III . −Matrice d'adjacence, endomorphisme d'adjacence

III.0 . −Introduction

Dans ce chapitre (III,) les *graphes* sont toujours des *graphes finis simples non-orientés* (cf. la définition I.4.4.) Les propriétés combinatoires d'un tel *graphe* G sont en étroite relation avec les propriétés algébriques de l'*endomorphisme d'adjacence* $\Phi(G)$ de G (cf. la définition III.1.7,) ou de manière équivalente de la *matrice d'adjacence* G (cf. la définition III.1.9.)

En particulier la proposition III.1.14 et même la proposition III.1.15 relient le *nombre de parcours de longueur* ℓ d'un *sommet* à un autre aux itérés de l'*endomorphisme d'adjacence* .

On sait que le calcul d'itérés d'*endomorphismes* est grandement facilité lorsque ceux-ci sont *diagonalisables* (cf. la définition III.7.2.3.) On sait également que, la plupart du temps, il n'est pas vraiement possible de déterminer le *spectre* d'un *endomorphisme* puisqu'il est en fait rarement possible de factoriser son *polynôme caractéristique* (cf. la définition III.7.3.1.)

Dans le cas des *graphes finis simples non-orientés* :
d'abord l'*endomorphisme d'adjacence* est *diagonalisable* ;
le spectre de ce dernier peut, dans un certain nombre de cas être déterminé à partir du *graphe* lui-même (voir les paragraphes III.3, III.11.6, IV.3.)

Ainsi le *graphe* permet de déterminer le *spectre* de l'*endomorphisme d'adjacence* qui, en retour donne des informations combinatoires sur le *graphe* .

Le fait que l'*endomorphisme d'adjacence* est *diagonalisable* est justifié par le fait qu'il est *auto-adjoint* (cf. la définition III.10.5,) (ou encore que la *matrice d'adjacence* est *symétrique* dans une *base orthonormale* ,) pour une *structure euclidienne* (resp. *hermitienne* ,) bien choisie (cf. la proposition III.2.2 ;) la *diagonalisabilité* de l'*endomorphisme d'adjacence* découlant alors du théorème III.10.9.

On a sans doute déjà mesuré l'importance du théorème III.10.9, dans les questions de éduction d'*endomorphismes* . Le résultat technique permettant de démontrer ce *théorème* est la proposition III.10.8. Cette dernière fait appel, dans sont énoncé et sa démonstration, a un certain nombre de définitions et de résultats que nous rappellerons également dans ce chapitre.

On rappelle en particulier ce qu'est un *endomorphisme auto-adjoint* (cf. la définition III.10.5,) ce qui nous amènera naturellement à revenir sur les *structures euclidiennes* et *hermitiennes* aux paragraphes III.8, et III.9.

La proposition III.10.8 établissant précisément l'*existence* d'*éléments propres* pour un *endomorphisme auto-adjoint* , il nous a paru raisonnable de rappler ce qu'est une *valeur propre* (cf. le point i de la définition III.7.2.2,) et d'un *vecteur propre* (cf. le point ii de la définition III.7.2.2.)

III.1 . −L'espace $\mathbb{K}^G$ et l'endomorphisme d'adjacence

Dans tout ce paragraphe (III.1,) $\mathbb{K}$ est un *corps* (cf. la définition III.1.1.12.) En pratique nous ferons, le plus souvent, l'hypothèse que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$; même si nous ne nous interdisons pas, a priori, d'étudier d'autres situations.

On rappel, dans ce paragraphe (III.1) un certain nombre de définitions et de résultats d'algèbre linéaires. Ils font partie du programme des années précédentes ; et il n'est nul besoin de s'y attarder si vous êtes parfaitement à l'aise avec.

Il faut impérativement être en mesure de comprendre la définition III.1.7. Nous donnons un certain nombre d'éléments destinés à permettre cette compréhension ; mais s'ils sont acquis il n'est pas nécessaire de s'y attarder de nouveau.

III.1.1 . −Corps

Définition III.1.1.1 (Anneau) Un *anneau* est un triplet $(A, +, *)$ (le plus souvent noté $A,$) tel que :

Ann$_1$) Le couple $(A, +)$ est un groupe abélien (cf. la définition II.8.1.4 ;)
et la loi $* \ : \ A \times A \ \to \ A$ vérifie :

Ann$_2$) pour tout triplet (x, y, z) d'éléments de A,

$$x * (y * z) \ = \ (x * y) * z \ ,$$

(la loi $*$ est *associative*) ;

Ann$_3$) il existe un *élément* 1_A de A, appelé *élément neutre de* $(A, *)$, (souvent noté 1 lorsque le contexte est clair) tel que, pour tout $x \ \in \ A$, $1_A * x \ = \ x * 1_A \ = \ x$; (on supposera toujours que $1_A \ \neq \ 0_A$ où 0_A est l'*élément neutre* pour la loi $+$;)

Ann$_4$) pour tout triplet (x, y, z) d'éléments de A,

$$x * (y + z) \ = \ x * y + x * z, \ \text{ et } \ (x + y) * z \ = \ x * z + y * z \ ,$$

(la loi $*$ est *distributive* par rapport à la loi $+$.)

On dira aussi que les lois $+$ et $*$ *donnent à l'ensemble* A *une structure d'anneau*.

La loi $+$ est usuellement appelée *addition* et la loi $*$ *multiplication*, par analogie avec l'anneau "modèle" $(\mathbb{Z}, +, *)$. Pour tout couple (x, y) d'éléments de A, on appellera $x + y$ et $x * y$ respectivement *somme* et *produit* de x et y.

On remarque que pour tout $x \ \in \ A$, $0_A * x \ = \ x * 0_A \ = \ 0_A$. On dit que 0_A est un *élément absorbant*.

Définition III.1.1.2 (Morphisme d'anneaux) Une *application* $f \ : \ (A, +_A, *_A) \ \to \ (B, +_B, *_B)$ est un *morphisme d'anneaux* ou *homomorphisme d'anneaux* (ou simplement *morphisme* si le contexte ne prête pas à confusion,) si :

Ann$_5$) $f \ : \ (A, +_A) \ \to \ (B, +_B)$ est un *morphisme de groupes* (cf. la définition II.8.2.1.)

Ann$_6$) Pour tout couple (x, y) d'éléments de A,

$$f(x *_A y) \ = \ f(x) *_B f(y) \ .$$

Ann$_7$) $f(1_A) \ = \ 1_B$.

Cela revient à dire que f est un morphisme à la fois pour les magma $(A, +)$ et $(B, +)$ (cf. l'axiome Ann$_5$,) ainsi que pour les magma $(A, *)$ et $(B, *)$ (cf. l'axiome Ann$_6$.) Néanmoins on ajoute l'axiome Ann$_7$ dont on verra l'importance dans la suite.

Définition III.1.1.3 (Sous-annau) Étant donné un *anneau* $(A, +, *)$ un *sous-anneau* de A est une partie B de A telle que $1_A \ \in \ B$ et les restrictions respectives des lois $+$ et $*$ à B donnent à B une structure d'anneau.

En particulier $(B, +)$ est alors un sous-groupe (cf. la définition II.8.3.1,) de $(A, +)$.

Proposition III.1.1.4 (Caractérisation des sous-anneaux) *Étant donnés un anneau*

$$(A, +, *) \text{ et } B \ \subset \ A$$

une partie de A*, les assertions suivantes sont équivalentes :*

a) B *est un sous-anneau au sens de la définition III.1.1.3.*

b) B *est non vide,* $1_A \in B$, *et pour tout couple* (x, y) *d'éléments de* B,

$$y - x \in B \text{ et } x * y \in B .$$

c) La restriction

$$\mathrm{Id}_{A|B} : B \to A$$

de l'identité Id_A *à* B *est un morphisme d'anneaux . Ceci signifie implicitement que* B *possède une structure d'anneau.*

Démonstration *: (cf. l'exercice III.11.1.1.)*

Définition III.1.1.5 (Anneau commutatif) Étant donné un anneau $(A, +, *)$, si

$$\forall (x, y) \in A \times A,\ x * y = y * x$$

on dira que la loi $*$ est *commutative* ou encore que l'anneau $(A, +, *)$ est un *anneau commutatif.*

Définition III.1.1.6 (Anneau intègre) Si $(A, +, *)$ est un anneau tel que

$$\forall x \in A,\ \forall y \in A,\ (x * y = 0 \Rightarrow x = 0 \vee y = 0) ,$$

on dit que A est un anneau *intègre*.

Exemple III.1.1.7 (Anneaux) a) La *multiplication* $*$ sur $\mathbb{Z}$, donne a $(\mathbb{Z}, +, *)$ une structure d'anneau commutatif.

Par ailleurs la relation de *congruence* modulo n (cf. le point d de l'exemple II.8.1.2) est compatible à la *multiplication* (cf. la définition II.7.18) *i.e.* pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, et $(a', b') \in \mathbb{Z} \times \mathbb{Z}$, si

$$a \sim_n a' \text{ et } b \sim_n b' ,$$

alors

$$ab \sim_n a'b' .$$

Ce qui permet de définir une *multiplication* $*_{\mathbb{Z}/n}$ sur l'ensemble $\mathbb{Z}/n$ des classes modulo n par :

$$\overline{a} *_{\mathbb{Z}/n} \overline{b} \,! = \overline{a * b} .$$

Le triplet $(\mathbb{Z}/n, +_{\mathbb{Z}/n}, *_{\mathbb{Z}/n})$, le plus souvent noté $\mathbb{Z}/n$ est alors un *anneau commutatif* .

Attention : $(\mathbb{Z}/n, *)$ n'est jamais un *groupe* .

b) Un exemple fondamental qui entrera dans un certain nombre de constructions que nous allons envisager, est constitué par l'*anneau* $(\mathrm{End}_{\mathbf{Gr}}(G), +, \circ)$ où $(G, +)$ est un *groupe abélien* .

c) On dira qu'une fonction f: $\mathbb{R} \to \mathbb{R}$ est *à support compact*, s'il existe un intervalle $[a, b] \subset \mathbb{R}$ (*i.e.* un sous ensemble compact de $\mathbb{R}$,) tel que pour tout $x \notin [a, b]$, $f(x) = 0$. L'ensemble C des fonctions continues à support compact, muni de l'adition :

$$\begin{array}{rcl} + : C \times C & \to & C \\ (f, g) & \mapsto & f + g \mid (f + g)(x) = f(x) + g(x)\, \forall x \in \mathbb{R}, \ ; \end{array}$$

et de la *multiplication* :

$$\begin{array}{rcl} \star : C \times C & \to & C \\ (f, g) & \mapsto & f * g \mid (f * g)(x) = f(x) * g(x)\, \forall x \in \mathbb{R}\, ; \end{array}$$

n'est pas un anneau au sens de la définition III.1.1.1.

En effet, C ne possède pas d'élément neutre pour la *multiplication* $*$ et ne vérifie donc pas l'axiome Ann_3 de la définition III.1.1.1

Dans la suite de ce cours, nous n'aurons pas à considérer de tels objets, ce qui nous incite à donner une définition d'anneau plus restrictive à laquelle satisferont tous les objets de notre étude. Les anneaux que nous considérerons sont parfois appelés *anneaux unifères.*

Exemple III.1.1.8 (Sous-anneaux) a) Le noyau d'un morphisme d'anneau $f : A \to B$ n'est pas un sous-anneau de A. En effet, un sous-anneau de A contient nécessairement1_A. On aurait alors $f(1_A) = 0_B$. Or ùù l'axiome Ann_7 de la définition III.1.1.2 impose $f(1_A) = 1_B$. Par ailleurs l'axiome Ann_3 de la définition III.1.1.1 impose $1_B \neq 0_B$.

b) L'*anneau* $(\mathbb{Z}, +, *)$ est un *sous-anneau* du *corps* $\mathbb{Q}$ des *nombres rationnels* muni des lois $+$ et $*$ usuelles.

Définition III.1.1.9 (Élément inversible) Tous les *éléments* d'un anneau A différents de 0_A ne possédant pas nécessairement un *inverse* pour la loi $*$, on notera $A^\times$ l'ensemble des *éléments* de A *inversible* pour $*$ *i.e.* ceux qui possèdent un inverse. On appelle parfois également *unité* un *élément* de $A^\times$.

Remarque III.1.1.10 Soit $(B, +, *)$ un *sous-anneau* d'un anneau $(A+, *)$.

i) Notons que l'axiome Ann_1 de la définition III.1.1.1 a en particulier pour conséquence que $(B, +)$ est un *sous-groupe* de $(A, +)$; ce qui entraîne, en particulier (cf. II.8.3.4,) que l'*élément neutre* 0_A de $(A, +)$ est aussi l'*élément neutre* de $(B, +)$ et que l'opposé d'un *élément* $x \in B$ est son opposé dans A.

ii) Notons que la condition $1_A \in B$, entraîne que 1_A est l'*élément neutre* pour la loi $*$ sur B (cf. II.9.1.5.1,) et que tout *inversible* dans B est *inversible* dans A et que son *inverse* dans B est encore son *inverse* dans A (cf. II.9.1.5.2.) Il s'ensuit que $(B^\times, *)$ est alors un sous-groupe de $(A^\times, *)$.

iii) La condition $1_A \in B$ est automatiquement satisfaite dans le cas où A est intègre. En revanche si l'on considère un anneau R quelconque (même intègre) et $A := R \times R$ muni des lois $(x, y) +_A (z, t) := (x +_R z, y +_R t)$ et $(x, y) *_A (z, t) := (x *_R z, y *_R t)$, (ce qu'on appelle la structure produit (cf. la définition III.5.14.)) La partie

$$B := \{(x, 0), x \in R\}$$

est une partie qui est un sous-groupe pour la loi $+_A$ un sous-magma pour la loi $*_A$. B est même un anneau isomorphe à R dont l'*élément neutre* est $1_B = (1_R, 0)$ différent de l*élément neutre* $1_A = (1_R, 1_R)$ de A. On ne dira pas dans ce cas que B est un sous-anneau de A.

La condition $1_A \in B$ est à rapprocher de l'axiome Ann_7 de la définition III.1.1.2 .

Lemme III.1.1.11 *i) Pour tout morphisme d'anneaux* $Morf AB$, *la restriction* $f^\times := f_{|A^\times}$ *de* f *à* $A^\times$ *est un morphisme de groupes à valeurs dans* $B^\times$.

ii) Pour tout anneau A,

$$\mathrm{Id}_A{}^\times = \mathrm{Id}_{A^\times} .$$

iii) Pour tous morphisme s d'anneaux $f : A \to B$ *et* $g : B \to C$,

$$(g \circ f)^\times = g^\times \circ f^\times .$$

iv) Pour tout isomorphisme d'anneaux $f : A \to B$ *d'isomorphisme réciproque* $g : B \to A$,

$$f^\times : (A^\times, *) \to (B^\times, *)$$

est un isomorphisme de groupes d'isomorphisme réciproque $g^\times$.

Démonstration : *(cf. l'exercice III.11.1.3.)*

Définition III.1.1.12 (Corps) Un *anneau commutatif* $(A, +, *)$ est un *corps* si tous les *élément* s de A différents de 0_A possèdent un inverse pour la loi $*$; *i.e.* $A^\times = A \setminus \{0_A\}$. Un corps et bien évidemment un anneau intègre ; mais l'anneau $\mathbb{Z}$, par exemple, est un anneau intègre sans pour autant être un corps.

La proposition II.7.21 et la proposition II.8.1.7 ont leur pendant pour les anneaux :

Proposition III.1.1.13 *Étant donnés un anneau* $(A, +, *)$ *et un ensemble* E, *l'ensemble* A^E *des applications de* E *dans* A *muni des lois induites (cf. II.7.21,) est un anneau (commutatif si* A *l'est.)*

Démonstration : *(cf. la question 1 de l'exercice III.11.1.2.)*

III.1.2 . −Espace vectoriel

Définition III.1.2.1 (Espace vectoriel) Étant donné un corps $\mathbb{K}$ (cf. la définition III.1.1.12,) on rappelle qu'un $\mathbb{K}$-*espace vectoriel* est un triplet $(E, +, \cdot)$ (simplement noté E si cela ne doit être à l'origine d'aucune confusion,) tel que :

Vect$_0$) Le couple $(E, +)$ est un groupe abélien (cf. la définition II.8.1.4 ;)

$\cdot : \mathbb{K} \times E \to E$, appelée *application de structure* vérifie :

Vect$_1$) $\forall (a, x, y) \in \mathbb{K} \times E \times E,\ a \cdot x + y = a \cdot x + a \cdot y$;

Vect$_2$) $\forall (a, b, x) \in \mathbb{K} \times \mathbb{K} \times E,\ a + b \cdot x = a \cdot x + b \cdot x$;

Vect$_3$) $\forall (a, b, x) \in \mathbb{K} \times \mathbb{K} \times E,\ a * b \cdot x = a \cdot (b \cdot x)$;

Vect$_4$) $\forall x \in E,\ 1 \cdot x = x$.

Une application $f : E \to F$ est une *application linéaire* si :

Vect$_5$) $f : (E, +_E) \to (F, +_F)$ est un *morphisme de groupes* (cf. la définition II.8.2.1 ;)

Vect$_6$) pour tout $a \in \mathbb{K}$ et tout $x \in E$,

$$f(a \cdot_E x) = a \cdot_F f(x) .$$

Définition III.1.2.2 (Sous-espace) Étant donné un $\mathbb{K}$-*espace vectoriel* E, un sous-espace F est un sous-groupe de E tel que $\forall (a,x) \in \mathbb{K} \times F,\ a \cdot x \in F$.

Lemme III.1.2.3 (Caractérisation des sous-espaces) *une partie $F \subset E$ est un sous-espace de E si et seulement si*

$$F \neq \emptyset \text{ et } \forall (a,b,x,y) \in \mathbb{K} \times \mathbb{K} \times F \times F,\ a \cdot x + b \cdot y \in F \ ;$$

La proposition III.1.2.4 ce-dessous est l'exact analogue de la proposition II.8.3.7 ; ce qui n'est d'ailleurs pas absolument surprenant puisqu'un $\mathbb{K}$-*espace vectoriel* est en particulier un *groupe abélien* .

Proposition III.1.2.4 *Soit E un $\mathbb{K}$-espace vectoriel , F et G des sous-espaces vectoriels .*

*i) (**Intersection**)*
$F \cap G$ est un sous-espace vectoriel E ;

ii) Plus généralement pour $\mathcal{F}$ un ensemble non vide de sous-espaces vectoriels de E, $\bigcap_{\mathcal{F}} F$ est un sous-espace vectoriel de E.

*iii) (**réunion**)*
$F \cup G$ est un sous-espace vectoriel de E si et seulement si

$$F \subset G \text{ ou } G \subset F .$$

*iv) (**Famille filtrante**)*
Si $(F_n)_{,n \in \mathbb{N}}$ est une suite de sous-espaces vectoriels de E telle que

$$\forall (p,q) \in \mathbb{N} \times \mathbb{N},\ \exists r \in \mathbb{N},\ F_p \subset F_r \text{ et } F_q \subset F_r ,$$

alors $\bigcup_{n \in \mathbb{N}} F$ est un sous-espace vectoriel de E.

Un cas particulier est celui où $(F_n)_{,n \in \mathbb{N}}$ est croissante, i.e.

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p \leq q \Rightarrow F_p \subset F_q$$

car alors

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ F_p \subset F_{\max(p,q)} \text{ et } F_q \subset F_{\max(p,q)} .$$

Proposition III.1.2.5 *Étant donné un $\mathbb{K}$-espace vectoriel E et des sous-ensembles S et F de E, les assertions suivantes sont équivalentes :*

a) $F = \left\{ \sum_{i=1}^{n} a_i \cdot_E s_i \ ,\ n \in \mathbb{N} \ ,\ (a_i)_{1 \leq i \leq n} \in \mathbb{K} \ ,\ (s_i)_{1 \leq i \leq n} \in S \right\}$.

b) F est un sous-$\mathbb{K}$-espace vectoriel de E tel que, pour tout sous-$\mathbb{K}$-espace vectoriel G de E contenant S, $F \subset G$.

c) $F = \bigcap_{G \text{ sous-}\mathbb{K}\text{-espace vectoriel de} E\ ,\ S \subset G} G$.

Démonstration : *La preuve se fait sur le même modèle que dans le cas des groupes (cf. la proposition II.8.4.7 .)*

Définition III.1.2.6 Étant donnés un $\mathbb{K}$-*espace vectoriel* E et des sous-ensembles S et F de E, si F et S vérifient l'une des trois conditions équivalentes de la proposition III.1.2.5, on dira que F est le sous-$\mathbb{K}$-*espace vectoriel* de E *engendré* par S. On dira que S est un *partie génératrice* de F. On notera $F = \mathrm{Vect}(S)$.

Si $F = E$ on dira que le $\mathbb{K}$-*espace vectoriel* E est *engendré* par S, ou que S est une *partie génératrice* de E.

Définition III.1.2.7 (Partie libre) Étant donné un $\mathbb{K}$-*espace vectoriel* E, une partie $S \subset E$ est une *partie libre* de E si
pour tout $n \in \mathbb{N}$, tout n-uplet $(s_i)_{1 \leq i \leq n} \in S$, d'éléments deux à deux distincts de s, et tout n-uplet $(a_i)_{1 \leq i \leq n} \in \mathbb{K}$,

$$\sum_{i=1}^{n} a_i s_i = 0 \Rightarrow \forall i \leq 1 \leq n,\ a_i = 0\,.$$

Définition III.1.2.8 (base) Étant donné un $\mathbb{K}$-*espace vectoriel* E, une *base* de E est une partie de E à la fois libre et génératrice

.

ix) (**Propriétés des bases, dimension**)

a) Une *partie libre* de E peut toujours se compléter en une *base* .

b) Un *espace vectoriel* possède toujours une *base* .

c) Si un *espace vectoriel* E possède une *base* qui est une partie finie à $d \in \mathbb{N}$ *élément* s de E, alors toutes les *bases* de E sont des ensembles à d *élément* s ; et d s'appelle la *dimension* de E qui est notée $\dim_{\mathbb{K}} E$ ou même simplement $\dim E$ s'il n'y a aucune ambiguïté quant au corps considéré. On dit alors que E est de *dimension finie* .

III.1.3 . −Applications linéaires

On a rappelé la définition d'*application linéaire* (cf. la définition III.1.2.1,) il nous arrivera parfois d'employer le terme *morphisme d'espaces vectoriels* ou même *morphisme* si le contexte est clair comme synonyme d'*application linéaire* .

Ainsi les notions d'*isomorphisme* (cf. la définition II.8.2.4,) d'*endomorphisme* (cf. le point i de la définition II.8.2.7,) d'*automorphisme* (cf. le point ii de la définition II.8.2.7,) sont-elles encore pertinentes dans le cadre des *espaces vectoriels* . Et en particulier : **Soit** $u : E \to F$ **une *application linéaire* (ou morphisme de $\mathbb{K}$-*espaces vectoriels* :)**

Proposition III.1.3.1 (application linéaire surjective) *une application linéaire $u : E \to F$ est surjective (cf. le point ii de la définition I.1.13.18,) si et seulement si il existe une partie génératrice de E dont l'image est une partie génératrice de F, si et seulement si il existe une partie de E dont l'image est une partie génératrice de F, si et seulement si l'image de toute partie génératrice de E est une partie génératrice de F , si et seulement si $\operatorname{Im} u = F$;*

Proposition III.1.3.2 (application linéaire injective) *une application linéaire $u : E \to F$ est injective (cf. le point i de la définition I.1.13.18,) si et seulement si l'image de toutepartie libre de E est unepartie libre de F, si et seulement si $\operatorname{Ker} u = 0$;*

Proposition III.1.3.3 (Isomorphisme) *Une application linéaire $u : E \to F$ est un isomorphisme s'il existe une application linéaire $v : F \to E$ telle qaue $v \circ u = \mathrm{Id}_E$ et $u \circ v = \mathrm{Id}_F$.*

Néanmoins comme nous l'avons déjà constaté pour les magmas (cf. la proposition II.7.6,) et pour les groupes (cf. la proposition II.8.2.5,) ici encore, une application $u : E \to F$ est un isomorphisme si et seulement si c'est une application linéaire bijective .

Proposition III.1.3.4 (isomorphisme) *une application linéaire $u : E \to F$ est bijective i.e. un isomorphisme (cf. II.8.2.4, proposition II.8.2.5,) si et seulement si l'image de toute base de E est une base de F, si et seulement si il existe une base de E dont l'image est une base de F ;*

Proposition III.1.3.5 (Image d'une *base*) *Étant donnée une base $\mathcal{B}$ de E et une application $f : \mathcal{B} \to F$, il existe une unique application linéaire*

$$u : E \to F \text{ tel que } \forall b \in \mathcal{B},\ u(b) = f(b)$$

Définition III.1.3.6 (Endomorphisme/Automorphisme) Pour un $\mathbb{K}$-*espace vectoriel* , E,

i) (**Endomorphisme**)
Un *morphisme* $f : E \to E$ de E dans lui-même est appelé *endomorphisme* .
On note

$$\mathrm{End}_{\mathbf{Vect}}(E) \text{ ou } \mathrm{End}_{\mathbb{K}}(E) \text{ ou même simplement } \mathrm{End}(E)$$

l'*ensemble des endomorphismes d'espaces vectoriels* de E.

ii) (**Automorphisme**)
Un *morphisme* $f : E \to E$ est un *automorphisme* si c'est à la fois un *isomorphisme* et un *endomorphisme* . Il revient au même, grâce à la proposition III.1.3.3, de dire que f est un *bijectif* .
On note

$$\mathrm{Aut}_{\mathbf{Vect}}(E) \text{ ou même simplement } \mathrm{Aut}(E)$$

l'*ensemble des automorphismes*

Définition III.1.3.7 (Projecteurs symétries) Soit E un $\mathbb{K}$-*espace vectoriel* .

i) (**Projecteur**)
Un *projecteur* est un *endomorphisme* $p \in \mathrm{End}(E)$ tel que $p \circ p = \mathrm{Id}_E$. Il s'ensuit alors que

$$E = \operatorname{Ker} p \oplus \operatorname{Im} p \text{ (cf. l'exercice III.11.4.1 .)}$$

On dit alors que p est un *projecteur* sur $\operatorname{Im} p$ *parallèlement* à $\operatorname{Ker} p$.

ii) (**Symétrie**)
Une *symétrie* est un *endomorphisme* $s \in \mathrm{End}(E)$ tel que $s \circ s = \mathrm{Id}_E$. Il s'ensuit alors que

$$E = \mathrm{Ker}\,(\mathrm{Id}_E - s) \oplus \mathrm{Ker}\,(\mathrm{Id}_E + s) \text{ (cf. l'exercice III.11.4.2 .)}$$

On dit alors que s est une *symétrie* d'axe $\mathrm{Ker}\,(\mathrm{Id}_E - s)$ *parallèlement* à $\mathrm{Ker}\,(\mathrm{Id}_E + s)$.

Lemme III.1.3.8 (Projecteurs, symétries et sommes directes) *Soient E un $\mathbb{K}$-espace vectoriel F et G des sous-espaces vectoriels . Les assertions suivantes sont équivalentes :*

a) $E = F \oplus G$.

b) Il existe un projecteur $p \in \mathrm{End}(E)$ *tel que*

$$\mathrm{Ker}\, p = F \text{ et } \mathrm{Im}\, p = G\,.$$

c) Il existe une symétrie $s \in \mathrm{End}(E)$ *telle que*

$$\mathrm{Ker}\,(\mathrm{Id}_E - s) = G \text{ et } \mathrm{Ker}\,(\mathrm{Id}_E + s) = F\,.$$

De plus, lorsqu'ils existent, p et s sont uniques.

Démonstration : *Pour l'équivalence b ⇔ c voir l'exercice III.11.4.2 ainsi que pour b ⇒ a ou c ⇒ a.*

Établissons donc que a ⇒ b : Si $p \in \mathrm{End}(E)$ *est un projecteur tel que* $\mathrm{Ker}\, p = F$ *et* $\mathrm{Im}\, p = G$ *, alors, pour tout* $(y,z) \in F \times G$, $p(y) = 0$ *et* $p(z) = z$ *(cf. l'exercice III.11.4.1.)*

Si $E = F \oplus G$ *, pour tout* $x \in E$, *il existe un unique* $(y,z) \in F \times G$ *tel que* $x = y + z$ *. Alors nécessairement*

$$p(x) = p(y+z) = p(y) + p(z) = z\,.$$

On a ainsi montré l'unicité de p.

Reste à vérifier que l'application

$$p : E \to E\,,\ x = y+z \mapsto z$$

satisfait bien le point b.

Le point le moins formel est de vérifier que p ainsi défini est effectivment une application linéaire . Pour tout $(x,x',a,a') \in E \times E \times \mathbb{K} \times \mathbb{K}$, *il exist un unique* $(y,y',z,z') \in F \times F \times G \times G$ *tel que*

$$x = y + z \text{ et } x' = y' + z'\,.$$

Alors

$$ax + a'x' = a(y+z) + a'(y'+z') = ay + a'y' + az + a'az'\,.$$

Puisque la somme $F \oplus G$ *est directe ; puisque* $ay + a'y' \in F$ *; puisque* $az + a'z' \in G$ *; par unicité de la décomposition de* $ax + a'x'$, *on a :*

$$p(ax + a'x') = az + a'z' = ap(x) + a'p(x')\,.$$

Resterait à vérifier que

$$p \circ p = p\,,\ \mathrm{Ker}\, p = F \text{ et } \mathrm{Im}\, p = G\,;$$

ce qui est facile.

La proposition III.1.3.9 qui suit est en fait une généralisation du lemme III.1.3.8 ce-dessus.

Proposition III.1.3.9 (Propriété universelle des sommes directes) *Étant donnée un $\mathbb{K}$-espace vectoriel E et $\mathcal{F}$ un ensemble de sous-espaces vectoriels tel que la somme $\sum_{F \in \mathcal{F}} F = \bigoplus_{F \in \mathcal{F}} F$ est une somme directe , pour tout $\mathbb{K}$-espace vectoriel G et toute famille de morphismes*

$$\big(f_F : F \to G\big)_{F \in \mathcal{F}}$$

il existe un unique morphisme

$$f : \bigoplus_{F \in \mathcal{F}} F \to G \text{ tel que } \forall F \in \mathcal{F},\ f_{|F} = f_F .$$

Définition III.1.3.10 (Sous-espace stable) Étant donnés un $\mathbb{K}$-*espace vectoriel* E et un endomorphisme $\mathbb{K}$-linéaire $u \in \mathrm{End}_{\mathbb{K}}(E)$, on dit qu'une partie (éventuellement un sous-espace) $F \subset E$, est *stable par* u ou *stable sous* u ou même u-*stable* si $u(F) \subset F$.

III.1.4 . −Somme directe, supplémentaire

Définition III.1.4.1 (Somme de sous-$\mathbb{K}$-*espaces vectoriels*) Étant donné un *ensemble* $\mathcal{F}$ de sous-$\mathbb{K}$-*espaces vectoriels* d'un $\mathbb{K}$-*espace vectoriel* E, on appelle *somme* des sous-$\mathbb{K}$-*espaces vectoriels* $F \in \mathcal{F}$, le sous-$\mathbb{K}$-*espace vectoriel* noté $\sum_{F \in \mathcal{F}} F$, *engendré* par la *réunion* des $F \in \mathcal{F}$ *i.e.*

$$\sum_{F \in \mathcal{F}} F = \mathrm{Vect}\big(\bigcup_{F \in \mathcal{F}} F\big) .$$

Définition III.1.4.2 i) (**Somme directe**)
Étant donné un *ensemble* $\mathcal{F}$ de sous-$\mathbb{K}$-*espaces vectoriels* d'un $\mathbb{K}$-*espace vectoriel* E, on dit que la *somme* $\sum_{F \in \mathcal{F}} F = \mathrm{Vect}\big(\bigcup_{F \in \mathcal{F}} F\big)$ est une *somme directe* si, pour tout $x \in \sum_{F \in \mathcal{F}} F$ il existe un unique $r \in \mathbb{N}$ et un unique r-uplet
$(x_i)_{1 \le i \le r} \in \bigcup_{F \in \mathcal{F}} F$ tel que $\forall 1 \le i \le r,\ x_i \neq 0$ et $x = \sum_{i=1}^{r} x_i$. On notera alors

$$\sum_{F \in \mathcal{F}} F = \mathrm{Vect}\big(\bigcup_{F \in \mathcal{F}} F\big) = \bigoplus_{F \in \mathcal{F}} F .$$

Dans le cas où $\mathcal{F} = (F_i)_{1 \le i \le n}$ est une famille finie de sous-$\mathbb{K}$-*espaces vectoriels* de E, la *somme* $F_1 + \ldots + F_n$ est une *somme directe* si, pour tout
$x \in F_1 + \ldots + F_n$ il existe un unique n-uplet $(x_i)_{1 \le i \le n} \in F_1 \times \ldots \times F_n$ tel que $x = \sum_{i=1}^{n} x_i$.

