Université Paris Sud **Année 2019–2020**

L3/S6 M305 Algèbre II

Responsable Pierre Lorenzon
Bureau 2I3
IMO Bat. 307 91405 Orsay cedex
Tel. : +33 1 69 15 60 26
Courriel : lorenzon@math.u-psud.fr
http://www.math.u-psud.fr/∼lorenzon

Pour une impression papier de ce texte, adressez-vous au secrétariat du L3. Cependant il n'est pas exclu que des modifications qui seront sans doute mineures soient apportées à cette version électronique. À ce propos, toute suggestion, est la bienvenue. Signalez-moi toute erreur.

Avant-propos

On montre, au chapitre II, que les groupes abéliens sont essentiellement du genre $\mathbb{Z}^r$ ou $\mathbb{Z}/n\mathbb{Z}$ ou bien des produits de ce type d'objets. On verra, au chapitre IV, qu'une matrice à coefficients dans un corps, dans les cas les plus favorables, est semblable à une matrice composée de blocs de JORDAN :

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 & 0 & & & & & & & & & & \\ 1 & \lambda_1 & 0 & \dots & 0 & 0 & & & & & & & & & & \\ 0 & 1 & \lambda_1 & \dots & 0 & 0 & & & 0 & & & \dots & & & 0 & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & & & & & \\ 0 & 0 & 0 & \dots & 1 & \lambda_1 & & & & & & & & & & \\ & & & & & & \lambda_2 & 0 & 0 & \dots & 0 & 0 & & & & & \\ & & & & & & 1 & \lambda_2 & 0 & \dots & 0 & 0 & & & & & \\ & & 0 & & & & 0 & 1 & \lambda_2 & \dots & 0 & 0 & \dots & & 0 & & \\ & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & \\ & & & & & & 0 & 0 & 0 & \dots & 1 & \lambda_2 & & & & & \\ & & \vdots & & & & & \vdots & & & & & \vdots & & \vdots & & \\ & & & & & & & & & & & & \lambda_n & 0 & 0 & \dots & 0 & 0 \\ & & & & & & & & & & & & 1 & \lambda_n & 0 & \dots & 0 & 0 \\ & & 0 & & & & & 0 & & & & \dots & 0 & 1 & \lambda_n & \dots & 0 & 0 \\ & & & & & & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ & & & & & & & & & & & & 0 & 0 & 0 & \dots & 1 & \lambda_n \end{pmatrix}.$$

Même s'il n'est pas toujours possible d'obtenir une telle réduite de JORDAN, une matrice quelconque sera, en revanche, toujours semblable à une matrice diagonale par blocs, dont les blocs diagonaux sont des matrices compagnons :

$$\begin{pmatrix} SMCa_{1,}d_1 & & & & 0 & & \dots & & & 0 & & \\ & 0 & 0 & \dots & 0 & 0 & -a_{2,0} & & & & & \\ & 1 & 0 & \dots & 0 & 0 & -a_{2,1} & & & & & \\ 0 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & & 0 & & \\ & 0 & 0 & \dots & 1 & 0 & -a_{2,d_2-2} & & & & & \\ & 0 & 0 & \dots & 0 & 1 & -a_{2,d_2-1} & & & & & \\ \vdots & & & & \vdots & & & \vdots & & \vdots & & \\ & & & & & & & 0 & 0 & \dots & 0 & 0 & -a_{r,0} \\ & & & & & & & 1 & 0 & \dots & 0 & 0 & -a_{r,1} \\ 0 & & & & 0 & & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ & & & & & & & 0 & 0 & \dots & 1 & 0 & -a_{r,d_r-2} \\ & & & & & & & 0 & 0 & \dots & 0 & 1 & -a_{r,d_r-1} \end{pmatrix}.$$

On constate que, même si les questions paraissent, au premier abord tout du moins, assez dissemblables, dans l'un et l'autre cas, celui des groupes abéliens et celui des matrices, on cherche à « décomposer« l'objet de départ en objets élémentaires puis à assurer que deux objets possédant la même décomposition sont en fait « identiques ».

Il conviendra bien évidemment de préciser ce que sont ces « décompositions » et ce que signifie être « identique« qui peut être précisé en « isomorphe« mais ne sera tout à fait précis que lorsqu'on aura bien spécifié de quel isomorphisme on veut parler.

La ressemblance entre les deux démarches évoquées ci-dessus n'est ni fortuite ni complètement formelle. Nous verrons en effet que les résultats les plus précis qu'on peut obtenir concernant les groupes abéliens sont en fait conséquences du théorème de structure (théorème II.10.5 ;) tandis que ceux concernant les matrices proviennent du théorème de réduction de FROBENIUS (théorème IV.11.5.) On pourra alors se convaincre que ces deux résultats sont des avatars du théorème B.6.13, de structure des modules de torsion sur un anneau principal.

On pourait donc tout à fait introduire le formalisme général, à savoir celui des A-modules et faire découler les résultats qu'on veut obtenir de résultats généraux sur ces objets. Cependant on préfère laisser découvrir de telles formulations générales après avoir étudié en détail les cas particuliers ; sans compter que les preuves des résultats généraux, exposés au paragraphe B.6 par exemple, nécéssitent l'usage d'outils plus techniques que dans les cas particuliers des paragraphes II.10 et IV.11. Le formalisme des A-modules cependant développé à l'appendice A, n'est en aucun cas un prérequis à la compréhension des résultats de ce cours, mais doit davantage apparaître comme une synthèse des énoncés précédents. En particulier il est recommandé d'étudier l'appendice A après avoir compris comment les constructions données dans les paragraphes I.6 et IV.1 se formalisent dans le cadre plus général de la théorie des A-modules.

Dans cette perspective, on trouvera nombre de titres de paragraphes prenant, par exemple, la forme :

« I.1 Structures de groupe, d'anneau … (cf. A.1) »

signifiant que le paragraphe A.1 peut être lu en parallèle avec le paragraphe I.1.

De la même manière :

« Théorème II.10.5 (cf. IV.11.5, B.6.13) »

signifie que ces trois énoncés sont de même nature.

I . −Groupes, anneaux, quelques constructions

I.0 . −Introduction

Ce chapitre (I,) pourra sembler être essentiellement constitué de révisions, ce qui est d'ailleurs le cas. on recommande néanmoins de porter une attention particulière aux paragraphes I.7, I.8 et I.9 qui introduisent à un formalisme dont il est très utile de disposer dans la suite. les notions de quotients et leur propriétés universelles en particulier sont indispensables à nombre de constructions ultérieures.

on a placé ci-après (I.0.1, I.0.2) les définitions de *magma* et de leur morphismes à seule fin de pouvoir y référer librement dans la suite, sans que ces objets n'aient un véritable intérêt en eux-mêmes eu égard au peu de résultats qu'on peut obtenir avec aussi peu de structure. Bien entendu les structures algébriques qui seront étudiées en détails au long de ce cours sont celles de groupes et d'anneaux exposées dans le paragraphe I.1 et suivants.

Les notations données en I.0.3 sont autant de conventions commodes utilisées dans tout ce texte.

I.0.1 . −Magma

Définition I.0.1.1 (Loi de composition) Pour un ensemble M on appelle *loi de composition* (ou *loi de composition interne* ou *loi interne*) $*$ sur M une application

$$* \,:\, M \times M \,\to\, M\,.$$

Le couple $(M, *)$ est appelé *magma*.

Définition I.0.1.2 (Associativité) On dit qu'une loi de composition $*$ sur un ensemble M est *associative* si

$$\forall x \in M,\ \forall y \in M,\ \forall z \in M,\ ((x * y) * z \,=\, x * (y * z))\,.$$

On peut alors parler pour $(M, *)$ de *magma associatif*.

Définition I.0.1.3 (Éléments particuliers) Soit $(M, *)$ un ensemble muni d'une loi de composition associative (magma associatif)

i) (**Élément neutre**)
Un *élément neutre* pour $(M, *)$ est un élément $\epsilon \,\in\, M$ tel que

$$\forall x \in M,\ (x * \epsilon \,=\, \epsilon * x \,=\, x)\,.$$

ii) (**Symétrique**)
Si M possède un élément neutre ϵ on dit qu'un élément $x \,\in\, M$ possède un symétrique pour la loi $*$ s'il existe $y \,\in\, M$ tel que

$$x * y \,=\, y * x \,=\, \epsilon\,.$$

Remarque I.0.1.4 Dans la suite on ne considérera que des magmas associatifs dans la mesure où ce seront les seuls que nous rencontrerons. Il se peut que certains énoncés puissent être formulés sans cette hypothèse mais nous ne cherchons pas le plus grand degré de généralité possible mais une présentation que nous espérons la plus claire et la plus lisible ainsi que la moins répétitive.

Proposition I.0.1.5 (Propriétés) *Soient $(M, *)$ un magma associatif.*

i) Si ϵ et ϵ' sont des éléments neutres de $(M, *)$ alors $\epsilon \,=\, \epsilon'$.

ii) Si $(M,*)$ possède un élément neutre et si y et z éléments de M sont des symétriques pour $x \in M$, $y = z$.

Remarque I.0.1.6 On pourra donc parler de L'élément neutre d'un magma lorsqu'il en possède un et du symétrique d'un élément lorsqu'il en possède un.

Exemple I.0.1.7 Si X est un ensemble l'ensemble M des applications de X dans lui-même est un magma associatif pour la loi $\circ$ de composition des applications. Il possède un élément neutre Id_X. En revanche un élément $f : X \to X$ de M n'a pas de symétrique en général puisque f n'est pas bijective en général. La loi $\circ$ n'est en général pas commutative non plus.

Définition I.0.1.8 (Commutativité) On dit qu'une loi de composition $*$ sur un ensemble M est *commutative* si

$$\forall x \in M,\ \forall y \in M,\ (x * y = y * x)\ .$$

I.0.2 . $-$morphisme

Définition I.0.2.1 (Morphisme homomorphisme) Étant donnés deux magmas

$$(M,*) \text{ et } (N,\cdot)$$

on dit qu'une application $f : M \to N$ est un *morphisme* ou *homomorphisme* de $(M,*)$ dans $(N,\cdot)$ si

$$\forall x \in M,\ \forall y \in M,\ (f(x*y) = f(x) \cdot f(y))\ .$$

Lemme I.0.2.2 *i) Pour tout magma $(M,*)$ l'identité Id_M est un morphisme du magma M dans lui-même.*

ii) Pour $(M,*_M)$, $(N,*_N)$ et $(P,*_P)$ des magmas, $f : M \to N$ et $g : N \to P$ des morphismes, le composé $g \circ f$ est un morphisme.

Définition I.0.2.3 Étant donnés deux magmas $(M,*)$ et $(N,\cdot)$, un morphisme $f : M \to N$ est un *isomorphisme* s'il existe un morphisme $g : N \to M$ tel que

$$g \circ f = \mathrm{Id}_M \text{ et } f \circ g = \mathrm{Id}_N\ .$$

On notera $\mathrm{Isom}(M,N)$ l'ensemble des isomorphismes de $(M,*)$ dans $(N,\cdot)$.

Proposition I.0.2.4 *Étant donnés deux magmas $(M,*)$ et $(N,\cdot)$, une application $f : M \to N$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

***Preuve** : Si f est un isomorphisme, c'est par définition un morphisme qui est bijectif puisque possédant une application réciproque.*

Réciproquement si $f : M \to N$ est une application bijective, il existe une application

$$g : N \to M \text{ telle que } g \circ f = \mathrm{Id}_M \text{ et } f \circ g = \mathrm{Id}_N\ .$$

Alors :

$$\begin{array}{rcl} \forall (u,v) \in N \times N,\quad g(u \cdot v) & = & g\big[f[g(u)] \cdot f[g(v)]\big] \\ & = & g\big[f[g(u) * g(v)]\big] \\ & = & g(u) * g(v)\ . \end{array}$$

Définition I.0.2.5 Soit $(M, *)$ un magma.

i) (**Enndomorphismes**)
Un morphisme $f : M \to M$ de M dans lui-même est appelé *endomorphisme*. On note $\mathrm{End}(M)$ l'ensemble des endomorphismes de M.

ii) (**Automorphisme**)
Un morphisme $f : M \to M$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition I.0.2.4, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}(M)$ l'ensemble des automorphismes de M.

Exemple I.0.2.6 Pour un magma M, l'identité Id_M est un automorphisme de M.

Proposition I.0.2.7 *Soient $(M, *)$ un magma, E un ensemble et M^E l'ensemble des applications de E dans M. Pour tout $(f, g) \in M^E \times M^E$, on définit $f *_{M^E} g \in M^E$ de la manière suivante : Pour tout $x \in E$,*

$$f *_{M^E} g(x) := f(x) * g(x) .$$

i) $(M^E, *_{M^E})$ est un magma c'est-à-dire que $*_{M^E}$ est une loi de composition interne sur M^E.

ii) La loi $*_{M^E}$ est la seule loi sur l'ensemble M^E telle que, pour tout $x \in E$, l'application

$$M^E \to M , f \mapsto f(x)$$

soit un morphisme.

iii) Le magma $(M^E, *_{M^E})$ est associatif dès que $(M, *)$ l'est.

iv) Le magma $(M^E, *_{M^E})$ est commutatif dès que $(M, *)$ l'est.

v) Si $(M, *)$ possède un élément neutre ϵ, l'application

$$\epsilon_{M^E} : E \to M , x \mapsto \epsilon$$

est l'élément neutre de M^E.

Notation I.0.3 i) (**Triangle/carré commutatif**)
On dit que

$$\begin{array}{ccc} X & & \\ {\scriptstyle f}\downarrow & \searrow {\scriptstyle g} & \\ Y & \xrightarrow{h} & Z \end{array} \qquad \left(\text{resp.} \begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ Z & \xrightarrow{i} & T \end{array} \right)$$

est un triangle (resp ; un carré) *commutatif* si X, Y, Z et T sont des ensembles f, g, h, i des applications dont la sources et le but sont évidemment donnés par le sens des flèches et que

$$g = h \circ f \% (\text{resp. } i \circ g = h \circ f .)$$

ii) (**Diagramme commutatif**)

Un diagramme plus élaboré sera dit *commutatif* si tous les triangles et carrés le constituant le sont. Par exemple, dire que le diagramme

$$\begin{array}{ccccc} X & \xrightarrow{f} & X & & \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} & \searrow{\scriptstyle i} & \\ Z & \xrightarrow{j} & T & \xrightarrow{k} & U \end{array}$$

est commutatif signifie que

$$k \circ h = i\,,\ h \circ f = j \circ g$$

ce qui entraîne en particulier que

$$i \circ f = k \circ j \circ g\,.$$

Autrement dit encore, en termes de graphes, si deux parcours sont possibles d'un sommet à un autre, il sont équivalents au sens ou les composées des applications que l'ont trouve le long de l'un et l'autre parcours sont les mêmes.

iii) Bien entendu les ensembles en jeu peuvent bénéficier de structures supplémentaires (groupes I.1.1, anneaux I.1.6, modules A.1.1 ...) auquel cas les applications en jeu sont des morphismes (de groupes I.2.1, anneaux I.2.4, modules A.2.1 ....)

I.1 . −Structures de groupe, d'anneau ... (cf. A.1)

Définition I.1.1 (Groupe) Un *groupe* est un couple $(G, *)$ (le plus souvent simplement noté $G,$) où G est un ensemble et $* : G \times G \to G$ est une application appelée *loi de composition* vérifiant :

Gr_1) Pour tout triplet (x, y, z) d'éléments de G,

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

on dit que la loi interne $*$ est *associative*.

Gr_2) Il existe un élément $e \in G$ appelé *élément neutre* de G tel que, pour tout $x \in G$, $x * e = e * x = x$.

Gr_3) Pour tout élément $x \in G$, il existe un élément $x' \in G$ appelé *symétrique* de x et tel que $x*x' = x'*x = e$.

Il revient au même de dire que $(G, *)$ est un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique au sens des définitions du paragraphe I.0.1.

Les formulations « $(G, *)$ est un groupe » ou « $*$ munit G d'une *structure de groupe* » sont synonymes.

Exemple I.1.2 a) L'axiome I.1.1.Gr_2) entraîne qu'il n'existe aucune structure de groupe sur l'ensemble vide $\emptyset$. Un groupe est donc un ensemble possédant au moins 1 élément.

b) On peut définir une unique loi de composition qui donne à l'ensemble $\{\emptyset\}$ à un élément une structure de groupe :

$$\emptyset * \emptyset := \emptyset\,.$$

c) (**Le groupe** $\mathcal{S}(X)$)

Un des premiers groupes qu'on peut introduire, au sens où sa définition ne nécessite guère plus que les premiers axiomes de la théorie des ensembles, est le groupe $\mathcal{S}(E)$ des bijections d'un ensemble E muni de la loi $\circ$. C'est une partie du magma considéré dans l'exemple I.0.1.7, et précisément celle constituée des éléments qui ont un symétrique. Pour ne nécessiter que très peu de matériel pour être défini, ce groupe n'est cependant pas le plus aisé à étudier.

d) Si $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel, l'ensemble $\mathrm{GL}(E)$ des applications linéaires bijectives de E dans lui-même (endomorphismes) est un groupe pour la loi de composition $\circ$. Si E est de dimension finie n, une base de E étant fixée, cette dernière définit un isomorphisme de $\mathbb{K}$-espace vectoriel $E \cong \mathbb{K}^n$ qui définit lui-même un isomorphisme de $\mathrm{GL}(E)$ sur le groupe $\mathrm{GL}_n(\mathbb{K})$ des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{K}$.

Définition I.1.3 Étant donné un groupe $(G, *)$, si pour tout couple (x, y) d'éléments de G, $x * y = y * x$, on dira que G est *abélien* ou *commutatif*.

Dans ce cas on notera usuellement $+$ la loi interne et 0 l'élément neutre en référence au groupe abélien $(\mathbb{Z}, +)$.

Un groupe n'étant rien de plus (ni de moins d'ailleurs) qu'un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique, la proposition I.0.1.5 vaut encore ici mutatis mutandis.

Proposition I.1.4 (Propriétés) *Soient $(G, *)$ un grouepe.*

i) Si ϵ et ϵ' sont des éléments neutres de $(G, *)$ alors $\epsilon = \epsilon'$.

ii) Si y et z éléments de E sont des symétriques pour $x \in E$, $y = z$.

Remarque I.1.5 On pourra donc parler de L'élément neutre d'un groupe et du symétrique d'un élément dans un groupe.

L'élément neutre est souvent noté 1 et même 0 dans le cas des groupes abéliens par analogie avec le groupe $(\mathbb{Z}, +)$. Le symétrique d'un élément x est usuellement noté x^{-1} et appelé *inverse* de x, voire $-x$ dans le cas d'un groupe abélien et appelé alors *opposé* de x.

Définition I.1.6 (Anneau) Un *anneau* est un triplet $(A, +, *)$ (le plus souvent noté $A,)$ tel que :

Ann$_1$) $(A, +)$ est un groupe abélien (cf. I.1.3 ;)
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*.

Il est usuel de désigner le groupe abélien $(A, +)$ sous le terme de *groupe abélien sous-jacent* à l'anneau A.

Remarque I.1.7 On aurait pu formuler les axiomes I.1.6.Ann$_2$) et I.1.6.Ann$_3$) en disant que $(A, *)$ est un magma associatif possédant un élément neutre (cf. I.0.1.)

Définition I.1.8 (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.*

Exemple I.1.9 a) L'ensemble $\mathbb{Z}$ des entiers relatifs muni de ses opérations $+$ et $*$ est un anneau commutatif.

b) La relation $\sim_n$ de *congruence* modulo n est compatible à la multiplication *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 $*_{\mathbb{Z}/n\mathbb{Z}}$ sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes modulo n par :

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

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

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

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 $\mathcal{C}$ des fonctions continues à support compact, muni de l'addition :

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

et de la multiplication :

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

n'est pas un anneau au sens de la définition I.1.6. En effet, $\mathcal{C}$ ne possède pas d'élément neutre pour la multiplication $*$ et ne vérifie donc pas l'axiome I.1.6.Ann$_3$).

Dans la suite de ce cours, nous n'aurons pas à considérer de tels objets, ce qui nous a incité 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*.

Les propositions I.0.1.5 et I.1.4 s'étendent encore au cas des anneaux. On peut en effet remarquer qu'un anneau est un magma à la fois pour sa loi d'addition $+$ ainsi que pour sa loi de multiplication $*$ si bien que :

Proposition I.1.10 (Propriétés) *Soient $(A, +, *)$ un Anneau. Le couple $(A, +)$ est en particulier un groupe abélien si bien que :*

i) L'élément neutre 0_A pour la loi $+$ est unique.

ii) Tout élément de A possède un unique opposé pour la loi $+$.

iii) L'élément neutre 1_A pour la loi $*$ est unique.

iv) Un élément de A possède au plus un symétrique pour la loi $*$ qu'on appellera inverse.

Définition I.1.11 (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 *inversibles* pour $*$ *i.e.* ceux qui possèdent un inverse. On appelle parfois également *unité* un élément de $A^\times$.

