Algèbre Linéaire Avancée (1er Semestre)[1]

Philippe Michel

[1]Tuesday 3rd November, 2020, 09:14

Table des matieres

Introduction 5

Chapitre 1. Le language des ensembles 7
1. Ensembles 7
2. Operations sur les ensembles 9
3. Applications entre ensembles 11
4. Cardinal d'un ensemble 17

Chapitre 2. Groupes 21
1. Le cas du groupe symetrique 21
2. Groupes abstraits 23
3. Sous-groupes 26
4. Morphismes de groupes 29

Chapitre 3. Anneaux et Modules 37
1. Anneaux 37
2. Modules sur un anneau 42

Chapitre 4. Corps 49
1. Corps 49
2. Corps des fractions 49
3. Caracteristique d'un corps, Sous-corps premier 52

Chapitre 5. Espaces Vectoriels 55
1. Un changement de terminologie 55
2. Famille generatrice, libre, base 58
3. Espaces vectoriels de dimension infinie 64

Chapitre 6. Applications lineaires 67
1. Le Theoreme Noyau-Image 67
2. Structure et dimension des espaces d'applications lineaires 69

Chapitre 7. Matrices 75
1. Matrices et applications lineaires 75
2. L'algebre des matrices carrees 83
3. Changement de base 85

Chapitre 8. Interlude: le corps des nombres complexes 89
1. L'algebre des nombres complexes 89
2. Proprietes de base des nombres complexes 90
3. Le plan complexe 93

4. Equations polynomiales complexes 93

Chapitre 9. Operations elementaires sur les matrices 95
1. Operation elementaires sur les lignes 95
2. Echelonnage 97

Chapitre 10. L'anneau des polynomes sur un corps 99
1. Les polynomes sont des suites 99
2. Structure d'anneau 100
3. Division et factorisation 101

Chapitre 11. Determinant 107
1. Formes multilineaires 107
2. Le Theoreme de Cayley-Hamilton 107

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

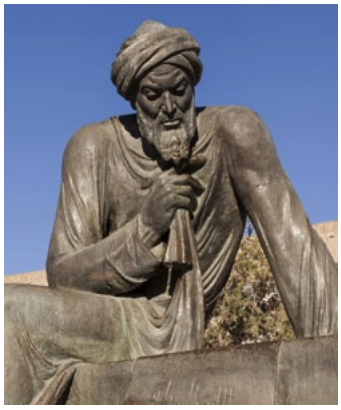
Kitab al-mukhtasar fi hisab al-jabr wa-l-muqabala

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. 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. 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. 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.

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

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

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

1.2. 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. *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.

2. Operations sur les ensembles

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

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

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 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.

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
$$\forall a, a', a'' \in A,\ a\mathcal{R}a' \text{ et } a'\mathcal{R}a'' \Longleftrightarrow a\mathcal{R}a''.$$
- $\mathcal{R}$ est une relation d'equivalence si elle est reflexive, symetrique et transitive.

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

$$f : X \mapsto Y.$$

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).

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

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

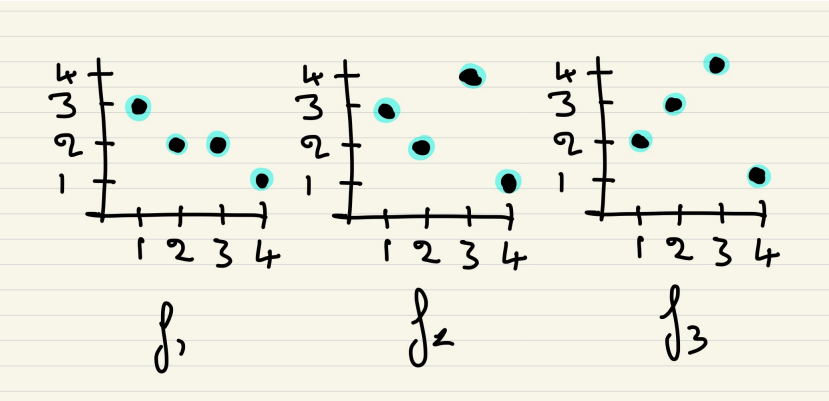


FIGURE 1. Graphes de f_1, f_2, f_3.

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.

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 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 $f(f^{-1}(B))$?

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 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 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.*

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 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.

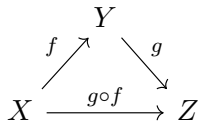
EXEMPLE 3.3. On a

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

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)

$$\circ : \begin{array}{ccc} \mathrm{Hom}_{ENS}(X,Y) \times \mathrm{Hom}_{ENS}(Y,Z) & \mapsto & \mathrm{Hom}_{ENS}(X,Z) \\ (f,g) & \mapsto & g \circ f \end{array} \tag{3.1}$$

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

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

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

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

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.

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 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".

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

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 (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.

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

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

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. 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 2.1. 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. 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

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

Dememe 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. *Soit G un groupe. On a*

- *Involutivite de l'inversion: $\forall g,\ (g^{-1})^{-1} = g,\ g^{-1} \star g = e_G$.*
- *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 $e'_G \star g' = e'_G$.*
- *Unicite de l'inverse: si $g' \in G$ verifie $g \star g' = e_G$ alors $g' = g^{-1}$.*
- *On a $(g \star g')^{-1} = {g'}^{-1} \star g^{-1}$.*

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

Pour le dernier point on a

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

et donc (par unicite de l'inverse)

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

2.1. Exemples de groupes.

- 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.
- 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.
- 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).
- 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.
- 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,
- de meme que le sous-ensemble $\mathbb{Z}^\times := \{\pm 1\}$ muni des memes structures.

– 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

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

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

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

$$g^0=e_G \tag{2.1}$$

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 $m,n\in\mathbb{Z}$

$$g^{m+n}=g^m\star g^n. \tag{2.2}$$

On a alors defini une fonction

$$\exp_g:\begin{array}{ccc}\mathbb{Z}&\mapsto&G\\ n&\mapsto&\exp_g(n)=g^n\end{array} \tag{2.3}$$

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. 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 $\sigma\circ\tau=\tau\circ\sigma$.

2.2.1. *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 $n \geqslant 1$,

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

de sorte que (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.

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 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):

(1) En prenant $h' = h$, on a $h \star h^{-1} = e_G \in H$ donc H contient l'element neutre.
(2) En applicant $h \star h'^{-1} \in H$ avec $h = e_G$ on a que si $h' \in H$ alors $h'^{-1} \in H$.
(3) 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 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.*

3.1. Groupe engendre par un ensemble.

PROPOSITION 2.3. *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. *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 3.2. Soit $g \in G$ alors le sous-groupe engendre par g, $\langle\{g\}\rangle$ vaut

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

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. *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 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. *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. *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

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

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

PROPOSITION 2.6. *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" ...)

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

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 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

$$Z(G).$$

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"

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 1.1.

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

(2) Si A est un anneau de lois $+, .$ le singleton

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

est un anneau (l'anneau "nul" ou trivial) d'unite

$$1_{\mathrm{Nul}(A)} = 0_A.$$

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

(4) Soit

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

(5) 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.

(6) 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).

(7) 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

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

(8) 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

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

(9) (Produits d'anneaux) Soient a et B des anneaux alors le produit $A\times B$ muni de l'addition et de la multiplication

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

est un anneau avec $(0_A, 0_B)$ comme element neutre et $(0_A, 0_B)$ 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. Exercice 5 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:

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

et $-\varphi$ est encore un morphisme d'anneaux.