On notera alors

$$F_1 + \ldots + F_n = F_1 \oplus \ldots \oplus F_n .$$

ii) (**Sous-$\mathbb{K}$-*espace vectoriel* supplémentaire**)
Pour un sous-$\mathbb{K}$-*espace vectoriel* $F \subset E$ de E on dit qu'un sous-$\mathbb{K}$-*espace vectoriel* $G \subset E$ de E est un *supplémentaire* de F si $E = F \oplus G$ est la *somme directe* de F et G.

Lemme III.1.4.3 (Supplémentaire) *un sous-espace F possède toujours un supplémentaire G, i.e. il existe un sous-espace*

$$G \text{ tel que } E = F \oplus G \text{ (cf. III.1.2.ix.a.)}$$

Notation III.1.5 Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$, un *graphe fini simple non-orienté* (cf. la définition I.4.4.)

i) On rappelle que $\mathbb{K}^{\mathcal{V}(G)}$ (cf. I.1.13.13,) est l'*ensemble* des *application* s de $\mathcal{V}(G)$ dans $\mathbb{K}$. Afin d'alléger un peu la notation, on notera, dans tout ce qui suit $\mathbb{K}^G := \mathbb{K}^{\mathcal{V}(G)}$.

ii) Puisque $(\mathbb{K}, +)$ est en particulier un *groupe* et même un *groupe commutatif* , on dispose d'une *loi interne* naturelle (ou canonique) (cf. la proposition II.8.1.7,) $+_{\mathbb{K}^G} : \mathbb{K}^G \times \mathbb{K}^G \to \mathbb{K}^G$ définie par $\forall (u, \alpha, \beta) \in \mathcal{V}(G) \times \mathbb{K}^G \times \mathbb{K}^G$, $(\alpha +_{\mathbb{K}^G} \beta)(u) := \alpha(u) + \beta(u)$. On notera évidemment simplement $\alpha + \beta$.

iii) De la même manière, la
multiplication $*$ sur $\mathbb{K}$ définit une *loi externe* $\cdot_{\mathbb{K}^G} : \mathbb{K} \times \mathbb{K}^G \to \mathbb{K}^G : \forall (u, a, \alpha) \in \mathcal{V}(G) \times \mathbb{K} \times \mathbb{K}^G$, $(a \cdot_{\mathbb{K}^G} \alpha)(u) := a * \alpha(u)$. Ici encore on notera simplement $a \cdot \alpha$ voire $a\alpha$.

Proposition III.1.6 (Structure de $\mathbb{K}$-*espace vectoriel* sur $\mathbb{K}^G$) *Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ un graphe fini simple non-orienté .*

i) Le triplet $(\mathbb{K}^G, +_{\mathbb{K}^G}, \cdot_{\mathbb{K}^G})$ est un $\mathbb{K}$-espace vectoriel au sens de la définition III.1.2.1.

***Démonstration** : Ce sont des vérifications très formelles laissées en exercice.*

ii) Pour tout $u \in \mathcal{V}(G)$ on note :

$$\begin{array}{rccl} \alpha_u : & \mathcal{V}(G) & \longrightarrow & \mathbb{K} \\ & u & \longmapsto & 1 \\ & v \neq u & \mapsto & 0 \, ; \end{array} \qquad 1$$

autrement dit $\forall (u, v) \in \mathcal{V}(G) \times \mathcal{V}(G)$, $\alpha_u(v) = \delta_{u,v}$.

Alors

$$\mathcal{B}_G := \{\alpha_u\}_{u \in \mathcal{V}(G)} \text{ est une base (cf. la définition III.1.2.8,) de } \mathbb{K}^G . \qquad 2$$

si bien que

$$\dim_{\mathbb{K}} \mathbb{K}^G = \#\big(\mathcal{V}(G)\big) . \qquad 3$$

***Démonstration** :*

$\mathcal{B}_G$ est génératrice Puisque $\mathcal{V}(G)$ est un ensemble fini , $\forall \alpha \in \mathbb{K}^G$, $\alpha = \sum_{\beta \in \mathcal{B}_G} \alpha(u)\beta = \sum_{u \in \mathcal{V}(G)} \alpha(u)\alpha_u$; ce qui assure que $\mathcal{B}_G$ est une partie génératrice de $\mathbb{K}^G$.

$\mathcal{B}_G$ est libre *Pour tout $(a_u)_{u\,\in\,\mathcal{V}(G)}\,\in\,\mathbb{K}$, rappelons une fois encore que $\sum_{u\,\in\,\mathcal{V}(G)} a_u\alpha_u$ a un sens et est une combinaison linéaire des $(\alpha_u)_{u\,\in\,\mathcal{V}(G)j}$, puisque $\mathcal{V}(G)$ est un ensemble fini . Alors :*

$$\begin{aligned}
&\sum_{u\,\in\,\mathcal{V}(G)} a_u\alpha_u &&= 0\\
\Rightarrow\ \forall v\in\mathcal{V}(G),\quad &\left(\sum_{u\,\in\,\mathcal{V}(G)} a_u\alpha_u\right)(v) &&= 0\\
\Rightarrow\ \forall v\in\mathcal{V}(G),\quad &\sum_{u\,\in\,\mathcal{V}(G)} a_u\alpha_u(v) &&= 0\\
\Rightarrow\ \forall v\in\mathcal{V}(G),\quad &\sum_{u\,\in\,\mathcal{V}(G)} a_u\delta_{u,v} &&= 0\\
\Rightarrow\ \forall v\in\mathcal{V}(G),\quad &a_v &&= 0\,.
\end{aligned}$$

$\mathcal{B}_G$ est donc une partie libre de $\mathbb{K}^G$. Un autre argument sera donné à la remarque III.2.3.

Définition III.1.7 (Endomorphisme d'adjacence) Étant donné un *graphe fini simple non-orienté* $G := \big(\mathcal{V}(G),\mathcal{E}(G),\varepsilon(G)\big)$, l'*endomorphisme d'adjacence* $\Phi(G)$ est l'*endomorphisme* de $\mathbb{K}^G$ défini par :

$$\forall(\alpha,u)\in\mathbb{K}^G\times\mathcal{V}(G),\ \Phi(G)(\alpha)(u) := \sum_{v\,\in\,N_G(u)}\alpha(v)\,.$$

Proposition III.1.8 *Soit $G := \big(\mathcal{V}(G),\mathcal{E}(G),\varepsilon(G)\big)$ un graphe fini simple non-orienté . L'application $\Phi(G)$ de la définition III.1.7 est bien un endomorphisme de $\mathbb{K}^G$; ce qui justifie l'appellation d'endomorphisme d'adjacence .*

***Démonstration** : Il est immédiat de vérifier que $\forall(\alpha,\beta)\in\mathbb{K}^G\times\mathbb{K}^G,\ \forall(a,b)\in\mathbb{K}\times\mathbb{K},\ \Phi(G)(a\alpha+b\beta) = a\Phi(G)(\alpha)\,+\,b\Phi(G)(\beta)$.*

Définition III.1.9 (Matrice d'adjacence) Étant donné un *graphe fini simple non-orienté* (cf. la définition I.4.4,) $G := \big(\mathcal{V}(G),\mathcal{E}(G),\varepsilon(G)\big)$, la *matrice d'adjacence* de G est la *matrice* $\mathcal{A}(G)$ définie par

$$\Big(a(G)_{u,v}\Big)_{\substack{u\,\in\,\mathcal{V}(G)\\ v\,\in\,\mathcal{V}(G)}} := \#\big(\varepsilon(G)^{-1}\big(\{\{u,v\}\}\big)\big)\,.$$

Proposition III.1.10 *Soit $G := \big(\mathcal{V}(G),\mathcal{E}(G),\varepsilon(G)\big)$ un graphe fini simple non-orienté . La matrice de $\Phi(G)$ dans la base $\mathcal{B}_G$ (cf. III.1.6.ii.2,) est la matrice d'adjacence de G au sens de la définition III.1.9.*

***Démonstration** : Pour tout $(u,v,w)\,\in\,\mathcal{V}(G)\times\mathcal{V}(G)\times\mathcal{V}(G)$, $\sum_{u\,\in\,N_G(w)}\alpha_v(u)$ est égal à 1 si $v\,\in\,N_G(w)$ et 0 sinon. Or $v\,\in\,N_G(w)\,\Leftrightarrow\,w\,\in\,N_G(v)$; si bien que*

$$\begin{aligned}
\sum_{u\,\in\,N_G(w)}\alpha_v(u) &= \sum_{u\,\in\,N_G(v)}\alpha_w(u)\\
&= \sum_{u\,\in\,N_G(v)}\delta_{u,w}\\
&= \sum_{u\,\in\,N_G(w)}\alpha_u(w)\,.
\end{aligned}$$

Il s'ensuit que

$$\begin{aligned}\forall (v,w) \in \mathcal{V}(G) \times \mathcal{V}(G), \quad \Phi(G)(\alpha_v)(w) &= \sum_{u \,\in\, N_G(w)} \alpha_v(u) \\ &= \sum_{u \,\in\, N_G(v)} \alpha_u(w)\ ;\end{aligned}$$

ce qui entraîne finalement que

$$\forall v \in \mathcal{V}(G),\ \Phi(G)(\alpha_v) = \sum_{u \,\in\, N_G(v)} \alpha_u\ ;$$

ce qui correspond à la définition III.1.9 de la matrice d'adjacence .

Exemple III.1.11 (Matrices d'adjacence) Les *matrices d'adjacence* des *graphes finis simples non-orientés* déjà présentées I.4.9 à I.4.15 peuvent être déterminées sans difficulté :

a) (**Graphe isolé**)
Pour tout *entier naturel* $n \in \mathbb{N}$ la *matrice d'adjacence* du *graphe isolé* $\mathbf{I}_n$ (cf. la définition I.4.9,) est la *matrice nulle* .

b) (**Graphe complet**)
Pour le *graphe complet* (cf. la définition I.4.14,) on a :

$$\begin{aligned}\mathcal{A}(Gphcmp2) &= \begin{pmatrix}0&1\\1&0\end{pmatrix} \\ \mathcal{A}(Gphcmp3) &= \begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix} \\ \mathcal{A}(Gphcmp4) &= \begin{pmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix}\ .\end{aligned}$$

c) (**Chemin**)
Pour le *chemin* (cf. la définition I.4.10,) on a :

$$\begin{aligned}\mathcal{A}(\mathbf{P}_1) &= \begin{pmatrix}0&1\\1&0\end{pmatrix} \\ \mathcal{A}(\mathbf{P}_2) &= \begin{pmatrix}0&1&0\\1&0&1\\0&1&0\end{pmatrix} \\ \mathcal{A}(\mathbf{P}_3) &= \begin{pmatrix}0&1&0&0\\1&0&1&0\\0&1&0&1\\0&0&1&0\end{pmatrix}\ .\end{aligned}$$

d) (**Cycle**)
Pour le *cycle* (cf. la définition I.4.12,) on a :

$$\begin{aligned}\mathcal{A}(\mathbf{C}_2) &= \begin{pmatrix}0&1\\1&0\end{pmatrix}\\ \mathcal{A}(\mathbf{C}_3) &= \begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix}\\ \mathcal{A}(\mathbf{C}_4) &= \begin{pmatrix}0&1&0&1\\1&0&1&0\\0&1&0&1\\1&0&1&0\end{pmatrix}.\end{aligned}$$

Remarque III.1.12 (Matrice d'adjacence) Étant donné un *graphe fini simple non-orienté* G,

i) (**Symétrie**)
la *matrice d'adjacence* $\mathcal{A}(G)$ de G est une *matrice symétrique* : $\forall (u,v) \in \mathcal{V}(G)\times\mathcal{V}(G),\ a(G)_{u,v} = a(G)_{v,u}$;

ii) (**Diagonale**)
$\forall u \in \mathcal{V}(G),\ a(G)_{u,u} = 0$; puisqu'un *graphe simple* (cf. la définition I.4.1,) n'a pas de *boucle* ;

iii) (**Trace**)
En particulier le point ii entraîne que $\mathrm{tr}(\mathcal{A}(G)) = 0$.

iv) (**Valeurs**)
toujours parce que G est un *graphe simple* , $\forall (u,v) \in \mathcal{V}(G)\times\mathcal{V}(G),\ a(G)_{u,v} = 0$ ou 1 .

Notation III.1.13 (Matrice/endomorphisme d'adjacence) Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ un *graphe fini simple non-orienté* . On notera $\mathcal{A}(G) := \Big(a(G)_{u,v}\Big)_{\substack{u\in\mathcal{V}(G)\\ v\in\mathcal{V}(G)}}$ la *matrice d'adjacence* de G ; et pour tout $n \in \mathbb{N}, \mathcal{A}(G)^n := \Big(a^{(n)}_{u,v}(G)\Big)_{\substack{u\in\mathcal{V}(G)\\ v\in\mathcal{V}(G)}}$.

Proposition III.1.14 (Itérés de la matrice d'adjacence et parcours sur le graphe) *Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ un graphe fini simple non-orienté (cf. la définition I.2.8.) Pour deux sommets v et w le nombre de parcours de longueur ℓ (cf. le point i de la définition II.6.2.1,) est le coefficient (v,w) de la puissance $\ell^{\text{ième}}$ de la matrice d'adjacence :*

$$\forall (v,w,\ell) \in \mathcal{V}(G)\times\mathcal{V}(G)\times\mathbb{N},\ \#\big(P_{v,w,\ell}(G)\big) = a^{(\ell)}_{v,w}(G)\ .$$

Démonstration *: (cf. l'exercice III.11.7.1.)*

Proposition III.1.15 (Le cas sommet-transitif) *Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ un graphe fini simple non-orienté . Si G est sommet-transitif (cf. la définition II.5.6,)*

$$\forall (v,\ell) \in \mathcal{V}(g),\ \#\left(P_{v,v,\ell}(G)\right) = \frac{\mathrm{tr}(\mathcal{A}(G))}{\#\big(\mathcal{V}(G)\big)}\ .$$

Démonstration *: C'est une conséquence de la proposition III.1.14 et de la proposition II.6.2.3.*

III.2 . −Structure hermitienne (euclidienne) sur $\mathbb{K}^G$

Notation III.2.1 i) Dans la suite on suppose que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Pour tout $z \in \mathbb{C}$, on note $\overline{z}$ son conjugué ; et pour $z \in \mathbb{R}$, on a donc $\overline{z} = z$.

ii) On pose $\forall (\alpha, \beta) \in \mathbb{K}^G \times \mathbb{K}^G,\ \langle \alpha \mid \beta \rangle := \sum_{u \in \mathcal{V}(G)} \overline{\alpha(u)}\beta(u)$; cette formule s'écrivant simplement $\langle \alpha \mid \beta \rangle = \sum_{u \in \mathcal{V}(G)} \alpha(u)\beta'(u)$ si $\mathbb{K} = \mathbb{R}$.

Proposition III.2.2 (Structure hermitienne/euclidienne sur $\mathbb{K}^G$) *Étant donné un graphe fini simple non-orienté $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$, $\mathbb{K}$ étant $\mathbb{R}$ (resp. $\mathbb{C}$,)*

*i) (**Produit scalaire**)*
Le couple $\big(\mathbb{K}^G, \langle \cdot \mid \cdot \rangle\big)$ est un espace euclidien (cf. la définition III.9.1,) (resp. un espace hermitien (cf. la définition III.9.2.))

***Démonstration** : Puisque G est un graphe fini non-orienté $\mathbb{K}^G$ est un $\mathbb{K}$-espace vectoriel de dimension finie (cf. III.1.6.ii.3.)*

Reste donc à vérifier que la formule du point ii de la notation III.2.1, définit bien un produit scalaire euclidien (cf. la définition III.8.1,) (resp. un produit scalaire hermitien (cf. la définition III.8.2.)) La plupart du temps, il est presque immédiat de vérifier que l'axiome Eucl_1 de la définition III.8.1 (resp. Herm_1,) et l'axiome Eucl_2 de la définition III.8.1 (resp. Herm_2,) sont satisfaits. Il en va presque de même ici pour l'axiome Eucl_4 de la définition III.8.1 (resp. Herm_4,) et l'axiome Eucl_3 de la définition III.8.1 (resp. Herm_3.) En effet pour tout $\alpha \in \mathbb{K}^G$ $\langle \alpha \mid \beta \rangle = \sum_{u \in \mathcal{V}(G)} \overline{\alpha(u)}\alpha(u)$ est une somme de réels positifs qui est donc positive et nulle si et seulement si $\forall u \in \mathcal{V}(G),\ \alpha(u) = 0$.

*ii) (**Base orthonormée**)*
La base $\mathcal{B}_G$ définie en III.1.6.ii.2 est orthonormale (cf. le point iii de la définition III.8.5.)

***Démonstration** : Il est immédiat de vérifier que $\forall (u, v) \in \mathcal{V}(G) \times \mathcal{V}(G),\ \langle \alpha_u \mid \alpha_v \rangle = \delta_{u,v}$.*

Remarque III.2.3 (Orthogonalité) Le fait que $\langle \alpha_u \mid \alpha_v \rangle = \delta_{u,v}$ et le point b de la question 2 de l'exercice III.11.2.4 assurent également que $\mathcal{B}_G$ est une *partie libre* de $\mathbb{K}^G$.

III.3 . −Spectre d'un graphe

Dans ce paragraphe (III.3) le *corps* $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

Définition III.3.1 (Spectre d'un graphe fini simple non-orienté) Étant donné un *graphe fini simple non-orienté* $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$, le *spectre* $\text{Sp}(G)$ est, par définition, le *spectre* $\text{Sp}(\Phi(G))$ de l'*endomorphisme d'adjacence* $\Phi(G)$ de G (cf. la définition III.1.7,) au sens du point ii de la définition III.7.3.4.

Proposition III.3.2 (Endomorphisme auto-adjoint) *Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ un graphe fini simple non-orienté . L'endomorphisme d'adjacence $\Phi(G)$ (cf. la définition III.1.7,) est auto-adjoint (cf. la définition III.10.5,) pour le produit scalaire donné par la formule III.2.1.ii.*

Démonstration : *On peut bien entendu voir ce résultat comme une conséquence du fait que la base $\mathcal{B}_G$ est orthonormée (cf. le point ii de la proposition III.2.2,) et que la matrice de $\Phi(G)$ (cf. la proposition III.1.10,) est une matrice symétrique (cf. le point i de la remarque III.1.12.) On applique ensuite la proposition III.10.6.*

On peut aussi donner un calcul direct qui découle du même fait, à savoir que, puisque G est un graphe non-orienté , $\forall (u,v) \in \mathcal{V}(G) \times \mathcal{V}(G),\ v \in N_G(u) \Leftrightarrow u \in N_G(v)$,

$$\begin{aligned}
\forall (\alpha,\beta) \in \mathbb{K}^G \times \mathbb{K}^G,\quad \langle \Phi(G)(\alpha) \mid \beta \rangle &= \sum_{u \in \mathcal{V}(G)} \overline{\Phi(G)(\alpha)(u)}\beta(u) \\
&= \sum_{u \in \mathcal{V}(G)} \overline{\sum_{v \in N_G(u)} \alpha(v)\beta(u)} \\
&= \sum_{u \in \mathcal{V}(G)} \sum_{v \in N_G(u)} \overline{\alpha(u)}\beta(v) \\
&= \sum_{(u,v) \in \mathcal{V}(G)\times\mathcal{V}(G)\ ,\ v \in N_G(u)} \overline{\alpha(u)}\beta(v) \\
&= \sum_{(u,v) \in \mathcal{V}(G)\times\mathcal{V}(G)\ ,\ u \in N_G(v)} \overline{\alpha(u)}\beta(v) \\
&= \langle \alpha \mid \Phi(G)(\beta) \rangle\ .
\end{aligned}$$

Proposition III.3.3 (Diagonalisabilité) *Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ un graphe fini simple non-orienté . L'endomorphisme d'adjacence $\Phi(G)$ est diagonalisable (cf. la définition III.7.2.3 ;) et*

$$\mathrm{Sp}(G) \subset \mathbb{R}\,.$$

Démonstration : *C'est une conséquence de la proposition III.3.2 et du théorème III.10.9.*

Exemple III.3.4 (Exemples de spectres) Voir l'exercice III.11.6.1, l'exercice III.11.6.2, l'exercice III.11.6.3,

Proposition III.3.5 (Graphes k-réguliers)

III.4 . −Divisibilité dans les anneaux, PPCM PGCD

Dans ce paragraphe (III.4,) A est un *anneau intègre* (cf. la définition III.1.1.6.) On notera $A^\times$ l'*ensemble des éléments inversibles* de A (cf. la définition III.1.1.9.)

Définition III.4.1 (Idéal) Étant donné un anneau commutatif $(A,+,*)$, une partie $\mathfrak{I} \subset A$ de A est un *idéal* si $\mathfrak{I}$ est un sous-groupe (cf. la définition II.8.3.1,) de $(A,+)$ tel que $\forall (a,x) \in A \times \mathfrak{I},\ a * x \in \mathfrak{I}$.

Notation III.4.2 Si $a \in A$, on note $aA := \{b \in A\ ;\ \exists c \in A,\ b = ac\}$ qui est l'idéal engendré par $\{a\}$. Un tel idéal est dit *principal*

Exemple III.4.3 (Idéaux) a) Les sous-ensembles $\{0\}$, et A de A sont des idéaux de A. Ce sont les seuls idéaux de A si A est un corps.

b) Le noyau d'un *morphisme d'anneaux* $f : A \to B$ est toujours un idéal de A.

c) Les idéaux de l'anneau $(\mathbb{Z}, +, *)$ sont exactement les sous-groupes du groupe $(\mathbb{Z}, +)$ c'est-à-dire les sous-ensemble de $\mathbb{Z}$ de la forme $d\mathbb{Z}$ avec $d \in \mathbb{Z}$.

d) (**Idéaux de** $A[X]$)
Pour tout entier $v \in \mathbb{N}$

$$\mathfrak{I} := \{\alpha \in A[X](\text{resp. } A[[X]]) \; ; \; \text{val}(\alpha) \geq v\} \text{ (cf. la définition III.6.1.16 ,)}$$

est un idéal de $A[X]$ (resp. $A[[X]]$,) qui s'identifie en fait à lidéal

$$\begin{array}{c} X^v A[X] \text{ (resp. } X^v A[[X]]) \\ = \quad \{\alpha \in A[X] \text{ (resp. } A[[X]]) \; ; \; \exists \beta \in A[X] \text{ (resp. } A[[X]]), \; \alpha = X^v \beta\} \end{array} \quad \text{(cf. la notation III.4.2 .)}$$

(cf. le point d de la question 3 de l'exercice III.11.3.4 pour d'autres exemples.)

Définition III.4.4 (Divisibilité) Pour tout couple $(a, b) \in A \times A$, on dit que a *divise* b ou que a est un *diviseur* de b ou encore que b est un *multiple* de a et l'on note $a|b$, s'il existe $c \in A$ tel que $a * c = b$.

Notation III.4.5 On notera

$$\forall X \subset A \; , \; \mathcal{D}(X) := \{y \in A \; ; \; \forall x \in X, \; y|x\} \text{ (resp. } \mathcal{M}(X) := \{y \in A \; ; \; \forall x \in X, \; x|y\} \text{)}$$

l'ensemble des diviseurs (resp. multiples) communs à tous les éléments de X.

De manière un peu abusive, on notera encore

$$\mathcal{D}(x, y) := \mathcal{D}(\{x, y\}) \text{ (resp. } \mathcal{M}(x, y) := \mathcal{M}(\{x, y\}) \text{ .)}$$

Définition III.4.6 (Élément premier) Un élément $x \in A$ de A est dit *premier* si $x \notin A^\times$ n'est pas un *élément inversible* (cf. la définition III.1.1.9,) et $\forall y \in A, \; \forall z \in A, \; \big(x|y * z \; \Rightarrow \; x|y \; \vee \; x|z\big)$.

Définition III.4.7 (Éléments irréductibles) Un élément $x \in A$ de A est dit *irréductible* si $x \notin A^\times$ n'est pas inversible (cf. la définition III.1.1.9,) et $\forall y \in A, \; \forall z \in A, \; \big(y * z = x \; \Rightarrow \; y \in A^\times \; \vee \; z \in A^\times\big)$.

Remarque III.4.8 Les définitions III.4.7 et III.4.6 sont présentées ici de manière tout à fait indépendantes l'une de l'autre contrairement à l'habitude qu'on peut en avoir en travaillant dans les anneaux usuels $\mathbb{Z}$ ou $\mathbb{K}[X]$. Ces deux notions n'entretiennent en effet de rapports étroit que si on fait des hypothèses sur l'anneau A. Un premier résultat sera obtenu à la proposition III.4.9 en supposant que A est intègre. Finalement dans le cas des anneaux principaux , en particulier dans le cas de l'anneau $\mathbb{K}[X]$ considérér ici, le lemme de GAUSS et son corollaire le lemme d'EUCLIDE (cf. le théorème III.6.5.2.4,) permettra de « presque » confondre les deux notions d'irréductibilité et de primalité et de retrouver la définition usuelle de *nombre premier*

Proposition III.4.9 *Dans un anneau commutatif intègre A, tout élément premier (cf. la définition III.4.6,) non nul est irréductible (cf. la définition III.4.7.)*

Démonstration *: Soit en effet $p \in A$ et $(a, b) \in A \times A$ tels que $p = a * b$. Alors $p|a * b$ et puisque p est premier , $p|a$ ou $p|b$. Si $p|a$ il existe $c \in A$ tel que $a = p * c$. L'égalité $p = a * b$ entraîne alors $p = p * c * b$ qui entraîne encore*

$$p * (1 - c * b) = 0 \; .$$

Or $p \neq 0$ et A est intègre donc

$$c * b = 1$$

c'est-à-dire que b est inversible, ce qui assure que p est irréductible .

Définition III.4.10 Pour $X \subset A$, si $\mathcal{D}(X) = A^\times$ on dit que les éléments de X sont *premiers entre eux (dans leur ensemble)*.

Lemme III.4.11 ((cf. III.4.3.c,))

$$\forall (a,b) \in A \times A,\ a|b \Leftrightarrow bA \subset aA \Leftrightarrow b \in aA$$

(où aA est l'idéal principal engendré par a ,)

Définition III.4.12 (Éléments associés) Pour $(x,y) \in A \times A$, on dit que y est *associé* à x s'il existe un *élément inversible* $u \in A^\times$, tel que $y = u * x$.

Lemme III.4.13 *La relation d'association (cf. III.4.12,) est une relation déquivalence dont les classes seront appelées classes d'association .*

Démonstration *: (cf. l'exercice III.11.3.5.)*

Lemme III.4.14 *Si A est un anneau intègre, pour tout $(a,b) \in A \times A$, les assertions suivantes sont équivalentes :*

a) $a|b$ et $b|a$;

b) $aA = bA$;

c) $\exists u \in A^\times,\ b = a * u$;

d) $\exists u \in A^\times,\ a = b * u$;

e) a *et* b *sont associés.*

Démonstration *:*

i) ***(a $\Leftrightarrow$ b)***
L'équivalence entre a et b est une conséquence immédiate du lemme III.4.11.

ii) ***(c $\Rightarrow$ d $\Leftrightarrow$ e)***
L'équivalence entre c et d signifie exactement que la relation « être associés » est symétrique. L'équivalence avec e est tautologique.

iii) ***(c $\Rightarrow$ a)***
Puisque d et c sont équivalentes, c entraîne c et d qui entraînent tautologiquement a.

iv) ***(a $\Rightarrow$ d)***

Remarque iv.1 Notons que dans cette partie seulement de la démonstration l'hypothèse que A est intègre sera utilisée.

Si $a|b$ et $b|a$, il existe $(u,v) \in A \times A$ tels que $a = b*u$ et $b = a*v$. Il s'ensuit que $a = a*v*u$ ou encore que $a*(1-v*u) = 0$.
$a = 0$ Si $a = 0$, $a|b$ entraîne $b = 0$, et pour tout $w \in A^\times$, $a = b*w$.
$a \neq 0$ Si $a \neq 0$, puisque A est intègre $1 - v*u = 0$ c'est-à-dire que $v*u = 1$ si bien que u et v sont inversibles, ce qui achève la preuve.

Définition III.4.15 (Pgcd Ppcm) Étant donné un ensemble $X \subset A$, on appelle *plus grand commun diviseur* ou ***Pgcd*** (resp. *plus petit commun multiple* ou ***Ppcm***)

$$\text{un plus grand élément de } \mathcal{D}(X) (\text{resp. un plus petit élément de } \mathcal{M}(X),)$$

au sens de la relation | bien entendu, autrement dit, un élément $d \in \mathcal{D}(X)$ (resp. $m \in \mathcal{M}(X)$) tel que :

$$\forall a \in X,\ d|a \text{ et } \forall b \in \mathcal{D}(X),\ b|d \text{ (resp. } \forall a \in X,\ a|m \text{ et } \forall b \in \mathcal{M}(X),\ m|b \text{ .)} \qquad \text{III.4.15.1}$$

Lemme III.4.16 *Étant donné une partie $X \subset A$, tous les **Pgcd** (resp. **Ppcm**) de X s'ils existent engendrent un même idéal De manière équivalente (cf. le lemme III.4.14,) ils constituent une même classe d'association.*

Démonstration *: An effet si d et d' (resp. m et m') sont deux **Pgcd** (resp. **Ppcm**) de X, par définition on a*

$$d'|d \text{ et } d|d' \text{ (resp. } m'|m \text{ et } m|m' \text{)}$$

ce qui entraîne, en vertu du lemme III.4.11 $dA = d'A$ (resp. $A = m'A$.)

Notation III.4.17 Le lemme ci-dessus peux motiver les notations suivantes : Pour $X \subset A$ d (resp. m) un **Pgcd** (resp. **Ppcm**) de X, on notera :

$$\bigwedge X := dA \text{ et } (X\vee\ ) := mA\ . \qquad \text{III.4.17.1}$$

Pour tout $(x, y) \in A \times A$, on notera :

$$x \wedge y := \bigwedge \{x, y\} \text{ et } (x, y\vee\ ) = (\{x, y\}\vee\ ). \qquad \text{III.4.17.2}$$

Remarque III.4.18 (Éléments inversibles) L'*ensemble des éléments inversibles* $\mathbb{K}[X]^\times$ des de l'*anneau* $(\mathbb{K}[X], +, *)$ s'identifie au *groupe des éléments inversibles* $\mathbb{K}^\times$ de $\mathbb{K}$ lui-même (cf. le point iii de la proposition III.6.2.5.)

Remarque III.4.19 (Éléments associés) Par conséquent, deux éléments P et Q de $\mathbb{K}[X]$ sont *associés* (cf. la définition III.4.12,) si et seulement s'il existe $u \in \mathbb{K}^\times$ tel que $P = u * Q$.

III.5 . −Anneau quotient et factorisation des morphismes

Remarque III.5.1 On a remarqué (cf. le point a de l'exemple III.1.1.8,) que pour un *morphisme d'anneaux* $f : A \to B$, le noyau $\operatorname{Ker} f$ de f n'est pas un sous-anneau de A. En revanche, puisque c'et le noyau du *morphisme de groupes*
$f : (A, +) \to (B, +)$ c'est un sous-groupe de $(A, +)$ (cf. II.8.3.10.)

De plus pour tout couple (x, y) d'éléments de $\operatorname{Ker} f$ et tout couple $((a, b)$ d'éléments de A, puisque f est un *morphisme d'anneaux* ,

$$f(a * x + b * y) = a * f(x) + b * f(y) = 0,$$

si bien que $a * x + b * y \in \operatorname{Ker} f$. On constate que le noyau d'un *morphisme d'anneaux* est un idéal (cf. la définition III.4.1.)

Remarque III.5.2 Pour un anneau $(A, +, *)$ puisque $(A, +)$ est un groupe abélien tout idéal $\mathfrak{I}$ de A est en particulier un *sous-groupe distingué* de $(A, +)$. les consttructions de la section II.8.11 peuvent s'appliquer mutatis mutandis. Néanmoins elles sont plus riches en générale, puisqu'on dispose d'une *structure* plus riche que celle de *groupe* .

Proposition III.5.3 (Relations déquivalences compatibles) *Soient $(A, +, *)$ un anneau commutatif et $\mathfrak{I}$ un idéal de A la relation $\sim_{\mathfrak{I}}$ définie par*

$$\forall (x, y) \in A \times A,\ x \sim_{\mathfrak{I}} y \ \Leftrightarrow\ y - x \ \in\ \mathfrak{I}$$

est une relation d'équivalence compatible aux lois $+$ et $*$ de A. Il s'ensuit qu'il existe une unique structure d'anneau sur le quotient $A/\mathfrak{I} := A/\sim_{\mathfrak{I}}$ telle que la surjection canonique $\pi : A \to A/\mathfrak{I}$ soit un morphisme d'anneaux .