Proposition I.1.12 *Si A est un anneau (resp. un anneau commutatif) $(A^\times, *)$ est un groupe (resp. un groupe abélien.)*

Exemple I.1.13 a) Le groupe $(\mathbb{Z}^\times, *)$ des inversibles de $\mathbb{Z}$ est $(\{-1, 1\}, *)$ qui est isomorphe au groupe abélien $\mathbb{Z}/2\mathbb{Z}$.

b) Pour un $\mathbb{K}$-espace vectoriel V l'ensemble $\mathrm{End}(V)$ des endomorphismes de V est un anneau dont le groupe des inversibles $\mathrm{End}(V)^\times$ est le *groupe linéaire* $\mathrm{GL}(V)$.

Définition I.1.14 (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 I.1.15 Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ (cf. III.2.5.i),) sont intègres.

Définition I.1.16 (Corps) Un anneau commutatif $(A, +, *)$ est un *corps* si tous les éléments de A différents de 0_A possèdent un inverse pour la loi $*$; *i.e.* $A^\times = A \setminus \{0_A\}$.

Remarque I.1.17 Un corps est un anneau intègre mais la réciproque est fausse. En effet l'anneau $(\mathbb{Z}, +, *)$ est intègre mais n'est pas un corps.

Exemple I.1.18 Les ensembles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de leurs lois usuelles sont des corps commutatifs ainsi que $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ pour p premier ; en revanche le corps des *quaternions de Hamilton* n'est pas commutatif.

I.2 . −Morphismes (cf. A.2)

Définition I.2.1 (Morphisme de groupes) Étant donnés des groupes

$$(G, *) \text{ et } (H, \cdot),$$

un *morphisme de groupes* (ou *homomorphisme de groupes*) est une application $f : G \to H$ telle que pour tout couple (x, y) d'éléments de G,

$$f(x * y) = f(x) \cdot f(y) .$$

On notera $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ (ou simplement $\mathrm{Hom}(G, H)$ si le contexte ne prête pas à confusion) l'ensemble des morphismes de G dans H. On verra également au paragraphe I.6 que la notation $\mathrm{Hom}_{\mathbb{Z}}(G, H)$ est tout à fait naturelle.

Remarque I.2.2 On constate que dans la définition ci-dessus aucune condition supplémentaire n'est exigée par rapport à un morphisme de magma (cf. I.0.2.1.)

Proposition I.2.3 (Propriétés des morphismes) *de groupes* *Étant donné un morphisme de groupe*

$$f : (G, *) \to (H, \cdot) \text{ avec } e_G(\text{resp. } e_H) \text{ l'élément neutre de } G(\text{resp. } H :)$$

i) $f(e_G) = e_H$;

ii) pour tout $x \in G$, *si* $y \in G$ *est son symétrique,* $f(y)$ *est le symétrique de* $f(x)$ *dans* H.

Définition I.2.4 (Morphisme d'anneaux) Une application

$$f : (A, +_A, *_A) \to (B, +_B, *_B)$$

est un *morphisme (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. I.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. Ann$_5$),) ainsi que pour les magma $(A, *)$ et $(B, *)$ (cf. Ann$_6$).) Néanmoins on ajoute la condition Ann$_7$) dont on verra l'importance dans la suite.

On parlera, ici encore, du *morphisme de groupe sous-jacent* à f.

Lemme I.2.5 ((cf. A.2.3)) *i) Étant donné un ensemble* X, *si* $(X, +)$ *est un groupe (resp.* $(X+, *)$ *un anneau) l'identité* Id_X *de* X *et un morphisme de groupes (resp. d'anneaux.)*

ii) Soient

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

des applications (où X, Y et Z sont des ensembles) si $(X,+)$, $(Y,+)$ et $(Z,+)$ sont des groupes, f et g des morphismes de groupes (resp. $(X,+,*)$ $(Y,+,*)$ et $(Z,+,*)$ sont des anneaux, f et g des morphismes d'anneaux,) $g \circ f$ est un morphisme de groupes (resp. d'anneaux.)

Définition I.2.6 (Isomorphisme (cf. A.2.4)) Soit $f : X \to Y$ une application (où X et Y sont des ensembles,) si $(X,+)$ et $(Y,+)$ sont des groupes (resp. $(X,+,*)$ et $(Y,+,*)$ des anneaux,) f est un *isomorphisme* de groupes (resp. d'anneaux,) s'il existe un morphisme de groupes (resp. d'anneaux,)

$$g : Y \to X \text{ tel que } g \circ f = \mathrm{Id}_X \text{ et } f \circ g = \mathrm{Id}_Y .$$

On notera

$$\mathrm{Isom}_{\mathbf{Gr}}(X,Y) \text{(resp. } \mathrm{Isom}_{\mathbf{Ann}}(X,Y) \text{) ou simplement } \mathrm{Isom}(X,Y)$$

si le contexte ne prête pas à confusion, l'ensemble des isomorphismes de groupes (resp. d'anneaux) de X dans Y.

Proposition I.2.7 (Morphisme bijectif (cf. A.2.5)) *Étant donnée une application*

$$f : X \to Y \text{ (où } X \text{ et } Y \text{ sont des ensembles,)}$$

si $(X,+)$ et $(Y,+)$ sont des groupes (resp. $(X,+,*)$ et $(Y,+,*)$ des anneaux,) f est un isomorphisme de groupes (resp. d'anneaux,) si et seulement si f est un morphisme de groupe (resp. d'anneaux,) bijectif.

***Preuve** : Si f est un isomorphisme c'est une application bijective puisque possédant une application réciproque.*

Réciproquement si f est un morphisme bijectif (de groupes (resp. d'anneaux,)) c'est en particulier un morphisme du magma $(X,+)$ dans le magma $(Y,+)$ (resp. et du magma $(X,*)$ dans le magma $(Y,*)$.) Il découle alors de la proposition I.0.2.4 qu'il existe une application réciproque

$$\begin{array}{ll} g : Y \to X \text{ telle que} & \\ \forall (u,v) \in Y \times Y, & g(u+v) = g(u) + g(v) \\ \text{(resp.} & g(u+v) = g(u) + g(v) \quad \text{et} \quad g(u*v) = g(u) * g(v) \text{ .)} \end{array}$$

Dans le cas où $f : (X,+,*) \to (Y,+,*)$ est un morphisme d'anneaux reste uniquement à vérifier que g satisfait bien à l'axiome I.2.4.Ann$_7$) à savoir $g(1_Y) = 1_X$. Or f est un morphisme d'anneaux et g son application réciproque, si bien que $f(1_X) = 1_Y$ et $g \circ f = \mathrm{Id}_X$. Il s'ensuit que

$$1_X = g(f(1_X)) = g(1_Y) .$$

Définition I.2.8 (Endomorphisme/Automorphisme (cf. A.2.6)) Étant donné

$$\text{un groupe } (X,+) \ (mathresp \text{ un anneau } (X,+,*), \ )$$

i) On appelle *endomorphisme* de X un morphisme de groupes (resp. d'anneaux) de $(X,+)$ (resp. $(X,+,*)$) dans lui-même et on note

$$\mathrm{End}_{\mathbf{Gr}}(X) \text{ (resp. .End}_{\mathbf{Ann}}(X) \text{) ou simplement } \mathrm{End}(X) \text{ si le contexte ne prête pas à confusion}$$

l'ensemble des endomorphismes de X.

ii) On appelle *automorphisme* de X un isomorphisme de groupes (resp. d'anneaux) de $(X,+)$ (resp. $(X,+,*)$) dans lui-même et on note

$$\mathrm{Aut}_{\mathbf{Gr}}(X) \text{ (resp. .}\mathrm{Aut}_{\mathbf{Ann}}(X)\text{) ou simplement } \mathrm{Aut}(X)\text{si le contexte ne prête pas à confusion}$$

l'ensemble des automorphismes de X. Un automorphisme est donc un morphisme qui est à la fois un endomorphisme et un isomorphisme. À noter qu'en vertu de la proposition I.2.7, une application $f : X \to X$ est un automorphisme de groupe (resp. d'anneau) si et seulement si c'est un endomorphisme de groupe (resp. d'anneau) bijectif.

Exemple I.2.9 a) Pour $(X,+)$ un groupe (resp. $(X,+,*)$) un anneau, Id_X est un automorphisme.

b) On a construit, pour tout $n \in \mathbb{N}$, $n > 1$, un isomorphisme de groupes

$$\mathrm{Aut}_{\mathbf{Gr}}((\mathbb{Z}/n\mathbb{Z},+)) \cong (\mathbb{Z}/n\mathbb{Z},+,*)^\times \text{ donné par : } \tau \mapsto \tau(1)\ .$$

Lemme I.2.10 *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 morphismes 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 $g^\times$.

I.3 . −Sous-groupes, sous-anneaux, idéaux (cf. A.3)

Définition I.3.1 (Sous-groupe) Une partie H d'un groupe $(G, *)$ est un *sous-groupe* si la restriction de $*$ à $H \times H$ donne à H une structure de groupe.

Exemple I.3.2 Étant donné un groupe $(G, *)$ d'élément neutre ϵ, les ensembles $\{\epsilon\}$ et G lui-même sont des sous-groupes de G.

Définition I.3.3 (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 de $(A, +)$.

Remarque I.3.4 i) Notons que l'axiome I.1.6.Ann$_1$) a en particulier pour conséquence que $(B, +)$ est un sous-groupe de $(A, +)$; ce qui entraîne, en particulier, 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 et que tout inversible dans B est inversible dans A et que son inverse dans B est encore son inverse dans A. 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

$$(x, y) +_A (z, t) := (x +_R z, y +_R t) \text{ et } (x, y) *_A (z, t) := (x *_R z, y *_R t),$$

(ce qu'on appelle la structure produit,) 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 lélément 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 la condition I.2.4.Ann$_7$) et donne sa cohérence à un énoncé comme la proposition I.3.10.c).

Définition I.3.5 (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 de $(A, +)$ tel que

$$\forall (a, x) \in A \times \mathfrak{I},\ a * x \in \mathfrak{I}\,.$$

Exemple I.3.6 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) Pour tout $a \in A$, le sous-ensemble

$$aA := \{a * b\,,\ b \in A\}$$

est 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 $d \in \mathbb{Z}$.

Définition I.3.7 (Idéal stricte/propre) Un idéal $\mathfrak{I} \subset A$, est un *idéal strict* ou un *idéal propre* si $\mathfrak{I} \neq A$.

Définition I.3.8 Un idéal $\mathfrak{p} \subset A$ est *premier* si $\mathfrak{p} \neq A$ (*i.e.* $\mathfrak{p}$ est un idéal propre) et

$$\forall (a,b) \in A \times A,\ a * b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}\ .$$

Code :

Proposition I.3.9 (Caractérisation des sous-groupes (cf. A.3.6)) *Étant donnés un groupe $(G,*)$ et $H \subset G$ une partie de G, les assertions suivantes sont équivalentes :*

a) H est un sous-groupe au sens de la définition I.3.1.

b) H est non vide et pour tout couple (x,y) d'éléments de H, $x * y^{-1} \in H$.

c) H est non vide, pour tout couple (x,y) d'éléments de H, $x * y \in H$ et pour tout $x \in H$, $x^{-1} \in H$.

d) La restriction

$$\mathrm{Id}_{G|H} : H \to G$$

de l'identité Id_G à H est un morphisme de groupes. Ceci signifie implicitement que H possède une structure de groupe.

Proposition I.3.10 (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 I.3.3.

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.

Proposition I.3.11 (Caractérisation des idéaux) *Une partie $\mathfrak{I}$ d'un anneau commutatif $(A,+,*)$ est un idéal de a si et seulement si $\mathfrak{I} \neq \emptyset$ et*

$$\forall (x,y) \in \mathfrak{I} \times \mathfrak{I},\ \forall (a,b) \in A \times A,\ a * x + b * y \in \mathfrak{I}\ .$$

Proposition I.3.12 (Le « treillis » des sous-groupes (resp. idéaux) (cf. A.3.9)) *Soit*

$$(X,+) \textit{ un groupe } (\textit{resp. } (X,+,*) \textit{ un anneau },)(\textit{resp. } (X,+,*) \textit{ un anneau commutatif }.)$$

*i) (**Intersection**)*
Pour tout ensemble $\mathcal{Y}$ de sous-groupes (resp. de sous-anneaux) (resp. d'idéaux) de X, $\bigcap_{\mathcal{Y}} Y$ est un sous-groupe (resp. un idéal de X.)

*ii) (**Réunion**)*

Pour Y et Z deux sous-groupes (resp. deux sous-anneaux) (resp. deux idéaux) de X, $Y \cup Z$ est un sous-groupe (resp. un sous-anneau) (resp. un idéal) si et seulement si

$$Y \subset Z \text{ ou } Z \subset Y .$$

*iii) (**Union filtrante**)*

Étant donnée une suite $\left(Y_n\right)_{,n\in\mathbb{N}}$ de sous-groupes (resp. de sous-anneaux) (resp. d'idéaux) de X, telle que

$$\forall (p,q) \in \mathbb{N}\times\mathbb{N},\ \exists r \in \mathbb{N},\ Y_p \subset Y_r \text{ et } Y_q \subset Y_r$$

alors $\bigcap_{n\in\mathbb{N}} Y_n$ est un sous-groupe ((resp. un sous-anneau) (resp. un idéal) de X. C'est en particulier le cas si la suite $\left(Y_n\right)_{,n\in\mathbb{N}}$, est croissante pour l'inclusion.

I.4 . −Intersection, somme, engendrement (cf. A.4)

Corollaire I.4.1 (de la proposition I.3.12 (cf. A.4.1)) *Étant donné*

$$\begin{array}{rcl} & \textit{un groupe} & (X,+), \\ (\textit{resp.} & \textit{un anneau} & (X,+,*),\ ) \\ (\textit{resp.} & \textit{un anneau commutatif} & (X,+,*),\ ) \end{array}$$

et une partie $S \subset X$*, l'ensemble* $\mathcal{Y}$

$$\begin{array}{rcl} & \textit{des sous-ghroupes de} & X, \\ (\textit{resp.} & \textit{des sous-anneaux de} & X,\ ) \\ (\textit{resp.} & \textit{des idéaux de} & X,\ ) \end{array}$$

contenant S *possède un plus petit élément*

$$(S) \ = \ \bigcap_{Y \,\in\, \mathcal{Y}} Y \ .$$

Définition I.4.2 (Sous-groupe (resp. idéal,) engendré (cf. A.4.2)) Avec les notations du corollaire I.4.1, le sous-groupe (resp. sous-anneau) (resp. idéal) (S) s'appelle le *sous-groupe engendré*, (resp. le *sous-anneau engendré*,) (resp. l'*idéal engendré*,) par S. On dit que S est une *partie génératrice* de (S).

Exemple I.4.3 ((cf. A.4.3)) a) $< \emptyset > \ = \ \{0\}$ est le groupe à un élément ; l'idéal $(\emptyset)$ est l'idéal nul $\{0\}$.

b) Pour tout sous-groupe (resp. idéal) Y, $< Y > \ = \ Y$.

c) Le groupe abélien $(\mathbb{Z}/n\mathbb{Z},+)$ est engendré par $1_{\mathbb{Z}/n} \ = \ \overline{1}$ ou par tout élément inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,*)$.

Notation I.4.4 Si $a \ \in \ A$, l'idéal $(\{a\})$ engendré par le singleton $\{a\}$, est usuellement noté aA ou (a), et l'on a :

$$(\{a\}) \ = \ (a) \ = \ aA \ = \ \{a * b \ , \ b \ \in \ A\} \ .$$

un tel idéal est dit *principal* (cf. I.12.)

Lemme I.4.5 *Étant donné un idéal* $\mathfrak{I}$ *de* A*, les assertion suivantes sont équivalentes :*

a) $\mathfrak{I} \ = \ A$;

b) $\mathfrak{I} \cap A^{\times} \ \neq \ \emptyset$;

c) $\exists u \ \in \ A^{\times}, \ \mathfrak{I} \ = \ uA$.

d) $1 \ \in \ \mathfrak{I}$;

On peut donner une description explicite du sous-groupe (resp. de l'idéal) engendré. Ce serait aussi théoriquement possible pour le sous-anneau engendré mais ne présente pas de réel intérêt, dans le cadre de ce cours au moins.

Lemme I.4.6 ((cf. A.4.4)) *Si $(X,+)$ est un groupe le sous-groupe engendré par une partie $S \subset X$ est :*

$$< S >= \left\{ r \in \mathbb{N} \, ; \, \sum_{i=1}^{r} s_i \, , \, \forall 1 \leq i \leq r, \, s_i \in S \text{ ou } s_i^{-1} \in S \right\} . \qquad \textit{I.4.6.1}$$

Si $(X,+,*)$ est un anneau commutatif l'idéal engendré par une partie $S \subset X$ est :

$$(S) = \left\{ r \in \mathbb{N} \, ; \, \sum_{i=1}^{r} a_i * s_i \, , \, \forall 1 \leq i \leq r, \, s_i \in S \text{ et } a_i \in X \right\} . \qquad \textit{I.4.6.2}$$

Lemme I.4.7 (Somme (cf. A.4.5)) *Soit $(A,+)$ un groupe abélien, (resp. $(A,+,*)$) un anneau commutatif et $\mathcal{X}$ un ensemble de sous-groupes (resp. d'idéaux) de A.*

$$(\bigcup_{X \in \mathcal{X}} X) = \left\{ r \in \mathbb{N} \, ; \, \sum_{i} 1 r s_i \, , \, \forall 1 \leq i \leq r, \, \exists X \in \mathcal{X}, \, s_i \in X \right\} . \qquad \textit{I.4.7.1}$$

Autrement dit :

$$\forall x \in A, \, x \in (\bigcup_{X \in \mathcal{X}} X) \Leftrightarrow \exists r \in \mathbb{N}, \, \forall 1 \leq i \leq r, \, \exists X_i \in \mathcal{X}, \, \exists x_i \in X_i, \, x = \sum_{i=1}^{r} x_i \, . \qquad \textit{I.4.7.2}$$

Définition I.4.8 (Somme (cf. A.4.6)) Avec les notations du lemme I.4.7 :

i) (**Somme**)
$(\bigcup_{X \in \mathcal{X}} Y)$ s'appelle la *somme* des X pour X appartenant à $\mathcal{X}$ qu'on notera $\sum_{X \in \mathcal{X}} X$.

ii) (**Somme directe**)
On dit qu'on a une *somme directe* si dans la décomposition I.4.7.2 l'entier r, les X_i et les $x_i \neq 0$, sont uniques. On notera alors

$$\bigoplus_{X \in \mathcal{X}} X := (\bigcup_{X \in \mathcal{X}}) \, .$$

iii) (**Supplémentaires**)
Pour un groupe abélien A et deux sous-groupes B et C de A, si $A = B \oplus C$, on dit que B et C sont *supplémentaires* l'un de l'autre.

iv) (**Idéaux étrangers/comaximaux**)
Pour un anneau commutatif A et des idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A, on dit que $\mathfrak{I}$ et $\mathfrak{J}$ sont *comaximaux* ou *étrangers* si $A = \mathfrak{I} + \mathfrak{J}$.

Proposition I.4.9 (Propriété universelle des sommes directes (cf. A.4.7)) *Étant donnés*

$$\text{un groupe abélien } (A,+) \text{ et } \mathcal{X} \text{ une famille de sous-groupes}$$

telle que la somme

$$\sum_{X\,\in\,\mathcal{X}} X \;=\; \bigoplus_{X\,\in\,\mathcal{X}} X$$

est directte, pour tout ensemble de morphismes

$$\{f_X \,:\, X \,\to\, B\}\,,_{X\,\in\,\mathcal{X}}\,,$$

où B est un groupe abélien, il existe un unique morphisme

$$f \,:\, \bigoplus_{X\,\in\,\mathcal{X}} X \,\to\, B \text{ tel que } \forall X \in \mathcal{X},\; f_{|X} \;=\; f_X\;.$$

Preuve *: Ce résultat est en définitive plus long à énoncer qu'à démontrer.*

Remarque I.4.10 ((cf. A.4.8)) i) Il est bien sûr immédiat de vérifier que deux sous-groupes B et C d'un groupe abélien A sont supplémentaires l'un de l'autre si et seulement si

$$A \;=\; B \,+\, C \text{ et } B \,\cap\, C \;=\; \{0\}\;.$$

ii) La définition de supplémentaire donnée en I.4.8.iii) ne doit pas pour autant laisser penser que, pour un groupe abélien A quelconque et B un sous-groupe, un suplémentaire existe toujours. On se reportera au théorème I.9.15 qui assure que l'existence d'un supplémentaire pour B équivaut à l'existence d'une section pour la surjection canonique $A \,\to\, A/B$.

I.5 . −Images directes, images réciproques, noyaux (cf. A.5)

Proposition I.5.1 (Image réciproque/directe (cf. A.5.1)) *Soient X et Y des groupes (resp. des anneaux commutatifs) et $f : X \to Y$ un morphisme de groupes (resp. d'anneaux.)*

*i) (**Image réciproque**)*
Pour tout sous-groupe $Z \subset Y$ (resp. tout idéal $Z \subset Y$,) l'image réciproque $f^{-1}(Z)$ de Z par f, est un sous-groupe (distingué si Z l'est) (resp. un idéal) de X.
En particulier le noyau $\operatorname{Ker} f = f^{-1}(\{0\})$ est un sous-groupe distingué (resp. un idéal) de X.

*ii) (**Image directe**)*
Pour tout sous-groupe (resp. sous-anneau) $Z \subset X$ de X, l'image directe $f(Z)$ de Z par f, est un sous-groupe (resp. un sous-anneau) de Y.
En particulier l'image $\operatorname{Im} f = f(X)$ de f est un sous-groupe (resp. un sous-anneau de Y.)