(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.

1.1. Elements inversibles.

Définition 3.2. *Un element 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).

Exercice 3.2. Montrer que si a est inversible et que b' est un inverse de a, on a $b' = b$

Ainsi, l'inverse d'un element $a \in A$ si il existe est unique. On le notera

$$a^{-1}.$$

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

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

Proposition 3.1. *Soit $A^\times$ l'ensemble des elements inversibles, alors*

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

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

Remarque 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 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 parle 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 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 3.3. 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 et

$$M^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Montrer que

$$M.M^* = M^*.M = \det(M)\mathrm{Id}_2$$

et en deduire que

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

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 $\{0_B\}$,*
- *soit qui contient l'unite 1_A et qui est stable par .:*

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

Ainsi $(B, +, .)$ est un anneau.

LEMME 3.2. *(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*

$$\forall b, b', b'' \in B,\ b.b' - b'' \in B \tag{1.1}$$

Preuve: Exercice. □

EXEMPLE 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

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

est un sous-anneau de $M_2(\mathbb{R})$.
(3) Plus generalement $A.\mathrm{Id} \subset M_2(A)$ 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.

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

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

On note $\mathrm{Hom}_{Ann}(A,B)$ l'ensemble des morphismes d'anneaux. On note

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

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 3.4. On a deja vu que c'est un morphisme de groupe (pour l'addition). Verifier que c'est un morphisme d'anneaux.

1.4. Noyau, Image.

Proposition 3.2. *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 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 3.3. *Un morphisme d'anneaux $\varphi \in \mathrm{Hom}_{Ann}(A,B)$ est injectif ssi $\ker(\varphi) = \{0_A\}$.*

PROPOSITION. *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 3.1. *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 3.5. L'ensemble des automorphismes $\mathrm{Aut}_{Ann}(A)$ muni de la composition forme un sous-groupe de $\mathrm{Bij}(A)$.

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 3.6. 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 2.1. (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 structure 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 $d = 1$– 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:*
$$\forall a \in A,\ b, b' \in B\ a * (b._B b') = (a * b)._B b'.$$

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

Lemme 3.3. *(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*
$$\forall a \in A,\ n, n' \in N,\ a * n + n' \in N. \tag{2.1}$$

Preuve: Pour tout $n, n' \in N$, et applicant la condition (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 (2.1)
$$a * n + 0_M = a * n \in N.$$

□

Exemple 2.2. (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.

Un exemple important de A-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 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 2.3. Soit $\varphi : A \mapsto B$ un morphisme d'anneaux alors $\ker(\varphi)$ est un ideal de A.

2.2. Module engendre par un ensemble.

PROPOSITION 3.4. *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 3.5. *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 2.4. (1) Soit A^d le A-module libre de rang d. La famille suivante est generatrice de A^d (on pose $1 = 1_A, 0 = 0_A$)

$$\mathcal{B}_0 := \{\mathbf{e}_1 = (1, 0, \cdots, 0),\ \mathbf{e}_2 = (0, 1, 0, \cdots, 0), \cdots, \mathbf{e}_d = (0, 0, \cdots, 1)\}$$

($\mathbf{e}_i$ 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

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

On appelle la famille $\mathcal{B}_0$ *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 3.7. Soient $u_1, \cdots, u_d \in A^\times$ des elements inversibles. Montrer que la famille suivante est generatrice de A^d

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

EXERCICE 3.8. 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).

2.3. 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 2.1. Cela 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 3.4. *(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*

$$\forall a \in A,\ m, m' \in M,\ \varphi(a *_M m + m') = a *_N \varphi(m) + \varphi(m'). \tag{2.2}$$

Preuve: On applique (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

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

□

2.4. Noyau, Image.

PROPOSITION 3.6. *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 φ est injective ssi* $\ker(\varphi) = \{0_M\}$.

2.5. Structure des espaces de morphismes.

NOTATION 3.2. *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 3.7. *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 3.8. *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 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:

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

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 multilplication 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 $a.a' = a'.a$. □

2.6. 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 $\mathrm{Aut}_{A-mod}(M)$; de plus, si A est commutatif, $\mathrm{End}_{A-mod}(M)$ possede une structure naturelle de A-module qui en fait une A-algebre.*

$\mathrm{End}_{A-mod}(M)$ est appellee

l'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 endomorphisme 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 anneaz une A-algebre. □

DÉFINITION 3.13. *Soient M et N deux A-modules, on dit que M et N sont isomorphes si $\mathrm{Iso}_{A-mod}(M, N) \neq \emptyset$, est a dire si il existe un morphisme bijectif de A-modules*

$$\varphi : M \simeq N.$$

Du point de vue de la structure deux module isomorphes peuvent etre identifies l'un a l'autre ainsi que les differents objects qui leurs sont attaches; en particulier on a

THÉORÈME 3.2. *Soient $M \simeq N$ des modules isomorphes alors $\mathrm{End}_{A-mod}(M)$ et $\mathrm{End}_{A-mod}(N)$ sont des anneaux isomorphes (et des A-algebres isomorphes si A est commutatif).*

Preuve: Soit $\varphi_0 : M \simeq N$ un isomorphisme. Considerons l'application composee

$$\mathrm{Ad}_{\varphi_0} : \varphi \in \mathrm{End}_{A-mod}(M) \mapsto \mathrm{Ad}_{\varphi_0}(\varphi) := \varphi_0 \circ \varphi \circ \varphi_0^{-1}.$$

c'est une application de N vers N:

$$\mathrm{Ad}_{\varphi_0}(\varphi) : N \xrightarrow{\varphi_0^{-1}} M \xrightarrow{\varphi} M \xrightarrow{\varphi_0} N$$

de plus c'est la composee de morphismes de A-modules bijectif et donc c'est un morphismes de A-modules bijectif : ainsi

$$\mathrm{Ad}_{\varphi_0} : \mathrm{End}_{A-mod}(M) \mapsto \mathrm{End}_{A-mod}(N).$$

Montrons que c'est une application bijective en exhibant une application reciproque: par le meme raisonnement on a

$$\mathrm{Ad}_{\varphi_0^{-1}} : \psi \in \mathrm{End}_{A-mod}(N) \mapsto \varphi_0^{-1} \circ \psi\varphi_0 \in \mathrm{End}_{A-mod}(M)$$

et la composee (un application de $\mathrm{End}_{A-mod}(N)$ vers $\mathrm{End}_{A-mod}(N)$) verifie pour tout $\psi \in \mathrm{End}_{A-mod}(N)$,

$$\mathrm{Ad}_{\varphi_0} \circ \mathrm{Ad}_{\varphi_0^{-1}} : \psi \mapsto \varphi_0 \circ \varphi_0^{-1} \circ \psi \circ \varphi_0^{-1} \circ \varphi_0 = \psi$$

et donc

$$\mathrm{Ad}_{\varphi_0} \circ \mathrm{Ad}_{\varphi_0^{-1}} = \mathrm{Id}_{\mathrm{End}_{A-mod}(N)}$$

et de meme

$$\mathrm{Ad}_{\varphi_0^{-1}} \circ \mathrm{Ad}_{\varphi_0} = \mathrm{Id}_{\mathrm{End}_{A-mod}(M)}.$$