***Démonstration** : On a déjà remarqué mais on rappelle encore que $(A, +)$ étant un groupe abélien, et $\mathfrak{I}$ un sous-groue, il est distingué (cf. II.8.10.7.b.) On constate que, de plus, la relation $\sim_{\mathfrak{I}}$ définie ici est exactement celle définie dans la section II.8.10. Il s'ensuit que la proposition II.8.11.1 s'applique si bien qu'il existe une unique structure de groupe (encore notée $+$) sur $A/\mathfrak{I}$ telle que*

$$\pi : (A, +) \to (A/\mathfrak{I}, +)$$

soit un morphisme de groupes .

De plus :

$$\begin{array}{lrcl}
\forall x \in A,\ \forall z \in A, & & & \\
\forall y \in A,\ \forall t \in A, & x \sim_{\mathfrak{I}} z & \text{et} & y \sim_{\mathfrak{I}} t \\
\Rightarrow & z * t - x * y & = & z * t - z * y + z * y - x * y \\
 & & = & z * (t - y) + y * (z - x) \\
 & & \in & \mathfrak{I} \\
\Rightarrow & z * t & \sim_{\mathfrak{I}} & x * y
\end{array}$$

c'est-à-dire, du fait que I est un idéal, que la relation $\sim_{\mathfrak{I}}$ est compatible à $*$ et qu'il existe donc une unique loi $*$ sur $A/\mathfrak{I}$ telle que

$$\forall x \in A,\ \forall y \in A,\ \pi(x * y) \ =\ \pi(x) * \pi(y)$$

(cf. II.7.19.)

Il reste encore à vérifier que $(A/\mathfrak{I}, +, *)$ satisfait aux axiomes Ann_2 à Ann_4 de la définition III.1.1.1 et que π vérifie bien la définition III.1.1.2.

Certaines des propriétés de la *surjection canonique* $\pi : A \to A/\mathfrak{I}$ sont, pour ainsi dire, presque évidentes au vu de ce qui précède mais il n'est pas mauvais de les dégager de manière formelle :

Proposition III.5.4 (Propriétés de la surjection canonique) *Dans la situation de la proposition III.5.3 :*

i) Le morphisme π est surjectif .

ii) $\mathrm{Ker}\,\pi \ =\ \mathfrak{I}$.

Démonstration *:*

i) Remarqons encore une fois que pour tout élément $\alpha \in A/I$, α *est une classe d'équivalence qui est par conséquent non vide. Les écritures* $x \in \alpha$ *ou* $\pi(x) = \alpha$ *renvoient toute deux au même fait que* $x \in A$ *est un représentant de la classe* α.

Les expressions « x est au-dessus de α » « x relève α » ou « x est un relèvement de α » pourraient bien échapper au rédacteur de ces lignes sans qu'elles signfient pourtant ni plus ni moins que

$$\pi(x) = \alpha\ .$$

ii) Pour tout $x \in A$, $\pi(x) = 0$, *signifie exactement* $x \sim_{\mathfrak{I}} 0$, *c'est-à-dire* $x - 0 \in \mathfrak{I}$, *i.e.* $x \in \mathfrak{I}$.

Définition III.5.5 (Anneau quotient) L'*anneau*

$$A/\mathfrak{I} \text{ ou même le couple } \big(A/\mathfrak{i}, \pi : A \to A/\mathfrak{i}\big)$$

construit par la proposition III.5.3 est appelé *anneau quotient* . On dit encore que l'*ensemble* $A/\sim_{\mathfrak{I}}$ est muni de la *structure quotient* .

Remarque III.5.6 On remarque que, si on oublie la multiplication $*$ sur A, $(A, +)$ est un groupe abélien et $\mathfrak{I}$ un sous-groupe, nécessairement distingué. La *structure de groupe* qu'on obtient sur $A/\mathfrak{I}$ en oubliant aussi la multiplication, donne un groupe abélien qui est exactement le groupe quotient défini en définition II.8.11.2.

Exemple III.5.7 La situation considérée dans l'exemple II.8.11.3 peut être complétée. En effet pour tout $d \in \mathbb{Z}$, l'ensemble $d\mathbb{Z}$ des multiples de d est non seulement un sous-groupe de $(\mathbb{Z}, +)$ mais encore un idéal de $(\mathbb{Z}, +, *)$. Il s'ensuit, hormis pour $d = 1$, que $\mathbb{Z}/d\mathbb{Z}$ a une structure d'anneau telle que $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ soit un *morphisme d'anneaux* .

Proposition III.5.8 (Factorisation des *morphisme* s) *Soient* $(A, +, *)$ *un anneau comutatif et* $\mathfrak{I}$ *un idéal. On note* $\pi : A \to A/\mathfrak{I}$ *la surjection canonique* .

Pour tout morphisme d'anneaux $f : A \to B$ *les assertions suivantes sont équivalentes :*

a) $\mathfrak{I} \subset \operatorname{Ker} f$,

b) il existe un unique morphisme d'anneaux

$$\overline{f} : A/\mathfrak{I} \to B \text{ tel que } \overline{f} \circ \pi = f\ .$$

De plus, si $\mathfrak{I} = \operatorname{Ker} f$, $\overline{f}$ *est injectif et il est surjectif dès que* f *l'est.*

Démonstration *:*

b $\Rightarrow$ *a C'est un fait général et facile à vérifier que, dès qu'on a des morphisme s de groupes,* u, v, w $u = v \circ w \Rightarrow \operatorname{Ker} w \subset \operatorname{Ker} u$. *Or* $\operatorname{Ker} \pi = \mathfrak{I}$ *(cf. le point ii de la proposition III.5.4;) si bien que* $\overline{f} \circ \pi = f \Rightarrow \mathfrak{I} \subset \operatorname{Ker} f$.

a $\Rightarrow$ *b Unicité de* $\overline{f}$ *(analyse) Si* $\overline{f}$ *existe alors nécessairement pour tout* $\alpha \in A/\mathfrak{I}$, *il existe* $x \in A$ *tel que* $\alpha = \pi(x)$ *et* $\overline{f}(\alpha) = \overline{f}[\pi(x)] = f(x)$; *ce qui établit l'unicité de* $\overline{f}$.

Existence de $\overline{f}$ *(synthèse) Or si* $z \in A$ *est tel que* $\alpha = \pi(z)$ *on a encore* $\overline{f}(\alpha) = \overline{f}[\pi(z)] = f(z)$. *Or* $\pi(x) = \pi(z) \Rightarrow z - x \in \mathfrak{I} \subset \operatorname{Ker} f \Rightarrow f(z - x) = 0 \Rightarrow f(z) = f(x)$. *Il s'ensuit que* $\overline{f}$ *existe et est bien définie par la formulle :*

$$\overline{f}(\alpha) = f(x)\ \forall\, x, \alpha = \pi(x)\ .$$

$\overline{f}$ *est un morphisme de groupes* $\forall \alpha \in A/\mathfrak{I},\ \forall \beta \in A/\mathfrak{I},\ \big(\exists x \in A,\ \exists y \in A,\ (\alpha = \pi(x) \wedge \beta = \pi(y))\big)$. *On a alors :*

$$\begin{aligned}
\overline{f}(\alpha+\beta) &= \overline{f}[\pi(x)+\pi(y)] \\
&= \overline{f}[\pi(x+y)] \\
&= f(x+y) \\
&= f(x)+f(y) \\
&= \overline{f}[\pi(x)]+\overline{f}[\pi(y)] \\
&= \overline{f}(\alpha)+\overline{f}(\beta)\ .
\end{aligned}$$

$\overline{f}$ *est un morphisme d'anneaux*

$$\begin{array}{lll}
\forall \alpha \in A/\mathfrak{I},\ \forall \beta \in A/\mathfrak{I}, & & \\
\forall x \in A,\ \forall y \in A, & \big(\alpha = \pi(x) \text{ et } \beta = \pi(y) & \Rightarrow\ \overline{f}(\alpha * \beta) \\
& & =\ \overline{f}(\pi(x) * \pi(y)) \\
& & =\ \overline{f}(\pi(x * y)) \\
& & =\ f(x * y) \\
& & =\ f(x) * f(y) \\
& & =\ \overline{f}(\alpha) * \overline{f}(\beta)\big)
\end{array}$$

De plus $\overline{f}(1) = \overline{f}[\pi(1)] = f(1) = 1$.

$\overline{f}$ *est injective* $\forall \alpha \in A/\mathfrak{I},\ \exists x \in A,\ \alpha = \pi(x)\ .\ \overline{f}(\alpha) = 0 \Leftrightarrow \overline{f}[\pi(x)] = 0 \Leftrightarrow f(x) = 0 \Leftrightarrow x \in \operatorname{Ker} f = \mathfrak{I} \Leftrightarrow \alpha = 0$.

surjectivité Si f *est surjective,* $\forall y \in B,\ \exists x \in A,\ f(x) = y$. *Alors* $\overline{f}[\pi(x)] = y$.

Remarque III.5.9 Notons que dans la preuve de la proposition III.5.8, nous avons redonné des arguments que nous avions déjà donnés dans la preuve de la proposition II.8.11.4 et qu'on aurait pu simplement déduire les résultats concernant la *structure de groupe* de l'anneau $(A, +, *)$ de cette même proposition II.8.11.4.

Corollaire III.5.10 (de la proposition III.5.8) *Étant donné un morphisme d'anneaux* $f : A \to B$ *il existe un unique isomorphisme d'anneaux*

$$\overline{f} : A/\operatorname{Ker} f \cong \operatorname{Im} f \text{ tel que } f = \overline{f} \circ \pi$$

où $\pi : A \to A/\operatorname{Ker} f$ *est la surjection canonique . En particulier si* f *est surjectif*

$$\overline{f} : A/\operatorname{Ker} f \cong B$$

est un isomorphisme.

Démonstration : *Il suffit d'appliquer la proposition III.5.8 à* $\mathfrak{I} := \operatorname{Ker} f$.

Corollaire III.5.11 *Étant donné un morphisme surjectif d'anneaux* $p : A \to B$, *il existe un unique isomorphisme d'anneaux*

$$\phi : A/\operatorname{Ker} p \to B \text{ tel que } p = \phi \circ \pi \text{ où } \pi : A \to A/\operatorname{Ker} p \text{ est la surjection canonique .}$$

Démonstration : *C'est une conséquence immédiate du corollaire III.5.10 puisque* $\operatorname{Im} p = B$.

Remarque III.5.12 Les constructions du début de ce paragraphe et en particulier la proposition III.5.3 et la proposition III.5.8 peuvent être faites, sans presque d'ajout aux preuvent, dans le cadre de structures algébriques qui sont des groupes abéliens. Ainsi on obtiendrait facilement des résultats analogues dans le cas où A est un *espace vectoriel* et $\mathfrak{I}$ un *sous-espace vectoriel* . Pour peu qu'on connaisse la définition de ces objets, le cas où A est un module et $\mathfrak{I}$ un sous-module ne présenterait aucune difficulté supplémentaire.

La proposition III.5.13 ci-dessous étend au cas des anneaux les constructions donées dans les la proposition II.7.28 et la proposition II.8.11.8.

Proposition III.5.13 (Anneau produit) *Étant donnés un entier* $n \in \mathbb{N}^*$, $(A_k, +_k, *_k)_{,1 \leq k \leq n}$ *des anneaux*

$$\forall 1 \leq k \leq n,\ p_k \ :\ \prod_{i=1}^{n} A_i \ \to\ A_k \text{ les projections (cf. la définition I.1.13.17.)}$$

Alors :

i) Il existe un unique couple de lois de composition $(+, *)$ *sur* $\prod_{k=1}^{n} A_k$ *tel que pour tout* $1 \leq k \leq n$ p_k *soit un morphisme d'anneaux ; les loi* $+$ *et* $*$ *sont données par*

$$\begin{gathered}\forall\big((x_1,\dots,x_n),(y_1,\dots,x_n)\big) \in \prod_{k=1}^{n} A_k \times \prod_{k=1}^{n} A_K,\\ (x_1,\dots,x_n)\ +\ (y_1,\dots,y_n)\ =\ (x_1 +_1 y_1,\dots,x_n +_n y_n)\,,\\ (x_1,\dots,x_n)\ *\ (y_1,\dots,y_n)\ =\ (x_1 *_1 y_1,\dots,x_n *_n y_n)\,.\end{gathered}$$

ii) Les lois $+$ *et* $*$ *étant définies sur* P *comme ci-dessus, si*

a) pour tout $1 \leq k \leq n$ 0_k *est l'élément neutre de* $(A_k, +_k)$, $(0_1,\dots,0_n)$ *est l'élément neutre pour* $+$;

b) pour tout $1 \leq k \leq n$ 1_k *est l'élément neutre de* $(A_k, *_k)$, $(1_1,\dots,1_n)$ *est l'élément neutre pour* $*$;

c) $x \in \prod_{k=1}^{n} A_k$ *est tel que pour tout* $1 \leq k \leq n$ $y_k \in A_k$ *est l'opposé de* $p_k(x)$, *alors* $(y_1,\dots,y_n)$ *est l'opposé de* x *dans* $\big(\prod_{k=1}^{n} A_k, +\big)$;

d) $x \in \prod_{k=1}^{n} A_k$ *est tel que pour tout* $1 \leq k \leq n$ $y_k \in A_k$ *est l'inverse de* $p_k(x)$, *alors* $(y_1,\dots,y_n)$ *est l'inverse de* x *dans* $\big(\prod_{k=1}^{n} A_k, *\big)$;

iii) Si pour tout $1 \leq k \leq n$ $(A_k, +_k, *_k)$ *est un anneau commutatif,* $\big(\prod_{k=1}^{n} A_k, +, *\big)$ *est un anneau commutatif.*

iv) Pour tout n-uplet de morphismes d'anneaux $f_k : B \to A_k$,$1 \leq k \leq n$, il existe un unique morphisme d'anneaux

$$f : B \to \prod_{k=1}^{n} A_k \text{ tel que } \forall 1 \leq k \leq n,\ f_k = p_k \circ f .$$

Définition III.5.14 (Anneau produit) Avec les notations de la proposition III.5.13, les *loi* $+$ et $*$ définies sur $\prod_{k=1}^{n} A_k$ comme en III.5.13.i sont appelées *loi produits* et le triplet

$$(\prod_{k=1}^{n} G_k, +, *)$$

anneau produit .

Remarque III.5.15 On constatera que, contrairement aux points i à v de la proposition II.8.11.8, le point vi de la proposition II.8.11.8 ne peut se formuler de manière identique dans le cas des anneaux. En effet, en reprenant les notations du point vi de la proposition II.8.11.8, l'application

$$i_1 : A_1 \to A_1 \times A_2 , \text{ (resp. } i_2 : A_2 \to A_1 \times A_2 \text{)}$$

n'est pas un *morphisme d'anneaux* ; et son image n'est donc pas un *sous-anneau* de $A_1 \times A_2$ (cf. le point iii de la remarque III.1.1.10.) On pourrait néanmoins vérifier (et c'est un bon exercice) que $\operatorname{Im} i_1$ et $\operatorname{Im} i_2$ sont des idéaux de $A_1 \times A_2$ et qu'on a toujours

$$\operatorname{Ker} p_1 = \operatorname{Im} i_2 \text{ et } \operatorname{Ker} p_2 = \operatorname{Im} i_1 \text{ (cf. II.8.11.8.vi.c ,)}$$

ainsi que

$$p_1 \circ i_1 = \mathrm{Id}_{A_1} \text{ et } p_2 \circ i_2 = \mathrm{Id}_{A_2} \text{ (cf. le point b du point vi de la proposition II.8.11.8 .)}$$

III.6 . −Polynômes

Dans tout ce paragraphe (III.6), $(A, +_A, *_A, 0_A, 1_A)$ est un anneau (commutatif) (cf. la définition III.1.1.5,) qu'on supposera même assez vite intègre et l'on ne finira même par considérer, au paragraphe III.6.5 que le cas où A est un corps (cf. la définition III.1.1.12.)

III.6.1 . −L'anneau des séries formelles à coefficients dans A

On ne construit, dans ce paragraphe (III.6.1,) l'anneau $A[[X]]$ des séries formelles à coefficients dans A que pour servir de cadre à la construction de l'anneau $A[X]$ des polynômes à une indéterminée et à coefficients dans A construit au paragraphe III.6.2.

On n'aura malheureusement pas le loisir de sintéresser à l'anneau $A[[X]]$ pour lui-même ce qui pourtant est à la base de nombreux développements.

Définition III.6.1.1 On rappelle qu'une *suite à valeurs dans A* est une application $\mathbb{N} \to A$. On note le plus souvent $\alpha_n \in A$ et on appelle $n^{ième}$ *terme général* l'image d'un entier $n \in \mathbb{N}$ par la suite α.

Notation III.6.1.2 On rappelle que l'ensemble des suites à valeurs dans A est usuellement noté $A^{\mathbb{N}}$ (cf. I.1.13.13.) On notera $\left(\zeta_n\right)_{,n\,\in\,\mathbb{N}} \in A^{\mathbb{N}}$ (resp. $\left(\upsilon_n\right)_{,n\,\in\,\mathbb{N}} \in A^{\mathbb{N}}$) la suite définie par

$$\forall n \in \mathbb{N},\ \zeta_n\ :=\ 0 \text{ (resp. } \upsilon_0\ :=\ 1_A\ ,\ \forall n \in \mathbb{N},\ n \geq 1\ ,\ \upsilon_n\ :=\ 0\ .)$$

Pour tout $(\alpha, \beta)\ \in\ A^{\mathbb{N}} \times A^{\mathbb{N}}$, on définit l'élément $\alpha +_{A^{\mathbb{N}}} \beta\ \in\ A^{\mathbb{N}}$ par :

$$(\alpha +_{A^{\mathbb{N}}} \beta)_n\ :=\ \alpha_n\ +_A\ \beta_n \qquad \text{III.6.1.2.1}$$

et

$$(\alpha *_{A^{\mathbb{N}}} \beta)_n\ :=\ \sum_{k=0}^{n} \alpha_k\ *_A\ \beta_{n-k}\ =\ \sum_{(p,q)\,\in\,\mathbb{N}\times\mathbb{N}\ ,\ p+q\,=\,n} \alpha_p\ *_A \beta_q\ . \qquad \text{III.6.1.2.2}$$

Remarque III.6.1.3 On pourrait munir l'ensemble $A^{\mathbb{N}}$ d'une *structure d'anneau* (cf. la proposition III.1.1.13,) en multipliant les suites terme à terme ; mais la *structure d'anneau* alors obtenue n'est même pas *intègre* (cf. la définition III.1.1.6.) Nous définisssons le produit (cf. III.6.1.2.2,) d'une autre manière ; et l'on va montrer qu'alors l'anneau obtenu a de bien meilleures propriétés.

Définition III.6.1.4 (Produit de CAUCHY) Le produit défini en III.6.1.2.2 est usuellement appelé *produit de* CAUCHY .

Proposition III.6.1.5 (L'anneau des séries formelles) *Le triplet $(A^{\mathbb{N}},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$ est un anneau (commutatif si A l'est) d'élément neutre ζ pour la loi $+_{A^{\mathbb{N}}}$ et υ pour la loi $*_{A^{\mathbb{N}}}$.*

Démonstration *: Il s'agit, en premier lieu , de montrer que $(A,\ +_{A^{\mathbb{N}}})$ est un groupe abélien, ce qui résulte de la proposition II.8.1.7 Nous redonnons un argument ici :*

*i) (**Associativité**)*
Pour tout $(a, b, c) \in A^{\mathbb{N}} \times A^{\mathbb{N}} \times A^{\mathbb{N}}$,

$$((a+b)+c)_n\ =\ (a+b)_n + c_n\ =\ (a_n+b_n)+c_n\ =\ a_n+(b_n+c_n)\ =\ a_n+(b+c)_n\ =\ (a+(b+c))_n$$

en utilisant l'associativité de $+$ dans A. Ceci prouve que $+_{A^{\mathbb{N}}}$ est associative.

*ii) (**Élément neutre**)*
Notons $\zeta\ \in\ A^{\mathbb{N}}$ définie par $\zeta_n\ =\ 0\ \forall n \in \mathbb{N},$. Il est alors immédiat de vérifier que, pour tout $a\ \in\ A^{\mathbb{N}}$, $a + \zeta\ =\ \zeta + a\ =\ a$, si bien que ζ est l'élément neutre de $+_{A^{\mathbb{N}}}$.

*iii) (**Opposé**)*
Pour tout $a\ \in\ A^{\mathbb{N}}$, notons $b\ \in\ A^{\mathbb{N}}$ défini par

$$\forall n \in \mathbb{N},\ b_n\ :=\ -a_n$$

qui a un sens, puisque $(A, +)$ est un groupe. On a alors

$$a + b\ =\ b + a =\ \zeta$$

ce qui prouve que b est un opposé pour a.

iv) ***(Commutativité)***
Pour tout $(a,b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$,

$$(a+b)_n = a_n + b_n = b_n + a_n = (b+a)_n$$

grâce à la commutativité de $+_A$, *c'est-à-dire que* $a+b = b+a$ *autrement dit que* $+_{A^{\mathbb{N}}}$ *est commutative.*

Il découle de ce qui précède que $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}})$ *est un groupe abélien.*
On montre ensuite que $(A, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ *est un anneau commutatif*

v) ***(υ est un élément neutre (cf. III.1.1.1.Ann$_3$))***
Pour tout $a \in A^{\mathbb{N}}$, *et tout* $n \in \mathbb{N}$,

$$(a *_{A^{\mathbb{N}}} \upsilon)_n = \sum_{k=0}^{n} a_k * \upsilon_{n-k} = a_n * \upsilon_0 = a_n,$$

et

$$(\upsilon *_{A^{\mathbb{N}}} a)_n = \sum_{k=0}^{n} \upsilon_k * a_{n-k} = \upsilon_0 * a_n = a_n$$

d'où il découle que

$$\forall a \in A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} \upsilon = \upsilon *_{A^{\mathbb{N}}} a = a\,.$$

vi) ***(Commutativité)***

$$\begin{aligned}
\forall (a,b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ \forall n \in \mathbb{N}, \quad (a *_{A^{\mathbb{N}}} b)_n &= \sum_{k=0}^{n} a_k * b_{n-k} \\
&= \sum_{\ell=0}^{n} a_{n-\ell} * b_\ell \\
&= \sum_{\ell=0}^{n} b_\ell * a_{n-\ell} \\
&= (b *_{A^{\mathbb{N}}} a)_n
\end{aligned}$$

ce qui prouve le résultat grâce à la commutativité de $*$ *dans l'anneau* A.

vii) ***(Distributivité (cf. III.1.1.1.Ann$_4$))***

$$\begin{aligned}
\forall (a,b,c) \in A^{\mathbb{N}} \times A^{\mathbb{N}} \times A^{\mathbb{N}},\ \forall n \in \mathbb{N}, \quad \left(a *_{A^{\mathbb{N}}} (b +_{A^{\mathbb{N}}} c)\right)_n &= \sum_{k=0}^{n} a_k * (b +_{A^{\mathbb{N}}} c)_{n-k} \\
&= \sum_{k=0}^{n} a_k * (b_{n-k} + c_{n-k}) \\
&= \sum_{k=0}^{n} a_k * b_{n-k} + \sum_{k=0}^{n} a_k * c_{n-k} \\
&= (a *_{A^{\mathbb{N}}} b)_n + (a *_{A^{\mathbb{N}}} c)_n \\
&= \left(a *_{A^{\mathbb{N}}} b +_{A^{\mathbb{N}}} a *_{A^{\mathbb{N}}} c\right)_n .
\end{aligned}$$

.

Définition III.6.1.6 (Anneau des séries formelles) L'anneau $(A,\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$ est appelé *anneau des séries formelles à coefficients dans* A.

Notation III.6.1.7 Pour tout $a\ \in\ A$, on définit l'élément $i(a)$ de $A^{\mathbb{N}}$ par :

$$i(a)_0\ :=\ a \text{ et } \forall n \in \mathbb{N},\ n\ >\ 0\ \Rightarrow\ i(a)_n\ =\ 0\ . \qquad \text{III.6.1.7.1}$$

Pour tout $\alpha\ \in\ A^{\mathbb{N}}$, on définit $p(\alpha)\ \in\ A$ par :

$$p(\alpha)\ :=\ \alpha_0\ . \qquad \text{III.6.1.7.2}$$

Proposition III.6.1.8 (Morphisme structural) *i)* $p\ \circ\ i\ =\ \mathrm{Id}_A$.

ii) L'application i est injective et l'application p surjective.

***Démonstration** : Découle du point précédent.*

iii) Les applications i et p définies ci-dessus sont des morphisme s d'anneaux.

***Démonstration** :*

) (Morphisme de groupe**)*
Pour tout $(a,b)\ \in\ A\times A$,

$$i(a+b)_0\ =\ (a+b)\ =\ i(a)_0+i(b)_0\ =\ (i(a)+_{A^{\mathbb{N}}}i(b))_0$$

et

$$\forall n\in\mathbb{N},\ n>0\ ,\ i(a+b)_n\ =\ 0\,i(a)_n+i(b)_n\ =\ (i(a)+_{A^{\mathbb{N}}}i(b))_0$$

si bien que

$$i(a+b)\ =\ i(a)\ +_{A^{\mathbb{N}}}\ i(b)\,;$$

c'est-à-dire que

$$i\ :\ (A,+)\ \to\ (A^{\mathbb{N}},\ +_{A^{\mathbb{N}}}\ )$$

est un morphisme de groupes .

†) $(*_{A^{\mathbb{N}}}\ )$
Pour tout $(a,b)\ \in\ A\times A$,

$$i(a*b)_0\ =\ a*b\ =\ (i(a)*_{A^{\mathbb{N}}}i(b))_0\ .$$

Pour tout $n\ \in\ \mathbb{N}, n>0$,

$$\begin{aligned}(i(a)*_{A^{\mathbb{N}}}i(b))_n\ &=\ \sum_{k=0}^{n} i(a)_k*i(b)_{n-k}\\ &=\ i(a)_0*i(b)_n+\sum_{k=1}^{n} i(a)_k*i(b)_{n-k}\\ &=\ 0\end{aligned}$$

le premier terme étant nul puisque $n>0$ entraîne $i(b)_n\ =\ 0$, et le second étant nul puisque $k\geq 1$ entraîne $i(a)_k\ =\ 0$. On a donc

$$i(a*b)_n\ =\ 0\ =\ (i(a)*_{A^{\mathbb{N}}}i(b))_n\ .$$

Il s'ensuit que

$$i(a*b)\ =\ i(a)\ *_{A^{\mathbb{N}}}\ i(b)\ .$$

‡) $(1 \mapsto u)$
Par définition même de v et de i, il est immédiat de vérifier que $i(1)\ u$.
Les trois points précédents montrent que

$$i\ :\ (A,+,*)\ \to\ (A^{\mathbb{N}},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$$

est un morphisme d'anneau (cf. III.1.1.2.)

§) ***(Injectivité)***
Pour tout $a\ \in\ A, i(a)\ =\ z$, entraîne que $a\ =\ i(a)_0\ =\ 0$ ce qui assure l'injectivité de i.
La vérification du fait que p est aussi un morphisme est très simple et laissée en exercice.

Notation III.6.1.9 Pour tout $a\ \in\ A$ et tout $\alpha\ \in\ A^{\mathbb{N}}$, on note

$$a\ \cdot\ \alpha\ :=\ i(a)\ *_{A^{\mathbb{N}}}\ \alpha$$

qu'on finira par noter $a*\alpha$ en confondant A et l'image de i qui sont isomorphes et même $a\alpha$ si aucune confusion ne devait en résulter.

On remarque, en tout cas que :

$$\forall n \in \mathbb{N},\ (a\cdot\alpha)_n\ =\ \big(i(a)*_{A^{\mathbb{N}}}\alpha\big)_n\ =\ a*_A\alpha_n\ .$$

Proposition III.6.1.10 *On a alors :*

$$\forall a \in A,\ \forall b \in A,\ \forall\big(\alpha_n\big)_{,n\ \in\ \mathbb{N}} \in A^{\mathbb{N}},\ \forall\big(\beta_n\big)_{,n\ \in\ \mathbb{N}} \in A^{\mathbb{N}},\ :$$

Mod$_1$) $a\ \cdot\ (\alpha\ +_{A^{\mathbb{N}}}\ \beta)\ =\ a\ \cdot\ \alpha\ +_{A^{\mathbb{N}}}\ a\ \cdot\ \beta$;

Mod$_2$) $(a\ +_A\ b)\ \cdot\ \alpha\ =\ a\ \cdot\ \alpha\ +_{A^{\mathbb{N}}}\ b\ \cdot\ \beta$;

Mod$_3$) $(a\ *_A\ b)\ \cdot\ \alpha\ =\ a\ \cdot\ (b\ \cdot\ \alpha)$;

Mod$_4$) $1_A\ \cdot\ \alpha\ =\ \alpha$.

Démonstration : *C'est un exercice élémentaire.*

Remarque III.6.1.11 Si A était un corps les propriétés Mod_1 à Mod_4 de la proposition III.6.1.10 assureraient que $A^{\mathbb{N}}$ est un *A-espace vectoriel* (cf. la définition III.1.2.1.) Cependant dans le cas où A est simplement un anneau on parle de *A-module* . Cette structure ne pourra cependant pas être étudiée en détail dans le cadre de ce cours. On peut cependant se borner à remarquer qu'on a déjà rencontré des A-modules à savoir les idéaux de A. En outre, l'étude des A-modules pour lesquels on ne dispose pas d'une base, ce qui est le cas pour $A^{\mathbb{N}}$, peut se révélé assez dificile. La situation s'améliorera cependant un peu au paragraphe III.6.2.

Notation III.6.1.12 Pour tout $j\ \in\ \mathbb{N}$, on note $\varepsilon_j\ \in\ A^{\mathbb{N}}$ l'élément de $A^{\mathbb{N}}$ défini par :

$$(\varepsilon_j)_j\ :=\ 1 \text{ et } \forall n \in \mathbb{N},\ n\ \neq\ j\ \Rightarrow\ (\varepsilon_j)_n\ =\ 0\ .$$

Notons qu'on a immédiatement $\varepsilon_0\ =\ v$.

Lemme III.6.1.13 *Pour tout* $j \in \mathbb{N}$,

$$\varepsilon_{j+1} = \varepsilon_1 *_{A^{\mathbb{N}}} \varepsilon_j$$

et par conséquent

$$\forall (j,k) \in \mathbb{N} \times \mathbb{N},\ \varepsilon_j *_{A^{\mathbb{N}}} \varepsilon_k = \varepsilon_{j+k}\ .$$

Démonstration : *C'est un exercice.*

Notation III.6.1.14 Il est d'usage de noter $X := \varepsilon_1$; le lemme ci-dessus assurant que $X^j = \varepsilon_j$. L'anneau $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ est usuellement notté $A[[X]]$ et appelé *anneau des séries formelles à coefficients dans* A. Un élément $\left(\alpha_n\right)_{,n \in \mathbb{N}} \in A^{\mathbb{N}}$ est noté $\alpha = \sum_{n=0}^{+\infty} \alpha_n X^n$; cette notation ne devant cependant pas laisser croire qu'on ait pu écrire α comme combinaison linéaire et par conséquent trouver une base(cf. la définition III.1.2.8.)

La notation $A[[X]]$ ne recouvre pas seulement $A^{\mathbb{N}}$ en tant qu'ensemble mais bel et bien l'anneau $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}, \zeta, \upsilon)$ si bien que lorsqu'on écrit $A[[X]]$ il n'est nul besoin de spécifier quelle est la structure d'anneau. Les éléments

$$\zeta \text{ (resp. } \upsilon \text{)sont, bien entendu, notés } 0 \text{ (resp. } 1 \text{ .)}$$

Proposition III.6.1.15 *i) Pour tout* $\left(\alpha_n\right)_{,n \in \mathbb{N}} \in A^{\mathbb{N}}, \alpha \neq \zeta$, *il existe un entier naturel* $\mathrm{val}(\alpha)$ *tel que*

$$\alpha_{\mathrm{val}(\alpha)} \neq 0 \text{ et } \forall n \in \mathbb{N},\ n < \mathrm{val}(\alpha) \Rightarrow \alpha_n = 0\ .$$

Démonstration : *(cf. la question 2 de l'exercice III.11.3.1.)*

ii) $\forall (\alpha, \beta) \in (A^{\mathbb{N}} \setminus \{\zeta\}) \times (A^{\mathbb{N}} \setminus \{\zeta\}),\ \mathrm{val}(\alpha *_{A^{\mathbb{N}}} \beta) \geq \mathrm{val}(\alpha) + \mathrm{val}(\beta)$ *avec égalité dans le cas où* A *est un anneau intègre.*

Démonstration : *(cf. la question 3 de l'exercice III.11.3.1.)*

iii) $\forall (\alpha, \beta) \in (A^{\mathbb{N}} \setminus \{\zeta\}) \times (A^{\mathbb{N}} \setminus \{\zeta\}),\ \mathrm{val}(\alpha +_{A^{\mathbb{N}}} \beta) \geq \min\left(\mathrm{val}(\alpha)\ ,\ \mathrm{val}(\beta)\right)$ *avec égalité dans le cas où* $\mathrm{val}(\alpha) \neq \mathrm{val}(\beta)$.

