1, \cdots, \lambda.x_d + y_d) = (\lambda.x_1 + y_1)\mathbf{e}_1 + \cdots + (\lambda.x_d + y_d)\mathbf{e}_d \\ & = & \lambda.x_1.\mathbf{e}_1 + y_1.\mathbf{e}_1 + \cdots + \lambda.x_d.\mathbf{e}_d + y_d.\mathbf{e}_d \\ & = & \lambda.(x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d) + (y_1.\mathbf{e}_1 + \cdots + y_d.\mathbf{e}_d) \\ & = & \lambda.CL(\vec{x}) + CL(\vec{y}). \end{array}$$

□

5.2.2. Famille libre. Si $\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ est generatrice alors tout $v \in V$ admet une representation sous forme combinaison lineaire des $\mathbf{e}_i$

$$v = \sum_{i=1}^{d} x_i.\mathbf{e}_i,\ x_i \in K.$$

Une question naturelle est de savoir si cette representation est *unique* pour tout v.

Si tel est cas, on aura identifie chaque vecteur v de l'espace vectoriel "abstrait" V avec le d-uplet

$$(x_1, \cdots, x_d) \in K^d$$

qui est un element d'un espace vectoriel "concret" K^d.

Remarque 5.2.2. En general, on n'a pas unicite : supposons par exemple que $\mathbf{e}_d = 0_V$ alors v s'ecrira

$$v = \sum_{i=1}^{d-1} x_i.\mathbf{e}_i + \lambda.0_V$$

pour tout $\lambda \in K$ et on aura de multiple representations de v possibles (au moins autant que le cardinal de K).

On voit qu'on aurait pu omettre le dernier element $\mathbf{e}_d = 0_V$ et ne considerer qu'en fait $\{\mathbf{e}_1, \cdots, \mathbf{e}_{d-1}\}$ comme famille generatrice. C'est cette idee de prendre une famille generatrice la plus petite possible qui nous servira.

Dire que chaque element de V a une representation unique est equivalent a dire que l'application $CL_{\mathcal{G}}$ est *injective*; par le critere d'injectivite des applications lineaires cela equivaut a dire que

$$\ker(CL_{\mathcal{G}}) = \{\vec{x} \in K^d,\ x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d = 0_V\} = \{0_{K^d} = (0, \cdots, 0)\}.$$

En d'autres termes, chaque element $v \in V$ admet une unique representation sous forme de combinaison lineaire des $\mathbf{e}_i, i \leqslant d$ si et seulement si admet une unique representation sous forme de combinaison lineaire des $\mathbf{e}_i, i \leqslant d$, la combinaision *triviale* ou *nulle*:

$$x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d = 0_V \Longleftrightarrow x_1 = \cdots = x_d = 0_K.$$

REMARQUE 5.2.3. La direction $\Longleftarrow$ est bien sur evidente.

Cela nous conduit a la definition generale suivante:

DÉFINITION 5.8. *Un sous-ensemble fini $\mathscr{F} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \subset V$ d'un espace vectoriel forme une famille libre de V si et seulement si pour tous $x_1, \cdots, x_d \in K$*

$$x_1.\mathbf{e}_1 + \cdots + x_{d'}.\mathbf{e}_d = 0_V \Longrightarrow x_1 = \cdots = x_d = 0.$$

Une famille $\mathscr{F}$ qui n'est pas libre est dit liee.

En d'autres termes une famille est libre si et seulement si la seule representation de 0_V sous forme de combinaison lineaire des $\mathbf{e}_i,\ i \leqslant d$ est la combinaison lineaire triviale

$$0.\mathbf{e}_1 + \cdots + 0.\mathbf{e}_d.$$

EXEMPLE 5.2.1. Soit $\mathbf{e} \in V - \{0_V\}$ un vecteur non-nul alors $\{\mathbf{e}\}$ est libre: supposons que

$$x.\mathbf{e} = 0_V$$

pour $x \in K$; si $x \neq 0_K$ alors x est inversible et

$$x^{-1}.x.\mathbf{e} = \mathbf{e} = 0_V$$

qui est une contradiction donc $x = 0_K$.

EXEMPLE 5.2.2. Dans K^d, la base canonique

$$\mathscr{B}^0 := \{\mathbf{e}_i^0,\ i = 1, \cdots, d\}$$

qui est generatrice est egalement libre; on rappelle que $\mathbf{e}_i^0$ est le vecteur dont toutes les coordonnes sont nulles sauf la i-eme qui vaut 1,

$$\mathbf{e}_1^0 = (1, 0, \cdots, 0), \cdots,\ \mathbf{e}_d^0 = (0, 0, \cdots, 1).$$

En effet, pour tout $x_1, \cdots x_d \in K$ on a

$$\sum_{i=1}^{d} x_i.\mathbf{e}_i^0 = (x_1, x_2, \cdots, x_d)$$

et donc si

$$= \sum_{i=1}^{d} x_i.\mathbf{e}_i^0 = 0_d = (0, \cdots, 0)$$

on a

$$x_1 = \cdots = x_d = 0.$$

EXEMPLE 5.2.3. Dans $\mathbb{R}^3$, la famille

$$(1, 1, 0),\ (0, 1, 1),\ (1, 0, 1)$$

est libre.

En revanche si $\mathrm{car}(K) = 2$ alors la famille est liee:

$$(1, 1, 0) + (0, 1, 1) + (1, 0, 1) = (2, 2, 2) = \underline{0}_3.$$

En fait, cette famille est libre dans K^3 ou K est de caracteristique $\neq 2$.

PROPOSITION 5.7. *Une famille a d elements $\mathscr{F} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \subset V$ est liee ssi il existe $i \in \{1, \cdots, d\}$ tel que $\mathbf{e}_i$ peut s'exprimer comme combinaison lineaire des autres elements de $\mathscr{F}$:*

$$\mathbf{e}_i \in CL(\mathscr{F} - \{\mathbf{e}_i\}) = CL(\{\mathbf{e}_j,\ j \neq i\}).$$

Preuve: Si $\mathcal{F}$ est liee, il existe $x_1, \cdots, x_d \in K$ non-tous nuls tels que

$$0_V = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d.$$

Supposons (quitte a renumeroter) que $x_d \neq 0$ alors

$$-x_d.\mathbf{e}_d = x_1.\mathbf{e}_1 + \cdots + x_{d-1}.\mathbf{e}_{d-1}$$

et comme $-x_d$ est inversible

$$\mathbf{e}_d = (x_1/-x_d).\mathbf{e}_1 + \cdots + (x_{d-1}/-x_d).\mathbf{e}_{d-1} \in CL(\mathcal{F} - \{\mathbf{e}_d\}).$$

Reciproquement si $\mathbf{e}_d \in CL(\mathscr{F} - \{\mathbf{e}_d\})$ alors

$$\mathbf{e}_d = y_1.\mathbf{e}_1 + \cdots + y_{d-1}\mathbf{e}_{d-1}$$

et

$$0_V = y_1.\mathbf{e}_1 + \cdots + y_{d-1}\mathbf{e}_{d-1} + (-1).\mathbf{e}_d$$

avec $-1 \neq 0_K$. □

Les familles libres ne peuvent pas etre trop grandes.

THÉORÈME 5.2 (Majoration du cardinal d'une famille libre). *Soit V un espace vectoriel non-nul de dimension d et $\mathscr{F} = \{v_1, \cdots, v_f\} \subset V$ une famille finie et libre; alors $f \leqslant d$.*

Preuve: On procede par recurrence sur d.

Si $d = 1$ alors $V = K.\mathbf{e}$ avec $\mathbf{e} \neq 0_V$; soit $\mathscr{F} = \{v_1, \cdots, v_f\}$ une famille avec $f \geqslant 2$ elements. Montrons que $\mathscr{F}$ est liee. On a

$$v_1 = x_1.\mathbf{e},\ v_2 = x_2.\mathbf{e}$$

et x_1 ou x_2 est non-nul; par exemple $x_1 \neq 0$, alors x_1 est inversible et

$$\mathbf{e} = x_1^{-1}.v_1,\ v_2 = x_2.\mathbf{e} = (x_2/x_1).v_1$$

est combinaison lineaire de v_1 et ainsi $\mathscr{F}$ est liee.

Supposons qu'on a demontre le resultat pour tout espace vectoriel de dimension $\leqslant d-1$.

Soit V de dimension $d \geqslant 1$, $\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ une famille qui engendre V et $\mathscr{F} = \{v_1, \cdots, v_f\} \subset V$ une famille a $f > d$ elements. Montrons que $\mathscr{F}$ est liee.

Par definition chaque element de $\mathscr{F}$ est combinaison lineaire des elements de $\mathscr{G}$: pour $i = 1, \cdots, f$, il existe $(x_{i,j})_{j \leqslant d}$ tel que

$$v_i = x_{i,1}\mathbf{e}_1 + \cdots + x_{i,d}\mathbf{e}_d,\ i = 1, \cdots, f.$$

Comme $f > d \geqslant 1$, il existe un indice $j_0 \in \{1, \cdots, d\}$ et un indice $i_0 \in \{1, \cdots, f\}$ tels que

$$x_{i_0,j_0} \neq 0$$

(sinon tous les v_i seraient nuls). Supposons (quitte a renumeroter les v_i et les $\mathbf{e}_j$) que $i_0 = f,\ j_0 = d$ et $x_{f,d}$ est inversible. Posons

$$v'_i = v_i - (x_{i,d}/x_{f,d}).v_f,\ i = 1, \cdots, f.$$

On a

$$v'_f = v_f - (x_{f,d}/x_{f,d}).v_f = 0_V$$

et en general

$$v'_i = x'_{i,1}\mathbf{e}_1 + \cdots + x'_{i,d-1}\mathbf{e}_{d-1} + (x_{i,d} - (x_{i,d}/x_{f,d}).x_{f,d})\mathbf{e}_d = x'_{i,1}\mathbf{e}_1 + \cdots + x'_{i,d-1}\mathbf{e}_{d-1}.$$

ainsi la famille

$$\mathscr{F}' = \{v'_i,\ i \leqslant f-1\} \subset V' = \langle\{\mathbf{e}_1, \cdots, \mathbf{e}_{d-1}\}\rangle \subset V$$

possede $f-1$ elements et est contenue dans un sous-espace vectoriel engendre par $d-1$ elements donc de dimension $\leqslant d-1$. Par recurrence, $\mathscr{F}'$ est liee: l'un des v'_i est combinaison lineaire des autres. Supposons que ce soit v'_1: on a

$$v'_1 = y_2.v'_2 + \cdots + y_{f-1}.v'_{f-1}$$

et (ecrivant $v'_i = v_i - (x_{i,d}/x_{f,d}).v_f$) on obtient que

$$v'_1 = v_1 - (x_{1,d}/x_{f,d}).v_f$$

est combinaison lineaire de $v_2, \cdots, v_f$ et donc (en ajoutant $(x_{1,d}/x_{f,d}).v_f$) on voit que v_1 est combinaison lineaire de $v_2, \cdots, v_f$. La famille est donc liee.

□

5.2.3. Base.

Définition 5.9. *Soit V un espace vectoriel de dimension finie. Une famille $\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ est une base de V si lune des conditions equivalentes suivantes est verifiee:*

(1) $\mathscr{B}$ est generatrice et libre,
(2) L'application combinaison lineaire de $\mathscr{B}$,

$$CL_{\mathscr{B}} : K^d \mapsto V$$

est un isomorphisme,
(3) Pour tout $v \in V$ il existe un unique uplet $(x_1, \cdots, x_d) \in K^d$ tel que v s'ecrit sous la forme

$$v = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d.$$

Il resulte de la definition de la dimension et du theoreme precedent que si $\mathscr{B}$ est une base alors

$$|\mathscr{B}| = \dim(V). \tag{5.2.2}$$

En particulier

$$\dim(K^d) = d.$$

Définition 5.10. *Soit $\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ une base de V, si $v \in V$ s'ecrit*

$$v = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d$$

le scalaire x_i est la i-eme coordonnee de v dans la base $\mathscr{B}$.

On va maintenant pouvoir demontrer qu'un espace vectoriel de dimension finie possede une base et est donc libre de rang $d = \dim(V)$.

Théorème 5.3 (Existence d'un base). *Soit V un K-ev de dimension $d = \dim(V) \geqslant 1$ alors V possede une base $\mathscr{B}$ et on a donc un isomorphisme de K-ev*

$$V \simeq K^d.$$

Plus precisement,

(1) Soit $\mathscr{G} \subset V$ une famille generatrice alors $\mathscr{G}$ contient une base de V. Si de plus $|\mathscr{G}| = d$ alors $\mathscr{G}$ est une base.
(2) Si $\mathscr{L} \subset V$ est libre alors $\mathscr{L}$ est contenue dans une base de V. Si $|\mathscr{L}| = d$ alors $\mathscr{L}$ est une base.

Preuve: Soit $\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{G}|}\}$ une famille generatrice; par definition de la dimension $|\mathscr{G}| \geqslant d$.

Montrons que $\mathscr{G}$ contient une base. L'ensemble $\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{G}|}\}$ contient au moins une sous-famille non-vide qui est libre. En effet, il existe i tel que $\mathbf{e}_i \neq 0_V$ (sinon $V = \langle\mathscr{G}\rangle = \{0_V\}$ ce qui est exclut) et la famille reduite a un element $\{\mathbf{e}_i\}$ est libre. Soit $\mathscr{B} \subset \mathscr{G}$ une sous-famille libre dont le cardinal $|\mathscr{B}|$ maximal parmi les sous-familles libres de $\mathscr{G}$. Montrons que $\mathscr{B}$ est generatrice et est donc une base.

Quitte a reordonner $\mathscr{G}$, on peut supposer que

$$\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{B}|}\}.$$

(1) Si $|\mathscr{B}| = |\mathscr{G}|$ alors $\mathscr{B} = \mathscr{G}$ est generatrice et $\mathscr{B}$ est un base.
(2) Sinon on a $|\mathscr{B}| < |\mathscr{G}|$. Supposons que $\mathscr{B}$ n'est pas generatrice c'est a dire

$$CL(\{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{B}|}\}) \neq CL(\{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{G}|}\}) = V,$$

alors il existe $i > |\mathscr{B}|$ tel que

$$\mathbf{e}_i \notin CL(\mathscr{B})$$

c'est a dire que pour tout $x_1, \cdots, x_{|\mathscr{B}|} \in K$ on a toujours

$$\mathbf{e}_i \neq x_1.\mathbf{e}_1 + \cdots + x_{|\mathscr{B}|}\mathbf{e}_{|\mathscr{B}|}.$$

Montrons qu'alors la famille $\mathscr{B} \cup \{\mathbf{e}_i\}$ est encore libre ce qui contredira la maximalite de $|\mathscr{B}|$: supposons que pour $x_1, \cdots, x_{|\mathscr{B}|}, x_i \in K$ on ait

$$x_1.\mathbf{e}_1 + \cdots + x_{|\mathscr{B}|}\mathbf{e}_{|\mathscr{B}|} + x_i.\mathbf{e}_i = 0_V$$

alors
(a) si $x_i = 0$ on a

$$x_1.\mathbf{e}_1 + \cdots + x_{|\mathscr{B}|}\mathbf{e}_{|\mathscr{B}|} = 0_V$$

et comme $\mathscr{B}$ est libre on a $x_1 = \cdots = x_{|\mathscr{B}|} = x_i = 0$.
(b) Sinon $x_i \neq 0$ est inversible et on a

$$\mathbf{e}_i = -(x_1/x_i).\mathbf{e}_1 - \cdots - (x_{|\mathscr{B}|}/x_i)\mathbf{e}_{|\mathscr{B}|}$$

une contradiction: ainsi la famille est libre.

On obtient alors une contradiction avec la maximalite de $|\mathscr{B}|$ ce qui implique que $\mathscr{B}$ est generatrice.

Si $|\mathscr{G}| = d = |\mathscr{B}|$ alors l'inclusion $\mathscr{B} \subset \mathscr{G}$ implique que $\mathscr{G} = \mathscr{B}$ qui est donc une base.

Soit $\mathscr{L} = \{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{L}|}\}$ une famille libre non-vide. Montrons que $\mathscr{L}$ est contenue dans une base. Il existe une famille generatrice finie contenant $\mathscr{L}$: il suffit de prendre une famille generatrice finie $\mathscr{G}$ de V (par exemple une base) et de prendre $\mathscr{L} \cup \mathscr{G}$ qui est evidemment generatrice. Soit

$$\mathscr{L} \cup \mathscr{G} \supset \mathscr{B} \supset \mathscr{L}$$

une famille generatrice de cardinal $|\mathscr{B}|$ minimal parmi toutes les familles generatrices contenant $\mathscr{L}$ et contenues dans $\mathscr{L} \cup \mathscr{G}$; montrons que $\mathscr{B}$ est libre et est donc une base.

(1) Si $|\mathscr{B}| = |\mathscr{L}|$ alors $\mathscr{B} = \mathscr{L}$ est generatrice et libre et c'est une base.
(2) Si $|\mathscr{B}| > |\mathscr{L}|$ ecrivons

$$\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{L}|}, \cdots, \mathbf{e}_{|\mathscr{B}|}\}$$

et supposons que $\mathscr{B}$ ne soit pas libre: il existe $x_1, \cdots, x_{|\mathscr{B}|} \in K$ non tous nuls tels que

$$x_1.\mathbf{e}_1 + \cdots + x_{|\mathscr{L}|}\mathbf{e}_{|\mathscr{L}|} + \cdots + x_{|\mathscr{B}|}\mathbf{e}_{|\mathscr{B}|} = 0_V.$$

si $x_{|\mathscr{L}|+1} = \cdots = x_{|\mathscr{B}|} = 0$ alors on a

$$x_1.\mathbf{e}_1 + \cdots + x_{|\mathscr{L}|}\mathbf{e}_{|\mathscr{L}|} = 0_V$$

et comme $\mathscr{L}$ est libre on a

$$x_1 = \cdots = x_{|\mathscr{L}|} = x_{|\mathscr{L}|+1} = \cdots = x_{|\mathscr{B}|} = 0.$$

Sinon il existe $i > |\mathscr{L}|$ tel que $x_i \neq 0$ disons que c'est $x_{|\mathscr{B}|}$: on a alors

$$\mathbf{e}_{|\mathscr{B}|} = -(x_1/x_{|\mathscr{B}|}).\mathbf{e}_1 - \cdots - (x_{|\mathscr{B}|-1}/x_{|\mathscr{B}|})\mathbf{e}_{|\mathscr{B}|-1}$$

et alors comme $\mathbf{e}_{|\mathscr{B}|}$ est combinaison lineaire des $\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{B}|-1}$, la famille $\{\mathbf{e}_1, \cdots, \mathbf{e}_{|\mathscr{B}|-1}\}$ est generatrice ce qui contredit la minimalite de $|\mathscr{B}|$. Ainsi $\mathscr{B}$ est libre.

□

On a demontre dans la deuxieme partie un resultat un peu plus fort:

THÉORÈME 5.4 (de la base incomplete). *Etant donne $\mathscr{L}$ une famille libre de V et $\mathscr{B} \subset V$ une base, on peut extraire de $\mathscr{B}$ une sous-famille $\mathscr{L}' \subset \mathscr{B}$ de sorte que $\mathscr{L} \sqcup \mathscr{L}'$ forme une base de V.*

EXERCICE 5.2. Montrer que si X et Y sont de dimension finie

$$\dim(X \times Y) = \dim(X) + \dim(Y).$$

Montrer que si $V = X \oplus Y$,

$$\dim(V) = \dim(X) + \dim(Y).$$

5.2.4. Sous-espaces vectoriels et dimension.

THÉORÈME 5.5 (Bases et SEV). *Soit V un espace vectoriel de dimension finie, et $W \subset V$ un sous-espace vectoriel alors*

(1) W est de dimension finie et $\dim(W) \leqslant \dim(V)$.
(2) Si $\mathscr{B}_W$ est une base de W alors il existe une base $\mathscr{B}_V$ de V contenant $\mathscr{B}_W$.
(3) Si $\dim(W) = \dim(V)$ alors $W = V$.

Preuve: Si $W = \{0_V\}$ on a termine.

Sinon, soit $\mathscr{L} \subset W$ une famille finie, libre et contenue dans W. Une telle famille existe: si $\mathbf{e} \in W$ est un vecteur non-nul de W alors $\{\mathbf{e}\}$ est libre. De plus comme $\mathscr{L}$ est libre on a $|\mathscr{L}| \leqslant \dim(V)$. Supposons que $\mathscr{L} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ est de cardinal maximal parmi toutes les familles libres de W et montrons que $\mathscr{L}$ est generatrice de W.

Supposons que $\langle \mathscr{L} \rangle \neq W$ alors il existe $\mathbf{e}$ dans W qui n'est pas combinaison lineaire des elements de $\mathscr{L}$. Cela implique que la famille $\mathscr{L} \cup \{\mathbf{e}\}$ est libre et cela contredit la maximalite de $|\mathscr{L}|$. Ainsi $\mathscr{L}$ est generatrice et c'est une base. On a donc

$$\dim(W) = |\mathscr{L}| \leqslant \dim(V).$$

Soit $\mathscr{B}_W$ une base de W alors c'est une famille libre et on a vu qu'on peut trouver une base de V la contenant.

Si $\dim(W) = \dim(V)$ alors une base de W est libre et de cardinal $\dim(V)$ et c'est donc une base de V.

□

- Un sous-espace vectoriel de dimension 1 est appelle droite vectorielle.
- Un sous-espace vectoriel de dimension 2 est appelle plan vectoriel.
- Un sous-espace vectoriel de dimension $\dim(V) - 1$ est appelle hyperplan vectoriel.

5.3. Espaces vectoriels de dimension infinie

DÉFINITION 5.11. *Un K-ev qui ne possede pas de famille generatrice finie est dit de dimension infinie.*

Repetons la definition de famille generatrice:

DÉFINITION 5.12. *Soit V un K-e.v. Un sous-ensemble $\mathscr{G} \subset V$ est une famillle generatrice si*

$$\mathrm{Vect}(\mathscr{G}) = V,$$

ie. tout element $v \in V$ peut s'ecrire sous la forme d'une combinaison lineaire (finie) d'elements de $\mathscr{G}$: il existe $d \geqslant 1$, $\mathbf{e}_1, \cdots, \mathbf{e}_d \in \mathscr{G}$, $x_1, \cdots, x_d \in K$,, tels que

$$v = x_1\mathbf{e}_1 + \cdots + x_d\mathbf{e}_d. \tag{5.3.1}$$

Donnons une definition generale de famille libre:

DÉFINITION 5.13. *Soit V un K-e.v., un sous-ensemble $\mathscr{L} \subset V$ est une famille libre si tout sous-ensemble fini $\mathscr{L}' \subset \mathscr{L}$ est libre: $\forall d \geqslant 1$ et tout $\{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \subset \mathscr{L}$, on a*

$$x_1\mathbf{e}_1 + \cdots + x_d\mathbf{e}_d = 0_V \Longleftrightarrow x_1 = \cdots = x_d = 0_K. \tag{5.3.2}$$

DÉFINITION 5.14. *Une base $\mathscr{B} \subset V$ est une famille libre et generatrice: tout element de V est representable comme combinaison lineaire finie d'elements de $\mathscr{B}$ et une telle representation est unique.*

EXERCICE 5.3. Soit $\mathcal{F}(\mathbb{N}, \mathbb{R})$ l'espace des fonctions de $\mathbb{N}$ a valeurs reelles (ie. les suites a valeurs reelles) et $\mathcal{F}_f(\mathbb{N}, \mathbb{R})$ le sous-espace de fonctions a support fini: on rappelle que $f : \mathbb{N} \mapsto \mathbb{R}$

$$\text{supp}(f) = \{n \in \mathbb{N},\ f(n) = 0\} \text{ est fini.}$$

Pour $m \in \mathbb{N}$ un sous-ensemble, on note $1_{\{m\}}$ la fonction indicatrice de m:

$$1_{\{m\}}(n) = \begin{cases} 1 & \text{si } n = m \\ 0 & \text{si } n \neq m. \end{cases}.$$

(1) Montrer que la famille

$$\{1_{\{m\}},\ m \geqslant 0\}$$

est une base de $\mathcal{F}_f(\mathbb{N}, \mathbb{R})$.

Le resultat suivant necessite de travailler dans une theorie des ensembles qui contient *l' axiome du choix* (par exemple ZFC).

THÉORÈME 5.6 (Existence de bases sous l'axiome du choix). *Dans une theorie des ensembles contenant l'axiome du choix, tout espace vectoriel possede une base et toutes les bases de V ont meme cardinal: pour toutes bases $\mathscr{B}, \mathscr{B}'$ il existe une bijection*

$$\mathscr{B} \simeq \mathscr{B}'.$$

La dimension de V est de cardinal d'une base:

$$\dim(V) = |\mathscr{B}|.$$

REMARQUE 5.3.1. Le Theoreme de la base incomplete est vrai (sous l'axiome du choix): soit $\mathscr{L} \subset$ une famille libre et $\mathscr{G}$ un famille generatrice. Il existe une famille libre $\mathscr{L}' \subset \mathscr{G}$ telle que $\mathscr{L} \sqcup \mathscr{L}' = \mathscr{B}$ forme une base de V.

Preuve: (idee) Pour demontrer ce theoreme, on utilise l'axiome du choix sous la forme equivalente suivante qu'on appelle

LEMME DE ZORN. *Soit E un ensemble ordonne tel que tout sous-ensemble $A \subset E$ totalement ordonne possede une majorant alors E possede un element maximal.*

On applique le Lemme de Zorn a l'ensemble des familles libres de V ordonne par l'inclusion et on montre qu'une famille libre maximale pour l'inclusion est une base. □

REMARQUE 5.3.2. En fait on peut montrer que le Lemme de Zorn et donc l'axiome du choix sont equivalent a l'existence d'une base pour tout espace vectoriel.

CHAPITRE 6

Applications lineaires

6.1. Le Theoreme Noyau-Image

6.1.1. Preliminaires.

PROPOSITION 6.1. *Soit $\varphi : V \mapsto W$ une application lineaire avec V de dimension finie. Soit $\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_g\} \subset V$ une famille generatrice alors φ est completement determinee par l'ensemble de images des elements de $\mathscr{G}$:*

$$\varphi(\mathscr{G}) = \{\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_g)\} \subset W.$$

En particulier, $\varphi(\mathscr{G})$ est une famille generatrice de $\mathrm{Im}(\varphi)$ *et on a*

$$\dim(\mathrm{Im}\,\varphi) \leqslant \dim(V).$$

Preuve: Soit $v \in V$, comme $\mathscr{G}$ est generatrice il existe $x_1, \cdots, x_g \in K$ tels que

$$x_1.\mathbf{e}_1 + \cdots + x_g\mathbf{e}_g = v$$

et alors

$$\varphi(v) = x_1.\varphi(\mathbf{e}_1) + \cdots + x_g\varphi(\mathbf{e}_g).$$

Ainsi pour connaitre l'image d'un vecteur v il suffit de connaitre les vecteurs

$$\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_g)$$

et une decomposition de v en combinaison lineaire d'elements de $\mathscr{G}$.

En particulier pour $w \in \mathrm{Im}(\varphi)$, il existe $v \in V$ tel que $\varphi(v) = w$; ecrivant

$$x_1.\mathbf{e}_1 + \cdots + x_g\mathbf{e}_g = v$$

on a

$$w = \varphi(v) = x_1.\varphi(\mathbf{e}_1) + \cdots + x_g\varphi(\mathbf{e}_g)$$

Ainsi $\varphi(\mathscr{G})$ est generatrice de $\mathrm{Im}\,\varphi$. En particulier $\mathrm{Im}\,\varphi$ est de dimension finie et

$$\dim(\mathrm{Im}\,\varphi) \leqslant |\varphi(\mathscr{G})|.$$

En particulier si on prend pour $\mathscr{G}$ une base de V, on aura

$$\dim(\mathrm{Im}\,\varphi) \leqslant |\mathscr{G}| = \dim(V).$$

□

DÉFINITION 6.1. *Soit $\varphi : V \mapsto W$ une application lineaire. Le rang de φ est la dimension de* $\mathrm{Im}\,\varphi$*:*

$$\mathrm{rg}(\varphi) = \dim(\mathrm{Im}\,\varphi).$$

REMARQUE 6.1.1. On a l'inegalite

$$\mathrm{rg}(\varphi) \leqslant \min(\dim V, \dim W).$$

En effet on vient de voir que $\mathrm{rg}(\varphi) \leqslant \dim V$ et $\mathrm{rg}(\varphi)$ et c'est la dimension (finie) d'un espace contenu dans un autre espace vectoriel (W) de dimension (par forcement finie) $\dim(W)$ donc

$$\mathrm{rg}(\varphi) \leqslant \dim W.$$

EXERCICE 6.1. Soient V, W deux espaces vectoriels de dimension finie et $\varphi : V \mapsto W$ une application lineaire. Montrer que

(1) Si φ est injective alors l'image par φ d'une famille libre est libre et
$$\dim(V) \leqslant \dim(W)$$
(2) Si φ est surjective alors l'image par φ d'une famille generatrice est generatrice et
$$\dim(V) \geqslant \dim(W).$$
(3) Si φ est bijective, l'image d'une base de V est une base de W et $\dim(V) = \dim(W)$.

EXERCICE 6.2. montrer qu'une application lineaire envoyant une base sur une base est un isomorphisme.

6.1.2. Le Theoreme Noyau-Image.

THÉORÈME 6.1 (Noyau-Image). *Soit $\varphi : V \mapsto W$ une application lineaires avec V de dimension finie. On a*
$$\dim V = \dim(\ker \varphi) + \dim(\operatorname{Im} \varphi).$$

Preuve: Notons que si $\mathscr{B}$ est une base alors $\varphi(\mathscr{B})$ est une partie generatrice de $\operatorname{Im}\varphi$ qui est donc de dimension finie de dimension
$$\dim \operatorname{Im} \varphi \leqslant |\varphi(\mathscr{B})| \leqslant |\mathscr{B}| = \dim(V).$$
Soit $\{\varphi(\mathbf{e}'_1), \cdots, \varphi(\mathbf{e}'_r)\}$ une base de $\operatorname{Im}\varphi$ et $\{\mathbf{e}_1, \cdots, \mathbf{e}_k\}$ une base de $\ker\varphi$. Montrons que
$$\{\mathbf{e}_1, \cdots, \mathbf{e}_k, \mathbf{e}'_1, \cdots, \mathbf{e}'_r\}$$
est une base de V. Supposons que
$$x_1\mathbf{e}_1 + \cdots + x_k\mathbf{e}_k + x'_1\mathbf{e}'_1 + \cdots + x'_r.\mathbf{e}'_r = 0_V$$
alors
$$0_W = x'_1\varphi(\mathbf{e}'_1) + \cdots + x'_r.\varphi(\mathbf{e}'_r)$$
et donc $x'_1 = \cdots = x'_r = 0$. On a alors
$$x_1\mathbf{e}_1 + \cdots + x_k\mathbf{e}_k = 0_V$$
et donc $x_1 = \cdots = x_k = 0$.

Soit $v \in V$ alors
$$\varphi(v) = x'_1\varphi(\mathbf{e}'_1) + \cdots + x'_r.\varphi(\mathbf{e}'_r) = \varphi(x'_1\mathbf{e}'_1 + \cdots + x'_r.\mathbf{e}'_r) = \varphi(v').$$
On a
$$\varphi(v - v') = 0_V \Longrightarrow v - v' \in \ker\varphi$$
et donc
$$v - v' = x_1\mathbf{e}_1 + \cdots + x_k.\mathbf{e}_k$$
et
$$v = x_1\mathbf{e}_1 + \cdots + x_k.\mathbf{e}_k + x'_1\mathbf{e}'_1 + \cdots + x'_r.\mathbf{e}'_r.$$
□

COROLLAIRE 6.1 (Critere de bijectivite). *Soit $\varphi : V \mapsto W$ une application lineaire entre espaces de dimension finie.*

- *Si φ est injective et $\dim(V) = \dim(W)$ alors φ est bijective.*
- *Si φ est surjective et $\dim(V) = \dim(W)$ alors φ est bijective.*

Preuve: Si φ est injective $\dim(\ker\varphi) = 0$ et $\dim(V) = \dim(\operatorname{Im}\varphi)$ et donc $\dim(\operatorname{Im}\varphi) = \dim(W)$ ce qui implique que $W = \operatorname{Im}\varphi$ et la surjectivite et la bijectivite.

Si φ est surjective $\dim(\operatorname{Im}\varphi) = \dim(W) = \dim(V)$ et donc $\dim(\ker\varphi) = 0$ ce qui implique l' injectivite et la bijectivite. □

COROLLAIRE 6.2 (Critere dimensionel d'isomorphisme). *Deux espaces vectoriels de dimension finie sont isomorphes si et seulement si ils ont meme dimension.*

Preuve: Si $\dim V = \dim W$ on a deux isomorphismes donnes par des choix de bases de V et W:

$$CL_{\mathscr{B}} : K^d \simeq V,\ CL_{\mathscr{B}'} : K^d \simeq W$$

et un isomorphisme $CL_{\mathscr{B}'} \circ CL_{\mathscr{B}}^{-1} : V \simeq W$.

Reciproquement si $\varphi : V \simeq W$ est un isomorphisme on a (par injectivite et surjectivite)

$$\dim(V) = 0 + \dim(\mathrm{Im}\,\varphi) = \dim(W).$$

□

6.1.3. Exemple: les formes lineaires.

DÉFINITION 6.2. *Une forme lineaire sur V est une application lineaire a valeurs dans K*

$$\ell : V \mapsto K.$$

On a la proposition suivante:

PROPOSITION 6.2. *Soit ℓ une forme lineaire. Si elle est non-nulle, $\ell \neq \underline{0}_K$ alors* $\mathrm{Im}(\ell) = K$ *et* $\dim(\ker l) = \dim(V) - 1$.

Preuve: Soit $\ell \neq \underline{0}_K$. Soit $v \in V$ tel que $\ell(v) = \lambda \neq 0$; λ est donc inversible, alors pour tout $x \in K$, on a

$$\ell((x/\lambda).v) = (x/\lambda).\lambda = x$$

donc ℓ est surjective. Ainsi $\mathrm{Im}\,\ell = K$ est de dimension 1 et $\ker \ell$ est de diemsnion $\dim V - 1$. □

DÉFINITION 6.3. *Un sous-espace vectoriel de dimension* $\dim V - 1$ *est appelle un hyperplan vectoriel.*

6.2. Structure et dimension des espaces d'applications lineaires

On rappelle que $(\mathrm{Hom}_{K-ev}(V, W), +, .)$ a une structure naturelle de K-espace vectoriel, ou l'addition est donnee

$$\varphi + \psi : v \mapsto \varphi(v) + \psi(v)$$

et la multiplication externe, pour $\lambda \in K$

$$\lambda.\varphi : v \mapsto \lambda.\varphi(v).$$

Rappelons que le fait que $\lambda.\varphi \in \mathrm{Hom}_{K-ev}(V, W)$ provient du fait que K est commutatif: pour $x \in K$

$$\lambda.\varphi(x.v + v') = \lambda(\varphi(x.v + v')) = \lambda(x.\varphi(v) + \varphi(v')) = x.\lambda.\varphi(v) + \lambda.\varphi(v') = x.(\lambda.\varphi)(v) + (\lambda.\varphi)(v').$$

THÉORÈME 6.2 (Dimension de l'espace des applications lineaires). *Si V et W sont de dimension finie, alors* $\mathrm{Hom}_K(V, W)$ *est de dimension finie*

$$\dim(\mathrm{Hom}_K(V, W)) = \dim V. \dim W.$$

Preuve: Soit $\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ une base de V. Soit φ une application lineaire, alors φ est entierement determinee des que l'on connait les valeurs des elements de $\mathscr{B}$

$$\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d) \in W.$$

En effet si $v = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d$ alors

$$\varphi(v) = x_1.\varphi(\mathbf{e}_1) + \cdots + x_d.\varphi(\mathbf{e}_d).$$

En d'autres termes on dispose d'une application injective

$$\mathrm{eval}_{\mathscr{B}} : \varphi \in \mathrm{Hom}_K(V, W) \hookrightarrow (\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)) \in W^d.$$

L'application $\mathrm{eval}_{\mathscr{B}}$ est lineaire puisque

$$(\lambda\varphi+\psi)(\mathbf{e}_i)=\lambda.\varphi(\mathbf{e}_i)+\psi(\mathbf{e}_i)$$

Par ailleurs, cette application est surjective: soit un uplet

$$(f_1,\cdots,f_d)\in W^d$$

alors on associe a $(f_1,\cdots,f_d)$ l'application definie par

$$\varphi(x_1.\mathbf{e}_1+\cdots+x_d.\mathbf{e}_d)=x_1.f_1+\cdots+x_d.f_d.$$

Ainsi on a un isomorphisme

$$\mathrm{eval}_{\mathscr{B}}:\mathrm{Hom}_K(V,W)\simeq W^d$$

et

$$\dim(W^d)=d.\dim(W).$$

□

On va maintenant decrire une base de $\mathrm{Hom}_K(V,W)$.

6.2.1. Formes lineaires, dualite et base duale.

DÉFINITION 6.4. *On note l'espace des formes lineaires $\ell:V\mapsto K$,*

$$V^*:=\mathrm{Hom}_{K-ev}(V,K)$$

et on l'appelle le dual de V.

Comme $\dim K=1$, on a

$$\dim(V^*)=\dim\mathrm{Hom}_K(V,K)=\dim(V).$$

En particulier un espace vectoriel V et son dual sont isomorphes. Plus precisement, soit

$$\mathscr{B}=\{\mathbf{e}_1,\cdots,\mathbf{e}_d\}$$

une base de V, on a alors un isomorphisme

$$\mathrm{Eval}_{\mathscr{B}}:\ell\mapsto(\ell(\mathbf{e}_1),\cdots,\ell(\mathbf{e}_d))\in K^d.$$

DÉFINITION 6.5. *Soit $\mathscr{B}$ une base de V, la base duale de $\mathscr{B}$, $\mathscr{B}^*\subset V^*$ est l'image reciproque de la base canonique $\mathscr{B}_d^0=\{\mathbf{e}_i^0,\ i\leqslant d\}\subset K^d$ par l'application $\mathrm{Eval}_{\mathscr{B}}$. On pose*

$$\mathbf{e}_i^*=\mathrm{Eval}_{\mathscr{B}}^{-1}(\mathbf{e}_i^0),$$

De sorte que

$$\mathscr{B}^*=\{\mathbf{e}_i^*,\ i\leqslant d\}$$

et c'est une base (car image d'une base par un isomorphisme).

PROPOSITION 6.3. *Soit $\mathscr{B}=\{\mathbf{e}_1,\cdots,\mathbf{e}_d\}\subset V$ et $\mathscr{B}^*=\{\mathbf{e}_1^*,\cdots,\mathbf{e}_d^*\}\subset V^*$ la base duale. On a*

$$\forall i,j\leqslant d,\ \mathbf{e}_i^*(\mathbf{e}_j)=\delta_{i=j}=\begin{cases}1 & si\ i=j\\ 0 & si\ i\neq j\end{cases}.$$

Preuve: On a

$$\mathrm{Eval}_{\mathscr{B}}(\mathbf{e}_i^*)=(\mathbf{e}_i^*(\mathbf{e}_1),\cdots,\mathbf{e}_i^*(\mathbf{e}_d))=\mathbf{e}_i=(\delta_{i=j})_{j\leqslant d}.$$

□

COROLLAIRE 6.3. *Soit $\ell:V\mapsto K$ une forme lineaire. On a*

$$\ell=\sum_{i=1}^{d}\ell(\mathbf{e}_i)\mathbf{e}_i^*.$$

Autrement dit, les coordonnees de ℓ dans la base $\mathscr{B}^*$ sont donnees par les $(\ell(\mathbf{e}_i))_{i\leqslant d}$ (ie. les valeurs de ℓ en chacun des $\mathbf{e}_i$, $i\leqslant d$).

Preuve: On a

$$\ell = \sum_{i \leqslant d} l_i \mathbf{e}_i^*$$

et donc

$$\ell(\mathbf{e}_i) = \sum_{k \leqslant d} l_k \mathbf{e}_k^*(\mathbf{e}_i) = \sum_{k \leqslant d} l_k \delta_{k=i} = l_i.$$

□

REMARQUE 6.2.1. On a deux isomorphismes

$$\mathrm{Eval}_{\mathscr{B}} : V^* \simeq K^d,\ CL_{\mathscr{B}} : K^d \simeq V$$

et donc un isomorphisme

$$CL_{\mathscr{B}} \circ \mathrm{Eval}_{\mathscr{B}} : V^* \simeq V$$

entre V et son dual V^*. Il faut noter que cet isomorphisme depend du choix de $\mathscr{B}$.