Ainsi Ad_{φ_0} est bijective de reciproque $\mathrm{Ad}_{\varphi_0}^{-1} = \mathrm{Ad}_{\varphi_0^{-1}}$

Pour conclure il reste a montrer que Ad_{φ_0} est un morphisme d'anneaux (et de A-algebres si A est commutatif):

$$\mathrm{Ad}_{\varphi_0}(\mathrm{Id}_M) = \varphi_0 \circ \mathrm{Id}_M \circ \varphi_0^{-1} = \varphi_0 \circ \varphi_0^{-1} = \mathrm{Id}_M;$$

on doit egalement montrer que pour $\varphi, \phi \in \mathrm{End}_{A-mod}(M)$ et $a \in A$ on a

$$\mathrm{Ad}_{\varphi_0}(a * \varphi + \phi) = a * \mathrm{Ad}_{\varphi_0}(\varphi) + \mathrm{Ad}_{\varphi_0}(\phi)$$

et que

$$\mathrm{Ad}_{\varphi_0}(\varphi \circ \phi) = \mathrm{Ad}_{\varphi_0}(\varphi) \circ \mathrm{Ad}_{\varphi_0}(\phi).$$

Montrons la premiere egalite (la seconde est laissee en exercice): soit $n \in N$, et $m = \varphi_0^{-1}(n)$

$$\mathrm{Ad}_{\varphi_0}(a * \varphi + \phi)(n) = \varphi_0((a * \varphi + \phi)(\varphi_0^{-1}(n))) = \varphi_0((a * \varphi + \phi)(m)) = \varphi_0(a * \varphi(m) + \phi(m))$$

et par linearite de φ_0 on a

$$\begin{aligned} \mathrm{Ad}_{\varphi_0}(a * \varphi + \phi)(n) &= a * \varphi_0(\varphi(m)) + \varphi_0(\phi(m)) = a * \varphi_0(\varphi(\varphi_0^{-1}(n))) + \varphi_0(\phi(\varphi_0^{-1}(n))) \\ &= a * \mathrm{Ad}_{\varphi_0}(\varphi)(n) + \mathrm{Ad}_{\varphi_0}(\phi)(n). \end{aligned}$$

□

CHAPITRE 4

Corps

"Le corps conditionnne le raisonnement."

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

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

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*

$$\forall a, b \in A,\ a.b = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0. \tag{2.1}$$

Preuve: A est commutatif car K est commutatif. Pour (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 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 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* $\mathrm{Frac}(A)$.

EXERCICE 4.1. Soient A un anneau integre. Montrer que tout morphisme d'anneau $\varphi : A \mapsto K'$ non-nul et a valeurs dans un corps K' est injectif.

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*

$$\mathrm{car}(K).$$

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 $\mathbb{Q}$.

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 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).

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 $C_p^k = p.c_{p,k}$.*

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*

$$\mathrm{frob}_p : x \in K \mapsto x^p \in K.$$

PROPOSITION 4.4. *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: Exercice. □

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."

1. Un changement de terminologie

Tout comme les corps sont des cas particuliers d'anneau, 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 1.1.
(1) L'espace vectoriel nul $\{0_K\}$.
(2) K est un espace vectoriel sur lui-meme.
(3) Si V et W sont de K-ev leur produit

$$V \times W = \{(v, w),\ v \in V,\ w \in W\}$$

muni de l'addition

$$(v, w) + (v', w') := (v +_V v', w +_W w')$$

et de la mutliplication externe

$$x.(v, w) := (x.v, x.w)$$

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 precedent 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

$$\vec{0}_d = (0, \cdots, 0).$$

(5) Si X est un ensemble, $\mathcal{F}(X; K) = K^X$ a une structure de K-espace vectoriel.
(6) Plus generalement si V est un K-espace vectoriel et X est un ensemble, $\mathcal{F}(X; V) = V^X$ 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.

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 1.2.
- $\{0_V\}, V \subset V$.
- 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.

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 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. *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.*

1.3. Sous-espace engendre par un sous-ensemble. On rappelle egalement que

PROPOSITION 5.5. *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*

$$\langle\mathscr{F}\rangle=\mathrm{Vect}(\mathscr{F})=\mathrm{CL}_K(\mathscr{F})\subset V$$

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*

$$\mathrm{CL}_K(\mathscr{F}):=\{\sum_{i=1}^n \lambda_i.x_i,\ n\geqslant 1,\ \lambda_1,\cdots,\lambda_n\in K,\ x_1,\cdots,x_n\in\mathscr{F}\}.$$

Cette notion admet des cas particuliers.

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 $X \times Y$.

2. Famille generatrice, libre, base

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

$$v = \sum_{i=1}^{n} x_i \mathbf{e}_i, \tag{2.1}$$

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 5.2. *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 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

$$\begin{aligned} CL(\lambda.\vec{x} + \vec{y}) &= CL(\lambda.x_1 + y_1, \cdots, \lambda.x_d + y_d) = (\lambda.x_1 + y_1)\mathbf{e}_1 + \cdots + (\lambda.x_d + y_d)\mathbf{e}_d \\ &= \lambda.x_1.\mathbf{e}_1 + y_1.\mathbf{e}_1 + \cdots + \lambda.x_d.\mathbf{e}_d + y_d.\mathbf{e}_d \\ &= \lambda.(x_1.\mathbf{e}_1 + \cdots + x_d.\mathbf{e}_d) + (y_1.\mathbf{e}_1 + \cdots + y_d.\mathbf{e}_d) \\ &= \lambda.CL(\vec{x}) + CL(\vec{y}). \end{aligned}$$

□

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 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 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 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 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 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 5.3. *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.

□

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

$$|\mathscr{B}| = \dim(V). \tag{2.2}$$

En particulier

$$\dim(K^d) = d.$$

DÉFINITION 5.10. *Soit $\mathcal{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ 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 5.4. *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.

□

Remarque 2.4. On a demontre dans la deuxieme partie un resultat un peu plus fort:

Théorème (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 $V = X \oplus Y$,

$$\dim(V) = \dim(X) + \dim(Y).$$

2.4. Sous-espaces vectoriels et dimension.

THÉORÈME 5.5. *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.

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

$$v = x_1\mathbf{e}_1 + \cdots + x_d\mathbf{e}_d. \tag{3.1}$$

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*

$$x_1\mathbf{e}_1 + \cdots + x_d\mathbf{e}_d = 0_V \Longleftrightarrow x_1 = \cdots = x_d = 0_K. \tag{3.2}$$

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 $f : \mathbb{N} \mapsto \mathbb{R}$

$$\mathrm{supp}(f) = \{n \in \mathbb{N},\ f(n) = 0\} \text{ est fini.}$$

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. *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 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 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

1. Le Theoreme Noyau-Image

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*

$$\varphi(\mathscr{G}) = \{\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_g)\} \subset W$$

est une famille generatrice de $\mathrm{Im}(\varphi)$ *et on a*

$$\dim(\mathrm{Im}\,\varphi) \leqslant \dim(V).$$

Preuve: Soit $w \in \mathrm{Im}(\varphi)$, il existe $v \in V$ tel que $\varphi(v) = w$. 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

$$w = \varphi(v) = x_1.\varphi(\mathbf{e}_1) + \cdots + x_g\varphi(\mathbf{e}_g)$$

Ainsi $\varphi(\mathscr{G})$ est generatrice de $\mathrm{Im}\,\varphi$ et on a

$$|\varphi(\mathscr{G})| \geqslant \dim(\mathrm{Im}\,\varphi).$$

En particulier si $\mathscr{G}$ est une base, on a

$$\dim(V) = |\mathscr{G}| \geqslant |\varphi(\mathscr{G})| \geqslant \dim(\mathrm{Im}\,\varphi).$$

□

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 1.1. On a

$$\mathrm{rg}(\varphi) \leqslant \min(\dim V, \dim W).$$

En effet $\mathrm{rg}(\varphi)$ est la dimension d'un espace engendre par au plus $\dim(V)$ elements donc $\mathrm{rg}(\varphi) \leqslant \dim V$ et c'est la dimension d'un espace contenu dans un autre de dimension $\dim(W)$ 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.