Démonstration : *(cf. la question 5 de l'exercice III.11.3.1.)*

Définition III.6.1.16 (Valuation) Pour tout $\alpha \in A^{\mathbb{N}} \setminus \{\zeta\}$, on appellera *valuation* de α, l'entier $\mathrm{val}(\alpha)$.

Remarque III.6.1.17 a) On peut interpréter la valueation d'un élément α de $A^{\mathbb{N}} \setminus \{\zeta\}$, comme la plus grande puissance de X divisant α. et on aurait affaire ici à la « valuation X-adique » en quelque sorte.

b) On peut prolonger l'application valuation de $A^{\mathbb{N}} \setminus \{\zeta\}$ à $A^{\mathbb{N}}$ en posant :

$$\mathrm{val}(\zeta) \;=\; (+\infty)\,.$$

Si on note $\overline{\mathbb{N}} \;:=\; \mathbb{N} \cup \{(-\infty),(+\infty)\}$ $\mathrm{val}(\cdot)$ est une application de $A^{\mathbb{N}}$ à valeurs dans $\overline{\mathbb{N}}$.
On peut prolonger partiellement l'addition $+$ de $\mathbb{N}$ à $\overline{\mathbb{N}}$ en posant :

$$\begin{aligned}\forall n \in \mathbb{N},\, n+(+\infty) \;&=\; (+\infty)+n \;=\; (+\infty)\\ n+(-\infty) \;&=\; (-\infty)+n \;=\; (-\infty)\\ (+\infty)+(+\infty) \;&=\; (+\infty)\\ (-\infty)+(-\infty) \;&=\; (-\infty)\,.\end{aligned}$$

On peut aussi prolonger la relation d'ordre sur $\mathbb{N}$, en posant

$$\forall n \in \mathbb{N},\; (-\infty) \;<\; n \;<\; (+\infty)\,.$$

Avec ces définitions, les énoncés ii et iii de la proposition III.6.1.15 sont vérifiés pour tout $(\alpha,\beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$.

Proposition III.6.1.18 *Si A est un anneau commutatif intègre il en est de même de $A^{\mathbb{N}}$.*

Démonstration : *(cf. la question 4 de l'exercice III.11.3.1.)*

III.6.2 . −Anneau des polynômes à une indéterminée

On reprend les notations du paragraphe III.6.1.

Notation III.6.2.1 On notera $A^{\mathbb{N},0} \subset A^{\mathbb{N}}$ l'ensemble des éléments de $A^{\mathbb{N}}$ qui sont des « *suites presque nulles* » c'est-à-dire que $A^{\mathbb{N},0}$ est l'ensemble des éléments $\left(\alpha_n\right)_{,n\,\in\,\mathbb{N}} \in A^{\mathbb{N}}$ tel qu'il existe $p \in \mathbb{N}$, tel que

$$\forall n \in \mathbb{N},\; n \geq p \;\Rightarrow\; \alpha_n \;=\; 0\,.$$

Il est immédiat de constater que

$$\zeta \;\in\; A^{\mathbb{N},0}\,,\; \upsilon \;\in\; A^{\mathbb{N},0} \text{ et } \forall n \in \mathbb{N},\; \varepsilon_n \;\in\; A^{\mathbb{N},0}\,.$$

Proposition III.6.2.2 *i) Pour tout $\left(\alpha_n\right)_{,n\,\in\,\mathbb{N}} \in A^{\mathbb{N},0}$, $\alpha \neq \zeta$, il existe un unique entier naturel $\deg(\alpha)$ tel que*

$$\alpha_{\deg(\alpha)} \;\neq 0 \text{ et } \forall n \in \mathbb{N},\; n \;>\; \deg(\alpha) \;\Rightarrow\; \alpha_n \;=\; 0\,.$$

Démonstration : *(cf. la question 1 de l'exercice III.11.3.2.)*

ii) $\forall(\alpha,\beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0},\; \deg(\alpha *_{A^{\mathbb{N}}} \beta) \;\leq\; \deg(\alpha) \;+\; \deg(\beta)$ *avec égalité dans le cas où A est un anneau intègre.*

Démonstration : *(cf. la question 2 de l'exercice III.11.3.2.)*

iii) $\forall (\alpha, \beta) \in (A^{\mathbb{N},0} \setminus \{\zeta\}) \times (A^{\mathbb{N},0} \setminus \{\zeta\})$, $\deg(\alpha +_{A^{\mathbb{N}}} \beta) \leq \max\big(\deg(\alpha)\ ,\ \deg(\beta)\big)$ *avec égalité dans le cas où* $\deg(\alpha) \neq \deg(\beta)$.

Démonstration : *(cf. la question 3 de l'exercice III.11.3.2.)*

iv) ***(Divisibilité)***
Si A est un anneau intègre,

$$\forall \alpha \in A^{\mathbb{N},0}, \forall \beta \in A^{\mathbb{N},0}, \big(\alpha | \beta \text{ et } \beta \neq 0 \Rightarrow \deg(\alpha) \leq \deg(\beta)\ .\big)$$

Démonstration : *(cf. la question 6 de l'exercice III.11.3.2.)*

Définition III.6.2.3 (Degré) Pour tout $\alpha \in A^{\mathbb{N},0} \setminus \{\zeta\}$, l'entier $\deg(\alpha)$ sera appelé *degré* de α.

Remarque III.6.2.4 De même que pour la valuation, on peut prolonger le degré à $A^{\mathbb{N},0}$ en posant

$$\deg(\zeta) := (-\infty)$$

(cf. III.6.1.17.b.) Les assertions ii et iii de la proposition III.6.2.2 sont alors vérifiées pour tout $(\alpha, \beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0}$.

Proposition III.6.2.5 *i) Le triplet $(A^{\mathbb{N},0}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ est un anneau (commutatif si A l'est), (intègre si A l'est) qui est un sous-anneau (cf. la définition III.1.1.3,) de $A[[X]]$.*

Démonstration : *(cf. la question 4 de l'exercice III.11.3.2.)*

ii) Le morphisme $i : A \to A^{\mathbb{N}}$ étant celui défini en III.6.1.7.1, l'image de i est incluse dans $A^{\mathbb{N},0}$ et l'on a

$$\operatorname{Im} i = \{\alpha \in A^{\mathbb{N},0}\ ;\ \deg(\alpha) \leq 0\}\ .$$

Il s'ensuit que $i : A \to A^{\mathbb{N},0}$ est un morphisme injectif d'anneaux.

Démonstration : *(cf. la question 7 de l'exercice III.11.3.2.)*

iii) L'ensemble des éléments inversibles $A^{\mathbb{N},0\times}$ des de $A^{\mathbb{N},0}$ s'identifie (c'est-à-dire est isomorphe en tant que groupe abélien) à $A^{\times}$.

Démonstration : *(cf. la question 8 de l'exercice III.11.3.2.)*

iv) La loi externe $\cdot$ définie à la notation III.6.1.9 se restreint à $A^{\mathbb{N},0}$ et vérifie encore les axiomes Mod_1 à Mod_4 de la proposition III.6.1.10donnant encore à $A^{\mathbb{N},0}$ une structure de A-espace vectoriel (cf. la définition III.1.2.1 ;) pour peu toutefois, que A soit un corps (cf. la définition III.1.1.12.)

Démonstration : *Est une conséquence presque immédiate du point ii .*

v) La famille X^n ,$_{n\in\mathbb{N}}$ est une base (cf. la définition III.1.2.8,) de $A^{\mathbb{N},0}$ c'est-à-dire que :

*a) (**elle est génératrice**)*

pour tout $\alpha \in A^{\mathbb{N},0}$ il existe $d \in \mathbb{N}$ et un d-uplet $(a_i)_{1 \leq i \leq d} \in A$ tels que $\alpha = \sum_{j=0}^{d} a_j \cdot X^j$;

***Démonstration** : C'est presqu'uniquement un jeu d'écriture. On peut cependant donner un argument un peu plus formel par récurrence. On remarque en effet que si $\deg(\alpha) = 0$,*

$$\alpha = i(a) = i(a) *_{A^{\mathbb{N}}} \upsilon = a \cdot X^0 .$$

Pour $d \in \mathbb{N}$, si $\deg(\alpha) = d+1$, on écrit

$$\alpha = \alpha_d \cdot X^d + \beta$$

et l'on constate que $\deg(\beta) \leq d$. Si on fait donc l'hypothèse de récurrence qu'on peut écrire

$$\beta = \sum_{j=0}^{d} \beta_j \cdot X^j$$

on peut décomposer α de manière analogue ce qui prouve le résultat par récurrence sur le degré.

*b) (**elle est libre**)*
pour tout $n \in \mathbb{N}$, tout n-uplet $(a_i)_{1 \leq i \leq n} \in A$,

$$\sum_{j=0}^{n} a_j \cdot X^j = \zeta \Rightarrow \forall 1 \leq j \leq n,\ a_j = 0 .$$

***Démonstration** : Exercice.*

Notation III.6.2.6 Il est donc usuel de noter les éléments $\alpha \in A^{\mathbb{N},0}$:

$$\alpha = \sum_{j=0}^{\deg(\alpha)} \alpha_j X^j$$

et l'anneau $(A^{\mathbb{N},0}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})\ A[X]$.

De même que pour l'anneau des séries formelles (cf. III.6.1.14,) la notation $A[X]$ recouvre toute la structure d'anneau de $A^{\mathbb{N},0}$ si bien qu'il n'est n'ul besoin de spécifier que l'addition est donée par $+_{A^{\mathbb{N}}}$ et la multiplication par $*_{A^{\mathbb{N}}}$. L'*élément neutre* ζ sera bien entendu noté 0 et l'élément unité υ 1.

Définition III.6.2.7 L'anneau $A[X]$ est appelé *anneau des polynômes àune indéterminée à coefficients dans A*. Un élément de A est appelé *polynôme*.

Exemple III.6.2.8 Dans l'anneau $A := \mathbb{Z}/p^2\mathbb{Z}$, pour p un nombre premier, les éléments

$$\alpha := (1, p, 0, \ldots, 0, \ldots \text{ et } \beta := (1, -p, 0, \ldots, 0, \ldots$$

de $A^{\mathbb{N},0}$. On constate qu'alors

$$\alpha *_{A^{\mathbb{N}}} \beta = (1, 0, -p^2, 0, \ldots, 0, \ldots = (1, 0, \ldots, 0, \ldots = \upsilon$$

alors qu'on a $\deg(\alpha) = \deg(\beta) = 1$.

Proposition III.6.2.9 (Propriété universelle de l'anneau des polynômes) *Soient*

$$f \,:\, A \,\to\, B \text{ un morphisme d'anneaux } \text{ et } b \,\in\, B\,.$$

Il existe un unique morphisme d'anneaux

$$\phi_b \,:\, A[X] \,\to\, B \text{ tel que } \phi_b(X) \,=\, b \text{ et } f \,=\, \phi_b \,\circ\, i$$

(où $i \,:\, A \,\to\, A[X]$ est le morphisme défini en III.6.1.7.1.)

Ceci entraîne en particulier que :

$$\forall \alpha \in A[X], \alpha \,=\, \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \,\Rightarrow\, \phi_b(\alpha) \,=\, \sum_{k=0}^{\deg(\alpha)} f(\alpha_k) *_B b^k\,. \qquad \text{III.6.2.9.1}$$

Démonstration *:*

Unicité Un élément $b \,\in\, B$ étant fixé, s'il existe un morphisme $\phi_b \,:\, A[X] \,\to\, B$ tel que $\phi_b(X) \,=\, b$, nécessairement $\forall n \in \mathbb{N}^*,\ \phi_b(X^n) \,=\, b^n$. Puisque ϕ_b est un morphisme d'anneaux , $\phi_b(1_{A[X]} \,=\, 1_B$; ce qui entraîne $\phi_b(\upsilon) \,=\, 1_B$; qui entraîne encore $\phi_b(X^0) \,=\, 1_B$. Il en résulte finalement que :

$$\forall n \in \mathbb{N},\ \phi_b(X^n) \,=\, b^n\,. \qquad \text{III.6.2.9.1}$$

Par ailleurs si on note $\cdot$ la loi externe définie à la notation III.6.1.9, $\phi_b \circ i \,=\, f$ entraîne :

$$\begin{array}{lll} \forall \alpha \in A[X], \forall \beta \in A[X], & & \\ \forall a \in A,\ \forall b \in A, & \phi_b(a \cdot \alpha +_{A^{\mathbb{N}}} b \cdot \beta) & = \phi_b(i(a) *_{A^{\mathbb{N}}} \alpha +_{A^{\mathbb{N}}} i(b) *_{A^{\mathbb{N}}} \beta) \\ & & = \phi_b(i(a)) *_B \phi_b(\alpha) +_B \phi_b(i(b)) *_B \phi_b(\beta) \\ & & = f(a) *_B \phi_b(\alpha) +_B f(b) *_B \phi_b(\beta)\,. \end{array}$$

L'application ϕ_b est donc « A-linéaire » et l'image de la base $\{X^n\}_{n\in\mathbb{N}}$ étant déterminée d'après III.6.2.9.1, ϕ_b est nécessairement unique la proposition III.1.3.5.

Existence Il existe une unique application « A-linéaire » $\phi_b \,:\, A[X] \,\to\, B$ telle que $\forall n \in \mathbb{N},\ \phi_b(X^n) \,=\, b^n$. Puisque ϕ_b est linéaire, en particulier $\forall \alpha \in A[X], \forall \beta \in A[X], \phi_b(\alpha +_{A^{\mathbb{N}}} \beta) \,=\, \phi_b(\alpha) +_B \phi_b(\beta)$ si bien que l'axiome Ann_5 de la définition III.1.1.2 est satisfait.

Par ailleurs :

$$\begin{array}{lll} \forall \alpha \in A[X], \alpha \,=\, \displaystyle\sum_{k=0}^{\deg(\alpha)} \alpha_k X^k & & \\ \forall \beta \in A[X], \beta \,=\, \displaystyle\sum_{k=0}^{\deg(\beta)} \beta_k X^k \quad \phi_b(\alpha *_{A^{\mathbb{N}}} \beta) & = & \displaystyle\sum_{k=0}^{\deg(\alpha)+\deg(\beta)} \Big(\sum_{\ell+m\,=\,k} \alpha_\ell \beta_m \Big) \cdot X^k \\ & = & \displaystyle\sum_{k=0}^{\deg(\alpha)+\deg(\beta)} f\Big(\sum_{\ell+m\,=\,k} \alpha_\ell \beta_m \Big) *_B b^k \\ & = & \Big(\displaystyle\sum_{k=0}^{\deg(\alpha)} f(\alpha_k) *_B b^k \Big) *_B \Big(\sum_{k=0}^{\deg(\beta)} f(\beta_k) *_B b^k \Big) \\ & = & \phi_b(\alpha) *_B \phi_b(\beta)\,; \end{array}$$

ce qui prouve que ϕ_b vérifie l'axiome Ann_6 de la définition III.1.1.2.

Il est enfin clair que l'axiome Ann_7 de la définition III.1.1.2 est satisfait.

Notation III.6.2.10 Avec les hypothèses et notations de la proposition III.6.2.9 ci-dessus, on notera $A[b]$ l'image de $A[X]$ dans B par le morphisme ϕ_b.

Corollaire III.6.2.11 (Fonctorialité de l'anneau des polynômes) *En particulier, étant donné un morphisme d'anneaux $f : A \to B$, il existe un unique morphisme d'anneaux*

$$f[X] : A[X] \to B[X] \text{ caractérisé par : } f[X](X) = X \text{ et } f[X] \circ i_A = i_B \circ f$$

ce qui entraîne en particulier que :

$$\forall \alpha \in A[X], \alpha := \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow f[X](\alpha) = \sum_{k=0}^{\deg(\alpha)} f(\alpha_k) X^k . \qquad \text{III.6.2.11.1}$$

Démonstration : *Il suffit d'appliquer la proposition III.6.2.9 au morphisme d'anneaux $i_B \circ f : A \to B[X]$ et à l'élément $X \in B[X]$.*

Exemple III.6.2.12 Le corollaire III.6.2.11 justifie un certain nombre d'opérations :

a) Si $f : \mathbb{R} \to \mathbb{C}$ est l'inclusion naturelle du corps $\mathbb{R}$ des réels dans le corps $\mathbb{C}$ des complexes, le morphisme

$$f[X] : \mathbb{R}[X] \to \mathbb{C}[X]$$

consiste simplement à considérer les coefficients d'un polynôme à coefficients réels comme des nombres complexes.

b) En considérant l'inclusion $\mathbb{Z} \subset \mathbb{Q}$, on obtient également une inclusion $\mathbb{Z}[X] \subset \mathbb{Q}[X]$ et comme dans le point a elle consiste juste à considérer les coefficients entiers comme des nombres rationnels.

c) Soit $\sigma : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe. L'application σ est bien un *morphisme d'anneaux* de $\mathbb{C}$ dans lui-même si bien qu'on peut lui appliquer le corollaire III.6.2.11 pour en déduire un morphisme

$$\sigma[X] : \mathbb{C}[X] \to \mathbb{C}[X] \text{ qui vérifie,}$$

en vertu de III.6.2.11.1

$$\sigma[X]\big(\sum_{k=0}^{d} \alpha_k X^k\big) = \sum_{k=0}^{d} \sigma(\alpha_k) X^k$$

qu'on écrira de manière plus usuelle :

$$\overline{\sum_{k=0}^{d} \alpha_k X^k} = \sum_{k=0}^{d} \overline{\alpha_k} X^k .$$

d) Dans le cas où l'on considère la *surjection canonique* $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme $\pi_n[X]$ associe, à un polynôme $P := \sum_{i=0}^{d} a_k X^k$ à coefficients entiers, le polynôme $\overline{P} = \sum_{i=0}^{d} a_k \bmod n X^k$ dont les coefficients sont des entiers modulo n. En particulier si n est un nombre premier on obtient un polynôme à coefficients dans un corps et l'on peut appliquer tous les résultats relatifs aux anneaux principaux.

III.6.3 . −Évaluation et fonctions polynômes

Proposition III.6.3.1 (Évaluation) *Pour tout $a \in A$, il existe un unique morphisme d'anneaux*

$$\mathrm{ev}_a : A[X] \to A \mid \mathrm{ev}_a(X) = a \text{ et } \mathrm{ev}_a \circ i = \mathrm{Id}_A$$

et en particulier :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow \mathrm{ev}_a(\alpha) = \sum_{k=0}^{\deg(\alpha)} \alpha_k * a^k . \qquad \textit{III.6.3.1.1}$$

Démonstration : *Il suffit d'appliquer la proposition III.6.2.9 à l'identité de A et à l'élément a de A.*

Notation III.6.3.2 Étant donné un ensemble X, notons

$$\mathcal{F}(X, A) := \{f : X \to A\}$$

l'ensemble des fonctions $f : X \to A$ de X à valeurs dans A (cf. I.1.13.10.v.)

Lemme III.6.3.3 *i) Pour tout ensemble X, on peut munir l'ensemble A^X des applications de X dans A d'une structure d'anneau (commutatif) par :*

$$\forall f \in A^X, \forall g \in A^X, \forall x \in A, (f+g)(x) := f(a) +_A g(a) \text{ et } (f * g)(x) := f(x) *_A g(x) \qquad 1$$

lélément neutre pour $+$ (resp. $*$,) étant la fonction constante de valeurs 0_A (resp. 1_A.)

Démonstration : *Voir la proposition III.1.1.13*

ii) La loi externe $\cdot$ définie sur $A \times A^X$ par :

$$\forall a \in A, \forall f \in A^X, \forall x \in X, (a \cdot f)(x) := a \cdot f(x) \qquad 1$$

vérifie les axiomes Mod_1 à Mod_4 de la proposition III.6.1.10, autrement dit, dans le cas où A est un corps (cf. la définition III.1.1.12,) les axiomes $Vect_1$ à $Vect_4$ de la définition III.1.2.1.

iii) L'application :

$$j_A : A \to A^X , a \mapsto a \cdot 1_{A^X} \qquad 1$$

est un morphisme d'anneaux .

Proposition III.6.3.4 *Considérons l'ensemble A^A des applications de A dans lui-même muni de la structure $+, *$ définie à la notation III.6.3.2 et au lemme III.6.3.3.*

i) Il existe un unique morphisme d'anneaux :

$$\phi : A[X] \to A^A , X \mapsto \mathrm{Id}_A \mid \phi \circ i_A = j_A$$

et l'on a alors :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k , \phi(\alpha) = x \mapsto \sum_{k=0}^{\deg(\alpha)} \alpha_k x^k . \qquad 1$$

Démonstration : *Il suffit d'appliquer la proposition III.6.2.9 au morphisme j_A et à $\mathrm{Id}_A \in A^A$.*

ii) Si $\cdot$ désigne la loi externe définie à la notation III.6.1.9 (resp. la loi externe définie au point 1 du point ii du lemme III.6.3.3), selon le contexte :

$$\forall a \in A,\ \forall \alpha \in A[X],\ \phi(a \cdot \alpha) \ = \ a \cdot \phi(\alpha)\ . \qquad 1$$

Démonstration : *Vérification sans difficulté.*

iii) $\forall a \in A,\ \forall \alpha \in A[X],\ \mathrm{ev}_a(\alpha) \ = \ \phi(\alpha)(a) \ = \ \sum_{k=0}^{\deg(\alpha)} \alpha_k a^k$ *qu'on notera bien évidemment* $\alpha(a)$.

Démonstration : *Idem.*

Définition III.6.3.5 (Racine) Pour tout polynôme $\alpha \in A[X]$ on appelle *racine de α dans A* un élément $a \in A$ tel que : $\alpha(a) \ = \ 0_A$.

Définition III.6.3.6 (Fonctions polynômes) On appelle *ensemble des fonctions polynômes* l'image du morphisme ϕ défini au point i de la proposition III.6.3.4, dans A^A et *fonction polynôme* un élément de cette image.

Remarque III.6.3.7 On pourrait se demander pourquoi on a bien pris soin de distinguer les polynômes éléments de $A[X]$ des fonctions polynômes leurs image dans A^A. En effet :

a) Si A est le corps $\mathbb{R}$ le corps $\mathbb{C}$, et plus généralement un corps infini le morphisme ϕ défini au point i de la proposition III.6.3.4 est injectif c'est-à-dire que si deux polynômes définisssent la même fonction polynôme ils sont égaux (cf. III.6.6.4.)

b) <u>En revanche</u> si κ est un corps fini, typiquement le corps $\mathbb{F}_p \ := \ (\mathbb{Z}/p\mathbb{Z}, +, *)$ pour p un nombre premier, on peut considérer le polynôme $X^p - X \in \mathbb{F}_p[X]$. La fonction polynôme qu'il définit sur $\mathbb{F}_p$ est la fonction $x \mapsto x^p - x$ qui est la fonction nulle. Or $X^p - X$ n'est pas le polynôme nul à savoir l'élément $\zeta \in A[X]$ défini à la notation III.6.2.1.

III.6.4 . −Le théorème de la division euclidienne dans $\mathbb{K}[X]$

Dans ce paragraphe (III.6.4,) $\mathbb{K}$ est un corps (cf. la définition III.1.1.12,) et l'on s'intéresse à l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$.

Proposition III.6.4.1

$$\forall P \in \mathbb{K}[X],\ \forall Q \in \mathbb{K}[X],\ \big(P|Q \text{ et } Q \ \neq \ 0 \ \Rightarrow \ \deg(P) \leq \deg(Q)\big)\ .$$

Démonstration : *Résulte du point ii de la proposition III.6.2.2.*

Théorème III.6.4.2 (de la division euclidienne) *Pour tout couple (A, B) d'éléments de $\mathbb{K}[X]$, $B \neq 0$, il existe un unique couple (Q, R) d'éléments de $\mathbb{K}[X]$ tel que*

$$A = B * Q + R \text{ et } \deg(R) < \deg(B) .$$

***Démonstration** :*

i) Pour tout $a \in \mathcal{P}$, si $\deg(a) < \deg(b)$, il existe $(q, r) \in \mathcal{P} \times \mathcal{P}$ tel que

$$a = b *_{A^{\mathbb{N}}} q +_{A^{\mathbb{N}}} r \text{ et } \deg(r) < \deg(b) .$$

Il suffit de prendre

$$q := a \text{ et } r := \zeta .$$

ii) Pour tout $a \in \mathcal{P}$, si $\deg(a) \geq \deg(b)$, il existe $(s, c) \in \mathcal{P} \times \mathcal{P}$ tel que

$$a = b *_{A^{\mathbb{N}}} s +_{A^{\mathbb{N}}} c \text{ et } \deg(c) < \deg(a) .$$

Puisque $b \neq \zeta$, $b_{\deg(b)} \neq 0$. Puisque A est un corps $b_{\deg(b)}$ est donc inversible d'inverse $\beta \in A$. Définissons alors s par :

$$s_{\deg(a)-\deg(b)} := a_{\deg(a)} * \beta \text{ et } \forall n \in \mathbb{N},\ n \neq \deg(a) - \deg(b) ,\ s_n := 0 .$$

Il s'ensuit que $(b *_{A^{\mathbb{N}}} s)_{\deg(a)} = a_{\deg(a)}$ si bien que $\deg(a - b *_{A^{\mathbb{N}}} s) < \deg(a)$. Posons donc $c := a - b *_{A^{\mathbb{N}}} s$.

iii) Pour tout $a \in \mathcal{P}$ il existe un unique

$$(q, r) \in \mathcal{P} \times \mathcal{P} \text{ tel que } a = b *_{A^{\mathbb{N}}} q +_{A^{\mathbb{N}}} r \text{ et } \deg(r) < \deg(b) .$$

*) ***(Unicité)***
Supposons donnés deux couples (q_1, r_1) et (q_2, r_2) répondant à la question. On a alors

$$b * q_1 + r_1 = a = b * q_2 + r_2$$

ce qui entraîne $b * (q_1 - q_2) = r_2 - r_1$ et donc

$$b | r_2 - r_1 .$$

Or (cf. III.6.2.2.iii,) que

$$\deg(r_2 - f_1) \leq \max(\deg(r_1), \deg(r_2)) < \deg(b) .$$

Or (cf. III.6.2.2.iv,) si

$$b | r_2 - r_1 \text{ et } r_2 - r_1 \neq \zeta,\ \deg(b) \leq \deg(r_2 - r_1) .$$

Il en résulte que $r_1 = r_2$ et, puisque $\mathcal{P}$ est intègre (cf. III.6.1.18,) $q_1 = q_2$.

*†) (**existence**)*
Pour $\deg(a) < \deg(b)$, *le résultat a été établi (cf. i.)*
Si $\deg(a) \geq \deg(b)$, *il existe (cf. ii,)* (s, c) *tels que* $a = b * s + c$ *et* $\deg(c) < \deg(a)$. *Si on suppose donc, par récurrence, le résultat établi pour* c *il existe* (t, r) *avec*

$$c = b * t + r \text{ et } \deg(r) < \deg(b) .$$

Il s'ensuit que

$$a = b * s + c = b * s + bt + r = b * (s + t) + r$$

et il suffit finalement de poser $q := s + t$.

Remarque III.6.4.3 i) On peut faire ici la même observation que dans le cas des *entiers* à savoir qu'on a unicité du couple (quotient , rest) dans l'énoncé du théorème de la division euclidienne. Ce résultat d'unicité se déduit de la propriété $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ (cf. le point iii de la proposition III.6.2.2.)

ii) Les termes de *dividende*, *diviseur*, *quotient* et *reste* bien connus dans le cas des *entiers* sont bien entendu, utilisés dans le cas de l'anneau $\mathbb{K}[X]$ et l'on peut même, en vertu du point i , parler du reste et du quotient.

Théorème III.6.4.4 (Structure des idéaux de $\mathbb{K}[X]$**)** *Une partie* $\mathfrak{I} \subset \mathbb{K}[X]$ *est un idéal (cf. la définition III.4.1,) de* $\mathbb{K}[X]$ *si et seulement si :*

$$\exists P \in \mathbb{K}[X],\ \mathfrak{I} = P\mathbb{K}[X] = \{P * Q\ ;\ Q \in \mathbb{K}[X]\} \qquad \textit{III.6.4.4.1}$$

c'est-à-dire que l'anneau $\mathbb{K}[X]$ *est un anneau principal .*

***Démonstration** :*

i) Si $\mathfrak{I} = P\mathbb{K}[X]$:

$$\begin{array}{rrrl} & \forall P_1 \in \mathfrak{I}, & \exists Q_1 \in \mathbb{K}[X], & P_1 = P * Q_1 \\ & \forall P_2 \in \mathfrak{I}, & \exists Q_2 \in \mathbb{K}[X], & P_2 = P * Q_2 \\ \Rightarrow & \forall A_1 \in \mathbb{K}[X], & \forall A_2 \in \mathbb{K}[X], & \\ A_1 * P_1 + A_2 * P_2 & & = & A_1 * P * Q_1 + A_2 * P * Q_2 \\ & & = & P * (A_1 * Q_1 + A_2 * Q_2) \\ & & \in & \mathfrak{I} \end{array}$$

ce qui prouvve que $\mathfrak{I}$ *est un idéal.*

ii) Réciproquement si $\mathfrak{I}$ *est un idéal non nul, soit* $A := \{\deg(P)\ ;\ P \in \mathfrak{I} \setminus \{0\}\}$. *L'ensemble* A *est une partie non vide de* $\mathbb{N}$, *et possède donc un plus petit élément* d *(cf. I.3.11.1.9.) Soit* $P \in \mathfrak{I}$ *avec* $\deg(P) = d$. *Puisque* $\mathfrak{I}$ *est un idéal,* $\forall Q \in \mathbb{K}[X],\ PQ \in \mathfrak{I}$ *si bien que si on note* $\mathfrak{J} := P\mathbb{K}[X]$ *l'idéal* $\mathfrak{J}$ *est inclus dans* $\mathfrak{I}$.
Pour tout $S \in \mathfrak{I}$, *il existe un couple* $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ *tel que*

$$S = PQ + R \text{ et } \deg(R) < d .$$

Or

$$S \in \mathfrak{I} \wedge PQ \in \mathfrak{J} \subset \mathfrak{I} \Rightarrow R = S - PQ \in \mathfrak{I} \Rightarrow \deg(R) \geq d \text{ ou } R = 0$$

ce qui et entraîne $R = 0$ *et par conséquent* $S = PQ \in \mathfrak{J}$ *et finalement* $\mathfrak{I} = \mathfrak{J}$.

Remarque III.6.4.5 i) Dans la proposition précédente, et partant dans le théorème III.6.4.2 on ne peut pas omettre l'hypothèse que $\mathbb{K}$ est un corps. Prenons en effet $A := \mathbb{K}[X]$ alors $A[Y]$ est l'anneau $\mathbb{K}[X,Y]$ dans lequel l'idéal engendré par X et Y n'est pas de la forme III.6.4.4.1.

III.6.5 . −Propriétés arithmétiques de l'anneau $\mathbb{K}[X]$

Dans tout ce paragraphe (III.6.5,) $\mathbb{K}$ est un corps (cf. la définition III.1.1.12,) et l'anneau $\mathbb{K}[X]$ est l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ introduit au paragraphe III.6.2. Son *élément neutre* que nous avons jusqi'ci noté ζ (resp. son élément unité υ) sera dorénavant noté 0 (resp. 1.)

Remarque III.6.5.0 Il faut bien prendre garde que peu de résultats de ce paragraphe subsistent si l'on ne suppose pas que l'anneau des coefficients est un corps et en particulier celui qui est à l'origine des autres à savoir le théorème III.6.4.2 et son corollairele théorème III.6.4.4.

III.6.5.1. −PGCD et Ppcm dans $\mathbb{K}[X]$

Proposition III.6.5.1.1 *Pour tout entier $n \in \mathbb{N}^*$, et toute partie*

$$A := \{P_1, \ldots, P_n\} \subset \mathbb{K}[X]$$

finie à n éléments :

*i) (**PGCD**)*
A possède un PGCD (cf. la définition III.4.15.)

*ii) (**Identité de** BÉZOUT)*
Si D est un PGCD de A il existe un n-uplet $(U_1, \ldots, U_n) \in \mathbb{K}[X]^n$ tel que :

$$D = \sum_{i=1}^{n} U_i P_i \,. \qquad 1$$

Définition III.6.5.1.2 (Identité de BÉZOUT) La formule III.6.5.1.1.ii.1 est appelée *identité de* BÉZOUT et les *polynômes* $(U_i)_{1 \leq i \leq n}$ *coefficients de* BÉZOUT .