EXERCICE 6.3. Soit $V^{**} = (V^*)^*$ le bi-dual de V (le dual du dual V^* de V). On considere l'application:

$$\mathrm{eval}_\bullet : \begin{array}{ccc} V & \mapsto & V^{**} = (V^*)^* \\ v & \mapsto & \mathrm{eval}_v \end{array}$$

ou

$$\mathrm{eval}_v : \ell \mapsto \ell(v) \in K$$

est l'application qui a une forme lineaire ℓ associe sa valeur au vecteur v.

(1) Montrer que eval_v est bien une forme lineaire sur V^*.
(2) Montrer que $\mathrm{eval}_\bullet$ est un isomorphisme.

REMARQUE 6.2.2. A la difference de l'isomorphisme $CL_{\mathscr{B}} \circ \mathrm{Eval}_{\mathscr{B}} : V^* \simeq V$ qui depend du choix d'une base. L'isomorphisme $\mathrm{eval}_\bullet : V \simeq V^{**}$ n'en depend pas. On dit que le bidual de V est canoniquement isomorphe a V.

6.2.2. Application lineaire duale. Soit $\varphi : V \mapsto W$ une application lineaire. Alors φ induit une application entre les espaces duaux qui va dans "l'autre sens":

$$\varphi^* : W^* \mapsto V^*$$

qui a une forme lineaire $\ell : w \in W \mapsto \ell(w) \in K$ associe la forme lineaire sur V definie par composition

$$\varphi^*(\ell) := \ell \circ \varphi : \begin{array}{ccc} V & \mapsto & K \\ v & \mapsto & \ell(\varphi(v)) \end{array}.$$

En effet $\varphi^*(\ell)$ est a valeurs dans K et est lineaire comme composee de deux formes lineaires.

PROPOSITION 6.4. *L'application*

$$\varphi^* : \ell \in W^* \mapsto \ell \circ \varphi \in V^*$$

est lineaire:

$$\varphi^* \in \mathrm{Hom}(W^*, V^*).$$

Preuve: Soit $\ell, \ell' \in W^*$ et $\lambda \in K$, on veut montrer que

$$\varphi^*(\lambda.\ell + \ell') = \lambda\varphi^*(\ell) + \varphi^*(\ell').$$

Pour tout $v \in V$ on a

$$\varphi^*(\lambda.\ell + \ell')(v) = (\lambda.\ell + \ell')(\varphi(v)) = \lambda.\ell(\varphi(v)) + \ell'(\varphi(v)) = \lambda\varphi^*(\ell)(v) + \varphi^*(\ell')(v).$$

□

EXERCICE 6.4 (le bi-dual). Montrer que l'application

$$\bullet^* : \varphi \in \mathrm{Hom}(V,W) \mapsto \varphi^* \in \mathrm{Hom}(W^*,V^*)$$

qui a une application linaire associe l'application lineaire duale est elle meme lineaire:

$$\bullet^* \in \ \mathrm{Hom}(\mathrm{Hom}(V,W),\mathrm{Hom}(W^*,V^*)).$$

6.2.3. Representation parametrique et cartesienne d'un SEV. Soit $W \subset V$ un SEV d'un espace vectoriel de dimension finie $d_V = \dim V$ alors W est de dimension finie $d_W = \dim W$.

Soit $\mathscr{G}_W = \{\mathbf{e}_1, \cdots, \mathbf{e}_g\},\ g \geqslant d_W$ une famille generatrice de W, alors par definition W est l'ensemble des vecteur de v de la forme

$$W = \{v \in V,\ v = x_1.\mathbf{e}_1 + \cdots + x_g.\mathbf{e}_g\}$$

Une telle presentation s'appelle une *representation parametrique* de V. En particulier si $\mathscr{G}_W = \mathscr{B}_W$ est une base de W le nombre de vecteur $\mathbf{e}_i$ impliques dans cette representation est minimal et vaut d_W.

Par ailleurs un SEV admet egalement une representation cartesienne (sous forme d'equation):

PROPOSITION 6.5 (Representation cartesienne d'un SEV). *Soit $W \subset V$ un SEV. Il existe $d_V - d_W$ formes lineaires*

$$\mathscr{L}_W^* = \{\ell_1, \cdots, \ell_{d_V - d_W}\} \subset V^*$$

lineairement independantes (ie telles que $\mathscr{L}_W^*$ soit libre) telles que

$$W = \{v \in V,\ \ell_1(v) = \cdots = \ell_{d_V - d_W}(v) = 0\}.$$

De maniere equivalente, $W = \ker \varphi_{\mathscr{L}_W^*}$ avec

$$\varphi_{\mathscr{L}_W^*} : v \in V \mapsto (\ell_1(v), \cdots, \ell_{d_V - d_W}(v)) \in K^{d_V - d_W}.$$

Preuve: Soit $\mathscr{B}_W = \{\mathbf{e}_1, \cdots, \mathbf{e}_{d_W}\}$ une base de W et

$$\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_{d_W}, \mathbf{e}_{d_W+1}, \cdots, \mathbf{e}_{d_V}\}$$

une base de V contenant la base precedente. Soit

$$\mathscr{B}^* = \{\mathbf{e}_1^*, \cdots, \mathbf{e}_{d_W}^*, \mathbf{e}_{d_W+1}^*, \cdots, \mathbf{e}_{d_V}^*\}$$

la base duale. Alors

$$W = \{v \in V,\ \mathbf{e}_{d_W+1}^*(v) = \cdots = \mathbf{e}_{d_V}^*(v) = 0\}$$

□

EXERCICE 6.5. Dans $\mathbb{Q}^3$, soit $W = \langle (1,1,0), (1,0,3)\rangle$. Donner une equation cartesienne de W.

EXERCICE 6.6. Dans $\mathbb{Q}^3$, soit $W = \{(x,y,z) \in \mathbb{Q}^3,\ x + y - z = 0,\ x - 2y + 3z = 0\}$. Donner une equation parametrique de W.

6.2.4. Une base de $\mathrm{Hom}(V,W)$**.** Soient V et W des EVs de dimensions finies d et d'.

On a vu que $\dim \mathrm{Hom}(V,W) = \dim(W^d) = \dim V \dim W$. on va donner une base explicite de cet espace.

Etant donne $\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ et $\mathscr{B}' = \{\mathbf{f}_1, \cdots, \mathbf{f}_{d'}\}$ des bases de V et W, on va construire une base de $\mathrm{Hom}(V,W)$: soit

$$\mathscr{B}^* = \{\mathbf{e}_1^*, \cdots, \mathbf{e}_d^*\}$$

la base duale de $\mathscr{B}$, et definissons pour $i \in \{1, \cdots, d'\},\ j \in \{1, \cdots, d\}$ l'application

$$\mathcal{E}_{ij} : \begin{array}{ccc} V & \mapsto & W \\ v & \mapsto & \mathbf{e}_j^*(v).\mathbf{f}_i \end{array}$$

En d'autre termes, si

$$v = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d,$$

$\mathcal{E}_{ij}(v)$ est egal a $x_j.\mathbf{f}_i$, cad le produit de la j-eme coordonnee de v, x_j dans la base $\mathscr{B}$ et du i-ieme vecteur de la base $\mathscr{B}'$.

En particulier on a pour $k = 1, \cdots, d$

$$\mathcal{E}_{ij}(\mathbf{e}_k) = \begin{cases} \mathbf{f}_i & \text{si } k = j \\ 0_W & \text{si } k \neq j \end{cases}.$$

LEMME 6.1. *L'application $\mathcal{E}_{ij} : V \mapsto W$ est lineaire, de rang 1, d'image $K.\mathbf{f}_i$ et de noyau*

$$\ker \mathcal{E}_{ij} = \langle \mathscr{B} - \{\mathbf{e}_j\} \rangle = K.\mathbf{e}_1 + \cdots + K.\mathbf{e}_{j-1} + K.\mathbf{e}_{j+1} + \cdots + K.\mathbf{e}_d$$

l'hyperplan vectoriel engendre par les vecteur de la base $\mathscr{B}$ moins le vecteur $\mathbf{e}_j$.

Preuve: Comme $\mathbf{e}_j^*$ est lineaire on a

$$\mathcal{E}_{ij}(\lambda.v + v') = \mathbf{e}_j^*(\lambda.v + v').\mathbf{f}_i = (\lambda.x_j + x'_j).\mathbf{f}_j = \lambda.x_j.\mathbf{f}_i + x'_j.\mathbf{f}_i = \lambda\mathcal{E}_{ij}(v) + \mathcal{E}_{ij}(v').$$

Il est clair que $\operatorname{Im} \mathcal{E}_{ij} \subset K.\mathbf{f}_i$ et comme $\mathcal{E}_{ij}(\mathbf{e}_j) = \mathbf{f}_i$ on a egalite. Ainsi $\operatorname{rg}(\mathcal{E}_{ij}) = 1$ ($\mathbf{f}_i \neq 0_W$, ce vecteur etant dans une base).

Par ailleurs ($\mathbf{f}_i \neq 0_W$) il est clair que $\mathcal{E}_{ij}(v) = x_j.\mathbf{f}_i = 0_W$ si et seulement si la j-eme coordonnee x_j de v dans la base $\mathscr{B}$ est nulle. □

THÉORÈME 6.3 (Une base de l'espace des applications lineaires). *La famille d'applications lineaires*

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'} := \{\mathcal{E}_{ij},\ i \leqslant d',\ j \leqslant d\} \subset \operatorname{Hom}_{K-ev}(V, W)$$

forme une base de $\operatorname{Hom}_{K-ev}(V, W)$.

Preuve: Comme le cardinal de cette famille vaut $\dim(V)\dim(W) = \dim \operatorname{Hom}_{K-ev}(V, W)$ il suffit de montrer qu'elle est libre: soit $m_{ij} \in K, i \leqslant d', j \leqslant d$ des scalaires tels que

$$\sum_{i,j} \sum m_{ij}\mathcal{E}_{ij} = \underline{0}_W.$$

On a donc pour chaque $k \leqslant d$

$$(\sum_{i,j} \sum m_{ij}\mathcal{E}_{ij})(\mathbf{e}_k) = \sum_i \sum m_{ik}\mathbf{f}_i = 0_W.$$

Comme $\mathscr{B}'$ est une base de W on a

$$m_{ik} = 0,\ i \leqslant d'$$

et donc pour tout i, j on a $m_{ij} = 0$. □

REMARQUE 6.2.3. Comme la notation l'indique $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$ depend du choix d'une base de $\mathscr{B}$ et d'une base de $\mathscr{B}'$. Les applications $\mathcal{E}_{ij}$ sont appellees *applications elementaires* associees aux bases $\mathscr{B}$ et $\mathscr{B}'$.

6.2.5. Image d'un vecteur. Soient V, W de dimensions d, d' finies et de bases

$$\mathscr{B} = \{\mathbf{e}_j,\ j \leqslant d\}, \mathscr{B}' = \{\mathbf{f}_i,\ i \leqslant d'\}.$$

Soit

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'} = \{\mathcal{E}_{ij} = \mathbf{e}_j^*.\mathbf{f}_i,\ i \leqslant d',\ j \leqslant d\} \subset \operatorname{Hom}_{K-ev}(V, W)$$

la base de l'espace des application lineaires formee des applications elementaires.

PROPOSITION 6.6. *Soit $\varphi : V \mapsto W$ une application lineaire et $(m_{ij})_{i \leqslant d', j \leqslant d}$ les coordonnees de φ dans la base $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$. Alors pour $k = 1, \cdots, d$ les*

$$(m_{i,k})_{i \leqslant d'}$$

sont les coordonnees de $\varphi(\mathbf{e}_k)$ dans la base $\mathscr{B}'$.

Preuve: On a

$$\varphi(\mathbf{e}_k) = (\sum_{i,j}\sum m_{ij}\mathcal{E}_{ij})(\mathbf{e}_k) = \sum_{i,j}\sum m_{ij}\mathcal{E}_{ij}(\mathbf{e}_k) = \sum_{i\leqslant d'} m_{ik}\mathbf{f}_i.$$

□

Soit $v \in V$ un vecteur de coordonnees $(x_j)_{j\leqslant d}$ dans la base $\mathscr{B}$. Calculons les coordonnees $(y_i)_{i\leqslant d'}$ de $\varphi(v) \in W$ dans la base $\mathscr{B}'$:

PROPOSITION 6.7. *Avec les notations precedentes, si* $v = \sum_{j=1}^{d} x_j\mathbf{e}_j$, *on a*

$$\varphi(v) = \sum_{i=1}^{d'} y_i\mathbf{f}_i \text{ avec } y_i = \sum_{j\leqslant d} m_{ij}.x_j.$$

Preuve: on a

$$v = \sum_{j\leqslant d} x_j\mathbf{e}_j,\ \varphi(v) = \sum_{i\leqslant d'} y_i\mathbf{f}_i$$

et

$$\varphi(\mathbf{e}_j) = \sum_{i\leqslant d'} m_{ij}\mathbf{f}_i.$$

Ainsi on a

$$\varphi(v) = \sum_{j\leqslant d} x_j\varphi(\mathbf{e}_j) = \sum_{j\leqslant d} x_j(\sum_{i\leqslant d'} m_{ij}\mathbf{f}_i) = \sum_{i\leqslant d'}(\sum_{j\leqslant d} m_{ij}.x_j).\mathbf{f}_i$$

On a donc

$$y_i = \sum_{j\leqslant d} m_{ij}.x_j.$$

□

6.2.6. Combinaison lineaire d'applications lineaires.

PROPOSITION 6.8. *Soit*

$$\varphi, \psi : V \mapsto W$$

deux applications lineaires et $(m_{ij})_{i\leqslant d, j\leqslant d'}$, $(n_{ij})_{i\leqslant d, j\leqslant d'}$ *leurs coordonnees dans la base* $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$. *Pour tout* $\lambda \in K$, $\lambda.\varphi + \psi$ *est lineaire et ses coordonnees dans la base* $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$ *sont donnees par*

$$(\lambda.m_{ij} + n_{ij})_{i\leqslant d, j\leqslant d'}.$$

Preuve: En effet pour tout EV E et toute base $\mathscr{B}_E$ de E et tout vecteur $\mathbf{g} \in \mathscr{B}_E$ de cette base, la fonction coordonnee $\mathbf{g}^* : E \mapsto K$ qui a un element associe sa coordonne suivant le vecteur $\mathbf{g}$ est une forme lineaire. On applique cela a $\mathrm{Hom}(V, W)$ et aux vecteurs de la base $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$. □

6.2.7. Composition d' applications lineaires. Soient U, V, W trois espaces vectoriels. Soient deux applications lineaires

$$\varphi : U \mapsto V,\ \psi : V \mapsto W \text{ et } \psi \circ \varphi : U \mapsto W$$

leur composee. Soient

$$\mathscr{B} = \{\mathbf{e}_k,\ k \leqslant d\}, \mathscr{B}' = \{\mathbf{f}_j,\ j \leqslant d'\}, \mathscr{B}'' = \{\mathbf{g}_i,\ i \leqslant d''\}$$

des bases de U, V et W, on dispose alors de bases

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'} = \{\mathbf{e}_k^*.\mathbf{f}_j\},\ \mathcal{B}_{\mathscr{B}',\mathscr{B}''} = \{\mathbf{f}_j^*.\mathbf{g}_i\},\ \mathcal{B}_{\mathscr{B},\mathscr{B}''} = \{\mathbf{e}_k^*.\mathbf{g}_i\}$$

pour

$$\mathrm{Hom}(U, V),\ \mathrm{Hom}(V, W),\ \mathrm{Hom}(U, W),$$

THÉORÈME 6.4. *Soient $(n_{jk})_{j\leqslant d',k\leqslant d}$ les coordonnees de φ dans la base $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$ et $(m_{ij})_{i\leqslant d'',j\leqslant d'}$ les coordonnees de ψ dans la base $\mathcal{B}_{\mathscr{B}',\mathscr{B}''}$. Alors les coordonnees $(l_{ik})_{i\leqslant d'',k\leqslant d}$ de $\psi\circ\varphi$ dans la base $\mathcal{B}_{\mathscr{B},\mathscr{B}''}$ sont donnees par*

$$l_{ik}=\sum_{j=1}^{d'}m_{ij}.n_{jk}.$$

Preuve: Ecrivons

$$\varphi=\sum_{j\leqslant d',k\leqslant d}\sum n_{jk}\mathbf{e}_k^*.\mathbf{f}_j,\ \psi=\sum_{j\leqslant d',i\leqslant d''}\sum m_{ij}\mathbf{f}_j^*.\mathbf{g}_i.$$

On a pour tout $k\leqslant d$ et $j\leqslant d'$

$$\varphi(\mathbf{e}_k)=\sum_{j\leqslant d'}n_{jk}\mathbf{f}_j,\ \psi(\mathbf{f}_j)=\sum_{i\leqslant d''}m_{ij}\mathbf{g}_i$$

et

$$\psi(\varphi(\mathbf{e}_k))=\sum_{j\leqslant d'}n_{jk}\psi(\mathbf{f}_j)=\sum_{j\leqslant d'}n_{jk}\sum_{i\leqslant d''}m_{ij}\mathbf{g}_i=\sum_{i\leqslant d''}(\sum_{j\leqslant d'}m_{ij}n_{jk}).\mathbf{g}_i=\sum_{i\leqslant d''}l_{ik}.\mathbf{g}_i$$

Ainsi

$$l_{ik}=\sum_{j\leqslant d'}m_{ij}n_{jk}.$$

□

6.3. L'algebre des endomorphismes d'un espace vectoriel

soit V un K-ev de dimension $d\geqslant 1$. On a vu dans la section §3.2.7 que l'espace des endomorphismes de V

$$\mathrm{End}_K(V)=\{\varphi:V\mapsto V,\ \text{ lineaire }\}$$

muni de l'addition et de la composition des endomorphismes, de l'application nulle $\underline{\mathbf{0}}_V$ comme element neutre et de l'identite Id_V comme element unite est une K-algebre de dimension d^2.

Le groupes des elements inversibles de cette algebre $\mathrm{End}_K(V)^\times$ n'est autre que le groupe $\mathrm{Aut}_K(V)$ des automorphismes de l'espace vectoriel V et de maniere equivalente (par le Theoreme Noyau-Image)

(1) L'ensemble des applications lineaires de V sur V bijectives,
(2) L'ensemble des applications lineaires de V sur V injectives,
(3) L'ensemble des applications lineaires de V sur V surjectives.

DÉFINITION 6.6. *Le groupe $\mathrm{End}_K(V)^\times$ est egalement appelle le groupe lineaire de V et se note egalement*

$$\mathrm{GL}(V)=\mathrm{End}_K(V)^\times=\mathrm{Aut}_K(V).$$

Notons la propriete suivante de l'algebre $\mathrm{End}_K(V)$ qui n'est pas vraie pour l'algebre des endomorphisme d'un module sur un anneau general: pour qu'un endomorphisme soit inversible il suffit qu'il admette un inverse a gauche.

THÉORÈME 6.5 (Critere d'inversibilite des endomorphismes). *Soit $\varphi\in\mathrm{End}_K(V)$. Les proprietes suivantes sont equivalentes*

(1) φ est injectif.
(2) φ est surjectif.
(3) φ est inversible (ie. appartient a $\mathrm{GL}(V)$).
(4) φ admet un inverse a droite: il existe $\psi\in\mathrm{End}_K(V)$ tel que

$$\varphi\circ\psi=\mathrm{Id}_V.$$

(5) φ admet un inverse a gauche: il existe $\psi'\in\mathrm{End}_K(V)$ tel que

$$\psi'\circ\varphi=\mathrm{Id}_V.$$

Dans ce cas on a

$$\varphi^{-1} = \psi = \psi'.$$

Preuve: Exercice (utiliser le Theoreme Noyau-Image). □

CHAPITRE 7

Matrices

- M: Do you know what I'm talking about ?
- N: The Matrix ?
- M: Do you want to know what IT is ?
The Matrix is everywhere. It is all around us.
Even now, in this very room.

7.1. Matrices et applications lineaires

Soient V, W des ev de dimension finie munis de bases

$$\mathscr{B} = \{\mathbf{e}_j,\ j \leqslant d\}, \mathscr{B}' = \{\mathbf{f}_i,\ i \leqslant d'\}.$$

Alors on a des isomorphismes d'espaces vectoriels

$$CL_{\mathscr{B}} : K^d \simeq V,\ CL_{\mathscr{B}'} : K^d \simeq W$$

qui permettent d'identifier V et W aux espaces produits K^d et $K^{d'}$ et d'identifier des vecteurs $v \in V$ et $w \in W$ avec des uplets

$$(x_j)_{j\leqslant d} = (x_1, \cdots, x_d) \in K^d,\ (y_i)_{i\leqslant d'} = (y_1, \cdots, y_{d'}) \in K^{d'}.$$

On dispose egalement d'une base

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'} = \{\mathcal{E}_{ij} = \mathbf{e}_j^*.\mathbf{f}_i,\ i \leqslant d',\ j \leqslant d\}$$

de $\mathrm{Hom}(V, W)$. L'application

$$CL_{\mathcal{B}_{\mathscr{B},\mathscr{B}'}} : (m_{ij})_{i\leqslant d', j\leqslant d} \in (K^{d'})^d \mapsto \varphi = \sum_{i\leqslant d', j\leqslant d} m_{ij}\mathcal{E}_{ij} \in \mathrm{Hom}(V, W) \tag{7.1.1}$$

est un isomorphisme d'espaces vectoriels entre $(K^{d'})^d$ et $\mathrm{Hom}(V, W)$; cet isomorphisme permet d'identifier toute application lineaire φ avec un $d' \times d$ uplet $(m_{ij})_{i\leqslant d', j\leqslant d}$.

Définition 7.1. *L'espace vectoriel $(K^{d'})^d$ s'appelle l'espace des matrices de dimension $d' \times d$ a coefficients dans K et est note*

$$M_{d'\times d}(K) = \{(m_{ij})_{i\leqslant d', j\leqslant d},\ m_{ij} \in K\}.$$

Un element de $M_{d'\times d}(K)$ est appelle matrice de dimensions $d' \times d$ ou juste une matrice $d' \times d$.

On a coutume de representer une matrice $(m_{ij})_{i\leqslant d', j\leqslant d}$ comme un "tableau" de dimension 2 possedant d' lignes et d colonnes: ainsi m_{ij} est le coefficient de ce tableau qui se trouve a l'intersection de la i-ieme ligne et de la j-ieme colonne.

$$M = (m_{ij})_{i\leqslant d', j\leqslant d} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix}.$$

REMARQUE 7.1.1. Habituellement quand on repere un point dan le plan, la premiere coordonnee i donne la "position horizontale" et la seconde j la "position verticale". On prend ici la convention symetrique et il y a de bonnes rasions pour cela notamment lies au sens de l'ecriture gauche-droite.

DÉFINITION 7.2. *Soient $\mathscr{B} \subset V$, $\mathscr{B}' \subset W$ des bases comme ci-dessous et $\mathcal{B}_{\mathscr{B},\mathscr{B}'} \subset \mathrm{Hom}(V,W)$ la base de $\mathrm{Hom}(V,W)$ associee. L'application reciproque $CL^{-1}_{\mathcal{B}_{\mathscr{B},\mathscr{B}'}}$ sera egalement notee*

$$\mathrm{mat}_{\mathscr{B}',\mathscr{B}} : \mathrm{Hom}(V,W) \mapsto M_{d'\times d}(K).$$

Explicitement, si on la la decomposition $\varphi = \sum_{i\leqslant d',j\leqslant d} m_{ij}(\varphi)\mathcal{E}_{ij}$ alors on a

$$\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi) = (m_{ij}(\varphi))_{i\leqslant d',j\leqslant d} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix}.$$

La matrice $\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$ est appellee matrice associee a φ dans les bases $\mathscr{B},\mathscr{B}'$. Rappelons que pour tout $1 \leqslant j \leqslant d$, $(m_{i,j}(\varphi))_{i\leqslant d'}$ est l'ensemble des coordonnees de $\varphi(\mathbf{e}_j)$ pour $\mathbf{e}_j \in \mathscr{B}$ dans la base $\mathscr{B}'$: ie.

$$\varphi(\mathbf{e}_j) = \sum_{1\leqslant i\leqslant d'} m_{ij}(\varphi)\mathbf{f}_i.$$

EXEMPLE 7.1.1. Si $\varphi = \underline{0}_W$ alors

$$\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\underline{0}_W) = (0_K)_{i,j} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \underline{0}_{d'\times d}$$

est la matrice nulle.

Si $V = W$, $\mathscr{B} = \mathscr{B}'$ et $\varphi = \mathrm{Id}_V$ est l'identite alors

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_V) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = (\delta_{i=j})_{i,j} =: \mathrm{Id}_d \in M_{d\times d}(K). \tag{7.1.2}$$

est appelee matrice identite de rang d et est notee Id_d. Plus generalement une matrice de la forme, $\lambda \in K$

$$\lambda.\mathrm{Id}_d = \lambda.\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \cdots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix}$$

est appellee matrice scalaire. On note

$$K.\mathrm{Id}_d = \{\lambda.\mathrm{Id},\ \lambda \in K\} \subset M_d(K)$$

l'ensemble des matrices scalaires. C'est un SEV de dimension 1 isomorphe a K.

7.1.0.1. *Base canonique des matrices elementaires.* Une base de $M_{d'\times d}(K)$ est obtenue en transportant une base de $\mathrm{Hom}(V,W)$ via cet isomorphisme, en particulier la base des applications elementaires

$$\mathcal{E}_{ij} = \mathbf{e}_j^*.\mathbf{f}_i.$$

On note $E_{ij} = \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\mathcal{E}_{ij})$ la matrice correspondante qu'on appelle *matrice elementaire*. L' ensemble des matrices elementaires

$$\{E_{ij},\ i \leqslant d', j \leqslant d\}$$

est donc une base de $M_{d'\times d}(K)$ qu'on appelle egalement la *base canonique*.

De part sa definition, E_{ij} est la matrice dont le coefficient a l'intersection de la i-ieme ligne et de la j-ieme colonne vaut 1 et tous les autres coefficients sont nuls: pour $k \leqslant d', l \leqslant d$, on a

$$E_{ij,kl} = \delta_{k=i}.\delta_{l=j}.$$

7.1.0.2. *Quelques cas particuliers importants de matrices.*

– *Matrices colonnes.*

$$M_{d'\times 1}(K) =: \mathrm{Col}_{d'}(K)$$

sont des matrices "colonnes" de hauteur d'. on posera

$$\mathrm{Col}((x_i)_{i\leqslant d'}) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{d'} \end{pmatrix}.$$

– *Matrices lignes.* Les element de

$$M_{1\times d}(K) =: \mathrm{Lig}_d(K)$$

sont des matrices "lignes" de longueur d: on posera

$$\mathrm{Lig}((x_j)_{j\leqslant d}) = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix}.$$

– *Matrices carrees.* Si $d' = d$ on dit que la matrice est carree et notera l'espaces des matrices carrees de taille d par

$$M_d(K) = M_{d\times d}(K)$$

Définition 7.3. *Soient $\mathscr{B} \subset V$, $\mathscr{B}' \subset W$ des bases. Soit*

$$v = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d \in V$$

un vecteur decompose dans la base $\mathscr{B}$. Alors la matrices

$$\mathrm{C}_{\mathscr{B}}(v) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix},\ \mathrm{L}_{\mathscr{B}}(v) = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix}$$

sont appellees respectivement

- *la matrice colonne associee a v dans la base $\mathscr{B}$,*
- *La matrice ligne associee a v dans la base $\mathscr{B}$,*

Ces applications sont des isomorphisme entre V et $\mathrm{Col}_d(K)$ et $\mathrm{Lig}_d(K)$.

7.1.0.3. *Colonnes et lignes extraites d'une matrice.*

Définition 7.4. *Soit une matrice*

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix} \in M_{d'\times d}(K).$$

Pour $j \leqslant d$ (resp. $i \leqslant d'$), la j-ieme colonne de M (resp. la i-ieme ligne de M) est la matrice colonne (resp. ligne)

$$\mathrm{Col}_j(M) = \begin{pmatrix} m_{1j} \\ m_{2j} \\ \vdots \\ m_{d'j} \end{pmatrix} \in \mathrm{Col}_{d'}(K),\ \textit{resp.}\ \mathrm{Lig}_i(M) = \begin{pmatrix} m_{i1} & m_{i2} & \cdots & m_{id} \end{pmatrix} \in \mathrm{Lig}_d(K)$$

7.1.1. Addition et multiplication par les scalaires. Les espaces de matrices $M_{d',d}(K)$ sont naturellement des K-ev pour les lois d'addition et de multiplication par les scalaires evidentes

$$\lambda.M+M'=(\lambda.m_{ij}+m'_{ij})_{ij}=\begin{pmatrix}\lambda.m_{11}+m'_{11} & \lambda.m_{12}+m'_{12} & \cdots & \lambda.m_{1d}+m'_{1d}\\ \lambda.m_{21}+m'_{21} & \lambda.m_{22}+m'_{22} & \cdots & \lambda.m_{2d}+m'_{2d}\\ \vdots & \vdots & \cdots & \vdots\\ \lambda.m_{d'1}+m'_{d'1} & \lambda.m_{d'2}+m'_{d'2} & \cdots & \lambda.m_{d'd}+m'_{d'd}\end{pmatrix}$$

de sorte que l'application

$$\mathrm{mat}_{\mathscr{B}',\mathscr{B}}:\varphi\in\mathrm{Hom}(V,W)\mapsto\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)\in M_{d'\times d}(K)$$

est un isomorphisme de K-ev.

Il est facile de verifier que les applications lignes et colonnes

$$\mathrm{Col}_i:M_{d'\times d}(K)\mapsto\mathrm{Col}_{d'}(K)(K),\ \mathrm{Lig}_j:M_{d'\times d}(K)\mapsto\mathrm{Lig}_d(K)$$

sont lineaires.

7.1.2. Multiplication de matrices. Soient U,V,W trois espaces vectoriels munis de bases

$$\mathscr{B}=\{\mathbf{e}_k,\ k\leqslant d\},\mathscr{B}'=\{\mathbf{f}_j,\ j\leqslant d'\},\mathscr{B}''=\{\mathbf{g}_i,\ i\leqslant d''\}.$$

On dispose alors de bases

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'}=\{\mathbf{e}_k^*.\mathbf{f}_j\},\ \mathcal{B}_{\mathscr{B}',\mathscr{B}''}=\{\mathbf{f}_j^*.\mathbf{g}_i\},\ \mathcal{B}_{\mathscr{B},\mathscr{B}''}=\{\mathbf{e}_k^*.\mathbf{g}_i\}$$

pour

$$\mathrm{Hom}_{K-ev}(U,V),\ \mathrm{Hom}_{K-ev}(V,W),\ \mathrm{Hom}_{K-ev}(U,W).$$

Soient

$$\varphi:U\mapsto V,\ \psi:V\mapsto W$$

deux applications lineaires et

$$\psi\circ\varphi:U\mapsto W$$

leur composee.

Soient alors

$$N:=\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)=(n_{jk})_{j\leqslant d',k\leqslant d}\in M_{d'\times d}(K)$$

et

$$M:=\mathrm{mat}_{\mathscr{B}'',\mathscr{B}'}(\psi)=(m_{ij})_{i\leqslant d'',j\leqslant d'}\in M_{d''\times d'}(K)$$

et

$$L:=\mathrm{mat}_{\mathscr{B}'',\mathscr{B}}(\psi\circ\varphi)=(l_{ik})_{i\leqslant d'',k\leqslant d}\in M_{d''\times d}(K)$$

On a vu (Thm 6.4) que les l_{ik} pouvaient s'exprimer en fonction des m_{ij} et des n_{jk}. Plus precisement, on a

$$l_{ik}=\sum_{j=1}^{d'}m_{ij}.n_{jk}.$$

On definit ainsi une loi de multiplication (externe) sur les espaces de matrices en posant:

Définition 7.5. *Soient $d,d',d''\geqslant 1$ et $M\in M_{d''\times d'}(K)$, $N\in M_{d'\times d}(K)$, on defini le produit des matrices M et N comme etant la matrice*

$$L=M.N\in M_{d''\times d}(K)$$

avec

$$L=(l_{ik})_{i\leqslant d'',k\leqslant d}\in M_{d''\times d}(K)\ \textit{avec}\ l_{ik}=\sum_{j=1}^{d'}m_{ij}.n_{jk}.$$

Exemple 7.1.2. Quelques cas particuliers importants:

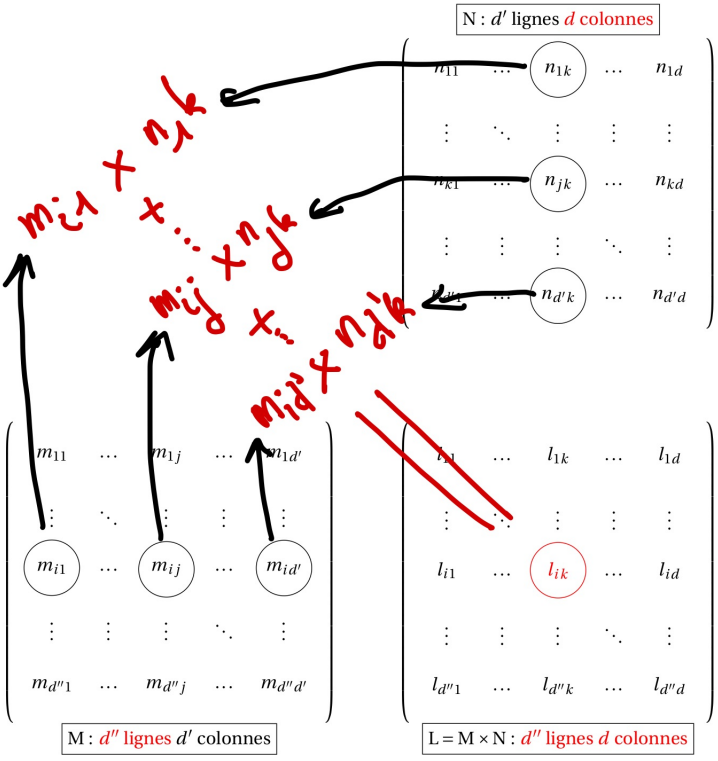


FIGURE 1. Calcul des coordonnees du produit de deux matrices

– Si $d = 1$: on dispose d'une multiplication "externe" (a gauche) a valeurs dans les matrices colonnes: on a $M_{d'\times 1}(K) = \mathrm{Col}_{d'}(K)$ et donc

$$\bullet.\bullet : M_{d''\times d'}(K) \times \mathrm{Col}_{d'}(K) \mapsto \mathrm{Col}_{d''}(K).$$

– Si $d'' = d' = d$: les matrices sont toutes carrees et on dispose d'une multiplication "interne" sur l'espace des matrices carrees de taille d:

$$\bullet \times \bullet : M_d(K) \times M_d(K) \mapsto M_d(K).$$

THÉORÈME 7.1 (Proprietes fonctionelles du produit de matrices). *Le produit de matrices ainsi defini a les proprietes suivantes*

(1) Distributive a gauche: pour $\lambda \in K$, $M, M' \in M_{d''\times d'}(K)$, $N \in M_{d'\times d}(K)$,

$$(\lambda.M + M').N = \lambda.M.N + M'.N.$$

(2) Distributive a droite: pour $\lambda \in K$, $M \in M_{d''\times d'}(K)$, $N, N' \in M_{d'\times d}(K)$,

$$M.(\lambda.N + N') = \lambda.M.N + M.N'.$$

(3) Neutralite de l'identite: pour $M \in M_{d''\times d'}(K)$,

$$\mathrm{Id}_{d''}.M = M,\ M.\mathrm{Id}_{d'} = M$$

(4) La matrice nulle est absorbante: pour $M \in M_{d''\times d'}(K)$,

$$\underline{0}_{d'''d''}.M = \underline{0}_{d'''d'},\ M.\underline{0}_{d'd} = \underline{0}_{d''d}.$$

(5) Associativite: Soit $d''' \geqslant 1$ *et* $L \in M_{d'''\times d''}(K)$, $M \in M_{d''\times d'}(K)$, $N \in M_{d'\times d}(K)$ *alors*

$$(L.M).N = L.(M.N) \in M_{d'''\times d}(K)$$

Preuve: On demontre ces enonces soit par un calcul direct, soit en interpretant la produit de matrices en terme de composition d'applications lineaires. □

Cette regle de produit a ete definie pour etre compatible avec la composition d'applications lineaire. Une consequence tautologique de cette definition est la

PROPOSITION 7.1. *Soit U, V, W des espaces vectoriels comme ci-dessus et*

$$\varphi : U \mapsto V,\ \psi : V \mapsto W \text{ avec}$$
$$\mathrm{mat}_{\mathscr{B},\mathscr{B}}(\varphi) = (n_{jk})_{jk},\ \mathrm{mat}_{\mathscr{B}'',\mathscr{B}'}(\psi) = (m_{ij})_{ij}, \mathrm{mat}_{\mathscr{B}'',\mathscr{B}}(\psi \circ \varphi) = (l_{ik})_{ik}$$

alors

$$\mathrm{mat}_{\mathscr{B}'',\mathscr{B}}(\psi \circ \varphi) = \mathrm{mat}_{\mathscr{B}'',\mathscr{B}'}(\psi).\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi) \tag{7.1.3}$$

Autrement dit on a

$$\begin{pmatrix} l_{11} & \cdots & l_{1d} \\ l_{21} & \cdots & l_{2d} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ l_{d''1} & \cdots & l_{d''d} \end{pmatrix} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d'} \\ m_{21} & m_{22} & \cdots & m_{2d'} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{d''1} & m_{d''2} & \cdots & m_{d''d'} \end{pmatrix} . \begin{pmatrix} n_{11} & \cdots & n_{1d} \\ n_{21} & \cdots & n_{2d} \\ \vdots & \cdots & \vdots \\ n_{d'1} & \cdots & n_{d'd} \end{pmatrix}$$

7.1.2.1. *Image de vecteurs.* Cette multiplication permet egalement de calculer l'image d'un vecteur par une application lineaire:

PROPOSITION 7.2. *Soit $\mathscr{B} \subset V$, $\mathscr{B}' \subset W$ des bases, $v \in V$ un vecteur de coordonnees $(x_j)_{j \leqslant d}$ dans la base $\mathscr{B}$ (ie. $v = x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d$) et $(y_i)_{i \leqslant d'}$ les coordonnees de $\varphi(v)$ dans la base $\mathscr{B}'$ (ie. $\varphi(v) = y_1.\mathbf{f}_1 + \cdots + y_{d'}.\mathbf{f}_{d'}$) alors on a*

$$\mathrm{C}_{\mathscr{B}'}(\varphi(v)) = \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\varphi).\mathrm{C}_{\mathscr{B}}(v).$$

Autrement dit si $\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\varphi) = (m_{ij})_{i \leqslant d', j \leqslant d}$, on a

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ \vdots \\ y_{d'} \end{pmatrix} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix}$$

7.1.2.2. *Le cas des isomorphismes.* On considere le cas ou $\varphi : U \mapsto V$ est un isomorphisme et $\psi = \varphi^{-1} : V \mapsto U$ est l'application reciproque. En particulier U et V sont de meme dimension de $d = d' = d''$.

PROPOSITION 7.3. *On a les relations*

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\varphi^{-1}).\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi) = \mathrm{Id}_d,$$
$$\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi).\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\varphi^{-1}) = \mathrm{Id}_d.$$

En particulier si $U = V$ et $\varphi = \mathrm{Id}_U$ est l'identite on a

$$\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_U).\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_U) = \mathrm{Id}_d. \tag{7.1.4}$$

Preuve: On applique la relation (7.1.3) au cas $U = W$, $\mathscr{B}'' = \mathscr{B}$ et $\psi = \varphi^{-1}$. On a donc

$$\psi \circ \varphi = \mathrm{Id}_U,\ \varphi \circ \psi = \mathrm{Id}_V.$$

On a donc par (7.1.3)

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_U) = \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\varphi^{-1}).\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$$

Comme

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_U) = \mathrm{Id}_d$$

on obtient

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\varphi^{-1}).\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi) = \mathrm{Id}_d.$$

L'autre relation se demontre de la meme maniere. □

7.1.2.3. *Produit de matrices elementaires.*

PROPOSITION 7.4. *Soit $E_{i_0j_0} \in M_{d''\times d'}$ et $E_{j_0'k_0} \in M_{d'\times d}$ alors*

$$E_{i_0j_0}.E_{j_0'k_0} = \delta_{j_0=j_0'}E_{i_0k_0}.$$

Preuve: Raisonne en terme d'applications elementaires $\mathcal{E}_{i_0j_0}$, $\mathcal{E}_{j_0'k_0}$: on a

$$\mathcal{E}_{i_0j_0} \circ \mathcal{E}_{j_0'k_0}(\mathbf{e}_k) = \mathcal{E}_{i_0j_0}(\delta_{k=k_0}\mathbf{f}_{j_0'}) = \delta_{k=k_0}\delta_{j_0=j_0'}\mathbf{g}_{i_0} = \delta_{j_0=j_0'}\mathcal{E}_{i_0k_0}(\mathbf{e}_k).$$

□

7.1.3. Rang d'une matrice. On a definit le rang d'un application lineaire $\varphi : V \mapsto W$ comme etant la dimension de l'image

$$\mathrm{rg}(\varphi) = \dim \mathrm{Im}\,\varphi.$$

Soit $M = \mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$ la matrice associee. Comme l'image $\mathrm{Im}\,\varphi$ est le SEV engendre par

$$\{\varphi(\mathbf{e}_j),\ j \leqslant d\} \subset W,$$

l'image s'identifie avec le SEV de l'espace vectoriel des matrices colonnes $\mathrm{Col}_{d'}(K)$ engendre par les j-colonnes de M,

$$\{\mathrm{Col}_j(M) = \mathrm{Col}_{\mathscr{B}'}(\varphi(\mathbf{e}_j)),\ j \leqslant d\}.$$

DÉFINITION 7.6. *Soit $M \in M_{d'\times d}(K)$, le rang d'une matrice M est la dimension de l'espace engendre par des d colonnes de M dans $\mathrm{Col}_{d'}(K)$:*

$$\mathrm{rg}(M) = \dim\langle\{\mathrm{Col}_j(M),\ j \leqslant d\}\rangle.$$

Autrement dit $\mathrm{rg}(M)$ est la taille maximale d'une sous-famille libre de la famille $\{\mathrm{Col}_j(M),\ j \leqslant d\}$ des colonnes de M.