1.2. Le Theoreme Noyau-Image.

THÉORÈME 6.1. *Soit $\varphi : V \mapsto W$ une application lineaires avec V de dimension finie. On a*

$$\dim V = \dim(\ker \varphi) + \dim(\mathrm{Im}\, \varphi).$$

Preuve: Notons que si $\mathscr{B}$ est une base alors $\varphi(\mathscr{B})$ est une partie generatrice de $\mathrm{Im}\, \varphi$ qui est donc de dimension finie de dimension

$$\dim \mathrm{Im}\, \varphi \leqslant |\varphi(\mathscr{B})| \leqslant |\mathscr{B}| = \dim(V).$$

Soit $\{\varphi(\mathbf{e}'_1), \cdots, \varphi(\mathbf{e}'_r)\}$ une base de $\mathrm{Im}\, \varphi$ 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 $\dim(V) = \dim(\mathrm{Im}\, \varphi)$ et donc $\dim(\mathrm{Im}\, \varphi) = \dim(W)$ ce qui implique que $W = \mathrm{Im}\, \varphi$ et la surjectivite et la bijectivite.

Si φ est surjective $\dim(\mathrm{Im}\, \varphi) = \dim(W) = \dim(V)$ et donc $\dim(\ker \varphi) = 0$ ce qui implique l' injectivite et la bijectivite. □

COROLLAIRE 6.2. *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)

$$\dim(V) = 0 + \dim(\mathrm{Im}\, \varphi) = \dim(W).$$

□

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.*

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. *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 $\mathrm{Hom}_K(V, W)$.

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. Les coordonnees de ℓ dans la base $\mathscr{B}^*$ sont donnees par les $(\ell(\mathbf{e}_i))_{i \leqslant d}$ (autrement dit par les valeurs de ℓ en les $\mathbf{e}_i$).*

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 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 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.

2.1.1. *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

$$\varphi^*(\ell) := \ell \circ \varphi : \begin{array}{ccc} V & \mapsto & K \\ v & \mapsto & \ell(\varphi(v)) \end{array}$$

EXERCICE 6.4. Montrer que l'application φ^* est lineaire.

2.2. 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 6.4. *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.

2.3. Une base de $\mathrm{Hom}(V,W)$**.** Soient V et W des EV 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 $\mathrm{Im}\,\mathcal{E}_{ij} \subset K.\mathbf{f}_i$ et comme $\mathcal{E}_{ij}(\mathbf{e}_j) = \mathbf{f}_i$ on a egalite. Ainsi $\mathrm{rg}(\mathcal{E}_{ij}) = 1$ ($\mathbf{f}_i \neq 0_W$, 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. *La famille d'applications lineaires*

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'} := \{\mathcal{E}_{ij},\ i \leqslant d',\ j \leqslant d\} \subset \mathrm{Hom}_{K-ev}(V,W)$$

forme une base de $\mathrm{Hom}_{K-ev}(V,W)$.

Preuve: Comme le cardinal de cette famille vaut $\dim(V)\dim(W) = \dim \mathrm{Hom}_{K-ev}(V,W)$ 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 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 $\mathscr{B}'$.

2.4. 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

$$\mathcal{B}_{\mathscr{B},\mathscr{B}'} = \{\mathcal{E}_{ij} = \mathbf{e}_j^*.\mathbf{f}_i,\ i \leqslant d',\ j \leqslant d\} \subset \mathrm{Hom}_{K-ev}(V, W)$$

la base de l'espace des application lineaires formee des applications elementaires.

PROPOSITION 6.5. *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 6.6. *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

$$y_i = \sum_{j\leqslant d} m_{ij}.x_j.$$

□

2.5. Combinaison lineaire d'applications lineaires.

PROPOSITION 6.7. *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 $\mathcal{B}_{\mathscr{B},\mathscr{B}'}$. □

2.6. 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

$$l_{ik} = \sum_{j\leqslant d'} m_{ij}n_{jk}.$$

□

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.

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

$$CL_{\mathcal{B}_{\mathscr{B},\mathscr{B}'}} : (m_{ij})_{i\leqslant d', j\leqslant d} \in (K^{d'})^d \mapsto \varphi = \sum_{i\leqslant d', j\leqslant d} m_{ij}\mathcal{E}_{ij} \in \mathrm{Hom}(V, W) \tag{1.1}$$

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 coefficient 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 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 $\varphi(\mathbf{e}_j)$ dans la base $\mathscr{B}'$: ie.

$$\varphi(\mathbf{e}_j) = \sum_{1\leqslant i\leqslant d'} m_{ij}(\varphi)\mathbf{f}_i.$$

EXEMPLE 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

$$\mathrm{Mat}_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_V) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = (\delta_{i=j})_{i,j} =: \mathrm{Id}_d \in M_{d\times d}(K). \tag{1.2}$$

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.

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

$$E_{ij,kl} = \delta_{k=i}.\delta_{l=j}.$$

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 $\mathrm{Lig}_d(K)$.

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)

$$\mathrm{Col}_j(M) = \begin{pmatrix} m_{1j} \\ m_{2j} \\ \vdots \\ m_{d'j} \end{pmatrix} \in \mathrm{Col}_{d'}(K),\ \textit{resp.}\ \mathrm{Lig}_i(M) = \begin{pmatrix} m_{i1} & m_{i2} & \cdots & m_{id} \end{pmatrix} \in \mathrm{Lig}_d(K)$$

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.

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

$$L = (l_{ik})_{i \leqslant d'', k \leqslant d} \in M_{d'' \times d}(K) \text{ avec } l_{ik} = \sum_{j=1}^{d'} m_{ij}.n_{jk}.$$

Exemple 1.2. Quelques cas particuliers importants:

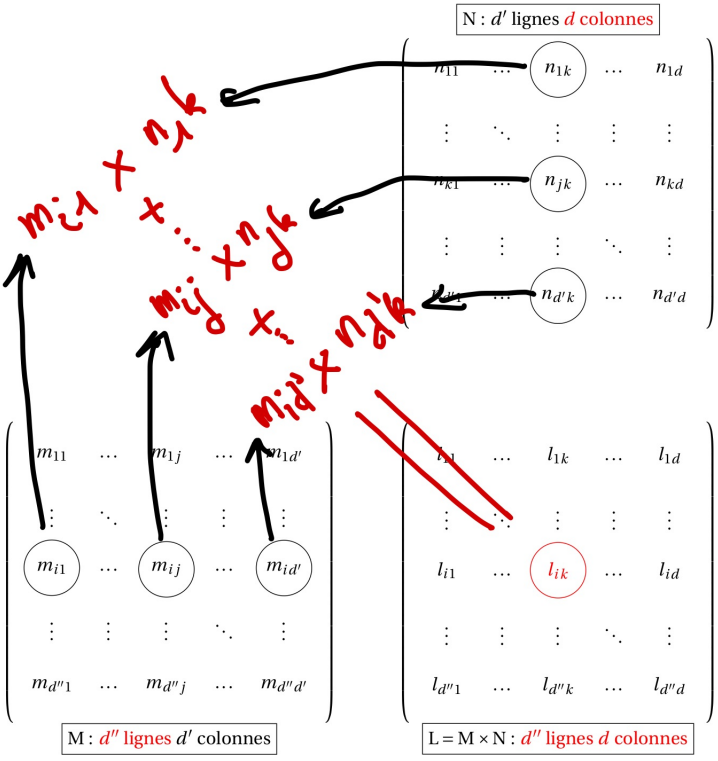


FIGURE 1. Calcul des coordonnees du produit de deux matrices

– 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. *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

$$\mathrm{Mat}_{\mathscr{B}'',\mathscr{B}}(\psi \circ \varphi) = \mathrm{Mat}_{\mathscr{B}'',\mathscr{B}'}(\psi).\mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\varphi) \tag{1.3}$$

Autrement dit on a

$$\begin{pmatrix} l_{11} & \cdots & l_{1d} \\ l_{21} & \cdots & l_{2d} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ l_{d''1} & \cdots & l_{d''d} \end{pmatrix} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d'} \\ m_{21} & m_{22} & \cdots & m_{2d'} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{d''1} & m_{d''2} & \cdots & m_{d''d'} \end{pmatrix} . \begin{pmatrix} n_{11} & \cdots & n_{1d} \\ n_{21} & \cdots & n_{2d} \\ \vdots & \cdots & \vdots \\ n_{d'1} & \cdots & n_{d'd} \end{pmatrix}$$

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

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ \vdots \\ y_{d'} \end{pmatrix} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix}$$

1.2.2. *Le cas des isomorphismes.* On consider 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

$$\mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_U).\mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_U) = \mathrm{Id}_d. \tag{1.4}$$

Preuve: On applique la relation (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 (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. □

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

$$\mathcal{E}_{i_0j_0} \circ \mathcal{E}_{j_0'k_0}(\mathbf{e}_k) = \mathcal{E}_{i_0j_0}(\delta_{k=k_0}\mathbf{f}_{j_0'}) = \delta_{k=k_0}\delta_{j_0=j_0'}\mathbf{g}_{i_0} = \delta_{j_0=j_0'}\mathcal{E}_{i_0k_0}(\mathbf{e}_k).$$

□

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 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 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.

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. *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

$$(m_{ij})_{i\leqslant d',j\leqslant d} = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix}, \text{ on a } (m^*_{ij})_{i\leqslant d,j\leqslant d'} = \begin{pmatrix} m_{11} & m_{21} & \cdots & \cdots & m_{d'1} \\ m_{12} & m_{22} & \cdots & \cdots & m_{d'2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{1d} & m_{2d} & \cdots & \cdots & m_{d'd} \end{pmatrix}$$

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*

$$\begin{array}{rccc} {}^t\bullet : & M_{d'\times d}(K) & \mapsto & M_{d\times d'}(K) \\ & M = (m_{ij})_{i\leqslant d',j\leqslant d} & \mapsto & {}^tM = (m_{ij})_{j\leqslant d,i\leqslant d'} \end{array}.$$

PROPOSITION 7.5. *La transposition a les proprietes suivantes:*

1. *Linearite: ${}^t(\lambda.M + M') = \lambda {}^tM + {}^tM'$.*
2. *Involutivite: ${}^t({}^tM) = M$.*
3. *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

$$(\psi \circ \varphi)^*(\ell'') = \ell'' \circ (\psi \circ \varphi) = (\ell'' \circ \psi) \circ \varphi = \varphi^*(\ell'' \circ \psi) = \varphi^*(\psi^*(\ell'')) = \varphi^* \circ \psi^*(\ell'')$$

□

PROPOSITION 7.6. *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

$$\mathrm{rg}(\varphi) = \mathrm{rg}(\varphi^*).$$

□

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 $\dim M_d(K) = d^2$.

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 7.3. *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).

Soit V de dimension d. On rappelle par ailleurs 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 notera cet isomorphisme $\mathrm{Mat}_{\mathscr{B}}$ (ou juste Mat si la base $\mathscr{B}$ est implicite) et la matrice associee

$$\mathrm{Mat}_{\mathscr{B}}(\varphi) := \mathrm{Mat}_{\mathscr{B},\mathscr{B}}(\varphi).$$

Remarque 2.1. 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 7.4. *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 multiplications 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. □

2.1. 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 7.1. *On a un isomorphisme de groupes*

$$\mathrm{Mat}_{\mathscr{B}} : \mathrm{GL}(V) \simeq \mathrm{GL}_d(K).$$

PROPOSITION 7.7. *(Critere d'inversibilite) 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 2.2. 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 2.3. Dans ce critere on peut remplacer "colonnes" par "lignes" car le rang de M est celui de sa trasnposee:

$$\mathrm{rg}(M) = \mathrm{rg}({}^tM).$$

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 $\Delta \neq 0_K$.

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 $\mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\varphi)$.

PROPOSITION 7.8. *(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 (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 $\mathbf{e}_{n,j}$ 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 7.9. *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 es la matrice de passage de la 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 (1.4) et de (1.3) appliques a $\varphi = \psi = \mathrm{Id}_V$ et a des bases convenables. □

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

$$\mathrm{Mat}_{\mathscr{B}_1}(\varphi) = \mathrm{Mat}_{\mathscr{B}_1,\mathscr{B}}.\mathrm{Mat}_{\mathscr{B}}(\varphi)\mathrm{Mat}_{\mathscr{B},\mathscr{B}_1} = \mathrm{Mat}^{-1}_{\mathscr{B},\mathscr{B}_1}.\mathrm{Mat}_{\mathscr{B}}(\varphi)\mathrm{Mat}_{\mathscr{B},\mathscr{B}_1}$$

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 7.10. *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 7.11. *Si M et N sont equivalentes alors*

$$\mathrm{rg}(M) = \mathrm{rg}(N).$$

3.2. Conjugaison.

La formule de changement de base dans $M_d(K)$ met en evidence une operation particulier 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 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 7.12. *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 7.13. *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 cette 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

les racines imaginaires sont une subtile
et magnifique ressource de l'esprit divin,
sorte d'hermaphrodite entre l'existence
et la non-existence

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.

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

$$I^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathrm{Id}_2.$$

On a donc

$$I^3 = -I, I^4 = \mathrm{Id}_2, I^5 = I, \cdots$$

et donc

$$I^n = \pm \mathrm{Id}_2 \text{ ou bien } \pm I$$

suivant que n est pair ou impair.