Code :

Définition I.5.2 (Noyau/Image (cf. A.5.2)) Étant donné un morphisme de groupes $f : G \to H$, (resp. un morphisme d'anneaux $f : A \to B$,) ϵ_H étant l'élément neutre de H, (resp. 0 l'élément neutre de B, cette notation étant plus usuelle puisque $(B, +)$ est un groupe abélien,) on appelle

i) (**Noyau**)
noyau de f le sous-ensemble

$$\operatorname{Ker} f := f^{-1}(\{\epsilon\}_H) = \{x \in G\,;\, f(x) = \epsilon_H\} \text{ (resp. } .f^{-1}\{0\}\text{)},$$

ii) (**Image**)
image de f l'ensemble

$$\operatorname{Im} f := f(G) = \{y \in H\,;\, \exists x \in G,\ ,\ y = f(x)\} \text{ (resp. } f(A)\text{)}\,.$$

Remarque I.5.3 (Noyau/Image (cf. A.5.3)) Le noyau (resp. l'image) d'un morphisme d'anneaux est encore le noyau (resp. l'image) du morphisme de groupes sous-jacent.

Proposition I.5.4 (Injectivité/surjectivité (cf. A.5.5)) *Soit*

$$f : X \to Y \text{ un morphisme de groupes (resp. d'anneaux.)}$$

i) Le morphisme f est injectif si et seulement si $\operatorname{Ker} f = \{0\}$.

ii) Le morphisme f est surjectif si et seulement si $\operatorname{Im} f = Y$.

I.6 . −Compléments sur les groupes abéliens

Proposition I.6.1 *i) Étant donnés un groupe $(G, *)$ et un ensemble E, l'ensemble G^E des applications de E dans G muni de la loi induite (cf. I.0.2.7,) est un groupe (abélien si G l'est.) C'est la seule loi sur G^E telle que pour tout $x \in E$, l'évaluation en x,*

$$G^E \to G\ ,\ f \mapsto f(x)$$

soit un morphisme de groupes.

ii) Étant donnés un anneau $(A, +, *)$ et un ensemble E, l'ensemble A^E des applications de E dans A muni des lois induites (cf. I.0.2.7,) est un anneau (commutatif si A l'est.) Ce sont les seules lois sur A^E telles que pour tout $x \in E$, l'évaluation en x,

$$A^E \to G\ ,\ f \mapsto f(x)$$

soit un morphisme d'anneaux.

Preuve *: (cf. I.14.1.question 5).)*

Proposition I.6.2 *Pour deux groupes abéliens A et B, $\mathrm{Hom}_{\mathbf{Gr}}(A, B)$ est un sous-groupe commutatif du groupe B^A considéré en I.6.1.i).*

Preuve *: (cf. TD n° I, exercice B, question 1).)*

Proposition I.6.3 *Soit $(G, +)$ un groupe abélien (cf. I.1.3.)*

i) L'ensemble $\mathrm{End}_{\mathbf{Gr}}(G) = \mathrm{Hom}_{\mathbf{Gr}}(G, G)$ est un sous-groupe du groupe G^G (cf. I.6.1.i).)

Preuve *: (cf. A.2.12.)*

ii) Le triplet $(\mathrm{End}_{\mathbf{Gr}}(G), +, \circ)$ est un anneau.

Proposition I.6.4 *Pour tout groupe $(G, *)$ et tout élément $x \in G$, il existe un unique morphisme de groupes $\epsilon_x : (\mathbb{Z}, +) \to (G, *)$ tel que $\epsilon_x(1) = x$.*

Notation I.6.5 On note usuellement $x^n := \epsilon_x(n)$ pour tout $n \in \mathbb{Z}$.
Comme $\epsilon_x(-1)$ est l'inverse de $\epsilon_x(1) = x$, on notera x^{-1} l'inverse de x dans G.
Si G est abélien et sa loi interne notée $+$, on notera $n \cdot x := \epsilon_x(n)$.
Notons qu'ici, $\cdot$ n'est pas une loi interne et que par conséquent, les propriétés qui suivent ne sont pas tautologiques et demandent une démonstration, même si cette dernière est très élémentaire :

Proposition I.6.6

Étant donné un groupe abélien $(A, +)$,

il existe une unique loi externe $\cdot : \mathbb{Z} \times A \to A$ telle que pour tout couple d'entiers relatifs (p, q) et tout couple (x, y) d'éléments de A,

$$p \cdot (x +_A y) = p \cdot x +_A p \cdot y\ . \qquad \textit{I.6.6.1}$$

$$(p +_{\mathbb{Z}} q) \cdot x = p \cdot x +_A q \cdot x\ ; \qquad \textit{I.6.6.2}$$

$$(p *_{\mathbb{Z}} q) \cdot x \;=\; p \cdot (q \cdot x)\,; \qquad \textit{I.6.6.3}$$

$$1 \cdot x \;=\; x\,; \qquad \textit{I.6.6.4}$$

Il est nécessaire de faire l'hypothèse que $(A,+)$ est abélien, pour obtenir la propriété I.6.6.1.

Preuve : *(cf. I.14.1.question 6).)*

Corollaire I.6.7 (de la proposition I.6.6) *Les propriétés énoncées dans la proposition I.6.6 ont, entre autres, pour conséquences, que pour tout $n \in \mathbb{Z}$ et tout $x \in A$,*

$$\begin{array}{rcl} n \cdot 0_A & = & 0_A \\ 0_{\mathbb{Z}} \cdot x & = & 0_A \\ (-n) \cdot x & = & -(n \cdot x) \;=\; n \cdot (-x)\,. \end{array} \qquad \textit{I.6.7.1}$$

Corollaire I.6.8 (de la proposition I.6.6) *Soit $(A,+)$ un groupe abélien.*

i) Pour tout $n \in \mathbb{Z}$, on note

$$\phi(n) \;:\; A \;\to\; A\,,\; x \;\mapsto\; n \cdot x\,.$$

On définit ainsi un morphisme d'anneaux

$$\phi \;:\; \mathbb{Z} \;\to\; \mathrm{End}_{\mathbf{Gr}}(A)\,.$$

Preuve : *La propriété I.6.6.1 assure que $\phi(n)$ est bien un morphisme de groupes i.e. un élément de $\mathrm{End}_{\mathbf{Gr}}(A)$. La propriété I.6.6.2 assure alors que ϕ est un morphisme de groupes si bien que l'axiome I.2.4.Ann$_5$) est satisfait.*

Enfin les propriétés I.6.6.3 et I.6.6.4 correspondent respectivement aux axiomes I.2.4.Ann$_6$) et I.2.4.Ann$_7$).

ii) Réciproquement si $\phi \;:\; \mathbb{Z} \;\to\; \mathrm{End}_{\mathbf{Gr}}(A)$ est un morphisme d'anneaux, la loi externe

$$\cdot \;:\; \mathbb{Z} \times A \;\to\; A\,,\; (n,x) \;\mapsto\; \phi(n)(x)$$

vérifie les propriétés I.6.6.1 à I.6.6.4.

Remarque I.6.9 L'énoncé d'unicité dans la proposition I.6.6 permettrait d'établir l'unicité d'un morphisme $\phi \;:\; \mathbb{Z} \;\to\; EndoGrA$ pour peu qu'on établisse rigoureusement (ce qui n'est en réalité pas très difficile) que les procédés I.6.8.i) et I.6.8.ii) sont inverses l'un de l'autre. Cependant un résultat d'unicité plus général est établi à la proposition I.6.11.

Proposition I.6.10 *Pour deux groupes abéliens A et B, une application $f \;:\; A \;\to\; B$ est un morphisme de groupes si et seulement si*

$$\forall (x,y) \in A \times A,\; \forall (p,q) \in \mathbb{Z} \times \mathbb{Z},\; f(p \cdot x + q \cdot y) \;=\; p \cdot f(x) + q \cdot f(y)\,.$$

Proposition I.6.11 *Pour tout anneau $(A,+,*)$ (pas nécessairement commutatif) il existe un unique morphisme d'anneau $\mathbb{Z} \;\to\; A$ appelé morphisme structural de A.*

Preuve *:*

i) ***(Existence)***
— *Puisque* $(A,+,*)$ *est un anneau* $(A,+)$ *est en particulier un groupe abélien. Il s'ensuit, en vertu de la proposition I.6.6 qu'on dispose d'une loi externe* $\cdot\ :\ \mathbb{Z}\times A\ \to\ A$*. Il s'ensuit que*

$$\phi\ :\ \mathbb{Z}\ \to\ A\ ,\ n\ \mapsto\ n\cdot 1_A$$

est une application de $\mathbb{Z}$ *dans* A*.*
— *De plus la propriété I.6.6.2 assure que*

$$\forall (p,q)\in\mathbb{Z}\times\mathbb{Z},\ \phi(p+q)\ =\ (p+q)\cdot 1_A\ =\ p\cdot 1_A\ +_A\ q\cdot 1_A\ =\ \phi(p=\ +_A\phi(q)$$

si bien que ϕ *satisfait l'axiome I.2.4.Ann*$_5$*).*
— *La propriété I.6.6.4 assure que*

$$\phi(1)\ =\ 1\cdot 1_A\ =\ 1_A$$

si bien que l'axiome I.2.4.Ann$_7$*) est satisfait.*
— *On laisse le soin au lecteur de vérifier que l'axiome I.2.4.Ann*$_6$*) est satisfait.*

ii) ***(Unicité)***
Un morphisme d'anneaux $\phi\ :\ \mathbb{Z}\ \to\ A$ *est en particulier un morphisme de groupes et vérifie* $\phi(1)\ =\ 1_A$ *ce qui le détermine complètement.*

Remarque I.6.12 On aurait pu établir a priori l'unicité du morphisme structural (cf. I.6.11) et en déduire l'unicité de la loi externe sur un groupe abélien (cf. I.6.6) grâce à la correspondance établie au corollaire I.6.8.

Remarque I.6.13 Soit $(A,+,*)$ un anneau.
— On dispose du morphisme structural $\phi\ :\ \mathbb{Z}\ \to\ A$ grâce à la proposition I.6.11.
— De plus, en vertu du corollaire I.6.8.i), puisque $(A,+)$ est un groupe abélien, on dispose d'un morphisme d'anneaux $\psi\ :\ \mathbb{Z}\ \to\ \mathrm{End}_{\mathbf{Gr}}(A)$.
— Enfin pour tout $a\ \in\ A$, lapplication

$$\mu(a)\ :\ A\ \to\ A\ ,\ x\ \mapsto\ a*x$$

est un endomorphisme du groupe $(A,+)$ (cf. I.1.6.Ann$_4$).)
Le même axiome assure que

$$\mu\ :\ A\ \to\ \mathrm{End}_{\mathbf{Gr}}(A)$$

est un morphisme de groupes. Les axiomes I.1.6.Ann$_2$) et I.1.6.Ann$_3$) assurent que μ est un morphisme d'anneaux.
— Le composé

$$\mu\circ\phi\ :\ \mathbb{Z}\ \to\ \mathrm{End}_{\mathbf{Gr}}(A)$$

est alors un morphisme d'anneau qui ne peut-être que le morphisme structural ψ de $\mathrm{End}_{\mathbf{Gr}}(A)$ en vertu de la proposition I.6.11. On a alors le diagramme commutatif de morphismes d'anneaux :

$$\begin{array}{ccc}\mathbb{Z} & \xrightarrow{\ \phi\ } & A\\ & \searrow\psi & \big\downarrow\mu\\ & & \mathrm{End}_{\mathbf{Gr}}(A)\ .\end{array}\qquad\text{I.6.13.1}$$

Remarque I.6.14 Étant donné un idéal $\mathfrak{I}$ d'un anneau A, on peut définir une loi externe

$$\cdot \,:\, A \times \mathfrak{I} \,\to\, \mathfrak{I}\,,\ (a,x) \,\mapsto\, a \cdot x \,:=\, a * x$$

sur $\mathfrak{I}$. On remarque alors que, pour tout $(x,y) \,\in\, \mathfrak{I} \,\times\, \mathfrak{I}$, et tout $(a,b) \,\in\, A \,\times\, A$,

$$a \cdot (x+y) \,=\, a \cdot x \,+\, a \cdot y\,; \tag{I.6.14.1}$$

$$(a+b) \cdot x \,=\, a \cdot x \,+\, b \cdot x\,; \tag{I.6.14.2}$$

$$(a * b) \cdot x \,=\, a \cdot (b \cdot x)\,; \tag{I.6.14.3}$$

$$1 \cdot x \,=\, x\,. \tag{I.6.14.4}$$

On avait déjà mis en évidence des propriétés très analogues à la proposition I.6.6, auxquelles on donnera un cadre général et formel avec la définition A.1.1.

On pourra alors constater qu'un idéal de A n'est, ni plus ni moins, qu'un sous-A-module de A (cf. A.3.1.)

I.7 . –Produits

La construction du *produit* est d'abord une construction ensembliste comme expliqué en I.7.0. À ce stade déjà le produit possède une *propriété universelle* I.7.0.iii) qui ne peut être formulée sans le secours des projections introduites en I.7.0.ii). Ces dernières sont, en définitives partie prenantes du produit qui n'est en réalité pas constitué du seul ensemble produit mais aussi des projections. Ce sont, comme on va le voir, les idées qui guident la construction du produit, lorsque les ensembles impliqués acquièrent davantage de structure notamment algébrique. La « bonne structure » sur le produit cartésien sera celle qui aura tendance à préserver une propriété universelle analogue pour la structure algébrique considérée. De tels énoncés ne pourront être raisonnablement formulés que si les projections deviennent des morphismes pour la structure considérée. Dès lors on s'apercevra que, pour les structures algébriques considérées au moins (groupes abéliens, anneaux, modules algèbres) cette seule exigence sur les projections suffisent à déterminer uniquement la structure sur le produit.

Proposition I.7.0 *Soient $n \in \mathbb{N}^*$, et E_k ,$1\leq k\leq n$, des ensembles.*

i) On définit par récurrence le produit cartésien des ensembles E_k ,$1\leq k\leq n$ par

$$\prod_{k=1}^{n+1} E_k := \prod_{k=1}^{n} E_k \times E_{n+1} .$$

ii) On définit également des projections

$$p_k : P := \prod_{i=1}^{n+1} E_k \to E_k \text{ ,} 1 \leq k \leq n+1$$

en supposant construites p_k ,$1\leq k\leq n$, on définit p_{n+1} par

$$p_{n+1} : (\prod_{k=1}^{n} E_k) \times E_{n+1} \to (x, y) , y \mapsto .$$

Ce qu'on peut écrire

$$p_k(x_1, \ldots, x_n) = x_k .$$

iii) Pour tout ensemble F et tout n-uplet d'applications $f_k : F \to E_k$,$1 \leq k \leq n$, il existe une unique application

$$f : F \to P := \prod_{k=1}^{n} E_k \text{ telle que } \forall 1 \leq k \leq n,\ f_k = p_k \circ f .$$

iv) Dans le cas où il existe un ensemble E tel que $\forall 1 \leq k \leq n,\ E_k = E$, on rappelle que $E^{[1;n]}$ désigne l'ensemble des applications de $[1; n]$ à valeurs dans E. Pour tout $1 \leq k \leq n$, on définit

$$q_k : E^{[1;n]} \to E , f \mapsto f(k) .$$

En vertu de iii), il existe une unique application

$$\phi : E^{[1;n]} \to \prod_{k=1}^{n} E \text{ telle que } \forall 1 \leq k \leq n,\ q_k = p_k \circ \phi .$$

L'application ϕ est alors une bijection ;

Preuve : *Pour tout* $y \in \prod_{k=1}^{n} E$, *l'application* $f : [1;n] \to E$ *définie par*

$$\forall 1 \leq k \leq n,\ f(k) := p_k(y)$$

vérifie évidemment $\phi(f) = y$ *ce qui assure que* ϕ *est surjective ;*

Pour tout $(f,g) \in E^{[1;n]} \times E^{[1;n]}$, $\phi(f) = \phi(g)$ *entraîne que pour tout* $1 \leq k \leq n$, $p_k[\phi(f)] = p_k[\phi(g)]$ *c'est-à-dire* $q_k(f) = q_k(g)$ *ou encore* $f(k) = g(k)$ *ce qui entraîne* $f = g$, *et assure donc finalement que* ϕ *est injective.*

Notation I.7.1 Dans tout le paragraphe I.7, on garde les notations de la proposition I.7.0, à savoir que, $n \in \mathbb{N}^*$ est un entier, $E_{k\ ,1\leq k\leq n}$ des ensembles dont on note

$$P := \prod_{k=1}^{n} E_k$$

le produit cartésien *i.e.*

$$P = \left\{(x_1,\ldots,x_n) \forall 1 \leq k \leq n,\ x_k \in E_k\right\}.$$

On note enfin

$$\forall 1 \leq k \leq n,\ p_k : P \to E_k\ ,\ (x_1,\ldots,x_n) \mapsto x_k$$

la *projection sur le* $k^{ième}$ *facteur*.

Pour tout $1 \leq k \leq n$, on considérera les cas où E_k est muni de l'une des structures algébriques suivantes (en sachant que la structure de magma n'est pas étudiée en soit mais comme ingrédient pour la construction des autres structures algébriques) :

0) (**magma**)
$(E_k, \dagger_k)$ est un *magma associatif* (cf. I.0.1.1 ;)

i) (**groupe**)
$(E_k, *_k)$ est un *groupe* (éventuellement abélien) (cf. I.1.1) d'élément neutre ε_k ;

ii) (**anneau**)
$(E_k, +_k, *_k, 0_k, 1_k)$ est un anneau (éventuellement commutatif) (cf. I.1.6 ;)

iii) (A-**module**)
$(E_k, +_k, \cdot_k)$ est un A-module pour A un anneau fixé, (cf. A.1.1 ;)

iv) (A-**algèbre**)
$(E_k, +_k, *_k, s_k : A \to E_k)$ est une A-algèbre (cf. A.1.6.)

Proposition I.7.2 (Existence de produits) *Si pour tout $1 \leq k \leq n$, E_k est muni de l'une des structures algébrique I.7.1.0) à I.7.1.iv) il existe une unique structure de même nature sur le produit P et telle que*

$$\forall 1 \leq k \leq n,\ p_k \ :\ P \ \to\ E_k \text{ est un morphisme}$$

pour la structure correspondante sur les $E_{k\,,1\leq k\leq n}$, (i.e. un morphisme de magmas (cf. I.0.2.1,) (resp. de groupes (cf. I.2.1,)) (resp. d'anneaux (cf. I.2.4,)) (resp. de A-modules (cf. A.2.1,)) (resp. de A-algèbres (cf. A.2.2.)))

Si $\forall 1 \leq k \leq n,$ on a une loi interne $\dagger_k$ sur E_k, la loit interne correspondante sur $\prod_{k=1}^{n} E_k$ est donnée par :

$$\begin{array}{c} \forall\big((x_1,\dots,x_n),(y_1,\dots,x_n)\big) \in P\times P, \\ (x_1,\dots,x_n)\ \dagger\ (y_1,\dots,y_n)\ =\ (x_1\dagger_1 y_1,\dots,x_n\dagger_n y_n)\,; \end{array} \qquad \text{I.7.2.1}$$

si $\forall 1 \leq k \leq n,\ \varepsilon_k$ est un élément neutre pour $\dagger_k$, alors

$$(\varepsilon_1,\dots,\varepsilon_n) \text{ est un l'élément neutre pour } \dagger\,; \qquad \text{I.7.2.2}$$

si

$$\forall 1 \leq k \leq n,\ \forall x_k \in E_k,$$

y_k est le symétrique de x_k pour $\dagger_k$,

$$(y_1,\dots,y_n) \text{ est le symétrique de } (x_1,\dots,x_n) \text{ pour } \dagger\,; \qquad \text{I.7.2.3}$$

si $\forall 1 \leq k \leq n,$ on a une loi externe $\cdot_k\ :\ A\times E_k\ \to\ E_k$, la loi externe correspondante sur $\prod_{k=1}^{n} E_k$ est donnée par :

$$\begin{array}{c} \forall (x_1,\dots,x_n)\in P,\ \forall a\in a,\ A \\ a\cdot(x_1,\dots,x_n)\ =\ (a\cdot_1 x_1,\dots,a\cdot_n x_n)\,. \end{array} \qquad \text{I.7.2.4}$$

***Preuve** :*

*0) (**Le cas des magmas**)*
Si

$$\forall 1 \leq k \leq n,\ p_k\ :\ \big(P,\dagger\big)\ \to\ (E_k,\dagger_k)$$

est un morphisme, alors :

$$\begin{array}{lll} \forall (x_1,\dots,x_n)\in P, & & \\ \forall (y_1,\dots,x_n)\in P, & p_k\big((x_1,\dots,x_n)\dagger(y_1,\dots,y_n)\big) & = \ p_k\big((x_1,\dots,x_n)\big)\dagger_k p_k\big((y_1,\dots,y_n)\big) \\ & & = \ x_k\dagger_k y_k\,, \end{array}$$

ce qui assure, d'une part l'unicité de la loi $\dagger$ et, d'autre part, au cas où elle existe, qu'elle est définie par la formule I.7.2.1. Reste à vérifier, ce qui est très élémentaire, qu'ainsi définie, elle convient bien et a les propriétés requises.