REMARQUE 7.1.2. On a $\mathrm{rg}(M) \leqslant d$ (puisque d vecteurs engendre un espace de dimension au plus d) et

$$\mathrm{rg}(M) \leqslant d' = \dim \mathrm{Col}_{d'}(K).$$

Ainsi

$$\mathrm{rg}(M) \leqslant \min(d, d').$$

Compte-tenu de la definition on a

$$\mathrm{rg}(\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)) = \mathrm{rg}(\varphi).$$

EXEMPLE 7.1.3. Determiner le rang de la matrice

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

en fonction de la caracteristique du corps K.

7.1.4. Transposition. Soient V et W de bases $\mathscr{B} = \{\mathbf{e}_j,\ j \leqslant d\}$ et $\mathscr{B}' = \{\mathbf{f}_i,\ i \leqslant d'\}$. Soient V^* et W^* les espaces duaux. On a vu qu'a toute application lineaire $\varphi \in \mathrm{Hom}(V, W)$ on pouvait associe une application lineaire duale $\varphi^* \in \mathrm{Hom}(W^*, V^*)$ donnes par

$$\ell' : W \mapsto K,\ \varphi^*(\ell') = \ell' \circ \varphi : v \mapsto \ell'(\varphi(v)).$$

On va relie la matrice de φ a celle de sa duale pour des bases bien choisies.

Théorème 7.2 (Coordonnees de l'application duale). *Soit $\mathscr{B} \subset V$, $\mathscr{B}' \subset W$ des bases et $\mathscr{B}^* \subset V^*$, $\mathscr{B}'^* \subset W^*$ les bases duales. Soient*

$$(m_{ij})_{i\leqslant d', j\leqslant d} = \mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi), (m^*_{ij})_{i\leqslant d, j\leqslant d'} = \mathrm{mat}_{\mathscr{B}^*,\mathscr{B}'^*}(\varphi^*)$$

les matrices de φ et de φ^* dans les bases et leurs duales. Alors on a pour $i \leqslant d', j \leqslant d$

$$m_{ij} = m^*_{ji}.$$

Autrement dit si

$$(m_{ij})_{i\leqslant d', j\leqslant d} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix},\ \textit{on a}\ (m^*_{ij})_{i\leqslant d, j\leqslant d'} = \begin{pmatrix} m_{11} & m_{21} & \cdots & \cdots & m_{d'1} \\ m_{12} & m_{22} & \cdots & \cdots & m_{d'2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{1d} & m_{2d} & \cdots & \cdots & m_{d'd} \end{pmatrix}$$

qui est obtenu par symetrie par rapport a la premiere diagonale.

Preuve: Exercice. □

En termes matriciels cette operation de symetrie est appellee "transposition" :

Définition 7.7. *La transposition est l'application des matrices $d' \times d$ vers les matrice $d \times d'$ definie par*

$$^t\bullet : \begin{array}{ccc} M_{d'\times d}(K) & \mapsto & M_{d\times d'}(K) \\ M = (m_{ij})_{i\leqslant d', j\leqslant d} & \mapsto & {}^tM = (m_{ij})_{j\leqslant d, i\leqslant d'} \end{array}.$$

Théorème 7.3. *(Proprietes fonctionelles de la transposition) La transposition a les proprietes suivantes:*

1. *Linearite: $^t(\lambda.M + M') = \lambda {}^tM + {}^tM'$.*
2. *Involutivite: $^t({}^tM) = M$.*
3. *Anti-multiplicativite: pour $M \in M_{d'',d'}(K)$, $N \in M_{d',d}(K)$, $M.N \in M_{d'',d}(K)$ et*

$$^t(M.N) = {}^tN.{}^tM.$$

Preuve: Seul le dernier point est un peu plus difficile: on peut le verifier par un calcul explicite sur les produits de matrices ou l'obtenir de maniere abstraite. Pour cela on note que si on a

$$\varphi : U \mapsto V,\ \psi : V \mapsto W,\ \psi \circ \varphi : U \mapsto W$$

alors on a les applications duales

$$\varphi^* : V^* \mapsto U^*,\ \psi^* : W^* \mapsto V^*,\ (\psi \circ \varphi)^* : W^* \mapsto U^*$$

On a d'autre part la composee

$$\varphi^* \circ \psi^* : W^* \mapsto U^*$$

et il suffira de montrer que

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$$

(et de passer aux matrices). On a par definition, pour $\ell'' \in W^*$ et par associativite

$$(\psi \circ \varphi)^*(\ell'') = \ell'' \circ (\psi \circ \varphi) = (\ell'' \circ \psi) \circ \varphi = \varphi^*(\ell'' \circ \psi) = \varphi^*(\psi^*(\ell'')) = \varphi^* \circ \psi^*(\ell'')$$

□

THÉORÈME 7.4 (Invariance du rang par transposition). *Soit $M \in M_{d'\times d}(K)$ on a*

$$\mathrm{rg}(M) = \mathrm{rg}({}^tM).$$

Soit $\varphi \in \mathrm{Hom}(V,W)$, on a

$$\mathrm{rg}(\varphi) = \mathrm{rg}(\varphi^*).$$

Preuve: Il suffit de le demontrer pour φ. Soit $\mathscr{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \subset V$ une base alors

$$\varphi(\mathscr{B}) = \{\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)\}$$

possede une famille libre de $r = \mathrm{rg}(\varphi) \leqslant d$ vecteurs lineairement independants disons que c'est

$$\{\mathbf{f}_1 := \varphi(\mathbf{e}_1), \cdots, \mathbf{f}_r := \varphi(\mathbf{e}_r)\}.$$

Comme cette famille est libre elle est contenue dans une base

$$\mathscr{B}' = \{\mathbf{f}_1, \cdots, \mathbf{f}_r, \mathbf{f}_{r+1}, \cdots, \mathbf{f}_{d'}\}.$$

Soit

$$\mathscr{B}'^* = \{\mathbf{f}_1^*, \cdots, \mathbf{f}_r^*, \cdots, \mathbf{f}_{d'}^*\}$$

la base duale. On va montrer que

$$\varphi^*(\mathscr{B}'^*) = \{\varphi^*(\mathbf{f}_1^*), \cdots, \varphi^*(\mathbf{f}_r^*), \cdots, \varphi^*(\mathbf{f}_{d'}^*)\}$$

contient r elements lineairement independants et donc que $\mathrm{rg}(\varphi^*) \geqslant r$.

En fait on va montrer que $\{\varphi^*(\mathbf{f}_1^*), \cdots, \varphi^*(\mathbf{f}_r^*)\}$ est libre: supposons que

$$x_1\varphi^*(\mathbf{f}_1^*) + \cdots + x_r\varphi^*(\mathbf{f}_r^*) = \underline{0}_K$$

On a

$$0_K = (x_1\varphi^*(\mathbf{f}_1^*) + \cdots + x_r\varphi^*(\mathbf{f}_r^*))(\mathbf{e}_j) = x_1\varphi^*(\mathbf{f}_1^*)(\mathbf{e}_j) + \cdots + x_r\varphi^*(\mathbf{f}_r^*)(\mathbf{e}_j) = x_j$$

car

$$\varphi^*(\mathbf{f}_k^*)(\mathbf{e}_j) = \mathbf{f}_k^*(\varphi(\mathbf{e}_j)) = \mathbf{f}_k^*(\mathbf{f}_j) = \delta_{j=k}.$$

Ainsi la famille est libre.

Cette inegalite montre que $\mathrm{rg}(\varphi) \leqslant \mathrm{rg}(\varphi^*)$ et donc que pour toute matrice M

$$\mathrm{rg}(M) \leqslant \mathrm{rg}({}^tM)$$

mais comme ${}^t{}^tM = M$ on a

$$\mathrm{rg}({}^tM) \leqslant \mathrm{rg}({}^t{}^tM) = \mathrm{rg}(M)$$

et qui implique que

$$\mathrm{rg}(\varphi) = \mathrm{rg}(\varphi^*).$$

□

Comme la transposee d'une matrice transforme les colonnes en lignes on obtient:

COROLLAIRE 7.1. *La rang d'une matrice est egal a la dimension de l'espace K^d engendre par les vecteurs lignes de M*

$$\mathrm{Lig}_j(M),\ j = 1, \cdots, d'.$$

7.2. L'algebre des matrices carrees

Si $d' = d$, on obtient l'espace vectoriel des matrices carres

$$M_{d\times d}(K) = M_d(K)$$

qui est de dimension $\dim M_d(K) = d^2$.

7.2.1. Structure d'anneau. Comme on l'a vu, la multiplication des matrices

$$(M, M') \in M_d(K) \times M_d(K) \mapsto M.M' \in M_d(K)$$

est alors une loi de composition interne et par le Theoreme 7.1, on a

THÉORÈME 7.5. *L'espace $M_d(K)$ muni de l'addition des matrices et de la multiplication est un anneau (non-commutatif en general) dont l'element neutre est la matrice carree nulle $\underline{0}_d = \underline{0}_{d\times d}$ et dont l'unite est la matrice identite Id_d. De plus la structure de K-EV de $M_d(K)$ fait de l'anneau $(M_d(K), +, .)$ une K-algebre (de dimension d^2).*

On l'appelle l'algebre des matrices carres de dimension d sur le corps K (ou a coefficient dans K).

7.2.1.1. *La transposition est un antimorphisme.* Si une matrice M est carree $d \times d$ sa transposee ${}^tM$ est encore carree $d \times d$. Compte tenu des proprietes generales de la transposition (cf. Prop 7.3), on a

PROPOSITION 7.5. *La transposition*

$${}^t\bullet : M_d(K) \mapsto M_d(K)$$

est un endomorphisme de $M_d(K)$ qui est

(1) Involutif: On a ${}^t({}^tM) = M$.
(2) En particulier ${}^t\bullet$ est inversible et son inverse est lui-meme:

$${}^t({}^t\bullet) = \mathrm{Id}_{M_d(K)},\ ({}^t\bullet)^{-1} = {}^t\bullet.$$

(3) Anti-multiplicatif: ${}^t(M.N) = {}^tN.{}^tM$.

REMARQUE 7.2.1. On dit que la transposition est un anti-automorphisme d'algebres.

7.2.2. Lien avec l'algebre des endomorphismes. Soit V de dimension d. On rappelle (§6.3) que l'ensemble de endomorphismes de V, $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ est non seulement un espace vectoriel (pour l'addition des applications lineaires) mais egalement possede une structure d'anneau (et donc de K-algebre) ou la "multiplication" est la composition des endomorphismes: pour $\varphi, \psi \in \mathrm{End}(V)$

$$\varphi \circ \psi : V \xrightarrow{\psi} V \xrightarrow{\varphi} V.$$

L'element neutre est l'endomorphisme nul $\underline{0}_V$ et l'element unite est l'application identite Id_V.

Soit $\mathscr{B}$ une base de V, on dispose alors d'un isomorphisme d'espaces vectoriels

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}} : \varphi \in \mathrm{End}(V) \mapsto \mathrm{mat}_{\mathscr{B},\mathscr{B}}(\varphi) \in M_d(K).$$

Pour simplifier les notations on ecrira cet isomorphisme $\mathrm{mat}_{\mathscr{B}}$ (ou juste mat si la base $\mathscr{B}$ est implicite) et la matrice associee a un endomorphisme φ sera notee

$$\mathrm{mat}_{\mathscr{B}}(\varphi) := \mathrm{mat}_{\mathscr{B},\mathscr{B}}(\varphi).$$

REMARQUE 7.2.2. En tout generalite, etant donne un endomorphisme $\varphi : V \mapsto V$, on aurait pu prendre deux bases $\mathscr{B}, \mathscr{B}' \subset V$ et associer la matrice $\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$. Un avantage de choisir $\mathscr{B}' = \mathscr{B}$ est que l'identite Id_V est alors representee par la matrice identite Id_d. Mais l'avantage principal de choisir $\mathscr{B}' = \mathscr{B}$ est le suivant:

THÉORÈME 7.6. *Soit V de dimension finie d et $\mathscr{B}$ une base de V, l'application*

$$\mathrm{mat}_{\mathscr{B}} : \mathrm{End}(V) \mapsto M_d(K)$$

est un isomorphisme d'anneaux (et donc de K-algebres) pour les lois d'addition et de multiplication decrites precedemment.

Preuve: On sait deja que $\mathrm{mat}_{\mathscr{B}}$ est un isomorphisme d'espace vectoriel (et est donc bijectif). Pour montrer qu'on a un isomorphisme d'anneaux il suffit de verifier que pour $\varphi, \psi \in \mathrm{End}(V)$

$$\mathrm{mat}_{\mathscr{B}}(\varphi \circ \psi) = \mathrm{mat}_{\mathscr{B}}(\varphi).\mathrm{mat}_{\mathscr{B}}(\psi).$$

Mais cela resulte immediatement de la definition du produit de matrices: si $\mathrm{mat}_{\mathscr{B}}(\varphi) = M = (m_{ij})_{i,j\leqslant d}$ et $\mathrm{mat}_{\mathscr{B}}(\psi) = N = (n_{ij})_{i,j\leqslant d}$ alors

$$M.N = L = (l_{ik})_{i,k\leqslant d}$$

avec

$$l_{ik} = \sum_{j=1\cdots d} m_{ij}.n_{jk}$$

et c'est precisement

$$L = (l_{ik})_{i,k\leqslant d} = \mathrm{mat}_{\mathscr{B}}(\varphi \circ \psi)$$

par le Thm 6.4. □

7.2.3. Le groupe lineaire.

Définition 7.8. *Le groupe (pour la multiplication) des matrices inversibles $M_d(K)^\times \subset M_d(K)$ est appelle groupe lineaire de dimension d sur K (ou a coefficients dans K) et on le note*

$$\mathrm{GL}_d(K) := M_d(K)^\times$$

Rappelons que le groupe des endomorphismes bijectifs (ie. des automorphismes de V) $\mathrm{End}(V)^\times$ est egalement note $\mathrm{GL}(V)$ et est appelle le groupe lineaire de V. On a donc

Corollaire 7.2. *On a un isomorphisme de groupes*

$$\mathrm{mat}_{\mathscr{B}} : \mathrm{GL}(V) \simeq \mathrm{GL}_d(K).$$

Théorème 7.7 (Critere d'inversibilite des colonnes). *Pour qu'une matrice carree $M = (m_{ij})_{i,j\leqslant d} \in M_d(K)$ soit inversible (ie. $M \in \mathrm{GL}_d(K)$), il faut et il suffit que la famille des colonnes*

$$\mathrm{Col}(M) = \{\mathrm{Col}_j(M) = \mathrm{Col}((m_{ij})_{i\leqslant d}),\ j \leqslant d\}$$

de M forme une famille libre (resp. generatrice) de l'espace de matrices colonnes de M, $\mathrm{Col}_d(K)$.

Preuve: La matrice M est la matrice $M = \mathrm{mat}_{\mathscr{B}_d^0}(\varphi)$ de l'endomorphisme $\varphi = \varphi_M$ de K^d qui a un vecteur $\mathbf{e}_j^0,\ j \leqslant d$ de la base canonique, associe le vecteur $\varphi_M(\mathbf{e}_j),\ j \leqslant d$ dont les coordonnees dans $\mathscr{B}_d^0$ sont les $(m_{ij})_{i\leqslant d}$.

La matrice M est inversible si et seulement si φ est inversible et (par le Thm Noyau-Image) c'est le cas ssi

$$\mathrm{rg}(\varphi) = \dim(\mathrm{Im}\,\varphi) = d = \dim(K^d)$$

mais

$$\mathrm{rg}(\varphi) = \mathrm{rg}(M)$$

est la taille maximal d'une famille de colonnes de M qui est libre. □

Remarque 7.2.3. Notons qu'alors l'inverse de M est la matrice

$$M^{-1} = M' = \mathrm{mat}_{\mathscr{B}_d^0}(\varphi^{-1}) :$$

en effet

$$M.M' = \mathrm{mat}_{\mathscr{B}_d^0}(\varphi).\mathrm{mat}_{\mathscr{B}_d^0}(\varphi^{-1}) = \mathrm{mat}_{\mathscr{B}_d^0}(\varphi.\varphi^{-1}) = \mathrm{mat}_{\mathscr{B}_d^0}(\mathrm{Id}_{K^d}) = \mathrm{Id}_d$$

et de meme $M'.M = \mathrm{Id}_d$. Ainsi M' est l'inverse de M.

Remarque 7.2.4. Dans le critere d'inversibilite, on peut remplacer "colonnes" par "lignes" car le rang de M est celui de sa transposee:

$$\mathrm{rg}(M) = \mathrm{rg}({}^tM).$$

On a egalement le critere d'inversibilite suivant qui resulte de l'isomorphisme d'algebres

$$\mathrm{End}_K(V) \simeq M_d(K)$$

et du Theoreme 6.5:

THÉORÈME 7.8 (Critere d'inversibilite matriciel). *Soit $M \in M_d(K)$ une matrice carree. Les proprietes suivantes sont equivalentes*

(1) M est inversible (ie. appartient a $\mathrm{GL}_d(K)$).
(2) $\mathrm{rang}(M) = d$.
(3) M admet un inverse a droite: il existe $M_d \in M_d(K)$ tel que

$$M.M_d = \mathrm{Id}_d.$$

(4) M admet un inverse a gauche: il existe $M_g \in M_d(K)$ tel que

$$M_g.M = \mathrm{Id}_d.$$

Dans ce cas on a

$$M^{-1} = M_d = M_g.$$

7.2.3.1. *Transposition.*

PROPOSITION 7.6. *La transposition est une bijection de $\mathrm{GL}_d(K)$ sur lui-meme qui verifie:*

$$\forall M, N \in \mathrm{GL}_d(K),\ ({}^tM)^{-1} = {}^t(M^{-1}),\ {}^t(M.N) = {}^tN.{}^tN.$$

Preuve: Si M est inversible on a

$$M.M^{-1} = M^{-1}.M = \mathrm{Id}_d$$

et donc

$${}^t(M.M^{-1}) = {}^t(M^{-1}).{}^tM = {}^t(M^{-1}.M) = {}^t(M^{-1}).{}^t(M) = {}^t(\mathrm{Id}_d) = \mathrm{Id}_d.$$

Ainsi ${}^tM$ est inversible d'inverse ${}^t(M^{-1})$. □

EXERCICE 7.1. Soit

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

une matrice carree de taille 2.

(1) Calculer M^2 et montrer qu'il existe $t, \Delta \in K$ (qui dependes de a, b, c, d tels que

$$M^2 - t.M + \Delta.\mathrm{Id}_2 = 0_2.$$

(2) Montrer que M est inversible ssi $\Delta \neq 0_K$.

7.3. Changement de base

La question est la suivante: soit $\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$ la matrice associee a $\varphi : V \mapsto W$ dans des bases $\mathscr{B} \subset V$ et $\mathscr{B}' \subset W$; soit

$$\mathscr{B}_n = \{\mathbf{e}_{nj},\ j \leqslant d\} \subset V,\ \mathscr{B}'_n = \{\mathbf{f}_{ni},\ i \leqslant d\} \subset W$$

de nouvelles bases, la proposition suivante permet de calculer la matrice de φ dans ces nouvelles bases, $\mathrm{mat}_{\mathscr{B}'_n,\mathscr{B}_n}(\varphi)$ en fonction de $\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$.

THÉORÈME 7.9 (Formule de changement de base). *Soient $\mathscr{B}, \mathscr{B}_n \subset V$ et $\mathscr{B}', \mathscr{B}'_n \subset W$ des bases de V et W. On a la relation*

$$\mathrm{mat}_{\mathscr{B}'_n,\mathscr{B}_n}(\varphi) = \mathrm{mat}_{\mathscr{B}'_n,\mathscr{B}'}(\mathrm{Id}_W).\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi).\mathrm{mat}_{\mathscr{B},\mathscr{B}_n}(\mathrm{Id}_V).$$

Preuve: On a evidemment

$$\varphi = \mathrm{Id}_W \circ \varphi \circ \mathrm{Id}_V.$$

Il suffit alors d'appliquer deux fois la relation (7.1.3). avec des bases convenables: une fois pour $\varphi \circ \mathrm{Id}_V = \varphi$ et l'autre pour $\mathrm{Id}_W \circ \varphi = \varphi$. □

DÉFINITION 7.9. *La matrice carree de taille $d = \dim V$,*

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}_n} := \mathrm{mat}_{\mathscr{B},\mathscr{B}_n}(\mathrm{Id}_V)$$

est appelle matrice changement de base de la base $\mathscr{B}_n$ a la base $\mathscr{B}$ ou encore la matrice de passage de la base $\mathscr{B}_n$ a la base $\mathscr{B}$.

Sa j-ieme colonne est formee par les coordonnees du j-ieme vecteur $\mathbf{e}_{nj}$ dans la base $\mathscr{B}$.

La formule de changement de base se reecrit alors

$$\mathrm{mat}_{\mathscr{B}'_n,\mathscr{B}_n}(\varphi) = \mathrm{mat}_{\mathscr{B}'_n,\mathscr{B}'}.\mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\varphi).\mathrm{mat}_{\mathscr{B},\mathscr{B}_n}.$$

Notons que la matrice de passage $\mathrm{mat}_{\mathscr{B},\mathscr{B}_n}$ est inversible par le critere d'inversibilite. On va calculer son inverse:

PROPOSITION 7.7. *Soit trois bases $\mathscr{B}, \mathscr{B}_1, \mathscr{B}_2 \subset V$ on a*

(1) Formule d'inversion:

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}_1}.\mathrm{mat}_{\mathscr{B}_1,\mathscr{B}} = \mathrm{Id}_d.$$

En particulier une matrice de passage est inversible (dans $M_d(K)$) et son inverse est la matrice de passage de la base initiale a la nouvelle base:

$$\mathrm{mat}^{-1}_{\mathscr{B},\mathscr{B}_1} = \mathrm{mat}_{\mathscr{B}_1,\mathscr{B}}.$$

(2) Formule de transitivite:

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}_2} = \mathrm{mat}_{\mathscr{B},\mathscr{B}_1}.\mathrm{mat}_{\mathscr{B}_1,\mathscr{B}_2}$$

Preuve: Cela resulte de (7.1.4) et de (7.1.3) appliques a $\varphi = \psi = \mathrm{Id}_V$ et a des bases convenables. □

7.3.0.1. *Changement de base pour les endomorphismes.* Si $V = W$ et qu'on prend $\mathscr{B}' = \mathscr{B}$ et qu'on se donne une nouvelle base $\mathscr{B}_n = \mathscr{B}'_n$, la formule de changement de base devient alors

$$\mathrm{mat}_{\mathscr{B}_n}(\varphi) = \mathrm{mat}_{\mathscr{B}_n,\mathscr{B}}.\mathrm{mat}_{\mathscr{B}}(\varphi)\mathrm{mat}_{\mathscr{B},\mathscr{B}_n} = \mathrm{mat}^{-1}_{\mathscr{B},\mathscr{B}_n}.\mathrm{mat}_{\mathscr{B}}(\varphi)\mathrm{mat}_{\mathscr{B},\mathscr{B}_n}$$

7.3.1. Matrices equivalentes.

DÉFINITION 7.10. *Deux matrices $M, N \in M_{d'\times d}(K)$ sont dites equivalentes si il existe des matrices inversibles $A \in \mathrm{GL}_{d'}(K)$, $B \in \mathrm{GL}_d(K)$ telles que*

$$N = A.M.B.$$

Par la formule de changement de bases on a:

PROPOSITION 7.8. *Deux matrices sont equivalentes ssi il existe V de dimension d et W de dimension d', des bases $\mathscr{B}, \mathscr{B}_n \subset V$ et $\mathscr{B}', \mathscr{B}'_n \subset W$ et une application lineaire $\varphi : V \mapsto W$ telle que*

$$M = \mathrm{mat}_{\mathscr{B}'\mathscr{B}}(\varphi),\ N = \mathrm{mat}_{\mathscr{B}'_n\mathscr{B}_n}(\varphi)$$

En particulier

PROPOSITION 7.9. *Si M et N sont equivalentes alors*

$$\mathrm{rg}(M) = \mathrm{rg}(N).$$

7.3.2. Conjugaison.

La formule de changement de base dans $M_d(K)$ met en evidence une operation particuliere sur $M_d(K)$, la conjugaison:

DÉFINITION 7.11. *Soit $C \in GL_d(K)$ une matrice inversible. Note note $\mathrm{Ad}(C)$ l'application dite de conjugaison par C:*

$$\mathrm{Ad}(C) : \begin{array}{ccc} M_d(K) & \mapsto & M_d(K) \\ M & \mapsto & C.M.C^{-1}. \end{array}$$

EXEMPLE 7.3.1. Si $C = \mathrm{mat}_{\mathscr{B}_1,\mathscr{B}}$ est une matrice de changement de base (de la base $\mathscr{B}$ a la base $\mathscr{B}_1$) alors la formule de changement de base pour les matrices carrees s'ecrit

$$\mathrm{mat}_{\mathscr{B}_1}(\varphi) = \mathrm{Ad}(\mathrm{mat}_{\mathscr{B}_1,\mathscr{B}})(\mathrm{mat}_{\mathscr{B}}(\varphi)).$$

PROPOSITION 7.10. *La conjugaison* $\mathrm{Ad}(C)$ *est un automorphisme de l'algebre* $M_d(K)$*:*

(1) Linearite: On a $\mathrm{Ad}(C)(\lambda.M+N) = \lambda\mathrm{Ad}(C)(M) + \mathrm{Ad}(C)(N)$.
(2) Multiplicativite: $\mathrm{Ad}(C)(M.N) = \mathrm{Ad}(C)(M).\mathrm{Ad}(C)(N)$.
(3) Inversibilite: $\mathrm{Ad}(C)$ *est bijective et* $\mathrm{Ad}(C)^{-1} = \mathrm{Ad}(C^{-1})$.

Preuve: On a

$$\begin{aligned}\mathrm{Ad}(C)(\lambda.M+N) &= C.(\lambda.M+N).C^{-1} = (\lambda.C.M + C.N).C^{-1}\\ &= \lambda.C.M.C^{-1} + C.N.C^{-1} = \lambda\mathrm{Ad}(C)(M) + \mathrm{Ad}(C)(N).\end{aligned}$$

On a

$$\mathrm{Ad}(C)(M.N) = C.M.N.C^{-1} = C.M.\mathrm{Id}_d.N.C^{-1} = C.M.C^{-1}.C.N.C^{-1} = \mathrm{Ad}(C)(M).\mathrm{Ad}(C)(N).$$

Par ailleurs

$$\mathrm{Ad}(C^{-1})(\mathrm{Ad}(C)(M))) = C^{-1}.c.M.C^{-1}.C = M$$

et donc

$$\mathrm{Ad}(C^{-1}) \circ \mathrm{Ad}(C) = \mathrm{Id}_{M_d(K)}$$

□

On dispose donc d'une application

$$\mathrm{Ad}(\bullet) : C \in \mathrm{GL}_d(K) \mapsto \mathrm{Aut}(M_d(K)) \simeq \mathrm{GL}_{d^2}(K)$$

appellee application *adjointe*.

PROPOSITION 7.11. *L'application adjointe* $\mathrm{Ad}(\bullet)$ *est un morphisme de groupes. Son noyau est forme par les matrices scalaires:*

$$\ker \mathrm{Ad} = K^{\times}\mathrm{Id}.$$

Preuve: On a deja vu que $\mathrm{Ad}(C)^{-1} = \mathrm{Ad}(C^{-1})$. Reste a voir que

$$\mathrm{Ad}(B.C) = \mathrm{Ad}(B) \circ \mathrm{Ad}(C).$$

On a

$$\mathrm{Ad}(B.C)(M) = B.C.M.(B.C)^{-1} = B.C.M.C^{-1}.B^{-1} = \mathrm{Ad}(B)(\mathrm{Ad}(C)(M)).$$

Soit $C = (c_{kl})_{k,l\leqslant d}$ une matrice inversible telle que pour tout M on ait

$$C.M.C^{-1} = M.$$

On a donc pour tout M

$$C.M = M.C.$$

En particulier $\forall i,j \leqslant d$

$$C.E_{ij} = E_{ij}.C.$$

On a par la proposition 7.4

$$(\sum_{k,l} c_{kl}E_{kl}).E_{ij} = \sum_{k,l} c_{kl}E_{kl}.E_{ij} = \sum_{k,l} c_{kl}\delta_{l=i}E_{kj} = \sum_{k} c_{ki}E_{kj}$$

et

$$E_{ij}.(\sum_{k,l} c_{kl}E_{kl}) = \sum_{k,l} c_{kl}E_{ij}.E_{kl} = \sum_{k,l} c_{kl}\delta_{k=j}E_{il} = \sum_{l} c_{jl}E_{il}$$

On a donc necessairement dans les sommes ci-dessus $c_{ki} = 0$ si $k \neq j$ et comme c'est valable pour tout j on voit que $c_{ij} = 0$ sauf si $i = j$. on a donc

$$C.E_{ij} = c_{ii}E_{ij} = E_{ij}.C = c_{jj}E_{ij}$$

ce qui force les c_{ii} a etre tous egaux et donc $C = c_{11}.\mathrm{Id}_d$ est une matrice scalaire. □

DÉFINITION 7.12. *L' image est appellee groupe des automorphisme interieurs de $M_d(K)$ et est notee* $\mathrm{Int}(M_d(K))$.

DÉFINITION 7.13. *On dit que deux matrices M, N sont semblables ou conjuguees si il existe $C \in GL_d(K)$ tel que*

$$N = C.M.C^{-1}.$$

La relation "etre semblables" ou "etre conjuguees" est une relation d'equivalence car $\mathrm{GL}_d(K)$ *est un groupe et* $\mathrm{Ad} : \mathrm{GL}_d(K) \mapsto \mathrm{Int}(M_d(K))$ *est un morphisme de groupes.*

Une classe d'equivalence, l'ensemble des matrices de la forme

$$M^\natural := \mathrm{Ad}(\mathrm{GL}_d(K))(M) = \{C.M.C^{-1},\ C \in \mathrm{GL}_d(K)\}$$

ou une matrice $M \in M_d(K)$ est appellee classe de conjugaison (de M) et on note

$$M_d(K)^\natural = \{M^\natural\} = M_d(K)/\sim$$

l'ensemble dess classes de conjugaison.

EXERCICE 7.2. Montrer que si $M = \mathrm{mat}_{\mathscr{B}}(\varphi)$ est la matrice representant un endomorphisme $\varphi \in \mathrm{End}(V)$ dans une base $\mathscr{B} \subset V$ alors $M^\natural$ est l'ensemble des matrices $\mathrm{mat}_{\mathscr{B}'}(\varphi)$ quand $\mathscr{B}'$ parcourt toutes les bases de V.

On peut definir une notion de conjugaison pour l'algebre (abstraite) $\mathrm{End}(V)$ des endomorphismes d'un espace V en disant que $\varphi, \phi \in \mathrm{End}(V)$ sont conjugues si il existe $\psi \in \mathrm{Aut}(V)$ tel que

$$\phi = \psi \circ \varphi \circ \psi^{-1}.$$

Si on choisit une base de V et qu'on l'utilise pour identifier $\mathrm{End}(V)$ avec $M_d(K)$ on obtient exactement la meme notion ($C = \mathrm{mat}_{\mathscr{B}}(\psi)$).

EXERCICE 7.3. Soit V et W des espaces vectoriels de dimension finie isomorphes alors $\mathrm{End}(V)$ et $\mathrm{End}(W)$ sont des K-algebres isomorphes: construire un tel isomorphisme

$$\mathrm{End}(V) \simeq \mathrm{End}(W)$$

a partir d'un isomorphisme $\psi : V \simeq W$.

CHAPITRE 8

Interlude: le corps des nombres complexes

... eine feine und wunderbare Zuflucht des menschlichen Geistes,
beinahe ein Zwitterwesen zwischen Sein und Nichtsein.

Dans ce chapitre, on va construire le corps des nombres complexe comme une sous-algebre de l'algebre des matrice reeles 2×2, $M_2(\mathbb{R})$. C'est en fait un cas particulier d'une construction generale basee sur l'anneau des polynomes a coefficients dans un corps K,

$$K[X] = \{a_0 + a_1.X + \cdots + a_d.X^d, d \geqslant 0,\ a_0, \cdots, a_d \in K\}$$

qu'on verra au chapitre sur les anneaux de polynomes.

8.1. L'algebre des nombres complexes

Prenons $K = \mathbb{R}$ et $\mathcal{M} = M_2(\mathbb{R})$. Soit I la matrice

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

DÉFINITION 8.1. *L'espace des nombres complexes* $\mathbb{C}$ *est les sous-espace vectoriel engendre par* Id_2 *et* I*,*

$$\mathbb{C} = \mathbb{R}.\mathrm{Id}_2 + \mathbb{R}.I = \left\{ z = x.\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + y\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix},\ x, y \in \mathbb{R} \right\}.$$

THÉORÈME 8.1. *L'espace des nombres complexes est de dimension* 2 *et* $\{\mathrm{Id}, I\}$ *en forme une base.*

De plus $\mathbb{C}$ *est une sous-algebre commutative de* $M_2(\mathbb{R})$ *et est en fait un corps. Le corps des nombres reel s'injecte dans* $\mathbb{C}$ *via l'application*

$$x \in \mathbb{R} \mapsto x.\mathrm{Id}_2 \in \mathbb{C}.$$

(les nombres reels s'identifient aux matrices scalaires).

Preuve: La famille $\{\mathrm{Id}, I\}$ est libre: si

$$x.\mathrm{Id}_2 + y.I = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

alors $x = y = 0$. Montrons que $\mathbb{C}$ est un sous-anneau et comme $\mathbb{C}$ est un SEV ce sera alors une sous-algebre. Il suffit de montrer que $\mathbb{C}$ est stable par produit. Notons que

$$I^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathrm{Id}_2.$$

En particulier I est inversible et son inverse est

$$-I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = {}^tI.$$

Soient alors

$$z = x.\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + y\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}x & -y\\ y & x\end{pmatrix},\ z' = x'.\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + y'\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}x' & -y'\\ y' & x'\end{pmatrix}$$

alors

(8.1.1)

$$z.z' = \begin{pmatrix}x & -y\\ y & x\end{pmatrix}.\begin{pmatrix}x' & -y'\\ y' & x'\end{pmatrix} = \begin{pmatrix}xx'-yy' & -(xy'+x'y)\\ xy'+x'y & xx'-yy'\end{pmatrix} = (xx'-yy')\mathrm{Id}_2 + (xy'+x'y)I \in \mathbb{C}$$

et donc $\mathbb{C}$ est stable par produit; de plus (puisque $\mathbb{R}$ est commutatif)

$$z'.z = (x'x-y'y)\mathrm{Id}_2 + (x'y+xy')I = (xx'-yy')\mathrm{Id}_2 + (xy'+x'y)I = z.z'.$$

Ainsi $\mathbb{C}$ est une algebre commutative.

Montrons que $\mathbb{C}$ est un corps (que tout matrice de $\mathbb{C}$ non-nulle est inversible): soit $z \in \mathbb{C} - \{0_2\}$, on a

$$z^2 = (x^2-y^2)\mathrm{Id}_2 + 2xy.I$$

et donc

$$z^2 - 2x.z = z^2 - 2x(x.\mathrm{Id}_2 + y.I) = (x^2-y^2-2x^2).\mathrm{Id}_2 = -(x^2+y^2).\mathrm{Id}_2.$$

On peut factoriser par z dans l'expression $z^2 - 2x.z$: en effet, $2x.z = z.(2x.\mathrm{Id}_2)$ de sorte que

$$z^2 - 2x.z = z.(z - 2x.\mathrm{Id}_2)$$

et donc

$$z(2x.\mathrm{Id}_2 - z) = (x^2+y^2).\mathrm{Id}_2.$$

On a

$$z \neq \mathbf{0}_2 \Longleftrightarrow x^2+y^2 \neq 0$$

et donc x^2+y^2 est inversible dans $\mathbb{R}$ et

$$z.\frac{1}{x^2+y^2}(2x.\mathrm{Id}_2 - z) = \mathrm{Id}_2$$

ce qui montre que z est inversible avec

$$z^{-1} = \frac{1}{x^2+y^2}(2x.\mathrm{Id}_2 - z) = \frac{1}{x^2+y^2}(x.\mathrm{Id}_2 - y.I)$$

Soit ${}^t z$ la transposee de z:

$$z = x.\mathrm{Id}_2 + y.I = \begin{pmatrix}x & -y\\ y & x\end{pmatrix},\ {}^t z = \begin{pmatrix}x & y\\ -y & x\end{pmatrix} = x.\mathrm{Id}_2 - y.I.$$

On a donc

$$z^{-1} = \frac{1}{x^2+y^2}\,{}^t z = \begin{pmatrix}\frac{x}{x^2+y^2} & \frac{y}{x^2+y^2}\\ -\frac{x}{x^2+y^2} & \frac{x}{x^2+y^2}\end{pmatrix}. \tag{8.1.2}$$

□

Remarque 8.1.1. On a

$$I^3 = -I, I^4 = \mathrm{Id}_2, I^5 = I, \cdots$$

et donc

$$I^n = \pm\mathrm{Id}_2 \text{ ou bien } \pm I$$

suivant que n est pair ou impair.

8.2. Proprietes de base des nombres complexes

NOTATION 8.1. *Un nombre complexe general s'ecrit comme une matrice* 2×2 *de la forme.*

$$z = x.\mathrm{Id}_2 + y.I.$$

D'autre part on a vu qu'on peut identifier $\mathbb{R}$ *avec une sous-algebre de* $\mathbb{C}$ *en envoyant un reel* x *sur la matrice scalaire* $x.\mathrm{Id}_2$ *de qui est une maniere un peu compliquee d'erire un nombre reel. Pour simplifier les notations, quand on designera un nombre complexe, on remplacera la matrice* Id_2 *par* 1*, la matrice nulle* $\mathbf{0}_2$ *par* 0 *et on remplacera* I *par la lettre* i *et on ecrira* z *(sous forme de "nombre")*

$$z = x + iy.$$

Avec cette nouvelle notation, on a

$$i^2 = -1$$

et la somme et le produit de deux nombres complexes $z = x + iy,\ z' = x' + iy'$ devient

$$z + z' = x + x' + i(y + y'),\ z.z' = (x + iy).(x' + iy') = (xx' - yy') + i(xy' + y'y).$$

DÉFINITION 8.2. *Le reel* x *est appele "partie reelle" de* z *et le reel* y *est la "partie imaginaire" de* z

$$x = \mathrm{Re}z,\ y = \mathrm{Im}\, z.$$

Dans la notation matricielle la transposition $z \mapsto {}^t z$ *envoie*

$$z = x.\mathrm{Id}_2 + y.I \mapsto {}^t z = x.\mathrm{Id}_2 - y.I.$$

Avec la notation simplifiee cette operation se note

$$z = x + iy \mapsto \overline{z} = x - yi$$

et s'appelle la conjugaison complexe de z*. On a alors*

$$z.\overline{z} = x^2 + y^2 \geqslant 0.$$

Le nombre $(z.\overline{z})^{1/2}$ *se note*

$$|z| = (z.\overline{z})^{1/2} = (x^2 + y^2)^{1/2}$$

et s'appelle le module de z*. On a donc*

$$z\overline{z} = |z|^2.$$

PROPOSITION 8.1. *On a la proprietes suivantes:*

(1) Les applications "partie reelle" et "imaginaire"

$$\mathrm{Re}, \mathrm{Im} : \mathbb{C} \mapsto \mathbb{R}$$

sont lineaires:

$$\lambda \in \mathbb{R}, \mathrm{Re}(\lambda.z + z') = \lambda.\mathrm{Re}z + \mathrm{Re}z',\ \mathrm{Im}(\lambda.z + z') = \lambda.\,\mathrm{Im}\, z + \mathrm{Im}\, z'.$$

Les noyaux valent $\ker(\mathrm{Im}) = \mathbb{R}$ *et* $\ker(\mathrm{Re}) = \mathbb{R}.i$ *est l'ensemble des nombres complexes imaginaires purs.*

(2) La conjugaison complexe

$$\overline{\bullet} : z \in \mathbb{C} \mapsto \overline{z} \in \mathbb{C}$$

est un automorphisme du corps $\mathbb{C}$*: in particulier*

$$\lambda \in \mathbb{R}, \overline{\lambda.z + z'} = \lambda.\overline{z} + \overline{z}',\ \overline{z.z'} = \overline{z}.\overline{z}'.$$

De plus $\overline{\bullet}$ *est involutif*

$$\overline{\overline{z}} = z$$

et on a

$$\overline{z} = z \Longleftrightarrow z = x \in \mathbb{R}.$$

(3) Le module $z \mapsto |z| = (z.\overline{z})^{1/2}$ *est multiplicatif:*

$$|z.z'| = |z|.|z'|$$

et on a

$$z = 0 \Longleftrightarrow |z| = 0$$

et pour tout $x \in \mathbb{R} \subset \mathbb{C}$ *on a*

$$|x| = |x|_{\mathbb{R}} = \max(x, -x) \tag{8.2.1}$$

Autrement dit, le module d'un nombre reel est egale a la "valeur absolue" usuelle de ce nombre reel.