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

(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 $z \in \mathbb{C} - \{0_2\}$ et ${}^t z$ sa transposee:

$$z = x.\mathrm{Id}_2 + y.I = \begin{pmatrix} x & -y \\ y & x \end{pmatrix},\ {}^t z = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x.\mathrm{Id}_2 - y.I.$$

On a

$$z.{}^t z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} x^2 + y^2 & 0 \\ 0 & x^2 + y^2 \end{pmatrix} = (x^2 + y^2).\mathrm{Id}_2.$$

Comme $(x, y) \neq (0, 0)$ on a $x^2 + y^2 > 0$ (on est dans $\mathbb{R}$) et donc on a

$$z.\frac{1}{x^2 + y^2}{}^t z = \mathrm{Id}_2.$$

De meme

$$\frac{1}{x^2 + y^2}{}^t z.z = \mathrm{Id}_2$$

donc z est inversible et

$$z^{-1} = \frac{1}{x^2 + y^2}{}^t z = \begin{pmatrix} \frac{x}{x^2+y^2} & \frac{y}{x^2+y^2} \\ -\frac{x}{x^2+y^2} & \frac{x}{x^2+y^2} \end{pmatrix}.$$

□

EXERCICE 8.1. Montrer que $z \in \mathbb{C} - \{0_2\}$ est inversible en utilisant l'exercice 7.1.

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 *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:

$$|z.z'| = |z|.|z'|.$$

Preuve: Il est evident que Re et Im sont lineaires (ce sont les formes lineaires " premiere et seconde coordonnee" de la base $\{\mathrm{Id}_2, I\}$) mais on peut egalement le verifier directement.

On peut egalement verifier immediatement 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 involutif est immediat (ou vient du fait que la transposition est involutive)

– De plus $\overline{\bullet}$ est injectif est immediat (ou vient du fait que c'est un morphisme de corps (non-nul)).

– La multiplicativite du module provient de la multiplicativite de la conjegaison complexe (et le fait que $\mathbb{C}$ est commutatif.)

□

2.1. Nombres complexes de module 1. Considerons le module mais restreindre 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 $\mathbb{C}^{(1)}$ 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 $||z|| = |z|$, on a

$$|z/|z|| = |z|/|z| = 1.$$

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 surjectif : pour tout $\rho > 0$ et $z^{(1)} \in \mathbb{C}^1$, on a

$$\mathrm{pol}(\rho.z^{(1)}) = (\rho, z^{(1)}).$$

□

DÉFINITION 8.3. *Soit $z \in \mathbb{C}^\times$, $\mathrm{pol}(z) = (|z|, z/|z|)$ s'appelle la decomposition polaire de z. Le premier terme $|z|$ est le module et se note aussi $\rho(z) = r(z) > 0$ et le second terme $z/|z| \in \mathbb{C}^{(1)}$ est appelle argument complexe de z et on le note*

$$z/|z| = e^{i\theta(z)}.$$

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

$$z = x + iy = \rho(z).e^{i\theta(z)} = \rho(z)(\mathrm{c}(z) + i\mathrm{s}(z)),\ x = \rho(z)\mathrm{c}(z),\ y = \rho(z)\mathrm{s}(z).$$

2.2. Formules de trigonometrie. On retrouve les formules habituelles de trigonometrie:
– Formules de produit: pour $z, z' \in \mathbb{C}^\times$

$$e^{i\theta(z.z')} = e^{i\theta(z)}.e^{i\theta(z')}$$

$$\mathrm{c}(z.z') = \mathrm{c}(z).\mathrm{c}(z') - \mathrm{s}(z).\mathrm{s}(z'),\ \mathrm{s}(z.z') = \mathrm{s}(z).\mathrm{c}(z') + \mathrm{s}(z').\mathrm{c}(z).$$

– Formule d'inversion:

$$z^{-1} = |z|^{-1}(z/|z|)^{-1} = \rho^{-1}e^{i\theta(1/z)}$$

$$e^{i\theta(1/z)} = \overline{e^{i\theta(1/z)}} = \mathrm{c}(1/z) + i\mathrm{s}(1/z) = \mathrm{c}(z) - i\mathrm{s}(z).$$

– Formule de l'angle double:

$$\mathrm{c}(z^2) = \mathrm{c}(z)^2 - \mathrm{s}(z)^2,\ \mathrm{s}(z^2) = 2\mathrm{s}(z)\mathrm{c}(z).$$

et plus generalement pour $n \geqslant 0$

$$e^{i\theta(z^n)} = (e^{i\theta(z)})^n = \mathrm{c}(z^n) + i\mathrm{s}(z^n) = (\mathrm{c}(z) + i\mathrm{s}(z))^n = \sum_{k=0}^{n} C_n^k i^k \mathrm{c}^{n-k}\mathrm{s}^k$$

par la formule du binome de Newton. Comme

$$i^k = (-1)^{(k-1)/2}i, \text{ ou bien } (-1)^{k/2}$$

suivant que k est pair ou impair, on a en substituant k par $2k$ ou $2k+1$

$$\mathrm{c}(z^n) = \sum_{0\leqslant k\leqslant n/2} C_n^{2k}(-1)^k \mathrm{c}^{n-2k}\mathrm{s}^{2k}.\ \mathrm{s}(z^n) = \sum_{0\leqslant k\leqslant n/2} C_n^{2k+1}(-1)^k \mathrm{c}^{n-2k-1}\mathrm{s}^{2k+1}.$$

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 $\mathbb{R}^2$:

4. Equations polynomiales complexes

Le corps des nombres complexes $\mathbb{C}$ a ete introduit (pas de cette maniere) dans la renaissance italienne dans l'etude des equations polynomiales: l'etude des solution z des equations de la forme

$$P(z) = a_d.z^d + a_{d-1}.z^{d-1} + \cdots + a_1.z + a_0 = 0, \tag{4.1}$$

avec $a_0, \cdots, a_d \in \mathbb{R}$ des nombres reels[1]. En particulier pour $d = 2$ (les equations quadratiques)

$$az^2 + bz + c = 0 \tag{4.2}$$

l'equation n'avait pas de solution si $\Delta = b^2 - 4ac < 0$ en particulier pour l'equation

$$z^2 + 1 = 0.$$

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 donnees par les formules usuelles

$$z_\pm = \frac{-b \pm \sqrt{\Delta}}{2a}$$

[1]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

avec pour $\Delta < 0$

$$\sqrt{\Delta} := \sqrt{|\Delta|}.i$$

On a egalement pu resoudre dans $\mathbb{C}$ de nombreuses autres equations polynomiales a coefficient reels jusqu'aux travaux de Gauss qui a montrer que

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 (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.*

EXERCICE 8.2. 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

1. Operation elementaires sur les lignes

Soit $M = (m_{ij}) \in M_{d' \times d}(K)$ une matrice. Pour simplifier les notation on notera sa i-ieme ligne $(i \leqslant d')$

$$M_i = \mathrm{Lig}_i(M) = (m_{ij})_{j \leqslant d}$$

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) Echanger deux lignes $i \neq j \leqslant d'$ de M:

$$M_i \longleftrightarrow M_j$$

(ii) Multiplier la i-eme ligne par un scalaire $\lambda \neq 0$:

$$M_i \to \lambda.M_i.$$

(iii) Additioner a la ligne i un multiple scalaire de la la j-ieme ligne: $\mu \in K$

$$M_i \to M_i + \mu M_j$$

Ces transformations sont appellees transformations *elementaires*.