*i) (**Le cas des groupes**)*
Un groupe étant en particulier un magma associatif le point 0) assure que si

$$\forall 1 \leq k \leq n,\ (E_k, *_k) \text{ est un groupe d'élément neutre } \varepsilon_k,$$

il existe une unique loi $*$ sur P telle que

$$\forall 1 \leq k \leq n,\ \forall (x,y) \in P \times P,\ p_k(x * y) \ = \ p_k(x) *_k p_k(y)$$

i.e. les p_k sont des morphismes de groupe en particulier. Il suffit alors, ce qui est très élémentaire, de vérifier que les formules I.7.2.2 et I.7.2.3 sont satisfaites.

*ii) (**Le cas des anneaux**)*
Si

$$\forall 1 \leq k \leq n,\ (E_k, +_k, *_k, 0_k, 1_k) \text{ est un anneau,}$$

$(E_k, +_k, 0_k)$ est un groupe abélien et le point i) assure donc qu'il existe une unique structure de groupes $+$ sur P telle que

$$\forall 1 \leq k \leq n,\ p_k \ : \ P \ \to \ E_k \text{ est un morphisme de groupes } .$$

Il est en outre immédiat de vérifier, en utilisant par exemple l'expression I.7.2.1 de $+$ que cette dernière est commutative.

En appliquant le point 0) aux $(E_k, *_k)$ on conclut à l'existence et à l'unicité d'une loi $*$ sur P faisant de P un anneau et des p_k ,$1 \leq k \leq n$ des morphismes d'anneaux.

*iii) (A**-modules**)*
Si

$$\forall 1 \leq k \leq n,\ (E_k, +_k, \cdot_k) \text{ est un } A\text{-module pour un anneau } A \text{ fixé,}$$

$(E_k, +_k)$ est en particulier un groupe abélien et P hérite dès lors d'une structure de groupe en vertu du point i) telle que les p_k ,$1 \leq k \leq n$ soient des morphismes de groupes. Reste alors à vérifier la formule I.7.2.4 ce qui est sans difficulté.

*iv) (A**-algèbres**)*
Si

$$\forall 1 \leq k \leq n,\ , (E_k, +_k, *_k, s_k \ : \ A \ \to \ E_k) \text{ est une } A\text{-algèbre pour un anneau } A \text{ fixé,}$$

en particulier $(E_k, +_k, *_k)$ est un anneau et le point ii) assure qu'il existe une unique structure d'anneau $(+, *)$ sur P telle que les p_k ,$1 \leq k \leq n$ soient des morphismes.

Pour construire le morphisme structural $s \ : \ A \ \to \ P$ il faut disposer du résultat de la proposition I.7.4 pour les anneaux. En dépit du fait que celui-ci est présenté immédiatement après, aucun défaut de logique n'est cependant à déplorer.

Définition I.7.3 (Structure produit) Avec les notations I.7.1, si P est muni de l'unique structure faisant de p_k ,$1 \leq k \leq n$ des morphismes on dit que P est muni de la *structure produit*. On parlera ainsi de *groupe produit* d'*anneau produit* de *A-module produit* de *A-algèbre produit* ....

Lorsqu'on écrira $P \ = \ \prod_{k=1}^{n} E_k$ sans précision supplémentaire c'est que P sera muni de la structure produit héritée des structures des E_k.

Proposition I.7.4 (Propriété universelle du produit) *Pour tout ensemble F et tout*

$$n-\text{uplet de morphismes, } f_k \,:\, F \,\to\, E_k \text{ pour l'une des structures I.7.1.0) à I.7.1.iv)}$$

il existe un unique morphisme

$$f \,:\, F \,\to\, P \text{ tel que } \forall 1 \leq k \leq n,\ f_k \,=\, p_k \,\circ\, f\ .$$

Remarque I.7.4.1 i) Dès l'instant où l'on fait l'hypothèse que $\forall 1 \leq k \leq n,\ f_k \,:\, F \,\to\, E_k$ est un morphisme c'est qu'on suppose implicitement que F et E_k sont munis de la structure algébrique (I.7.1.0) à I.7.1.iv)) correspondante.

ii) Le résultat de cette proposition est, bien entendu, une particularisation au cas des morphismes de l'énoncé I.7.0.iii) ; ce dernier constituant d'ailleurs l'ingrédient principal de la preuve qui suit.

***Preuve* (*de la proposition I.7.4*)**: *Les $f_k\ ,1\leq k\leq n}$ étant en particulier des applications il résulte de I.7.0.iii) qu'il existe une unique application*

$$f \,:\, F \,\to\, P \text{ telle que } \forall 1 \leq k \leq n,\ f_k \,=\, p_k \,\circ\, f\ .$$

Il suffit donc de vérifier que f est un morphisme pour les structures considérées ; ce qui est tout à fait facile et laissé au lecteur.

Remarque I.7.4.1 (Le cas des A-algèbrs) On peut alors compléter le point I.7.2.iv) de la preuve de la proposition I.7.2 tout en justifiant aussi la proposition I.7.4 dans le cas des A-algèbres. Si, en effet les $E_k\ ,1\leq k\leq n}$ sont des A-algèbres ce sont des anneaux si bien que P acquiert, en vertu de I.7.2.ii) une unique structure d'anneau telle que les $p_k\ ,1\leq k\leq n}$ sont des morphismes. Les morphismes structuraux $s_k \,:\, A \,\to\, E_k$ étant, par définition, des morphismes d'anneaux, la proposition I.7.4 appliquée au cas des anneaux assure qu'il existe un unique morphisme d'anneaux

$$s \,:\, A \,\to\, P \text{ tel que } \forall 1 \leq k \leq n,\ s_k \,=\, p_k \,\circ\, s\ .$$

Si maintenant $f_k \,:\, F \,\to\, E_k$ sont des morphismes de A-algèbres ce sont en particulier des morphismes d'anneaux, et il existe donc, en vertu de la proposition I.7.4 un unique morphisme d'anneaux

$$f \,:\, F \,\to\, P \text{ tel que } \forall 1 \leq k \leq n,\ f_k \,=\, p_k \,\circ\, f\ .$$

Reste à vérifier que ce dernier morphisme est bien compatible aux morphismes structuraux

$$u \,:\, A \,\to\, F \text{ et } s \,:\, A \,\to\, P\ ;$$

cette vérification étant laissée en exercice.

Proposition I.7.5 *Dans le cas où il existe E tel que*

$$\forall 1 \leq k \leq n,\ E_k \,=\, E,\ \text{la bijection } \phi \,:\, M^{[1;n]} \,\cong\, \prod_{k=1}^{n} M$$

définie par la proposition I.7.0.iv) est un isomorphisme pour l'une des structure I.7.1.0) à à I.7.1.iv), pour peu que $E^{[1;n]}$ soit muni de la structure considérée en I.0.2.7, (resp. I.6.1.i),) (resp. I.6.1.ii),) (resp. A.1.2.d) . . . .)

Proposition I.7.6 *Supposons que* $\forall 1 \leq k \leq n$, $(E_k, +_k)$ *(resp.* $(E_k, +_k, \cdot_k)$*) est un groupe (abélien) (resp. un* A*-module.) Soit alors*

$$i_k : E_k \to P , x \mapsto (0_1, \ldots, 0_{k-1}, x, 0_{k+1}, \ldots, 0_n) ;$$

ce qui revient à dire que i_k *est caractérisée par le fait que*

$$\forall 1 \leq j \leq n,\ p_j \circ i_k \text{ est } \begin{matrix} \mathrm{Id}_{E_j} & \text{si } j = k \\ 0 & \text{sinon .} \end{matrix} .$$

i) Pour tout $1 \leq k \leq n$ i_k *est un morphisme injectif et*

$$p_k \circ i_k = \mathrm{Id}_{E_k} .$$

Preuve *: Immédiat sur la définition de* i_k*.*

ii) Le groupe (resp. A*-module,)* P *est la somme directe (cf. I.4.8.ii),) (resp. (cf. A.4.6.ii),)) des images des* i_k *:*

$$P = \bigoplus_{k=1}^{n} \mathrm{Im}\, i_k$$

qu'on écrira, dans l'a mesure où i_k *induit un isomorphisme* $E_k \cong \mathrm{Im}\, i_k$*,*

$$P = \bigoplus_{k=1}^{n} E_k .$$

Remarque I.7.7 (Attention !) Dans la proposition I.7.6, ci-dessus on a uniquement considéré le cas des groupes et des A-modules mais on n'a pas de résultat analogue pour les anneaux ou les A-algèbnres (cf. I.14.4.)

Remarque I.7.8 Si l'on considère avec attention les propriétés universelles énoncées d'une part en I.7.4 et d'autre part en I.4.9 (resp. A.4.7,) on constate qu'elles sont en fait, en un certain sens « duales » l'une de l'autre au sens où la structure de produit permet de construire des morphismes de but P tandis que la structure de somme directe permet de construire des morphisme dont la source est précisément la somme directe.

La proposition I.7.6 réconcilie les deux aspects mais il faut quand-même bien avouer que c'est un petit miracle qui ne concerne, parmi les structures que nous avons envisagées (cf. I.7.1.0)à I.7.1.iv)) que les groupes abéliens et les A-modules. Il faut notamment prêter toute l'attention qu'il mérite à l'élément neutre 0_k de E_k qui permet de construire le morphisme i_k de manière suffisamment naturelle.

I.8 . −Quotients

De même que pour le produit traité au paragraphe I.7, la question des quotients comence avec une construction ensembliste qui s'enrichit en même temps que les structures dont on peut disposer sur les ensembles considérés.

Rappel I.8.0 (sur les relations d'équivalence) On rappelle que si E est un ensemble muni d'une relation d'équivalence $\sim$, et qu'on note $E/\sim$ l'ensemble des classes d'équivalence, on dispose d'une application surjective $\pi : E \to E/\sim$ qu'on appelle *surjection canonique*. Cette dernière, pou plus exactement le couple $(E/\sim, \pi)$ a la propriété universelle suivante :

Proposition I.8.0.1 (Propriété universelle) *Pour toute application $f : E \to F$, les assertions suivantes sont équivalentes :*

a)
$$\forall (x,y) \in E \times E,\ x \sim y \Rightarrow f(x) = f(y)\ .$$

b) Il existe une unique application
$$g : E/\sim \to F \text{ tel que } g \circ \pi = f\ .$$
De plus, si f est surjective g l'est aussi et g est injective si l'implication dans a) est une équivalence.

Corollaire I.8.0.2 *En particulier si $p : E \to F$ est une application surjective et que l'on définit la relation $\sim$ sur E, par :*
$$forallset(x,y)E \times Ex \sim y \Leftrightarrow p(x) = p(y), \qquad \text{I.8.0.2.1}$$
on a un unique diagramme commutatif :
$$\begin{array}{ccc} E & & \\ {\scriptstyle\pi}\downarrow & \searrow {\scriptstyle p} & \\ E/\sim & \xrightarrow[g]{} & F \end{array} \qquad \text{I.8.0.2.2}$$
où g est bijective.

Lemme I.8.0.3 *Ceci établit une correspondance bijective entre relations déquivalences et applications surjectives qui a toute relation déquivalence associe sa surjection canonique et à toute application surjective la relation d'équivalence définie comme en I.8.0.2.1.*

Lemme I.8.0.4 *Pour toute relation d'équivalence $\sim$ sur E, l'ensemble $E/\sim$ des classes d'équivalence est une partition de E.*

Réciproquement pour toute partition P de E, la relation $\sim$ définie sur E par
$$\forall (x,y) \in E \times E,\ x \sim y \Leftrightarrow \exists A \in P,\ x \in Ay \in A$$
est une relation d'équivalence telle que
$$E/\sim \cong P\ .$$

Remarque I.8.0.5 Les lemmes I.8.0.3 et I.8.0.4 devraient donc établir une correspondance bijective entre applications surjective $p : E \to F$ et partitions de E. On peut expliciter cette correspondance en remarquant que l'ensemble des *fibres* de p

$$\{y \in F \,;\, p^{-1}(\{y\})\}$$

est une partition de E qui correspond bien à la relation d'équivalence I.8.0.2.1

Les relations d'équivalences sur E, les partitions de E ou les applications surjectives $p : E \to F$ sont donc en fait trois manières de rendre compte d'une même réalité.

Néanmoins on constatera assez rapidement que si l'on ajoute des structures sur E et notamment des structures algébriques (groupe (cf. I.1.1,) anneau (cf. I.1.6,) A-module (cf. A.1.1,)) le choix d'une relation d'équivalence ne sera pas indifférent si l'on veut que le quotient $E/\sim$ soit muni d'une structure de même nature et tant qu'à faire de manière canonique (c'est-à-dire unique,) que la surjection canonique soit alors un morphisme et qu'on ait une propriété universelle analogue à I.8.0.1 mais mettant cette fois en jeu des morphismes pour la structure considérée.

On est alors amené à donner la définition suivante :

Définition I.8.1 Étant donné un magma associatif $(M, *)$, on dit qu'une relation d'équivalence $\sim$ sur l'ensemble M est *compatible à la loi* $*$ ou simplement compatible si

$$\forall (x, y, z, t) \in M \times M \times M \times M,\ \big(x \sim z \text{ et } y \sim t\big) \Rightarrow x * y \sim z * t\,.$$

Définition I.8.2 De même si A est un anneau et M est muni dune loi externe $\cdot : A \times M \to M$, une relation d'équivalence $\sim$ sur M sera dite *compatible* à $\cdot$ si

$$\forall (a, x, y) \in A \times M \times M,\ \big(x \sim y\big) \Rightarrow a \cdot x \sim a \cdot y\,.$$

Lemme I.8.3

Soit $(X, +)$ *un groupe abélien,*
(resp. $(X, +, *)$ *un anneau commutatif,)*
(resp. $(X, +, \cdot)$ *un A-module pour A un anneau commutatif fixé.)*

Soit $\sim$ une relation d'équivalence sur X, alors les assertions suivantes sont équivalentes :

a) La relation $\sim$ est compatible avec la loi $+$ (resp. avec les lois $+$ et $*$,) (resp. avec les lois $+$ et $\cdot$.)

b) Si $\overline{0_X}$ est la classe modulo $\sim$ de l'élément neutre 0_X de $(X, +)$), $\overline{0_X}$ est un sous-groupe de $(X, +)$ (resp. un idéal de $(X, +, *)$) (resp un sous-A-module de $(X, +, \cdot)$,) et

$$\forall x \in X,\ \overline{x} = x + \overline{0_X} = \{y \in \overline{0_X} \,;\, x + y\}\,.$$

c) $\overline{0_X}$ est un sous-groupe (resp. idéal) (resp. sous-module) de X et

$$\forall (x, y) \in X \times X,\ x \sim y \Leftrightarrow x - y \in \overline{0_X}\,.$$

Preuve *:*

i) ***(a)*** $\Rightarrow$ ***b))***

Si $\sim$ *est compatible, comme* $0_X \in \overline{0_X}, \overline{0_X} \neq \emptyset$. *En outre*

$$\begin{array}{lllll} \forall (x,y) \in \overline{0_X} \times \overline{0_X}, & x \sim 0_X \text{ et } y \sim 0_X & \Rightarrow & x+y \sim 0 & \Leftrightarrow \quad x+y \in \overline{0_X} \\ & x \sim 0 \text{et } -x \sim -x & \Rightarrow & 0 = x-x \sim -x & \Leftrightarrow \quad -x \in \overline{0_X}\,; \end{array}$$

ce qui prouve que $\overline{0_X}$ *est un sous-groupe de* $(X,+)$

Par ailleurs :

$$\begin{array}{lrcl} \forall (x,y) \in X \times X, & x & \sim & y \\ \Leftrightarrow & x \sim y \quad et & & -x \sim -x \\ \Rightarrow & y-x & \sim & 0 \\ \Rightarrow & y-x & \in & \overline{0_X} \\ \Rightarrow & y & \in & x+\overline{0_X} \\ \textit{i.e.} & \overline{x} & \subset & x+\overline{0_X}\,; \\ \textit{Réciproquement} & y & \in & x+\overline{0_X} \\ \Rightarrow & x-y & \in & \overline{0_X} \\ \Rightarrow & y-x & \sim & 0_X \\ \Rightarrow & y-x \sim 0_X & \text{et} & x \sim x \\ \Rightarrow & y = y-x+x & \sim & x = 0_X + x \\ \textit{i.e.} & x+\overline{0_X} & \subset & \overline{x}\,. \end{array}$$

Si l'on suppose de plus que $(X,+,*)$ *est un anneau commutatif et que* $\sim$ *est compatible à* $*$,

$$\forall (ax) \in X \times X,\ x \in \overline{0_X} \ \Rightarrow\ x \sim 0 \ \Rightarrow\ a*x \sim 0 = a*0 \ \Rightarrow\ a*x \in \overline{0_X}$$

ce qui prouve que $\overline{0_X}$ *est un idéal de* X.

On laisse le lecteur traiter le cas d'un A*-module en utilisant par exemple la caractérisation des sous-modules donnée en A.3.6.*

ii) ***(b)*** $\Rightarrow$ ***c))***

Est presque tautologique.

iii) ***(c)*** $\Rightarrow$ ***a))***

$$\begin{array}{lrcl} \forall (x,y,z,t) \in X \times X \times X \times X, & x \sim y \quad \text{et} \quad z \sim t & & \\ \Leftrightarrow & y-x \in \overline{0_X} \quad \text{et} \quad t-z \in \overline{0_X} & & \\ \Rightarrow & y+t-(x+z) = y-x+z-t & \in & \overline{0_X} \\ \Rightarrow & x+z & \sim & y+t \end{array} \qquad 1$$

en utilisant le fait que $\overline{0_X}$ *est un sous-groupe de* $(X,+)$.

Dans le cas où c'est un idéal (si bien entendu $(X,+,*)$ *est un anneau commutatif,) il est tout aussi immédiat de montrer que*

$$x \sim y \ \Rightarrow\ a*x \sim a*y\,.$$

Enfin le cas d'un A*-module est laissé encore en exercice mais consiste en réalité formellement à remplacer* $*$ *par* $\cdot$ *dans la formule ci-dessus.*

Lemme I.8.4 *Étant donnés $(X,+)$ un groupe abélien, (resp. $(X,+,*)$ un anneau commutatif,) (resp. $(X,+,\cdot)$ un A-module pour A un anneau commutatif fixé) et Y $subset$ X un sous-groupe (resp. un idéal,) (resp. un sous-A-module,) il existe une unique relation d'équivalence $\sim$ sur X compatible à $+$, (resp. à $+$ et $*$,) (resp. à $+$ et $\cdot$,) telle que $Y = \overline{0_X}$ (où $\overline{0_X}$ est la classe de 0_X modulo $\sim$). Elle est caractérisée par le fait que*

$$\forall (x,y) \in X \times X,\ x \sim y \Leftrightarrow y - x \in \overline{0_X}\ . \qquad \textit{I.8.4.1}$$

Preuve *: Il faut remarquer que le fait que $\sim$ soit compatible à $+$ ce qui est exigé dans tous les cas entraîne que $\sim$ est nécessairement définie par la formule I.8.4.1. L'unicité est ainsi assurée et la formule I.8.4.1 définit bien une relation binaire. Le fait que Y soit un sous groupe assure que $\sim$ est bien une relation d'équivalence.*

Le fait que Y soit un idéal (resp. un sous-module) entraînera que $\sim$ est compatible à $*$ (resp. $\cdot$.)

Définition I.8.5 Si $(X,+)$ est un groupe abélien (resp. $(X,+,*)$, un anneau commutatif,) (resp. $(X,+,\cdot)$ un A-module,) on dira simplement qu'une relation d'équivalence $\sim$ sur X est *compatible* à la structur de groupe (resp. d'anneau) (resp. de A-module) ou même *compatible* (sans précision supplémentaire si le contexte est clair) si elle est compatible à la loi $+$ (resp. aux lois $+$ et $*$,) (resp. aux lois $+$ et $\cdot$.)

Les lemmes I.8.3 et I.8.4 assurent que $^\sim$ est alors la relation d'équivalence donnée par un sous-groupe (resp. un idéal,) (resp. un sous-module) Y de X et la formule I.8.4.1.

On parlera alors indifféremment de *congruence modulo* $\sim$ ou de *congruence modulo* Y et de *classes selon* $\sim$ ou de *classes selon* Y.

Remarque I.8.6 Le caractère un peu disparate de la définition ci-dessus ainsi que des constructions dans les lemmes I.8.3 et I.8.4, tiens au fait qu'on n'a pas formulé ces énoncé dans le langage des A-module.

Si en effet on considère un groupe abélien $(X,+)$ muni de sa structure naturelle de $\mathbb{Z}$-module (cf. A.1.11.i),) il est équivalent pour une relation d'équivalence $\sim$ d'être compatible à la structure de groupe où à la structure de $\mathbb{Z}$-module (la compatibilité à $\cdot$ étant une conséquence de la compatibilité à $+$.) La condition que $\overline{0_X}$ soit un sous-groupe équivaut alors à ce que ce soit un sous-$\mathbb{Z}$-module (cf. A.3.10.i).)

De même si $(X,+,*)$ est un anneau commutatif, la compatibilité d'une relation d'équivalence $\sim$ à la structure d'anneau sur X n'est autre que la compatibilité à sa structure de X-module sur lui-même (cf. A.1.2.b),) et la condition pour $\overline{0_X}$ d'être un idéal équivaut à celle d'être un sous-X-module de X (cf. A.3.2.b).)