Preuve: (1) Les applications $\mathrm{Re} : \mathbb{C} \mapsto \mathbb{R}$ et $\mathrm{Im} : \mathbb{C} \mapsto \mathbb{R}$ sont lineaires car ce sont les formes lineaires " premiere et seconde coordonnee" de la base $\{\mathrm{Id}_2, I\}$ et on peut egalement le verifier directement.

Ces formes lineaires sont non-nulles donc surjectives sur $\mathbb{R}$. On a

$$\ker(\mathrm{Re}) = \{0 + iy,\ y \in \mathbb{R}\} = \mathbb{R}.i,\ \ker(\mathrm{Im}) = \{x + 0i,\ x \in \mathbb{R}\} = \mathbb{R}.$$

(2) On peut egalement verifier immediatement par le calcul que $z \mapsto \overline{z}$ est lineaire et multiplicative. On peut egalement raisonner en terme de matrices et dire que la transposition est lineaire et multiplicative: on a

$$\overline{z.z'} = {}^t z.z' = {}^t z'.{}^t z = \overline{z}'\overline{z} = \overline{z}\overline{z}'$$

puisque $\mathbb{C}$ est commutatif.

– Le fait que $\overline{\bullet}$ soit involutive est immediat (ou vient du fait que la transposition est involutive) et cela implique que $\overline{\bullet}$ est bijective d'application reciproque elle-meme.

–On a

$$\overline{z} = z \Longleftrightarrow \overline{z} = x - iy = x + iy = z \Longleftrightarrow 2iy = 0 \Longleftrightarrow y = 0 \Longleftrightarrow z = x \in \mathbb{R}.$$

(en effet $2.i$ est non nul donc inversible dans $\mathbb{C}$).

(3) La multiplicativite du module provient de la multiplicativite de la conjugaison complexe (et le fait que $\mathbb{C}$ est commutatif.)

– On a de plus

$$z = 0 \Longleftrightarrow x + iy = 0 \Longleftrightarrow (x, y) = (0, 0) \Longleftrightarrow x^2 + y^2 = 0 \Longleftrightarrow |z| = 0.$$

(en effet comme $x^2, y^2 \geqslant 0$ on ne peut avoir $x^2 + y^2 = 0$ que si $x = y = 0$).

– Soit $z = x \in \mathbb{R}$ alors

$$|z| = |x + i.0| = (x^2 + 0^2)^{1/2} = (x^2)^{1/2} = \max(x, -x) = |x|_{\mathbb{R}}.$$

□

Remarque 8.2.1. On notera egalement la formule d'inversion suivante qui est la traduction de la formule d'inversion (8.1.2):

$$\forall z \in \mathbb{C}^\times,\ z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}. \tag{8.2.2}$$

Pour retrouver cette formule il suffit de ce souvenir que

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

et si $|z|^2 = x^2 + y^2 \neq 0$ on a

$$z.\frac{\overline{z}}{|z|^2} = 1.$$

8.2.1. Nombres complexes de module 1. Considerons le module mais restreint au groupe multiplicatif $\mathbb{C}^\times = \mathbb{C} - \{0\}$:

$$|\bullet| : \begin{array}{ccc} \mathbb{C}^\times & \mapsto & \mathbb{R}_{>0} \\ z & \mapsto & |z| = (x^2+y^2)^{1/2}. \end{array}$$

On note

$$\mathbb{C}^{(1)} = \{z \in \mathbb{C},\ |z| = 1\}$$

l'ensemble des nombres complexes de module 1. Comme le module $|\bullet|$ est multiplicatif, sa restriction a $\mathbb{C}^\times$ est un morphisme de groupe (multiplicatif) a valeurs dans $\mathbb{R}_{>0}$; ce morphisme est surjectif (car pour $x \in \mathbb{R}_{>0}$, $|x| = x$) et

$$\ker |\bullet| = \mathbb{C}^{(1)};$$

ainsi $\mathbb{C}^{(1)}$ est un sous-groupe de $\mathbb{C}^\times$ (pour la multiplication).

PROPOSITION 8.2. *On a un isomorphisme de groupes*

$$\mathrm{pol} : \mathbb{C}^\times \simeq \mathbb{R}_{>0} \times \mathbb{C}^{(1)}$$

donne par

$$z \in \mathbb{C}^\times \mapsto \mathrm{pol}(z) = (|z|, z/|z|)$$

Preuve: Soit $z \in \mathbb{C}^\times$. On a $|z| > 0$ et comme $||z|| = |z|$ ($|z|$ est un nombre reel positif de sorte que sont module est egal a sa valeur absolue et donc a $|z|$), on a

$$|z/|z|| = |z|/||z|| = |z|/|z| = 1.$$

Ainsi

$$\mathrm{pol}(z) \in \mathbb{R}_{>0} \times \mathbb{C}^{(1)}.$$

De plus on a

$$|z.z'| = |z|.|z'| \text{ et } z.z'/|z.z'| = (z/|z|).(z'/|z'|).$$

Ce morphisme de groupe pol est injectif:

$$(|z|, z/|z|) = (1,1) \Longrightarrow |z| = 1 = z/|z| \Longrightarrow z = 1.$$

Il est egalement surjectif : pour tout $\rho > 0$ et $z^{(1)} \in \mathbb{C}^1$, on a

$$\mathrm{pol}(\rho.z^{(1)}) = (|\rho.z^{(1)}|, \rho.z^{(1)}/|\rho.z^{(1)}|) = (\rho, z^{(1)});$$

en effet

$$|\rho.z^{(1)}| = |\rho|.|z^{(1)}| = \rho.1 = \rho$$

car $\rho \in \mathbb{R}_{>0}$. □

DÉFINITION 8.3. *Soit $z \in \mathbb{C}^\times$, $\mathrm{pol}(z) = (|z|, z/|z|)$ s'appelle la decomposition polaire de z.*

(1) Le premier terme $|z|$ est le module et se note aussi $\rho(z) = r(z) > 0$,

(2) le second terme $z/|z| \in \mathbb{C}^{(1)}$ est appelle argument complexe de z et on le note

$$z/|z| = e^{i\theta(z)}.$$

(3) Si on decompose l'argument complexe en partie reelle et imaginaire,

$$z/|z| = e^{i\theta(z)} = \mathrm{Re}(z/|z|) + i.\,\mathrm{Im}(z/|z|) = \mathrm{c}(z) + \mathrm{s}(z).i$$

on a donc

$$\mathrm{c}(z)^2 + \mathrm{s}(z)^2 = 1$$

- *le reel* $\mathrm{c}(z) \in [-1,1]$ *s'appelle le* cosinus de z,
- *le nombre* $\mathrm{s}(z) \in [-1,1]$ *s'appelle le* sinus de z.

On a donc

$$z = x + iy = \rho(z).e^{i\theta(z)} = \rho(z)(\mathrm{c}(z) + i\mathrm{s}(z)),\ x = \rho(z)\mathrm{c}(z),\ y = \rho(z)\mathrm{s}(z).$$

REMARQUE 8.2.2. Compte tenu des definitions, on a

$$\rho(z) = |z| = (x^2+y^2)^{1/2},$$
$$\mathrm{c}(z) = \frac{x}{(x^2+y^2)^{1/2}},\ \mathrm{s}(z) = \frac{y}{(x^2+y^2)^{1/2}}$$

8.2.2. Formules de trigonometrie. On retrouve les formules habituelles de trigonometrie:

8.2.2.1. *Formules de produit.* Pour $z, z' \in \mathbb{C}^\times$

$$\rho(z.z') = |z.z'| = |z|.|z'| = \rho(z).\rho(z'),\ e^{i\theta(z.z')} = e^{i\theta(z)}.e^{i\theta(z')} \tag{8.2.3}$$
$$\mathrm{c}(z.z') = \mathrm{c}(z).\mathrm{c}(z') - \mathrm{s}(z).\mathrm{s}(z'),\ \mathrm{s}(z.z') = \mathrm{s}(z).\mathrm{c}(z') + \mathrm{s}(z').\mathrm{c}(z).$$

Preuve: Les premieres identites resultent du fait que pol($\bullet$) est un morphisme de groupes. Ecrivant

$$e^{i\theta(z.z')} = \mathrm{c}(z.z') + i\mathrm{s}(z.z') =$$
$$e^{i\theta(z)}.e^{i\theta(z')} = (\mathrm{c}(z) + i\mathrm{s}(z)).(\mathrm{c}(z') + i\mathrm{s}(z'))$$

on obtient en developpant (suivant la regle de produit des complexes)

$$\mathrm{c}(z.z') + i\mathrm{s}(z.z') = \mathrm{c}(z)\mathrm{c}(z') + i\mathrm{s}(z)\mathrm{c}(z') + i\mathrm{c}(z)\mathrm{s}(z') + i^2\mathrm{s}(z)\mathrm{s}(z')$$
$$= \mathrm{c}(z)\mathrm{c}(z') - \mathrm{s}(z)\mathrm{s}(z') + i(\mathrm{s}(z)\mathrm{c}(z') + \mathrm{c}(z)\mathrm{s}(z')).$$

□

8.2.2.2. *Formule d'inversion.* Pour $z \in \mathbb{C}^\times$, on a

$$\rho(z^{-1}) = |z^{-1}| = \rho(z)^{-1} = |z|^{-1}$$
$$e^{i\theta(z^{-1})} = \mathrm{c}(z^{-1}) + i\mathrm{s}(z^{-1}) = (e^{i\theta(z)})^{-1} = \overline{e^{i\theta(z)}} = \mathrm{c}(z) - i\mathrm{s}(z).$$

En particulier on a

$$\mathrm{c}(z) = \mathrm{c}(z^{-1}),\ \mathrm{s}(z) = -\mathrm{s}(z^{-1}).$$

Preuve: Cela resulte a nouveau du fait que pol($\bullet$) est un morphisme de groupes. De plus, on a vu que (8.2.2)

$$(e^{i\theta(z)})^{-1} = \frac{\overline{e^{i\theta(z)}}}{|e^{i\theta(z)}|^2} = \overline{e^{i\theta(z)}} = \mathrm{c}(z) - i\mathrm{s}(z)$$

car $|e^{i\theta(z)}| = 1$. □

8.2.2.3. *Formule de l'angle double.* On a

$$|z^2| = |z|^2,\ \mathrm{c}(z^2) = \mathrm{c}(z)^2 - \mathrm{s}(z)^2,\ \mathrm{s}(z^2) = 2\mathrm{s}(z)\mathrm{c}(z).$$

Preuve: Appliquer la formule du produit a $z' = z$. □

Plus generalement on a les

8.2.2.4. *Formules de de Moivre.* Pour tout entier $n \geqslant 0$, on a[1]

$$|z^n| = |z|^n,\ e^{i\theta(z^n)} = (e^{i\theta(z)})^n$$
$$\mathrm{c}(z^n) = \sum_{0\leqslant k\leqslant n/2} C_n^{2k}(-1)^k\mathrm{c}(z)^{n-2k}\mathrm{s}(z)^{2k}, \tag{8.2.4}$$
$$\mathrm{s}(z^n) = \sum_{0\leqslant k\leqslant \frac{n-1}{2}} C_n^{2k+1}(-1)^k\mathrm{c}(z)^{n-2k-1}\mathrm{s}(z)^{2k+1}.$$

Preuve: Les premieres identites resultent a nouveau du fait que pol($\bullet$) est un morphisme de groupes.

Pour les deux autres on ecrit

$$e^{i\theta(z^n)} = \mathrm{c}(z^n) + i\mathrm{s}(z^n) = (e^{i\theta(z)})^n = (\mathrm{c}(z) + i\mathrm{s}(z))^n.$$

[1] d'apres Abraham de Moivre (1667-1754)

Par la formule du binome de Newton cela vaut

$$\sum_{0\leqslant k\leqslant n} C_n^k \mathrm{c}(z)^{n-k} i^k \mathrm{s}(z)^k.$$

On a

$$i^k = \begin{cases} (-1)^{k/2} & k \text{ pair} \\ (-1)^{(k-1)/2} i & k \text{ impair} \end{cases}$$

et on decompose la somme precedente suivant ces deux possibilites: la somme precedente s'ecrit

$$\mathrm{c}(z^n) + i\mathrm{s}(z^n) = \sum_{\substack{0\leqslant k\leqslant n \\ n\equiv 0 \,(\mathrm{mod}\, 2)}} C_n^k \mathrm{c}(z)^{n-k}(-1)^{k/2}\mathrm{s}(z)^k + \sum_{\substack{0\leqslant k\leqslant n \\ n\equiv 1 \,(\mathrm{mod}\, 2)}} C_n^k \mathrm{c}(z)^{n-k} i.(-1)^{\frac{k-1}{2}}\mathrm{s}(z)^k.$$

On met i en facteur dans le second terme et on identifie les parties reelles et imaginaires des complexes de part et d'autre ce cette identite: remplacant k par $2k \leqslant n$ dans la premiere somme et k par $2k+1 \leqslant n$ dans la seconde, on obtient les identites annoncees. □

Exemple 8.2.1. Par exemple pour $n = 2$, on obtient

$$\mathrm{c}(z^2) = \mathrm{c}(z)^2 - \mathrm{s}(z)^2,\ \mathrm{s}(z^2) = 2\mathrm{c}(z)\mathrm{s}(z).$$

Pour $k = 3$, on obtient

$$\mathrm{c}(z^3) = \mathrm{c}(z)^3 - 3\mathrm{c}(z)\mathrm{s}(z)^2,\ \mathrm{s}(z^3) = 3\mathrm{c}(z)^2\mathrm{s}(z) - \mathrm{s}(z)^3.$$

Pour $n = 4$, on obtient

$$\mathrm{c}(z^4) = \mathrm{c}(z)^4 - 6\mathrm{c}(z)^2\mathrm{s}(z)^2 + \mathrm{s}(z)^4,\ \mathrm{s}(z^4) = 4\mathrm{c}(z)^3\mathrm{s}(z) - 4\mathrm{c}(z)\mathrm{s}(z)^3.$$

8.2.3. Argument (reel) d'un nombre complexe. Dans ce cours qui est de nature algebrique, on a resiste jusqu'a present a parler *d' argument d'un nombre complexe*. La raison est la definition precise necessite des notions elaborees d'analyse (notamment la definition de l'exponentielle sur les complexes). On peut parler *d'argument reel* d'un nombre complexe une fois qu'on a demontrer (ou admis) le resultat suivant:

Théorème 8.2 (Existence de l'exponentielle complexe). *Il existe un unique morphisme de groupe*

$$e^{i\bullet} : \begin{array}{ccc} (\mathbb{R},+) & \mapsto & (\mathbb{C}^{(1)},\times) \\ \theta & \mapsto & \exp(i\theta) \end{array}$$

qui est derivable (comme fonction de $\mathbb{R}$ a valeurs dans $\mathbb{C} \simeq \mathbb{R}^2$) et qui verifie

$$e^{i\bullet\prime}(0) = i.$$

Ce morphisme est surjectif et son noyau est de la forme

$$\ker e^{i\bullet} = 2\pi.\mathbb{Z}$$

ou π est un nombre reel dont le developpement decimal commence par $\pi = 3.14159\cdots$.

Remarque 8.2.3. On dit qu'une fonction a valeurs complexes

$$f : \theta \in \mathbb{R} \mapsto f(\theta) \in \mathbb{C}$$

est derivable sur $\mathbb{R}$ si les fonctions associees "partie reelle" et "partie imaginaire" sont derivables: on ecrit

$$f(\theta) = \mathrm{Re} f(\theta) + i.\,\mathrm{Im}\, f(\theta)$$

et on demande que les deux fonctions

$$\mathrm{Re} f,\ \mathrm{Im}\, f : \theta \in \mathbb{R} \mapsto \mathrm{Re} f(\theta),\ \mathrm{Im}\, f(\theta) \in \mathbb{R}$$

soient derivables sur $\mathbb{R}$.

REMARQUE 8.2.4. On peut montrer que si un morphisme de groupes

$$\varphi : \mathbb{R} \mapsto \mathbb{C}^\times$$

est continu (ie. ses parties reeles et imaginaires sont continuees) alors il est automatiquement derivable et meme infiniment derivable.

Admettant ce Theoreme, on obtient par surjectivite que pour tout $z \in \mathbb{C}^{(1)}$ il existe $\theta \in \mathbb{R}$ tel que

$$z = e^{i\theta}.$$

D'autre part, comme $e^{i\bullet}$ est un morphisme de groupes, l'ensemble des θ' verifiant $z = e^{i\theta'}$ (l'ensemble des antecedents de z, $(e^{i\bullet})^{-1}(\{z\})$) est egale a la classe de θ modulo 2π (cf. Exercice 2.4)

$$(e^{i\bullet})^{-1}(\{z\}) = \theta + \ker(e^{i\bullet}) = \theta + 2.\pi.\mathbb{Z} = \{\theta + 2\pi.k,\ k \in \mathbb{Z}\}.$$

On obtient alors une bijection (qu'on notera encore $e^{i\bullet}$)

$$e^{i\bullet} : \begin{array}{ccc} \mathbb{R}/2\pi\mathbb{Z} & \simeq & \mathbb{C}^{(1)} \\ \theta + 2\pi\mathbb{Z} & \mapsto & z = e^{i\theta}. \end{array}$$

REMARQUE 8.2.5. En fait cette bijection est un isomorphisme de groupes (Theoreme Noyau-Image pour les groupes).

La reciproque de cette bijection s'appelle *l'argument (reel)*:

DÉFINITION 8.4. *Soit z un nombre complexe de module 1 L'argument reel (encore appelle "angle") de z,*

$$\arg(z) := \theta \,(\mathrm{mod}\, 2\pi) = \theta + 2\pi\mathbb{Z} \in \mathbb{R}/2\pi\mathbb{Z}$$

est l'unique classe $\theta \,(\mathrm{mod}\, 2\pi) \in \mathbb{R}/2\pi\mathbb{Z}$ telle que $e^{i\theta} = z$.

Plus generalement, pour $z \in \mathbb{C}^\times$, on defini son argument par

$$\arg(z) := \arg(z/|z|) \in \mathbb{R}/2\pi\mathbb{Z}.$$

Notons que l'application

$$\arg : \mathbb{C}^\times \mapsto \mathbb{R}/2\pi\mathbb{Z}$$

est un morphisme de groupes: $\forall z, z' \in \mathbb{C}^\times$ on a

$$\arg(1) = 0,\ \arg(z.z') = \arg(z) + \arg(z'),\ \arg(1/z) = -\arg(z).$$

et la decomposition polaire se reecrit sous la form de l'isomorphisme

$$\mathrm{pol} : \begin{array}{ccc} \mathbb{C}^\times & \simeq & \mathbb{R}_{>0} \times \mathbb{R}/2\pi\mathbb{Z} \\ z & \mapsto & (|z|, \arg(z)) \end{array}.$$

DÉFINITION 8.5. *Soit $\theta \in \mathbb{R}$, le cosinus et le sinus de θ sont defini par*

$$\cos(\theta) = \mathrm{Re}(e^{i\theta}),\ \sin(\theta) = \mathrm{Im}(e^{i\theta}).$$

On a donc

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

En particulier on a

$$1 = e^{i0} = \cos(0) + i\sin(0)$$

et donc

$$\cos(0) = 1,\ \sin(0) = 0.$$

8.2.4. Formules de trigonometrie classiques. On "retrouve" les formules de trigonometrie sous leur forme usuelle:

8.2.4.1. *Formule des sommes.* On a

$$\cos(\theta+\theta') = \mathrm{Re}(e^{i\theta+\theta'}) = \mathrm{Re}(e^{i\theta}.e^{i\theta'}) = \cos(\theta)\cos(\theta') - \sin(\theta).\sin(\theta')$$

et

$$\sin(\theta+\theta') = \mathrm{Im}(e^{i\theta+\theta'}) = \mathrm{Im}(e^{i\theta}.e^{i\theta'}) = \sin(\theta)\cos(\theta') + \cos(\theta).\sin(\theta').$$

Preuve: On a

$$e^{i\theta+\theta'} = \cos(\theta+\theta') + i\sin(\theta+\theta') = e^{i\theta}.e^{i\theta'} = (\cos(\theta)+i\sin(\theta)).(\cos(\theta')+i\sin(\theta'))$$

et on obtient le result en developpant et en isolant les parties reeles et imaginaires. □

8.2.4.2. *Formule de l'angle oppose.* On a

$$\cos(-\theta) = \cos(\theta),\ \sin(-\theta) = -\sin(\theta).$$

Preuve: En effet comme on a un morphisme de groupes

$$e^{-i\theta} = \cos(-\theta) + i\sin(-\theta) = 1/e^{i\theta} = \overline{e^{i\theta}} = \cos(\theta) - i\sin(\theta).$$

□

8.2.4.3. *Formule de l'angle double.* En prenant $\theta' = \theta$ on obtient

$$\cos(2\theta) = \cos(\theta)^2 - \sin(\theta)^2,\ \sin(2\theta) = 2\sin(\theta)\cos(\theta)$$

et plus generalement

8.2.4.4. *Formules de de Moivre.*

$$e^{in\theta} = \cos(n\theta) + i\sin(n\theta) = (e^{i\theta})^n = (\cos(\theta)+i\sin(\theta))^n$$

et en developpant par le binome d eNewton et identifiant parties reelles et imaginaires, on obtient

$$\cos(n\theta) = \sum_{0\leqslant k\leqslant n/2} C_n^{2k}(-1)^k\cos(\theta)^{n-2k}\sin(\theta)^{2k}.$$

$$\sin(n\theta) = \sum_{0\leqslant k\leqslant (n-1)/2} C_n^{2k+1}(-1)^k\cos(\theta)^{n-2k-1}\sin(\theta)^{2k+1}.$$

8.3. Le plan complexe

Comme $\mathbb{C}$ est un $\mathbb{R}$-ev de dimension 2, on peut identifier $\mathbb{C}$ a $\mathbb{R}^2$ en choisissant une base. Ainsi si on prend pour base $\{\mathrm{Id}, I\}$ l'isomorphisme est donne par les parties reele et imaginaire:

$$(\mathrm{Re},\mathrm{Im}) : \begin{array}{ccc} \mathbb{C} & \mapsto & \mathbb{R}^2 \\ z = x.\mathrm{Id} + y.I & \mapsto & (x,y) \end{array}.$$

On parle alors du plan complexe et on represente un nombre complexe par un point dans le plan reel $\mathbb{R}^2$. Le groupe des nombres complexes de module 1 est alors identifier avec le cercle unite

$$S^1 = \{(x,y)\in\mathbb{R}^2,\ x^2+y^2 = 1\}.$$

8.4. Equations polynomiales complexes

Le corps des nombres complexes $\mathbb{C}$ a ete introduit (pas sous forme de matrices) dans la renaissance italienne dans l'etude des equations polynomiales: l'etude des solutions z des equations de la forme

$$P(z) = a_d.z^d + a_{d-1}.z^{d-1} + \cdots + a_1.z + a_0 = 0, \tag{8.4.1}$$

avec $a_0,\cdots,a_d\in\mathbb{R}$ des nombres reels[2].

[2]en fait c'etait plutot les nombres rationels car le corps des reels n'existait pas encore mais on s'autorisait a extraire des racines n-iemes de nombres rationnels positifs ou nuls

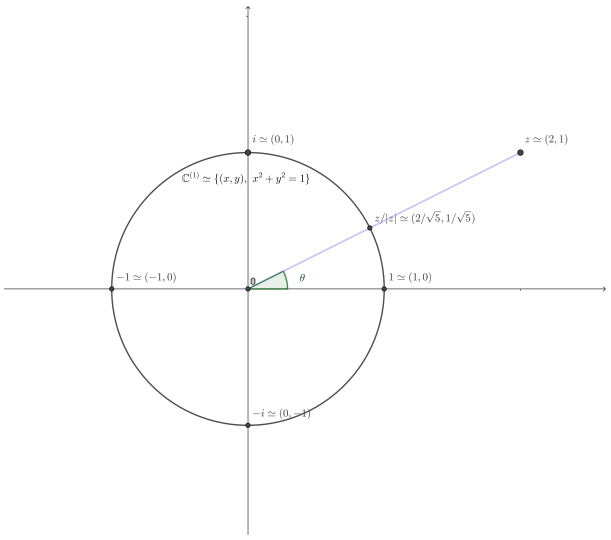


FIGURE 1. Le plan complexe et le cercle unite.

DÉFINITION 8.6. *Soit*

$$P(X) = a_d.X^d + a_{d-1}.X^{d-1} + \cdots + a_1.X + a_0$$

un polynome a coefficient dans $\mathbb{C}$. *L'ensemble des racines de* P *dans* $\mathbb{C}$, $\mathrm{Rac}_P(\mathbb{C})$ *est l'ensemble des solution dans* $\mathcal{C}_c$ *de l'equation* $P(z) = 0$*:*

$$\mathrm{Rac}_P(\mathbb{C}) = \{z \in \mathbb{C},\ P(z) = 0\}.$$

On rappelle (cf. Thm 12.4 dans le chapitre sur les polynomes) que

$$|\mathrm{Rac}_P(\mathbb{C})| \leqslant \deg P \leqslant d.$$

En particulier pour $d = 2$ (les equations quadratiques)

$$az^2 + bz + c = 0 \tag{8.4.2}$$

l'equation n'avait pas de solution si le discriminant $\Delta = b^2 - 4ac < 0$; en particulier c'est le cas de l'equation

$$z^2 + 1 = 0$$

dont le discriminant vaut $-4 < 0$. On a alors introduit "formellement" une solution i verifiant

$$i^2 = -1$$

qu'on a appelle nombre "imaginaire" et obtenu le corps $\mathbb{C}$. On a alors trouve dans $\mathbb{C}$ des solutions de toutes les equations quadratiques a coefficients reels : elles sont donnees par la formule usuelle

$$z_\pm = \frac{-b \pm \sqrt{\Delta}}{2a}$$

ou $\sqrt{\Delta}$ est l'une des racines carrees de Δ si $\Delta > 0$ et si $\Delta < 0$ on prend

$$\sqrt{\Delta} := \sqrt{|\Delta|}.i$$

8.4.1. Equations quadratiques a coefficients complexes. Considerons maintenant la meme equation

$$az^2 + bz + c = 0 \tag{8.4.3}$$

mais avec $a, b, c \in \mathbb{C}$. Les meme manipulations algebriques nous disent que les solutions de cette equation sont de la forme

$$z_\pm = \frac{-b \pm \sqrt{\Delta}}{2a}$$

ce qui nous reduit a trouver les solution de l'equation quadratique "monomiale"

$$Z^2 = \Delta$$

pour $\Delta \in \mathbb{C}$. Pour cela on ecrit $\Delta = A + IB$ et $Z = X + iY$ et on a donc

$$Z^2 = X^2 - Y^2 + 2XY.i = A + iB$$

ce qui nous amene a un systeme de deux equations polynomiales a coefficients dans $\mathbb{R}$ en deux inconnues X, Y dans $\mathbb{R}$:

$$X^2 - Y^2 = A,\ 2XY = B.$$

On peut supposer que $B \neq 0$ car sinon on a $\Delta = A \in \mathbb{R}$ et on sait resoudre l'equation (meme si $A < 0$). On a donc $X, Y \neq 0$ et on peut ecrire $Y = B/2X$ et substituer:

$$X^2 - B^2/(4X^2) = A \Longleftrightarrow 4X^4 - 4AX^2 - B^2 = 0,\ X \neq 0$$

Posant $U = 2X^2$ on doit resoudre l'equation quadratique

$$U^2 - 2AU - B^2 = 0$$

dont le discriminant vaut

$$\Delta' = 4(A^2 + B^2) > 0.$$

On trouve donc deux racines reelles

$$U_\pm = A \pm \sqrt{A^2 + B^2}.$$

Comme $\sqrt{A^2 + B^2} > A$, l'une de ses solution est positive et l'autre negative mais comme $U = X^2$ et que $X \in \mathbb{R}$ on doit avoir $U \geqslant 0$ et on prend

$$U_+ = A + \sqrt{A^2 + B^2}$$

et on prend

$$X_\pm = \pm\sqrt{U_+}.$$

On trouve alors $Y_\pm = \pm B/(2\sqrt{U_+})$ et on obtient deux solutions

$$Z_\pm = \pm(\sqrt{U_+} + iB/(2\sqrt{U_+})).$$

8.4.2. Nombres complexes ayant des arguments particuliers. Il y a extremement peu de nombres complexes de module 1 pour lesquel on dispose d'une formule simple pour leur argument reel et il y a de bonnes raisons a cela. Pour $n \geqslant 1$ un entier on pose

$$\omega_n = e^{i2\pi/n}.$$

On va calculer quelques ω_n.

Pour cela on remarque que comme $\ker(e^{i\bullet}) = 2\pi\mathbb{Z}$ et que $e^{i\bullet}$ est surjective sur $\mathbb{C}^{(1)}$, $e^{i\bullet}$ induit une bijection

$$e^{i\bullet} : [0, 2\pi[\simeq \mathbb{C}^{(1)}.$$

On peut commencer:

8.4.2.1. $n = 1$. On a

$$\omega_1 = e^{i0} = 1$$

car un morphisme de groupe envoie l'element neutre sur l'element neutre.

8.4.2.2. $n = 2$. On a (formule d'Euler)

$$\omega_2 = e^{i\pi} = -1.$$

En effet on a

$$(\omega_2)^2 = e^{i2\pi} = 1$$

donc ω_2 est une racine carree de 1 et donc vaut ± 1. Comme on sait que $e^{i0} = 1$ et que $e^{i\pi} \neq e^{i0}$ c'est que $\omega_2 = -1$.

8.4.2.3. $n = 4$. On a

$$\omega_4 = e^{i\pi/2} = i.$$

Preuve: Exercice. □

8.4.2.4. $n = 8$. On a

$$\omega_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

Preuve: Exercice. □

8.4.2.5. $n = 3$. On a

$$\omega_3 = \frac{-1 + i\sqrt{3}}{2}.$$

Preuve: Exercice. □

8.4.2.6. $n = 5$. On a

$$\omega_5 = \cos(2\pi/5) + i\sin(2\pi/5)$$

avec

$$\cos(2\pi/5) = -\frac{1+\sqrt{5}}{4},\ \sin(2\pi/5) = \sqrt{1 - (\frac{1+\sqrt{5}}{4})^2}.$$

Preuve: Exercice. □

8.4.2.7. *Formule de l'angle moitie.* Le calcul de $\omega_2, \omega_4, \omega_8$ proviennent d'un principe general: si on connait $\omega_n = e^{i2\pi/n}$ alors on saura exprimer simplement $\omega_{2n} = e^{i2\pi/2n}$ des parties reelles et imaginaires de ω_n. En effet

$$\omega_{2n}^2 = \omega_n$$

et ω_{2n} est solution de l'equation

$$X^2 = \omega_n$$

que l'on sait resoudre. On obtient ainsi

$$\omega_6 = \frac{\sqrt{3} + i}{2}.$$

On voit que les parties reelles et imaginaires de tous ces nombres complexes s'expriment par extractions successives de racines carrees. En fait il n'y a pas beaucoup d'autre cas ou cela est possible:

THÉORÈME 8.3 (Gauss-Wantzel). *On peut exprimer les parties reelles et imaginaires du nombre complexe $\omega_n = e^{i2\pi/n}$ par extraction successive de racines carrees si et seulement si*

$$n = 2^k \text{ ou bien } n = 2^k \prod_i p_i$$

ou $\prod_i p_i$ est un produit (non-vide) de nombres premiers tous distincts et "de Fermat": on dit qu'un nombre premier p_i est de Fermat si $p_i = F_{f_i} := 2^{2^{f_i}} + 1$ avec $f_i \geqslant 0$ un entier.

REMARQUE 8.4.1. Les nombres premiers $F_0 = 3, F_1 = 5, F_2 = 17$ sont de Fermat et Gauss est devenu celebre quand a 19 ans il a montre que la condition etait suffisante et a exprimer ω_{17} sous cette forme; un peu plus tard Wantzel a montre qu'elle etait necessaire. Les autres premiers de Fermat connus sont $F_3 = 257$ et $F_4 = 65537$; les entiers $F_5, \cdots, F_{32}$ ne sont pas premiers et on ne sait pas si F_{33} ou les entiers de Fermat suivant sont premiers ou pas.

8.4.3. Equations de degre superieur. On a egalement pu resoudre dans $\mathbb{C}$ de nombreuses autres equations polynomiales a coefficient reels. En particulier pour les equations de degre 2, 3 ou 4, on (les italiens) a pu obtenir des expressions algebriques explicites pour les solutions des equations polynomiales en fonction des coefficients du polynome (formules de Cardan) ainsi que pour des polynomes de degre superieur mais speciaux cela en extrayant des racines carrees, cubiques ou quartiques ou d'ordre superieur: on parle d'equation resolubles par radicaux.

Le resultat le plus general est du a Gauss qui a demontre le

THÉORÈME (fondamental de l'algebre). *Soit $P(X) \in \mathbb{R}[X] = a_d.z^d + a_{d-1}.z^{d-1} + \cdots + a_1.z + a_0$ un polynome reel non-constant alors l'equation (8.4.1) admet au moins une solution dans $\mathbb{C}$: il existe $z \in \mathbb{C}$ tel que $P(z) = 0$. En fait c'est egalement vrai si $P(X) \in \mathbb{C}[X]$ c'est a dire si l'equation polynomiale est a coefficient dans $\mathbb{C}$. On dit que $\mathbb{C}$ est algebriquement clos.*

REMARQUE 8.4.2. Ce theoreme n'est pas constructif : il demontre l'existence de solutions mais ne donne pas d'expression des solutions en fonctions des coefficients de P (comme c'est le cas pour les equations quadratiques ou cubiques ou quartiques). Ce probleme a ete analyse en details par Abel et Galois. En particulier Abel a donne un polynome explicite

$$X^5 - X - 1$$

dont les racines ne peuvent s'exprimer par l'extractino de racines carrees, cubiques, quartique, quintiques (ou de tout ordre) de nombres rationnels (cette equation n'est pas resoluble par radicaux). Galois a ensuite donne une condition necessaire et suffisante (en terme d'un certain groupe associe au polynome) pour decider si l'equation est resoluble par radicaux ou pas. C'est l'objet de ce qu'on appelle la *Theorie de Galois*.

EXERCICE 8.1. Demontrer la partie facile du Theoreme de Gauss: si tout polynome a coefficient reel admet une racine alors tout polynome a coefficient complexes admet une racine.

Pour cela considerer

$$P(X) = a_d.z^d + a_{d-1}.z^{d-1} + \cdots + a_1.z + a_0 \in \mathbb{C}[X]$$

et

$$\overline{P}(X) = \overline{a_d}.z^d + \overline{a_{d-1}}.z^{d-1} + \cdots + \overline{a_1}.z + \overline{a_0}$$

et montrer que $Q(X) = P(X).\overline{P}(X) \in \mathbb{R}[X]$ et conclure.

On n'a pas encore les moyens de demontre ce resultat fondamental. On peut le faire soit

(1) Avec de l'analyse reele classique (theoreme des valeurs intermediaires) et de la *Theorie de Galois*.
(2) Ou bien avec de l'analyse complexe: soit

$$z \in \mathbb{C} \mapsto P(z) \in \mathbb{C}$$

un polynome non-constant qui ne s'annule pas sur $\mathbb{C}$ alors la fonction

$$z \mapsto 1/P(z)$$

est holomorphe sur $\mathbb{C}$ et bornee; cela implique necessairement qu'elle est constante et donc que $P(z)$ est constant.

CHAPITRE 9

Operations elementaires sur les matrices

The first matrix I designed was quite naturally perfect.
It was a work of art. Flawless. Sublime.
A triumph only equaled by its monumental failure.

9.1. Operation elementaires sur les lignes

Soit $M = (m_{ij}) \in M_{d' \times d}(K)$ une matrice. Pour simplifier les notations on ecrira sa i-ieme ligne $(i \leqslant d')$

$$L_i = L_i(M) = \mathrm{Lig}_i(M) = (m_{ij})_{j \leqslant d}$$

DÉFINITION 9.1. *Les operations elementaires sur les lignes d'une matrice sont les applications suivantes de $M_{d' \times d}(K)$ vers $M_{d' \times d}(K)$: pour $i, j \in \{1, \cdots, d'\}$ et $\lambda \in K^\times$ et $\mu \in K$*

(I) Transposition: Echanger deux lignes $i \neq j \leqslant d'$ de M:

$$L_i \longleftrightarrow L_j$$

(II) Dilatation: Multiplier la i-eme ligne par un scalaire $\lambda \neq 0$:

$$L_i \to \lambda . L_i.$$

(III) Combinaison Lineaire: Additioner a la ligne i un multiple scalaire de la la j-ieme ligne: $\mu \in K$

$$L_i \to L_i + \mu L_j$$

Ces transformations sont appellees transformations *elementaires*.

EXEMPLE 9.1.1. Considerons la matrice

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 2 & 2 & 2 \\ 2 & 1 & 2 \end{pmatrix}. \tag{9.1.1}$$

On lui applique la transposition $L_1 \leftrightarrow L_2$ et on obtient

$$M_1 = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 1 & 1 \\ 2 & 1 & 2 \end{pmatrix}.$$

On applique $L_1 \to (1/2).L_1$ et on obtient

$$M_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 2 \end{pmatrix}.$$

On applique $L_3 \to L_3 - 2.L_1$ et on obtient

$$M_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

On applique $L_3 \to L_3 + L_2$ et on obtient

$$M_4 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

On applique $L_1 \to L_1 - L_2$ et on obtient

$$M_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

On applique $L_2 \to L_2 - L_3$ et on obtient

$$M_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{Id}_3.$$

PROPOSITION 9.1. *Ces trois operations sont des applications lineaires bijectives*

$$(I), (II), (III) : \ M_{d' \times d}(K) \mapsto M_{d' \times d}(K).$$

Preuve: La linearite vient du fait que les applications

$$\mathrm{Lig}_i(\bullet), \ \mathrm{Lig}_j(\bullet) : M \in M_{d' \times d}(K) \mapsto M_i \in \mathrm{Lig}_d(K)$$

sont lineaires et que l'application

$$(\mathrm{Lig}_i + \mu \mathrm{Lig}_j)(\bullet) : M \in M_{d' \times d}(K) \mapsto L_i + \mu.L_j \in \mathrm{Lig}_d(K)$$

est lineaire. Elle sont bijectives car elle admettent des applications reciproques:

(I) Echanger les deux memes lignes $i, j \leqslant d'$ de M:

$$L_i \longleftrightarrow L_j$$

(II) Multiplier la i-eme ligne par le scalaire λ^{-1}:

$$L_i \to \lambda^{-1}.L_i.$$

(III) Soustraire a la ligne i un multiple scalaire de la j-ieme ligne: $\mu \in K$

$$L_i \to L_i - \mu L_j$$

□

PROPOSITION 9.2. *Les trois operations elementaires sont obtenues par multiplication a gauche de M par des matrices convenables: pour $1 \leqslant i, j \leqslant d'$*

(I) $T_{ij}.\bullet : M \mapsto T_{ij}.M$
(II) $D_{i,\lambda}.\bullet : M \mapsto D_{i,\lambda}.M$
(III) $Cl_{ij,\mu}.\bullet : M \mapsto Cl_{ij,\mu}.M$.

ou les matrices carrees $T_{ij}, \ D_{i,\lambda}, \ Cl_{ij,\mu} \in M_{d'}(K)$ *sont definies par:*

$$T_{ij} = \mathrm{Id}_{d'} - E_{ii} - E_{jj} + E_{ij} + E_{ji}.$$

$$D_{i,\lambda} = \mathrm{Id}_{d'} + (\lambda - 1).E_{ii}, \ \lambda \neq 0$$

$$Cl_{ij,\mu} = \mathrm{Id}_{d'} + \mu.E_{ij}, \ i \neq j \ ou \ \mu \neq -1 \ si \ i = j.$$

Preuve: Notons $E_{ij} = (e_{ij,kl})_{k,j \leqslant d'}$ la matrice elementaire sous forme de coefficients: on a

$$e_{ij,kl} = \delta_{k=i}.\delta_{l=j}$$

On a donc pour $1 \leqslant k, l \leqslant d'$

$$(E_{ij}.M)_{kl} = \sum_{u \leqslant d'} e_{ij,ku}.m_{ul} = \sum_{u \leqslant d'} \delta_{k=i}\delta_{u=j}.m_{ul} = \delta_{k=i} m_{jl}.$$

Ainsi le produit $E_{ij}.M$ est la matrice dont la i-ieme ligne est la j-ieme ligne $L_j = (m_{jl})_{l\leqslant d'}$ et dont toutes les autres coordonnees sont nulles.