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

$$(\mathrm{Lig}_i + \mu \mathrm{Lig}_j)(\bullet) : M \in M_{d' \times d}(K) \mapsto M_i + \mu.M_j \in \mathrm{Lig}_d(K)$$

est lineaire. Elle sont bijectives car elle admettent des applications reciproques:

(i) Echanger les deux memes lignes $i, j \leqslant d'$ de M:

$$M_i \longleftrightarrow M_j$$

(ii) Multiplier la i-eme ligne par le scalaire λ^{-1}:

$$M_i \to \lambda^{-1}.M_i.$$

(iii) Soustraire a la ligne i un multiple scalaire de la j-ieme ligne: $\mu \in K$

$$M_i \to M_i - \mu M_j$$

□

PROPOSITION 9.2. *Les trois operations elementaires sont obtenus 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) $L_{i,j,\mu}.\bullet : M \mapsto L_{i,j,\mu}.M$.

ou les matrices carrees $T_{ij},\ D_{i,\lambda},\ L_{i,j,\mu} \in M_{d'}(K)$ *sont definie par:*

$$T_{ij} = \mathrm{Id}_{d'} - E_{ii} - E_{jj} + E_{ij} + E_{ji}.$$

$$D_{i,\lambda} = \mathrm{Id}_{d'} + (\lambda - 1).E_{ii},\ \lambda \neq 0$$

$$L_{i,j,\mu} = \mathrm{Id}_{d'} + \mu.E_{ij},\ i \neq j \text{ ou } \mu \neq -1 \text{ si } i = j.$$

Preuve: On a 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 est la matrice dont la i-ieme ligne est la j-ieme ligne $M_j = (M_{jl})_{l \leqslant d'}$ et dont toutes les autres coordonnees sont nulles.

– Ainsi $(\mathrm{Id}_{d'} + \mu.E_{ij}).M$ est la matrice forme a partir de M et ou la i-ligne M_i est remplacee par $M_i + \mu.M_j$.

– 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 M_i est remplacee par $M_i + \mu.M_i = (1 + \mu).M_i$. 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 M_j est ajoutee a la i-ieme ligne et ou la ligne M_j est ajoutee a la j-ieme ligne de M et c'est donc la matrice M ou les ligne i et j on ete echangees. □

Remarque 1.1. En particulier le fait que ces applications sont lineaires provient du fait que pour tout 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).

Notons que les matrices $T_{ij},\ D_{i,\lambda},\ L_{i,j,\mu}$ sont inversibles (si $\lambda \neq 0$ ou $i \neq j$ pour $L_{i,j,\mu}$ et on a

$$T_{ij}^{-1} = T_{ij},\quad D_{i,\lambda}^{-1} = D_{i,\lambda^{-1}},\ L_{i,j,\mu}^{-1} = L_{i,j,-\mu}.$$

Remarque 1.2. On peut le verifier directement en utilisant que

$$E_{ij}.E_{kl} = \delta_{j=k}E_{il}$$

Définition 9.2. *On dit que* N *est ligne-equivalente a* M *si il existe une suite de transformations elementaires qui transforme* M *en* N*.*

Remarque 1.3. Notons que comme toutes les transfomations elementaires sont inversibles et que leur inverse sont elementaires, cette relation "ligne-equivalence" est une relation d'equivalence: reflexive, symetrique et transitive.

Remarque 1.4. Si N est ligne equivalente a M alors toute ligne de N est combinaison lineaire des lignes de M et vice versa.

Proposition 9.3. *Deux matrice ligne-equivalente et echelonnees reduites sont egales.*

Preuve. Admis. □

2. Echelonnage

DÉFINITION 9.3. *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
- *$m_{1j} = 0$ pour tout $j < j_1$ et $m_{1j_1} \neq 0$,*
- *$m_{12j} = 0$ pour tout $j < j_2$ et $m_{2j_2} \neq 0$,*
- *$\vdots$*
- *$m_{rj} = 0$ pour tout $j < j_r$ et $m_{rj_r} \neq 0$*

(2) Si $r < d$ les lignes $M_{r+1}, \cdots, M_{d'}$ 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 9.4. *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 M_1 par $m_{ij_1}^{-1}.M_1$ et supposons que $m_{1,j_1} = 1$. En remplacant les $M_i, i > 1$ par $M_i - m_{ij_1}M_1$ annule les autres coefficients de la colonne j_1 et on obtient une matrice ligne-equivalente de la forme (ici $j_1 = 3$)

$$\begin{pmatrix} 0 & 0 & 1 & * & * & \cdots & * \\ 0 & 0 & 0 & m'_{2,j_1+1} & * & \cdots & * \\ 0 & 0 & 0 & * & * & \cdots & \cdots \\ 0 & 0 & 0 & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & m'_{d',j_1+1} & * & * & * \end{pmatrix}$$

On repete la procedure avec la matrice extraite 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. □

CHAPITRE 10

L'anneau des polynomes sur un corps

Dans ce chapitre on rappelle la construction algebrique des polynomes sur un corps (cf. Serie). 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)

1. Les polynomes sont des suites

On rappelle que l'on construit $K[X]$ comme etant l'ensemble $K_f^{\mathbb{N}}$, des suites

$$P(X) = (a_n)_{n\geqslant 0} \subset K^{\mathbb{N}}$$

a valeurs dans K et a *support fini*:

$$\mathrm{supp}(P) = \{n \in \mathbb{N},\ a_n \neq 0_K\}.$$

Comme tel $K[X]$ est un K-ev pour l'addition des suites a valeurs dans K et la multiplication par les scalaires que nous rappelons: pour $\lambda \in K$ et (a_n) a support fini

$$\lambda.(a_n)_{n\geqslant 0} = (\lambda.a_n)_{n\geqslant 0}.$$

L'element nul est la suite identiquement nulle $\underline{0}_K$).

Une base de $K[X]$ est donnee par l'ensemble *monomes unitaires* qui sont les suites

$$\{X^d,\ d \geqslant 1\} \subset K[X]$$

definies de la maniere suivante:

$$X^d := (\delta_{n=d})_{n\geqslant 0} = (0, \cdots, 1_k, 0, \cdots)$$

cad la suite dont le d-ieme terme vaut 1_K et tous les autres termes valent 0_K: ici on a note le symbole de Kronecker (a valeurs dans K)

$$\delta_{n=d} = \begin{cases} 1_K & \text{si } n = d \\ 0_K & \text{sinon} \end{cases}.$$

Ainsi tout polynome peut se noter pour un certain $d \geqslant 0$

$$P(X) = a_0.X^0 + a_1.X + \cdots + a_d.X^d.$$

Définition 10.1. *Le degree d'un polynome non-nul P 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

$$P(X) = a_0.X^0 + a_1.X + \cdots + a_d.X^d = (a_0, \cdots, a_d, 0, \cdots)$$

le n-ieme terme de cette suite a_n est appelle coefficient de degre n de P.

Définition 10.2. *Un polynome non-nul est unitaire si le coefficient de son term de plus haut degre $a_{\deg P} = 1$.*

REMARQUE 1.1. Quitte a multplier par un sclaire on peut toujours se ramener au cas d'un polynome unitaire: $(a_{\deg P})^{-1}.P(X)$ est unitaire.

EXEMPLE 1.1. Le monome X^d est de degre d. Le polynome constant $\lambda = \lambda.X^0$ est de degre 0 si $\lambda \neq 0_K$.

NOTATION 10.1. *En particulier on dispose d'un application lineaire injective de K dans $K[X]$*

$$\text{Cst} : \begin{array}{ccc} K & \mapsto & K[X] \\ \lambda & \mapsto & \lambda.X^0 = (\lambda, 0, 0, \cdots) \end{array}.$$

On appelle $\text{Cst}(\lambda) = \lambda.X^0$ le "polynome constant de valeur λ" et pour simplifier les notation on ecrira λ au lieu de $\lambda.X^0$.