Remarque III.6.5.1.3 L'hypothèse que A est fini dans la proposition III.6.5.1.1 n'est pas indispensable et l'on peut tout à fait s'en passer .

Proposition III.6.5.1.4 *Toute famille de polynômes admet un **Ppcm**.*

III.6.5.2. −Théorème de BÉZOUT,

lemme de GAUSS,
lemme d'EUCLIDE
dans l'anneau $\mathbb{K}[X]$

Théorème III.6.5.2.1 (de BÉZOUT) *Pour tout entier naturel n et toute partie $A := \{P_1, \ldots, P_n\} \subset \mathbb{K}[X]$, les assertions suivantes sont équivalentes :*

a) $\mathcal{D}(A) = \mathbb{K}^\times$ c'est-à-dire que les éléments de A sont premiers entre eux dans leur ensemble (cf. la définition III.4.10.)

b) $\bigwedge A = 1$.

c) Il existe un n*-uplet de polynômes* $(U_i)_{1 \leq i \leq n}$ *tel que*

$$\sum_{i=1}^{n} P_i U_i = 1 .$$

Remarque III.6.5.2.2 Le théorème de BÉZOUT III.6.5.2.1 est le plus souvent appliqué pour deux éléments puisque dans un certain nombre d'applications la condition utilisée est qu'une famille d'éléments soit constituée d'éléments deux à deux premiers entre eux et non premiers entre eux dans leur ensemble. C'est notamment le cas pour la proposition III.6.5.6.1 chinois des restes. C'est de toute façon la situation à laquelle on peut avoir accès de manière calculatoire à travers l'*algorithme d'Euclide* (cf. III.6.5.4.1.)

Théorème III.6.5.2.3 (lemme de GAUSS) *Étant donnés trois polynômes* P, Q, R*, si* P *et* Q *sont premiers entre eux, et* $P|QR$ *alors* $P|R$.

Théorème III.6.5.2.4 (lemme d'EUCLIDE) *Dans l'anneau des polynômes* $\mathbb{K}[X]$ *tous les éléments irréductibles (cf. la définition III.4.7,) sont premiers (cf. la définition III.4.6.)*

Remarque III.6.5.2.5 (Éléments irréductibles) Le théorème III.6.5.2.4 assure que les deux notions de premier et d'irréductible sont équivalentes dans l'anneaux $\mathbb{K}[X]$ mais elle ne permet pas pour autant facilement de donner l'ensemble des polynômes irréductibles de $\mathbb{K}[X]$. Rappelons d'abord quelques résultats qui sont des conséquences directes du fait que le corps $\mathbb{K}$ est en particulier un anneau intègre :

i) (**Intégrité**)
L'anneau $\mathbb{K}[X]$ est intègre.

ii) (**Inversibles**)
L'ensemble $\mathbb{K}[X]^\times$ s'identifie à $\mathbb{K}^\times$ qui dans le cas d'un corps s'identifie à $\mathbb{K} \setminus \{0\}$ qu'on peut encore identifier à l'ensemble des polynômes de degré 0 et l'on a ainsi :

$$\forall P \in \mathbb{K}[X],\ P \in \mathbb{K}[X]^\times \Leftrightarrow \deg(P) = 0 . \qquad 1$$

Lemme III.6.5.2.6 *Pour tout* $P \in \mathbb{K}[X]\ \deg(P) = 1$ *entraîne* P *irréductible.*

Démonstration *: En effet si*

$$\deg(P) = 1 \text{ et } \exists Q \in \mathbb{K}[X],\ \exists R \in \mathbb{K}[X],\ P = Q * R$$

alors d'après le point ii de la proposition III.6.2.2 et proposition III.6.2.2,point iii,

$$0 \leq \deg(Q) \leq 1\ 0 \leq \deg(R) \leq 1 \text{ et } \deg(Q) + \deg(R) = 1 \Rightarrow \deg(Q) = 0 \text{ ou } \deg(R) = 0$$

ce qui, en vertu du point 1 du point ii de la remarque III.6.5.2.5 entraîne Q *ou* R *inversible et donc* P *irréductible.*

Remarque III.6.5.2.7 (Polynômes irréductibles) Nous venons de montrer au lemme III.6.5.2.6 que les polynômes de degré 1 à coefficients dans un corps sont irréductibles mais il n'existe pas d'argument aussi élémentaire pour dire qu'il n'en existe pas d'autres ou bien sous quelle(s) condition(s) il n'en existe pas d'autre. On peut certes dire que si $\mathbb{K}$ est *algébriquement clos* les seuls polynômes irréductibles sont les polynômes de degré 1 mais c'est pratiquement une définition et l'on n'a donc pas donné beaucoup plus d'information.

a) (**Le cas complexe**)
Le théorème de d'Alembert-GAUSS assure justement que dans $\mathbb{C}[X]$ les seuls polynômes irréductibles sont les polynômes de degré 1, c'està-dire que $\mathbb{C}$ est algébriquement clos. Cependant la démonstration de ce théorème fait intervenir des arguments d'analyse qu'on ne peut pas développer ici.

b) (**Le cas réel**)
On peut déduire de la situation sur $\mathbb{C}[X]$ que les polynômes irréductibles de $\mathbb{R}[X]$ sont au plus de degré 2 en utilisant la conjugaison complexe. Néanmoins il existe aussi des polynômes de degré 2 qui ne sont pas irréductibles.

c) (**Le cas rationnel/entier**)
La situation dans $\mathbb{Q}[X]$ est beaucoup plus compliquée, puisqu'on peut montrer qu'il existe des polynômes irréductibles de degré arbitrairement grand.

III.6.5.3. −Théorème fondamental de l'arithmétique

Théorème III.6.5.3.1 (fondamental de l'arithmétique) *Pour tout polynômes $P \in \mathbb{K}[X]$, $P \neq 0$, il existe une unique (à permutation près) famille de polynômes irréductibles unitaires $(P_i)_{1 \leq i \leq d}$ deux à deux premiers entre eux, une unique famille $(\alpha_i)_{1 \leq i \leq d}$ et un unique $\lambda \in \mathbb{K}$ tels que*

$$P \;=\; \lambda \prod_{i=1}^{d} P_i^{\alpha_i} \,.$$

III.6.5.4. −Algorithme d'EUCLIDE sur $\mathbb{K}[X]$

Proposition III.6.5.4.1 (Algorithme d'EUCLIDE) *Soient P_0 et P_1 des éléments de $\mathbb{K}[X]$ non tous deux nuls. On définit une suite P_n par récurrence pour tout $n \geq 2$:*
— si $P_{n-1} \;=\; 0$, $P_n \;:=\; 0$;
— sinon, P_n est le reste de la division euclidienne de P_{n-2} par P_{n-1}.
Alors :

i) Il existe un entier naturel m, tel que $P_m \neq 0$ et pour tout $n > m$, $P_m = 0$.

ii) Pour tout entier naturel n, il existe un couple (U_n, V_n) d'éléments de $\mathbb{K}[X]$ tel que

$$P_n \;=\; U_n * P_0 \;+\; V_n * P_1 \,.$$

En particulier, il existe un couple (U, V) d'éléments de $\mathbb{K}[X]$ tel que

$$P_m \;=\; U * P_0 \;+\; V * P_1 \qquad 1$$

iii) Si pour tout élément $P \in \mathbb{K}[X]$, on note $\mathcal{D}(P)$ l'ensemble de ses diviseurs, pour tout $n \in \mathbb{N}$ $P_{n+1} = 0$ ou

$$\mathcal{D}(P_n) \cap \mathcal{D}(P_{n+1}) \;=\; \mathcal{D}(P_{n+1}) \cap \mathcal{D}(P_{n+2})$$

en particulier

$$\mathcal{D}(P_m) \;=\; \mathcal{D}(P_0) \;\cap\; \mathcal{D}(P_1) \,. \qquad 1$$

Démonstration *: Pour $n \geq 2$, si $P_n \neq 0, \deg(P)_n < \deg(P)_{n-1}$ (cf. III.6.4.2.) On en déduit, par récurrence, que P_{n+1} est soit nul, soit $\deg(P)_{n+1} \leq \deg(P)_1 - n$. Le degré d'un polynôme étant un entier positif, nécessairement, soit $P_1 = 0$ et dans ce cas, $P_n = 0$ pour tout $n \geq 1$, soit pour $n > \deg(P)_1$, $P_{n+1} \;=\; 0$.*

On vient donc de montrer que l'ensemble des entiers n tels que $P_n \neq 0$, est une partie majorée de $\mathbb{N}$ et possède donc un plus grand élément m.

III.6.5.5. −Arithmétique modulaire sur $\mathbb{K}[X]$

Proposition III.6.5.5.1 *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible non nul (ou premier ce qui revient au même en vertu du lemme d'Euclide (cf. III.6.5.2.4,)) de degré $d > 0$. Alors :*

i) L'anneau $\mathbb{K}[X]/P\mathbb{K}[X]$ est un corps contenant $\mathbb{K}$.

ii) De plus l'inclusion $\mathbb{K} \subset \mathbb{K}[X]/P\mathbb{K}[X]$ donne à $\mathbb{K}[X]/P\mathbb{K}[X]$ une structure naturelle de $\mathbb{K}$-espace vectoriel qui est de dimension d.

Démonstration *:* Notons

$$\pi \,:\, \mathbb{K}[X] \,\to\, \mathbb{K}[X]/P\mathbb{K}[X]\,,\; P \,\mapsto\, \overline{P}$$

la *surjection canonique* dont on sait que c'est un *morphisme d'anneaux* .

i)

$$\forall \alpha \in \mathbb{K}[X]/P\mathbb{K}[X],\; \exists Q \,\in\, \mathbb{K}[X],\; \alpha \,=\, \pi(Q) \,\wedge\, \alpha \,\neq\, 0 \,\Rightarrow\, P \not| \, Q\,.$$

Comme P est irréductible, il existe $(U, V) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$PU + QV \,=\, 1 \,\Rightarrow\, \pi(PU + QV) \,=\, 1 \,\Rightarrow\, \alpha\pi(V) \,=\, 1$$

c'est-à-dire que tout $\alpha \in \mathbb{K}[X]/P\mathbb{K}[X]$ $\alpha \,\neq\, 0$ est inversible autrement dit que $\mathbb{K}[X]/P\mathbb{K}[X]$ est un corps.

Il est clair que l'injection naturelle $i \,:\, \mathbb{K} \,\to\, \mathbb{K}[X]$ qui à tout élément λ de $\mathbb{K}$ associe le polynôme constant λ est un *morphisme d'anneaux* . Il en va donc de même de $\pi \circ i$.

$$\forall \lambda \in \mathbb{K},\; \forall \mu \in \mathbb{K},\; \pi[i(\lambda)] \,=\, \pi[i(\mu)] \,\Leftrightarrow\, P | i(\lambda - \mu)\,.$$

Or $\deg(P) \,=\, d \,>\, 0$ et $\deg(i(\lambda - \mu)) \,\leq\, 0$, par conséquent, $i(\lambda - \mu) \,=\, 0 \,\Rightarrow\, \lambda - \mu \,=\, 0$ c'est-à-dire que $\pi \circ i$ est injective et qu'on peut donc considérer que $\mathbb{K}$ est un sous-corps de $\mathbb{K}[X]/P\mathbb{K}[X]$.

ii) On laisse le soin au lecteur de vérifier que

$$\cdot \,:\, \mathbb{K} \times \mathbb{K}[X]/P\mathbb{K}[X] \,\to\, \mathbb{K}[X]/P\mathbb{K}[X]\,,\; (\lambda, \alpha) \,\mapsto\, \lambda \cdot \alpha \,:=\, \pi[i(\lambda)]\alpha$$

donne à $\mathbb{K}[X]/P\mathbb{K}[X]$ une structure de $\mathbb{K}$-*espace vectoriel* .

$$\forall \alpha \in \mathbb{K}[X]/P\mathbb{K}[X],\; \exists Q \,\in\, \mathbb{K}[X],\; \alpha \,=\, \pi(Q)\,.$$

Or si R est le reste de la division euclidienne de Q par P, $\deg(R) \,<\, d$ et $\pi(R) \,=\, \alpha$. Il existe donc $(\lambda_j)_{0 \,\leq\, j \,\leq\, d-1} \,\in\, \mathbb{K}$ tels que

$$R \,=\, \sum_{j=0}^{d-1} \lambda_j X^j$$

(où l'on revient ici à une notation plus conventionnelle et où l'on note simplement $\lambda \,=\, i(\lambda)$.) Si bien que :

$$\alpha \,=\, \sum_{j=0}^{d-1} \pi(\lambda_j)\pi(X)^j\,. \qquad 1$$

Il s'ensuit que la famille $\pi(X)^j\,,_{0 \,\leq\, j \,\leq\, d-1}$ est une famille génératrice de $\mathbb{K}[X]/P\mathbb{K}[X]$.

Or si

$$\alpha \,=\, \sum_{j=0}^{d-1} \pi(\mu_j)\pi(X)^j,$$

en posant $S := \sum_{j=0}^{d-1} \mu_j X^j$, *on a* $\pi(R) = \alpha = \pi(S)$ *c'est-à-dire que* $P|R-S$. *Or* $\deg(R-S) \leq d-1 < d$ *si bien que* $R - S = 0$ *c'est-à-dire que la décomposition 1 est unique et que par conséquent la famille* $\pi(X)^j$,$0 \leq j \leq d-1$ *est une base du* $\mathbb{K}$*-espace vectoriel* $\mathbb{K}[X]/P\mathbb{K}[X]$.

III.6.5.6. −Théorème chinois des restes sur $\mathbb{K}[X]$

Proposition III.6.5.6.1 (Théorème chinois des restes) *Soient* $(P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$ *un couple de polynômes et* M *leur* ***Ppcm****. On note*

$$\pi_P : \mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X]\,,\ \pi_Q : \mathbb{K}[X] \to \mathbb{K}[X]/Q\mathbb{K}[X] \text{ et } \pi_M : \mathbb{K}[X] \to \mathbb{K}[X]/M\mathbb{K}[X]$$

les surjections canoniques , $\mathbb{K}[X]/P\mathbb{K}[X] \times \mathbb{K}[X]/Q\mathbb{K}[X]$ *l'anneau produit défini comme à la définition III.5.14, et*

$$\begin{array}{rccc} \pi: & \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]/P\mathbb{K}[X] \times \mathbb{K}[X]/Q\mathbb{K}[X] \\ & R & \longmapsto & \big(\pi_P(R), \pi_Q(R)\big)\,. \end{array}$$

i) Il existe un unique morphisme injectif d'anneaux γ *tel que le diagramme suivant soit commutatif (cf. le point 1 du point iii de la notation 0.1 :)*

$$\begin{array}{ccc} & \mathbb{K}[X] & \\ & {\scriptstyle \pi_M}\big\downarrow \quad \searrow {\scriptstyle \pi} & \\ \mathbb{K}[X]/M\mathbb{K}[X] & \xrightarrow{\ \gamma\ } & \mathbb{K}[X]/P\mathbb{K}[X] \times \mathbb{K}[X]/Q\mathbb{K}[X]\,. \end{array}$$

ii) Si P *et* Q *sont premiers entre eux,* γ *est surjectif et est donc un isomorphisme.*

Démonstration *: (cf. l'exercice III.11.3.3.)*

Remarque III.6.5.6.2 Bien entendu le résultat de la proposition III.6.5.6.1 ci-dessus peut s'étendre à une famille finie de polynômes deux à deux premiers entre eux .

III.6.6 . −Étude des racines d'un polynôme

Dans cette section (III.6.6,) $\mathbb{K}$ **est un corps si bien que tou les résultat du paragraphe III.6.4 peuvent être utilisés.**

Certain résultat du paragraphe III.6.6 peuvent être établis dans un cadre un peu moins strict que celui des corps, notamment celui des anneaux intègres, mais nécessiteraient des arguments techniques supplémentaires. On se limitera donc au cas des corps.

Proposition III.6.6.1 (Racine et factorisation d'un polynôme) *Pour tout polynôme* $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ *est une racine de* P *(cf. la définition III.6.3.5,) si et seulement si il existe* $Q \in \mathbb{K}[X]$ *tel que* $P = (X-a) *_{\mathbb{K}[X]} Q$.

Démonstration *:*

a est racine de P *Supposons que a est une racine de P. Considérons le morphisme $\mathrm{ev}_a : \mathbb{K}[X] \to \mathbb{K}$ défini par la proposition III.6.3.1.*

Un élément $a \in \mathbb{K}$ est racine de P si et seulement si $P \in \mathrm{Ker}\,\mathrm{ev}_a$. Or $\mathrm{Ker}\,\mathrm{ev}_a$ est un idéal de $\mathbb{K}[X]$ non égal à $\mathbb{K}[X]$. En effet, un corps contient au moins deux éléments distincts, il existe donc $b \in \mathbb{K}$ $b \neq a$, ce qui implique que $X - b \notin \mathrm{Ker}\,\mathrm{ev}_a$.

En vertu du théorème III.6.4.4, $\mathrm{Ker}\,\mathrm{ev}_a$ est engendré par un élément M. Comme $\mathrm{Ker}\,\mathrm{ev}_a \neq \mathbb{K}[X]$, $\deg(M) > 0$. Or $X - a \in \mathrm{Ker}\,\mathrm{ev}_a$, ce qui implique que M divise $X - a$ et que $\deg(M) \leq 1$ d'après la proposition III.6.4.1.

Il en résulte que $X - a$ est un générateur de $\mathrm{Ker}\,\mathrm{ev}_a$ donc qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a) *_{\mathbb{K}[X]} Q$.

$X - a | P$ *Réciproquement si $P = (X - a) *_{\mathbb{K}[X]} Q$ il est clair que $P(a) = 0$.*

Corollaire III.6.6.2 (Nombre de racines d'un polynôme) *Un polynôme $P \in \mathbb{K}[X]$ non nul possède au plus $\deg(P)$ racines.*

***Démonstration** :*

i) *($\deg(P) = 0$)*
Un polynôme constant non nul n'a pas de racines et le résultat est donc établi pour $\deg(P) = 0$.

ii) *($\deg(P) > 0$)*
Si P n'a pas de racines le résultat est établi. Si a est une racine de P, $X - a | P$ (cf. la proposition III.6.6.1 ;) c'est-à-dire qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a) * Q$. Il s'ensuit que

$$\deg(Q) = \deg(P) - 1 < \deg(P)\,.$$

Si l'on fait donc lh'ypothèse de récurrence que Q a au plus $\deg(Q)$ racines P qui a une racine de plus que Q en aura donc au plus $\deg(P)$ ce qui achève la preuve en raisonnant par récurrence sur le degré des polynômes.

Proposition III.6.6.3 (Multiplicité des racines) *Étant donné un polynôme $P \in \mathbb{K}[X]$, et $a \in \mathbb{K}$, l'ensemble des entiers naturels k tels que $(Xa)^k | P$ possède un plus grand élément qu'on appellera la multiplicité de la racine a. À noter que si a n'est pas effectivement racine de P, sa multiplicité vaut 0.*

***Démonstration** : L'ensemble $D := \{k \in \mathbb{N}\,;\, (X - a)^k | P\}$ est non vide puisque $1 = (X - a)^0 | P$ pour tout $a \in \mathbb{K}$.*

Par ailleurs, $\forall k \in \mathbb{N},\ (X - a)^k | P \Rightarrow k \leq \deg(P)$ (cf. la proposition III.6.4.1 ;) si bien que l'ensemble D est non-vide et majoré et possède donc un plus grand élément .

Corollaire III.6.6.4 (Polynôme nul) *Si $P \in \mathbb{K}[X]$ est un polynôme tel qu'il existe $n \in \mathbb{N}$ tel que $\deg(P) < n$ et P possèd n racines alors $P = 0$ est le polynôme nul.*

***Démonstration** : C'est une conséquence immédiate du corollaire III.6.6.2.*

Proposition III.6.6.5 (Groupe de racines de l'unité) *Pour tout entier $d \in \mathbb{N}^*$ l'ensemble $\Gamma_d \subset \mathbb{K}^\times$ des racines du polynôme $X^d - 1$ est un sous-groupe de $\mathbb{K}^\times$ et $card\Gamma_d \leq d$.*

Démonstration : *Le fait que $\#(\Gamma_d) \leq d$ est une conséquence immédiate du corollaire III.6.6.2.*
En suite il est clair que $1^d = 1$ i.e. $1 \in \Gamma_d$. De plus

$$\forall x \in \Gamma_d,\ x * x^{d-1} = 1 \wedge (x^{d-1})^d = (x^d)^{-1} = 1$$

si bien que x possède un inverse dans Γ_d. Enfin puisque $(\mathbb{K}^\times, *)$ est commutatif,

$$\forall x \in \Gamma_d,\ \forall y \in \Gamma_d,\ (x*y)^d = x^d * y^d = 1 \Rightarrow x * y \in \Gamma_d\,.$$

Proposition III.6.6.6 (Polynômes dérivé) *i) Il existe une unique application $\mathbb{K}$-linéaire*

$$\mathbb{K}[X] \to \mathbb{K}[X]\,,\ X^n \mapsto nX^{n-1}\,.$$

L'image d'un polynômes P par cette application sera notée P' et appelée polynôme dérivé.

Démonstration : *L'ensemble des X^n ,$_{n\in\mathbb{N}}$ étant une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]$ (cf. III.6.2.5.v,) et une application linéaire étant uniquement déterminée par l'image d'une base le résultat est clair.*

ii) La dérivation définie ci-dessus satisfait à la règle de Leibnitz à savoir

$$(PQ)' = P'Q + PQ'\,.$$

Démonstration : *C'est une vérification très élémentaire.*

Proposition III.6.6.7 (Polynômes à racines simples) *Si $\mathbb{K}$ est un corps de caractéristique 0, (en pratique $\mathbb{Q}$, $\mathbb{R}$ou $\mathbb{C}$,) pour tout polynôme $P \in \mathbb{K}[X]$ si P et P' sont premiers entre eux les racines de P sont simples.*

Démonstration : *Soit $a \in \mathbb{K}$ une racine de P. Alors il existe $k \in \mathbb{N}^*$, et $Q \in \mathbb{K}[X]$ tels que $P = (X-a)^kQ$. On a alors $P' = k(X-a)^{k-1}Q + (X-a)^kQ'$. Si P et P' sont premiers entre eux, il existe $(U,V) \in \mathbb{K}[X]\times\mathbb{K}[X]$ (cf. le théorème III.6.5.2.1,) tel que $PU + P'V = 1 \Rightarrow (X-a)^kQU + [k(X-a)^{k-1}Q + (X-a)^kQ']V = 1$. Or $k > 1$ entraîne que a est racine de $(X-a)^kQU + \big(k(X-a)^{k-1}Q + (X-a)^kQ'\big)V$ donc racine du polynôme constant 1 ce qui n'est pas. Par conséquent, $k = 1$ c'est-à-dire que a est racine simple.*

III.7 . −Réduction des endomorphismes

III.7.1 . −Polynômes annulateurs, minimaux ...

Dans ce paragraphe (III.7.1,) $\mathbb{K}$ est un *corps* (cf. la définition III.1.1.12,) E un $\mathbb{K}$-*espace vectoriel* (cf. la définition III.1.2.1,) de *dimension finie* (cf. le point c du point ix III.1.2,) et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un *endomorphisme* de E (cf. le point i de la définition III.1.3.6.)

C'est ici (III.7.1,) que nous utiliserons significativement les définitions et résultats du paragraphe III.6.

Définition III.7.1.1 (Polynômes annulateur) Un *polynôme annulateur* de u est un *polynôme* $P \in \mathbb{K}[X]$ tel que $P(u) = 0_{\mathrm{End}(E)}$ *i.e.*

$$\forall x \in E,\ P(u)(x) = 0_E\ .$$

Lemme III.7.1.2 (Annulateur) *Pour tout $x \in E$ et $P \in \mathbb{K}[X]$,*

i) ***(Polynôme minimal en x)***
Il existe un unique polynôme unitaire $P^x_{\min u}$ tel que

$$P^x_{\min u}(u)(x) = 0 \text{ et } \forall P \in \mathbb{K}[X],\ P(u)(x) = 0 \Rightarrow P^x_{\min u} | P\ ;$$

c'est-à-dire que

$$P^x_{\min u} \text{ est unitaire et } \left\{P \in \mathbb{K}[X]\ ;\ P(u)(x) = 0\right\} = P^x_{\min u}\mathbb{K}[X]\ .$$

ii) ***(Polynôme minimal)***
Il existe un unique polynôme unitaire $P_{\min u}$, tel que

$$P_{\min u}(u) = 0 \text{ et } \forall P \in \mathbb{K}[X],\ P(u) = 0 \Rightarrow P_{\min u} | P\ ;$$

c'est-à-dire que

$$\forall x \in E,\ P_{\min u}(u)(x) = 0 \text{ et } \forall P \in \mathbb{K}[X],\ \forall x \in E,\ P(u)(x) = 0 \Rightarrow P_{\min u} | P\ .$$

Définition III.7.1.3 (Polynôme minimal en x) Pour tout $x \in E$, le *polynôme* $P^x_{\min u}$ (cf. le point i du lemme III.7.1.2,) est appelé *polynôme minimal* de u en x.

Définition III.7.1.4 (Polynôme minimal) Le *polynôme* $P_{\min u}$ (cf. le point ii du lemme III.7.1.2,) est appelé *polynôme minimal* de u.

Proposition III.7.1.5 *Le polynôme minimal*

$$P_{\min u} \text{ de } u \text{ est le } \textbf{Ppcm} \text{ des polynômes minimaux } P^x_{\min u} \text{ en } x \in E\ .$$

Démonstration *: Pour tout $P \in \mathbb{K}[X]$:*
— *D'une part P est un polynôme annulateur de u si et seulement si $P_{\min u} | P$ (cf. la définition III.7.1.4.)*
— *D'autre part P est un polynôme annulateur de u si et seulement si*

$$\begin{array}{lll} \forall x \in E, & P \cdot x = P(u)(x) & = 0 \\ \Leftrightarrow & P^x_{\min u} & | \quad P\ ; \end{array}$$

c'est-à-dire si et seulement si le **Ppcm** *des $P^x_{\min u}$ divise P.*

Proposition III.7.1.6 *Soient F et G deux sous-espaces u-stables de E . Alors $F+G$, est u-stable et $P_{\min u_{|F+G}}$ et le* ***Ppcm*** *de $P_{\min u_{|F}}$ et $P_{\min u_{|G}}$.*

Démonstration *: Notons M le* ***Ppcm*** *de $P_{\min u_{|F}}$ et $P_{\min u_{|G}}$. Alors :*

$$\begin{array}{rrcl} & P_{\min u_{|F}} & | & M \\ \Rightarrow & \forall x \in F,\ M(u)(x) & = & 0 \\ & P_{\min u_{|G}} & | & M \\ \Rightarrow & \forall x \in G,\ M(u)(x) & = & 0\,; \end{array}$$

ce qui entraîne que

$$\forall (x,y) \in F \times G,\ M(u)(x+y) \ = \ M(u)(x) \ + \ M(u)(y) \ = \ 0\,;$$

ce qui entraîne que

$$P_{\min u_{|F+G}} | M\ .$$

Or $F \ \subset \ F+G$ (resp. $G \ \subset \ F+G$) si bien que

$$\forall x \in F,\ \ (\text{resp. } \forall x \in G,\ ,\ )\ P_{\min u_{|F+G}}(u)(x) \ = \ 0\,;$$

c'est-à-dire que

$$P_{\min u_{|F}} | P_{\min u_{|F+G}}\ (\text{resp. } P_{\min u_{|G}} | P_{\min u_{|F+G}}\ ;)$$

c'est-à-dire que

$$M | P_{\min u_{|F+G}}\ ,$$

d'où finalement

$$M \ = \ P_{\min u_{|F+G}}\ .$$

Lemme III.7.1.7 (Lemme des noyaux) *Soient $(P,Q) \ \in \ \mathbb{K}[X] \times \mathbb{K}[X]$ des polynômes premiers entre eux.*

i) $\operatorname{Ker}(PQ)(u) \ = \ \operatorname{Ker} P(u) \ \oplus \ \operatorname{Ker} Q(u)$

Démonstration *: Puisque P et Q sont premiers entre eux, il existe, d'après le théorème III.6.5.2.1 de* BÉZOUT *pour l'anneau principal (cf. le théorème III.6.4.4,) $\mathbb{K}[X]$,*

$$(A,B) \ \in \ \mathbb{K}[X] \times \mathbb{K}[X] \text{ tel que } AP + BQ \ = \ 1\ .$$

Il s'ensuit que :

$$\forall v \in E,\ (AP)(u)(v) \ + \ (BQ)(u)(v) \ = \ v, \qquad 1$$

puis que :

$$\begin{array}{lrcl} \forall v \in \operatorname{Ker}(PQ)(u), & (AP)(u) \circ (AP)(u)(v) & = & (AP)(u) \circ (AP+BQ)(u)(v) \\ & & = & (AP)(u)(v) \\ \big(\text{resp.} & (BQ)(u) \circ (BQ)(u)(v) & = & (BQ)(u) \circ (AP+BQ)(u)(v) \\ & & = & (BQ)(u)(v)\ .\big)\ . \end{array} \qquad 2$$

Soient :

$$\pi_P \ := \ (BQ)(u) \ : \ \operatorname{Ker}(PQ)(u) \ \to \ \operatorname{Ker} P(u) \text{ et } \pi_Q \ := \ (AP)(u) \ : \ \operatorname{Ker}(PQ)(u) \ \to \ \operatorname{Ker} Q(u). \qquad 3$$

Le calcul 2 ci-dessus montre que π_P et π_Q sont des projecteurs. Enfin l'égalité 1 assure que

$$\pi_P \ + \ \pi_Q \ = \ \mathrm{Id}_{\operatorname{Ker}(PQ)(u)}$$

ce qui achève la preuve.

ii) Les projections $\pi_P : \operatorname{Ker}(PQ)(u) \to \operatorname{Ker} P(u)$ *et* $\pi_Q : \operatorname{Ker}(PQ)(u) \to \operatorname{Ker} Q(u)$ *sont des polynômes en* u *i.e. des éléments de* $\mathbb{K}[u] = \operatorname{Im}\big(\mathbb{K}[X] \to \operatorname{End}_{\mathbb{K}}(E)\ ,\ X \mapsto u\big)$.

Démonstration *: (cf. i.3.)*

iii) De plus si $(PQ) = P_{\min u}$ *est le polynôme minimal de* u *sur* $\operatorname{Ker}(PQ)(u)$,

$$P = P_{\min u_{|\operatorname{Ker} P(u)}} \text{ et} Q = P_{\min u_{|\operatorname{Ker} Q(u)}} .$$

Démonstration *: Il est tout d'abord immédiat que* $P_{\min u_{|\operatorname{Ker} P(u)}} | P$ *(resp.* $P_{\min u_{|\operatorname{Ker} Q(u)}} | Q$ *;) ce qui entraîne* $(P_{\min u_{|\operatorname{Ker} P(u)}} \wedge P_{\min u_{|\operatorname{Ker} Q(u)}}) | (P \wedge Q) = 1$.

Or d'après le point i , $\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u)$ *; si bien que d'après la proposition III.7.1.6,* $(PQ) = P_{\min u_{|\operatorname{Ker}(PQ)(u)}} = (P_{\min u_{|\operatorname{Ker} P(u)}} \vee P_{\min u_{|\operatorname{Ker} Q(u)}})$ *; ce qui entraîne finalement*

$$P_{\min u_{|\operatorname{Ker} P(u)}} = P \text{ et } P_{\min u_{|\operatorname{Ker} Q(u)}} = Q .$$

III.7.2 . – Valeurs propres, vecteurs propres, espaces propres

Lemme III.7.2.1 (Valeur/vecteur propre) *Pour tout* $\lambda \in \mathbb{K}$ *les conditions suivantes sont équivalentes :*

a) L'endomorphisme $u - \lambda \mathrm{Id}_E$ *n'est pas injectif ;*

b) il existe $x \in E \setminus \{0\}$ *tel que* $u(x) = \lambda x$;

c) il existe $x \in E$ *tel que* $X - \lambda = P^x_{\min u}$ *soit le polynôme minimal de* u *en* x *(cf. la définition III.7.1.3 ;)*

d) $X - \lambda | P_{\min u}$.