– Ainsi $(\mathrm{Id}_{d'} + \mu.E_{ij}).M$ est la matrice formee a partir de M et ou la i-ligne L_i est remplacee par $L_i + \mu.L_j$.

– En particulier, si $i = j$, $(\mathrm{Id}_{d'} + \mu.E_{ii}).M$ est la matrice forme a partir de M et ou la i-ligne L_i est remplacee par $L_i + \mu.L_i = (1 + \mu).L_i$. Ainsi en prenant $\lambda = 1 + \mu$, on multiplie la i-ieme ligne de M par λ.

– De meme $(\mathrm{Id}_{d'} - E_{ii} - E_{jj}).M$ est la matrice M ou les lignes i et j sont remplacees par la ligne nulle $(0)_{l\leqslant d'}$ et

$$(\mathrm{Id}_{d'} - E_{ii} - E_{jj}).M + (E_{ij} + E_{ji}).M$$

est la matrice precedente ou la ligne L_j est ajoutee a la i-ieme ligne et ou la ligne L_j est ajoutee a la j-ieme ligne de M et c'est donc la matrice M ou les ligne i et j ont ete echangees. □

Remarque 9.1.1. En particulier, le fait que ces applications sont lineaires provient du fait que pour toute matrice $D \in M_{d'}(K)$ la multiplication a gauche par D

$$D.\bullet : M \in M_{d'\times d}(K) \mapsto D.M \in M_{d'\times d}(K)$$

est lineaire (par distributivite de la multiplication a gauche, Thm. 7.1).

De plus si D est inversible: $D \in \mathrm{GL}_{d'}(K)$ alors $D.\bullet$ est inversible d'inverse $D^{-1}.\bullet$: en effet

$$D^{-1}.(D.M) = (D^{-1}.D).M = \mathrm{Id}_{d'}.M = M,\ D.(D^{-1}.M) = (D.D^{-1}).M = \mathrm{Id}_{d'}.M = M.$$

Notons que les matrices $T_{ij},\ D_{i,\lambda},\ Cl_{ij,\mu}$ sont inversibles (si $\lambda \neq 0$ ou $i \neq j$ pour $Cl_{ij,\mu}$) et on a

$$T_{ij}^{-1} = T_{ij},\ \ D_{i,\lambda}^{-1} = D_{i,\lambda^{-1}},\ Cl_{ij,\mu}^{-1} = L_{ij,-\mu}.$$

Remarque 9.1.2. On peut verifier directement que

$$T_{ij}.T_{ij} = \mathrm{Id}_{d'},\ D_{i,\lambda}.D_{i,\lambda^{-1}} = \mathrm{Id}_{d'},\ Cl_{ij,\mu}.Cl_{ij,-\mu} = \mathrm{Id}_{d'}$$

en utilisant que

$$E_{ij}.E_{kl} = \delta_{j=k}E_{il}$$

Définition 9.2. *Les matrices*

$$T_{ij},\ D_{i,\lambda},\ \lambda \neq 0,\ Cl_{ij,\mu}$$

pour $i, j \leqslant d'$, $\lambda \neq 0$, $\mu \neq -1$ si $i = j$ sont appellees matrices de transformations elementaires.

Remarque 9.1.3. On ne confondra pas les matrices de transformations elementaires avec les matrices elementaires qui sont les matrices E_{ij}.

Définition 9.3. *On dit que N est ligne-equivalente a M ssi il existe une suite de transformations elementaires qui transforme M en N.*

– De maniere equivalente, N est ligne-equivalente a M ssi il existe une suite finie de matrices des transformations elementaires telle que N est obtenue a partir de M par multiplications a gauche par cette suite de matrices.

Exemple 9.1.2. La matrice M de (9.1.1) est ligne equivalente a la matrice identite Id_3: on a

$$\mathrm{Id}_3 = Cl_{23,-1}Cl_{12,-1}Cl_{32,1}Cl_{31,-2}D_{1,1/2}T_{12}M$$

Proposition 9.3. *La relation etre "ligne-equivalente" est une relation d'equivalence sur $M_{d'\times d}(K)$.*

– De plus deux matrices M, N ligne-equivalentes sont equivalentes au sens de la notion d'equivalence de deux matrices de la Definition 7.10.

Preuve: Comme toutes les transfomations elementaires sont inversibles et que leur inverse sont des transformations elementaires, cette relation est reflexive, symetrique et transitive.

Si M et N sont lignes-equivalentes, alors

$$N = A.M = A.M.\mathrm{Id}_d$$

ou ou A le produit des matrices de transformations elementaires qui permettrent de passer de M a N et M et N sont donc equivalentes. □

PROPOSITION 9.4. *Si $N \in M_{d'\times d}(K)$ est ligne-equivalente a M alors toute ligne de N est combinaison lineaire des lignes de M:*

$$\forall i \leqslant d',\ \mathrm{Lig}_i(N) \in \langle L_1, \cdots, L_{d'}\rangle \subset K^d$$

et inversement les lignes de M sont combinaisons lineaires des lignes de N.

Preuve: Par definition des transformations elementaires, les lignes de N sont des combinaisons lineaires des lignes de M. Mais comme la relation "ligne-equivalente" est une relation d'equivalence les lignes de M sont CL des lignes de N. □

9.2. Echelonnage

DÉFINITION 9.4. *Une matrice $M = (m_{ij}) \in M_{d'\times d}(K)$ est echelonnee si elle est nulle ou bien si*

(1) Il existe $1 \leqslant j_1 < \cdots < j_r \leqslant d$ tels que
- *Pour la ligne L_1, le premier terme non-nul est le j_1-ieme: on a $m_{1j} = 0$ pour tout $j < j_1$ et $m_{1j_1} \neq 0$,*
- *Pour la ligne L_2, le premier terme non-nul est le j_2-ieme: on a $m_{2j} = 0$ pour tout $j < j_2$ et $m_{2j_2} \neq 0$,*
- $\vdots$
- *Pour la ligne L_r, le premier terme non-nul est le j_r-ieme: on a $m_{rj} = 0$ pour tout $j < j_r$ et $m_{rj_r} \neq 0$*

(2) Si $r < d$ les lignes $L_{r+1}, \cdots, L_{d'}$ sont toutes nulles.

Si M est non-nulle les $j_1 < \cdots < j_r$ sont appeles les echelons de M et les m_{ij_i}, $1 \leqslant i \leqslant r$ sont les pivots de M.

La matrice ci-dessous a $r = 3$ echelons: $j_1 = 2, j_2 = 4, j_3 = 5$

$$\begin{pmatrix} 0 & m_{12} & m_{13} & m_{14} & \cdots & \cdots & m_{1d} \\ 0 & 0 & 0 & m_{24} & \cdots & \cdots & m_{2d} \\ 0 & 0 & 0 & 0 & m_{35} & \cdots & \cdots\cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

DÉFINITION 9.5. *Si de plus*

$$m_{1j_1} = m_{2j_2} = \cdots = m_{rj_r} = 1$$

et $m_{ij} = 0$ pour tout $(i,j) \neq (i,j_i), 1 \leqslant i \leqslant r$ la matrice M est dite echelonnee reduite.

La matrice ci-dessous a $r = 3$ echelons: $j_1 = 2, j_2 = 4, j_3 = 5$ et est echelonnee reduite.

$$\begin{pmatrix} 0 & 1 & m_{13} & 0 & 0 & \cdots & m_{1d} \\ 0 & 0 & 0 & 1 & 0 & \cdots & m_{2d} \\ 0 & 0 & 0 & 0 & 1 & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

THÉORÈME 9.1 (Gauss). *Toute matrice est ligne-equivalente a une matrice echelonnee reduite.*

Preuve: Si $M = 0_{d'\times d}$ on a termine. Si $M \neq 0_{d'\times d}$, soit j_1 le plus petit indice d'une colonne non-nulle. Soit $m_{ij_1} \neq 0$. Quitte a remplacer M par $T_{1i}.M$ ops $i = 1$.

On peut remplacer la premiere ligne L_1 par $m_{ij_1}^{-1}.L_1$ et supposons que $m_{1,j_1} = 1$. En remplacant les $L_i, i > 1$ par $L_i - m_{ij_1}L_1$ annule les autres coefficients de la colonne j_1 et on obtient une matrice ligne-equivalente de la forme (ici $j_1 = 3$)

$$M' = \begin{pmatrix} 0 & 0 & 1 & * & * & \cdots & * \\ 0 & 0 & 0 & m'_{2,j_1+1} & * & \cdots & * \\ 0 & 0 & 0 & * & * & \cdots & \cdots \\ 0 & 0 & 0 & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & m'_{d',j_1+1} & * & * & * \end{pmatrix}$$

On repete la procedure avec la matrice extraite de M' a partir de la deuxieme ligne et de la $j_1 + 1$-ieme colonne. On effectue des operations sur les lignes a partir de la deuxieme et donc sans changer la premiere. La matrice M est remplacee par une matrice de la forme

$$M'' = \begin{pmatrix} 0 & 0 & 1 & * & m''_{1j_2} & * & * & \cdots & * \\ 0 & 0 & 0 & 0 & 1 & * & * & \cdots & * \\ 0 & 0 & 0 & 0 & 0 & * & * & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & * & * & * & * \\ \vdots & \vdots & \vdots & 0 & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & 0 & * & * & * & * \end{pmatrix}$$

et on peut alors remplacer la premiere ligne L''_1 par $L''_1 - m''_{1j_2}L''_2$ pour force le coefficient au dessus du deuxieme pivot egal a 0. Notons que cette transformation ne modifie par les coefficients de la ligne L_1 qui sont en position $< j_2$ car les coefficent de L''_2 dans ces positions sont nuls.

□

Exemple 9.2.1. L'exemple 9.1.1 est l'echelonnage de la matrice

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 2 & 2 & 2 \\ 2 & 1 & 2 \end{pmatrix}$$

en la matrice echelonnee reduite Id_3.

Proposition 9.5. *Deux matrices ligne-equivalentes et echelonnees reduites sont egales.*

Preuve. Admis. □

Corollaire 9.1. *(Unicite de la forme echelonne reduite) Soit $M \in M_{d'\times d}(K)$ une matrice alors M est ligne-equivalente a une unique matrice echelonnee reduite (qu'on appelle la forme echelonnee reduite de M).*

Preuve: Si M est ligne-equivalente a deux matrices echelonnees reduites R, R' alors R et R' sont ligne-equivalentes (car c'est une relation d'equivalence) et donc $R = R'$. □

9.3. Applications

9.3.1. Calcul du rang. Comme on a observe si M et N sont lignes-equivalentes elles sont equivalentes; on a donc

Proposition 9.6. *Si M et N sont lignes equivalentes*

$$\mathrm{rg}(M) = \mathrm{rg}(N).$$

Ensuite on a

PROPOSITION 9.7. *Si R est echelonnee avec r echelons alors*

$$\mathrm{rg}(R) = r.$$

Preuve: Il s'agit de voir que R possede exactement r lignes lineairement independantes (cf. Corollaire 7.1). Comme R est echelonnee reduite elle possede $d' - r$ ligne nulles et r lignes de la forme

$$L_i = (0, \cdots, p_1, *, \cdots, *)$$

ou $p_i = m_{ij_i} \neq 0$ est en position $j_i,\ i \leqslant r$ sur la ligne L_i. Si

$$x_1.L_1 + \cdots + x_r.L_r = \mathbf{0}_d$$

la coordonnee j_1 donne $x_1 p_1 = 0$ et donc $x_1 = 0$, ensuite (sachant que $x_1 = 0$) la coordonnee j_2 donne $x_2 = 0$,..., et enfin $x_r = 0$. □

9.3.2. Generation du groupe lineaire.

PROPOSITION 9.8 (Critere d'inversibilite par operations elementaires). *Soit $M \in M_d(K)$ une matrice carree alors M est inversible ssi M est ligne equivalente a la matrice identite* Id_d.

Preuve: La matrice M est inversible ssi elle est de rang d. Une matrice echelonne reduite carree de taille d et de rang d possede d echelons et est donc triangulaire superieure avec des 1 sur la diagonale; comme elle est reduite, on dessu de chaque 1 on n'a que des 0 et la matrice ne peut etre que l'identite. □

THÉORÈME 9.2 (Engendrement par les matrices de transformations elementaires). *Le groupe lineaire* $\mathrm{GL}_d(K)$ *est engendre par les matrices des transformations elementaires*

$$T_{ij}, D_{i,\lambda},\ Cl_{ij,\mu},\ i,j \leqslant d,\ \lambda,\mu \in K,\ \lambda \neq 1.$$

En d'autres termes (puisque l'ensemble des matrices de transformations elementaires est stable par inverse) tout matrice $M \in GL_d(K)$ s'ecrit comme un produit fini de ces matrices.

Preuve: Si M est inversible elle est ligne equivalente a l'identite ce qui signifie qu'on peut multiplier a gauche M par un produit Π de matrices de transformations elementaires et obtenir Id_d:

$$\Pi.M = \mathrm{Id}_d.$$

On a donc

$$M = \Pi^{-1}$$

est un produit d'inverses de matrices de transformations elementaires et donc un produit de matrices de transformations elementaires. □

9.3.2.1. *Inversion de matrices par la methode de Gauss.* Cette preuve donne une methode systematique pour inverser une matrice: supposons d'pares une suite de transformations elementaires on passe de la matrice inversible M a la matrice identite: il existe des matrices de transformations elementaires

$$E_1, E_2, \cdots, E_n$$

telles que

$$E_n.\cdots E_2.E_1.M = \mathrm{Id}$$

alors

$$M^{-1} = E_n.\cdots E_2.E_1.$$

En pratique on ecrit l'une a cote de l'autre la matrice M et la matrice Id_d, ensuite

- 1. On effectue la premiere transformation elementaire permettant d'echelonner M et on fait la meme transformation sur la matrice Id_d, ce qui revient a multiplier M et Id_d a gauche par E_1 (ce qui donne $E_1.M$ et E_1)
- 2. On effectue la deuxieme transformation elementaire sur $E_1.M$ et on fait la meme transformation sur la matrice $E_1.Id_d$, ce qui revient a multiplier les deux matrices a gauche par E_2 (ce qui donne $E_2.E_1.M$ et $E_2.E_1$),

– $\vdots$
– n. On effectue la n-ieme transformation elementaire sur $E_{n-1}.\cdots.E_1.M$ et on fait la meme transformation sur la matrice $E_{n-1}.\cdots.E_1.Id_d$, ce qui revient a multiplier les deux matrices a gauche par E_n (ce qui donne $E_n.\cdots E_2.E_1.M = \mathrm{Id}_d$ et $E_n.\cdots E_2.E_1 = M^{-1}$).

9.3.3. Base extraite d'une famille generatrice. Soit

$$\mathscr{G} = \{w_1, \cdots, w_l\} \subset K^d$$

une famille de vecteurs (lignes) et

$$W = \langle \mathscr{G} \rangle$$

l'espace vectoriel qu'ils engendrent. On cherche une base de W.

PROPOSITION 9.9 (Description matricielle d'une base d'un SEV). *Soit $M \in M_{l\times d}(K)$ la matrice dont les l lignes sont formees des vecteurs lignes w_i, $i \leqslant l$. Soit R la matrice echelonee reduite associee a M et*

$$w'_i = \mathrm{Lig}_i(R),\ i \leqslant l$$

les lignes de R alors si R possede r echelons on a

$$\dim W = r$$

et les r premieres lignes

$$\mathscr{B}_W = \{w'_i,\ i \leqslant r\}$$

forment une base de W (et les $l - r$ autres lignes sont nulles).

Preuve: En effet, les $\{w'_i,\ i \leqslant r\}$ forment une famille libre et par la proposition 9.4

$$\langle \{w'_i,\ i \leqslant r\} \rangle \subset \langle \{w_i,\ i \leqslant l\} \rangle = W$$

et comme les w'_i sont nuls pour $i > r$, on a

$$W = \langle \{w_i,\ i \leqslant l\} \rangle \subset \langle \{w'_i,\ i \leqslant l\} \rangle = \langle \{w'_i,\ i \leqslant r\} \rangle.$$

□

REMARQUE 9.3.1. On peut alors completer $\mathscr{B}_W$ en un base $\mathscr{B}$ de K^d en prenant

$$\mathscr{B} = \mathscr{B}_W \sqcup \{\mathbf{e}^0_j,\ j \text{ n'est pas un echelon de } R\}$$

9.3.4. Resolution de systemes lineaires. Soit $\varphi : V \mapsto W$ une application lineaire entre espaces vectoriel de dimension finies ($d = \dim V$ et $d' = \dim W$). Le probleme qu'on se pose est le suivant:

Etant donne $w \in W$, trouver les $v \in V$ tels que

$$\varphi(v) = w. \tag{9.3.1}$$

Autrement dit, il s'agit de determiner si w appartient a $\varphi(V)$, l'image de V par φ et de calculer l'ensemble des antecedents de w

$$\mathrm{Sol}_\varphi(w) = \varphi^{-1}(\{w\}) = \{v \in V,\ \varphi(v) = w\}.$$

L'equation (9.3.1) s'appelle un *systeme lineaire*.

Rappelons (dans le cadre plus general des groupes quelconques) la structure generale de l'ensemble des solutions de cette equation.

THÉORÈME 9.3 (Resolution d'equations dans les groupes). *Soit $\varphi : G \mapsto H$ un morphisme de groupes alors pour tout $h \in H$, on pose*

$$\mathrm{Sol}_\varphi(h) = \varphi^{-1}(\{h\}) = \{g \in G,\ \varphi(g) = h\} \subset G$$

la preimage de h par φ. En particulier $\mathrm{Sol}_\varphi(e_H) = \ker\varphi$. Alors $\mathrm{Sol}_\varphi(h)$ est

– *soit l'ensemble vide (ssi $h \notin \varphi(G)$),*

– *soit il existe* $g_0 \in \mathrm{Sol}_\varphi(h)$ *(ce qui equivaut a dire que* $h \in \varphi(G)$*) et*

$$\mathrm{Sol}_\varphi(h) = g_0.\mathrm{Sol}_\varphi(e_H) = g_0.\ker\varphi = \{g_0.k,\ \varphi(k) = e_H\}.$$

Preuve: Si $\varphi^{-1}(\{h\}) \neq \emptyset$, soit $g_0 \in G$ tel que $\varphi(g_0) = h$. Alors pour tout g tel que $\varphi(g) = h$ on a

$$\varphi(g_0^{-1}.g) = \varphi(g_0)^{-1}.\varphi(g) = h^{-1}.h = e_H$$

et donc $g = g_0.k$ avec $k = g_0^{-1}.g \in \ker\varphi$ ce qui montre que

$$\mathrm{Sol}_\varphi(h) \subset g_0.\mathrm{Sol}_\varphi(e_H).$$

Reciproquement pour $k \in \ker\varphi$

$$\varphi(g_0.k) = \varphi(g_0).\varphi(k) = \varphi(g_0) = h$$

ce qui montre

$$\mathrm{Sol}_\varphi(h) \supset g_0.\mathrm{Sol}_\varphi(e_H).$$

□

On applique ce resultat general au cas des groupes additifs $G = V, H = W$ et $\varphi : V \mapsto W$ et on a donc que pour $w \in W$, $\mathrm{Sol}_\varphi(w)$ est

– soit l'ensemble vide (ssi $w \notin \varphi(V)$),
– soit il existe $v^0 \in \mathrm{Sol}_\varphi(w)$ (ce qui equivaut a dire que $w \in \varphi(V)$) et

$$\mathrm{Sol}_\varphi(w) = v^0 + \mathrm{Sol}_\varphi(\mathbf{0}_d) = v^0 + \ker\varphi = \{v_0 + k,\ k \in \ker\varphi\}.$$

On va maintenant resoudre ce systeme "abstrait" en le transformant en un probleme concret. Pour cela on se donne des bases

$$\mathscr{B} \subset V,\ \mathscr{B}' \subset W$$

et

$$M = (m_{ij})_{ij} = \mathrm{mat}_{\mathscr{B}'\mathscr{B}}(\varphi)$$

la matrice de φ dans ces bases. Soient $(v_j)_{j\leqslant d}$ les coordonnes d'un vecteur $v \in V$ et $(w_i)i \leqslant d'$ celles de $w \in W$. L'equation (9.3.1) est equivalente au systeme lineaire a d' equations et d inconnues dans K, $v_j,\ j \leqslant d$

$$\begin{aligned} m_{11}.v_1 + \cdots + m_{1d}.v_d &= w_1 \\ m_{21}.v_1 + \cdots + m_{2l}.v_d &= w_2 \\ &\vdots \\ m_{d'1}.v_1 + \cdots + m_{d'd}.v_d &= w_{d'} \end{aligned}$$

ou a l'equation matricielle

$$\begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \vdots\ \vdots & \vdots \\ m_{d1} & m_{12} & \cdots & m_{d'd} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_{d'} \end{pmatrix} \tag{9.3.2}$$

On cherche alors une condition necessaire et suffisante sur les $(w_i)_{i\leqslant d'}$ pour que ces equations admettent des solutions $(v_j)_{j\leqslant d}$.

Remarque 9.3.2. En particulier si $w = \mathbf{0}_{d'}$ est le vecteur nul, les solutions nous donnerons les coordonnees des elements du noyau $\ker\varphi$.

Définition 9.6. *L'equation lineaire* (9.3.2) *pour un vecteur colonne* $\mathrm{Col}(w)$ *general s'appelle equation (ou systeme) lineaire avec second membre (ou non-homogene).*

L'equation lineaire (9.3.2) *pour le vecteur colonne nul* $\mathrm{Col}(\mathbf{0}_{d'})$ *general s'appelle equation (ou systeme) lineaire sans second membre ou homogene.*

Pour trouver ces conditions, on applique une suite de transformations elementaires de part et d'autre de l'egalite (9.3.2) de maniere a echelonner-reduire la matrice de gauche. On multiplie les deux termes par un produit $\Pi_n = E_n.\cdots.E_1$ de matrices de transformations elementaires. Ici, on ne fixe pas la valeurs de w mais on les considere comme des *variables*:

$$\Pi_n.\begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \vdots\ \vdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix}.\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \Pi_n.\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_{d'} \end{pmatrix}$$

On obtient alors un produit dont la premiere matrice est reduite

$$\begin{pmatrix} 1 & * & 0 & 0 & * & * \\ 0 & 0 & 1 & 0 & * & * \\ 0 & 0 & 0 & 1 & * & * \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} \vdots \\ w'_r \\ 0 \\ 0 \end{pmatrix} = \Pi_n.\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_{d'} \end{pmatrix} = \begin{pmatrix} \vdots \\ w'_r \\ w'_{r+1} \\ \vdots \end{pmatrix}.$$

ou les $w'_i,\ i \leqslant d'$ sont des combinaisons lineaires des $w_i,\ i \leqslant d'$. Notons egalement que comme les lignes d'indice $\geqslant r+1$ sont nulles le premier produit fournit un vecteur colonne dont les coordonnes d'indice $\geqslant r+1$ sont nulles.

Définition 9.7. *Les inconnues v_{j_i} pour $j_i,\ i \leqslant r$ etant un echelon sont appelles inconnues principales du systeme. Les inconnues v_j pour $j \leqslant d$ qui n'est pas un echelon sont appelles inconnues libres du systeme.*

On en retire plusieurs informations:

(1) Le nombre d'echelons est egal au rang de M qui est le rang de φ.
(2) Les egalites obtenues
$$w'_{r+1} = \cdots = w'_{d'} = 0$$
forment un systeme de $d' - r$ equations qui sont les equations cartesienne l'image $\varphi(V)$:
$$\varphi(V) = \{(w_i)_{i\leqslant d},\ w'_k = 0,\ k \geqslant r+1\} \subset W.$$
(3) Si $w \in W$ ne satisfait pas les equations ci-dessus alors $w \notin \varphi(V)$ et l'ensemble des solutions est vide.
(4) Si $w \in W$ satisfait les equations ci-dessus alors $w \in \varphi(V)$ et l'ensemble des solutions est non-vide. Il est obtenu en fixant de maniere arbitraire les inconnues libres v_j (j pas un echelon) et en fixant de maniere unique la valeur des inconnues principales $v_{j_i}, i \leqslant r$ en fonction de w'_i et des inconnues libresprealablement fixees v_j de sorte que pour $i \leqslant r$, l'equation
$$v_{j_i} + \cdots = w'_i$$
soit satisfaite. Par exemple on peut fixer $v^0_j = 0$ si j n'est pas un echelon et poser $v^0_{j_i} = w'_i$ pour $i \leqslant r$.
(5) Alternativement on obtient les solutions en calculant une solution particuliere v^0 comme ci-dessus et en lui ajoutant un vecteur arbitraire du noyau $\ker\varphi$. Une base du noyau (qui est de dimension $d-r$) est obtenue en fixant une des inconnue libre egale a 1, et toutes les autres inconnues libres egales a 0 et en fixant (de maniere unique) les inconnues principales de sorte que le systeme d'equations
$$\begin{pmatrix} 1 & * & 0 & 0 & * & * \\ 0 & 0 & 1 & 0 & * & * \\ 0 & 0 & 0 & 1 & * & * \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

soit satisfait.

CHAPITRE 10

Determinants

That object was to present the subject as a continuous chain of argument, separated from all accessories of explanation or illustration, a form which I venture to think better suited for a treatise on exact science than the semi -colloquial semi-logical form often adopted by Mathematical writers.

Lewis Carroll (1867)

10.1. Formes multilineaires

DÉFINITION 10.1. *Soit V un K-espace vectoriel et $n \geqslant 1$ un entier. Une forme multilineaire en n variables sur V est une application*

$$\Lambda : \begin{array}{ccc} V^n & \mapsto & K \\ (v_1, \cdots, v_n) & \mapsto & \Lambda(v_1, \cdots, v_n) \end{array}$$

telle que pour tout $i = 1, \cdots, n$ et tout choix de $n-1$ vecteurs $v_j \in V$, $j \neq i$, l'application "restriction a la i-ieme composante"

$$v_i \in V \mapsto \Lambda(v_1, \cdots, v_i, \cdots, v_n) \in K$$

est lineaire:

$$\Lambda(v_1, \cdots, \lambda.v_i + v_i', \cdots, v_n) = \lambda.\Lambda(v_1, \cdots, v_i, \cdots, v_n) + \Lambda(v_1, \cdots, v_i', \cdots, v_n).$$

L'ensemble des formes multilineaires en n variables sur V est note

$$\mathrm{Mult}^{(n)}(V, K) \text{ ou bien } (V^*)^{\otimes n} (\text{notation "produit tensoriel"}).$$

REMARQUE 10.1.1. Si $n = 1$ c'est la definition usuelle d'une forme lineaire. Si $n = 2$ on parle de forme bi-lineaire, $n = 3$ tri-lineaire, etc...

REMARQUE 10.1.2. Attention, V^n est muni d'une structure naturelle de K-ev en posant

$$\lambda.(v_1, \cdots, v_n) + (v_1', \cdots, v_n') = (\lambda.v_1 + v_1', \cdots, \lambda.v_n + v_n')$$

mais une application $\Lambda : V^n \mapsto K$ qui est lineaire pour cette structure (une forme lineaire sur V^n) n'est pas forcement multilineaire.

Par exemple prenons $V = K$, $n = 2$ et considerons la forme lineaire

$$\Sigma : (x_1, x_2) \in K^s \mapsto x_1 + x_2 \in K.$$

Fixons x_2 et calculons

$$\Sigma(\lambda x_1 + x_1', x_2) = \lambda x_1 + x_1' + x_2$$

et si la forme etait lineaire en la variable x_1 on aurait

$$\Sigma(\lambda x_1 + x_1', x_2) = \lambda\Sigma(x_1, x_2) + \Sigma(x_1', x_2) = \lambda.x_1 + x_2 + x_1' + x_2$$

qui ne vaut pas $\lambda x_1 + x_1' + x_2$ (sauf si $x_2 = 0_K$).

Notons egalement que si Λ est multilineaire alors pour tout $i \leqslant n$ pour tout choix de $n-1$ vecteurs $v_j \in V$ $j \neq i$, l'application

$$v_i \mapsto \Lambda(v_1, \cdots, v_i, \cdots, v_d)$$

est une forme lineaire et sa valeur en 0_V est nulle

$$\Lambda(v_1, \cdots, 0_V, \cdots, v_d) = 0_K$$

(le 0_V est place "en position i"). C'est n'est pas forcement le cas d'une forme lineaire sur l'espace vectoriel V^n (sauf si $(v_1, \cdots, 0_V, \cdots, v_d)$ est dans le noyau).

REMARQUE 10.1.3. Quelques exemple en base dimension:

- Si $V = K$, $n = 2$ l'application

$$\prod_2 : \begin{array}{ccc} K^2 & \mapsto & K \\ (x_1, x_2) & \mapsto & \prod_2(x_1, x_2) = x_1.x_2 \end{array}$$

  est multilineaire. Plus generalement

$$\prod_n : \begin{array}{ccc} K^n & \mapsto & K \\ (x_1, \cdots, x_n) & \mapsto & \prod_n(x_1, \cdots, x_n) = x_1 \times \cdots \times x_n \end{array}$$

  est multilineaire.
- Soit $V = K^2$ et $n = 2$, on a l'application "produit scalaire"

$$\bullet.\bullet : \begin{array}{ccc} K^2 \times K^2 & \mapsto & K \\ ((x_1, y_1), (x_2, y_2)) & \mapsto & (x_1, y_1).(x_2, y_2) = x_1.x_2 + y_1.y_2 \end{array}$$

  qui est bilineaire.
- Soit $V = K^2$ et $n = 2$, on a l'application "produit alterne"

$$\bullet \wedge \bullet : \begin{array}{ccc} K^2 \times K^2 & \mapsto & K \\ ((x_1, y_1), (x_2, y_2)) & \mapsto & (x_1, y_1) \wedge (x_2, y_2) = x_1.y_2 - y_1.x_2 \end{array}$$

  qui est bilineaire.

REMARQUE 10.1.4. Soient $\lambda_1, \cdots, \lambda_n, \mu_1, \cdots, \mu_n \in K$ et Λ multilineaire alors

$$\Lambda(\lambda_1.v_1 + \mu_1.v'_1, \cdots, \lambda_n.v_n + \mu_n.v'_n)$$

est la somme de 2^n termes (2^n est le nombre de decompositions de l'ensemble $\{1, \cdots, n\}$ en deux sous-ensembles disjoints):

$$\sum_{I \sqcup J = \{1, \cdots, n\}} (\prod_{i \in I} \lambda_i).(\prod_{j \in J} \mu_j) \Lambda(w_{IJ,1}, \cdots, w_{IJ,n})$$

avec

$$w_{IJ,i} = \begin{cases} v_i & \text{si } i \in I \\ v'_i & \text{si } i \in J \end{cases}.$$

En particulier

$$\Lambda(\lambda_1.v_1, \cdots, \lambda_n.v_n) = \lambda_1. \cdots .\lambda_n.\Lambda(v_1, \cdots, v_n)$$

et

$$\Lambda(\lambda.v_1, \cdots, \lambda.v_n) = \lambda^n.\Lambda(v_1, \cdots, v_n).$$

EXEMPLE 10.1.1. Soient $\ell_1, \cdots, \ell_n : V \mapsto K$ des formes lineaires, alors l'application

$$\ell_1 \otimes \cdots \otimes \ell_n : V^n \mapsto K$$

definie par

$$\ell_1 \otimes \cdots \otimes \ell_n(v_1, \cdots, v_n) = \prod_{i=1}^{n} \ell_i(v_i) = \ell_1(v_1). \cdots .\ell_n(v_n)$$

est une forme multilineaire en n variables. C'est en fait l'exemple principal. En effet soit $i \in [1,d]$ fixons des vecteurs v_j pour chaque $j \in [1,d]$ different de im, l'application

$$v \mapsto \ell_1(v_1).\cdots.\ell_i(v).\cdots.\ell_n(v_n) = (\prod_{j\neq i}\ell_j(v_j))\ell_i(v)$$

est un multiple scalaire (de facteur $(\prod_{j\neq i}\ell_j(v_j))$) de la forme lineaire $v \mapsto \ell_i(v)$ et est donc une forme lineaire en v.

PROPOSITION 10.1. *L'ensemble* $\mathrm{Mult}^{(n)}(V,K) = (V^*)^{\otimes n}$ *des formes multilineaires en n variables est un K-espace vectoriel quand on le muni de l'addition et de la multiplication par les scalaires usuelle pour les fonctions a valeurs dans K:* $\forall \Lambda, \Xi \in (V^*)^{\otimes n}$

$$(\lambda\Lambda + \Xi)(v_1,\cdots,v_n) = \lambda\Lambda(v_1,\cdots,v_n) + \Xi(v_1,\cdots,v_n).$$

Preuve: Exercice. □

THÉORÈME 10.1 (Dimension et base de l'espace des formes multilineaires). *Soit* $d = \dim V$, $\mathscr{B} = \{\mathbf{e}_1,\cdots,\mathbf{e}_d\} \subset V$ *une base et* $\mathscr{B}^* = \{\mathbf{e}_1^*,\cdots,\mathbf{e}_d^*\} \subset V^*$ *la base duale. Alors* $V^{*\otimes n}$ *est de dimension finie egale a* d^n*; une base de* $V^{*\otimes n}$ *est donnee par l'ensemble des formes multilineaires de la forme*

$$\mathbf{e}_{j_1}^* \otimes \cdots \otimes \mathbf{e}_{j_n}^*, \text{ quand } j_1,\cdots,j_n \text{ parcourent } \{1,\cdots,d\}.$$

On note cette base

$$(\mathscr{B}^*)^{\otimes n} = \{\mathbf{e}_{j_1}^* \otimes \cdots \otimes \mathbf{e}_{j_n}^*,\ (j_1,\cdots,j_n) \in [1,d]^n\}.$$

Pour tout $\Lambda \in (V^*)^{\otimes n}$ *on a la decomposition*

$$\Lambda = \sum_{j_1,\cdots,j_n\leqslant d}\cdots\sum\Lambda(\mathbf{e}_{j_1},\cdots\mathbf{e}_{j_n})\mathbf{e}_{j_1}^* \otimes \cdots \otimes \mathbf{e}_{j_n}^*$$

Preuve: Avant de traiter le cas general on commence par $n = 2$ (les formes bilineaires). On veut donc montrer que cet espace est de dimension d^2.

Soit $\Lambda : V \times V \mapsto K$ une forme bilineaire, et $v_1, v_2 \in V$ 2 vecteurs. On ecrit pour $i = 1, 2$

$$v_i = \sum_{j=1}^d x_{ij}\mathbf{e}_j = \sum_{j=1}^d \mathbf{e}_j^*(v_i)\mathbf{e}_j$$

et alors on a

$$\Lambda(v_1,v_2) = \Lambda(\sum_{j_1=1}^d x_{1j_1}\mathbf{e}_{j_1}, v_2).$$

On a par linearite en la premiere variable

$$\Lambda(v_1,v_2) = \sum_{j_1\leqslant d} x_{1j_1}\Lambda(\mathbf{e}_{j_1},v_2) = \sum_{j_1\leqslant d} x_{1j_1}\Lambda(\mathbf{e}_{j_1},\sum_{j_2=1}^d x_{2j_2}\mathbf{e}_{j_2})$$

et par linearite en la deuxieme variable on a

$$\Lambda(\mathbf{e}_{j_1},\sum_{j_2=1}^d x_{2j_2}\mathbf{e}_{j_2}) = \sum_{j_2=1}^d x_{2j_2}\Lambda(\mathbf{e}_{j_1},\mathbf{e}_{j_2})$$

et donc

$$\Lambda(v_1,v_2) = \sum_{j_1,j_2\leqslant d}\sum\Lambda(\mathbf{e}_{j_1},\mathbf{e}_{j_2})x_{1j_1}x_{2j_2} = \sum_{j_1,j_2\leqslant d}\sum\Lambda(\mathbf{e}_{j_1},\mathbf{e}_{j_2})\mathbf{e}_{j_1}^*(v_1).\mathbf{e}_{j_2}^*(v_2)$$

$$\sum_{j_1,j_2\leqslant d}\sum\Lambda(\mathbf{e}_{j_1},\mathbf{e}_{j_2})\mathbf{e}_{j_1}^* \otimes \mathbf{e}_{j_2}^*(v_1,v_2).$$

Ainsi

$$\Lambda = \sum_{j_1,j_2\leqslant d}\sum \Lambda(\mathbf{e}_{j_1},\mathbf{e}_{j_2})\mathbf{e}^*_{j_1}\otimes\mathbf{e}^*_{j_2}.$$

Ainsi la famille des formes multilineaires (de cardinal d^2)

$$\{\mathbf{e}^*_{j_1}\otimes\mathbf{e}^*_{j_2},\ j_1,j_2\in[1,d]\}$$

est une famille generatrice de $\mathrm{Mult}^{(2)}(V,K)$.

Montrons qu'elle est libre: soient d^2 scalaires $\lambda_{j_1,j_2}\in K,\ j_1,j_2\leqslant d$ tels que

$$\sum_{j_1,j_2\leqslant d}\sum \lambda_{j_1,j_2}\mathbf{e}^*_{j_1}\otimes\mathbf{e}^*_{j_2}=\underline{0}$$

et on veut montrer que

$$\forall j_1,\cdots j_2\leqslant d,\ \lambda_{j_1,j_2}=0.$$

Fixons la deuxieme variable egale a $\mathbf{e}_1$: on prend $(v_1,v_2)=(v,\mathbf{e}_1)$ pour $v\in V$; on dispose d'une forme lineaire

$$v\in V\mapsto\Lambda(v,\mathbf{e}_1)=\sum_{j_1,j_2\leqslant d}\sum\lambda_{j_1j_2}\mathbf{e}^*_{j_1}(v)\mathbf{e}^*_{j_2}(\mathbf{e}_1)$$

qui par hypothese est la forme lineaire nulle.

Notons que $\mathbf{e}^*_{j_2}(\mathbf{e}_1)=0$ sauf is $j_2=1$ auquel cas $\mathbf{e}^*_1(\mathbf{e}_1)=1$. Ainsi notre forme lineaire s'ecrit

$$v\in V\mapsto\Lambda(v,\mathbf{e}_1)=\sum_{j_1\leqslant d}\lambda_{j_11}\mathbf{e}^*_{j_1}(v)$$

Comme cette forme lineaire est nulle et que $\{\mathbf{e}^*_{j_1},\ j_1\leqslant d\}$ forme une base de V^* on a

$$\lambda_{j_1,1}=0,\ j_1\in[1,d].$$

Remplacant $\mathbf{e}_1$ par $\mathbf{e}_j$ on obtient que pour tout $j\in[1,d]$,

$$\lambda_{j_1,j}=0,\ j_1\in[1,d]$$

et les $\lambda_{j_1j_2}$ sont tous nuls.