PROPOSITION 10.1. *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

$$P = a_0 + a_1.X + \cdots + a_d.X^d,\ Q = b_0 + b_1.X + \cdots + b_{d'}.X^{d'}$$

avec $a_d, b_{d'} \neq 0$.

Supposons $d \geqslant d'$. En posant $b_n = 0$ pour $n > d'$, on a

$$P+Q = a_0+a_1.X+\cdots+a_d.X^d+b_0+b_1.X+\cdots+b_d.X^d = (a_0+b_0)+(a_1+b_1).X+\cdots+(a_d+b_d).X^d$$

et $\deg(P+Q) \leqslant d$ (avec egalite ssi $a_d + b_d \neq 0$). □

COROLLAIRE 10.1. *Soit $d \geqslant 0$ et*

$$K[X]_{\leqslant d} = \{P(X) = a_0.X^0 + a_1.X + \cdots + a_d.X^d,\ a_n \in K\}$$

l'ensemble des polynomes de degre $\leqslant d$. Alors $K[X]_{\leqslant d}$ est un SEV de $K[X]$ de dimension finie egale a $d+1$. Une base de cet espace est donnee par les monomes unitaires de degree $\leqslant d$:

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

2. Structure d'anneau

$K[X]$ est egalement muni d'une multiplication interne

$$\bullet.\bullet : \begin{array}{ccc} K[X] \times K[X] & \mapsto & K[X] \\ (P, Q) & \mapsto & P.Q \end{array}$$

definie par

$$P = (a_n)_{n\geqslant 0},\ Q = (b_n)_{n\geqslant 0},\ P.Q = (c_n)_{n\geqslant 0}$$

avec

$$c_n = \sum_{p+q=n} a_p.b_q = a_0.b_n + a_1.b_{n-1} + \cdots + a_n.b_0.$$

Comme cette multiplication est associative distributive et commutative et fait de $(K[X], +, .)$ un anneau commutatif dont l'element unite est le polynome constant

$$1_K = (1_K, 0, \cdots).$$

De plus comme $K[X]$ est un K-ev et que la multiplication par les scalaires coincide avec la multiplication par les polynomes constants, $K[X]$ est une K-algebre.

La multiplication correspond a la multiplication usuelle pour les fonctions polynomiales en regroupant les monomes de meme degre

$$(a_0.X^0 + a_1.X + \cdots + a_d.X^d).(b_0.X^0 + b_1.X + \cdots + b_d.X^d) = \sum_{p,q\leqslant d} a_p.X^p.b_q.X^q = \sum_{p,q\leqslant d} a_p.b_q.X^{p+q} = \sum_{n\leqslant 2d}(\sum_{p+q=n} a_p.b_q)X^n$$

PROPOSITION 10.2. *Soient P, Q des polynomes, on a*

$$\deg(P.Q) = \deg P + \deg Q.$$

Preuve: C'est evident si P ou $Q = 0$ compte-tenu du fait que $\deg 0 = -\infty$ et que $P.Q = 0$:

$$\deg(P.Q) = -\infty = \deg P + \deg Q.$$

Sinon soit $d = \deg P \geqslant d' = \deg Q$, on a

$$P = a_0 + a_1.X + \cdots + a_d.X^d,\ Q = b_0 + b_1.X + \cdots + b_{d'}.X^{d'}$$

avec $a_d, b_{d'} \neq 0$. Ainsi

$P.Q = (a_0+a_1.X+\cdots+a_d.X^d).(b_0+b_1.X+\cdots+b_{d'}.X^{d'}) = a_0.b_0+(a_1.b_0+a_0.b_1).X+\cdots+a_d.b_{d'}.X^{d+d'}$

On a $a_d,\ b_{d'} \neq 0$ et comme K est integre (c'est un corps) avec $a_d.b_{d'} \neq 0$ et $\deg P.Q = d + d'$. □

COROLLAIRE 10.2. *L'anneau $K[X]$ est integre.*

Preuve: Si $P.Q = 0$ alors $\deg P.Q = -\infty = \deg P + \deg Q$ ce qui implique que $\deg P$ ou $\deg Q$ vaut $-\infty$ et que P ou Q est nul. □

DÉFINITION 10.3. *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 2.1. 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.

3. Division et factorisation

La division euclidienne des polynomes sur $\mathbb{R}$ se generalise a un corps arbitraire:

THÉORÈME 10.1. *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 10.4. *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

$$Q|P.$$

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 10.2. *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. □

Comme un noyau d'un morphisme d'anneau $\varphi : K[X] \mapsto A$ est un ideal on a:

COROLLAIRE 10.3. *Soit A un anneau et $\varphi : K[X] \mapsto A$ un morphisme d'anneaux. Alors il existe $Q \in K[X]$ tel que*

$$\ker(\varphi) = Q.K[X].$$

DÉFINITION 10.5. *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.*

3.1. Decomposition en polynomes irreductibles.

DÉFINITION 10.6. *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

$$Q|P \Longleftrightarrow \deg Q = 0 \text{ ou } P.$$

REMARQUE 3.1. En effet si $Q|P$ et $\deg Q = \deg P$ alors $Q = \lambda.P$

PROPOSITION 10.3. *(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 10.3. *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 $\sigma : \{1, \cdots\} \mapsto \{1, \cdots\}$ 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 result 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

$$Q = a_{\deg Q}.Q_1,\ Q_1 = a^{-1}_{\deg Q}.Q.$$

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. □

3.2. PGCD et PPCM. 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

$$(P) \cap (Q) \subset (P), (Q) \subset (P) + (Q) = \langle P, Q\rangle \subset K[X].$$

3.2.1. *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 $P, Q \in \langle P, Q\rangle$, on a

$$R|P \& R|Q.$$

D'autre part si S divise 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 de P et Q au sens ou tout diviseur commun de P et Q doit diviser R.

Définition 10.7. *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.

Proposition 10.4. *(Bezout) Il existe $A, B \in K[X]$ tels que*

$$(P, Q) = A.P + B.Q.$$

Définition 10.8. *On dit que P et Q sont premiers entre eux ssi*

$$(P, Q) = 1 \Longleftrightarrow K[X].P + K[X].Q = K[X] = 1.K[X].$$

Ou de maniere equivalente ssi il existe $A, B \in K[X]$ tels que

$$1 = A.P + B.Q.$$

Remarque 3.2. Si $A.P + B.Q = 1$ alors $1 \in K[X].P + K[X].Q$ et donc

$$K[X] = K[X].1 \in K[X].P + K[X].Q \subset K[X].$$

On a donc bien $K[X].P + K[X].Q = K[X] = 1.K[X]$ autrement dit

$$(P, Q) = 1$$

3.2.2. *Le PPCM.* Soit l'intersection $\subset K[X]$. 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 les le plus petit multiple commun (unitaire) de P et Q.

Définition 10.9. *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 10.5. *(Formule du produit)Soient $P,Q\in K[X]-\{0\}$ et unitaires. On a*

$$P.Q=[P,Q](P,Q).$$

3.3. Un critere d'irreductibilite.

Théorème 10.4. *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*

$$Q \text{ est irreductible } \Longleftrightarrow B \text{ est un corps}$$

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. □

3.4. 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 10.6. *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 10.1. 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 10.2. 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 $Q \in K[X]_{\leqslant d-1}$.

CHAPITRE 11

Determinant

1. Formes multilineaires

2. Le Theoreme de Cayley-Hamilton