Remarque I.8.7 Dans les énoncés I.8.3 à I.8.6, on n'a considéré que des groupes abéliens. On laisse le lecteur rappeler ses souvenirs dans le cas d'un groupe quelconque et formuler des énoncé analogue ; ce qui revient grosso modo à remplacer sous-groupe par sous-groupe distingué.

Proposition I.8.8 (existence de quotients) *Soient $(X,+)$ un groupe abélien (resp. $(X,+,*)$ un anneau commutatif,) (resp. $(X,+,\cdot)$ un A-module,.) (resp. $(X,+,*,s : A \to X)$ une A-algèbre (cf. A.1.6.)) Étant donné un sous-groupe de $(X,+)$ (resp. un idéal de $(X,+,*)$) (resp. un sous-A-module de $(X,+,\cdot)$,) (resp. un idéal de $(X,+,*,s : A \to X)$,) Y ou, de manière équivalente (cf. I.8.3,) une relation d'équivalence compatible $\sim$ sur X, il existe une unique structure de groupe (resp. d'anneau,) (resp. de A-module,) (resp. de A-algèbre,) sur l'ensemble $X/\sim$ des classes d'équivalence modulo $\sim$ (ou modulo Y) telle que la surjection canonique $\pi : X \to X/\sim$ soit un morphisme de groupes (cf. I.2.1,) (resp. d'anneaux (cf. I.2.4,)) (resp. de A-modules (cf. A.2.1,)) (resp. de A-algèbres (cf. A.2.2.))*

On a alors :

$$Y = \overline{0_X} = \operatorname{Ker} \pi\ l \qquad \textit{I.8.8.1}$$

et

$$\forall (x,y) \in X \times X,\ x \sim y \Leftrightarrow y - x \in Y\ . \qquad \textit{I.8.8.2}$$

Preuve *:*

Lemme I.8.8.1 *Si $(M, *)$ est un magma associatif, et $\sim$ une relation d'équivalence compatible,*

i) il existe une unique structure de magma sur l'ensemble quotient $M/\sim$ (ensemble des classes d'équivalence pour la relation $\sim$,) telle que la surjection canonique $\pi : M \to M/\sim$ soit un morphisme.

ii) Le magma $M/\sim$ est alors associatif (resp. commutatif) (resp. possède un élément neutre) s'il en est ainsi pour $(M, *)$.

Grâce au lemme I.8.8.1, on peut munir $X/\sim$ d'une unique structure de groupe (resp. d'anneau.) Le cas des A-modules consiste à faire des vérifications analogues à celles du lemme I.8.8.1 dans le cas d'une loi externe ce qui est tout à fait formel et laissé en exercice.

Définition I.8.9 (Structure quotient) Pour un groupe abélien $(X, +)$ (resp. un anneau commutatif $(X, +, *)$,) (resp. un A-module $(X, +, \cdot)$,) (resp. une A-algèbre $(X, +, *, s : A \to X)$,) et Y un sous-groupe (resp. un idéal) (resp. un sous-A-module,) (resp. un idéal ;) on notera X/Y l'ensemble $X/\sim$ muni de la structure de groupe (resp. d'anneau,) (resp. de A-module,) (resp. de A-algèbre,) définie par la proposition I.8.8 que l'on appellera *structure quotient*.

On appellera

$$X/Y \text{ ou même le couple } \big(X/Y, \pi : X \to X/Y\big)$$

groupe quotient (resp. *anneau quotient*,) (resp. *module quotient*) (resp. *algèbre quotient*.)

Remarque I.8.10 Dans la définition ci-dessus il s'agit en fait dans tous les cas de modules quotient, qui peuvent éventuellement disposer d'autres structures.

La proposition qui suit assure que les quotients au sens où on les a construits par la proposition I.8.8 l'on été de manière à « prolonger » la propriété universelle dont on disposait dans le cadre ensembliste (cf. I.8.0.1.) Il s'agit en quelque sorte de « remplacer » les applications par des morphismes pour la structure algébrique à laquelle on a affaire :

Proposition I.8.11 (Propriété universelle des quotients)

Soit	$(X, +)$	*un groupe abélien,*
(resp.	$(X, +, *)$	*un anneau commutatif,*)
(resp.	$(X, +, \cdot)$	*un A-module,*)
(resp.	$(X, +, *, s : A \to X)$	*une A-algèbre.*)

Pour tout morphisme $f : X \to Y$ (de groupes (cf. I.2.1,)) (d'anneaux (cf. I.2.4,)) (resp. de A-modules (cf. A.2.1,)) (resp. de A-algèbres (cf. A.2.2,)) et tout sous-groupe (resp. idéal,) (resp. sous- A-module,) (resp. idéal,) $Z \subset X$, notons

$$\forall (x, y) \in X \times X,\ x \sim y \Leftrightarrow y - x \in Z\ .$$

Alors les assertions suivantes sont équivalentes :

a)

$$\forall (x, y) \in X \times X,\ x \sim y \Rightarrow f(x) = f(y)\ ;$$

b)

$$f(Z) \;=\; \{0_Y\} \textit{ i.e. } Z \;\subset\; \operatorname{Ker} f\ .$$

c) Il existe un unique morphisme de groupes (resp. d'anneaux) (resp. de A-modules,) (resp. de A-algèbres,)

$$g \;:\; X/Z \;\to\; Y \textit{ tel que } f \;=\; g\circ\pi \;\textit{ où }\pi \;:\; X \;\to\; X/Z$$

est la surjection canonique.

De plus le morphisme g est injectif si et seulement si $Z = \operatorname{Ker} f$, ou de manière équivalente si et seulement si l'implication dans a) est une équivalence.

Le morphisme g est surjectif si et seulement si f l'est.

***Preuve** :*

*i) **(a) $\Leftrightarrow$ b))***
C'est une conséquence immédiate de la proposition I.8.3.

*ii) **(c) $\Rightarrow$ b))***
Est immédiat.

*iii) **(b) $\Rightarrow$ c))***
On est alors dans la situation de l'implication I.8.0.1.a) entraîne I.8.0.1.b) si bien qu'il

$$\textit{existe une unique application } g \;:\; X/Z \;\to\; Y \textit{ tel que } f \;=\; g\circ\pi\ .$$

Reste donc uniquement à prouver que g est un morphisme :

*$*$) **(de magmas)***

$$\begin{array}{lrcl} \forall (u,v)\in X/Z\times X/Z,\ \exists (x,y)\ \in\ X\times X, & \pi(x)=u & \text{et} & \pi(y)=v \\ \textit{ce qui entraîne que} & g(u\dagger v) & = & g[\pi(x)\dagger\pi(y)] \\ & & = & g[\pi(x\dagger y)] \\ & & = & f(x\dagger y) \\ & & = & f(x)\dagger f(y) \\ & & = & g[\pi(x)]\dagger g[\pi(y)] \\ & & = & g(u)\dagger g(v) \end{array}$$

f est π étant des morphismes.

*$\dagger$) **(de groupes)***
Cela découle immédiatement de $*$).

*$\ddagger$) **(d'anneaux)***
Cela découle immédiatement de $*$) appliqué aux lois $+$ et $*$ et au fait que

$$g(1_{X/Z}) \;=\; g[\pi(1_X)] \;=\; f(1_X) \;=\; 1_Y$$

puisque f et π sont des morphismes d'anneaux.

*§) (A-**modules**)*
D'après †), g est déjà un morphisme de groupes. De plus

$$\begin{array}{lrcl} \forall (a,u) \in A \times X/Z,\ \exists x \in X,\ u & = & \pi(x) & \\ \text{d'où} \qquad\qquad\qquad\qquad\qquad\qquad & g(a \cdot_{X/Z} u) & = & g[a \cdot_{X/Z} \pi(x)] \\ & & = & g[\pi(a \cdot_X x)] \\ & & = & f(a \cdot_X x) \\ & & = & a \cdot_Y f(x) \\ & & = & a \cdot_Y g[\pi(x)] \\ & & = & a \cdot_Y g(u) \end{array}$$

f et π étant des morphismes.

*¶) (A-**algèbres**)*
Il résulte de ‡) que g est d'ores et déjà un morphisme d'anneaux. De plus

$$g \circ s_{X/Z} = g \circ \pi \circ s_X = f \circ s_X = s_Y .$$

*iv) (**Injectivité/surjectivité**)*
Sont des questions purement ensemblistes déjà établies en I.8.0.1.

Notation I.8.12 On dit souvent, dans la situation de la proposition I.8.11, que *f se factorise à travers X/Z* ou encore à travers π.

Corollaire I.8.13 *Étant donné un morphisme surjectif de groupes, (resp. d'anneaux,) (resp. de A-modules,) (resp. de A-algèbres,) $q : X \to Y$ il existe un unique isomorphisme de groupes (resp. anneaux,) (resp. A-modules,) (resp. A-algèbres,)*

$$\phi : X/\mathrm{Ker}\, q \to Y \text{ tel que } \phi \circ \pi = q \text{ où } \pi : X \to X/\mathrm{Ker}\, q\ , \text{ est la surjection canonique.}$$

Corollaire I.8.14 (Factorisation canonique des morphismes)

Étant donné un morphisme $f : X \to Y$ de groupes (resp. d'anneaux,) (resp. de A-modules,) (resp. de A-algèbres,)

il existe un unique isomorphisme de groupes (resp. d'anneaux,) (resp. de A-modules,) (resp. de A-algèbres,)

$$\phi : X/\mathrm{Ker}\, f \cong \mathrm{Im}\, f \text{ tel que } \phi \circ \pi = f$$

où π est la surjection canonique.

Corollaire I.8.15 *Soient $(X,+)$ un groupe abélien (resp. $(X,+,\cdot)$ un A-module,) Y et Z des sous-groupes (resp. sous-A-modules de X.)*

i) Si $Z \subset Y$, la surjection canonique $\pi_Y : X \to X/Y$ se factorise à travers le quotient X/Z en un morphisme surjectif π tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} & X & \\ {\scriptstyle \pi_Z}\downarrow & \searrow {\scriptstyle \pi_Y} & \\ X/Z & \xrightarrow{\ \pi\ } & X/Y\ . \end{array}$$

ii) Si $Z \subset Y$, restriction $\pi_{Z|Y}$ à Y de la surjection canonique $\pi_Z : X \to X/Z$ se factorise en un diagramme commutatif où j et injective :

$$\begin{array}{ccc} Y & \to & Y/Z \\ {\scriptstyle \mathrm{Id}_{X|Y}}\downarrow & & \downarrow{\scriptstyle j} \\ X & \xrightarrow{\pi_Z} & X/Z\,. \end{array}$$

iii) Toujours sous l'hypothèse que $Z \subset Y$, et avec les notations du point ii), notons

$$(X/Z)/(Y/Z) := (X/Z)/\mathrm{Im}\, j \text{ et } \pi : X/Z \to (X/Z)/(Y/Z) \text{ la surjection canonique.}$$

Alors la composée $\pi \circ \pi_Z$ ce factorise à travers la surjection canonique $\pi_Y : X \to X/Y$ de sorte que le diagramme du point ii) se complète en un diagramme commutatif où ϕ est un isomorphisme :

$$\begin{array}{ccc} Y & \to & Y/Z \\ {\scriptstyle \mathrm{Id}_{X|Y}}\downarrow & & \downarrow{\scriptstyle j} \\ X & \xrightarrow{\pi_Z} & X/Z \\ {\scriptstyle \pi_Y}\downarrow & & \downarrow{\scriptstyle \pi} \\ X/Y & \xrightarrow{\phi} & (X/Z)/(Y/Z)\,. \end{array}$$

iv) En ne supposant plus nécessairement que $Z \subset Y$, la composée de la surjection canonique $Y + Z \to Z$ avec l'inclusion naturelle $Y \subset Y + Z$, se factorise à travers le quotient $Y/(Y \cap Z)$, donnant lieu au diagramme commutatif suivant où ϕ est un isomorphisme :

$$\begin{array}{ccc} Y & \to & Y + Z \\ \downarrow & & \downarrow \\ Y/(Y \cap Z) & \xrightarrow{\phi} & (Y + Z)/Z\,. \end{array}$$

Corollaire I.8.16 *Soient $(X, +)$ un groupe abélien (resp. $(X, +, *)$ un anneau commutatif,) (resp. $(X, +, \cdot)$ un A-module,) (resp. $(X, +, *, s : A \to X)$ une A-algèbre,) et $Y \subset X$ un sous-groupe (resp. un idéal,) (resp. un sous- A-module,) (resp. un idéal.)*

Soit $\pi : X \to X/Y$ la surjection canonique.

Un sous-ensemble Z de X/Y est un sous-groupe (resp. un idéal,) (resp. un sous- A-module,) (resp. un idéal,) de X/Y si et seulement si $\pi^{-1}(Z)$ est un sous-groupe (resp. un idéal,) (resp. un sous- A-module,) (resp. un idéal,) de X.

On a alors

$$Z \cong \pi^{-1}(Z)/Y\,.$$

L'application $Z \mapsto \pi^{-1}(Z)$ est alors une bijection croissante (pour la relation d'inclusion) de l'ensemble des sous-groupes (resp. idéaux,) (resp. sous- A-modules,) (resp. idéaux,) de X/Y, dans l'ensemble des sous-groupes (resp. idéaux,) (resp. sous- A-modules,) (resp. idéaux) de X contenant Y.

Remarque I.8.17 Étant donné un groupe abélien (resp. un A-module,) X. les données suivantes sont équivalentes au sens où la donnée de l'une d'entre elles permet de construire canoniquement les trois autres :

a) Un sous-groupe (resp. sous- A-module,) Y de X.

b) Un morphisme injectif $i : Y \hookrightarrow X$.

c) Une relation d'équivalence compatible sur X.

d) Un morphisme surjectif $q : X \to Z$.

Par exemple d) $\Rightarrow$ a) consiste à prendre le noyau du morphisme surjectif, tandis que a) $\Rightarrow$ d) consiste à prendre le quotient par le sous-groupe (resp. sous-A-module.)

L'équivalence a) $\Leftrightarrow$ c) a été établie dans la proposition I.8.3.

Le reste des vérifications est laissé au lecteur.

Remarque I.8.18 (Le cas des A-algèbres) Le cas des A-algèbres apparaît toujours à l'intersection des A-modules et des anneaux et il convient toujours de vérifier que lorsqu'une consttruction est possible dans les deux cadres, elle coïncide bien dans le cas des A-algèbres.

I.9 . –Suites exactes

Dans toute cette section (I.9,) A **désigne un anneau commutatif (cf. I.1.8.)**

Définition I.9.1 (Suite exacte courte) La notation

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0 \qquad \text{I.9.1.1}$$

signifie que :

Ex_1) N, X et Q sont des groupes abéliens (resp. des A-modules.)

Ex_2) i et p sont des morphismes de groupes (resp. de A-modules.)

Ex_3)

$$\mathrm{Im}\, i = \mathrm{Ker}\, p\,.$$

Ex_4) i est un morphisme injectif (*i.e.* le noyau de i est l'image du morphisme nul $\{0\} \to N$.)

Ex_5) p est un morphisme surjectif

(*i.e.* l'image de p est le noyau du morphisme nul $Q \to \{0\}$.)

On dit alors que I.9.1.1 est une *suite exacte courte de groupes abéliens* (resp. *de A-modules*.)

On dira aussi que

$$N \xrightarrow{i} X \xrightarrow{p} Q$$

est une *suite exacte* si l'on exige seulement que la condition Ex_3) soit satisfaite.

On peut encore généraliser la notion à

$$\ldots \to X_i \xrightarrow{f_i} X_{i+1} \xrightarrow{f_{i+1}} X_{i+2} \to \ldots$$

dont on dit que c'est une *suite exacte longue* si pour tout i, $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$.

Remarque I.9.2 La donnée d'une suite exacte courte de groupes abéliens (resp. de A-modules,) équivaut à l'une des données équivalentes de la remarque I.8.17.

Plus précisément si $i : N \hookrightarrow X$ est un morphisme injectif il se complète en une suite exacte courte $0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0$ en prenant $Q := X/\mathrm{Im}\, i$ et p la surjection canonique. On notera d'ailleurs souvent $X/N := X/\mathrm{Im}\, i$ puisque le morphisme injectif i induit un isomorphisme $i : N \cong \mathrm{Im}\, i$.

De même si $p : X \to Q$ est un morphisme surjectif, il se complète en une suite exacte courte $0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0$ en prenant $N := \mathrm{Ker}\, p$; Le morphisme p se factorise alors en un isomorphisme

$$X/\mathrm{Ker}\, p = X/\mathrm{Im}\, i = X/N \cong Q \text{ (cf. I.8.14 .)}$$

Remarque I.9.3 Dans le cas d'un morphisme de A-modules les notions de noyau et d'image étant celle du morphisme de groupes sous-jacent une suite est exacte au sens des A-modules si et seulement si elle l'est au sens des groupes abéliens sous-jacents. En particulier pour une suite de groupes abéliens il est équivalent d'être exacte comme suite de groupes abéliens ou comme suite de $\mathbb{Z}$-modules.

Définition I.9.4 Étant donnée une suite exacte courte de groupes abéliens (resp. A-modules,)

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0,$$

on dira que :

i) (**quotient**)
Q, ou le couple (Q, p) ou même p est un *quotient* de X ;

ii) (**Sous-module**)

N, ou le couple (N, i) ou même i est un *sous-groupe* (resp. *sous-module*,) de M. Cette dernière définition ne représentant d'ailleurs presque aucune nouveauté par rapport à celles qui ont été données dans la section I.3 (resp. A.3.)

Remarque I.9.5 Les deux notions définies ci-dessus de quotient et de sous-groupe (resp. sous- A-module,) ont « rarement » tendance à coïncider pour une paire de sous-modules donnée : si X et Y sont des groupes abéliens (resp. A-modules,) « généralement » Y n'est pas simultanément un quotient et un sous-groupe (resp. sous- A-module,) de X.

Le cadre des $\mathbb{K}$-espaces vectoriels, qui rappelons-le, sont un cas particulier de groupes abéliens (resp. A-modules,) peut induire en erreur. En effet dans ce cas la distinction entre quotient et sous-module n'est pas nécessairement facile à faire. Cela est lié, comme nous allons le voir précisément dans la suite à l'existence de supplémentaires pour un sous-espace, ou de scindage pour les suites exactes ce qui revient au même.

L'exemple suivant est néanmoins peut-être plus éclairant et il srait bon de le garder à l'esprit :

Exemple I.9.6 a) Dans la proposition I.7.6 on a donné les ingrédients permettant de construires les couples de suites exactes

$$0 \to X_1 \xrightarrow{i_1} X_1 \times X_2 \xrightarrow{p_2} X_2 \to 0 \text{ et } 0 \to X_2 \xrightarrow{i_2} X_2 \times X_1 \xrightarrow{p_1} X_1 \to 0$$

qui font manifestement apparaître les objets X_1 et X_2 simultanément comme des quotients et des sous-objets de $X_1 \times X_2$.

Cependant, on est parti de la situation d'un produit ce qui n'est pas forcément le cas général mais bel et bien celui développé dans les propositions I.9.9 et I.9.10.

b) Pour un entier $d \geq 2$, on a une suite exacte de groupes abéliens bien connue :

$$0 \to d\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \to 0$$

qui fait naturellement de $\mathbb{Z}/d\mathbb{Z}$ un quotient de $\mathbb{Z}$.

On a établi dans un ou plusieurs exercices et si on l'a oublié il serait opportun désormais de ne pas le perdre de vue, qu'il n'existe pas de morphisme de groupes injectif de $\mathbb{Z}/d\mathbb{Z}$ dans $\mathbb{Z}$. Ainsi $\mathbb{Z}/d\mathbb{Z}$ ne peut en aucun cas se réaliser comme (ous-groupe (sous-$\mathbb{Z}$-module) de $\mathbb{Z}$. Il résulte de a) ou plus exactement de la proposition I.7.6 qu'on ne peut pas écrire $\mathbb{Z} = d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$.

Définition I.9.7 (Projecteur) On dit qu'un endomorphisme p d'un groupe abélien (resp. A-module,) X est un *projecteur* si (come dans le cas de l'algèbre linéaire) $p \circ p = p$.