On traite maintenant le cas general ou $n\geqslant 1$ est arbitraire: soit Λ multilineaire en n varaibles, et $v_i\in V,\ j\leqslant n$ n vecteurs. On ecrit

$$v_i=\sum_{j=1}^d x_{ij}\mathbf{e}_j=\sum_{j=1}^d\mathbf{e}^*_j(v_i)\mathbf{e}_j$$

et alors on a

$$\Lambda(v_1,\cdots,v_n)=\Lambda(\sum_{j=1}^d x_{1j}\mathbf{e}_j,\cdots,\sum_{j=1}^d x_{nj}\mathbf{e}_j)$$

$$=\sum_{j_1,\cdots,j_n\leqslant d}\sum\cdots\sum x_{1j_1}.\cdots.x_{nj_n}\Lambda(\mathbf{e}_{j_1},\cdots,\mathbf{e}_{j_n})$$

$$=\sum_{j_1,\cdots,j_n\leqslant d}\sum\cdots\sum\Lambda(\mathbf{e}_{j_1},\cdots,\mathbf{e}_{j_n})\mathbf{e}^*_{j_1}(v_1).\cdots.\mathbf{e}^*_{j_n}(v_n)=\sum_{j_1,\cdots,j_n\leqslant d}\sum\cdots\sum\Lambda(\mathbf{e}_{j_1},\cdots,\mathbf{e}_{j_n})(\bigotimes_{i=1}^n\mathbf{e}^*_{j_i})(v_1,\cdots,v_n).$$

Ainsi

$$\Lambda=\sum_{j_1,\cdots,j_n\leqslant d}\sum\cdots\sum\Lambda(\mathbf{e}_{j_1},\cdots,\mathbf{e}_{j_n})\bigotimes_{i=1}^n\mathbf{e}^*_{j_i}.$$

Ainsi la famille ci-dessus est generatrice.

Montrons qu'elle est libre: supposons que

$$\Lambda = \sum_{j_1,\cdots,j_n\leqslant d} \cdots \sum \lambda_{j_1,\cdots,j_n} \bigotimes_{i=1}^{n} \mathbf{e}_{j_i}^* = \underline{0}$$

et on veut montrer que

$$\forall j_1, \cdots j_n \leqslant d,\ \lambda_{j_1,\cdots,j_n} = 0.$$

Fixons toutes les variables sauf la premiere: par exemple, on pose $v_2 = \cdots = v_n = \mathbf{e}_1$; on dispose alors d'une forme lineaire

$$v \mapsto \sum_{j_1,\cdots,j_n\leqslant d} \cdots \sum \lambda_{j_1,\cdots,j_n} \mathbf{e}_{j_1}(v). \bigotimes_{i=2}^{n} \mathbf{e}_{j_i}^*(\mathbf{e}_1)$$

qui par hypothese est nulle.

Notons que pour tout $2 \leqslant i \leqslant n$ $\mathbf{e}_{j_i}(\mathbf{e}_1) = 0$ si $j_i \neq 1$ et si $j_i = 1$ on a $\mathbf{e}_1(\mathbf{e}_1) = 1$. La forme lineaire precedente se reecrit donc

$$v \in V \mapsto \Lambda(v, \mathbf{e}_1, \cdots, \mathbf{e}_1) = \sum_{j_1\leqslant d} \lambda_{j_1,1,\cdots,1} \mathbf{e}_{j_1}^*(v).$$

Cette forme est identiquement nulle par hypothese et comme les $\{\mathbf{e}_{j_1}^*,\ j_1 \leqslant d\}$ forment une base de V^* (la base duale de $\mathscr{B}$), on en deduit que

$$\lambda_{j,1,\cdots,1} = 0,\ j \leqslant d.$$

De meme en fixant $(v_2, \cdots, v_d)$ parmi tous les uplets possibles d'elements de $\mathscr{B}$ on obtient que

$$\forall j_2, \cdots, j_n \leqslant d,\ \forall j \leqslant d,\ \lambda_{j,j_2,\cdots,j_n} = 0.$$

□

10.1.1. Formes symetriques/alternees. A partir d'une forme multilineaire en n variables on peut en obtenir des nouvelles par "permutation" des variables: par exemple soit $i \neq j \leqslant n$ et $\Lambda \in \mathrm{Mult}^{(n)}(V, K)$, on definit alors

$$\Lambda_{|ij} : (v_1, \cdots, v_i, \cdots, v_j, \cdots, v_n) \mapsto \Lambda(v_1, \cdots, v_j, \cdots, v_i, \cdots, v_n).$$

Cette formes est a nouveau multilineaire (le verifier).

Définition 10.2. *Une forme multilineaire*

$$\Lambda : V^n \mapsto K$$

est dite

- *Symetrique si* $\forall i \neq j \leqslant n$

  $$\Lambda(v_1, \cdots, v_i, \cdots, v_j, \cdots, v_n) = \Lambda(v_1, \cdots, v_j, \cdots, v_i, \cdots, v_n).$$

  Autrement dit si sa valeur ne change pas quand on echange deux composantes.
- *Alternee si* $\forall i \neq j \leqslant n$

  $$\Lambda(v_1, \cdots, v_i, \cdots, v_j, \cdots, v_n) = -\Lambda(v_1, \cdots, v_j, \cdots, v_i, \cdots, v_n).$$

  Autrement dit si sa valeur est changee en son opposee si on echange deux composantes distinctes.

L'ensemble des formes multilineaires symetriques en n variables sur V est note

$$\mathrm{Sym}^{(n)}(V; K).$$

L'ensemble des formes multilineaires alternees en n variables sur V est note

$$\mathrm{Alt}^{(n)}(V; K).$$

PROPOSITION 10.2. *Les ensembles* $\mathrm{Sym}^{(n)}(V;K)$ *et* $\mathrm{Alt}^{(n)}(V;K)$ *sont des SEV de l'espace vectoriel* $\mathrm{Mult}^{(n)}(V;K)$.

Preuve: Exercice. □

On va s'interesse particulierement a l'espace des formes alternees.

THÉORÈME 10.2 (Dimension des espaces de formes alternees). *On suppose que* $\mathrm{car}(K) \neq 2$. *Soit* $d = \dim V$. *On a*

$$\dim \mathrm{Alt}^{(n)}(V;K) = \begin{cases} 0 & si\ n > d \\ 1 & si\ n = d \\ C_d^n\ si\ n \leqslant d \end{cases}$$

REMARQUE 10.1.5. Si $\mathrm{car}(K) = 2$ alors $-1_K = 1_K$ et

$$\mathrm{Sym}^{(n)}(V;K) = \mathrm{Alt}^{(n)}(V;K).$$

Preuve: (debut) On va seulement demontrer les cas $n > d$ et $n = d$ (qui est celui qui nous interesse le plus.

Notons que si Λ est alternee alors on a

$$\Lambda(v_1, \cdots, v, \cdots, v, \cdots, v_n) = -\Lambda(v_1, \cdots, v, \cdots, v, \cdots, v_n)$$

et donc

$$2\Lambda(v_1, \cdots, v, \cdots, v, \cdots, v_n) = 0_K$$

et donc (car $2_K \neq 0_K$)

$$\Lambda(v_1, \cdots, v, \cdots, v, \cdots, v_n) = 0_K.$$

Plus generalement si la famille

$$\{v_1, \cdots, v_n\} \subset V$$

est liee alors

$$\Lambda(v_1, \cdots, \cdots, v_n) = 0.$$

En effet si les famille est liee il existe i tel que v_i est combinaison lineaire des autres vecteur: supposons par exemple que ce soit v_n:

$$v_n = x_1.v_1 + \cdots + x_{n-1}.v_{n-1}$$

alors

$$\begin{aligned} \Lambda(v_1, \cdots, \cdots, v_n) &= \Lambda(v_1, \cdots, \cdots, v_{n-1}, x_1.v_1 + \cdots + x_{n-1}.v_{n-1}) \\ &= x_1\Lambda(v_1, \cdots, v_{n-1}, v_1) + \cdots + x_{n-1}\Lambda(v_1, \cdots, v_{n-1}, v_{n-1}) = 0. \end{aligned}$$

car on a toujours deux vecteurs egaux dans chacun des $n-1$ termes de la somme.

En particulier si $n > d$ une famille $\{v_1, \cdots, v_n\}$ de n vecteurs est toujours liee et donc

$$\Lambda(v_1, \cdots, v_n) = 0.$$

Cela montre que pour $n > d$

$$\mathrm{Alt}^{(n)}(V;K) = \{\underline{0}\}.$$

Supposons que $n = d$. Comme Λ est multilineaire

$$\Lambda(v_1, \cdots, v_d) = \sum_{j_1, \cdots, j_d \leqslant d} \cdots \sum x_{1j_1}.\cdots.x_{nj_d}\Lambda(\mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_d})$$

et Λ est completement determinees si on connait les valeurs des

$$\Lambda(\mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_d})$$

pour tout les choix possibles de $j_1, \cdots j_d \in \{1, \cdots, d\}$. Notons que si pour $i \neq i'$ on a $j_i = j_{i'}$ alors

$$\Lambda(\mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_i}, \cdots, \mathbf{e}_{j_{i'}}, \mathbf{e}_{j_d}) = \Lambda(\mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_i}, \cdots, \mathbf{e}_{j_i}, \mathbf{e}_{j_d}) = 0.$$

On peut donc se restreindre aux $j_1, \cdots, j_d \in \{1, \cdots, d\}$ qui dont distincts. Mais cela signifie que

$$i \in \{1, \cdots, d\} \mapsto j_i \in \{1, \cdots, d\}$$

est une permutation σ de $\{1, \cdots, d\}$. On sait que toute permutation de $\{1, \cdots, d\}$ est la composee de transpositions c'est a dire de permutations qui echangent deux indices $i \neq j$ et qui laissent les autres indices fixes. Appliquant cette suite de transpositions on voit que

$$\Lambda(\mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_d}) = \Lambda(\mathbf{e}_{\sigma(1)}, \cdots, \mathbf{e}_{\sigma(d)}) = (\pm 1)^t \Lambda(\mathbf{e}_1, \cdots, \mathbf{e}_d)$$

ou l'exposant t est le nombre de transpositions qui composent σ. On voit donc que Λ est entierement determinee des qu'on connait $\Lambda(\mathbf{e}_1, \cdots, \mathbf{e}_d)$. Cela montre que

$$\dim \mathrm{Alt}^{(d)}(V; K) \leqslant 1.$$

Pour montrer que la dimension vaut exactement 1, on va devoir raffiner la discussion precedente...

10.1.2. Permutation et signature. La transformation

$$\Lambda \mapsto \Lambda_{|ij}$$

est un cas particulier d'une construction plus generale: soit $n \geqslant 1$ et

$$\sigma : i \in \{1, \cdots, n\} \mapsto \sigma(i) \in \{1, \cdots, n\}$$

est une permutation de $\{1, \cdots, n\}$, on definit alors

$$\Lambda_{|\sigma} : (v_1, \cdots, v_i, \cdots, v_n) \mapsto \Lambda(v_{\sigma(1)}, \cdots, v_{\sigma(i)}, \cdots, v_{\sigma(n)}).$$

On verifie facilement que si Λ est multilineaire alors $\Lambda_{|\sigma}$ est encore multilineaire.

Théorème 10.3 (Action par permutation sur les formes multilineaires). *Pour tout $\sigma \in \mathfrak{S}_n$, l'application*

$$\bullet_{|\sigma} : \Lambda \in \mathrm{Mult}^{(n)}(V, K) \mapsto \Lambda_{|\sigma} \in \mathrm{Mult}^{(n)}(V, K)$$

definit un endomorphisme du K-ev $\mathrm{Mult}^{(n)}(V, K)$.

Cet endomorphisme est en fait un automorphisme dont la reciproque est $\bullet_{|\sigma^{-1}}$.

L'application

$$\sigma \in \mathfrak{S}_n \mapsto \bullet_{|\sigma} \in \mathrm{Aut}(\mathrm{Mult}^{(n)}(V, K))$$

verifie

- $\forall \Lambda$, $\Lambda_{|\mathrm{Id}_n} = \Lambda$ *autrement dit* $\bullet_{|\mathrm{Id}_n} = \mathrm{Id}_{\mathrm{Mult}^{(n)}(V,K)}$,
- $\forall \Lambda$, $\forall \sigma, \tau \in \mathfrak{S}_n$, *on a*

$$\Lambda_{|\sigma\circ\tau} = (\Lambda_{|\tau})_{|\sigma}$$

autrement dit

$$\bullet_{|\sigma\circ\tau} = \bullet_{|\sigma} \circ \bullet_{|\tau};$$

Ainsi $\sigma \mapsto \bullet_{|\sigma}$ est un morphisme de groupes de $\mathfrak{S}_n$ vers $\mathrm{Aut}(\mathrm{Mult}^{(n)}(V, K))$.

Preuve: On va montrer que

$$\bullet_{|\sigma\circ\tau} = \bullet_{|\sigma} \circ \bullet_{|\tau}$$

et le reste s'en deduit. On a

$$\Lambda_{|\sigma\circ\tau}(v_1, \cdots, v_d) = \Lambda(v_{\sigma(\tau(1))}, \cdots, v_{\sigma(\tau(n))}).$$

Par ailleurs

$$\bullet_{\sigma}(\bullet_{|\tau}(\Lambda)) = (\Lambda_{|\tau})_{|\sigma}(v_1, \cdots, v_d) = \Lambda_{|\sigma}(v_{\tau(1)}, \cdots, v_{\tau(n)}) = \Lambda_{|\sigma}(V_1, \cdots, V_n)$$

avec

$$V_i = v_{\tau(i)}.$$

On a

$$\Lambda_{|\sigma}(V_1, \cdots, V_n) = \Lambda(V_{\sigma(1)}, \cdots, V_{\sigma(n)}) = \Lambda(v_{\tau(\sigma(1))}, \cdots, v_{\tau(\sigma(n))})$$

□

Par ailleurs on rappelle que le groupe symetrique $\mathfrak{S}_n$ possede un (unique) morphisme non-trivial de $\mathfrak{S}_n$ vers le groupe multiplicatif $(\{\pm 1\}, \times)$ appelle *signature*

$$\begin{array}{rccc} \text{sign}: & \mathfrak{S}_n & \mapsto & \{\pm 1\} \\ & \sigma & \mapsto & \text{sign}(\sigma) \end{array}$$

defini de la maniere suivante: si σ est la composee de t transposition

$$\sigma = \tau_1 \circ \cdots \tau_t$$

alors

$$\text{sign}(\sigma) = (-1)^t.$$

REMARQUE 10.1.6. On rappelle que toute permutation est composee de transpositions (ie. l'ensemble des transpositions engendre $\mathfrak{S}_n$) mais cette decomposition n'est pas unique. En revanche la parite $t \,(\text{mod}\, 2)$ du nombre de ces transpositions est uniquement definit et ainsi

$$\text{sign}(\sigma) = (-1)^t = \begin{cases} 1 & \text{si } t \equiv 0 \,(\text{mod}\, 2) \\ -1 & \text{si } t \equiv 1 \,(\text{mod}\, 2) \end{cases}$$

est bien definie.

THÉORÈME 10.4. *Les formes multilineaires alternees* $\text{Alt}^{(n)}(V; K)$ *(resp. symetriques* $\text{Sym}^{(n)}(V; K)$*) sont exactement les formes multilineaires verifiant*

$$\forall \sigma \in \mathfrak{S}_n, \Lambda_{|\sigma} = \text{sign}(\sigma)\Lambda \ (\textit{resp.}\ \Lambda_{|\sigma} = \Lambda). \tag{10.1.1}$$

Preuve: Il est clair qu'une forme verifiant (10.1.1) est alternee (resp. symetrique) puisque la signature de la transposition τ_{ij} echangeant $i \neq j$ vaut -1. Inversement soit Λ est alternee , pour tout $\sigma \in \mathfrak{S}_n$, si on ecrit $\sigma = \tau_1 \circ \cdots \tau_t$ alors

$$\Lambda_{|\sigma} = \Lambda_{|\tau_t|\tau_{t-1}|\cdots|\tau_1} = \text{sign}(\tau_t)\Lambda_{|\tau_{t-1}|\cdots|\tau_1} = \cdots = \text{sign}(\tau_t).\cdots.\text{sign}(\tau_1)\Lambda = \text{sign}(\sigma)\Lambda$$

puisque sign est un morphisme de groupes. □

10.1.3. Construction d'une forme alternee. On va maintenant construire des formes alternees suivant un principle general de moyenne:

THÉORÈME 10.5 (Processus de symetrisation pour l'action d'un groupe fini). *Soit K un corps, $(G, .)$ un groupe fini, V un K-ev de dimension finie et*

$$\iota : G \mapsto \text{GL}(V)$$

un morphisme de groupe de G vers le groupe des automorphismes de V. Soit

$$\chi : G \mapsto (K^\times, \times)$$

un morphisme de G vers le groupe multiplicatif de K. Soit $v \in V$ alors le vecteur

$$v_\chi := \sum_{h \in G} \chi(h)^{-1}.\iota(h)(v)$$

verifie pour tout $g \in G$

$$\iota(g)(v_\chi) = \chi(g).v_\chi.$$

Preuve: Pour simplifier les notations on ecrira g pour l'automorphisme $\iota(g)$; cela ne prete a a consequence. Comme g est lineaire

$$g(v_\chi) = g(\sum_{h \in G} \chi(h)^{-1}.h(v)) = \sum_{h \in G} \chi(h)^{-1}.g(h(v)) = \sum_{h \in G} \chi(h)^{-1}.(g \circ h)(v)$$

Posons $h' = g.h$ alors quand h parcours G, h' parcourt G, on a donc (changement de variable $h = g^{-1}.h'$)

$$\sum_{h \in G} \chi(h)^{-1}.(g.h)(v) = \sum_{h' \in G} \chi(g^{-1}.h')^{-1}.h'(v) = \chi(g^{-1}) \sum_{h' \in G} \chi(h')^{-1}.h'(v) = \chi(g).v_\chi;$$

en effet comme χ est un morphisme

$$\chi(g^{-1}.h')^{-1} = \chi(g).\chi(h')^{-1}.$$

□

On peut alors construire simplement des formes alternees

COROLLAIRE 10.1. *Soit Λ une forme multilineaire en n variables sur V alors*

$$\Lambda_{\text{sign}} = \sum_{\sigma\in\mathfrak{S}_n} \text{sign}(\sigma)\Lambda_{|\sigma}$$

est alternee.

Preuve: On ce lemme au cas

$$V = \text{Mult}^{(n)}(V;K),\ G = \mathscr{S}_n,\ \iota : \sigma \mapsto \bullet_{|\sigma},\ \chi(\sigma) = \text{sign}(\sigma) = \{\pm 1_K\}$$

(ici on abuse legerement des notations: la signature est a valeurs dans $\{\pm 1\} \in \mathbb{Z}$ et on envoie $\mathbb{Z}$ dans K via $n \mapsto n.1_K$.)

Noter que comme $\text{sign}(\sigma) = \pm 1$, on a

$$\text{sign}(\sigma)^{-1} = \text{sign}(\sigma)$$

et on a donc

$$\Lambda_{\text{sign}} = \sum_{\sigma\in\mathfrak{S}_n} \text{sign}(\sigma)^{-1}\Lambda_{|\sigma} = \sum_{\sigma\in\mathfrak{S}_n} \text{sign}(\sigma)\Lambda_{|\sigma}.$$

□

REMARQUE 10.1.7. On a demontre que si $n > d$, $\text{Alt}^{(n)}(V;K) = \{\underline{0}_K\}$ donc pour tout forme multilineaire Λ en $n > d$ variables

$$\Lambda_{\text{sign}} = \underline{0}_K.$$

Par contre pour $n \leqslant d$ cette construction produit une forme alternee non-nulle.

10.2. Determinants

10.2.1. Determinant relatif a une base.

THÉORÈME 10.6. *L'espace $\text{Alt}^{(d)}(V;K)$ est de dimension 1 exactement et on a*

$$\text{Alt}^{(d)}(V;K) = K.(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}}$$

ou $(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}}$ est la forme alternee en d variables

$$(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}} = \sum_{\sigma\in\mathfrak{S}_d} \text{sign}(\sigma)\mathbf{e}^*_{\sigma(1)} \otimes \cdots \otimes \mathbf{e}^*_{\sigma(d)} \neq 0$$

En d'autres termes, toute forme lineaire alternee Λ en d variables est proportionelle a celle-ci. Plus precisement on a la formule

$$\Lambda = \Lambda(\mathbf{e}_1, \cdots, \mathbf{e}_d).(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}}$$

Preuve: Comme on sait que la dimension de $\text{Alt}^{(d)}(V;K)$ est au plus 1, is on montre que $(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}}$ est non-nulle, on saura que cet espace est de dimension 1 et que $(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}}$ en est une base.

Calculons

$$(\mathbf{e}_1^* \otimes \cdots \otimes \mathbf{e}_d^*)_{\text{sign}}(\mathbf{e}_1, \cdots, \mathbf{e}_d) = \sum_{\sigma\in\mathfrak{S}_d} \text{sign}(\sigma)\mathbf{e}^*_{\sigma(1)} \otimes \cdots \otimes \mathbf{e}^*_{\sigma(d)}(\mathbf{e}_1, \cdots, \mathbf{e}_d)$$

$$= \sum_{\sigma\in\mathfrak{S}_d} \text{sign}(\sigma)\mathbf{e}^*_{\sigma(1)}(\mathbf{e}_1).\cdots.\mathbf{e}^*_{\sigma(d)}(\mathbf{e}_d).$$

Mais

$$\mathbf{e}_i^*(\mathbf{e}_j) = \delta_{i=j}$$

donc la seulle possibilite pour que le produit

$$\mathbf{e}^*_{\sigma(1)}(\mathbf{e}_1)\otimes\cdots\otimes\mathbf{e}^*_{\sigma(d)}(\mathbf{e}_d)$$

soit non-nul est que

$$\sigma(1)=1,\cdots,\sigma(d)=d$$

autrement dit que σ est l'identite. ainsi dans cette somme de $d!$ termes un peu est non nul et

$$(\mathbf{e}^*_1\otimes\cdots\otimes\mathbf{e}^*_d)_{\mathrm{sign}}(\mathbf{e}_1,\cdots,\mathbf{e}_d)=\mathrm{sign}(\mathrm{Id}_n).1=1.$$

Soit $\Lambda\in\mathrm{Alt}^{(d)}(V;K)$ une autre forme alternee. On sait que

$$\Lambda=\lambda.(\mathbf{e}^*_1\otimes\cdots\otimes\mathbf{e}^*_d)_{\mathrm{sign}}$$

avec $\lambda\in K$. Pour calculer λ on evalue en $(\mathbf{e}_1,\cdots,\mathbf{e}_d)$:

$$\Lambda(\mathbf{e}_1,\cdots,\mathbf{e}_d)=\lambda.(\mathbf{e}^*_1\otimes\cdots\otimes\mathbf{e}^*_d)_{\mathrm{sign}}(\mathbf{e}_1,\cdots,\mathbf{e}_d)=\lambda.1=\lambda.$$

□

DÉFINITION 10.3. *La forme alternee* $(\mathbf{e}^*_1\otimes\cdots\otimes\mathbf{e}^*_d)_{\mathrm{sign}}$ *est appellee le determinant de* V *relatif a la base* $\mathscr{B}=\{\mathbf{e}_1,\cdots,\mathbf{e}_d\}$ *et est note* $\det_{\mathscr{B}}$. *C'est unique forme lineaire alternee en* d *variables verifiant*

$$\Lambda(\mathbf{e}_1,\cdots,\mathbf{e}_d)=1.$$

10.2.1.1. *Expression explicite de* $\det_{\mathscr{B}}$. Soient $v_1,\cdots,v_d$ des vecteurs et

$$(x_{ij})_{j\leqslant d}$$

les coordonnees de v_i dans la base $\mathscr{B}$:

$$v_i=\sum_{j=1}^d x_{ij}\mathbf{e}_j.$$

THÉORÈME 10.7 (Formule combinatoire pour le determinant). *On a la formule suivante*

$$\det_{\mathscr{B}}(v_1,\cdots,v_d)=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)\prod_{i=1}^d x_{i\sigma(i)}=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)x_{1\sigma(1)}.\cdots.x_{d\sigma(d)}. \tag{10.2.1}$$

Preuve: On a

$$\begin{aligned}\det_{\mathscr{B}}(v_1,\cdots,v_d)&=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)\mathbf{e}^*_{\sigma(1)}\otimes\cdots\otimes\mathbf{e}^*_{\sigma(d)}(v_1,\cdots,v_d)\\&=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)\mathbf{e}^*_{\sigma(1)}(v_1).\cdots.\mathbf{e}^*_{\sigma(d)}(v_d)\end{aligned}$$

On a

$$\mathbf{e}^*_{\sigma(i)}(v_i)=x_{i\sigma(i)}$$

(puisque $\mathbf{e}^*_{\sigma(i)}$ calcule la $\sigma(i)$-ieme coordonnee d'un vecteur). Ainsi

$$\det_{\mathscr{B}}(v_1,\cdots,v_d)=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)x_{1\sigma(1)}.\cdots.x_{d\sigma(d)}.$$

□

PROPOSITION 10.3. *On a egalement la formule symetrique suivante:*

$$\det_{\mathscr{B}}(v_1,\cdots,v_d)=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)\prod_{j=1}^d x_{\sigma(j)j}=\sum_{\sigma\in\mathfrak{S}_d}\mathrm{sign}(\sigma)x_{\sigma(1)1}.\cdots.x_{\sigma(d)d}. \tag{10.2.2}$$

Preuve: Ecrivons $j = \sigma(i)$, on a alors $i = \sigma^{-1}(j)$ et quand i parcours $\{1, \cdots, d\}$, j parcours egalement $\{1, \cdots, d\}$. On a donc

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} \operatorname{sign}(\sigma) \prod_{i=1}^{d} x_{i\sigma(i)} = \sum_{\sigma \in \mathfrak{S}_d} \operatorname{sign}(\sigma) \prod_{j=1}^{d} x_{\sigma^{-1}(j)j}.$$

On fait le changement de variable $\sigma \leftrightarrows \sigma^{-1}$ et la somme s'ecrit

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} \operatorname{sign}(\sigma^{-1}) \prod_{j=1}^{d} x_{\sigma(j)j}$$

et comme

$$\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)^{-1} = \operatorname{sign}(\sigma)$$

car $\operatorname{sign}(\sigma) = \pm 1$ on obtient

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} \operatorname{sign}(\sigma) \prod_{j=1}^{d} x_{\sigma(j)j}.$$

□

Remarque 10.2.1. La formule (10.2.1) (ou (10.2.2)) aurait pu etre prise comme definissant le determinant de d vecteurs dans un espace de dimension d sans parle de formes multilineaires alternees et c'est ce qu'on trouve dans de nombreux cours d'algebre lineaires de base. Cependant une telle formule n'est pas vraiment motivee si on n'a pas commencer par introduire la notion de formes multilineaires et le processus de symetrisation.

10.2.2. Determinant d'un endomorphisme. Soit $\varphi : V \mapsto V$ un endomorphisme. A toute forme multilineaire Λ (en n variables) on associe une nouvelle forme (inspire de la construction de l'application adjointe pour les formes lineaires) en posant

$$\varphi^*(\Lambda)(v_1, \cdots, v_n) := \Lambda(\varphi(v_1), \cdots, \varphi(v_n)).$$

Remarque 10.2.2. Cette notation $\varphi^*(\Lambda)$ est analogue avec la notation pour l'application lineaire duale dans le cas des formes lineaires (ie. les formes multilineaires en une variable). Il faut cependant remarquer que $\varphi^*(\Lambda)$ est la composee $\Lambda \circ \varphi^{\Delta}$ ou $\varphi^{\Delta} : V^n \mapsto V^n$ est l'application

$$\varphi^{\Delta} : (v_1, \cdots, v_n) \mapsto (\varphi(v_1), \cdots, \varphi(v_n)).$$

On verifie facilement que si Λ est alternee ou symetrique $\varphi^*(\Lambda)$ est alternee ou symetrique. En particulier si $n = d$, $\varphi^*(\det_{\mathscr{B}})$ est proportionel a $\det_{\mathscr{B}}$. Le facteur de proportionalite s'appelle le determinant de φ.

Définition 10.4. *Le determinant de φ, $\det \varphi \in K$ est le scalaire verifiant*

$$\varphi^*(\det_{\mathscr{B}}) = \det(\varphi) \det_{\mathscr{B}}.$$

Théorème 10.8 (Proprietes fonctionelles du determinant). *Soit $\varphi : V \mapsto V$ un endomorphisme. Pour tout $\Lambda \in \operatorname{Alt}^{(d)}(V; K)$, on a*

$$\varphi^*(\Lambda) = \det(\varphi)\Lambda.$$

En particulier $\det(\varphi)$ ne depend pas du choix de la base $\mathscr{B}$.

L'application $\det : \operatorname{End}(V) \mapsto K$ a les proprietes suivantes

(1) Homogeneite: soit $\lambda \in K$ alors

$$\det(\lambda.\varphi) = \lambda^d . \det(\varphi).$$

(2) Multiplicativite: on a

$$\det(\psi \circ \varphi) = \det(\psi) \det(\varphi) = \det(\varphi) \det(\psi) = \det(\varphi \circ \psi).$$

(3) Critere d'inversibilite: on a

$$\det(\varphi) \neq 0 \Longleftrightarrow \varphi \in \mathrm{GL}(V).$$

(4) Morphisme: L'application

$$\det : \mathrm{GL}(V) \mapsto K^{\times}$$

est un morphisme de groupes. En particulier $\det(\mathrm{Id}_V) = 1$.

Preuve: Soit $\det(\varphi)$ tel que

$$\varphi^*(\det_{\mathscr{B}}) = \det(\varphi)\det_{\mathscr{B}}.$$

soit Λ une forme alternee quelconque, alors

$$\Lambda = \lambda.\det_{\mathscr{B}},\ \lambda \in K$$

et

$$\varphi^*(\Lambda) = \varphi^*(\lambda.\det_{\mathscr{B}}) = (\lambda.\det_{\mathscr{B}}) \circ \varphi = \lambda.(\det_{\mathscr{B}} \circ \varphi) = \lambda.\varphi^*(\det_{\mathscr{B}}) = \lambda.\det(\varphi)\det_{\mathscr{B}} = \det(\varphi)\Lambda.$$

– Homogeneite: on calcule

$$(\lambda.\varphi)^*(\Lambda)(v_1, \cdots, v_d) = \Lambda(\lambda.\varphi(v_1), \cdots, \lambda.\varphi(v_d)) = \lambda^d\Lambda(\varphi(v_1), \cdots, \varphi(v_d)) = \lambda^d\varphi^*(\Lambda)(v_1, \cdots, v_d)$$

car Λ est multilineaire en d variables. Ainsi

$$(\lambda.\varphi)^*(\Lambda) = \det(\lambda\varphi)\Lambda = \lambda^d\varphi^*(\Lambda) = \lambda^d \det(\varphi)\Lambda.$$

– *Multiplicativite*: Soient $\varphi, \psi \in \mathrm{End}(V)$, on a

$$(\psi \circ \varphi)^*\Lambda = \Lambda(\psi \circ \varphi) = \varphi^*(\psi^*\Lambda) = \varphi^* \circ \psi^*(\Lambda).$$

Prenant $\Lambda = \det_{\mathscr{B}}$ on obtient que

$$\det(\psi \circ \varphi)\det_{\mathscr{B}} = \det(\varphi)\psi^*(\det_{\mathscr{B}}) = \det(\varphi)\det(\psi)\det_{\mathscr{B}}.$$

Ainsi

$$\det(\psi \circ \varphi) = \det(\psi)\det(\varphi)$$

car le corps est commutatif. Si $\psi = \mathrm{Id}_V$, on a a bien sur

$$\det(\mathrm{Id}_V) = 1.$$

– *Critere d'inversibilite (condition necessaire)* En particulier si φ est inversible, on a

$$1 = \det(\mathrm{Id}_V) = \det(\varphi^{-1} \circ \varphi) = \det(\varphi^{-1})\det(\varphi)$$

ce qui implique que $\det(\varphi^{-1}), \det(\varphi)$ sont non-nuls et inverse l'un de l'autre.

– *Morphisme*: On a donc montre que

$$\det : \mathrm{GL}(V) \mapsto K^{\times}$$

etait un morphisme de groupes.

– *Critere d'inversibilite (condition suffisante)* Soit $\varphi \in \mathrm{End}(V) - \mathrm{GL}(V)$ (qui n'est pas inversible) alors

$$\{\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)\}$$

n'est pas une base et est donc liee. En particulier

$$\det_{\mathscr{B}}(\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)) = 0$$

mais

$$\det_{\mathscr{B}}(\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)) = \varphi^*(\det_{\mathscr{B}})(\mathbf{e}_1, \cdots, \mathbf{e}_d) = \det(\varphi)\det_{\mathscr{B}}(\mathbf{e}_1, \cdots, \mathbf{e}_d) = \det(\varphi).$$

□

DÉFINITION 10.5. *Le noyau du morphisme* $\det : \mathrm{GL}(V) \mapsto K^\times$ *est appelle "groupe special lineaire de* V*" et on le note*

$$\mathrm{SL}(V) = \ker \det = \{\varphi \in \mathrm{GL}(V),\ \det \varphi = 1\}.$$

C'est un sous-groupe distingue de $\mathrm{GL}(V)$ *(car c'est un noyau).*

10.2.3. Determinant d'une matrice.

DÉFINITION 10.6. *Soit* $M \in M_d(K)$ *une matrice carree avec* $M = (m_{ij})_{ij\leqslant d}$*. Le determinant* $\det(M)$ *de* M *est (de maniere equivalente):*

(1) Le scalaire

$$\det M = \det \varphi$$

ou $\varphi : K^d \mapsto K^d$ *est l'application lineaire sur* K^d *dont la matrice dans la base canonique*

$$\mathrm{mat}_{\mathscr{B}^0}(\varphi) = M.$$

(2) Le determinant relatif a la base canonique des vecteurs colonnes de M *dans l'espace des vecteurs colonnes* $\mathrm{Col}_d(K)$*:*

$$\det(M) = \det_{\mathscr{B}^0}(\mathrm{Col}_1(M), \cdots, \mathrm{Col}_d(M))$$

(3) Le determinant relatif a la base canonique des vecteurs lignes de M *dans l'espace des vecteurs lignes* $\mathrm{Lig}_d(K)$*:*

$$\det(M) = \det_{\mathscr{B}^0}(\mathrm{Lig}_1(M), \cdots, \mathrm{Lig}_d(M))$$

(4) La somme

$$\det(M) = \sum_{\sigma\in\mathfrak{S}_d} \mathrm{sign}(\sigma) m_{\sigma(1)1}.\cdots.m_{\sigma(d)d}. \tag{10.2.3}$$

(5) La somme

$$\det(M) = \sum_{\sigma\in\mathfrak{S}_d} \mathrm{sign}(\sigma) m_{1\sigma(1)}.\cdots.m_{1\sigma(d)}. \tag{10.2.4}$$

Preuve: (de l'equivalence de la premiere definition avec les autres) Soit $\varphi : K^d \mapsto K^d$ telle que $\mathrm{mat}_{\mathscr{B}^0}(\varphi) = M$. C'est a dire que la j-ieme colonne de M est formee par les coordonnees de $\varphi(\mathbf{e}_j)$ dans la base canonique:

$$\varphi(\mathbf{e}_j) = \sum_{i=1}^{d} m_{ij}\mathbf{e}_i.$$

Par definition

$$\det(M) = \det(\varphi)$$

ou $\det(\varphi)$ verifies

$$\varphi^*(\det_{\mathscr{B}^0}) = \det(\varphi)\det_{\mathscr{B}^0}.$$

Evaluons cette egalite a $(\mathbf{e}_1, \cdots, \mathbf{e}_d)$. On obtient

$$\det_{\mathscr{B}^0}(\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)) = \det(\varphi)\det_{\mathscr{B}^0}(\mathbf{e}_1, \cdots, \mathbf{e}_d) = \det(\varphi) = \det(M).$$

– Cela montre l'equivalence de la premiere et de la deuxieme definition.
– La quatrieme egalite (10.2.3) provient du fait que les coordonnees de $\mathrm{Col}_j(M)$ sont donnees par les $(m_{ij})_{i\leqslant d}$ et de (10.2.1).
– La cinquieme egalite (10.2.4) provient de (10.2.2).
– La troisieme egalite provient alors de (10.2.4). □

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}$$

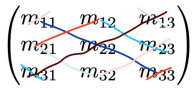


FIGURE 1. Regle de Sarrus

EXEMPLE 10.2.1. Si $d = 2$ et

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

et $\mathfrak{S}_2 = \{\mathrm{Id}_2, (12)\}$ On trouve

$$\det(M) = m_{11}m_{22} - m_{12}m_{21}.$$

Autrement dit si

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\det(M) = ad - bc.$$

Si $d = 3$,

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}$$

$$\mathfrak{S}_3 = \{\mathrm{Id}_3, (12), (13), (23), (123), (132)\}$$

$$\det(M) = m_{11}m_{22}m_{33} - m_{12}m_{21}m_{33} - m_{13}m_{22}m_{31} - m_{11}m_{23}m_{31} + m_{12}m_{23}m_{31} + m_{13}m_{21}m_{32}.$$

On reecrit quelquefois ce determinant en groupant ensemble les terme avec un $+$ et ceux avec $-$ pour calculer selon la regle de Sarrus.

$$\det(M) = m_{11}m_{22}m_{33} + m_{12}m_{23}m_{31} + m_{13}m_{21}m_{32} - m_{12}m_{21}m_{33} - m_{13}m_{22}m_{31} - m_{11}m_{23}m_{31}.$$

Il resulte immediatement des proprietes du determinant d'une application lineaire et de (10.2.3) et (10.2.4) que:

THÉORÈME 10.9 (Proprietes fonctionelles du determinant des matrices). *Le determinant d'une matrice a les proprietes suivantes*

(1) Homogeneite: soit $\lambda \in K$ alors

$$\det(\lambda.M) = \lambda^d.\det(M).$$

(2) Invariance par transposition:

$$\det(M) = \det({}^tM).$$

(3) Multiplicativite: on a

$$\det(M.N) = \det(M)\det(N) = \det(N)\det(M) = \det(N.M).$$

(4) Critere d'inversibilite: on a

$$\det(M) \neq 0 \Longleftrightarrow M \in \mathrm{GL}_d(K).$$

(5) Morphisme: L'application

$$\det : \mathrm{GL}_d(K) \mapsto K^\times$$

est un morphisme de groupes. En particulier $\det(\mathrm{Id}_d) = 1$.

COROLLAIRE 10.2. *Soient M et N deux matrices semblables (ie. conjugues): il existe $P \in \mathrm{GL}_d(K)$ tel que*

$$N = P.M.P^{-1}.$$

Alors

$$\det(M) = \det(N).$$

Le determinant ne depend que de la classe de conjugaision (d'une matrice ou d'un endomorphisme).

Preuve: On a

$$\det(N) = \det(P.M.P^{-1}) = \det(P)\det(M)\det(P)^{-1} = \det(M).$$

□

REMARQUE 10.2.3. Ce resultat s'interprete en terme de changement de base: si $M = \mathrm{mat}_{\mathscr{B}}(\varphi)$ est la matrice dans une certaine base d'une application lineaire φ et $N = \mathrm{mat}_{\mathscr{B}'}(\varphi)$ est la matrice de la meme application calculee dans une autre base. On a par la formule de changement de base

$$N = P.M.P^{-1}$$

ou $P = \mathrm{mat}_{\mathscr{B}'\mathscr{B}}$ est une matrice de changement de base et on obtient que

$$\det N = \det M = \det \varphi.$$

DÉFINITION 10.7. *Le noyau du morphisme* $\det : \mathrm{GL}_d(K) \mapsto K^\times$ *est appelle "groupe special lineaire des matrices de taille d" et on le note*

$$\mathrm{SL}_d(K) = \ker \det = \{M \in \mathrm{GL}_d(K),\ \det M = 1\}.$$

C'est un sous-groupe distingue de $\mathrm{GL}_d(K)$ *(car c'est un noyau).*

COROLLAIRE 10.3. *(Invariance du determinant par dualite) Soit $\varphi \in \mathrm{End}(V)$ et $\varphi^* \in \mathrm{End}(V^*)$ l'application lineaire duale. On*

$$\det \varphi^* = \det \varphi.$$

10.3. Le determinant en caracteristique 2

Si $\mathrm{car}(K) = 2$ une partie des raisonnements precedents ne s'appliquent pas car l'espace des formes alternees en d variables n'est pas forcement de dimension 1 (cet espace coicide avec l'espace des formes symetriques car $-1_K = 1_K$).

Neammoins on dispose toujours de la forme multilineaire alternee:

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) x_{1\sigma(1)} . \cdots . x_{d\sigma(d)}.$$

Observons qu'on a egalement

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} x_{1\sigma(1)} . \cdots . x_{d\sigma(d)}.$$

car dans un corps de caracteristique 2, $\mathrm{sign}(\sigma)_K = (\pm 1)_K = 1_K$.

THÉORÈME 10.10. *Soit K un corps quelconque et V un K-ev de dimension d. La forme* $\det_{\mathscr{B}}$ *verifie que si pour $i \neq j$, on a $v_i = v_j$ alors*

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = 0_K$$

et c'est plus generalement vrai si la famille $\{v_1, \cdots, v_d\}$ est liee.