Démonstration *:*

a $\Leftrightarrow$ *b Est tautologique.*

b $\Rightarrow$ *c Si* $x \neq 0$ *et* $u(x) = \lambda x$, $X - \lambda | P^x_{\min u}$. *Or* $\deg(P^x_{\min u}) = 0$, *entraîne qu'il existe* $\mu \in \mathbb{K}$ *tel que* $\mu x = 0$, *c'est-à-dire que* $x = 0$. *Il s'ensuit donc que* $P^x_{\min u} = X - \lambda$.

c $\Rightarrow$ *d (cf. la proposition III.7.1.5.)*

d $\Rightarrow$ *b Si* $X - \lambda | P_{\min u}$, *il existe*

$$k \in \mathbb{N}^*, \text{ et } Q \in \mathbb{K}[X] \text{ tels que } P_{\min u} = (X - \lambda)^k Q \text{ et } X - \lambda \text{ et } Q \text{ sont premiers entre eux} .$$

Il découle alors du lemme III.7.1.7 que $E = \operatorname{Ker} P_{\min u}(u) = \operatorname{Ker}(u - \lambda \mathrm{Id}_e)^k \oplus \operatorname{Ker} Q(u)$. *Or* $\operatorname{Ker}(u\lambda \mathrm{Id}_E)^k = \{0\}$ *entraîne* $E = \operatorname{Ker} Q(u)$, *ce qui entraîne* $P_{\min u} = Q$ *et contredit l'hypothèse. Ainsi il existe* $w \in \operatorname{Ker}(u - \lambda \mathrm{Id}_E)^k \setminus \{0\}$. *ainsi* $(u - \lambda \mathrm{Id}_E)^0(w) = w \neq 0$. *Il existe donc un plus grand entier* $\ell < k$, *tel que* $(u - \lambda \mathrm{Id}_E)^\ell \neq 0$ *et* $(u - \lambda \mathrm{Id}_E)^{\ell+1}(w) = 0$. *Posant*

$$x := (u - \lambda \mathrm{Id}_E)^\ell(w) , \quad \text{on a : } x \neq 0 \text{ et } u(x) = \lambda x .$$

Définition III.7.2.2 (Éléments propres) i) (**Valeur propre**)
On dit que $\lambda \in \mathbb{K}$, est une *valeur propre* pour u s'il vérifie les conditions équivalentes du lemme III.7.2.1.

ii) (**Vecteur propre**)
Un vecteur $x \in E$ vérifiant (de manière équivalente) les points b ou c du lemme III.7.2.1 est appelé *vecteur propre* associé à la valeur propre λ.

iii) (**Espace propre**)
Pour toute valeur propre λ de u, on appelle *espace propre* de u associé à λ le sous-espace $\mathrm{Ker}\, u - \lambda \mathrm{Id}_E$ de E qui est l'ensemble des vecteurs propres de u associés à λ (union $\{0\}$.)

Définition III.7.2.3 (Endomorphisme diagonalisable) On dit que u est *diagonalisable* si E est somme directe des espaces propres de u.

Proposition III.7.2.4 (Caractérisation des enromorphismes diagonalisables) *L'endomorphisme u est diagonalisable si et seulement si*

$$P_{\min u} \text{ est scindé à racines simples},$$

si et seulement si il existe un polynôme annulateur de u scindé à racines simples .

Démonstration : *C'est un résultat que le lecteur aura sans doute déjà démontré et il est invité à rappeler ses souvenirs.*

Exemple III.7.2.5 (Exemples fondamentaux) Soit E un $\mathbb{K}$-*espace vectoriel* .

a) (**Projecteur**)
Un *projecteur i.e.* un *endomorphisme* $p \in \mathrm{End}(E)$ tel que $p \circ p = p$ est *diagonalisable* (cf. l'exercice III.11.4.1.)

b) (**Symétrie**)
Une *symétrie i.e.* un *endomorphisme* $s \in \mathrm{End}(E)$ tel que $s \circ s = \mathrm{Id}_E$, est *diagonalisable* (cf. l'exercice III.11.4.2.)

Définition III.7.2.6 (Endomorphismes trigonalisables) On dit que u est trigonalisable s'il existe une base dans laquelle la matrice de u est triangulaire supérieure.

Proposition III.7.2.7 *L'endomorphisme u est trigonalisable si et seulement si $P_{\min u}$ est scindé.*

III.7.3 . −Polynôme caractéristique

Définition III.7.3.1 (Polynôme caractéristique) Pour tout endomorphisme $u \in \mathrm{End}_{\mathbb{K}}(E)$, le *polynôme caractéristique* de u est le polynômes $P_{\mathrm{car}\, u} := \det(X\mathrm{Id}_E - u) \in \mathbb{K}[X]$.

Lemme III.7.3.2 *Un élément $\lambda \in \mathbb{K}$ est une valeur propre de u (cf. le point i de la définition III.7.2.2,) si et seulement si $P_{\mathrm{car}\, u}(\lambda) = 0$ i.e. λ est une racine de $P_{\mathrm{car}\, u}$.*

Démonstration : *Il suffit de remarquer qu'un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie est injectif si et seulement si son déterminant est non nul et d'utiliser la caractérisation du point a du lemme III.7.2.1 des valeurs propres.*

Lemme III.7.3.3 (Propriétés du polynôme caractéristique) *i)* $\deg(P_{\mathrm{car}\, u}) = \dim_{\mathbb{K}} E$.

ii) Si on écrit $P_{car\,u} = \det(X\mathrm{Id}_E - u) = X^d + \sum_{i=0}^{d-1} a_i X^i$, $d = \dim_{\mathbb{K}} E$, *on a* $a_{d-1} = -\mathrm{tr}(u)$ et $a_0 = (-1)^d \det(u)$.

iii) Si $E = F \oplus G$ *avec* F *et* G *stables par* u, $P_{car\,u} = P_{car\,u_{|F}} \cdot P_{car\,u_{|G}}$.

Démonstration : *(cf. l'exercice III.11.4.3.)*

Définition III.7.3.4 (Spectre d'un endomorphisme) Soient $d \in \mathbb{N}$, $\mathbb{K}$ un *corps* , E un $\mathbb{K}$-*espace vectoriel* de *dimension finie* et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un *endomorphisme* de E.

i) (**Multiplicité**)
Pour toute *valeur propre* λ de u, la *multiplicité* de λ est sa *multiplicité* en tant que racine du *polynôme caractéristique* au sens de la proposition III.6.6.3.

ii) (**Spectre**)
Le *spectre* de u, noté $\mathrm{Sp}(u)$ est l'*ensemble* des *valeurs propres* de u.

On tient souvent compte de la *multiplicité* m_λ d'une *valeur propre* λ, et il est usuel de noter $\mathrm{Sp}(u) = \{\lambda^{(m_\lambda)}\}$; sans pour autant s'intterdire d'écrire $\lambda \in \mathrm{Sp}(u)$; les deux notations n'étant pas formellement rigoureusement compatibles.

III.8 . −Espaces préhilbertiens réels ou complexs

Dans ce paragraphe (III.8,) $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ **est le *corps* (cf. la définition III.1.1.12,) des *nombres réels* ou des *nombres complexes* .**

Le but de ce paragraphe étant, dans le contexte de ce cours, d'éclairer la proposition III.2.2, on aurait pu se contenter d'exposer les résultats qui suivent uniquement dans le cadre des *espaces euclidiens* (cf. la définition III.9.1,) ou des *espaces hermitiens* (cf. la définition III.9.2 ;) sans faire le détour par les *espaces pré-hilbertiens* (cf. la définition III.8.4.) Le seule mérite de la présentation que nous adoptons est sans doute de clairement distinguer quels énoncés n'ont pas besoin de l'hypothèse de *dimension finie* (cf. le point c du point ix III.1.2.)

Définition III.8.1 (Produit scalaire euclidien) Étant donné un $\mathbb{R}$-*espace vectoriel* E (cf. la définition III.1.2.1,) un *produit scalaire euclidien* sur E est :

Eucl_1) Une *forme bilinéaire* *i.e.* une *application* $\phi : E \times E \to \mathbb{R}$ telle que

$$\forall (x,y,z,a,b) \in E \times E \times E \times \mathbb{R} \times \mathbb{R}, \quad \begin{array}{rcl} \phi(ax+by,z) & = & a\phi(x,z) + b\phi(y,z) \\ \text{et} \quad \phi(x,ay+bz) & = & a\phi(x,y) + b\phi(x,z) \, . \end{array}$$

Eucl_2) La *forme bilinéaire* ϕ est *symétrique* *i.e.*

$$\forall (x,y) \in E \times E, \ \phi(x,y) = \phi(y,x) \, .$$

Eucl_3) La *forme bilinéaire* ϕ est *positive* *i.e.*

$$\forall x \in E, \ \phi(x,x) \geq 0 \, .$$

Eucl$_4$) La *forme bilinéaire* ϕ est *définie positive* *forme définie positive* *i.e.*

$$\forall x \in E,\ \phi(x,x) = 0 \Leftrightarrow x = 0\,.$$

Définition III.8.2 (Produit scalaire hermitien) Étant donné un $\mathbb{C}$-*espace vectoriel* E (cf. la définition III.1.2.1,) un *produit scalaire hermitien* sur E est :

Herm$_1$) Une *forme sesqui-linéaire* *i.e.* une *application* $\phi : E \times E \to \mathbb{C}$ telle que

$$\begin{array}{rcccccc} \forall (x,y,z,a,b) \in E\times E\times E\times\mathbb{C}\times\mathbb{C}, & \phi(ax+by,z) & = & \overline{a}\phi(x,z) & + & \overline{b}\phi(y,z) \\ \text{et} & \phi(x,ay+bz) & = & a\phi(x,y) & + & b\phi(x,z)\,. \end{array}$$

Herm$_2$) La *forme sesqui-linéaire* ϕ est à *symétrie hermitienne* *i.e.*

$$\forall (x,y) \in E\times E,\ \phi(x,y) = \overline{\phi(y,x)}\,.$$

Herm$_3$) La *forme sesqui-linéaire* ϕ est *positive* *i.e.*

$$\forall x \in E,\ \phi(x,x,) \geq 0\,.$$

Herm$_4$) La *forme sesqui-linéaire* ϕ est *définie positive* *i.e.*

$$\forall x \in E,\ \phi(x,x) = 0 \Leftrightarrow x = 0\,.$$

Remarque III.8.3 On pourrait s'étonner de l'axiome Herm$_3$ de la définition III.8.2, puisqu'a priori un *produit scalaire hermitien* est à *valeurs* dans $\mathbb{C}$. Cependant l'l'axiome Herm$_2$ de la définition III.8.2 entraîne que

$$\forall x \in E,\ \phi(x,x) = \overline{\phi(x,x)}\,;$$

ce qui entraîne

$$\forall x \in E,\ \phi(x,x) \in \mathbb{R}$$

et assure que $\phi(x,x) \geq 0$ a bien un sens.

Définition III.8.4 (espace préhilbertien) i) (**Réel**)

Un *espace pré-hilbertien réel* est un *couple* (E,ϕ) où E est un $\mathbb{R}$-*espace vectoriel* (cf. la définition III.1.2.1,) et ϕ un *produit scalaire euclidien* sur E au sens de la définition III.8.1.

ii) (**Complexe**)

Un *espace pré-hilbertien complexe* est un *couple* (E,ϕ) où E est un $\mathbb{C}$-*espace vectoriel* (cf. la définition III.1.2.1,) et ϕ un *produit scalaire hermitien* sur E au sens de la définition III.8.2.

Définition III.8.5 (Orthogonalité) Soit (E,ϕ) un *espace pré-hilbertien réel* (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou *complexe* (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.)

i) (**Éléments orthogonaux**)

On dit que deux *éléments* x et y de E sont ϕ-*ortogonaux* (ou même simplement *ortogonaux* s'il n'y a pas d'ambigûité) et l'on note $x \perp^{\phi} y$ ou ou simplement $x \perp y$ si $\phi(x,y) = 0$.

Ceci équivaut bien évidemment à $\phi(y,x) = 0$; si bien que

$$x \perp^{\phi} y \Leftrightarrow y \perp^{\phi} x\,.$$

cf

ii) (**Base orthogonale**)
Une *base* $(e_1, \ldots, e_d)$ de E est ϕ- (ou même simplement *ortogonale*) si $\phi(e_i, e_j) = 0$, pour tout $1 \leq i \leq d$, tout $1 \leq j \leq d$, $i \neq j$.

Plus généralement on pourrait dire d'une *partie* $S \subset E$, qu'elle est *ortogonale* si

$$\forall (x, y) \in S \times S,\ x \neq y \Rightarrow \phi(x, y) = 0 .$$

iii) (**Base orthonormale**)
On appelle *base* ϕ- (ou même *base orthonormale*) de E une *base* $(e_1, \ldots, e_d)$ telle que :

$$\begin{array}{ll} \forall 1 \leq i \leq d,\ \forall 1 \leq j \leq d, & \\ i \neq j \Rightarrow & \phi(e_i, e_j) = 0 \\ \text{et} & \phi(e_i, e_i) = 1 . \end{array}$$

On écrit parfois à l'aide du *symbole de* KRONECKER $\forall 1 \leq i \leq d,\ \forall 1 \leq j \leq d,\ \phi(e_i, e_j) = \delta_{i,j}$.

On pourrrait également généraliser la définition à une *partie* quelconque $S \subset E$ dont on dira qu'elle est *orthonormale* si :

$$\begin{array}{rcl} \forall (s, t) \in S \times S, \quad s \neq t & \Rightarrow & \phi(s, t) = 0 \\ \phi(s, s) & = & 1 . \end{array}$$

iv) (**Orthogonal d'une partie**)
pour toute partie $S \subset E$, on appelle *ϕ-orthogonal* de S (ou simplement *orthogonal* de S) et l'on note

$$S^{\perp,\phi} := \{x \in E\ ;\ \phi(s, x) = 0\ ,\ \forall s \in S,\ \} = \{x \in E\ ;\ s \perp^{\chi} x \forall s \in S,\ \}. \qquad 1$$

On notera $S^{\perp}$ pour $S^{\perp,\phi}$ si aucune confusion ne peut en résulter.
De même pour tout $x \in E$, on notera abusivement $x^{\perp}$ pour $\{x\}^{\perp}$.

v) (**Sous-espaces orthogonaux**)
Deux *sous-espaces vectoriels* F et G de E sont *ϕ-ortogonaux* (ou simplement *ortogonaux* ,) si

$$\forall (x, y) \in F \times G,\ q(x, y) = 0 .$$

On écrira (ou $F \perp^{\phi} G$ ou même simplement $F \perp G$.
À noter que F et $F^{\perp}$ sont *ortogonaux* et même que

$$F \perp G \Leftrightarrow G \subset F^{\perp} \Leftrightarrow F \subset G^{\perp} .$$

Proposition III.8.6 (Propriétés de l'orthogonalité) *Soit (E, ϕ) un espace pré-hilbertien réel (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou complexe (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.)*

i) Pour tout $S \subset E$, $S \subset \left(S^{\perp,\phi}\right)^{\perp,\phi}$.

ii) Pour tous $S \subset T \subset E$, $T^{\perp,\phi} \subset S^{\perp,\phi}$.

iii) Pour tout $S \subset E$, $S^{\perp,\phi}$ est un sous-espace vectoriel de E et

$$S^{\perp,\phi} = \mathrm{Vect}\{S\}^{\perp,\phi} .$$

iv) Pour tous $S \subset E$ *et* $T \subset E$, $(S \cup T)^{\perp,\phi} = S^{\perp,\phi} \cap T^{\perp,\phi}$; *en particulier si* F *et* G *sont deux sous-espaces vectoriels de* E,

$$(F+G)^{\perp,\phi} = F^{\perp,\phi} \cap G^{\perp,\phi} .$$

v) (***Parties orthogonales***)

Une partie ortogonale $S \subset E$ *(cf. le point ii de la définition III.8.5,) est une partie libre si* $0 \notin S$; *par conséquent une partie orthonormale (cf. le point iii de la définition III.8.5,) orthonormale est une partie libre .*

Démonstration *: (cf. l'exercice III.11.2.3.)*

Définition III.8.7 (Somme directe orthogonale) Pour $(F_i)_{1 \leq i \leq k}$ une famille de sous-espaces de E, on dira que la *somme* $F := F_1 + \ldots + F_k$ est une *somme directe ortogonale* $F = F_1 \oplus \ldots \oplus F_k$ est une *somme directe* et si de plus

$$\forall 1 \leq i < j \leq k,\ F_i \perp^{\chi} F_j . \qquad \text{III.8.7.1}$$

On notera alors

$$E = F_1 \oplus^{\perp_\chi} \ldots \oplus^{\perp_\chi} F_k \text{ ou simplement } E = F_1 \oplus^{\perp} \ldots \oplus^{\perp} F_k .$$

Si la condition III.8.7.1 est satisfaite, la somme est nécessairement directe (cf. l'exercice III.11.2.4.)

Définition III.8.8 (Projecteurs et symétries) Soit (E, ϕ) un *espace pré-hilbertien réel* (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou *complexe* (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.)

i) (**Projecteur orthogonal**)

Un *projecteur* ϕ*-orthogonal* (ou simplement *projecteur orthogonal*) de E dans lui-même est un *endomorphisme* p, qui est un *projecteur i.e.*

$$p \circ p = p \text{ et tel que de plus } \operatorname{Ker} p \perp^{\chi} \operatorname{Im} p ;$$

si bien qu'alors

$$E = \operatorname{Ker} p \oplus^{\perp_\chi} \operatorname{Im} p \text{ (cf. l'exercice III.11.2.1 .)}$$

ii) (**Symétrie orthogonale**)

Une *symétrie* ϕ- (ou simplement *symétrie ortogonale*) de E dans lui-même est un *endomorphisme* s qui est une *symétrie i.e.*

$$s \circ s = \mathrm{Id}_E \text{ et tel que de plus } \operatorname{Ker} s - \mathrm{Id}_E \perp^{\chi} \operatorname{Ker} s + \mathrm{Id}_E ;$$

si bien que

$$E = \operatorname{Ker} s - \mathrm{Id}_E \oplus^{\perp_\phi} \operatorname{Ker} s + \mathrm{Id}_E \text{ (cf. l'exercice III.11.2.2 .)}$$

Proposition III.8.9 *Soit (E,ϕ) un espace pré-hilbertien réel (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou complexe (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.) pour tout $x \in E$, $x \neq 0$, $E = \mathrm{Vect}\{x\} \oplus^{\perp} \chi\, x^{\perp,\chi}$.*

Démonstration *: On remarque tout d'abord que l'application*

$$p \,:\, E \,\to\, E \,,\; y \,\mapsto\, \frac{\phi(x,y)}{\phi(x,x)}x$$

est bien définie puisque $\phi(x,x) \neq 0$. De plus p est manifestement linéaire. Enfin pour tout $y \in E$,

$$\begin{aligned} p[p(y)] &= p\left(\frac{\phi(x,y)}{\phi(x,x)}x\right) \\ &= \frac{1}{\phi(x,x)}\phi\left(\frac{\phi(x,y)}{\phi(x,x)}x, x\right)x \\ &= \frac{1}{\phi(x,x)^2}\phi[\phi(x,y)x,x]x \\ &= \frac{\phi(x,y)}{\phi(x,x)}x \\ &= p(y)\,. \end{aligned}$$

Il en résulte que $p \circ p = p$ c'est-à-dire que p est un projecteur et donc que

$$E \,=\, \mathrm{Im}\, p \,\oplus\, \mathrm{Ker}\, p \text{ (cf. l'exercice III.11.4.1 .)}$$

$$\begin{array}{lrcl} \forall y \in E, & y & \in & \mathrm{Ker}\, p \\ \Leftrightarrow & p(y) & = & 0 \\ \Leftrightarrow & \dfrac{\phi(x,y)}{\phi(x,x)} & = & 0 \\ \Leftrightarrow & \phi(x,y) & = & 0 \\ \Leftrightarrow & y & \in & x^{\perp}\,; \end{array}$$

si bien que

$$\mathrm{Ker}\, p \,=\, x^{\perp}\,.$$

Il est clair que $\mathrm{Im}\, p \,\subset\, \mathrm{Vect}\{x\}$ et pour tout $a \in \mathbb{K}$,

$$p(ax) \,=\, \frac{\phi(x,ax)}{\phi(x,x)}x \,=\, ax\,;$$

si bien que

$$\mathrm{Im}\, p \,=\, \mathrm{Vect}\{x\}\,.$$

On a donc établi que

$$E \,=\, \mathrm{Vect}\{x\} \,\oplus\, x^{\perp,\phi}\,.$$

Il est presque tautologique de dire que cette somme est ϕ- .

Proposition III.8.10 (Généralisation) *Soit (E, ϕ) un espace pré-hilbertien réel (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou complexe (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.) Soit $F \subset E$ un sous-espace vectoriel de dimension finie alors F et $F^{\perp,\chi}$ sont supplémentaires i.e.*

$$E = F \oplus^{\perp} \chi F^{\perp,\phi} .$$

Démonstration *: Pour $\dim_{\mathbb{K}} F = 1$, le résultat est bien entendu donné par la proposition III.8.9.*

Soit $d \in \mathbb{N}^*$ et F de dimension $d+1$. Pour $x \neq 0 \in F$. Notons $D := \mathrm{Vect}\{x\}$ et $H := x^{\perp}$. Il résulte de la proposition III.8.9 que $E = D \oplus^{\perp} H$.

Notons $G := H \cap F$. Alors pour tout $x \in F$, puisque $x \in E$, il existe $(y, z) \in D \times H$ tel que $x = y + z$. Comme $z = x - y$, $z \in F$ donc $z \in F \cap H$ i.e. $z \in G$; si bien que $F = D + G$. Comme

$$D \cap G \subset D \cap H = \{0\} , F = D \oplus G .$$

Ainsi $\dim_{\mathbb{K}} G = \dim_{\mathbb{K}} F - 1 = d$. Notons $I := G^{\perp}$ et faisons l'hypothèse de récurrence que $E = G \oplus^{\perp} I$. Alors posons

$$J := F^{\perp} = (D \oplus G)^{\perp} = D^{\perp} \cap G^{\perp} = H \cap I \text{ (cf. le point iv de la proposition III.8.6.)}$$

Pour tout $x \in E$, il existe d'une part $(y, z) \in D \times H$ et d'autre part $(v, w) \in G \times I$ tels que

$$x = y + z = v + w .$$

Notons $u := z - v = w - y$. Or

$$z \in H \text{ et } v \in G \subset H \Rightarrow u \in H$$

et

$$w \in I \text{ et } y \in D \subset I \Rightarrow u \in I .$$

Il s'ensuit que

$$u \in J = H \cap I \text{ et } x = y + v + u .$$

Comme $y + v \in F$, on en déduit que

$$E = F + J .$$

On a nécessairement $F \cap J = \{0\}$, si bien que

$$E = F \oplus^{\perp} J = F \oplus^{\perp} F^{\perp} .$$

Proposition III.8.11 (Existence d'un projecteur orthogonal) *Soit (E, ϕ) un espace pré-hilbertien réel (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou complexe (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.) Soit $F \subset E$ un sous-espace vectoriel de dimension finie . Alors :*

i) Il existe un unique projecteur (cf. le point i de la définition III.1.3.7,)

$$p : E \to E \text{ tel que } \mathrm{Im}\, p = F \text{ et } \mathrm{Ker}\, p = F^{\perp} .$$

Démonstration *: Puisque F est de dimension finie la proposition III.8.10 assure que $E = F \oplus^{\perp_\phi} F^{\perp}$. L'existence et l'unicité de d'un projecteur p tel que $\mathrm{Ker}\, p = F^{\perp}$ et $\mathrm{Im}\, p = F$ découlent alors du lemme III.1.3.8.*

ii) Le projecteur p est un projecteur orthogonal (cf. le point i de la définition III.8.8.)

Démonstration : *(cf. l'exercice III.11.2.1.)*

iii) De plus, pour toute base orthonormale $(f_j)_{1 \leq j \leq \dim_{\mathbb{K}} F}$ de F,

$$\forall x \in E,\ p(x) \ = \ \sum_{j=1}^{\dim_{\mathbb{K}} F} \phi(f_j, x) f_j \ .$$

Démonstration : *Étant donnée une base orthonormale $(f_j)_{1 \leq j \leq d}$ de F, considérons l'application $q : E \to F$, $x \mapsto \sum_{j=1}^{d} q$*

L'application q est manifestement linéaire . De plus

$$\begin{aligned} \forall x \in E, \quad q\big(q(x)\big) &= q\big(\sum_{j=1}^{d} \phi(f_j, x) f_j\big) \\ &= \sum_{j=1}^{d} \phi(f_j, x) q(f_j) \\ &= \sum_{j=1}^{d} \phi(f_j, x) \big(\sum_{k=1}^{d} \phi(f_k, f_j) f_k\big) \\ &= \sum_{j=1}^{d} \phi(f_j, x) f_j \\ &= q(x) \ . \end{aligned}$$

L'endomorphisme q est donc un projecteur dont on constate immédiatement ou presque que $\operatorname{Im} q = F$ et $\operatorname{Ker} q = F^{\perp}$. C'est le seul vérifiant ces conditions en vertu du lemme III.1.3.8.

Le lemme III.8.12 qui suit est un ingrédient dans la démonstration du théorème III.8.13 ; mais présente un intérêt pour lui-même dans la mesure où il donne un critère pour qu'une *partie* soit *libre* (cf. le point c du point iii du lemme III.8.12.)

Lemme III.8.12 (avant GRAM–SCHMIDT) *Soit (E, ϕ) un espace pré-hilbertien réel (et dans ce cas on note $\mathbb{K} = \mathbb{R}$,) ou complexe (et dans ce cas on note $\mathbb{K} = \mathbb{C}$,) (cf. la définition III.8.4.) Soient $d \in \mathbb{N}^*$ un entier naturel et $(v_i)_{1 \leq i \leq d} \in E$ une d'famille d'éléments de E.*

i) Il existe une famille ortogonale $(o_i)_{1 \leq i \leq d} \in E$ telle que

$$\forall 1 \leq k \leq e,\ \operatorname{Vect}\big\{v_1, \ldots, v_k\big\} \ = \ \operatorname{Vect}\big\{o_1, \ldots, o_k\big\} \ .$$

Démonstration : *Raisonnons par récurrence sur l'entier $1 \leq k \leq d$.*
$k = 1$ $o_1 := v_1$ répond à la question.

$k \leq d$ *Supposons construite une famille ortogonale* $(o_i)_{1 \leq i \leq k} \in E$ *telle que*

$$\forall 1 \leq j \leq k,\ V_j := \mathrm{Vect}\{v_1, \ldots, v_j\} = \mathrm{Vect}\{o_1, \ldots, o_j\}\ .$$

Le sous-espace vectoriel V_k *étant de dimension finie il existe d'après la proposition III.8.11 un unique projecteur orthogonal* p_k *tel que*

$$\mathrm{Ker}\, p_k = V_k^{\perp} \text{ et } \mathrm{Im}\, p_k = V_k\ .$$

Si $k = d$, *le résultat est établi. Sinon posons* $o_{k+1} := v_{k+1} - p_k(v_{k+1})$. *Dès lors* $o_{k+1} \in v_k^{\perp}$; *si bien que* $(o_i)_{1 \leq i \leq k+1} \in E$ *est une famille ortogonale .*

Par définitionn de o_{k+1}, $o_{k+1} \in \mathrm{Vect}\{v_{k+1}, V_k\}$; *si bien que, sous l'hypothèse de récurrence*

$$\mathrm{Vect}\{o_1, \ldots, o_{k+1}\} \subset \mathrm{Vect}\{v_1, \ldots, v_{k+1}\}\ .$$

Enfin $v_{k+1} = o_{k+1} + p_k(v_{k+1})$; *si bien que* $v_{k+1} \in \mathrm{Vect}\{o_{k+1}, V_k\}$; *c'est-à-dire, par hypothèse de récurrence,* $v_{k+1} \in \mathrm{Vect}\{o_1, \ldots, o_{k+1}\}$. *Il s'ensuit que*

$$\mathrm{Vect}\{v_1, \ldots, v_{k+1}\} \subset \mathrm{Vect}\{o_1, \ldots, o_{k+1}\}\ .$$

Il en résulte finalement que

$$\mathrm{Vect}\{o_1, \ldots, _{k+1}\} = \mathrm{Vect}\{v_1, \ldots, v_{k+1}\}\ ;$$

ce qui achève le raisonnment par récurrence.

ii) Si $(o_i)_{1 \leq i \leq d} \in E$ *est construite comme au point i , pour tout* $1 \leq k \leq d$, $(v_i)_{1 \leq i \leq k} \in E$ *est une famille libre si et seulement si* $(o_i)_{1 \leq i \leq k} \in E$ *est une famille libre .*

Démonstration *: En effet,* $(v_i)_{1 \leq i \leq k}$ *est une famille libre si et seulement si*

$$\dim\big(\mathrm{Vect}\{v_1, \ldots, v_k\}\big) = k\ .$$

Ceci équivaut, en vertu du point i à

$$\dim\big(\mathrm{Vect}\{o_1, \ldots, _k\}\big) = k\ ;$$

ce qui équivaut au fait que $(o_i)_{1 \leq i \leq k}$ *est une famille libre .*

iii) Si $(o_i)_{1 \leq i \leq d} \in E$ *est construite comme au point i , pour tout* $0 \leq k \leq d-1$, *les assertions suivante sont équivalentes*

a) Les famille $(v_i)_{1 \leq i \leq k}$ *et* $(v_i)_{1 \leq i \leq k+1}$ *sont libres .*

b) Les famille $(o_i)_{1 \leq i \leq k}$ *et* $(o_i)_{1 \leq i \leq k+1}$ *sont libres .*

c) La famille $(o_i)_{1 \leq i \leq k}$ *est libre et* $o_{k+1} \neq 0$.

Démonstration :

a $\Leftrightarrow$ *b se déduit du point ii .*

b $\Leftrightarrow$ *c découle du point v de la proposition III.8.6.*

iv) Soient $(p_i)_{1 \leq i \leq d} \in E$ *et* $(q_i)_{1 \leq i \leq d} \in E$ *deux familles orthogonales telles que*

$$\forall 1 \leq k \leq d,\ \mathrm{Vect}\{p_1, \ldots, p_k\} = \mathrm{Vect}\{v_1, \ldots, v_k\} = \mathrm{Vect}\{q_1, \ldots, q_k\} .$$

Alors pour tout $1 \leq k \leq d$, $\{p_k, q_k\}$ *est une partie liée.*

Démonstration : *Pour tout* $1 \leq k \leq d$, *notons* $V_k := \mathrm{Vect}\{v_1, \ldots, v_k\}$ *et* $V_0 := \{0\}$. *Pour tout* $1 \leq k \leq d$,

$$p_k \in V_k\ ,\ p_k \in V_{k-1}^{\perp}\ ,\ q_k \in V_k\ ,\ q_k \in V_{k-1}^{\perp} .$$

Or $V_k \cap V_{k-1}^{\perp}$ *est supplémentaire de* V_{k-1} *dans* V_k *donc de dimension inférieure ou égale à* 1 ; *il en résulte que* p_k *et* q_k *sont liés.*

Théorème III.8.13 (Orthonormalisation de GRAM–SCHMIDT) *Soit* (E, ϕ) *un espace pré-hilbertien réel (et dans ce cas on note* $\mathbb{K} = \mathbb{R}$,*) ou complexe (et dans ce cas on note* $\mathbb{K} = \mathbb{C}$,*) (cf. la définition III.8.4.) Pour toute famille libre* $(e_i)_{1 \leq i \leq d} \in E$, *il existe une famille orthonormale* $(f_i)_{1 \leq i \leq d} \in E$ *telle que*

GS$_1$*) pour tout* $1 \leq j \leq d\ \mathrm{Vect}\{f_1, \ldots, f_j\} = \mathrm{Vect}\{e_1, \ldots, e_j\}$;

si de plus

GS$_2$*) pour tout* $1 \leq j \leq d\ \phi(e_j, f_j) \in \mathbb{R}^+$,

la famille $(f_i)_{1 \leq i \leq d}$ *est unique.*

Démonstration : *On notera* $\mathbb{K} = \mathbb{R}$ *(resp.* $\mathbb{K} = \mathbb{C}$,*) si* E *est un espace pré-hilbertien réel (resp. un espace pré-hilbertien complexe .)*

Existence D'après le point i du lemme III.8.12, il existe une famille orthogonale $(o_i)_{1 \leq i \leq d} \in E$, *satisfaisant la condition GS*$_1$. *Puisque* $(e_i)_{1 \leq i \leq d}$ *est une famille libre , il en est de même, d'après le point ii du lemme III.8.12, de la famille* $(o_i)_{1 \leq i \leq d}$. *Il s'ensuit, d'après le point v de la proposition III.8.6, que* $\forall 1 \leq i \leq d,\ o_i \neq 0$; *ce qui entraîne encore, en vertu de l'axiome Eucl*$_4$ *de la définition III.8.1, ou de l'axiome Herm*$_4$ *de la définition III.8.2,*

$$\forall 1 \leq i \leq d,\ \phi(o_i, o_i) > 0 .$$

Il découle du point iii et du point iv du lemme III.8.12 que les familles orthogonales satisfaisant la condition GS$_1$ *sont de la forme* $(\alpha_i o_i)_{1 \leq i \leq d}$ *avec*

$$\forall 1 \leq i \leq d,\ \alpha_i \in \mathbb{K}^* .$$

Une telle famille est orthonormale si de plus

$$\forall 1 \leq i \leq d,\ 1 = \phi(\alpha_i o_i, \alpha_i o_i) = \|\alpha_i\|^2 \phi(o_i, o_i) ;$$

c'est-à-dire si

$$\forall 1 \leq i \leq d,\ \|\alpha_i\|^2 = \frac{1}{\phi(o_i, o_i)} .$$

Or on peut toujours trouver

$$(\alpha_i)_{1 \leq i \leq d} \in \mathbb{K}^* \text{ tel que } \forall 1 \leq i \leq d,\ \|\alpha_i\|^2 = \frac{1}{\phi(o_i, o_i)} ;$$

ce qui prouve l'existence d'une famille orthonormale satisfaisant la condition GS$_1$.