Lemme I.9.8 (Propriétés des projecteurs) *Soit $p : X \to X$ un projecteur (où X est un groupe abélien (resp. A-module :)*

i)

$$X = \operatorname{Ker} p \oplus \operatorname{Im} p \,;$$

ii)

$$\operatorname{Id}_X - p \text{ est un projecteur, } \operatorname{Ker} p = \operatorname{Im}(\operatorname{Id}_X - p)\,,\ \operatorname{Im} p = \operatorname{Ker} \operatorname{Id}_X - p\,.$$

Proposition I.9.9 *Soient*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0, \qquad \text{I.9.9.1}$$

une suite exacte courte de groupes abéliens (resp. A-modules,) et un morphisme

$$s : Q \to X \text{ tel que } p \circ s = \mathrm{Id}_Q . \qquad \text{I.9.9.2}$$

i) Le morphisme s est injectif.

ii)

$$X = \mathrm{Im}\, s \oplus \mathrm{Im}\,(\mathrm{Id}_X - s \circ p) \text{ et } \mathrm{Im}\,(\mathrm{Id}_X - s \circ p) = \mathrm{Ker}\, p = \mathrm{Im}\, i .$$

Preuve *: Remarquons d'abord que*

$$(s \circ p)^2 = s \circ p \circ s \circ p = s \circ p$$

si bien que $s \circ p$ est un projecteur et que l'on peut appliquer le lemme I.9.8. On a donc

$$X = \mathrm{Im}\,(s \circ p) \oplus \mathrm{Ker}\,(s \circ p) .$$

Le morphisme p étant surjectif, $\mathrm{Im}\,(s \circ p) = \mathrm{Im}\, s$. *Le morphisme s étant injectif,*

$$\mathrm{Ker}\,(s \circ p) = \mathrm{Ker}\, p = \mathrm{Im}\, i$$

puisque la suite I.9.9.1 est exacte.

iii) On peut donc noter

$$r := i^{-1} \circ (\mathrm{Id}_X - s \circ p) : X \to N$$

et l'on a

$$r \circ i = \mathrm{Id}_N :$$

En effet

$$r \circ i = i^{-1} \circ (\mathrm{Id}_X - s \circ p) \circ i = i^{-1} \circ (i - s \circ p \circ i) = i^{-1} \circ i = \mathrm{Id}_N .$$

Ce qui entraîne que r est surjectif. De plus $r \circ i$ est un projecteur et

$$(r \circ i) + (s \circ p) = \mathrm{Id}_X .$$

iv)

$$\mathrm{Im}\, s = \mathrm{Ker}\, r .$$

Preuve *: En effet,*

$$\mathrm{Ker}\, r = \mathrm{Ker}\,(i^{-1} \circ (\mathrm{Id}_- s \circ p)) = \mathrm{Ker}\,(IdM - s \circ p)$$

puisque i^{-1} est injectif. Or

$$\mathrm{Ker}\,(\mathrm{Id}_X - s \circ p) = \mathrm{Im}\,(s \circ p)$$

en vertu du lemme I.9.8. Or p étant surjectif, $\mathrm{Im}\, s \circ p = \mathrm{Im}\, s$.

v) Il résulte de ce qui précède que

$$0 \to Q \xrightarrow{s} M \xrightarrow{r} N \to 0$$

est une suite exacte courte.

Proposition I.9.10 *Soient*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0, \qquad \text{I.9.10.1}$$

une suite exacte courte de groupes abéliens (resp. A-modules,) et un morphisme

$$r : X \to N \text{ tel que } r \circ i = \mathrm{Id}_N . \qquad \text{I.9.10.2}$$

i) Le morphisme r est surjectif.

ii)

$$X = \mathrm{Im}\, i \oplus \mathrm{Im}\,(\mathrm{Id}_X - i \circ r) \text{ et } \mathrm{Im}\, i = \mathrm{Ker}\, p .$$

Preuve *: Remarquons d'abord que*

$$(i \circ r)^2 = i \circ r \circ i \circ r = i \circ r$$

si bien que $i \circ r$ est un projecteur et que l'on peut appliquer le lemme I.9.8. On a donc

$$X = \mathrm{Ker}\,(i \circ r) \oplus \mathrm{Im}\,(i \circ r) .$$

De plus $\mathrm{Ker}\,(i \circ r) = \mathrm{Im}\,(\mathrm{Id}_X - i \circ r)$. *Enfin, r étant surjectif,*

$$\mathrm{Im}\,(i \circ r) = \mathrm{Im}\, i = \mathrm{Ker}\, p$$

puisque la suite I.9.10.1 est exacte.

iii) Il en résulte que $p_{|\mathrm{Im}\,(\mathrm{Id}_X - i \circ r)}$ est un isomorphisme. On note $s : Q \to M$ son isomorphisme inverse. Il s'ensuit immédiatement que s est injectif et

$$p \circ s = \mathrm{Id}_Q .$$

De plus $s \circ p$ est un projecteur et

$$(r \circ i) + (s \circ p = \mathrm{Id}_X .$$

iv)

$$\mathrm{Im}\, s = \mathrm{Ker}\, r .$$

Preuve *: En effet, en utilisant encore le lemme I.9.8,*

$$\mathrm{Im}\, s = \mathrm{Im}\,\mathrm{Id}_X - i \circ r = \mathrm{Ker}\, i \circ r = \mathrm{Ker}\, r$$

puisque i est injectif.

v) Il résulte de ce qui précède que

$$0 \to Q \xrightarrow{s} M \xrightarrow{r} N \to 0$$

est une suite exacte courte.

Définition I.9.11 i) (**Section**)
Un morphisme $s : Q \to M$ comme en I.9.9.2 est usuellement appelée une *section* de p ou un *scindage de la suite exacte* et l'on di que la suite exacte courte I.9.9.1 est *scindée* ;

ii) (**Rétraction**)
On dit qu'un morphisme $r : M \to N$ come en I.9.10.2 est une *rétraction* de i et l'on dit que la suite exacte courte I.9.10.1 est *rétractée*.

En fait les proposition I.9.9 et I.9.10 montrent qu'une suite exacte courte de groupes abéliens (resp. A-modules,) est scindée si et seulement si elle est rétractée ;

Exemple I.9.12 a) Bien entendu les situations envisagées en I.7.6 fournissent des exemples de suites exactes courtes scindées (ou de manière équivalente rétractée.) Nous allons en fait voir à la proposition I.9.13, qu'on a là en quelque sorte une situation modèle de suites scindées ou rétractées.

b) Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie m et F un sous espace vectoriel de E de dimension $n \leq m$. notons $G := E/F$ si bien qu'on a une suite exacte

$$0 \to F \xrightarrow{i} E \xrightarrow{p} G \to 0$$

où p est la surjection canonique et i l'inclusion naturelle de F dans E (*i.e.* la restriction de l'identité Id_E à F.) Une base $(u_1, \ldots, u_n)$ de F se complète en une base $(u_1, \ldots, u_m)$ de E. C'est précisément un des points essentiels de la théorie des espaces vectoriels et qui nous fera défaut dans le cadre des groupes abéliens (resp. A-modules,) et auquel nous chercherons les meilleurs paliatifs possibles.

C'est alors un exercice facile (mais qu'ill est néanmoins bon d'avoir fait au moins une fois) que de montrer que $p(u_i)\,,_{n+1 \leq i \leq m}$ est une base de G qui se trouve donc être de dimension finie également.

On définit $s : G \to E$ comme l'unique morphisme (application linéaire) tel que

$$\forall n+1 \leq i \leq m,\ s[p(u_i)] = u_i\ .$$

Il est alors immédiat de vérifier que $p \circ s = \mathrm{Id}_G$ c'est-à-dire que s est une section de p.

La proposition suivante est une sorte de réciproque de l'exemple I.9.6.a) :

Proposition I.9.13 *Étant donnée une suite exacte courte de groupes abéliens (resp. A-modules,)*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0,$$

s'il existe

une section $s : Q \to M$ de p (cf. I.9.9.2 ,)

(resp. une rétraction $r : M \to N$ de i (cf. I.9.10.2 ,)

il existe une rétraction r de i (resp. une section s de p,) et le morphismes

$$f : M \to N \times Q\ ,\ x \mapsto \big(r(x), p(x)\big) \text{ et } g : N \times Q \to M\ ,\ (y,z) \mapsto i(y) + s(z)$$

sont des isomorphismes inverses l'un de l'autre.

Preuve : *En effet :*

$$\begin{array}{rcl} \forall x \in M, \quad g[f(x)] & = & g[r(x), p(x)] \\ & = & i[r(x)] + p[p(x)] \\ & = & x \text{ (cf. I.9.9.iii) ou I.9.10.iii))} . \end{array}$$

Réciproquement :

$$\begin{array}{rcl} \forall (y,z) \in N \times Q, \quad f[g[(y,z)]] & = & f[i(y) + s(z)] \\ & = & \big(f[i(y)], p[s(z)]\big) \\ & = & (y,z) . \end{array}$$

Remarque I.9.14 La proposition I.9.13 ci-dessus est en fait un énoncé réciproque de la proposition I.7.6. En effet, avec les notations de la proposition I.7.6, les points I.7.6.i) à I.7.6.ii) assurent que l'on a deux suites exactes scindées

$$0 \to X_1 \xrightarrow{i_1} M \xrightarrow{p_2} X_2 \to 0 \text{ et } 0 \to X_2 \xrightarrow{i_2} M \xrightarrow{p_1} X_1 \to 0 .$$

On pourrait synthétiser ces résultats dans l'énoncé suivant :

Théorème I.9.15 *Soient X et Y deux groupes abéliens (resp. A-modules,) alors les données suivantes sont équivalentes :*

a) Un morphisme injectif $i : Y \hookrightarrow X$ tel que la suite exacte

$$0 \to Y \xrightarrow{i} X \xrightarrow{p} Q \to 0$$

qui s'en déduit soit scindée/rétractée.

b) Un morphisme surjectif $p : X \to Y$ tel que la suite exacte

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Y \to 0$$

qui s'en déduit soit scindée/rétractée.

c) Un morphisme injectif $i : Y \to X$ et un sous-groupe (resp. sous- A-module,) $Z \subset X$ tel que

$$X = i(Y) \oplus Z .$$

d) Un groupe abélien (resp. A-module,) Z et un isomorphisme

$$f : Y \times Y \cong X .$$

Définition I.9.16 (Facteur direct) Dans le cas où X et Y sont des groupes abéliens (resp. A-modules,) vérifiant les conditions équivalentes du théorème I.9.15, on dit que Y est un *facteur direct* de X. Ceci signifie que Y est <u>à la fois</u> un quotient et un sous-groupe (resp. sous- A-module,) de X.

Corollaire I.9.17 *Étant donné un groupe abélien (resp. A-module,) X,*

i) si Y et Z sont des sous-groupes (resp. sous- A-modules,) de X tels que

$$X = Y \oplus Z,$$

le morphissme naturel $Y \times Z \to M$, $(x,y) \mapsto x + y$ est un isomorphisme ;

ii) Réciproquement, si Y et Z sont des groupes abéliens (resp. A-modules,) tels qu'on ait un isomorphisme

$$f \,:\, Y \times Z \,\cong\, X,$$

que lon note

$$i \,:\, Y \,\to\, X \,,\, x \,\mapsto\, f(x,0) \text{ et } j \,:\, Z \,\to\, X \,,\, x \,\mapsto\, f(0,x),$$
$$X \,=\, i(Y) \,\oplus\, j(Z)$$

qu'on abrègera, si aucune confusion n'est à craindre en

$$X \,=\, Y \,\oplus\, Z\,.$$

Proposition I.9.18 *Soient $f \,:\, X_1 \,\to\, X_2$ un morphisme de groupes abéliens (resp. A-modules,), (Y_i, Z_i) un couple de sous-groupes (resp. sous- A-modules,) de $X_{i\,,i\,=\,1 \text{ ou } 2}$, tel que*

$$X_i \,=\, Y_i \,\oplus\, Z_i \,,\, f(Y_1) \,\subset\, Y_2 \text{ et } f(Z_1) \,\subset\, Z_2\,.$$

On note alors

$$f_Y \,:=\, f_{|Y_1} \text{ (resp. } f_Y \,:=\, f_{|Z_1} \text{) la restriction de } f \text{ à } Y_1 \text{ (resp. .} Z_1 \text{ .)}$$

i)

$$\operatorname{Ker} f \,=\, \operatorname{Ker} f_Y \,\oplus\, \operatorname{Ker} f_Z\,.$$

***Preuve** : Puisque*

$$\operatorname{Ker} f_Y \,\subset\, Y_1 \text{ et } \operatorname{Ker} f_Z \,\subset\, Z_1,$$

que Z_1 et Y_1 sont en somme directe, la somme $\operatorname{Ker} f_Y \,+\, \operatorname{Ker} f_Z$ est nécessairement directe. Or pour tout $x \,\in\, X_1$, il existe un unique couple $(y,z) \,\in\, Y_1 \times Z_1$ tel que $x \,=\, y+z$. Or

$$f(x) \,=\, 0 \,\Leftrightarrow f(y+z) \,=\, 0 \,\Leftrightarrow\, f_Y(y) + f_Z(z) \,=\, 0,$$

$f_Y(y) \,\in\, Y_2$ $f_Z(z) \,\in\, Z_2$, Y_2 et Z_2 sont en somme directe si bien que

$$f_Y(y) + f_Z(z) \,=\, 0 \,\Leftrightarrow\, f_Y(y) \,=\, f_Z(z) \,=\, 0 \,\Leftrightarrow\, y \,\in\, \operatorname{Ker} f_Y \text{ et } z \,\in\, \operatorname{Ker} f_Z\,.$$

ii)

$$\operatorname{Im} f \,=\, \operatorname{Im} f_Y \,\oplus\, \operatorname{Im} f_Z\,.$$

***Preuve** : Ici encore, comme ci-dessus, la somme $\operatorname{Im} f_Y \,+\, \operatorname{Im} f_Z$ est directe ; l'inclusion $\operatorname{Im} f_Y \,+\, \operatorname{Im} f_Z \,\subset\, \operatorname{Im} f$ est immédiate.*

Pour tout $x \,\in\, \operatorname{Im} f$, il existe $u \,\in\, X_1$ tel que $x \,=\, f(u)$. Or il existe $(v,w) \,\in\, Y_1 \times Z_1$ tel que $u \,=\, v+w$ si bien que

$$x \,=\, f(u) \,=\, f(v+w) \,=\, f_Y(v) + f_Z(w) \,\in\, \operatorname{Im} f_Y \,+\, \operatorname{Im} f_Z\,.$$

Le théorème qui suit permetra notamment de donner une preuve moins technique que dans le cas général du théorème II.10.5 dans le cas des groupes abéliens et des $\mathbb{K}[X]$-modules (E, u).

Théorème I.9.19 (Principe d'EULER–POINCARÉ) *i) Si*

$$0 \to K \longrightarrow G \longrightarrow H \to 0$$

est une suite exacte courte de groupes abéliens, G est un groupe fini si et seulement si il en est de même de K et H et dans ce cas

$$\#(G) = \#(K) * \#(H) .$$

ii) Si

$$0 \to N \longrightarrow E \longrightarrow Q \to 0$$

est une suite exacte courte de $\mathbb{K}$-espaces vectoriels, E est de dimension finie si et seulement si N et Q le sont et dans ce cas

$$\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} N + \dim_{\mathbb{K}} Q .$$

I.10 . −Divisibilité et idéaux

Supposons donc dans cette section (I.10) que $(A, +, *)$ est un anneau commutatif (cf. I.1.8.)

Définition I.10.1 (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 $a * c = b$.

Lemme I.10.2

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

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

Remarque I.10.3 On sait que dans un anneau A, pour tout $a \in A$, $0 * a = 0$ .Il en résulte que pour tout $a \in A$, $a|0$.

Par ailleurs

$$\forall a \in A,\ \forall b \in A,\ \forall c \in A,\ \big(a|b \text{ et } a|c \Rightarrow a|b + c\big) .$$

Remarque I.10.4 On remarque que la notion de divisibilité « correspond » à l'inclusion sur les idéaux laquelle est une relation d'ordre partielle. La réflexivité et la transitivité ne posent aucune difficulté pour la relation de divisibilité mais il n'est pas clair qu'elle soit antisymétrique : $a|b$ et $b|a$ n'implique pas forcément que $a = b$. Même dans $\mathbb{Z}$ $5| - 5$ et $-5|5$.

On verra comment on peut affiner cette notion de manière intéressante dans le paragraphe concernant les anneaux intègres (cf. I.11.)

Définition I.10.5 (Élément premier) Un élément $a \in A$ est dit *premier* si l'idéal principal engendré par a aA est premier (cf. I.3.8 ;) ce qui équivaut à dire que $a \notin A^\times$ (cf. I.4.5,) et

$$\forall (b, c) \in A \times A,\ a|b * c \Rightarrow a|b \vee a|c .$$

Définition I.10.6 (Élément irréductible) Un élément $a \in A$ est irréductible si $a \notin A^\times$ (a n'est pas inversible) et

$$\forall (b, c) \in A \times A,\ a = b * c \Rightarrow b \in A^\times \vee c \in A^\times .$$

Remarque I.10.7 Les définitions I.10.6 et I.10.5 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 dans la proposition I.11.1 en supposant que A est intègre. Finalement dans le cas des anneaux principaux le lemme de GAUSS et son corollaire le lemme d'EUCLIDE (cf. I.13.2.6,) permettra de « presque » confondre les deux notions d'irréductibilité et de primalité et de retrouver la définition usuelle de *nombre premier*

Notation I.10.8 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

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

Proposition I.10.9 *Pour tout $X \subset A$,*

$$d \in \mathcal{D}(X) \Leftrightarrow (X) \subset dA,$$

(où (X) est l'idéal engendré par X défini en (cf. I.4.2.)

Corollaire I.10.10 *Pour tout $X \subset A$, $A^\times \subset \mathcal{D}(X)$.*

Définition I.10.11 Pour $X \subset A$, si $\mathcal{D}(X) = A^\times$ on dit que les éléments de X sont *premiers entre eux (dans leur ensemble).*

Remarque I.10.12 Cependant la situation que nous aurons souvent à considérer par la suite est celle où deux éléments x et y de A sont premiers entre eux *i.e.*où $\mathcal{D}(\{x,y\}) = A^\times$ ou vien où $X \subset A$ est constitué d'éléments *deux à deux premiers entre eux* c'est-à-dire

$$\forall (x,y) \in X \times X,\ \mathcal{D}(\{x,y\}) = A^\times .$$

Bien sûr que cette situation entraîne que les éléments de X sont premiers entre eux dans leur ensemble mais le fait que les éléments de X sont deux à deux premiers entre eux est une hypothèse plus forte. Les éléments 2, 5, 6 de $\mathbb{Z}$ sont premiers entre eux dans leur ensemble mais pas deux à deux premiers entre eux.

Définition I.10.13 (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 :

$$\forall a \in X,\ d|a \text{ et } \forall b \in \mathcal{D}(X),\ b|d \text{ (resp. } \forall a \in X,\ a|m \text{ et } \forall b \in \mathcal{M}(X),\ m|b\ .) \qquad \text{I.10.13.1}$$

Remarque I.10.14 La définition I.10.13 peut sembler un peu abusive au sens où nous n'avons parlé de *plus grand élément* ou de *plus petit élément* que pour une relation d'ordre. Nous verrons en outre que la relation $\cdot|\cdot$ n'est pas « vraiment » une relation d'ordre (cf. I.11.6,) met en particulier en défaut le fait que de tels éléments, s'ils existent, (ce que nous n'avons pas encore établi mais qui le sera pour les anneaux principaux (cf. I.13.1.3 et I.13.1.6) est unique.

Lemme I.10.15 *Étant donné une partie $X \subset A$, tous les PGCD (resp. PPCM) de X s'ils existent engendrent un même idéal (cf. I.4.4.)*

Notation I.10.16 Le lemme ci-dessus peux motiver les notations suivantes : Pour $X \subset A$ d (resp. m) un PGCD (resp. PPCM) de X, on notera :

$$\bigwedge X := dA \text{ et } \mathrm{PPCM}(X) := mA\ . \qquad \text{I.10.16.1}$$

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

$$x \wedge y := \bigwedge \{x,y\} \text{ et } \mathrm{PPCM}(x,y) = \mathrm{PPCM}(\{x,y\})\ . \qquad \text{I.10.16.2}$$

I.11 . –Éléments remarquables d'un anneau intègre

Dans cette section (I.11,) $(A, +, *)$ est un anneau commutatif intègre (cf. I.1.8, I.1.14.)

Proposition I.11.1 *Dans un anneau commutatif intègre A, tout élément premier (cf. I.10.5,) non nul est irréductible (cf. I.10.6.)*

Définition I.11.2 (Éléments associés) Pour $(a, b) \in A \times A$, on dit que b est *associé* à a s'il existe un élément inversible $u \in A^\times$, tel que $b = u * a$.

Lemme I.11.3 *La relation d'association est une relation déquivalence.*

Lemme I.11.4 *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.*

Remarque I.11.5 L'équivalence entre I.11.4.b) et I.11.4.e) peut se reformuler en disant qu'on a une bijection naturelle entre les classes d'équivalences pour la relation d'association et les idéaux principaux de A.

Remarque I.11.6 Bien qu'elle soit réflexive et transitive, la relation $|$ (divise) n'est pas « vraiment » *antisymétrique*, fait qu'on ne peut pas dire que $|$ est une relation d'ordre.

Cependant la relation d'association est une *relation d'équivalence*. On dira dans ce cas que $|$ est une relation de *pré-ordre*. Ce pré-ordre n'est pas total, en effet on ne peut pas toujours comparer deux éléments de $\mathbb{Z}$ du point de vue de la divisibilité. Par exemple, on n'a ni $3|5$ ni $5|3$.

Lemme I.11.7 *L'élément neutre pour $+$ 0 est le plus grand élément pour $|$ tandis que tout élément $u \in A^\times$ est un plus petit élément pour $|$.*

Remarque I.11.7.1 On constate d'ores et déjà que $|$ ne se comporte pas tout à fait comme une relation d'ordre puisqu'il n'y a pas unicité d'un plus petit élément.