PREUVE. On donne la preuve en caracteristique generale: comme la forme est alternee, on peut supposer en appliquant une permutation convenable que $i = 1$ et $j = 2$ et donc pour $j = 1, \cdots, d$, on a

$$x_{2j} = x_{1j}.$$

Soit $\tau = (12)$ la transposition qui permute 1 et 2. Soit

$$\mathfrak{A}_d = \ker(\text{sign}) = \{\sigma \in \mathfrak{S}_d,\ \text{sign}(\sigma) = +1\}$$

le groupe alterne des permutation paires. alors $\mathfrak{A}_d$ est d'indice 2 dans $\mathfrak{S}_d$ et comme $\tau \notin \mathfrak{A}_d$ on a

$$\mathfrak{S}_d = \mathfrak{A}_d \sqcup \mathfrak{A}_d \circ (12).$$

On a alors

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} \text{sign}(\sigma) x_{1\sigma(1)}.x_{2\sigma(2)} \cdots .x_{d\sigma(d)} = \sum_{\sigma \in \mathfrak{S}_d} \text{sign}(\sigma) x_{1\sigma(1)}.x_{1\sigma(2)} \cdots .x_{d\sigma(d)}$$

$$= \sum_{\sigma \in \mathfrak{A}_d} \text{sign}(\sigma) x_{1\sigma(1)}.x_{1\sigma(2)} \cdots .x_{d\sigma(d)} + \sum_{\sigma \in \mathfrak{A}_d} \text{sign}(\sigma \circ \tau) x_{1\sigma\circ\tau(1)}.x_{1\sigma\circ\tau(2)}.\cdots .x_{d\sigma(d)}$$

$$= \sum_{\sigma \in \mathfrak{A}_d} x_{1\sigma(1)}.x_{1\sigma(2)} \cdots .x_{d\sigma(d)} - \sum_{\sigma \in \mathfrak{A}_d} x_{1\sigma(2)}.x_{1\sigma(1)}.\cdots .x_{d\sigma(d)} = 0_K.$$

□

On developpe alors la theorie du determinant en caracteristique quelconque de la maniere suivante:

(1) Prenant $V = K^d$ et $\mathscr{B} = \mathscr{B}^0$, on definit ainsi le determinant de d vecteurs de K^d.
(2) On definit egalement le determinant d'une matrice par la meme formule:

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_d} \text{sign}(\sigma) m_{1\sigma(1)}.\cdots .m_{d\sigma(d)}.$$

et on montre par un calcul direct sur les matrices et les permutations que le theoreme 10.9 reste vrai.
(3) On definit alors le determinant d'une application lineaire generale $\varphi : V \mapsto V$ en posant

$$\det(\varphi) := \det \text{mat}_{\mathscr{B}}(\varphi)$$

pour une base quelconque $\mathscr{B}$ de V. On peut montrer par un calcul direct (utilisant la Theoreme 10.10) que

$$\varphi^*(\det_{\mathscr{B}}) = \det \varphi.\det_{\mathscr{B}}.$$

Par ailleurs la formule de changement de base, conjuguee au Theoreme 10.9 montre que cette definition ne depend pas du choix de la base. On deduit du Theoreme 10.9 que le Theoreme 10.8 est vrai.

10.4. Calcul de determinants

10.4.1. Matrices blocs.

THÉORÈME 10.11 (Determinant des matrices par blocs). *Supposons que la matrice $M \in M_d(K)$ s'ecrive sous forme triangulaire superieure par blocs:*

$$M = \begin{pmatrix} M_1 & * \\ \mathbf{0} & M_2 \end{pmatrix},\ M_1 \in M_{d_1}(K),\ M_2 \in M_{d_2}(K),\ d_1 + d_2 = d$$

alors

$$\det(M) = \det(M_1) \det(M_2)$$

Preuve: Notons que pour $j \leqslant d_1$ et $i > d_1$ on a $m_{ij} = 0$. On considere l'expression du determinant sous la forme

$$\det(M) = \det({}^tM) = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) m_{\sigma(1)1}. \cdots .m_{\sigma(d)d}.$$

Dans cette somme, on voit donc que les σ tels qu'il existe $1 \leqslant j \leqslant d_1$ verifiant $\sigma(j) > d_1$ ont une contribution nulle car $m_{\sigma(j)j} = 0$. Ainsi la somme definissant le determinant est le long de l'ensemble $\mathfrak{S}_{d,d_1}$ des σ verifiant

$$\sigma(\{1, \cdots, d_1\}) \subset \{1, \cdots, d_1\}$$

et donc

$$\sigma(\{d_1 + 1, \cdots, d_1 + d_2\}) \subset \{d_1 + 1, \cdots, d_1 + d_2\}.$$

Notons qu'un tel σ induit alors (par restriction) deux permutations

$$\sigma_1 = \sigma_{|\{1,\cdots,d_1\}} \in \mathfrak{S}_{d_1}$$

$$\sigma_2 = \sigma_{|\{d_1+1,\cdots,d_1+d_2\}} \in \mathfrak{S}_{\{d_1+1,\cdots,d_1+d_2\}} \simeq \mathfrak{S}_{d_2}$$

et on a

$$\sigma = \sigma_1.\sigma_2$$

en considerant σ_1 donne la permutation de $\{1, \cdots, d\}$ qui permute le sous-ensemble $\{1, \cdots, d_1\}$ par σ_1 et qui est l'identite sur $\{d_1 + 1, \cdots, d_1 + d_2\}$ (et similairement pour σ_2). En particulier on a

$$\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma_1)\mathrm{sign}(\sigma_2).$$

On laisse le lemme suivant au lecteur:

LEMME 10.1. *L'ensemble $\mathfrak{S}_{d,d_1}$ est un sous groupe de $\mathfrak{S}_d$ et l'application*

$$\sigma \mapsto (\sigma_1, \sigma_2)$$

est un isomorphisme de groupes

$$\mathfrak{S}_{d,d_1} \simeq \mathfrak{S}_{d_1} \times \mathfrak{S}_{\{d_1+1,\cdots,d_1+d_2\}} \simeq \mathfrak{S}_{d_1} \times \mathfrak{S}_{d_2}.$$

On peut donc reecrire

$$\det(M) = \sum_{\sigma_1 \in \mathfrak{S}_{d_1}} \sum_{\sigma_2 \in \mathfrak{S}_{d_2}} \mathrm{sign}(\sigma_1)\mathrm{sign}(\sigma_2) \prod_{i=1}^{d_1} m_{\sigma_1(i)i} \times \prod_{i=1}^{d_2} m_{d_1+\sigma_2(i),d_1+i}.$$

$$= \Big(\sum_{\sigma_1 \in \mathfrak{S}_{d_1}} \mathrm{sign}(\sigma_1) \prod_{i=1}^{d_1} m_{\sigma_1(i)i} \Big) \times \Big(\sum_{\sigma_2 \in \mathfrak{S}_{d_2}} \mathrm{sign}(\sigma_2) \prod_{i=1}^{d_2} m_{d_1+\sigma_2(i),d_1+i} \Big) = \det(M_1) \det(M_2).$$

□

COROLLAIRE 10.4. *soit $k \geqslant 2$ un entier, si M est une matrice triangulaire superieure a k blocs*

$$M = \begin{pmatrix} M_1 & * & * \\ \mathbf{0} & \ddots & * \\ \mathbf{0} & \mathbf{0} & M_k \end{pmatrix}, \ M_i \in M_{d_i}(K), \ i \leqslant k, \ d_1 + \cdots + d_k = d$$

on a

$$\det M = \det(M_1). \cdots . \det(M_k).$$

En particulier, si M est triangulaire superieure ($k = d$) –par exemple diagonale–

$$M = \begin{pmatrix} \lambda_1 & * & \cdots & \cdots \\ 0 & \lambda_2 & * & * \\ \vdots & 0 & \ddots & * \\ 0 & \cdots & \cdots & \lambda_d \end{pmatrix},$$

on a

$$\det M = \lambda_1. \cdots .\lambda_d.$$

10.4.1.1. *Matrices triangulaires inferieures par blocs.* Un matrice M est triangulaire *inferieure* par blocs si elle est de la forme

$$M = \begin{pmatrix} M_1 & \mathbf{0} \\ & M_2 \end{pmatrix},\ M_1 \in M_{d_1}(K),\ M_2 \in M_{d_2}(K),\ d_1 + d_2 = d.$$

Sa transposee ${}^tM$ est alors triangulaire superieure par blocs de la forme

$${}^tM = \begin{pmatrix} {}^tM_1 & \mathbf{0} \\ & {}^tM_2 \end{pmatrix}.$$

alors on a par invariance du determinant par transposition

$$\det(M) = \det({}^tM) = \det({}^tM_1)\det({}^tM_2) = \det(M_1)\det(M_2).$$

Ainsi le Theoreme 10.11 ainsi que ces colollaires restent vraie pour les matrices triangulaires inferieures par blocs.

10.4.2. Calcul par operations elementaires sur les lignes.

LEMME 10.2. *Soient $T_{ij},\ D_{i,\lambda}, CL_{ij,\mu}$ les matrices associees aux transformations elementaires sur les lignes d'une matrice. On a*

$$\det T_{ij} = -1\ (si\ i \neq j)$$

$$\det D_{i,\lambda} = \lambda$$

$$\det Cl_{ij,\mu} = 1,\ (si\ i \neq j).$$

Preuve: Notons $T_{ij} = (t_{ij,kl})_{k,l \leqslant d}$. On a $t_{ij,kl} = 1$ si $k = l$ et $k \neq i, j$ ou bien si $(k,l) = (i,j)$ ou (j,i). Ainsi dans la somme

$$\det T_{ij} = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) t_{ij,1\sigma(1)} . \cdots . t_{ij,d\sigma(d)}.$$

Un seul terme est non nul: celui correspondant a σ tel que

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

c'est a dire la transposition τ_{ij} echangeant i et j et alors

$$\det T_{ij} = \mathrm{sign}(\tau_{ij}) = -1.$$

La matrice $D_{i,\lambda}$ est diagonale avec des 1 sur la diagonale sauf en i-eme position ou on a λ et donc

$$\det D_{i,\lambda} = 1. \cdots .1.\lambda = \lambda.$$

On a pour $i \neq j$,

$$Cl_{ij,\mu} = \mathrm{Id}_d + \mu . E_{ij},\ i \neq j$$

qui est une matrice triangulaire inferieure ou superieure (suivant que $i < j$ ou $i > j$) avec des 1 sur la diagonale, son determinant vaut donc 1. □

COROLLAIRE 10.5. *Supposons que N soit deduite de M par une des trois type de transformations elementaires sur les lignes de M alors on a*

- *Type (I):* $\det M = -\det N$.
- *Type (II):* $\det M = \lambda^{-1} \det N$
- *Type (III):* $\det M = \det N$

Preuve: En effet on a suivant les cas

$$N = T_{ij}.M,\ N = D_{i,\lambda}.M,\ N = Cl_{ij,\mu}$$

et $\det(N)$ est le produit du determinant de M et de cette matrice. □

En utilisant ce corollaire on peut calculer $\det M$ en echelonnant la matrice M et en gardant la trace des transformations elementaires effectuees. Si E est une forme echelonnee de M, on a $\det E = 0 = \det M$ si E a $< d$ echellons et si E a d echellons E est triangulaire superieure et son determinant se calcule facilement.

10.4.3. Operations elementaires sur les colonnes. On peut egalement effectuer les memes operations elementaires sur les colonnes d'une matrice:

Définition 10.8. *Les operations elementaires sur les colonnes d'une matrice sont les applications suivantes de $M_{d'\times d}(K)$ vers $M_{d'\times d}(K)$: pour $i, j \in \{1, \cdots, d\}$ et $\lambda \in K^\times$ et $\mu \in K$.*

Pour $M \in M_{d'\times d}(K)$ une matrice dont les d colonnes sont notees

$$C_i = \mathrm{Col}_i(M),\ i \leqslant d,$$

(I) Transposition T^c_{ij}: Echanger deux colonnes $i \neq j \leqslant d$ de M:

$$C_i \longleftrightarrow C_j$$

(II) Dilatation $D^c_{i,\lambda}$: Multiplier la i-eme colonne par un scalaire $\lambda \neq 0$:

$$C_i \to \lambda.C_i.$$

(III) Combinaison Lineaire $C^c_{ij,\mu}$: Additioner a la colonne i un multiple scalaire de la la j-ieme colonne: $\mu \in K$

$$C_i \to C_i + \mu C_j$$

En fait ces operation correspondonent a des operations elementaires sur les lignes via la transposition: on a

(I) Transposition:

$$T^c_{ij}(M) = {}^t(T_{ij}({}^tM)).$$

(II) Dilatation:

$$D^c_{i,\lambda}(M) = {}^t(D_{i,\lambda}({}^tM)).$$

(III) Combinaison Lineaire:

$$C^c_{ij,\mu}(M) = {}^t(C_{ij,\lambda}({}^tM)).$$

et ces transformations elementaires correspondent a des multiplication a droites par des matrices convenables:

$$T^c_{ij}(M) = M.{}^tT_{ij}$$

$$D^c_{i,\lambda}(M) = M.{}^tD_{i,\lambda},$$

$$C^c_{ij,\mu}(M) = M.{}^tC_{ij,\mu}.$$

et comme le determinant est preserve par transposition, on a

Corollaire 10.6. *Supposons que N soit deduite de M par une des trois type de transformations elementaires sur les colonnes de M alors on a*

- *Type (I):* $\det M = -\det N$.
- *Type (II):* $\det M = \lambda^{-1} \det N$
- *Type (III):* $\det M = \det N$

10.4.4. Developpement –de Lagrange– le long d'une ligne-colonne. On va maintenant donner une methode (due a Lagrange) de calcul du determinant par recurrence sur la dimension d. Soit $M = (m_{ij}) \in M_d(K)$ une matrice de dimension d et $k, l \leqslant d$, on pose $M(k|l) \in M_{d-1}(K)$ la matrice de dimension $d-1$ obtenue a partir de M en effacant la i-ieme ligne et la j-ieme colonne.

DÉFINITION 10.9. *Pour $k, l \leqslant d$*

- *le determinant $\det(M(k|l))$ est le (k,l) mineur de M.*
- *$(-1)^{k+l}\det(M(k|l))$ est le (k,l) cofacteur de M.*

THÉORÈME 10.12 (Developpement de Lagrange le long d'une colonne). *On a pour tout $j \leqslant d$*

$$\det M = \sum_{i=1}^{d} m_{ij}(-1)^{i+j}\det(M(i|j)).$$

Preuve:

Soient $v_1, \cdots, v_d \in K^d$ les vecteurs de coordonnees les colonnes de M: On note

$$v_j = m_{1j}\mathbf{e}_1 + \cdots + m_{dj}\mathbf{e}_d.$$

On a

$$\det M = \det_{\mathscr{B}}(v_1, \cdots, v_j, \cdots, v_d).$$

Quitte a echanger v_1 et v_j ce qui remplace det par $-\det$, on suppose que $j = 1$. On a

$$v_1 = m_{11}\mathbf{e}_1 + \cdots + m_{d1}\mathbf{e}_d$$

et par multilinearite on a

$$\det_{\mathscr{B}}(v_1, v_2, \cdots, v_d) = \sum_{i=1}^{d} m_{i1}\det_{\mathscr{B}}(\mathbf{e}_i, v_2, \cdots, v_d).$$

Notons pour $j \geqslant 2$

$$v_j^{(i)} = \sum_{k\neq i} m_{kj}\mathbf{e}_k;$$

alors on a

$$\det_{\mathscr{B}}(\mathbf{e}_i, v_2, \cdots, v_d) = \det_{\mathscr{B}}(\mathbf{e}_i, v_2^{(i)}, \cdots, v_d^{(i)}).$$

On suppose maintenant que $\mathrm{car}(K) \neq 2$. Notons que l'application

$$\Lambda^{(i)} : (v_2^{(i)}, \cdots, v_d^{(i)}) \mapsto \det_{\mathscr{B}}(\mathbf{e}_i, v_2^{(i)}, \cdots, v_d^{(i)})$$

est une forme multilineaire alternee en $d-1$ variables sur le sous-espace vectoriel des vecteurs de V dont la coordonnee suivant $\mathbf{e}_i$ est nulle

$$K^{d(i)} = \{v \in K^d,\ \mathbf{e}_i^*(v) = 0\}.$$

Une base de cet espace est donne par

$$\mathscr{B}^{(i)} = \{\mathbf{e}_k,\ 1 \leqslant k \neq i \leqslant d\}.$$

Comme ($\mathrm{car}(K) \neq 2$) l'espace des formes alternees est de dimension 1, on a

$$\Lambda^{(i)}(\bullet) = \Lambda^{(i)}(\mathbf{e}_2, \cdots, \hat{\mathbf{e}}_i, \cdots, \mathbf{e}_d)\det_{\mathscr{B}^{(i)}}(\bullet) = \det_{\mathscr{B}}(\mathbf{e}_i, \mathbf{e}_2, \cdots, \hat{\mathbf{e}}_i, \cdots, \mathbf{e}_d)\det_{\mathscr{B}^{(i)}}(\bullet)$$

mais

$$\det_{\mathscr{B}}(\mathbf{e}_i, \mathbf{e}_2, \cdots, \hat{\mathbf{e}}_i, \cdots, \mathbf{e}_d) = (-1)^{i-1}\det_{\mathscr{B}}(\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_i, \cdots, \mathbf{e}_d) = (-1)^{i+1}$$

car on ramene $\mathbf{e}_i$ en i-ieme position par $i-1$ transpositions. On obtient donc

$$\det_{\mathscr{B}}(v_1, \cdots, v_d) = \sum_{i=1}^{d} m_{i1}(-1)^{i+1}\det_{\mathscr{B}^{(i)}}(v_2^{(i)}, \cdots, v_d^{(i)})$$

et

$$\det_{\mathscr{B}^{(i)}}(v_2^{(i)}, \cdots, v_d^{(i)}) = \det(M(i|1)).$$

□

Par le meme raisonnement a partir des colonnes (ou par transposition) on obtient egalement

COROLLAIRE 10.7 (Developpement de Lagrange le long d'une ligne). *On a pour tout* $i \leqslant d$

$$\det M = \sum_{j=1}^{d} m_{ij}(-1)^{i+j} \det(M(i|j)).$$

CHAPITRE 11

Le polynome caracteristique

11.1. Le polynome caracteristique d'une matrice

Soit $K[X]$ l'anneau des polynomes a coefficients dans K. C'est un anneau integre dont le corps des fractions est le corps des fractions rationelles a coefficients dans K

$$K(X) = \{\frac{P(X)}{Q(X)},\ P, Q \in K[X],\ Q \neq 0\}.$$

Soit $M \in M_d(K)$ une matrice. Comme $K \hookrightarrow K(X)$ on peut voir M comme une matrice a coefficients dans $M_d(K(X))$ ainsi que la matrice

$$X.\mathrm{Id}_d - M \in M_d(K(X))$$

dont les coordonnees sont donnees par

$$(X.\mathrm{Id}_d - M)_{ij} = X\delta_{i=j} - m_{ij}.$$

On peut donc calculer son determinant

$$\det(X.\mathrm{Id}_d - M) = \sum_\sigma \mathrm{sign}(\sigma) \prod_{i=1}^d (X\delta_{i\sigma(i)} - m_{i\sigma(i)})$$

qui est en fait un polynome en X.

Définition 11.1. *Le polynome caracteristique de M est le determinant*

$$P_{car,M}(X) = \det(X.\mathrm{Id}_d - M) = \sum_\sigma \mathrm{sign}(\sigma) \prod_{i=1}^d (X\delta_{i\sigma(i)} - m_{i\sigma(i)}) \in K[X]$$

Théorème 11.1. *Le polynome caracteristique est un polynome unitaire de degree d et si on ecrit*

$$\det(X.\mathrm{Id}_d - M) = X^d + a_{d-1}X^{d-1} + \cdots + a_d$$

On a

$$a_d = P(0) = (-1)^d \det M,$$
$$a_{d-1} = -\mathrm{tr}(M) = m_{11} + \cdots + m_{dd}$$

est la trace de la matrice M.

Preuve: On voit que

$$\det(X.\mathrm{Id}_d - M) = \sum_\sigma \mathrm{sign}(\sigma) \prod_{i=1}^d (X\delta_{i\sigma(i)} - m_{i\sigma(i)})$$

est une somme de polynomes de degre au plus d; de plus la contribution de $\sigma = \mathrm{Id}_d$ est

$$\prod_{i=1}^d (X - m_{ii})$$

est un polynome unitaire de degree d.

Notons egalement que si $\sigma \neq \mathrm{Id}$ il existe i tel que $\sigma(i) \neq i$ et $X\delta_{i\sigma(i)} - m_{i\sigma(i)} = -m_{i\sigma(i)}$; ainsi $\prod_{i=1}^d (X\delta_{i\sigma(i)} - m_{i\sigma(i)})$ est degree $< d$ donc $\det(X.\mathrm{Id}_d - M)$ est unitaire de degree d.

On a

$$a_d = P(0) = \det(-M) = (-1)^d \det M.$$

Par ailleurs si $\sigma \neq \mathrm{Id}$ soit i tel que $\sigma(i) = j \neq i$ alors $\sigma(j) \neq j$ (car σ est injective) et on a

$$(X\delta_{i\sigma(i)} - m_{i\sigma(i)})(X\delta_{j\sigma(j)} - m_{j\sigma(j)}) = m_{i\sigma(i)}m_{j\sigma(j)}$$

ainsi si $\sigma \neq \mathrm{Id}_d$ le polynome $\prod_{i=1}^d (X\delta_{i\sigma(i)} - m_{i\sigma(i)})$ est de degre $\leqslant d-2$ et le terme de degree $d-1$ de $\det(X.\mathrm{Id}_d - M)$ est celui de

$$\prod_{i=1}^{d}(X - m_{ii}) = X^d - (m_{11} + \cdots + m_{dd})X^{d-1} + \cdots .$$

□

THÉORÈME 11.2 (Proprietes fonctionnelles du polynome caracteristique). *Soient M, N des matrices, on a*

$$P_{car,{}^tM}(X) = P_{car,M}(X)$$

et

$$P_{car,MN}(X) = P_{car,NM}(X).$$

Ainsi pour tout $k \leqslant d$

$$a_k(M.N) = a_k(N.M)$$

et en particulier

$$\mathrm{tr}(M.N) = \mathrm{tr}(N.M).$$

Preuve: On a

$$P_{car,{}^tM}(X) = \det(X.\mathrm{Id}_d - {}^tM) = \det({}^t(X.\mathrm{Id}_d - M)) = \det(X.\mathrm{Id}_d - M) = P_{car,M}(X).$$

On suppose d'abord que M est inversible. On a

$$P_{car,MN}(X) = \det(X.\mathrm{Id}_d - M.N) = \det(X.M.M^{-1} - M.N)$$

$$= \det(M.(X.M^{-1} - N)) = \det((X.M^{-1} - N)M) = \det(X.\mathrm{Id}_d - N.M).$$

Soit T une autre indeterminee; on considere le corps $K' = K(T)$.

On peut faire des calculs dans ce corps de base K' qui contient K. Notons $M_T := M - T.\mathrm{Id}_d \in M_d(K')$: c' est une matrice inversible car son determinant est un polynome de degre d en la variable T et est en particulier est non-nul. On a donc

$$\det(X.\mathrm{Id}_d - M_T.N) = \det(X.\mathrm{Id}_d - N.M_T).$$

Cet determinant est un polynome en T a coefficients dans $K[X]$ dont la valeur en $T = 0_K$ vaut (car $M_0 = M$)

$$\det(X.\mathrm{Id}_d - M.N) = \det(X.\mathrm{Id}_d - N.M).$$

□

THÉORÈME 11.3 (Invariance par conjugaison). *Le polynome caracteristique est un invariant de la classe de conjugaison de la matrice M: pour toute matrice inversible $P \in \mathrm{GL}_d(K)$, on a*

$$P_{car,P.M.P^{-1}}(X) = P_{car,M}(X).$$

Preuve: On a

$$P_{car,P.M.P^{-1}}(X) = \det(X.\mathrm{Id}_d - P.M.P^{-1}) = \det(P.X.\mathrm{Id}_d.P^{-1} - P.M.P^{-1})$$

$$= \det(P(X.\mathrm{Id}_d - M).P^{-1}) = \det(X.\mathrm{Id}_d - M) = P_{car,M}(X).$$

□

COROLLAIRE 11.1. *Soient $(a_k(M))_{0\leqslant k\leqslant d}$ les coefficients de $P_{car,M}(X)$:*

$$\det(X.\mathrm{Id}_d - M) = X^d + a_{d-1}(M)X^{d-1} + \cdots + a_d(M)$$

(on a $a_d(M) = 1$).

Ces coefficients sont des invariants de la classe de conjugaison de M.

Autrement dit, pour toute matrice inversible $P \in \mathrm{GL}_d(K)$ et $0 \leqslant k \leqslant d$

$$a_k(M) = a_k(P.M.P^{-1}).$$

REMARQUE 11.1.1. On retrouve ainsi que la trace d'une matrice ne depend que de la classe de conjugaison de celle-ci.

11.1.1. Exemple: la "matrice compagnon". On aura egalement besoin de la "matrice compagnon" qu'on a deja rencontre en seance d'exercices: soit un polynome unitaire de degre d,

$$P(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0;$$

on note $\mathrm{b} = (b_0, \cdots, b_{d-1}) \in K^d$ le vecteur de ces coefficients. La matrice compagnion de P est la matrice

$$M_P = M_{\mathrm{b}} = \begin{pmatrix} 0 & 0 & 0 & 0 & -b_0 \\ 1 & 0 & 0 & 0 & -b_1 \\ 0 & 1 & 0 & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -b_{d-1} \end{pmatrix} \in M_d(K).$$

On a vu en exercice que

$$P(M_P) = M_P^d + b_{d-1}M_P^{d-1} + \cdots + b_0\mathrm{Id}_d = \mathbf{0}_d.$$

Par exemple la matrice compagnon de $X^2 + 1$ est la matrice $I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ qui sert a definir les nombres complexes et qui verifie

$$I^2 + \mathrm{Id}_2 = \mathbf{0}_2.$$

PROPOSITION 11.1. *Soit*

$$P(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0 \in K[X]$$

un polynome et M_P la matrice compagnion associee au polynome P. Alors son polynome caracteristique est egal a P:

$$P_{car,M_P}(X) = \det(X.\mathrm{Id}_d - M_P) = P(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0.$$

PREUVE. (Exercice) On doit calculer

$$\det \begin{pmatrix} X & 0 & 0 & 0 & b_0 \\ -1 & X & 0 & 0 & b_1 \\ 0 & -1 & X & 0 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & -1 & X + b_{d-1} \end{pmatrix}$$

Pour cela on echelonnera la matrice par une suite d'operations de type (III) (dans le corps $K(X)$ des fractions rationelles) pour la rendre triangulaire superieure. □

11.1.2. Cas des matrices triangulaires par blocs.

PROPOSITION 11.2. *Supposons que la matrice $M \in M_d(K)$ s'ecrive sous forme triangulaire superieure par blocs:*

$$M = \begin{pmatrix} M_1 & * \\ \mathbf{0} & M_2 \end{pmatrix},\ M_1 \in M_{d_1}(K),\ M_2 \in M_{d_2}(K),\ d_1 + d_2 = d$$

alors

$$P_{car,M}(X) = P_{car,M_1}(X)P_{car,M_2}(X)$$

Preuve: Exercice. □En iterant on obtient

COROLLAIRE 11.2. *soit $k \geqslant 2$ un entier, si M est une matrice triangulaire superieure a k blocs*

$$M = \begin{pmatrix} M_1 & * & * \\ & \ddots & \\ \mathbf{0} & & * \\ \mathbf{0} & \mathbf{0} & M_k \end{pmatrix},\ M_i \in M_{d_i}(K),\ i \leqslant k,\ d_1 + \cdots + d_k = d$$

on a

$$P_{car,M}(X) = P_{car,M_1}(X).\cdots.P_{car,M_k}(X)$$

En particulier, si M est triangulaire superieure ($k = d$) –par exemple diagonale–

$$M = \begin{pmatrix} \lambda_1 & * & \cdots & \cdots \\ 0 & \lambda_2 & * & * \\ \vdots & 0 & \ddots & * \\ 0 & \cdots & \cdots & \lambda_d \end{pmatrix},$$

on a

$$P_{car,M}(X) = \prod_{i=1}^{d}(X - \lambda_i).$$

REMARQUE 11.1.2. Notons enfin que par invariance du polynome caracteristique par transposition le Corollaire reste vrai pour une matrice triangulaire inferieure par blocs.

11.2. Le polynome caracteristique d'un endomorphisme

L'invariance par conjugaison du polynome caracteristique permet de definir le polynome caracteristique d'une application lineaire:

DÉFINITION 11.2. *Soit $\varphi \in \mathrm{End}(V)$ une application lineaire, on definit son polynome caracteristique par*

$$P_{car,\varphi}(X) = P_{car,M}(X)$$

ou $M = \mathrm{mat}_{\mathscr{B}}(\varphi)$ est la matrice de φ dans une base quelconque de V.

Notons que cette definition ne depend pas de la base $\mathscr{B}$ choisie: si $M' = \mathrm{mat}_{\mathscr{B}'}(\varphi)$ est la matrice de φ dans une autre base alors par la formule de changement de base

$$M' = \mathrm{mat}_{\mathscr{B}'\mathscr{B}}.M.\mathrm{mat}^{-1}_{\mathscr{B}'\mathscr{B}}$$

et

$$P_{car,M'}(X) = P_{car,M}(X) = P_{car,\varphi}(X).$$

En particulier les coefficient $a_k(\varphi) = a_k(M)$ du polynome caracteristique ne dependent pas du choix de la base.

DÉFINITION 11.3. *On definit la trace de φ comme etant la trace de M*

$$\mathrm{tr}(\varphi) = \mathrm{tr}(M) = m_{11} + \cdots + m_{dd}$$

et cette definition ne depend pas du choix de la base $\mathscr{B}$.

PROPOSITION 11.3. *Le polynome caracteristique $P_{car,\varphi}(X)$ ne depend que de la classe de conjugaison de φ dans* $\mathrm{End}(V)$*: pour tout* $\psi \in \mathrm{GL}(V)$

$$P_{car,\psi.\varphi.\psi^{-1}}(X) = P_{car,\varphi}(X).$$

11.2.1. Sous-espaces propres. L'interet du polynome caracteristique est qu'il permet d'identifier des sous-espaces interessant de V relativement a φ:

THÉORÈME 11.4. *Soit $P_{car,\varphi}$ le polynome caracteristique d'une application lineaire φ.*
Les enonces suivants sont equivalents

(1) Le scalaire $\lambda \in K$ est racine de $P_{car,\varphi}$: $P_{car,\varphi}(\lambda) = 0$.
(2) Il existe $v \in V - \{0\}$ tel que $\varphi(v) = \lambda.v$

Preuve: On a les equivalences suivantes

- $P_{car,\varphi}(\lambda) = \det(\lambda.\mathrm{Id}_V - \varphi) = 0$,
- $\lambda.\mathrm{Id}_V - \varphi$ n'est pas inversible,
- $\lambda.\mathrm{Id}_V - \varphi$ n'est pas injective,
- $\ker(\lambda.\mathrm{Id}_V - \varphi) \neq \{0_V\}$,
- Il existe $v \in V - \{0_V\}$ tel que

$$0_V = (\lambda.\mathrm{Id}_V - \varphi)(v) = \lambda.v - \varphi(v).$$

□

DÉFINITION 11.4. *Soit $\lambda \in K$, le sous-espace*

$$V_{\varphi,\lambda} := \ker(\varphi - \lambda.\mathrm{Id}_V) = \{v \in V,\ \varphi(v) = \lambda.v\}$$

est appelle sous-espace propre associe a λ. Si $V_{\varphi,\lambda} \neq \{0_V\}$ on dit que λ est une valeur propre de φ et tout vecteur non-nul de $V_{\varphi,\lambda}$ (ie. verifiant $\varphi(v) = \lambda.v$) est appelle vecteur propre de φ associe a la valeur propre λ.
L'ensemble des valeurs propres de φ est appelle le spectre de φ (dans K) est est note

$$\mathrm{Spec}_\varphi(K).$$

Le Theoreme precedent dit ainsi que les racines dans K du polynome caracteristique sont exactement les valeurs propres de φ:

$$\mathrm{Rac}_{P_{car,\varphi}}(K) = \mathrm{Spec}_\varphi(K).$$

Voici quelques proprietes de base des sous-espaces propres:

THÉORÈME 11.5. *Soit $\varphi \in \mathrm{End}(V)$ et λ, λ' des valeurs propres de φ et $V_{\varphi,\lambda}$, $V_{\varphi,\lambda'}$ les sous-espaces propres associes.*

- *Le sous-espace $V_{\varphi,\lambda}$ est stable par φ:*

$$\varphi(V_{\varphi,\lambda}) \subset V_{\varphi,\lambda}.$$

- *Si $\lambda \neq \lambda'$ les sous-espaces $V_{\varphi,\lambda}$ et $V_{\varphi,\lambda'}$ sont en somme directe:*

$$V_{\varphi,\lambda} \cap V_{\varphi,\lambda'} = \{0_V\}.$$

Preuve: Soit $v \in V_{\varphi,\lambda}$, et $w = \varphi(v)$, on a

$$\varphi(w) = \varphi(\varphi(v)) = \varphi(\lambda.v) = \lambda.\varphi(v) = \lambda.w$$

et donc $w = \varphi(v) \in V_{\varphi,\lambda}$.
Soit $\lambda \neq \lambda'$ et $v \in V_{\varphi,\lambda} \cap V_{\varphi,\lambda'}$, on a

$$\varphi(v) = \lambda.v = \lambda'.v$$

et donc

$$(\lambda - \lambda').v = 0_V$$

mais comme $\lambda - \lambda' \neq 0_K$, on a $v = 0_V$. □

11.3. Le Theoreme de Cayley-Hamilton

Soit $K[X]$ l'agebre des polynomes sur un corps K , $(A,+,.)$ une K-algebre et $\varphi \in A$ un element de cette algebre. Cette donnee permet de definir une application appelle "evaluation en φ"

$$\mathrm{ev}_\varphi : \begin{array}{ccc} K[X] & \mapsto & A \\ P(X) & \mapsto & P(\varphi) \end{array}$$

ou on a note

$$P(\varphi) = a_n.\varphi^n + a_{n-1}.\varphi^{n-1} + \cdots + a_0.1_A$$

pour $P(X)$ un polynome a coefficients dans K

$$P(X) = a_n.X^n + a_{n-1}.X^{n-1} + \cdots + a_0,\ a_0, \cdots, a_d \in K.$$

On rappelle que

$$\varphi^d := \varphi.\cdots.\varphi\ (d \text{ fois si } d \geqslant 1),\ \varphi^0 := 1_A.$$

On verifie facilement que

PROPOSITION 11.4. *L'application* ev_φ *est un morphisme de* K*-algebres:*

$$\mathrm{ev}_\varphi(\lambda.P + Q) = \lambda P(\varphi) + Q(\varphi) = \lambda.\mathrm{ev}_\varphi(P) + \mathrm{ev}_\varphi(Q)$$

$$\mathrm{ev}_\varphi(P.Q) = P(\varphi).Q(\varphi) = \mathrm{ev}_\varphi(P).\mathrm{ev}_\varphi(Q).$$

Son image $\mathrm{ev}_\varphi(K[X])$ *est notee*

$$K[\varphi] = \{a_n.\varphi^n + a_{n-1}.\varphi^{n-1} + \cdots + a_0.1_A,\ n \geqslant 1, a_0, \cdots, a_n \in K\} \subset A$$

est une sous-algebre commutative de A *engendree comme* K*-ev par les puissance de* φ*:*

$$\{1_A = \varphi^0, \varphi, \cdots, \varphi^n, \cdots\}.$$

REMARQUE 11.3.1. La commutativite resulte du fait que $K[X]$ est commutatif et donc

$$P(\varphi).Q(\varphi) = (P.Q)(\varphi) = (Q.P)(\varphi) = Q(\varphi).P(\varphi).$$

On va appliquer cette construction a l'algebre des matrices $(M_d(K),+,.)$ pour une matrice $M \in M_d(K)$ et a l'algebre des endomorphismes d'un espace vectoriel V, $(\mathrm{End}(V),+,\circ)$ pour une application lineaire $\varphi \in \mathrm{End}(V)$.

THÉORÈME 11.6 (Cayley-Hamilton). *Soit* $M \in M_d(K)$ *(resp.* $\varphi \in \mathrm{End}(V)$*) alors son polynome caracteristique* $P_{car,M}(X)$ *(resp* $P_{car,\varphi}(X)$*) appartient a* $\ker \mathrm{ev}_M$ *(resp.* $\ker \mathrm{ev}_\varphi$*); en d'autre termes*

$$P_{car,M}(M) = \mathbf{0}_{d\times d},\ P_{car,\varphi}(\varphi) = \underline{0}_V,$$

Preuve: Soit $\varphi : V \mapsto V$. Il s'agit de montrer que pour tout $v \in V - \{0\}$,

$$P_{car,\varphi}(\varphi)(v) = 0_V.$$

Si $v = 0_V$ c'est evident. Sinon on considere la suite de vecteurs

$$v,\ \varphi(v),\ \varphi^2(v), \cdots, \cdots, \varphi^k(v), \cdots.$$

Comme V est de dimension finie il existe $d_1 \leqslant d$ tel que

$$v,\ \varphi(v),\ \varphi^2(v), \cdots, \cdots, \varphi^{d_1}(v)$$

est liee. Prenons $d_1 \geqslant 1$ le plus petit possible pour cette propriete de sorte que

$$\mathscr{B}_1 := \{v,\ \varphi(v),\ \varphi^2(v), \cdots, \cdots, \varphi^{d_1-1}(v)\}$$

est libre et il existe $b_0, \cdots, b_{d_1-1} \in K$ tels que

$$\varphi^{d_1}(v) = b_0.v + \cdots + b_{d_1-1}\varphi^{d_1-1}(v).$$

Completons la famille $\mathscr{B}_v$ en une base de V: $\mathscr{B} = \mathscr{B}_1 \sqcup \mathscr{B}_2$. Soit $M = \mathrm{mat}_{\mathscr{B}}(\varphi)$ la matrice de φ dans cette base. Elle est de la forme

$$\begin{pmatrix} 0 & 0 & 0 & 0 & b_0 & * \\ 1 & 0 & 0 & 0 & b_1 & * \\ 0 & 1 & 0 & 0 & b_2 & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & b_{d_1-1} & * \\ & & \mathbf{0} & & & M_2 \end{pmatrix} = \begin{pmatrix} & & & * \\ & & & * \\ & M_1 & & * \\ & & & * \\ & & & * \\ & & \mathbf{0} & M_2 \end{pmatrix}$$

de sorte que

$$P_{car,\varphi}(X) = P_{car,M}(X) = P_{car,M_1}(X)P_{car,M_2}(X) = P_{car,M_2}(X)P_{car,M_1}(X)$$

La matrice M_1 est une matrice compagnion dont on connait le polynome caracteristique (cf. Prop 11.1)

$$P_{car,M_1}(X) = \det \begin{pmatrix} X & 0 & 0 & 0 & -b_0 \\ -1 & X & 0 & 0 & -b_1 \\ 0 & -1 & X & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & -1 & X - b_{d_1-1} \end{pmatrix} = X^{d_1} - b_{d_1-1}X^{d_1-1} - \cdots - b_0$$

et

$$P_{car,\varphi}(\varphi)(v) = P_{car,M_2}(\varphi) \circ P_{car,M_1}(\varphi)(v) = P_{car,M_2}(\varphi)(P_{car,M_1}(\varphi)(v)) = 0_V$$

car

$$P_{car,M_1}(\varphi)(v) = \varphi^{d_1}(v) - b_{d_1-1}\varphi^{d_1-1}(v) - \cdots - b_0 v = 0_V$$

□

Remarque 11.3.2. Dans cette preuve on a implicitement utilise le fait que l'on connaissait deja le Theoreme pour les matrices compagnons (Prop 11.1 et la remarque qui suit).

Corollaire 11.3. *Soit φ un endomorphisme et M sa matrice associee dans une base quelconque. Si $\det(\varphi) = \det(M) \neq 0$ alors φ et M sont inversibles et on a*

$$\varphi^{-1} = \frac{(-1)^{d+1}}{\det \varphi}(a_1 \mathrm{Id}_V + \cdots + a_{d-1}\varphi^{d-2} + \varphi^{d-1})$$

$$M^{-1} = \frac{(-1)^{d+1}}{\det M}(a_1 \mathrm{Id}_d + \cdots + a_{d-1}M^{d-2} + M^{d-1})$$

ou

$$P_{car,\varphi}(X) = P_{car,M}(X) = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} + X^d.$$

En particulier $\varphi^{-1} \in K[\varphi]$ et $M^{-1} \in K[M]$.