Unicité Avec les notations précédentes, si l'on exige que la condition GS_2 soit satisfaite on a

$$\forall 1 \leq i \leq d,\ \phi(e_i, \alpha_i o_i) \ = \ \alpha_i \phi(e_i, o_i) \ \in \ \mathbb{R}^+ \, .$$

Comme par ailleurs $\|\alpha_i\|^2 \ = \ \dfrac{1}{\phi(o_i, o_i)}$ *, on a nécessairement*

$$\forall 1 \leq i \leq d,\ \alpha_i \ = \ \frac{1}{\sqrt{\phi(o_i, o_i)}} \cdot \frac{\overline{\phi(e_i, o_i)}}{\|\phi(e_i, o_i)\|} \, .$$

Ce qui prouve l'unicité.

Théorème III.8.14 (Inégalité de CAUCHY–SCHWARZ) *Soit (E, ϕ) un espace pré-hilbertien réel (et dans ce cas on note $\mathbb{K} \ = \ \mathbb{R}$,) ou complexe (et dans ce cas on note $\mathbb{K} \ = \ \mathbb{C}$,) (cf. la définition III.8.4.)*

i) $\forall (x, y) \in E \times E,\ \|\phi(x, y)\| \ \leq \ \phi(x, x)\phi(y, y)$;

ii) l'inégalité ci-dessus et une égalité si et seulement si x et y sont liés.

***Démonstration** : Si $\mathbb{K} \ = \ \mathbb{C}$, pour tous*

$$\theta \ \in \ \mathbb{R} \, , \ (x', y) \ \in \ E \times E \phi(e^{i\theta} x', y) \ = \ e^{-i\theta} \phi(x', y) \, .$$

Il existe donc

$$\theta(x') \ \in \ \mathbb{R} \ \text{tel que} \ \phi(e^{i\theta(x')} x', y) \ \in \ \mathbb{R} \, .$$

Alors

$$\phi(x', x') \ = \ \phi\big(e^{i\theta(x')} x', e^{i\theta(x')} x'\big) \ \text{et} \ \|\phi(x', y)\| \ = \ \big\|\phi\big(e^{i\theta(x')} x', y\big)\big\| \, .$$

On pose alors $x \ := \ e^{i\theta(x')} x'$.

Si $\mathbb{K} \ = \ \mathbb{R}$, $\phi(x', y) \ \in \ \mathbb{R}$. Puisque ϕ est positive par hypothèse,

$$\begin{array}{lll} \forall \lambda \in \mathbb{R}, & \phi(\lambda x + y, \lambda x + y) & \geq \ 0 \\ \Leftrightarrow & \lambda \overline{\lambda} \phi(x, x) + \overline{\lambda} \phi(x, y) + \lambda(\phi(y, x) + \phi(y, y) & \geq \ 0 \\ \Leftrightarrow & \lambda^2 \phi(x, x) + 2\lambda \phi(x, y) + \phi(y, y) & \geq \ 0 \, . \end{array}$$

— *Si $\phi(x, x) \ = \ 0$, on a*

$$\forall \lambda \in \mathbb{R},\ 2\lambda \phi(x, y) + \chi(y) \ \geq 0 \, ;$$

ce qui entraîne $\phi(x, y) \ = \ 0$ et prouve le point i.

— *Sinon on a un polynôme de degré 2 à coefficients réels qui a au plus une racine double ; ce qu'i entraîne que*

$$\phi(x, y)^2 - \phi(x, x)\phi(y, y) \ \leq \ 0 \, ;$$

qui prouve le point i.

Puisque ϕ définie (cf. l'axiome $Eucl_4$ de la définition III.8.1 ou l'axiome $Herm_4$ de la définition III.8.2,) est et égalité dans le point i. Si $x \ \neq \ 0$, $\phi(x, x) \ \neq \ 0$, et le discriminant $\phi(x, y)^2 - \phi(x, x)\phi(y, y)$ du polynôme $\phi(x, x)\lambda^2 + 2\lambda\phi(x, y) + \phi(y, y)$ est nul ; c'est-à-dire que ce dernier possède une racine λ_0. Il existe donc

$$\lambda_0 \ \in \ \mathbb{R} \ \text{tel que} \ \phi(\lambda_0 x + y, \lambda_0 x + y) \ = \ 0 \, ;$$

ce qui entraîne, puisque ϕ est définie $\lambda_0 x + y \ = \ 0$ et prouve donc le point ii.

Corollaire III.8.15 (Inégalité de MINKOWSKI)

$$\forall (x,y) \in E \times E,\ \phi(x+y,x+y)^{\frac{1}{2}} \ \leq\ \phi(x,x)^{\frac{1}{2}} \ +\ \phi(y,y)^{\frac{1}{2}}\ .$$

Démonstration *:*

$$\begin{array}{rcl} \forall (x,y) \in E \times E, \quad \phi(x+y,x+y) & = & \phi(x,x) + \phi(y,y) + \phi(x,y) + \overline{\phi(x,y)} \\ & = & \phi(x,x) + \phi(y,y) + 2\mathrm{Re}(\phi(x,y)) \\ & \leq & \phi(x,x) + \phi(y,y) + 2\|\phi(x,y)\|\ . \end{array}$$

Il vient alors, en utilisant le théorème III.8.14,

$$\begin{array}{rcl} \phi(x+y,x+y) & \leq & \phi(x,x) + \phi(y,y) + 2\phi(x,x)\phi(y,y) \\ & \leq & \left(\phi(x,x)^{\frac{1}{2}} + \phi(y,y)^{\frac{1}{2}}\right)^2\ . \end{array}$$

Proposition III.8.16 (Norme euclidienne/hermitienne) *Si (E,χ) est un espace préhilbertien réel (resp. complexe,)*

*i) (**Norme**)*
l'application

$$E\ \to\ \mathbb{R}^+\ ,\ x\ \mapsto\ ||x||_\chi\ :=\ \phi(x,x)^{\frac{1}{2}}$$

(qu'on notera le plus souvent simplement $||x||$ s'il n'y a pas d'ambiguïté sur la structure considérée,) est une norme , au sens où elle vérifie les propriétés Nor_1 à Nor_4. On l'apelle norme euclidienne (resp. norme hermitienne .

Le couple $(E, ||\cdot||)$ est alors un espace vectoriel normé .

$$\forall (x,y,\lambda) \in E \times E \times \mathbb{K},$$

Nor_1)

$$||x||\ \in\ \mathbb{R}^+\ ;$$

*Nor_2) (**Homogénéité**)*

$$||\lambda x||\ =\ \|\lambda\|||x||\ ;$$

*Nor_3) (**Séparation**)*
$||x||\ =\ 0$ *si et seulement si* $x\ =\ 0$;

*Nor_4) (**Inégalité triangulaire**)*

$$||x+y||\ \leq\ ||x|| + ||y||\ ;$$

Démonstration *: Seul l'axiome Nor_4 nécessite une justification qui n'est autre que l'inégalité de* MINKOWSKI *(cf. le corollaire III.8.15.)*

ii) ***(Distance)***
l'application $d : E \times E \to \mathbb{R}^+$, $(x, y) \mapsto ||x - y||$ *est une distance au sens où elle vérifie les axiomes* $Dist_1$ *à* $Dist_4$. *On l'appelle distance euclidienne .*

Le couple (E, d) *est donc un espace métrique .*

$$\forall (x, y) \in E \times E,$$

$Dist_1$*)*

$$d(x, y) \in \mathbb{R}^+ ;$$

$Dist_2$*)* ***(Séparation)***
$d(x, y) = 0$ *si et seulement si* $x = y$;

$Dist_3$*)* ***(Symétrie)***
$d(x, y) = d(y, x)$;

$Dist_4$*)*

$$d(x, z) \leq d(x, y) + d(y, z) \text{ (inégalité triangulaire.)}$$

III.9 . −Espaces vectoriels euclidiens, hermitiens

Dans ce paragraphe (III.9,) $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ **est le *corps* (cf. la définition III.1.1.12,) des *nombres réels* ou des *nombres complexes* .**

Définition III.9.1 (Espace euclidien) Un *espace euclidien* est un *espace pré-hilbertien réel* (cf. la définition III.8.4,) (E, ϕ) tel que E est un $\mathbb{R}$-*espace vectoriel* de *dimension finie* (cf. le point c du point ix III.1.2.)

Autrement dit c'est un *couple* (E, ϕ) où E est un $\mathbb{R}$-*espace vectoriel* de *dimension finie* et ϕ un *produit scalaire euclidien* sur E au sens de la définition III.8.1.

On dira aussi que le $\mathbb{R}$-*espace vectoriel* E est muni d'une *structure euclidienne* .

Définition III.9.2 (Espace hermitien) Un *espace hermitien* est un *espace pré-hilbertien complexe* (cf. la définition III.8.4,) (E, ϕ) tel que E est un $\mathbb{C}$-*espace vectoriel* de *dimension finie* (cf. le point c du point ix III.1.2.)

Autrement dit c'est un *couple* (E, ϕ) où E est un $\mathbb{C}$-*espace vectoriel* de *dimension finie* et ϕ un *produit scalaire hermitien* sur E au sens de la définition III.8.2.

On dira aussi que le $\mathbb{C}$-*espace vectoriel* E est muni d'une *structure hermitienne* .

Proposition III.9.3 (Supplémentaire orthogonal) *Dans un espace euclidien* (E, ϕ), *pour tout sous-espace* $F \subset E$,

i) $E = F \oplus^{\perp_\phi} F^{\perp,\phi}$.

ii) De plus $F = F^{\perp^\perp}$.

Démonstration : *C'est une conséquence immédiate de la proposition III.8.10 ; puisque tout sous-espace vectoriel de* E *est de dimension finie .*

Proposition III.9.4 (Bases orthonormales) *L'espace vectoriel E possède une base orthonormale $(e_i)_{1 \leq i \leq \dim E} \in E$.*

Démonstration *: Soit $(u_i)_{1 \leq i \leq \dim E} \in E$ une base de E. D'après le théorème III.8.13, il existe une famille orthonormale $(e_i)_{1 \leq i \leq \dim E} \in E$ telle que*

$$\mathrm{Vect}\big\{e_1, \ldots, e_{\dim E}\big\} \;=\; \mathrm{Vect}\big\{u_1, \ldots, u_{\dim E}\big\}\,;$$

si bien que $(e_i)_{1 \leq i \leq d}$ est une base de E.

Proposition III.9.5 (Compacité de la sphère unité) *Dans un espace euclidien (cf. la définition III.9.1,) (resp. espace hermitien (cf. la définition III.9.2,)) (E, ϕ), la sphère unité i.e. l'ensemble des éléments de norme 1, i.e. l'ensemble*

$$\mathbf{S}_E \;:=\; \{x \in E\,;\, ||x||_\phi \,=\, 1\} \subset E$$

est une partie compacte de l'espace métrique (E, d) où d est la distance euclidienne introduite au point ii de la proposition III.8.16 ; ou encore de l'espace vectoriel normé $(E, ||\cdot||)$ (cf. le point i de la proposition III.8.16.)

Démonstration *: Évidemment les détails de cette preuve échappent au cadre stricte de ce cours et l'on conseil de se rapporter au cours de topologie pour disposer de tous les arguments.*

Cependant la norme euclidienne ou hermitienne fait de E un $\mathbb{R}$-espace vectoriel normé de dimension finie . Il suffit donc alors de prouver que $\mathbf{S}_E$ est borné, ce qui est tautologique et fermé, ce qui est un exercice.

III.10 . –Endo*morphisme* s autoadjoints et théorème spectral

Dans ce paragraphe (III.10,) le corps $\mathbb{K}$ est :

- **soit le *corps* $\mathbb{R}$ des *réels* et dans ce cas (E, ϕ) est un *espace pré-hilbertien réel* (cf. le point i de la définition III.8.4 ;)**
- **soit le *corps* $\mathbb{C}$ des *nombres complexes* et dans ce cas (E, ϕ) est un *espace pré-hilbertien complexe* (cf. le point ii de la définition III.8.4.)**

Le lecteur pourra toujours lire ce paragraphe III.10, en supposant que E est un $\mathbb{K}$-*espace vectoriel* de *dimension finie* ; mais pour un certains nombre d'énoncés cette hypothèse n'est pas requise. Nous prendrons garde de signaler explicitement les situation dans lesquelles il est indispensable que E soit un $\mathbb{K}$-*espace vectoriel* de *dimension finie* .

Définition III.10.1 (Adjoint d'un endomorphisme) Étant donné un *endomorphisme* $u \in \mathrm{End}(E)$ de E *i.e.* une *application linéaire* de E dans lui-même, on dit qu'un endomorphisme $v \in \mathrm{End}(E)$ est *ϕ-adjoint* (ou même simplement *adjoint* , s'il n'y a pas d'ambiguïté sur la forme ϕ,) si

$$\forall (x, y) \in E \times E,\; \phi\big(u(x), y\big) \;=\; \phi\big(x, v(y)\big)\,. \qquad \text{III.10.1.1}$$

Proposition III.10.2 (Propriétés de l'adjoint) *Soient*

$$(u, v) \;\in\; \mathrm{End}(E) \times \mathrm{End}(E) \;\textit{tel que}\; v \;\textit{est adjoint de}\; u\,.$$

i) Alors u est adjoint de v et on dira simplement que u et v sont adjoints l'un de l'autre.

Démonstration : *Si v est adjoint de u, (cf. III.10.1.1 :)*

$$\begin{array}{lrcl} \forall (x,y) \in E \times E, & \underline{\phi\big(u(x),y\big)} & = & \underline{\phi\big(x,v(y)\big)} \\ \Leftrightarrow & \phi\big(u(x),y\big) & = & \phi\big(x,v(y)\big) \\ \Leftrightarrow & \phi\big(y,u(x)\big) & = & \phi\big(v(y),x\big)\ . \end{array} \qquad 1$$

ii) Si w est un adjoint de u, alors $v = w$. Ainsi sur un espace euclidien (resp. hermitien ,) un endomorphisme u possède au plus un adjoint .

Démonstration :

$$\begin{array}{lrcl} \forall (x,y) \in E \times E, & \phi(x, v(y) - w(y)) & = & \phi\big(x,v(y)\big) - \phi\big(x,w(y)\big) \\ & & = & \phi\big(u(x),y\big) - \phi\big(u(x),y\big) \\ & & = & 0 \\ \Rightarrow & \phi(w(y) - v(y), x) & = & 0 \\ \Rightarrow \forall y \in E, & v(y) & = & w(y) \\ \Rightarrow & v & = & w\ . \end{array}$$

Proposition III.10.3 (Existence et unicité de l'adjoint) *Si (E,ϕ) est un espace euclidien (cf. la définition III.9.1,) (resp. un espace hermitien (cf. III.9.2,)) tout endomorphisme u admet un unique adjoint v.*

Démonstration : *L'unicité est déjà établie au point ii de la proposition III.10.2 indépendamment de E soit de dimension finie*

Soit $(e_i)_{1 \leq i \leq d}$ une base orthonormale (cf. la proposition III.9.4.) Si un adjoint v de u existe, il est caractérisé, comme tout endomorphisme dans une base orthonormale par

$$\forall 1 \leq j \leq d,\ v(e_j) \ = \ \sum_{i=1}^{d} \phi(v(e_j), e_i) e_i\ .$$

On a donc

$$\forall 1 \leq h \leq d,\ v_j \ = \ \sum_{i=1}^{d} \phi(e_j, u(e_i)) e_i\ .$$

Ceci détermine complètement v.

Notation III.10.4 Si (E,ϕ) est un *espace euclidien* (resp. un *espace hermitien* , tout *endomorphisme* $u \in \mathrm{End}(E)$ de E possède un unique *adjoint* noté u^* .

Il découle immédiatement de la construction donnée à la proposition III.10.3 que
dans toute *base orthonormale* la *matrice* de u^* est la transposée de la matrice de u.

Définition III.10.5 (Endomorphisme autoadjoint) Un *endomorphisme* u de E est *auto-adjoint* si il est égal à son *adjoint* .

Cela signifie encore que

$$\forall (x,y) \in E \times E,\ \phi\big(u(x),y\big) \ = \ \phi\big(x,u(y)\big)\ .$$

Proposition III.10.6 (Caractérisation matricielle des endomorphismes autoadjoints) *Étant donné un espace euclidien* (E, ϕ), *un endomorphisme* u *de* E *est auto-adjoint si et seulement si la matrice*

$$M_{\mathcal{B}}^{\mathcal{B}}(u) \ := \ (m_{i,j})_{\substack{1 \leqslant i \leqslant \dim E \\ 1 \leqslant j \leqslant \dim E}}$$

de u *dans une base orthonormale* $\mathcal{B}$ *(cf. III.8.5.iii) vérifie*

$$\forall 1 \leq i \leq \dim E, \ \forall 1 \leq j \leq \dim E, \ m_{i,j} \ = \ \overline{m_{j,i}} \ .$$

Proposition III.10.7 (Semi-simplicité des endomorphisme autoadjoints) *Soit* $u \in \mathrm{End}(E)$ *autoadjoint.*

i) Pour tout sous-espace vectoriel $F \subset E$? *si* F *est* u*-stable (cf. la définition III.1.3.10,) son orthogonal* $F^{\perp}$ *(cf. la définition III.8.5,) est* u*-stable . De plus* $u_{|F}$ *(resp.* $u_{|F^{\perp}}$*,) est un endomorphisme auto-adjoint de* F *(resp.* $F^{\perp}$*.)*

Démonstration *:*

$$\begin{array}{lrcl} \forall y \in F^{\perp}, \ \forall x \in F, & u(x) & \in & F \\ \Rightarrow & \phi\big(u(x), y\big) & = & 0 \\ \Rightarrow & \phi\big(x, u(y)\big) & = & 0 \\ \Rightarrow & u(y) & \in & F^{\perp, \chi} \ . \end{array}$$

*ii) (**Semi-simplicité**)*

Si E *est un espace euclidien (cf. la définition III.9.1,) (resp. un espace hermitien (cf. la définition III.9.2 ;) ce qui entraîne en particulier que* E *est de dimension finie ; alors tout sous-espace vectoriel* u*-stable de* E *possède un supplémentaire orthogonal* u*-stable . On dit alors que* u *est un endomorphisme semi-simple .*

Démonstration *: D'après la proposition III.9.3, pour tout sous-espace vectoriel* $F \subset E$,

$$E \ = \ F \ \oplus^{\perp_{\chi}} F^{\perp} \ .$$

Si de plus, F *est* u*-stable , il découle de le point i , que* $F^{\perp}$ *l'est aussi.*

Proposition III.10.8 (Éléments propres d'un endomorphisme autoadjoint) *Un endomorphisme auto-adjoint*

$u \in \mathrm{End}(E)$ *de* E *(cf. la définition III.10.5,) possède toujours un vecteur propre (cf. le point ii de la définition III.7.2.2,)et une valeur propre (cf. le point i de la définition III.7.2.2,) associée ; cette dernière est réelle y compris dans le cas où* (E, ϕ) *est un espace hermitien .*

Démonstration *:*

Lemme III.10.8.1 *Pour tout* $x \in E, \phi\big(x, u(x)\big) \in \mathbb{R}$.

Démonstration *: Si* E *est un espace euclidien c'est tautologique. Si* E *est un espace hermitien l'*axiome Herm_2 *de la définition III.8.2 entraîne que*

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

Par définition de l'adjoint u^* *de* u *(cf. la définition III.10.1,)*

$$\phi\big(u(x), x\big) \ = \ \phi\big(x, u^*(x)\big) \ ;$$

Si donc on suppose u *auto-adjoint ,*

$$\overline{\phi\big(x, u(x)\big)} \ = \ \phi\big(u(x), x\big) \ = \ \phi\big(x, u^*(x)\big) \ = \ \phi\big(x, u(x)\big) \ ;$$

si bien que

$$\forall x \in E, \ \phi\big(x, u(x)\big) \ \in \ \mathbb{R} \ .$$

Posons donc :

$$\rho \,:\, E \,\to\, \mathbb{R}\,,\; x \,\mapsto\, \phi\big(x,u(x)\big)\,. \qquad \textit{III.10.8.2}$$

Lemme III.10.8.3 (Dévelopement limité) *L'espace E étant mnuni de la norme euclidienne (resp. hermitienne ,) l'application ρ définie ci-dessus admet un développement limité en tout point $x \in E$. Il s'ensuit que ρ est une application différentiable et, par conséquent, une application continue .*

***Démonstration** :*

$$\begin{array}{rcl}\forall (x,y)\in E\times E,\quad \rho(x+y) &=& \phi\big(x+y,u(x+y)\big)\\ &=& \phi\big(x,u(x)\big)+\phi\big(y,u(x)\big)+\phi\big(x,u(y)\big)+\phi\big(y,u(y)\big)\\ &=& \rho(x)+2\mathrm{Re}\big(\phi\big(u(x),y\big)\big)+\rho(y)\,.\end{array}$$

L'application $y \mapsto 2\mathrm{Re}\big(\phi\big(u(x),y\big)\big)$ est $\mathbb{R}$-linéaire .

Par ailleurs

$$\forall y\in E,\ |\rho(y)|\ \le\ ||y||||u(y)||$$

d'après l'inégalité de CAUCHY–SCHWARZ *(cf. le point i du théorème III.8.14.) De plus*

$$\lim_{y\to 0} u(y)\ =\ 0\,;$$

puisque u est linéaire et E de dimension finie .

Il résulte du lemme III.10.8.3, et de la proposition III.9.5 que ρ admet un minimum (resp. un maximum) en un élément $x_- \in \mathbf{S}_E$ (resp. $x_+ \in \mathbf{S}_E$.) Notons

$$\lambda_-\ :=\ \rho(x_-)\ \text{et}\ \lambda_+\ :=\ \rho(x_+)\,;$$

et encore :

$$\begin{array}{rccc}\theta_-: & E & \longrightarrow & \mathbb{R}\\ & x & \longmapsto & \lambda_-\phi(x,x)-\rho(x)\\ \theta_+: & E & \longrightarrow & \mathbb{R}\\ & x & \longmapsto & \lambda_+\phi(x,x)-\rho(x)\end{array}$$

Lemme III.10.8.4

$$\forall x\in E,\ \theta_-(x)\ \le\ 0\ \text{et}\ \theta_+(x)\ \ge\ 0\,.$$

***Démonstration** :*

$$\begin{array}{rcl}\forall x\in E\setminus\{0\},\quad \theta_+(x) &=& \theta_+\big(||x||\dfrac{1}{||x||}x\big)\\ &=& ||x||^2\theta_+\big(\dfrac{1}{||x||}x\big)\\ &=& \phi(x,x)\big(\lambda_+\phi\big(\dfrac{1}{||x||}x,\dfrac{1}{||x||}x\big)-\rho\big(\dfrac{1}{||x||}x\big)\big)\\ &=& \phi(x,x)\big(\lambda_+-\rho\big(\dfrac{1}{||x||}x\big)\big)\\ &\ge& 0\,.\end{array}$$

Le calcul pour θ_- est tout à fait analogue.

Notons

$$\begin{array}{rccl} \psi_- : & E\times E & \longrightarrow & \mathbb{K} \\ & (x,y) & \longmapsto & \lambda_-\phi(x,y) - \phi\big(x,u(y)\big) \\ \psi_+ : & E\times E & \longrightarrow & \mathbb{K} \\ & (x,y) & \longmapsto & \lambda_+\phi(x,y) - \phi\big(x,u(y)\big)\ . \end{array}$$

On constate alors que :

i) $\forall x\in E,\ \theta_-(x) \ =\ \psi_-(x,x)$ et $\theta_+(x) \ =\ \psi_+(x,x)$;

ii) ψ_- *et* ψ_- *satisfont l'axiome* Eucl_1 *de la définition III.8.1, (resp. l'axiome* Herm_1 *de la définition III.8.2,) suivant que* E *est un espace euclidien (resp. un espace hermitien ;)*

iii) ψ_- *et* ψ_+ *satisfont l'axiome* Eucl_2*, (resp. l'axiome* Herm_2*.)*

iv) ψ_+ *satisfait l'axiome* Eucl_3*, (resp. l'axiome* Herm_3*,) (cf. le lemme III.10.8.4 ;) cependant* $\forall x\in E,\ \psi_-(x,x) \ \leq\ 0$.

v) En revanche ni ψ_- *ni* ψ_+ *ne satisfont l'axiome* Eucl_4*, (resp. l'axiome* Herm_4 *; puisque précisément*

$$\psi_-(x_-,x_-) \ =\ \theta_-(x_-) \ =\ 0 \ =\ \theta_+(x_+) \ =\ \psi_+(x_+,x_+)\ .$$

Une lecture minutieuse de la démonstration du point i du théorème III.8.14, fait apparaître que seuls les axiomes Eucl_1 *à* Eucl_3 *de la définition III.8.1, (resp. les axiomes* Herm_1 *à* Herm_3 *de la définition III.8.2,) sont requis pour établir l'inégalité de* CAUCHY–SCHWARZ *; de manière tout à fait explicite, on n'a pas besoin de l'axiome* Eucl_4*, (resp. de l'axiome* Herm_4*. Ainsi les points ii à iv entraînent-ils que*

$$\forall (x,y)\in E\times E,\ \|\psi_-(x,y)\|^2 \ \leq\ \theta_-(x)\theta_-(y) \text{ et } \|\psi_+(x,y)\|^2 \ \leq\ \theta_+(x)\theta_+(y)\ .$$

Il s'ensuit alors (cf. le point v,) que pour $\varepsilon \ =\ +$ ou $-$,

$$\forall y\in E,\ \|\psi_\varepsilon(y,x_\varepsilon)\|^2 \ \leq\ \theta_\varepsilon(x_\varepsilon)\theta_\varepsilon(y) \ =\ 0\ .$$

On a alors la suite d'équivalences :

$$\begin{array}{lrcl} \forall y\in E, & \psi_\epsilon(y,x_\epsilon) & = & 0 \\ \Leftrightarrow & \lambda_\varepsilon\phi(y,x_\varepsilon) - \phi\big(y,u(x_\varepsilon)\big) & = & 0 \\ \Leftrightarrow & \phi\big(y,\lambda_\varepsilon x_\varepsilon - u(x_\varepsilon)\big) & = & 0 \\ \Leftrightarrow u(x_\varepsilon) & & = & \lambda_\varepsilon x_\varepsilon\ ; \end{array}$$

ce qui prouve bien que λ_- *et* λ_+ *sont des valeurs propres pour* u *associées respectivement aux vecteurs propres* x_- *et* x_+ .

Théorème III.10.9 (Théorème spectral) *Étant donné un espace euclidien (cf. la définition III.9.1,) (resp. un espace hermitien (cf. la définition III.9.2,)) (E, ϕ) et un endomorphisme auto-adjoint $u \in \mathrm{End}(E)$, (cf. la définition III.10.5,) il existe une base orthonormale de E (cf. le point iii de la définition III.8.5,) constituée de vecteurs propres pour u à chacun desquels est associée une valeur propre réelle .*

***Démonstration** : Ce résultat s'établit par récurrence sur la dimension de E.*

Si $\dim_{\mathbb{K}} E = 1$, un endomorphisme de E est une homothétie de rapport λ. Supposer l'endomorphisme auto-adjoint équivaut à supposer λ réel ; et le résultat est donc immédiat.

Soit $d \in \mathbb{N}$; et supposons que pour tout triplet (E, ϕ, u) où (E, ϕ) est un espace euclidien (resp. hermitien) de dimension d et $u \in \mathrm{End}(E)$ un endomorphisme auto-adjoint , le résultat est établi.

Soit donc (E, ϕ) un espace euclidien (resp. hermitien ,) de dimension $d+1$, et $u \in \mathrm{End}(E)$ un endomorphisme auto-adjoint de E. Il existe alors (cf. la proposition III.10.8,) $e_{d+1} \in E$ un vecteur propre associé à une valeur propre réelle λ_{d+1}. En considérant attentivement la preuve de la proposition III.10.8.

On constate même que l'on peut supposer que $\phi(e_{d+1}, e_{d+1}) = 1$. Cependant il nous suffit de savoir que $\phi(e_{d+1}, e_{d+1}) \neq 0$, puisqu'alors $\phi(e_{d+1}, e_{d+1}) \in \mathbb{R}^+$. Quitte à remplacer e_{d+1} par $\dfrac{1}{\sqrt{\phi(e_{d+1}, e_{d+1})}} e_{d+1}$, on a bien $\phi(e_{d+1}, e_{d+1}) = 1$.

Notons alors $F := e_{d+1}^{\perp}$; si bien que (cf. III.8.9,)

$$E = \mathrm{Vect}\{e_{d+1}\} \oplus^{\perp} F .$$

Ainsi F est de dimension d. La restriction de ϕ à $F \times F$ fait de $\big(F, \phi_{|F\times F}\big)$ un espace euclidien (resp. un espace hermitien .)

Par ailleurs (cf. le point ii de la proposition III.10.7,) F est u-stable (cf. la définition III.1.3.10.) Enfin, $u_{|F}$ est auto-adjoint ; si bien qu'on peut applicquer l'hypothèse de récurrence au triplet $(F, \phi_{|F\times F}, u_{|F})$ et conclure.

III.11 . −Exercices

III.11.1 . −Algèbre : généralités

Exercice III.11.1.1 (Caractérisation des sous-anneaux) Faire la preuve de la proposition III.1.1.4. À noter qu'une bonne partie de cette preuve a déjà été faite pour prouver la proposition II.8.3.5.

Exercice III.11.1.2 (Anneau des applications) **1)** Faire la démonstration de la proposition III.1.1.13.

2) Pour un anneau A, le fait que A soit intègre (respectivement un corps) entraîne-t-il que l'anneau A^E considéré à la proposition proposition III.1.1.13 soit intègre (resp. un corps ?)

Exercice III.11.1.3 (Groupe des inversibles (unités) d'un anneau) Si A est un anneau, on note $A^\times$ le groupe des éléments inversibles de A.

1) Calculer $\mathbb{Z}^\times$, et $\mathbb{K}[X]^\times$ quand $\mathbb{K}$ est un corps.

2) Si $\phi : A \to B$ est un homomorphisme d'anneaux, montrer que $\phi(A^\times) \subset B^\times$; si ϕ est surjectif, s'ensuit-il que $\phi(A^\times) = B^\times$?

III.11.2 . −Espaces préhilbertien

Dans ce paragraphe (III.11.2,) $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ **est le *corps* (cf. la définition III.1.1.12,) des *nombres réels* ou des *nombres complexes* ;** E **et un *espaces pré-hilbertiens réels* ou *complexe* (cf. la définition III.8.4.)**

Exercice III.11.2.1 (Caractérisation des projecteurs orthogonaux) Étant donné un projecteur $p \in \mathrm{End}_{\mathbb{K}}(E)$, montrer que les conditions suivantes sont équivalentes :

OrthProj$_1$) $\mathrm{Ker}\, p \perp \mathrm{Im}\, p$.

OrthProj$_2$) $\forall x \in E,\ ||p(x)|| \leq ||x||$.

OrthProj$_3$) $p = p^*$.

Dans ce cas on dit que p **est un *projecteur orthogonal*.**

Exercice III.11.2.2 (Caractérisation des symétries orthogonales) Étant donnée une symétrie $s \in \mathrm{End}_{\mathbb{K}}(E)$, montrer que les propriétés suivantes sont équivalentes :

SymOrth$_1$) $s \in \mathcal{O}(E)$ *i.e.* s est un endomorphisme orthogonal.

SymOrth$_2$) $\mathrm{Ker}\,(\mathrm{Id} + s) \perp \mathrm{Ker}\,(\mathrm{Id} - s)$.

SymOrth$_3$) Le projecteur $p^+ := \frac{1}{2}(\mathrm{Id} + s)$ est un projecteur orthogonal.

SymOrth$_4$) Le projecteur $p^- := \frac{1}{2}(\mathrm{Id} - s)$ est un projecteur orthogonal.