Lemme I.11.8 *Pour tout $X \subset A$, les PGCD de X (resp. PPCM de X) forment une classe d'équivalence pour la relation d'association.*

Remarque I.11.9 On n'a pas parlé jusqu'ici du PGCD ni du PPCM mais d'un PGCD ou d'un PPCM à cause du défaut d'unicité constaté dans le lemme ci-dessus. Ce dernier énoncé montre en outre que de toute évidence, le « bon objet » à considérer n'est pas un PGCD ou un PPCM mais la classe d'association des PGCD (resp PPCM) qui, pour le coup, et d'après le lemme I.11.8 est unique. Cette classe d'association elle-même ne semble pourtant pas être un objet très utilisable sauf à remarquer qu'on peut la représenter par un objet tout à fait maniable à savoir un idéal. Grâce au lemme I.11.4 on sait en effet que tous les PGCD (resp. PPCM) engendrent le même idéal.

Le défaut majeur de ces notions, dans ce cadre trop général, est de ne pas jouir d'un résultat d'existence. Un cadre confortable pour s'y intéresser est celui des anneaux principaux (cf. I.13,) à moins qu'on introduise la notion d'anneau factoriel, ce qui ne sera pas fait dans le cadre de ce cours.

I.12 . −Anneaux principaux

Définition I.12.1 (Idéal principal) Un idéal aA pour $a \in A$ comme dans l'exemple I.3.6.b), est dit *principal*. On dit que l'idéal aA est *engendré* par a ou encore que a est un *générateur* de l'idéal aA.

Définition I.12.2 (Anneau principal) Un anneau commutatif A est *principal* s'il est intègre (cf. I.1.14,) et si tout idéal de A est principal.

Exemple I.12.3 a) Un corps est un anneau principal, puisqu'on a déjà remarqué (cf. I.3.6.a),) que ses seuls idéaux sont $\{0\}$ et lui-même qui sont évidemment principaux. Néanmoins cet exemple ne présente qu'un intérêt très limité du point de vue de l'arithmétique.

b) La proposition I.13.6.4 nous permettra de donner un certain nombre d'exemple d'anneaux principaux qui ne sont pas des corps à savoir les anneaux euclidiens :

Exemple I.12.4 D'autres exemples d'anneaux principaux sont donnés par :

a) (**L'anneau des entiers relatifs**)
l'anneau $\mathbb{Z}$. des entiers relatifs ;

b) (**Les anneaux de polynômes**)
les anneaux de polynômes $\mathbb{K}[X]$ (cf. III.4.4,) où κ est un corps ;

c) (**Les entiers de GAUSS**)
l'anneau des entiers de GAUSS ;

d) (**Les entiers d'Eisenstein**)
et l'anneau des entiers d'Eisenstein.

I.13 . −Arithmétique des anneaux principaux

I.13.1 . −Existence de PGCD et de PPCM dans les anneaux principaux

Dans la suite, c'est-à-dire dans les paragraphes I.13.1 à I.13.5 A est un anneau principal.

Lemme I.13.1.1 *Pour tout $X \subset A$, il existe $d \in A$, tel que $(X) = dA$.*

Lemme I.13.1.2 *Pour $X \subset A$, si d est un générateur de (X), i.e.si $(X) = dA$, il existe $n \in \mathbb{N}$, $a_{i\ ,1\leq i\leq n} \in A$ et $x_{i\ ,1\leq i\leq n} \in X$ tels que*

$$d = \sum_{i=1}^{n} a_i * x_i \ .$$

Proposition I.13.1.3 (PGCD) *Soit $X \subset A$ une partie de A (qui peut être finie ou non.)*

i) X admet un PGCD (cf. I.10.13 ;)

ii) $d \in A$ est un PGCD de X si et seulement si $(X) = dA$;

iii) pour tout PGCD d de X :

$$\exists n \in \mathbb{N},\ \forall 1 \leq i \leq n,\ \left(\exists x_i \in X,\ \exists a_i \in A,\ \right),\ d = \sum_{i=1}^{n} a_i * x_i \ . \qquad 1$$

Définition I.13.1.4 (Identité de BÉZOUT) La formule I.13.1.3.iii).1 est appelée *identité de* BÉZOUT et les éléments $a_{i\ ,1\leq i\leq n} \in A$ *coefficients de* BÉZOUT.

Remarque I.13.1.5 La proposition I.13.1.3 montre en particulier que, dans le cas où A est un anneau principal et $X \subset A$, les notations (X) introduite en I.4.1 et $\bigwedge X$ introduite en I.10.16.1, sont redondantes au sens où elles désignent le même objet, à savoir l'idéal engendré par X. Cependant dans le cas où A est principal, cet idéal est aussi celui engendré par n'importe quel PGCD des éléments de X.

On pourrait aussi sans grande difficulté constater que les éléments de X eux-mêmes sont bien moins déterminants que les idéaux qu'ils engendrent. En effet, si on remplace les éléments de X par des éléments qui leurs sont associés, l'idéal (X) n'est pas changé et partant l'ensemble des PGCD non plus.

Proposition I.13.1.6 (PPCM) *Pour tout $X \subset A$, X admet un PPCM et les PPCM de X sont les générateurs de l'idéal*

$$\cap(X) := \bigcap x \in XxA \ .$$

I.13.2 . −Théorème de BÉZOUT,

lemme de GAUSS,
lemme d'EUCLIDE

On insiste que dans cettte section (I.13.2) l'anneau A est principal. Certains résultats comme le lemme de GAUSS (cf. I.13.2.3,) le lemme d'EUCLIDE (cf. I.13.2.6,) pourrraient être obtenus dans un cadre plus général, à savoir celui des anneaux factoriels, mais l'hypothèse A principal est indispensable pour disposer du théorème de BÉZOUT I.13.2.1. Dans la mesure où, dans ce paragraphe les résultas qui suivent sont des corollaires de ce premier théorème, il est évident que la stratégie de démonstration devra être tout à fait différente pour les obtenir dans un autre cadre que celui des anneaux principaux.

Théorème I.13.2.1 (de BÉZOUT) *Pour tout $X \subset A$, les assertions suivantes sont équivalentes :*

a) $\mathcal{D}(X) = A^\times$ *c'est-à-dire que les éléments de X sont premiers entre eux dans leur ensemble (cf. I.10.11.)*

b)

$$(X) = \bigwedge X = A\,.$$

c) L'élément 1 *de A est un PGCD pour X.*

d) Il existe un entiers $n \in \mathbb{N}$, un n-uplet $a_{i\ ,1\leq i\leq n} \in A$, un n-uplet $x_{i\ ,1\leq i\leq n} \in X$ tels que

$$\sum_{i=1}^{n} a_i * x_i = 1\,.$$

Corollaire I.13.2.2 (Idéaux comaximau) *Deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A sont comaximaux (cf. I.4.8.iv),) si et seulement si pour tout couple $(x, y) \in A \times A$ tel que $\mathfrak{I} = xA$ et $\mathfrak{J} = yA$ x et y sont premiers entre eux.*

Théorème I.13.2.3 (Lemme de GAUSS) *Pour tout $(a, b, c) \in A \times A \times A$, si a et b sont premiers entre eux, et $a|bc$ alors $a|c$.*

Remarque I.13.2.4 Il se peut que dans la littérature, le lemme de GAUSSne soit pas habituellement déduit du théorème de BÉZOUT mais plutôt du théorème fondamental de l'arithmétique (théorème I.13.5.3.) Il pourrait alors sembler surprenant de procéder comme on l'a fait. Pour expliquer cette différence d'approche, il faudrait mentionner qu'il existe des anneaux dans lesquels le théorème I.13.5.3 est satisfait mais dans lesquels le théorème de BÉZOUT I.13.2.1 ne l'est pas. Dans de tels anneaux dits *factoriels* le lemme de GAUSSest encore vérifié mais ne peut alors se déduire du théorème de BÉZOUT. Pour donner une quelconque pertinence aux considérations qui précède il faudrait encore montrer qu'il existe vraiment des anneaux factoriels qui n'ont pas la propriété de BÉZOUT, ce qui est effectivement le cas.

Lemme I.13.2.5 *Pour tout $p \in A$ irréductible et tout $a \in A$, si p ne divise pas a, a et p sont premiers entre eux.*

Théorème I.13.2.6 (Lemme d'EUCLIDE) *Dans un anneau principal A, tout éléments irréductibles (cf. I.10.6,) est premier (cf. I.10.5.)*

Remarque I.13.2.7 Comme on a supposé dans cette section que A est intègre, tout élément premier non nul de A est irréductible (cf. I.11.1,). Le lemme d'EUCLIDE ci-dessus montre donc que les notions de premiers et d'irréductibles coïncident peu ou prou, et correspondent à l'idée que l'on a depuis longtemps des nombres premiers.

Proposition I.13.2.8 *Étant donné un anneau principal A qui n'est pas un corps, pour tout élément $p \in A$, le quotient A/pA est un corps si et seulement si p est irréductible (cf. I.10.6.)*

I.13.3 . −Arithmétique modulaire

Proposition I.13.3.1 *Étant donné un anneau principal A et $p \in A$, si p est irréductible l'anneau quotient A/Ap est un corps. La réciproque est vraie, pour peu que A ne soit pas déjà lui-même un corps.*

I.13.4 . −Le théorème chinois des restes

Notation I.13.4.1 i) Pour tout idéal I de A, on notera $\pi_I : A \to A/I$ la surjection canonique

Pour $n \in \mathbb{N}$ et $\mathcal{I} := I_k\,,_{1\leq k\leq n}$ une famille d'idéaux, on notera :

ii)
$$\forall 1 \leq k \leq n,\ p_k\ :\ \prod_j 1nA/I_j\ \to\ A/I_k$$

la projection du produit sur le $k^{\text{ième}}$ facteur (cf. I.7.1,)

iii) Il existe alors un unique morphisme d'anneaux

$$\pi_{\mathcal{I}}\ :\ A\ \to\ \prod_j 1nA/I_j$$

caractérisé par le fait que
$$\forall 1 \leq k \leq n,\ p_k\ \circ\ \pi_{\mathcal{I}}\ =\ \pi_{I_k}$$

Plus explicitement, pour tout $x \in A$,

$$\pi_{\mathcal{I}}(x)\ =\ \big(\pi_{I_1}(x), \ldots, \pi_{I_n}(x)\big)\ .$$

iv) On simplifiera autant que possible la notation π_{I_k} en π_k si aucune confusion ne peut en résulter. De même on notera simplement π au lieu de $\pi_{\mathcal{I}}$ s'il n'y a pas d'ambiguîté sur la famille d'idéaux considérée.

v) Enfin on notera
$$\psi_{\mathcal{I}} \text{ ou simplement } \psi\ :\ A\ \to\ A/\big(\bigcap_{1\,\leq\, j\,\leq\, n} A/I_j\big)$$

la surjection canonique.

On peut synthétiser ces notations dans le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{\pi_{\mathcal{I}}} & \prod_j 1nA/I_j \\ {\scriptstyle \psi_{\mathcal{I}}}\big\downarrow & \searrow \pi_{I_k} & \big\downarrow{\scriptstyle p_k} \\ A/\big(\bigcap_{1\,\leq\, j\,\leq\, n} A/I_j\big) & & A/I_k\ . \end{array} \qquad \text{I.13.4.1.1}$$

Proposition I.13.4.2 *Soient $n \in \mathbb{N}, \mathcal{I} := I_1\,,_{k\leq 1\leq n}$ un n-uplet d'idéaux de A.*

i) Il existe un unique morphisme injectif d'anneaux

$$\gamma\ :\ A/\big(\bigcap_{1\,\leq\, j\,\leq\, n} A/I_j\big)\ \to\ \prod_j 1nA/I_j\ \text{ tel que }\ \gamma\ \circ\ \psi\ =\ \pi\ .$$

ii) Si les idéaux $I_k\,,_{1\leq k\leq n}$ sont deux à deux comaximaux (cf. I.4.8.iv),) π est surjective et partant γ est surjective et donc un isomorphisme.

Remarque I.13.4.3 Une lecture attentive montrera que dans la preuve de la proposition I.13.4.2 il n'a jamais été fait usage du fait que A est un anneau principal ni d'aucun des résultats que nous avons établis pour ce type d'anneau (cf. TD n° II, exercice B.)

La particularité du cas des anneaux principaux va consister à traduire en termes de PGCD l'hypothèse que les idéaux sont deux à deux comaximaux grâce au corollaire I.13.2.2, et conduira à la forme suivante (théorème I.13.4.4,) plus usuelle, du théorème chinois des restes. Des formulations plus particulières encores dans le cas de l'anneau $\mathbb{Z}$ (resp. de l'anneau $\mathbb{K}[X]$) pourront être données .

Théorème I.13.4.4 *Soient $n \in \mathbb{N}$, a_k ,$1\leq k\leq n$ des éléments de A et m un PPcM (cf. I.13.1.6,) des a_k ,$1\leq k\leq n$.*

Pour tout $1 \leq k \leq n$ on note $\pi_k : A \to A/a_kA$ (qui correspond à la notation donnée en I.13.4.1.iv) pour peu qu'on définisse l'idéal I_k par $I_k := a_kA$. Il s'en déduit comme en I.13.4.1.iii) un morphisme d'anneaux

$$\pi : A \to \prod_{j=1}^{n} A/a_jA = \prod_{j} 1nA/I_j .$$

Notons encore $\psi : A \to A/mA$ la surjection canonique (qui n'est autre que le morphisme ψ défini en I.13.4.1.v) dans la mesure où

$$mA = \bigcap_{1 \leq j \leq n} a_jA$$

(cf. I.13.1.6.))

Alors :

i) Il existe un unique morphisme injectif d'anneaux

$$\gamma : A/mA \to \prod_{j=1}^{n} A/a_jA \text{ tel que } \gamma \circ \psi = \pi .$$

ii) Si les a_k ,$1\leq k\leq n$ sont <u>deux à deux</u> premiers entre eux (cf. I.10.11,) le morphisme π est surjectif ce qui entraîne que γ est surjectif et donc un isomorphisme.

I.13.5 . –Théorème fondamental de l'arithmétique

La preuve des résultats de cette section peut être assez appréciablement simplifiée dans le cas de $\mathbb{Z}$ ou $\mathbb{K}[X]$ en utilisant la valeur absolue ou le degré. Il peut cependant être instructif de savoir que ces énoncés sont valables dans un cadre plus général.

Lemme I.13.5.1 *Tout élément $a \in A \setminus A^\times$ possède un diviseur irréductible.*

***Preuve** : Construisons des suites (a_n) ,$n\in\mathbb{N}$ et (b_n) ,$n\in\mathbb{N}$ à valeurs dans A de la manière suivante. On pose $a_0 := a$, et $b_0 := 1$.*

— Si a_n n'est pas irréductible, il existe a_{n+1} et b_{n+1} tous deux non inversibles tels que $a_n = a_{n+1} * b_{n+1}$.

— Sinon on pose $a_{n+1} := a_n$ et $b_{n+1} := 1$.

Les suites (a_n) ,$n\in\mathbb{N}$ et (b_n) ,$n\in\mathbb{N}$ sont bien définies par récurrence.

Notons $\mathfrak{I}_n := a_nA$, l'idéal engendré par a_n. Puisque $a_{n+1}|a_n$, la suite $(\mathfrak{I}_n)$,$n\in\mathbb{N}$ est croissante. Il résulte alors de la proposition I.3.12.iii), que $\mathfrak{I} := \bigcup_{n\in\mathbb{N}} \mathfrak{I}_n$ est un idéal de A.

Puisque A est principal, il existe $c \in A$ tel que $\mathfrak{I} = cA$. Or $c \in \mathfrak{I}$, donc $c \in \bigcup_{nn\in\mathbb{N}} \mathfrak{I}_n$; donc il existe $p \in \mathbb{N}$ tel que $c \in \mathfrak{I}_p$. Il en résulte que $\mathfrak{I} \subset \mathfrak{I}_p$. Comme $\mathfrak{I}_p \subset \mathfrak{I}$ par construction, $\mathfrak{I} = \mathfrak{I}_p$. Comme

$$\forall q \in \mathbb{N},\ q \geq p \ \Rightarrow\ \mathfrak{I}_p \subset \mathfrak{I}_q,$$

On a

$$\mathfrak{I}_p \subset \mathfrak{I}_q \subset \mathfrak{I} = \mathfrak{I}_p$$

si bien que

$$\forall q \in \mathbb{N},\ q \geq p \ \Rightarrow\ \mathfrak{I}_q = \mathfrak{I}_p\ .$$

En particulier $\mathfrak{I}_{p+1} = \mathfrak{I}_p$. Ceci entraîne que $a_{p+1} \in \mathfrak{I}_p$ i.e. $a_p | a_{P+1}$. Comme, par hypothèse, $a_{p+1} | a_p$, a_{p+1} et a_p sont associés. Il existe donc $u \in A^\times$ tel que $a_{p+1} * u = a_p$. Par construction on a $a_p = a_{p+1} * b_{p+1}$, il en résulte que $b_{p+1} = u$. Ceci entraîne par construction des suites $\left(a_n\right)_{,n\in\mathbb{N}}$ et $\left(b_n\right)_{,n\in\mathbb{N}}$, que a_p est irréductible. Or $a_p | a$, si bien qu'on a mis en évidence un diviseur irréductible de a.

Remarque I.13.5.2 En considérant attentivement la preuve du lemme I.13.5.1, on constate qu'on a montré que dans un anneau principal toute suite croissante d'idéaux est stationnaire à partir d'un certain rang. Un anneau possédant cette propriété est dit *noethérien*.

Théorème I.13.5.3 (fondamental de l'arithmétique) *i) Pour tout élément $a \in A, a \neq 0$, il exist un entier $n \in \mathbb{N}$ des éléments irréductibles $p_i\,_{,1\leq i\leq n}$ deux à deux non associés, des entiers naturels $\alpha_i\,_{,1\leq i\leq n} \in \mathbb{N}$, et un élément inversible u tels que :*

$$a = u * \prod_{i=1}^{n} p_i^{\alpha_i}\ . \qquad 1$$

ii) La décomposition ci-dessus d'un élément $a \in A, a \neq 0$, est unique au sens où si

$$a = u * \prod_{i=1}^{d} p_i^{\alpha_i} = v * \prod_{i=1}^{e} q_i^{\beta_i}, \qquad 1$$

$m = n$ et il existe une bijection $\sigma : [1;d] \to [1;d]$ tel que

$$\forall 1 \leq i \leq n,\ \alpha_i = \beta_{\sigma(i)}\ ,\ p_i et\ q_{\beta(i)}\ \text{sont associés}\ .$$

Remarque I.13.5.4 On pourra être surpris de voir ici que la décomposition en produit de facteurs premiers (irréductibles) apparaît comme une conséquence du lemme de GAUSS (cf. I.13.2.3,) ou du lemme d'Euclide (cf. I.13.2.6,) alors que souvent l'on présente ces deux résultats comme conséquence de la décomposition en produit de facteurs premiers. On pourrrait montrer qu'en fait ces propriétés sont équivalentes pour un anneau et qu'en particulier un anneau dans lequel le théorème de BÉZOUT est vérifié, les possède.

Définition I.13.5.5 (Valuation p-adique) Le théorème I.13.5.3.ii) assure que pour tout

$$a = u * \prod_{i=1}^{n} p_i^{\alpha_i} \in A \setminus \{0\},$$

l'entier naturel α_i est bien défini. On le notera $v_{p_i}(a)$ qu'on appellera *valuation p_i-adique* de a.

I.13.6 . −Algorithme d'Euclide

Il ne suffit pas que l'anneau A soit principal pour qu'on puisse mettre en œuvre l'algorithme d'Euclide, celui-ci s'appuyant en effet sur la *division euclidienne*. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ (cf. III.4.2,) disposent néanmoins de cette propriété. Nous allons introduire la notion d'anneau euclidien à seule fin de donner une dénommination commune à ces situations et remarquer que les anneaux euclidiens sont principaux de manière à pouvoir utiliser toutes les ressources dévloppées dans le paragraphe I.13, à propos des anneaux principaux.

Définition I.13.6.1 Étant donné un anneau commutatif intègre A, un *stathme euclidien* sur A est une application

$$\mathbf{v} \,:\, A \setminus \{0\} \,\to\, \mathbb{N}$$

vérifiant :

$$\forall (a,b) \in A \,\times\, (A \setminus \{0\}),\, \exists (q,)r \,\in\, A \,\times\, A,\, a \,=\, b * q \,+\, r \,\text{et}\, \big(r \,=\, 0 \,\text{ou}\, \mathbf{v}(r) \,<\, \mathbf{v}(b)\,\big), \quad \text{I.13.6.1.1}$$

$$\forall (a,b) \in (A \setminus \{0\}) \,\times\, (A \setminus \{0\}),\, \mathbf{v}(b) \,\leq\, \mathbf{v}(a * b)\,. \quad \text{I.13.6.1.2}$$

Un anneau commutatif intègre muni d'un stathme euclidien $\mathbf{v}$ est appelé *anneau euclidien* et on parle de *division euclidienne* suivant le stathme $\mathbf{v}$.

On adopte en général la terminologie usuelle suivante : a est le *dividende* b le *diviseur* q un *quotient* et r un *reste*.