Preuve: On a

$$\mathbf{0}_d = a_0 \mathrm{Id}_d + a_1 M + \cdots + a_{d-1}M^{d-1} + M^d$$

de sorte que

$$-a_0 \mathrm{Id}_d = a_1 M + \cdots + a_{d-1}M^{d-1} + M^d = M.(a_1 \mathrm{Id}_V + \cdots + a_{d-1}M^{d-2} + M^{d-1})$$

et si $a_0 = (-1)^d \det(M) \neq 0$, on a

$$\mathrm{Id}_d = M.\frac{-1}{a_0}(a_1 \mathrm{Id}_d + \cdots + a_{d-1}M^{d-2} + M^{d-1})$$

ce qui montre que M est inversible. □

CHAPITRE 12

L'anneau des polynomes sur un corps

Dans ce chapitre on donne la construction algebrique des polynomes a coefficients dans un anneau commutatif A (et en particulier quand $A = K$ est un corps). On rappellera ensuite la terminologie et les proprietes de bases concernant polynomes (degree, monomes, division euclidienne, factorisation, polynomes irreductibles, racines). on appliquera la theorie a la construction de sous-algebres dans des algebres sur un corps (algebres monogenes)

12.1. Les polynomes sont des suites

Soit A un anneau commutatif. L'ensemble des polynomes $A[X]$ sont construit algebriquement comme un sous-ensemble de l'ensemble des suites a valeurs dans A (ou encore l'ensemble des fonctions de $\mathbb{N}$ a valeurs dans A)

$$K^{\mathbb{N}} = \{(a_n)_{n\geqslant 0},\ a_n \in A\}.$$

DÉFINITION 12.1. *Soit $(a_n)_{n\geqslant 0} \in A^{\mathbb{N}}$ une suite a valeurs dans A. Le support de cette suite est defini par*

$$\mathrm{supp}((a_n)_{n\geqslant 0}) = \{n \in \mathbb{N},\ a_n \neq 0_A\} \subset \mathbb{N}.$$

DÉFINITION 12.2. *L'ensemble des polynomes a coefficients dans A est le sous-ensemble forme des suites a support fini:*

$$A[X] = K_f^{\mathbb{N}} = \{(a_n)_{n\geqslant 0},\ a_n \in A,\ |\mathrm{supp}((a_n)_{n\geqslant 0}| < \infty\}.$$

PROPOSITION 12.1. *L'ensemble $A[X]$ est un sous-A module de $K^{\mathbb{N}}$ pour l'addition et la multiplication par les scalaire sur l'espaces des suite.*

Preuve: Rappelons que si $\mathbf{a} = (a_n)_{n\geqslant 0})$, et $\mathbf{b} = (b_n)_{n\geqslant 0})$ sont des suite et $a \in A$, l'addition est definie par

$$\mathbf{a} + \mathbf{b} := (a_n + b_n)_{n\geqslant 0}$$

et la multiplication par a est definie par

$$a.\mathbf{a} := (a.a_n)_{n\geqslant 0})$$

et que $A^{\mathbb{N}}$ est un A-module. Comme on a

$$\mathrm{supp}(\mathbf{a}+\mathbf{b}) \subset \mathrm{supp}(\mathbf{a}) \cup \mathrm{supp}(\mathbf{b}),\ \mathrm{supp}(a.\mathbf{a}) \subset \mathrm{supp}(\mathbf{a})$$

si $\mathbf{a}$ et $\mathbf{b}$ sont a supports finis alors $\mathbf{a}+\mathbf{b}$ et $a.\mathbf{a}$ sont a supports finis et ainsi $A[X]$ est un sous A-module de $K^{\mathbb{N}}$. □

DÉFINITION 12.3. *Le degree d'un polynome non-nul $P = (a_n)_{n\geqslant 0}$ est le plus grand element de* $\mathrm{supp}(P)$*:*

$$\deg(P) = \max\{d \geqslant 0,\ a_d \neq 0\}.$$

Si $P = 0_K$ est le polynome nul, le support est l'ensemble vide et on pose

$$\deg(0_K) = -\infty.$$

Etant donne un polynome de degre $\leqslant d$

$$P = (a_0, \cdots, a_d, 0, \cdots)$$

le n-ieme terme de cette suite a_n est appelle coefficient de degre (ou d'ordre) n de P.

PROPOSITION 12.2. *Soient P, Q des polynomes, on a*

$$\deg(P+Q) \leqslant \max(\deg P, \deg Q)$$

avec egalite si $\deg P \neq \deg Q$.

Preuve: C'est evident si P ou $Q = 0$.

Sinon soit $d = \deg P \geqslant d' = \deg Q$, on a

$$P = (a_0, a_1, \cdots, a_d, 0, \cdots),\ Q = (b_0, b_1, \cdots, b_{d'}, 0, \cdots)$$

avec $a_d, b_{d'} \neq 0$.

Supposons $d' \geqslant d$, on a

$$P + Q = (a_0 + b_0, a_1 + b_1, \cdots, a_d + b_d, 0 + b_{d+1}, \cdots, 0 + b'_d, 0, \cdots)$$

et $\deg(P+Q) \leqslant d'$ (avec egalite ssi $d = d'$ et $a_{d'} + b_{d'} \neq 0$). □

COROLLAIRE 12.1. *Soit $d \geqslant 0$ et*

$$A[X]_{\leqslant d} = \{P \in A[X],\ \deg P \leqslant d\}$$

l'ensemble des polynomes de degre $\leqslant d$. Alors $A[X]_{\leqslant d}$ est un sous A-module de $A[X]$.

DÉFINITION 12.4. *Un polynome non-nul est unitaire si le coefficient de degre* $\deg P$ *verifie*

$$a_{\deg P} = 1.$$

12.1.1. La famille des monomes unitaires. On va maintenant identifier une famille particuliere de polynomes:

NOTATION 12.1. *Soit $k \geqslant 0$ un entier, on a note X^k le polynome (ie la suite de support fini) defini par*

$$X^k := (\delta_{n=k})_{n \geqslant 0}$$

avec ($\delta_{n=k}$ le symbole de Kronecker)

$$\delta_{n=k} = \begin{cases} 1_K & \text{si } n = k \\ 0_K & \text{sinon.} \end{cases}$$

Le polynome X^k est appelle monome unitaire d'ordre k et on note l'ensemble des monomes unitaire

$$\mathscr{M} = \{X^k,\ k \geqslant 0\} \subset A[X].$$

L'interet de la famille des monomes unitaires est le suivant:

THÉORÈME 12.1. *La famille des monomes $\mathscr{M}$ engendre $A[X]$ comme A-module: tout polynome se decompose en combinaison lineaire (a coefficient dans A) de monomes: pour tout $P \in A[X]$ il existe $d \geqslant 0$ et $a_0, \cdots, a_d \in A$ tels que*

$$P = a_0.X^0 + a_1.X^1 + \cdots + a_d.X^d.$$

De plus, cette decomposition est unique: si

$$P = a_0.X^0 + a_1.X^1 + \cdots + a_d.X^d = a'_0.X^0 + a'_1.X^1 + \cdots + a'_{d'}.X^{d'}$$

avec $d \leqslant d'$ alors pour tout $k \leqslant d$ on a $a_k = a'_k$ et pour $d < k \leqslant d'$ on a $a'_k = 0_K$.

DÉFINITION 12.5. *La famille des monomes unitaires est aussi appellee base canonique de $A[X]$.*

EXEMPLE 12.1.1. Le monome X^d est de degre d. Le polynome constant $\lambda = \lambda.X^0$ est de degre 0 si $\lambda \neq 0_K$.

En particulier on dispose d'un application lineaire injective de A dans $A[X]$ appellee "polynome constant"

$$\text{Cst} : \begin{array}{ccc} K & \mapsto & K[X] \\ \lambda & \mapsto & \lambda.X^0 = (\lambda, 0, 0, \cdots) \end{array}.$$

NOTATION 12.2. *On appelle* $\mathrm{Cst}(\lambda) = \lambda.X^0$ *le "polynome constant de valeur* λ*" et pour simplifier les notations on ecrira* λ *au lieu de* $\lambda.X^0$.

Par apreil on note egalment

$$X^1 =: X.$$

12.2. Structure d'anneau

12.2.1. Fonction polynomiale associee a un polynome. Soit

$$P = a_d.X^d + a_{d-1}.X^{d-1} + \cdots + a_1.X + a_0$$

un polynome a coefficient dans $\mathbb{R}$. La fonction polynomiale associee a P est la fonction de $P(\bullet) : \mathbb{R} \mapsto \mathbb{R}$ definie par

$$P(\bullet) : x \in \mathbb{R} \mapsto P(x) := a_d.x^d + a_{d-1}.x^{d-1} + \cdots + a_1.x + a_0 \in \mathbb{R}.$$

Plus generalement,

DÉFINITION 12.6. *Soit* A *un anneau et*

$$P = a_d.X^d + a_{d-1}.X^{d-1} + \cdots + a_1.X + a_0$$

un polynome a coefficient dans A*. La fonction polynomiale associee a* P *est la fonction*

$$P(\bullet) : A \mapsto A$$

definie par

$$P(\bullet) : x \in A \mapsto P(x) := a_d.x^d + a_{d-1}.x^{d-1} + \cdots + a_1.x + a_0 \in A.$$

On a

PROPOSITION 12.3. *L'application "fonction polynomiale"*

$$P \in A[X] \mapsto P(\bullet) \in \mathcal{F}(A, A)$$

est un morphisme de A*-modules pour la structure naturelle de* A*-module sur l'espaces des fonctions de* A *vers* A*: on a*

$$(P + Q)(\bullet) = P(\bullet) + Q(\bullet)$$

et

$$(\lambda.P)(\bullet) = \lambda.P(\bullet).$$

Cependant l'espace $\mathcal{F}(A, A)$ possede egalement une structure d'anneau (et meme de A-algebre) donnee par pour $f, g \in \mathcal{F}(A, A)$ et $\lambda \in A$

$$(f.g) : x \in A \mapsto f(x).g(x) \in A,\ (\lambda.f) : x \in A \mapsto \lambda.f(x).$$

PROPOSITION 12.4. *Soient* P *et* Q *deux polynomes alors le produit de leur deux fonctions polynomiales:*

$$P(\bullet).Q(\bullet) : x \in A \mapsto P(x).Q(x)$$

est encore une fonction polynomiale associee au polynome

$$P.Q = c_0 + c_1.X + \cdots + c_{2d}X^{2d}$$

ou on a note ($d = \max(\deg P, \deg Q)$)

$$P = a_d.X^d + a_{d-1}.X^{d-1} + \cdots + a_1.X + a_0,\ Q = b_d.X^d + b_{d-1}.X^{d-1} + \cdots + b_1.X + b_0,$$

et

$$c_n = \sum_{p+q=n} a_p.b_q = a_0.b_n + a_1.b_{n-1} + \cdots + a_n.b_0.$$

Preuve: Pour tout $x \in A$, on a (utilisant la distributivite, l'associativite et la commutativite de A)

$$P(x).Q(x) = (a_0. + a_1.x + \cdots + a_d.x^d).(b_0 + b_1.x + \cdots + b_{d'}.x^{d'}) = \sum_{p,q\leqslant d} a_p.X^p.b_q.X^q = \sum_{p,q\leqslant d} a_p.b_q.x^{p+q} = \sum_{n\leqslant 2d}(\sum_{p+q=n} a_p.b_q)x^n = \sum_{n\leqslant 2d} c_n.x^n$$

□

12.2.2. Multiplication abstraite des polynomes. La proposition precedente motive l'introdution de la loi de multiplication interne sur $A[X]$: on defini

$$\bullet.\bullet : \begin{array}{ccc} A[X]\times A[X] & \mapsto & A[X] \\ (P,Q) & \mapsto & P.Q = (c_n)_{n\geqslant 0} \end{array}$$

avec

$$c_n = \sum_{p+q=n} a_p.b_q = a_0.b_n + a_1.b_{n-1} + \cdots + a_n.b_0.$$

et

$$P = (a_n)_{n\geqslant 0},\ Q = (b_n)_{n\geqslant 0}.$$

Notons que si les suites $(a_n)_{n\geqslant 0}$ et $(b_n)_{n\geqslant 0}$ sont a support fini, $\mathrm{supp}((c_n)_{n\geqslant 0})$ est de support fini, plus precisement

PROPOSITION 12.5. *Soient P, Q des polynomes, on a*

$$\deg(P.Q) \leqslant \deg P + \deg Q.$$

Preuve: C'est evident si P ou $Q = 0$ compte-tenu du fait que $\deg 0 = -\infty$ et que $P.Q = 0_A$:

$$\deg(P.Q) = -\infty = \deg P + \deg Q.$$

Si P et Q sont non-nuls, on a pour $n > \deg P + \deg Q$

$$c_n = \sum_{p+q=n} a_p.b_q = 0_A$$

et donc $P.Q$ est a support fini et de degre $\leqslant \deg P + \deg Q$. En effet, si $p + q = n > \deg P + \deg Q$ alors ou bien $p > \deg P$ ou bien $q > \deg Q$ et alors $a_p.b_q = 0_A$. □

On verifie alors (exercice)

THÉORÈME 12.2. *La loi de multiplication interne $\bullet.\bullet$ sur $A[X]$ est associative, commutative et distributive par rapport a l'addition et fait de $(A[X], +, .)$ un anneau commutatif dont l'element unite est le polynome constant*

$$1_K = (1_K, 0, \cdots).$$

De plus comme $A[X]$ est un A-module et que la multiplication par les scalaires coincide avec la multiplication par les polynomes constants, $A[X]$ est une A-algebre.

12.2.3. Retour sur les fonctions polynomiales. L'interet d'avoir defini l'addition et la multiplication des polynomes comme on l'a fait est la Proposition suivante:

PROPOSITION 12.6. *Soit $\mathcal{F}(A; A)$ l'espace des fonctions de A a valeurs dans A: L'application "fonction polynomiale"*

$$P \in A[X] \mapsto P(\bullet) \in \mathcal{F}(A; A)$$

qui a un polynome associe sa fonction polynomiale est un morphisme d'anneaux.

REMARQUE 12.2.1. Notons qu'en general cette application n'est PAS injective: par exemple si $K = \mathbb{F}_p$ est le corps fini a p elements, la fonction polynomiale associe au polynome $X^p - X$ est identiquement nulle: on a vu que $\forall x \in \mathbb{F}_p$, on a

$$x^p - x = 0_{\mathbb{F}_p}.$$

On va analyser plus tard quand est ce que cette application est injective (et donc qu'on peut identifier l'algebre des polynomes a un espace de fonctions)

NOTATION 12.3. *En raison de ce lien avec les fonctions polynomiales, on note un polynome $P(X)$ au lieu de P.*

12.2.3.1. *Integralite de $A[X]$ et corps des fractions.*

PROPOSITION 12.7. *L'anneau $A[X]$ est integre ssi A est integre et on a alors pour tout $P, Q \in A[X]$,*

$$\deg(P.Q) = \deg P + \deg Q.$$

Preuve: Si A n'est pas integre alors $A[X]$ ne l'est pas: soient $a, b \in A$ tels que $a.b = O_A$ alors le produit des polynomes constants (de degre 0) a et b vaut le polynome constant $a.b = 0_A$.

Supposons que A est integre et soient P et Q tous deux non-nuls et $(c_n)_{n\geqslant 0}$ les coefficients de $P.Q$: alors pour $n = \deg P + \deg Q$, on a

$$c_n = \sum_{p+q=\deg P+\deg Q} a_p.b_q = a_{\deg P}.b.\deg Q$$

car $p \leqslant \deg P$ et $q \leqslant \deg Q$. Par definition du degre $a_{\deg P}, b_{\deg Q} \neq 0_A$ et comme A est integre $a_{\deg P}.b_{\deg Q} \neq 0_A$. Ainsi $\deg P.Q \geqslant \deg P + \deg Q$ et donc $\deg P.Q = \deg P + \deg Q$. □

DÉFINITION 12.7. *Le corps des fractions de l'anneau integre $K[X]$ est note*

$$K(X) := \mathrm{Frac}(K[X]) = \{F(X) = \frac{P(X)}{Q(X)},\ P, Q \in K[X],\ Q \neq 0\}$$

et on l'appelle le corps des fractions rationelles a coefficients dans K.

REMARQUE 12.2.2. De la meme maniere, on pourrait construire $A[X]$ l'anneau des polynomes a coefficients dans A pour un anneau commutatif general. En revanche la formule du degre du produit ne reste vraie que si A est integre.

12.2.3.2. *Racines d'un polynome.* Un invariant important d'un polynome est l'ensemble des valeurs ou sa fonction polynomiale s'annule:

DÉFINITION 12.8. *Soit*

$$P(X) = a_d.X^d + a_{d-1}.X^{d-1} + \cdots + a_1.X + a_0$$

un polynome a coefficient dans K. L'ensemble des racines de P dans K, $\mathrm{Rac}_P(K)$ est l'ensemble des solution dans K de l'equation $P(z) = 0$:

$$\mathrm{Rac}_P(K) = \{z \in K,\ P(z) = 0_K\}.$$

12.3. Division et factorisation

La division euclidienne des polynomes sur $\mathbb{R}$ se generalise a un corps arbitraire:

THÉORÈME 12.3. *Soit $Q \in K[X] - \{0\}$ un polynome non-nul. Pour tout P il existe des polynomes $S, R \in K[X]$ uniques verifiant*

$$\deg R < \deg Q \text{ et tels que } P = Q.S + R.$$

Preuve: Soit $q = \deg Q$:

$$Q = q_d.X^q + \cdots + q_1.X + q_0,\ q_d \neq 0.$$

Ecrivons

$$P = a_d.X^d + \cdots + a_0.$$

Si $d < q$, on prend $R = P$ et $S = 0$. Sinon, on precede par recurrence sur d:

$$P_1 := P - \frac{a_d}{q_d}Q.X^{d-q} = a_d.X^d - \frac{a_d}{q_d}q_d.X^d.X^{d-q} + \text{ polynome de degree } < d$$

et comme

$$a_d.X^d - \frac{a_d}{q_d}q_d.X^d.X^{d-q} = 0$$

Le polynome P_1 est degree $\leqslant d-1$. Par recurrence sur le degre il existe R_1, S_1 tels que

$$P_1 = Q.S_1 + R_1$$

avec $\deg R_1 < q$ et donc

$$P = \frac{a_d}{q_d}Q.X^{d-q} + Q.S_1 + R_1 = Q.S + R$$

avec

$$S = \frac{a_d}{q_d}X^{d-q} + S_1,\ R = R_1.$$

On conclut par recurrence. Montrons l'unicite: supposons que

$$P = Q.S + R = Q.S' + R'$$

avec $\deg R, \deg R' < q$. Alors

$$Q.S - Q.S' = Q.(S - S') = R' - R.$$

On a

$$\deg Q.(S - S') = q + \deg(S - S') = \deg(R' - R) < q$$

et la seule possibilite est que $S - S' = 0$ et donc $R' - R = 0$ □

DÉFINITION 12.9. *Les polynomes R et S sont appeles respectivement "reste" et "quotient" de la division euclidienne de P par Q.*

Si $R = 0$, on a $P = Q.S$ et on dit que Q divise P et on note cette relation

$$Q|P.$$

12.3.1. Ensemble des racines d'un polynome. On rappelle que l'ensemble des racine d'un polynome est l'ensemble des zeros de sa fonction polynomiale:

$$\mathrm{Rac}_P(K) = \{x \in K,\ P(x) = 0_K\}.$$

PROPOSITION 12.8. *Soit P un polynome et $z \in K$, les deux enonces suivants sont equivalents:*

(1) $P(z) = 0$ (ie. z est une racine de P).

(2) Le polynome $X - z$ divise $P(X)$.

Preuve: Si $P(X) = (X - z)Q(X)$ on a

$$P(z) = (z - z).Q(z) = 0_K.$$

Reciproquement si $P(z) = 0$, divisons P par $X - z$: on a

$$P(X) = Q(X).(X - z) + R$$

avec R de degre $< \deg X - z = 1$ et donc R est constant (eventuellement nul). Mais

$$P(z) = 0 = Q(z).(z - z) + R = R$$

et donc $R = 0$ c'est a dire

$$P(X) = Q(X).(X - z).$$

□

On deduit de cette proposition le resultat fondamental suivant:

THÉORÈME 12.4. *Soit P un polynome non nul alors*

$$|\mathrm{Rac}_P(K)| \leqslant \deg P.$$

Preuve: Par recurrence sur $\deg P$: si P est constant non-nul c'est evident. Soit $z \in K$ une racine de $P(X)$(si il n'y en a pas on a fini: $|\mathrm{Rac}_P(K)| = 0$) alors

$$P(X) = (X - z).Q(X)$$

et (comme K est integre)

$$P(z') = 0 \Longleftrightarrow z' = z \text{ ou bien } Q(z') = 0$$

donc

$$\mathrm{Rac}_P(K) = \{z\} \cup \mathrm{Rac}_Q(K).$$

comme $\deg Q = d - 1$ on conclut par recurrence. □

COROLLAIRE 12.2. *Soit K un corps et $|K|$ son cardinal (eventuellement infini) alors l'application lineaire*

$$P(X) \in K[X]_{\deg P \leqslant |K|} \mapsto P(\bullet) \in \mathscr{F}(K; K)$$

est injective (tout polynome de degre $\leqslant |K|$ peut etre identifier avec une fonction polynomiale). En particulier si $\mathrm{car}K = 0$ *alors $|K| \geqslant |\mathbb{Q}| = \infty$ l'application*

$$P(X) \in K[X] \mapsto P(\bullet) \in \mathscr{F}(K; K)$$

est injective.

Preuve: Soit $P \in K[X]_{\deg P \leqslant |K|}$ dans le noyau: la fonction $x \in K \mapsto P(x) \in K$ est donc identiquement nulle. Alors P possede au moins $|K|$ racines et ce n'est possible que si P est le polynome nul. □

12.3.2. Application: Structure des ideaux de $K[X]$. On rappelle qu'un ideal $I \subset K[X]$ de l'anneau $K[X]$ est un sous $K[X]$-module contenu dans $K[X]$. Il verifie la condition de stabilite suivante:

$$\forall P, Q \in I,\ S \in K[X],\ P + S.Q \in I.$$

L'existence d'une division euclidienne permet une classification des ideaux de $K[X]$ entierement similaire a celle des sous -groupes de $\mathbb{Z}$.

THÉORÈME 12.5. *Soit $I \subset K[X]$ un ideal alors il existe $Q \in K[X]$ tel que*

$$I = K[X].Q(X) = \{S.Q,\ S \in K[X]\}$$

est l'ensemble des multiples de Q. De plus si on suppose Q unitaire alors Q est unique.

Preuve: Si $I = \{0\} = 0.K[X]$ on a fini. Si $I \not\{0\}$ soit $Q \in I - \{0\}$ un polynome non-nul de degre q minimal parmi les polynomes non-nuls de I. Soit $P \in I$. Par division euclidienne on peut ecrire

$$P = Q.S + R$$

avec $\deg R < q$. On a

$$R = P - Q.S \in I$$

(car $P, Q \in I$ et pour tout $S \in K[X]$, $S.Q \in I$ par definition d'un ideal) et donc $R \in I$. Par minimalite de q la seule possibilite est que $R = 0$ et donc $P = S.Q \in K[X].Q$. Si L est tel que $I = K[X].Q = K[X].L$ alors L est un multiple de Q (et Q est un multiple de L) et il n'existe qu'un seul multiple de Q qui soit unitaire. □

DÉFINITION 12.10. *Soit $I \subset K[X]$ un ideal non-nul alors l'unique polynome unitaire Q_I tel que*

$$I = (Q_I) = Q_I.K[X]$$

est appelle le generateur normalise de l'deal I. Si $I = \{0_K\}$ est l'ideal nul on posera

$$Q_I = 0_K.$$

Comme un noyau d'un morphisme d'anneau $\varphi : K[X] \mapsto A$ est un ideal on a:

COROLLAIRE 12.3. *Soit A un anneau et $\varphi : K[X] \mapsto A$ un morphisme d'anneaux. Alors il existe $Q \in K[X]$ tel que*

$$\ker(\varphi) = Q.K[X].$$

On notera le lien suivant entre inclusion d'ideaux et divisibilite

PROPOSITION 12.9. *Soient*

$$I = (P) = P.K[X] \text{ et } J = (Q) = Q.K[X]$$

des ideaux de $K[X]$ engendres par des polynome P et Q alors on a

$$I \subset J \Longleftrightarrow Q|P.$$

Preuve: En effet si $I \subset J$ alors $P \subset J = Q.K[X]$ et donc

$$P = Q.R,\ R \in K[X].$$

Reciproquement si $P = Q.R$ alors pour tout $L \in I$ on a pour $S \in K[X]$

$$L = P.S = Q.R.S \in Q.K[X] = J$$

et donc $I \subset J$. □

DÉFINITION 12.11. *Un anneau $\mathcal{A}$ que tout ideal $I \subset A$ est de la forme $I = q.\mathcal{A}$ pour $q \in \mathcal{A}$ est dit principal. Un anneau de polynomes sur un corps est donc principal.*

12.3.3. Decomposition en polynomes irreductibles.

DÉFINITION 12.12. *Un polynome $P(X) \in K[X]$ non constant est irreductible si les seuls diviseurs de P sont les multiples de 1 ou de P:*

$$Q|P \Longrightarrow Q = \lambda \text{ ou } Q = \lambda.P,\ \lambda \in K^{\times}.$$

De maniere equivalente: P est irreductible si et seulement si

$$Q|P \Longleftrightarrow \deg Q = 0 \text{ ou } P.$$

On notera $\mathscr{P} \subset K[X]$ l'ensemble de tous les polynomes irreductibles et $\mathscr{P}_u \subset \mathscr{P}$ l'ensemble de ceux qui sont unitaires.

REMARQUE 12.3.1. En effet si $Q|P$ et $\deg Q = \deg P$ alors $Q = \lambda.P$

PROPOSITION 12.10. *(Lemme de Gauss) Soit P irreductible, si $P|Q_1.Q_2$ alors $P|Q_1$ ou $P|Q_2$.*

Preuve: Ecrivons $Q_1.Q_2 = P.S$. Supposons que $P \not| Q_1$ et soit l'ideal

$$I = K[X].P + K[X].Q_1 \subset K[X].$$

l'ideal engendre par P et Q_1. On va montrer que $I = K[X]$. On a $I = D(X).K[X]$ pour D un polynome. Comme $P \in I$ on a $D|P$ mais cela implique que D est soit un scalaire non nul soit un multiple de P. Dans ce dernier cas $I = P.K[X]$ et comme $Q \in I$ on a $P|Q_1$ ce qu'on a exclut. Si D est un scalaire alors $I = K[X] \ni 1$ et il existe $A(X), B(X)$ tels que

$$A(X)P(X) + B(X)Q_1(X) = 1.$$

On a alors

$$Q_2 = 1.Q_2 = (A.P + B.Q_1).Q_2 = A.P.Q_2 + B.Q_1.Q_2 = P.(A.Q_2 + B.S).$$

□

THÉORÈME 12.6. *Soient Q un polynome non constant alors Q se factorise de maniere unique sous la forme*

$$Q = \lambda.P_1.\cdots.P_s$$

ou les P_i sont des polynomes irreductibles unitaires et $\lambda \in K^\times$. De plus cette factorisation est unique: Si on a deux telles factorisation en irreductibles (unitaires)

$$Q = \lambda.P_1.\cdots.P_s = \mu.R_1.\cdots.R_r$$

alors $s = r$, $\lambda = \mu$ et il existe une permutation $\sigma : \{1, \cdots r\} \mapsto \{1, \cdots s = r\}$ telle que

$$R_i = P_{\sigma(i)}.$$

Preuve: On va montrer la factorisation par recurrence sur $\deg Q$. Si $\deg Q = 1$ on a fini car Q est forcement irreductible et si $Q(X) = a.X + b, a, b \in K,\ a \neq 0$ et on a l'ecriture unique

$$Q = a(X + b/a).$$

Supposons $\deg Q = q+1$ et qu'on a le resultat pour tous les polynomes de degree $\leqslant q$. Si Q possede un diviseur Q_1 non-constant et non multiple de Q on a alors $1 < \deg Q_1 < q+1$ et

$$Q = Q_1.Q_2$$

avec $\deg Q_1, \deg Q_2 < q+1$. Sinon Q est irreductible et on a la factorisation

$$Q = a_{\deg Q}.Q_1,\ Q_1 = a_{\deg Q}^{-1}.Q.$$

Dans le cas precedent, on a par recurrence

$$Q_1 = \lambda_1.P_1.\cdots.P_{s_1},\ Q_2 = \lambda_2.P_{s_1+1}.\cdots.P_{s_1+s_2}$$

avec les P_i irreductibles unitaires et

$$Q = \lambda_1.\lambda_2.P_1.\cdots.P_{s_1}.P_{s_1+1}.\cdots.P_{s_1+s_2}.$$

Montrons l'unicite par recurrence sur $\deg Q$. Si $\deg Q = 1$ c'est immediat.

Dans le cas general soit

$$Q = \lambda.P_1.\cdots.P_s = \mu.R_1.\cdots.R_r$$

alors $P_s | \mu.R_1.\cdots.R_r$ et par le lemme de Gauss P_1 divise un des R_i. Ops que c'est R_r. comme est irreductible, unitaire et P_s est non constant unitaire on a $P_s = R_r$ et

$$Q = \lambda.P_1.\cdots.P_s = \mu.R_1.\cdots.R_{r-1}.P_s$$

et

$$0 = (\lambda.P_1.\cdots.P_{s-1} - \mu.R_1.\cdots.R_{r-1})P_s$$

et comme $K[X]$ est integre

$$\lambda.P_1.\cdots.P_{s-1} = \mu.R_1.\cdots.R_{r-1}$$

et on applique la recurrence. □

12.3.3.1. *Valuation.* Soit $Q(X) = a_q X^q + a_{q-1}X^{q-1} + \cdots + a_0$ un polynome de degre $q \geqslant 0$ ($a_q \neq 0$) alors la decomposition de Q en irreductibles peut se reecrire de maniere compacte

$$Q = a_q \prod_{P \in \mathscr{P}_u} P^{v_P(Q)}$$

ou

- P parcourt l'ensemble infini des polynome irreductible,
- les $v_P(Q) \geqslant 0$ sont des entiers nuls pour tous les P sauf un nombre fini,
- on a pose

$$P^0 := 1.$$

Ainsi, l'entier $v_P(Q)$ est l'exposant de la plus grande puissance du polynome irreductible P divisant Q.

DÉFINITION 12.13. *L'entier $v_P(Q)$ est appelle la valuation de Q en P ou la valuation P-adique de Q. Pour $Q = 0$ on pose $v_P(Q) = +\infty$.*

Ces valuations ont les proprietes suivantes

THÉORÈME 12.7. *Soient $Q, R \in K[X] - \{0\}$ de degres respectif q et r et de coefficient dominant a_q et b_r; on a*

(1) Pour tout $P \in \mathscr{P}_u$, on a

$$v_P(Q.R) = v_P(Q) + v_P(R)$$

et plus precisement

$$Q.R = a_q.b_r \prod_{P \in \mathscr{P}_u} P^{v_P(Q)+v_P(R)}.$$

(2) On a

$$Q|R \Longleftrightarrow \forall P \in \mathscr{P}_u,\ v_P(Q) \leqslant v_P(R)$$

(3) Pour tout P on a

$$v_P(Q + R) \geqslant \min(v_P(Q), v_P(R))$$

avec egalite si $v_P(Q) \neq v_P(R)$.

12.3.4. PGDC et PPMC. Soient $P, Q \in K[X] - \{0\}$. On a alors les deux ideaux:

$$(P) := K[X].P,\ (Q) := K[X].Q$$

et on peut alors former deux autres ideaux: leur intersection et leur somme

$$(P) \cap (Q) \subset (P), (Q) \subset (P) + (Q) = \langle P, Q\rangle \subset K[X].$$

12.3.4.1. *Le PGCD.* L'ideal engendre par P et Q est de la forme

$$\langle P, Q\rangle = (P) + (Q) = K[X].P + K[X].Q = R.K[X]$$

avec R unitaire. Alors comme $P, Q \in \langle P, Q\rangle$, R divise et P et Q: on a

$$R|P\ \&\ R|Q.$$

D'autre part si un polynome S divise a la fois P et Q alors

$$K[X].P + K[X].Q = R.K[X] \subset S.K[X]$$

et donc $S|R$. Ainsi R est le *Plus Grand Diviseur Commun* (unitaire) de P et Q au sens ou tout diviseur commun de P et Q doit diviser R.

DÉFINITION 12.14. *Soient $P, Q \in K[X] - \{0\}$, note*

$$(P, Q) := R$$

le generateur unitaire de l'ideal $(P)+(Q) = \langle P, Q\rangle$ et on l'appelle le PGCD de P et Q. En particulier si $(P, Q) = 1$ on dit que P et Q sont premiers entre eux.

REMARQUE 12.3.2. Si $Q = 0$ alors $(P, 0) = P_u$ est l'unique polynome unitaire qui est multiple de P.

PROPOSITION 12.11. *(Bezout) Soient P, Q des polynomes. Il existe $A, B \in K[X]$ tels que*

$$(P, Q) = A.P + B.Q.$$

En particulier, deux polynomes P et Q sont premiers entre eux ssi il existe $A, B \in K[X]$ tels que

$$1 = A.P + B.Q.$$

Preuve: On a

$$(P) + (Q) = (P, Q).K[X] = P.K[X] + Q.K[X].$$

En particulier (P, Q) est de la forme

$$(P, Q) = P.A + Q.B.$$

Supposons qu'il existe A, B tels que $1 = A.P + B.Q$ alors $(P) + (Q)$ contient 1 et donc $1.K[X] = K[X]$ de sorte que $(P) + (Q) = K[X]$.

□

12.3.4.2. *Le PPCM.* Soit l'intersection $(P) \cap (Q) \subset K[X]$. C'est un ideal non-nul car il contient le produit $P.Q$. Il est donc de la forme $(P) \cap (Q) = K[X].S$ avec S unitaire. On a donc

$$P|S \& Q|S$$

et S est un multiple commun a P et a Q. De plus si $P|T$ et $Q|T$ alors

$$T \in K[X].P \cap K[X].Q = K[X].S$$

et $S|T$. Ainsi S est le *Plus Petit Multiple Commun* (unitaire) de P et Q.

DÉFINITION 12.15. *Soient $P, Q \in K[X] - \{0\}$, note*

$$[P, Q] := R$$

le generateur unitaire de l'ideal $(P) \cap (Q)$ et on l'appelle le PPCM de P et Q.

PROPOSITION 12.12. *(Formule du produit) Soient $P, Q \in K[X] - \{0\}$ et unitaires. On a*

$$P.Q = [P, Q](P, Q).$$

12.3.4.3. *Generalisation a un nombre arbitraires de polynomes.*

DÉFINITION 12.16. *Soient $P_1, \cdots, P_k$ des polynomes alors leur PGCD et leur PPCM notes*

$$(P_1, \cdots, P_k) \text{ et } [P_1, \cdots, P_k]$$

sont respectivement les generateurs unitaires des ideaux

$$(P_1) + \cdots + (P_k) \text{ et } (P_+) \cap \cdots \cap (P_k).$$

En particulier si

$$(P_1, \cdots, P_k)$$

on dit que $P_1, \cdots, P_k$ sont premiers dans leur ensemble.

REMARQUE 12.3.3. On a

$$(P_1, \cdots, P_k)|(P_1, P_2)$$

car

$$(P_1) + (P_2) \subset (P_1) + \cdots + (P_k).$$

12.3.4.4. *PGDC, PPMC et decomposition en irreductibles.*

THÉORÈME 12.8. *Soient Q, R des polynomes non-nuls de degres q et r et*

$$Q = a_q. \prod_{P \in \mathscr{P}_u} P^{v_P(Q)}, \ R = b_r. \prod_{P \in \mathscr{P}_u} P^{v_P(R)}$$

leur decompositions en polynomes irreductible unitaires alors

$$(Q, R) = \prod_{P \in \mathscr{P}_u} P^{\min(v_P(Q), v_P(R))}, \ [Q, R] = \prod_{P \in \mathscr{P}_u} P^{\max(v_P(Q), v_P(R))}.$$

Preuve: Exercice. □

12.3.5. Un critere d'irreductibilite.

THÉORÈME 12.9. *Soit A un anneau et $\varphi : K[X] \mapsto A$ un morphisme d'anneaux non-nul. Soit $B = \varphi(K[X]) \subset A$ son image et $\ker\varphi = Q.K[X]$. Alors on a*

$$Q \text{ est irreductible } \iff B \text{ est un corps}$$

Preuve: Soit $b = \varphi(P) \in B - \{0\}$. Supposons P irreductible. Considerons l'ideal $I = \langle P, Q\rangle = K[X].P + K[X].Q$ alors $I = K[X]$: en effet ecrivons$P, Q \in I = K[X].R$ et on doit avoir $R|P$ et $R|Q$. Si $R|P$ alors R est constant non-nul ou de la forme $\lambda.P$. Dans le second car on aurait $I = K[X].P = \ker\varphi$ ce qui contredit le fait que $b' \neq 0$. On a donc $I = K[X]$ et il existe $U, V \in K[X]$ tels que

$$U.P + V.Q = 1$$

et alors

$$1_A = \varphi(U.P + V.Q) = \varphi(U).\varphi(P) + \varphi(V).\varphi(Q) = \varphi(V).\varphi(Q) = \varphi(V).b$$

et b est inversible. □

12.3.6. Construction de sous-algebres. Soit $\mathcal{M}$ une K-algebre (pas forcement commutative, par exemple $\mathrm{End}(V)$ ou $M_d(K)$) d'unite $1_{\mathcal{M}}$ et $M \in \mathcal{M}$ un element. On associe a M une application (dite d'evaluation en M)

$$\mathrm{ev}_M : \begin{array}{ccc} K[X] & \mapsto & \mathcal{M} \\ P(X) & \mapsto & P(M) \end{array}$$

ou

$$P(M) = a_0.M^0 + a_1.M + \cdots + a_n.M^n + \cdots + a_d.M^d.$$

On a pose $M^0 = 1_{\mathcal{M}}$ et

$$M^n = M.M\cdots.M(n \text{ fois}).$$

PROPOSITION 12.13. *Cette application est un morphisme d'algebre: on a*

$$(\lambda.P + Q)(M) = \lambda.P(M) + Q(M),\ (P.Q)(M) = P(M).Q(M).$$

On notera l'image de cette aplication par

$$K[M] = \mathrm{ev}_M(K[X]) = \{P(M),\ P \in K[X]\}.$$

C'est une sous-algebre (un sous-anneau et un SEV) commutative de $\mathcal{M}$: l'algebre des polynomes en M.

Preuve: On ne fait que la multiplication:

$$P(M).Q(M) = (a_0.M^0 + a_1.M + \cdots + a_d.M^d).(b_0.M^0 + b_1.X + \cdots + b_d.M^d) =$$
$$\sum_{p,q\leqslant d} a_p.M^p.b_q.M^q = \sum_{p,q\leqslant d} a_p.b_q.M^{p+q} = \sum_{n\leqslant d+d'} (\sum_{p+q=n} a_p.b_q)M^n = (P.Q)(M)$$

ici on a utilise les proprietes des lois de composition de $\mathcal{M}$ (associativite, distributivite) et le fait (valable meme si $\mathcal{M}$ n'est pas commutative) que

$$a_p.M^p.b_q.M^q = a_p.b_q.M^p.M^q = a_p.b_q.M^{p+q}.$$

L'agebre $K[M]$ est commutative car $K[X]$ l'est:

$$P(M).Q(M) = (P.Q)(M) = (Q.P)(M) = Q(M).P(M).$$

□

EXERCICE 12.1. Montrer que $K[M]$ est la plus petite sous-algebre de $\mathcal{M}$ contenant M: c'est l'algebre engendree par M. On dit que $K[M]$ est monogene car elle est engendre par un seul element.

EXERCICE 12.2. Soit $\mathcal{M}$ de dimension finie et $M \in \mathcal{M}$. Soit $K[X]_{\leqslant d}$ le sous-espace vectoriel des polynomes de degree $\leqslant d$.

(1) Montrer que si $d > \dim \mathcal{M}$ il existe un polynome non-nul $P(X) = a_0 + a_1.X + \cdots + a_d.X^d$ de degree $\leqslant d$ tel que $P(M) = 0_d$.
(2) Montrer que si $P(0) = a_0 \neq 0$ alors M est inversible et en fait $M^{-1} = Q(M)$ avec $Q \in K[X]_{\leqslant d-1}$.