SymOrth$_5$) $s = s^*$. On rappelle qu'on dit alors que s et *autoadjoint*.

On dit dans ce cas que la symétrie est la *symétrie orthogonale* par rapport à $\mathrm{Ker}\,(\mathrm{Id} - s)$. **On dira aussi *réflexion* par rapport à** $\mathrm{Ker}\,(\mathrm{Id} - s)$.

Exercice III.11.2.3 (Propriétés de l'orthogonal) Faire la preuve de la proposition III.8.6.

Exercice III.11.2.4 (Somme directe orthogonale) Soit E **un espace quadratique défini**

1) $F_1, \ldots, F_n$ **des sous-espaces vectoriels tels que pour** $i \neq j$, $F_i \perp F_j$.
Montrer que la somme $F_1 + \ldots + F_n$ est directe.

2) Soit $S \subset E$ **tel que** $0 \notin S$ **et** $\forall (s,t) \in S \times S,\ s \neq t \Rightarrow \phi(s,t) = 0$.

a) Montrer que S est une *partie libre* de E.

b) En déduire que si $S \subset E$ est une partie orthonormale de E, S est une *partie libre* .

III.11.3 . −Arithmétique des polynômes

Soit $(A, +, *)$ un anneau commutatif dont on note 0 l'*élément neutre* pour $+$ et 1 l'*élément neutre* pour $*$. On note $A^{\mathbb{N}}$ l'ensemble des suites à valeurs dans A ou encore de manière équivalente l'ensemble des applications de $\mathbb{N}$ dans A. Pour tout $a \in A^{\mathbb{N}}$, on note a_n le $n^{\text{ième}}$ terme de a *i.e.* la valeur de a en $n \in \mathbb{N}$.

Exercice III.11.3.1 (Valuation) 1) Rappeler ce que signifie que l'anneau A est intègre.

On suppose, dans toute la suite que $(A, +, *)$ est intègre.

2) Pour tout $a \in A^{\mathbb{N}}$, $a \neq \zeta$, montrer qu'il existe un plus petit entier $v \in \mathbb{N}$ tel que $a_v \neq 0$.

On notera désormais $\mathrm{val}(a)$ l'entier v qu'on appellera la *valuation* de a et on adoptera les conventions suivantes : $\mathrm{val}(\zeta) = (+\infty)$, $(+\infty) \leq (+\infty)$, $(+\infty) + (+\infty) = (+\infty)$

$$\forall n \in \mathbb{N},\ n + (+\infty) = (+\infty) \text{ et } n < (+\infty)\ .$$

3) Montrer que

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ \mathrm{val}(a *_{A^{\mathbb{N}}} b) = \mathrm{val}(a) + \mathrm{val}(b)\ ;$$

4) En déduire que $(A^{\mathbb{N}},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}})$ est un anneau intègre.

5) Montrer que

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ \mathrm{val}(a +_{A^{\mathbb{N}}} b) \geq \min(\mathrm{val}(a), \mathrm{val}(b))$$

avec égalité si $\mathrm{val}(a) \neq \mathrm{val}(b)$.

6) Montrer que

$$\mathfrak{m} := \{a \in A^{\mathbb{N}}\ ;\ \mathrm{val}(a) > 0\}$$

est un idéal de $A^{\mathbb{N}}$ dont on donnera une autre caractérisation.

Exercice III.11.3.2 (degré) On suppose encore dans cette question que A est un anneau intègre.

1) Montrer que, pour tout $a \in \mathcal{P}$, $a \neq \zeta$, il existe un entier $d \in \mathbb{N}$ tel que

$$a_d \neq 0 \text{ et } \forall n \in \mathbb{N},\ n > d \Rightarrow a_n = 0\ .$$

On notera désormais $\deg(a)$ l'entier d qu'on appellera le *degré* de a et on adoptera les conventions suivantes : $\deg(\zeta) = (-\infty)$, $(-\infty) \leq (-\infty)$, $(-\infty) + (-\infty) = (-\infty)$

$$\forall n \in \mathbb{N},\ n + (-\infty) = (-\infty) \text{ et } n > (-\infty)\ .$$

2) Montrer que

$$\forall (a, b) \in \mathcal{P} \times \mathcal{P},\ \deg(a *_{A^{\mathbb{N}}} b) = \deg(a) + \deg(b)\ .$$

3) Montrer que

$$\forall (a, b) \in \mathcal{P} \times \mathcal{P},\ \deg(a +_{A^{\mathbb{N}}} b) \leq \max(\deg(a), \deg(b))$$

avec égalité si $\deg(a) \neq \deg(b)$.

4) En déduire que $(\mathcal{P},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$ est un anneau commutatif intègre.

5) Montrer que

$$\mathfrak{m}_0\ :=\ \mathcal{P}\cap\mathfrak{m}$$

est un idéal de $\mathcal{P}$ (où $\mathfrak{m}$ est l'idéal de $A^{\mathbb{N}}$ défini à la question 6 de l'exercice III.11.3.1.)

6) Montrer que pour tout $(a,b)\ \in\ \mathcal{P}\times\mathcal{P}$, si b divise a et $a\neq\zeta$, $\deg(b)\ \leq\ \deg(a)$

7) Montrer que l'image du morphisme i (cf. cours III.6.1.7.1,) est contenue dans $\mathcal{P}$ et que i est donc un morphisme injectif d'anneaux de A dans $\mathcal{P}$. Caractériser les éléments de $\operatorname{Im} i$ par leur degré.

8) Montrer que la restriction $i^\times\ :=\ i_{|A^\times}$ de i à l'*ensemble des éléments inversibles* $A^\times$ de A est un *morphisme de groupes bijectif* de $(A^\times,*)$ dans $(\mathcal{P}^\times,\ *_{A^{\mathbb{N}}}\ )$
Indication : *on pourra penser à caractériser les éléments de $\mathcal{P}^\times$ en termes de degré.*

Exercice III.11.3.3 (Théorème chinois des restes dans $\mathbb{K}[X]$) Dans tout cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{K}$.

Pour tout couple $(P,Q)\in\mathbb{K}[X]^2$, on notera Q mod P la *classe de Q modulo P* c'est-à-dire l'ensemble des $Q'\in\mathbb{K}[X]$ tels que $P|Q'-Q$ et

$$\mathbb{K}[X]/P\ =\ \{Q'\ \textbf{mod}\ P\ ,\ Q'\in\mathbb{K}[X]\}\ .$$

1) Montrer que $\mathbb{K}[X]/P$ est en fait l'anneau quotient $\mathbb{K}[X]/P\mathbb{K}[X]$ de $\mathbb{K}[X]$ par l'idéal engendré par P.

2) Montrer que si P_1 et P_2 sont deux éléments premiers entre eux de $\mathbb{K}[X]$, leur **Ppcm** est leur produit.

Pour tout couple $(P_1,P_2)\ \in\ \mathbb{K}[X]$, on notera $\mathbb{K}[X]/P_1\times\mathbb{K}[X]/P_2$ l'ensemble des couples (α_1,α_2) $\alpha_1\in\mathbb{K}[X]/P_1$ $\alpha_2\in\mathbb{K}[X]/P_2$, muni des lois :

$$\begin{array}{rcl}(\alpha_1,\alpha_2)+(\beta_1,\beta_2) & := & (\alpha_1+\beta_1,\alpha_2+\beta_2)\\ (\alpha_1,\alpha_2)*(\beta_1,\beta_2) & := & (\alpha_1*\beta_1,\alpha_2*\beta_2)\ .\end{array}$$

3) a) Pour tout $(P_1,P_2)\in\mathbb{K}[X]^2$, montrer que $\mathbb{K}[X]/P_1\times\mathbb{K}[X]/P_2$ est un anneau dont on déterminera l'unité et l'*élément neutre* pour $+$.

b) Montrer que l'application

$$\begin{array}{rccl}\phi:& \mathbb{K}[X] & \to & \mathbb{K}[X]/P_1\times\mathbb{K}[X]/P_2\\ & Q & \mapsto & (Q\bmod P_1, Q\bmod P_2)\end{array}$$

est un *morphisme d'anneaux* .

c) Déterminer le noyau K de ϕ puis en déduire qu'il existe un *morphisme d'anneaux* injectif

$$\gamma\ :\ \mathbb{K}[X]/K\ \to\ \mathbb{K}[X]/P_1\times\mathbb{K}[X]/P_2\ \text{ tel que }\ \phi\ =\ \gamma\circ\pi$$

où π est la *surjection canonique* $\mathbb{K}[X]\ \to\ \mathbb{K}[X]/K$.

d) Si P_1 et P_2 sont premiers entre eux, montrer que ϕ est surjectif ; en déduire, dans ce cas, que γ est un isomorphisme ; décrire K plus précisément.

4) Soient a et b deux éléments distincts de k et P un élément de $\mathbb{K}[X]$.

Déterminer le reste de la division euclidienne de P par $(X-a)(X-b)$ si le reste de la division euclidienne de P par $X-a$ (resp. $X-b$,) vaut 1.

Exercice III.11.3.4 (Idéaux de $\mathbb{Z}$ et $\mathbb{K}[X]$) **1)** Montrer qu'une partie $\mathfrak{I} \subset \mathbb{Z}$ de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$ si et seulement si $\mathfrak{I}$ est un idéal de $(\mathbb{Z},+,*)$.

2) Montrer qu'un idéal $\mathfrak{I} \subset \mathbb{Z}$ non nul de $\mathbb{Z}$, possède un plus petit élément $d \in \mathbb{N}^*$; puis que

$$\mathfrak{I} = d\mathbb{Z} = \{dz\ ,\ z \in \mathbb{Z}\}\ .$$

3) a) Vérifier que l'ensemble $\mathbb{K}[X]$ des polynômes à une indéterminée sur un corps $\mathbb{K}$ est un anneau (on pourra donner explicitement la somme et le produit de deux polynômes en fonction de leurs coefficients.)

b) Tout sous-groupe de $\mathbb{K}[X]$ est-il un idéal de $\mathbb{K}[X]$?

c) Déterminer les idéaux de $\mathbb{K}[X]$.

d) Les sous-ensembles suivants de $\mathbb{K}[X]$ sont-ils des idéaux :

— $$E_0 := \{P \in \mathbb{K}[X]\ ;\ P(0) = 0\}\ ;$$

— $$\forall a \in \mathbb{K},\ a \neq 0\ ,\ E_a := \{P \in \mathbb{K}[X]\ ;\ P(0) = a\}\ ;$$

— $$E'_0 := \{P \in \mathbb{K}[X]\ ;\ P'(0) = 0\}\ ?$$

Exercice III.11.3.5 (Éléments associés) Faire la démonstration du lemme III.4.13.

Exercice III.11.3.6 (Le $\mathbb{K}$-*espace vectoriel* $\mathbb{K}[X]/P\mathbb{K}[X]$) Soient $\mathbb{K}$ un *corps* , $P \in \mathbb{K}[X]$ un *polynôme* à coefficients dans $\mathbb{K}$ et

$$\pi\ :\ \mathbb{K}[X]\ \to\ \mathbb{K}[X]/P\mathbb{K}[X] \text{ la } \textit{surjection canonique}\ .$$

Montrer que :

1) $\mathbb{K}[X]/P\mathbb{K}[X]$ est un $\mathbb{K}$-*espace vectoriel* ;

2)
$$\big(\pi(1), \pi(X), \ldots, \pi(X^{\deg(P)-1})\big) \text{ en est une base ;}$$

3)
$$\text{par conséquent } \dim_{\mathbb{K}} \mathbb{K}[X]/P\mathbb{K}[X] = \deg(P)\ .$$

III.11.4 . −Réduction

Exercice III.11.4.1 (Caractérisation des projecteurs) Étant donné un endomorphisme $p \in \mathrm{End}_{\mathbb{K}}(E)$,

montrer que les assertions suivantes sont équivalentes :

Proj$_1$) $p \circ p = p$.

Proj$_2$) $E = \mathrm{Ker}\, p \oplus \mathrm{Ker}\, \mathrm{Id}_E - p$.

Proj$_3$) $E = \mathrm{Ker}\, p \oplus \mathrm{Im}\, p$ et $p_{|\mathrm{Im}\, p} = \mathrm{Id}_{\mathrm{Im}\, p}$.

Proj$_4$) Si E est de dimension finie n, il existe des entiers r et s, avec $r+s = n$ et une base de E dans laquelle la matrice de p est, par blocs, $\begin{pmatrix} I_r & 0 \\ 0 & 0_s \end{pmatrix}$.

Si p satisfait les conditions équivalentes ci-dessus, on dit que p et un *projecteur* .

Exercice III.11.4.2 (Caractérisation des symétries) Étant donné un endomorphisme $s \in \mathrm{End}_{\mathbb{K}}(E)$,.

Montrer que les propriétés suivantes sont équivalentes :

Sym$_1$) $s \circ s = \mathrm{Id}_E$.

Sym$_2$) $p^+ := \frac{1}{2}(\mathrm{Id}_E + s)$ est un projecteur.

Sym$_3$) $p^- := \frac{1}{2}(\mathrm{Id}_E - s)$ et un projecteur.

Sym$_4$) $E = \mathrm{Ker}\,(\mathrm{Id} + s) \oplus \mathrm{Ker}\,(\mathrm{Id} - s)$.

Sym$_5$) Si E est de dimension finie n, il existe des entiers r et s, avec $r+s = n$ et une base de E dans laquelle la matrice de s est $\begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$.

On dit alors que s et une *symétrie* ou une *involution linéaire*.

Exercice III.11.4.3 (Déterminants par blocs) Pour tout $n \in \mathbb{N}^*$, on note $I_n \in \mathcal{M}_n(\mathbb{R})$ la matrice identité. Dans la suite p et q sont dans $\mathbb{N}^*$.

1) Soient

$$A \in \mathcal{M}_p(\mathbb{R}) \text{ et } B \in \mathcal{M}_q(\mathbb{R}) .$$

a) Calculer en fonction de $\det(A)$ et $\det(B)$

$$\det(\begin{pmatrix} A & 0 \\ 0 & I_q \end{pmatrix}) \text{ et } \det(\begin{pmatrix} I_p & 0 \\ 0 & B \end{pmatrix}) .$$

b) En déduire $\det(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix})$ en fonction de $\det(A)$ et $\det(B)$.

Indication : *Utiliser la multiplicativité du déterminant.*

2) Soient

$$A \in \mathcal{M}_p(\mathbb{R}) \, , \; B \in \mathcal{M}_q(\mathbb{R}) \text{ et } C \in \mathcal{M}_{p,q}(\mathbb{R}) \, .$$

a) Calculer $\det(\begin{pmatrix} A & C \\ 0 & I_q \end{pmatrix})$ en fonction de $\det(A)$.

b) Pour

$$M := \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \in \mathcal{M}_{p+q}\mathbb{R},$$

calculer $\det(M)$ en fonction de $\det(A)$ et $\det(B)$.

Exercice III.11.4.4 (AB et BA ont même polynôme caractéristique) Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}$, et $A, B \in \mathcal{M}_n(\mathbb{K})$.

1) (Valeurs propres)

a) Montrer que si X est un vecteur propre de AB pour une valeur propre $\lambda \neq 0$, alors $Y = BX \neq 0$.

b) En déduire que AB et BA ont les mêmes valeurs propres.
Indication : *Pour $\lambda = 0$, on pourra se servir du déterminant.*

2) Montrer que si A ou B est inversible, alors AB et BA ont même *polynôme caractéristique* .

3) On ne supose plus nécessairement que A ou B est inversible. On note $I \in \mathcal{M}_n(\mathbb{K})$ la matrice identité et

$$P := \begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{K}) \, ; Q := \begin{pmatrix} BA & -B \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{K}) \, ; R := \begin{pmatrix} 0 & -B \\ 0 & AB \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{K}) \, .$$

a) Vérifier que P est inversible.

b) Vérifier que $QP = PR$.

c) Conclure.

Exercice III.11.4.5 (Polynômes caractéristiques de AA^* et A^*A) Soit $A \in \mathcal{M}_{p,q}(\mathbb{C})$ où p et q sont des *entiers naturels* tels que $p \leq q$.

Pour k et ℓ des *entiers naturels* on notera $0_{k,\ell} \in \mathcal{M}_{k,\ell}(\mathbb{C})$ la matrice nulle.

1) Montrer qu'il existe une matrice unitaire $P \in \mathcal{M}_q(\mathbb{C})$ et une matrice $B \in \mathcal{M}_p(\mathbb{C})$ telles que P^*A^* s'écrive par blocs $P^*A^* = \begin{pmatrix} B^* \\ 0_{q-p,p} \end{pmatrix}$.

2) En déduire que $\det\big(X\mathrm{Id}_p - AA^*\big) = \det\big(X\mathrm{Id}_p - BB^*\big)$.

3) Montrer que $\det\big(X\mathrm{Id}_q - A^*A\big) \;=\; X^{q-p}\det\big(X\mathrm{Id}_p - B^*B\big)$.

4) Montrer que $\det\big(X\mathrm{Id}_q - A^*A\big) \;=\; X^{q-p}\det\big(X\mathrm{Id}_p - AA^*\big)$.

5) Peut-on s'affranchir de l'hypothèse $p \;\leq q$?

III.11.5 . −Endomorphismes autoadjoints

Exercice III.11.5.1 (Comparaison de valeurs propres) Soient $h \in \mathcal{L}(E)$ autoadjoint, $\vec{x}_0 \in E$ unitaire, p la projection orthogonale sur vect$(\vec{x}_0)$, et $f = h + p$.

On note $\lambda_1 \leq \cdots \leq \lambda_n$ les valeurs propres de h et $\mu_1 \leq \cdots \leq \mu_n$ celles de f.

Montrer que $\lambda_1 \leq \mu_1 \leq \cdots \leq \lambda_n \leq \mu_n$.

Exercice III.11.5.2 (Rayon spectral) Soit $f \in \mathcal{L}(E)$. Montrer que $\|f\|^2 = \max\{|\lambda| \text{ tq } \lambda \in \mathrm{Sp}(f^* \circ f)\}$.

Exercice III.11.5.3 Soit E un espace euclidien de dimension 3.

1) Soit $\{e_1, e_2, e_3\}$ une base orthonormée de E.

Soient

$$x \;:=\; x_1e_1 + x_2e_2 + x_3e_3 \text{ et } y \;:=\; y_1e_1 + y_2e_2 + y_3e_3$$

deux vecteurs de E.

Calculer $\langle x \mid y\rangle$ en fonction des coefficients x_i et y_i (pour $i \in \{1, 2, 3\}$).

2) On considère $u \in \mathrm{End}(E)$ un endomorphisme auto-adjoint. On note λ sa plus petite valeur propre et λ' sa plus grande valeur propre.

Montrer que l'on a,

$$\forall x \in E,\; \lambda||x||^2 \;\leq\; \langle u(x) \mid x\rangle \;\leq\; \lambda'||x||^2 .$$

(On utilisera une base orthonormée convenable.)

3) Soit $v \in \mathrm{End}(E)$ un endomorphisme quelconque.

a) Montrer que $u \;:=\; \dfrac{1}{2}(v + v^*)$ est auto-adjoint.

b) Soient μ une valeur propre de v, λ la plus petite valeur propre de u et λ' la plus grande valeur propre de u. Montrer que $\lambda \leq \mu \leq \lambda'$.

III.11.6 . −Spectres de certains graphes

Exercice III.11.6.1 ($\mathbf{C}_4$) 1) (Matrice)

Donner la *matrice d'adjacence* du *cycle* $\mathbf{C}_4$.

2) (Spectre)

Déterminer le *spectre* du *cycle* $\mathbf{C}_4$.

Exercice III.11.6.2 (Le cycle $\mathbf{C}_n$) **Soit $n \in \mathbb{N}^*$ et $\Phi(\mathbf{C}_n)$ l'*endomorphisme d'adjacence* du *cycle* $\mathbf{C}_n$.**

Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ on note $\alpha_a \in \mathbb{C}^{\mathbf{C}_n} = \mathbb{C}^{\mathbb{Z}/n\mathbb{Z}}$ défini par $\alpha_a(a) = 1$ et $\forall b \in \mathbb{Z}/n\mathbb{Z},\ b \neq a\ ,\ \alpha_a(b) = 0$.

1) On note $\alpha := \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \alpha_a$.

a) Déterminer $\Phi(\mathbf{C}_n)(\alpha)$.

b) En déduire que 2 est *valeur propre* de $\Phi(\mathbf{C}_n)$ et donner un *vecteur propre* associé.

On note $\zeta := e^{\frac{2i\pi}{n}}$.

2) Rappler comment on peut donner un sens à ζ^a pour tout $a \in \mathbb{Z}/n\mathbb{Z}$.

3) Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ on définit $\beta_a \in \mathbb{C}^{\mathbf{C}_n}$ par :

$$\begin{array}{rccc} \beta_a : & \mathcal{V}(\mathbf{C}_n) & \longrightarrow & \mathbb{C} \\ & b & \longmapsto & \zeta^{ab} \ . \end{array}$$

a) Calculer $\Phi(\mathbf{C}_n)(\beta_a)$.

b) En déduire que pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ $\lambda_a := \zeta^{-a} + \zeta^a = 2\mathrm{Re}(\zeta^a)$ est une *valeur propre* de $\Phi(\mathbf{C}_n)$ et donner une base de l'*espace propre* associé.

c) Déterminer le *spectre* de $\mathbf{C}_n$ (c'est-à-dire le *spectre* de $\Phi(\mathbf{C}_n)$) et une base de *vecteurs propres* .

Exercice III.11.6.3 (Spectre des graphes bipartis) **Dans tout l'exercice III.11.6.3, on suppose que G est un *graphe fini simple non-orienté* *biparti* (cf. la définition II.6.1.2,) et on note**

$$\begin{array}{ccc} \mathcal{E}(G) & \xrightarrow{\mathcal{E}(\beta)} & \mathcal{E}(\mathbf{K}_2) \\ {\scriptstyle \varepsilon(G)}\downarrow & & \downarrow{\scriptstyle \varepsilon(\mathbf{K}_2)} \\ \mathcal{P}_{1,2}(\lceil\rfloor G] & \xrightarrow{\mathcal{P}_{1,2}(\lceil\rfloor\beta]} & \mathcal{P}_{1,2}(\lceil\rfloor \mathbf{K}_2] \end{array}$$

le *morphisme de graphes non-orientés* correspondant à la *bipartition* $\{\mathcal{V}_1, \mathcal{V}_2\}$. On note $E := \mathbb{C}^G$ et pour $k \in \{1,2\}, E_k := \{\alpha \in E\ ;\ \forall u \in \mathcal{V}_{3-k},\ \alpha(u) = 0\}$.

1) (**Somme directe**)
Montrer que

a) $E = E_1 \oplus^{\perp} E_2$,

b) il existe un *isomorphisme* (de $\mathbb{C}$-*espaces vectoriels*) $E_k \cong \mathbb{C}^{\mathcal{V}_k}$.

Soit $\Phi \in \mathrm{End}(\mathbb{C}^G)$ l'*endomorphisme d'adjacence* de G.

2) Montrer que pour $k \in \{1,2\}$ $\Phi(E_k) \subset E_{3-k}$.

On note $\sigma : E \to E$ **l'unique** ***endomorphisme*** **de** E **tel que** $\sigma_{|E_1} = -\mathrm{Id}$ **et** $\sigma_{|E_2} = \mathrm{Id}$.

3) Montrer que $\phi \circ \sigma = -\sigma \circ \Phi$.

4) Montrer que, pour tout $\lambda \in \mathbb{R}$,

a) si $\lambda \in \mathrm{Sp}(G)$, $-\lambda \in \mathrm{Sp}(G)$

b) et qu'alors λ et $-\lambda$ ont la même *multiplicité* .

On dit que G **est un** ***graphe biparti complet*** **si** G **est un** ***graphe biparti*** **et que, de plus l'implication dans ii est une équivalence *i.e.* pour tout** $\{x, y\} \in \mathcal{P}_{1,2}(G), \varepsilon(G)^{-1}\big(\{\{x, y\}\}\big) \neq \emptyset$, **si et seulement s'il existe** $k \in \{1, 2\}$ **tel que** $x \in \mathcal{V}_k$ **et** $y \in \mathcal{V}_{3-k}$.

Dans la suite de l'exercice III.11.6.3, on suppose que G **est un** ***graphe biparti complet*** **. On note** $n_k := \#(\mathcal{V}_k)_{k \in \{1,2\}}$. **Soit** $F := \{\alpha \in E \,;\, \alpha_{|\mathcal{V}_k\, k \in \{1,2\}}$ **est constante**$\}$.

5) Montrer que F est stable par Φ et σ .

6) Déterminer le *spectre* de la *restriction* $\Phi_{|F}$ de Φ à F.

7) Déterminer la *restriction* $\Phi_{|F^\perp}$ de Φ à l'orthogonal $F^\perp$ de F.

8) Déterminer $\mathrm{Sp}(G)$.

Exercice III.11.6.4 (Spectre du graphe des arêtes) Soit $G := \big(\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G)\big)$ **un** ***graphe fini simple non-orienté*** k***-régulier*** **et** L **son** ***graphe des arêtes*** **.**

On note $\mathcal{I}(G)$ **la matrice définie de la manière suivante :**

$$\begin{array}{rcl} \forall (u, e) \in \mathcal{V}(G) \times \mathcal{E}(G), \quad \mathcal{I}(G)ue & = & 1 \textbf{ si } u \in \varepsilon(G)(e) \\ & = & 0 \textbf{ sinon} . \end{array}$$

Si on note $\ell := \#\big(\mathcal{V}(G)\big)$, **c'est le nombre de lignes de** $\mathcal{I}(G)$, **et** $c := \#\big(\mathcal{E}(G)\big)$, **c'est le nombre de colonnes de** $\mathcal{I}(G)$; **si bien que** $\mathcal{I}(G) \in \mathcal{M}_{\ell,c}(\mathbb{C})$.

1) a) Donner $\mathcal{I}(G)$ pour un certain nombre *graphes* connus ; dans chacun de ces cas calculer ${}^t\mathcal{I}(G) \cdot \mathcal{I}(G)$ et $\mathcal{I}(G) \cdot {}^t\mathcal{I}(G)$.

b) Que vaut le produit scalaire de deux colonnes de $\mathcal{I}(G)$?

c) Que vaut le produit scalaire de deux lignes de $\mathcal{I}(G)$?

2) Montrer que

a) $\mathcal{I}(G) \cdot {}^t\mathcal{I}(G) = k\mathrm{Id}_\ell + \mathcal{A}(G)$;

b) ${}^t\mathcal{I}(G) \cdot \mathcal{I}(G) = 2\mathrm{Id}_c + \mathcal{A}(L)$.

c) Montrer que $\det\big(X\mathrm{Id}_c - {}^t\mathcal{I}(G)\cdot\mathcal{I}(G)\big) = X^{c-\ell}\det\big(X\mathrm{Id}_\ell - \mathcal{I}(G)\cdot{}^t\mathcal{I}(G)\big)$.

d) En déduire que $\chi_L(X) = (X+2)^{c-\ell}\chi_G(X-k+2)$.

e) Comparer $\mathrm{Sp}(L)$ et $\mathrm{Sp}(G)$.

III.11.7 . −Parcours sur les graphes finis simples non-orientés

Exercice III.11.7.1 (Itérés de la matrice d'adjacence) Les notations sont celles de ..0 et II.6.2.2.

Montrer que $\forall(u,v,\ell)\in\mathcal{V}(G)\times\mathcal{V}(G)\times\mathbb{N},\ \#\big(P_{u,v,\ell}(G)\big) = a^{(\ell)}_{u,v}(G)$.
Indication : *On pourra donner une démonstration par récurrence sur l'entier naturel* $\ell\in\mathbb{N}$.

Exercice III.11.7.2 (Parcours dans le graphe $\mathbf{K}_5$) Soit $A := \mathcal{A}(\mathbf{K}_5)$ la *matrice d'adjacence* du *graphe complet* $\mathbf{K}_5$.

1) Écrire la matrice A.

2) Montrer qu'il existe $\alpha\in\mathbb{N}$ tel que $A^2 = \alpha\mathrm{Id}_5 + A$.

3) Montrer que pour tout $\ell\in\mathbb{N}$, il existe un unique *couple* $(a_\ell,b_\ell)\in\mathbb{R}^2$ et un unique $Q\in\mathbb{R}[X]$ tels que $X^\ell = (X+1)(X-\alpha)\cdot Q + a_\ell X + b_\ell$.

4) Déterminer a_ℓ et b_ℓ en fonction de α et ℓ .

5) Calculer A^ℓ pour $\ell\in\mathbb{N}$ en fonction de A, Id_5, α et ℓ .

6) Si, pour tout $(u,\ell)\in\mathcal{V}(\mathbf{K}_5)\times\mathbb{N}$, $P_{u,u,\ell}(\mathbf{K}_5)$ est défini comme en II.6.2.2, calculer $\#\big(P_{u,u,\ell}(\mathbf{K}_5)\big)$ en fonction de α et ℓ .
Indication : *On pourra, bien entendu, utiliser le résultat de l'exercice III.11.7.1.*

7) Donner $\#\big(P_{u,u,\ell}(\mathbf{K}_5)\big)$ pour $\ell = 2,3,4$.

Exercice III.11.7.3 (Parcours dans le graphe $\mathbf{C}_6$) Dans l'exercice III.11.7.3, on suppose que $G = \mathbf{C}_6$ est le *cycle* à 6 *sommet* s que l'on peut considérer comme le *graphe* de CAYLEY associé à $\mathbb{Z}/6\mathbb{Z}$ et $\{-1,1\}$.

1) (**Parcours et graphe sommets-transitif**)

a) Montrer que, pour tout $(u,v)\in\mathcal{V}(G)\times\mathcal{V}(G)$, il existe un *automorphisme de graphes non-orientés* $\tau\in\mathrm{Aut}_{\mathbf{Gph^{N-O}}}(\mathbf{C}_6)$ tel que $\tau(u) = v$.

Définition a.1 On dit alors que $\mathbf{C}_6$ est *sommet-transitif* .

b) Pour tout $(u,v)\in\mathcal{V}(G)\times\mathcal{V}(G)$ et tout $\ell\in\mathbb{N}$, construire une bijection $P_{u,u,\ell}(G)\cong P_{v,v,\ell}(G)$.
Indication : *On pourra, bien entendu utiliser le point a .*

2) (**Spectre**)
On note $j := e^{\frac{2i\pi}{3}} \in \mathbb{C}$; **et on rappelle que** $j^3 = 1$, **et** $1 + j + j^2 = 0$. **On note encore** $\zeta := -j$.
On note $E := \mathbb{C}^{\mathcal{V}(G) = \mathbb{Z}/6\mathbb{Z}}$ **le** $\mathbb{C}$***-espace vectoriel*** **des** ***application*****s de** $\mathbb{Z}/6\mathbb{Z}$ **dans** $\mathbb{C}$; **et pour tout** $u \in \mathbb{Z}/6\mathbb{Z}$, $\beta_u \in E : \mathbb{Z}/6\mathbb{Z} \to \mathbb{C}$, $v \mapsto \zeta^{uv}$.
On note $\Phi(G) \in \mathrm{End}(E)$ **l'*endomorphisme d'adjacence*** **du** ***graphe*** G.

a) (**Vecteur propre**)
Calculer $\Phi(G)(\beta_u)$ pour tout $u \in \mathcal{V}(G)$.

b) Déterminer le *spectre* $\mathrm{Sp}(G) = \mathrm{Sp}(\Phi(G)) = \mathrm{Sp}(\mathcal{A}(G))$ de G et une base de E de *vecteurs propres* pour $\Phi(G)$.
Indication : *On pourra, bien entendu utiliser le calcul du point a .*

3) (**Parcours dans** $\mathbf{C}_6$)

a) (**Trace**)
Montrer que, pour tout $\ell \in \mathbb{N}$, $\mathrm{tr}\big(\mathcal{A}(G)^\ell\big) = (2^\ell + 2) \cdot \big(1 + (-1)^\ell\big)$; où $\mathrm{tr}\big(\mathcal{A}(G)^\ell\big) = \mathrm{tr}\big(\Phi(G)^\ell\big)$ est la trace de l'itérée $\ell^{\text{ième}}$(la puissance $\ell^{\text{ième}}$) de la *matrice d'adjacence* de G.

b) (**Parcours**)
Calculer en fonction de $\ell \in \mathbb{N}$, $\#\big(P_{u,u,\ell}(G)\big)$ pour tout $u \in \mathcal{V}(G)$.
Indication : *On pourra utiliser les résultats de l'exercice III.11.7.1, et du point b de la question 1 .*

c) (**Parcours de longueur impaire**)
Pour $(u, \ell) \in \mathcal{V}(G) \times \mathbb{N}$, quelle(s) propriété(s) de $P_{u,u,\ell}(G)$ peut-on énoncer ?