Exemple I.13.6.2 a) $((\mathbb{Z}, |\cdot|))$

L'anneau $\mathbb{Z}$ muni de la valeur absolue est un anneau euclidien .

b) $((\mathbb{K}[X], \deg(\cdot)))$

L'anneau $\mathbb{K}[X]$ muni du degré $\deg(\cdot)$ est un anneau euclidien (cf. III.4.)

c) $((\mathbb{K}[X], \mathrm{val}(\cdot)))$

L'anneau $\mathbb{K}[X]$ peut également être muni du stathme euclidien donné par la valuation $\mathrm{val}(\cdot)$ donnant lieu à la notion de *division suivant les puissances croissantes*.

d) (**Entiers de GAUSS**)

Remarque I.13.6.3 On constate que dans la définition I.13.6.1 aucun énoncé d'unicité du couple (q, r) n'est donné contrairement à ce qui est le cas dans le cas de l'anneau $\mathbb{Z}$ ou même pour l'anneau $\mathbb{K}[X]$ (cf. III.4.2.) Dans ces deux cas, le stathme euclidien considéré possède une propriété supplémentaire de « compatibilité » à l'addition $|a+b| \,\leq\, |a| \,+\, |b|$, $\deg(P+Q) \,\leq\, \max(\deg(P), \deg(Q))$ qui n'est pas exigé par les axiomes I.13.6.1.1 et I.13.6.1.2. On constatera que l'anneau des entiers de GAUSS n'a pas de telle propriété et que néanmoins une arithmétique similaire à celle des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ peut y être développée.

En particulier l'absence d'énoncé d'unicité dans la division euclidienne n'interdit pas de montrer que l'anneau est principal comme nous allons le voir dans la proposition I.13.6.4 qui peut servir de point de départ à toute l'arithmétique de ces anneaux.

Proposition I.13.6.4 *Un anneau euclidien $(A, \mathbf{v})$ (où A est un anneau commutatif intègre et $\mathbf{v}$ un stathme euclidien) est principal.*

Proposition I.13.6.5 (Algorithme d'Euclide) *Soit $(A, \mathbf{v})$ un anneau euclidien (cf. I.13.6.1.) Étant donnés deux éléments a_0 et a_1 de A, l'algorithme d'Euclide consiste en la donnée des suites*

$$\left(a_n\right)_{,n\in\mathbb{N}}\ ,\ \left(u_n\right)_{,n\in\mathbb{N}}\ ,\ \left(v_n\right)_{,n\in\mathbb{N}} \text{ et } \left(q_n\right)_{,n\in\mathbb{N}}$$

définies par récurrence de la manière suivante :

$$\begin{array}{rcl} u_0 & := & 1 \\ u_1 & := & 0 \\ v_0 & := & 0 \\ v_1 & := & 1\,; \end{array} \qquad \textit{I.13.6.5.1}$$

pour tout $n \in \mathbb{N}$, si $a_{n+1} = 0$,

$$a_{n+2} \ = \ u_{n+2} \ = \ v_{n+2} \ = \ q_n \ = \ 0\,;$$

sinon, q_n est un quotient de la division euclidienne de a_n par a_{n+1} et $a_{n+2} \ := \ a_n - q_n * a_{n+1}$ un reste. On pose alors :

$$\begin{array}{rcl} u_{n+2} & := & u_n - q_n * u_{n+1} \\ v_{n+2} & := & v_n - q_n * v_{n+1}\,. \end{array} \qquad \textit{I.13.6.5.2}$$

Alors :

i) Soit

$$\forall n \in \mathbb{N},\ a_n \ = \ 0,$$

et on pose $m \ := \ 0$, soit

$$\exists m \in \mathbb{N},\ ((a_m \ \neq \ 0) \text{ et } (\forall q > m\ ,\ a_q \ = \ 0))\,.$$

ii)

$$\forall n \in \mathbb{N},\ \left(n \leq m-2 \ \Rightarrow \ \mathcal{D}(a_n, a_{n+1}) \ = \ \mathcal{D}(a_{n+1}, a_{n+2})\right)\,;$$

d'où il résulte que d est un PGCD de a_n et a_{n+1} si et seulement si d est un PGCD de a_{n+1} et a_{n+2}.

iii)

$$\forall n \in \mathbb{N},\ a_n \ = \ a_0 * u_n \ + \ a_1 * v_n\,.$$

iv) L'élément $a_{m\,\in\,A}$ est un PGCD pour a_0 et a_1, u_m et v_m des coefficients de BÉZOUT *(cf. I.13.1.4.)*

Exemple I.13.6.6 On peut [1] mettre en oeuvre l'algorithme d'Euclide de la manière suivante :

q_n	a_n	u_n	v_n
	179	1	0
	11	0	1
16	3	1	-16
3	2	-3	49
1	1	4	-65

d'où il résulte que

$$179 \wedge 11 \ = \ 1 \text{ et } 4 * 179 \ - \ 65 * 11 \ = \ 1\,.$$

1. On n'a jamais dit « on doit »

Remarque I.13.6.7 En considérant attentivement la proposition I.13.6.5, on constaterait qu'il n'est nul besoin de savoir a priori qu'il existe un PGcD dans l'anneau A. En particulier nul besoin de savoir si l'anneau A est principal ou non. l'algorithme d'Euclide établit directement l'existence du pGCD à partir de la division euclidienne. Comme il donne également les coefficients de BÉZOUT il permet de démontrer le théorème de BÉZOUT sans recours au formalisme des idéaux. Reformuler le théorème chinois des restes dans ce contexte commencerait peut-être à devenir moins séduisant moins encore si on s'avisait d'en donner une formulation pour l'anneau $\mathbb{K}[X]$.

I.14 . −Exercices

Exercice I.14.1 [Loi de composition, (Magma)]

Cet exercice a été traité dans le premier TD d'algèbre I (M303).

Dans tout cet exercice A est un ensemble muni d'une loi de composition associative (*i.e.* un magma associatif (cf. I.0.1.2.)) Pour tout $(x, y) \in A \times A$, on note simplement xy leur composé qu'on appellera également produit.

1) a) Soit n un entier ≥ 2, et soient $a_1, \ldots, a_n$ des éléments de A. Pour calculer dans A le produit $a_1 a_2 \ldots a_n$, il faut mettre des parenthèses de façon à ne calculer, aux étapes successives, que des produits de deux éléments de A. Montrer que le résultat ne dépend pas du choix d'un tel parenthésage ; on le note $a_1 a_2 \ldots a_n$.

Indication : *On pourra procéder par une récurrence sur n, et comparer deux tels parenthésages, l'un où le dernier produit effectué regroupe les k premiers termes : $(a_1 \ldots a_k)(a_{k+1} \ldots a_n)$, l'autre où le dernier produit regroupe les $(k+1)$ premiers termes $(1 \leq k \leq n)$.*

b) Pour $a \in A$ et p entier ≥ 1, on note a^p le produit $a_1 \ldots a_p$ où $a_1 = a_2 = \ldots = a_p = a$. Montrer qu'on a

$$a^p a^q = a^{p+q} \text{ et } (a^p)^q = a^{pq} \text{ pour } p, q \text{ entiers } \geq 1 .$$

2) a) Supposons que A possède un élément neutre, c'est-à-dire un élément e tel que $ea = ae = a$ pour tout $a \in A$. Montrer qu'un tel élément est unique ; on le note souvent 1 et on pose $a^0 = 1$ pour tout $a \in A$.

b) Étendre aux entiers p et $q \geq 0$ les règles établies en question 1), b).

c) Soient a,b,c des éléments de A tels que $ab = bc = 1$; montrer qu'alors $a = c$. En déduire que si a possède un inverse b, cet inverse est unique ; on le note a^{-1}.

d) Prouver que si des éléments $a_1, \ldots, a_n$ de A ont chacun un inverse, alors $a_1 \ldots a_n$ est inversible aussi, et calculer son inverse.

e) Prouver que l'ensemble des éléments inversibles de A est un groupe pour la loi $(a, b) \mapsto ab$.

f) Si a est un élément inversible de A, on pose $a^{-p} := (a^{-1})^p$ pour p entier ≥ 1. Étendre les règles établies en question 1), b) à tous les entiers $p, q \in \mathbb{Z}$.

3) a) Soient x et y deux éléments de A qui commutent : $xy = yx$. Prouver que, quels que soient les entiers p et $q \geq 1$, x^p et y^q commutent aussi, et qu'on a $(xy)^p = x^p y^p$.

b) Étendre ces résultats aux entiers p et $q \geq 0$ si A a un élément neutre 1, et à tous les entiers p et q si x et y sont inversibles.

c) Si on prend pour A un groupe abélien avec une loi noté additivement $(a, b) \mapsto a + b$, on écrit 0 (plutôt que 1) pour l'élément neutre et on note nx au lieu de x^n (en particulier l'opposé de x, c'est-à-dire l'inverse pour la loi $+$, est noté $-x$.)

a) Écrire dans ces notations les résultats obtenus en question 1), question 2), question 3).

b) Pour x, y dans A on pose alors $x - y = x + (-y)$; prouver que c'est le seul élément z de A tel que $x = z + y$; calculer $-(x-y)$, $(x-y)+(x'-y')$, $(x-y)-(x'-y')$.

4) Pour $n \in \mathbb{N}^*$ et tout n-uplet $a_{i\ ,1\leq i\leq n}$ d'éléments de A, on définit le *produit des* $a_{i\ ,1\leq i\leq n}$ qu'on note $a_1 \times \ldots \times a_n$ par *récurrence* : Si $n = 1$, le produit de l'élément a est a lui-même et pour tout $n+1$-uplet $a_{i\ ,1\leq i\leq n+1}$,

$$(a_1 \times \ldots \times a_{n+1}) \ := \ (a_1 \times \ldots \times a_n) \times a_{n+1} \ .$$

a) Soit n un entier ≥ 1, et $(a_i)_{i\ \in\ I}$ une famille à n éléments de A, ces éléments commutent l'un à l'autre. Montrer que, quelle que soit la numérotation $i_1, \ldots, i_n$ qu'on mette sur I (*i.e.*quelle que soit la bijection $n \mapsto i_n$ de $\{1, \ldots, n\}$ sur I ,) le produit $a_{i_1} \times \ldots \times a_{i_n}$ est toujours le même ; on le note $\prod_{i\ \in\ I} a_i$ [on pourra procéder par récurrence sur n et comparer deux tels produits, tout d'abord dans le cas où un élément b de A se trouve en dernière position, puis dans le cas où un élément b de A se trouve en $k^{\text{ième}}$ position dans le premier produit, et en $(k+1)^{\text{ième}}$ position dans le second, $1 \leq k < n$.]

b) Soit $I = \bigcup_{k\ \in\ K} J_k$ une partition de I (en sous-ensembles deux à deux disjoints non vides.) Montrer qu'on a :

$$\prod_{i\ \in\ I} a_i \ = \ \prod_{k\ \in\ K} \ (\prod_{j \in J_k} a_j) \ .$$

Pour m entier ≥ 1, on a

$$(\prod_{i\ \in\ I} a_i)^m \ = \ \prod_{i\ \in\ I} a_i^m \ .$$

c) Supposons que A ait en outre un élément neutre 1 ; on pose alors $\prod_{i\ \in\ I} a_i = 1$ si I est vide ; étendre les règles précédentes aux cas où I, ou l'un des J_k est vide.

d) Supposons que A soit un groupe abélien noté additivement ; on écrit alors $\sum_{i\ \in\ I} a_i$; traduire dans ces notations les résultats précédents.

5) Soit X un ensemble. On munit l'ensemble A^X des applications de X dans A de la loi $(f, f') \mapsto ff'$ où $ff'(x) = f(x)f'(x)$ pour tout $x \in X$.

a) Montrer que la loi définie ci-dessus est la seule pour laquelle, pour tout $x \in XX$, $f \mapsto f(x)$ est un morphisme.

b) Montrer que cette loi sur A^X est associative et que A^X est un groupe pour cette loi si A est un groupe, un groupe abélien si A est un groupe abélien.

c) Si A est un groupe, et X un autre groupe, montrer que l'ensemble $\mathrm{Hom}(X, A)$ des homomorphismes de groupes de X dans A est un sous-groupe de A^X, pourvu que A soit abélien.

6) (**Groupe abélien**)

On suppose que A est un groupe abélien et pour tout $p \in \mathbb{Z}$, et tout $a \in A$, on note $p \cdot a := a^p$ avec les notations de question 2), f) et question 1), b).

Réécrire dans ce formalisme les résultats de question 1), b) et question 2), f).

Exercice I.14.2 Quelle différence y-a-til entre I.5.1.i) et I.5.1.ii) du point de vue des anneaux et de celui des groupes. Comparer à la proposition A.5.1.

Exercice I.14.3 Avec les notations I.7.1, montrer que pour tout F muni d'une des structures algébriques I.7.1.i) ou I.7.1.iii), l'application

$$\mathrm{Hom}(F,P) \to \prod_{k=1}^{n} \mathrm{Hom}(F,E_k)\ ,\ f \mapsto \big(p_1 \circ f, \dots, p_n \circ f\big)$$

est un isomorphisme pour la structure algébrique considérée.

Exercice I.14.4 Avec les notations I.7.1, si $\forall 1 \leq k \leq n$, E_k est un anneau, (resp. une A-algèbre,)

1) les applications i_k de la proposition I.7.6 sont-elles des morphismes d'anneaux (resp. de A-algèbres ?)

2) Que peut-on dire de $\mathrm{Im}\, i_k$?

Exercice I.14.5 Démontrer le théorème I.9.19.

Exercice I.14.6 Soit

$$0 \to B \xrightarrow{\ i\ } A \xrightarrow{\ p\ } C \to 0$$

une suite exacte courte de groupes abéliens finis. On suppose que $\#(B)$ et $\#(C)$ sont des entiers premiers entre eux. Montrer qu'alors la suite exacte courte est scindée.

Exercice I.14.7

Exercice I.14.8

Exercice I.14.9 [Valuations p-adiques]

Soit $p \in \mathcal{P}$.

On peut, dans cet exercice, remplacer $\mathbb{Z}$ par n'importe quel anneau principal A et $\mathbb{Q}$ par son corps des fractions $\mathbb{K}$.

1) Pour tout $x \in \mathbb{Q}\ ,\ x \neq 0$, montrer qu'il existe un unique triplet

$$(r_x, n_x, d_x) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \text{ tel que } x = p^{r_x}\frac{n_x}{d_x}\ ,\ n_x \wedge d_x = 1\ ,\ p \wedge d_x = 1 \text{ et } p \wedge n_x = 1\ .$$

On définit ainsi une application $v_p : \mathbb{Q} \to \overline{\mathbb{Z}}$ **en posant**

$$v_p(x) := r_x \,\forall\, x \in \mathbb{Q} \setminus \{0\} \text{ et } v_p(0) := (+\infty) .$$

Pour tout $x \in \mathbb{Q} \setminus \{0\}$, **on notera**

$$\mathcal{S}(x) := \{p \in \mathbb{P} \,;\, v_p(x) \neq 0\} \text{ et } \mathcal{S}(0) := \mathcal{P} .$$

2) (**Propriétés de** v_p)
Établir les propriétés suivantes de v_p :

Val_1)
$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{Z},\ x|y \ \Rightarrow\ \forall p \in \mathcal{P},\ v_p(x) \leq v_p(y) .$$

Val_2) Pour tout $x \in \mathbb{Z} \setminus \{0\}$, (resp. tout $x \in \mathbb{Q} \setminus \{0\}$,) $\mathcal{S}(x)$ est un ensemble fini éventuellement vide et que l'on a
$$x = \epsilon \prod_{p \in \mathcal{S}(x)} p^{v_p(x)} ,\ \epsilon \in \{-1, 1\} .$$

Val_3) La réciproque de Val_1) est vraie.

Val_4)
$$\forall x \in \mathbb{Q},\ x \in \mathbb{Z} \ \Leftrightarrow\ v_p(x) \geq 0 \,\forall\, p \in \mathcal{P} .$$

Val_5)
$$\forall x \in \mathbb{Q},\ \forall y \in \mathbb{Q},\ \forall p \in \mathbb{P},\ v_p(xy) = v_p(x) + v_p(y) \text{ et } v_p(x+y) \geq \min(v_p(x), v_p(y))$$
avec égalité dans la dernière inégalité si $v_p(x) \neq v_p(y)$.

Val_6)
$$\forall\, (x, y) \in \left(\mathbb{Z} \setminus \{0\}\right)^2 ,\ x \wedge y = \prod_{p \in \mathcal{P}} p^{\min(v_p(x), v_p(y))} \text{ et } [x, y] = \prod_{p \in \mathcal{P}} p^{\max(v_p(x), v_p(y))} .$$

II . −Structure des groupes abéliens de type fini

II.0 . −Introduction

le but de ce chapitre (II,) est d'établir de manière rigoureuse qu'un groupe abélien est essentiellement constitué d'une partie du type $\mathbb{Z}^r$ et d'une autre qui est un produit de groupes cycliques. Un énoncé précis sera obtenu au théorème II.6.4. il est dès lors nécessaire d'étudier les groupes abéliens libres (de type fini) (cf. II.3.2,) d'une part, et les groupes abéliens de type fini et de torsion (*i.e.* finis,) (cf. II.5.2.vi).) c

Les premiers ressemblent assez à des espaces vectoriels, mais qu'on ne sy 'laisse pas prendre : le théorème II.4.6 semble déjà suffisamment délicat à obtenir pour qu'on puisse douter que la situation de deux groupes abéliens libres inclus l'un dans l'autre soit aussi simple que celle de deux espaces vectoriels emboîtés. De fait le résultat optimal qui pourra être obtenu est celui dit du théorème de la base adaptée (théorème II.11.12 qui est tout de même assez éloigné, de ce qui lui est cependant le plus proche à savoir le théorème de la base incomplète en algèbre linéaire.

Les groupes abéliens de type finni et de torsion recevront quant à eux une description complète en termes des plus élémentaires d'entre eux, à savoir les groupes cycliques, au théorème II.10.5. le résultat en réalité le plus susceptible d'être utilisé dans le paragraphe II.10 est le corollaire II.10.7 qui permet de déterminer quand deux groupes abéliens de type fini sont isomorphes. À noter que le théorème II.8.3 s'il est un ingrédient clef de la construction aboutissant au théorème de structure II.10.5, est déjà un résultat significatif en soi et qui fournit une première description des groupes de torsion. **Dans ce chapitre (II,) les notations suivantes seront couramment utilisées :**

Notation II.0.1 Pour tout $n \in \mathbb{Z}$, on notera $\mathbb{Z}/n\mathbb{Z}$ ou même simplement $\mathbb{Z}/n$ le quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$ et

$$\pi_n : \mathbb{Z} \to \mathbb{Z}/n \text{ la surjection canonique.}$$

Notation II.0.2 (Éléments irréductibles, nombres premiers) On notera $\mathbb{P}_{\mathbb{Z}}$ ou simplement $\mathbb{P}$ l'ensemble des nombres premiers *i.e.* l'ensemble des éléments irréductibles de $\mathbb{Z}$ contenus dans $\mathbb{N}^*$.

Notation II.0.3 (Valuations p-adiques) Pour tout nombre premier

$$p \in \mathbb{P} \text{ et tout entier relatif } a \in \mathbb{Z}, \text{ on note } v_p(a)$$

sa *valuation p-adique* définie comme en I.13.5.5. On note encore

$$\mathcal{S}(a) := \{p \in \mathbb{P} \,;\, v_p(a) \neq 0\}$$

dont on rapelle que c'est un ensemble fini.

Notation II.0.4 (Décomposition en produit d'irréductibles) Pour tout $a \in \mathbb{Z} \setminus \{0\}$, on a

$$a = u \prod_{p \in \mathbb{P}} p^{v_p(a)} = \prod_{p \in \mathcal{S}(a)} p^{v_p(a)}, \; u \in \mathbb{Z}^\times, \textit{i.e. } u = \pm 1 \text{ (cf. I.13.5.3 ;)}$$

le produit ci-dessus étant en fait fini puisque $v_p(a) \neq 0$ pour un nombre fini de $p \in \mathbb{P}$ seulement.

II.1 . −Groupes abéliens de type fini

Dans ce paragraphe (II.1,) A est un anneau commutatif.

Rappel II.1.1 (Partie génératrice) Pour un groupe abélien $(X,+)$ (resp. un A-module $(X,+,\cdot),$) un sous-ensemble $S \subset X$ est une *partie génératrice* (cf. I.4.2 (resp. A.4.2,)) si $X = < S >$. On dit alors que X est *engendré* par S.

Remarque II.1.2 Pour un groupe abélien X, et $S \subset X$, il est équivalent de dire que X est engendré par S en tant que groupe abélien ou en tant que $\mathbb{Z}$-module.

Lemme II.1.3 *Soient X un groupe abéliens (resp. A-module.)*

i) Un morphisme de groupes abéliens (resp. A-modules,) $f : X \to Y$ est surjectif si et seulement s'il existe une partie S de X telle que $f(S)$ est une partie génératrice de Y ; si et seulement si l'image par f de toute partie génératrice de X est une partie génératrice de Y.

ii) Toute partie T de X contenant une partie génératrice S est génératrice.

Exemple II.1.4 a) Le groupe abélien $\mathbb{Z}$ est engendré par $\{1\}$ ou $\{-1\}$.

b) L'anneau A lui-même vu comme A-module comme en A.1.2.b) engendré par $\{1\}$ ou par $\{u\}$ pour tout $u \in A^\times$.

c) Plus généralment, pour tout entier $n \in \mathbb{N}$, le groupe abélien (resp. A-module,) $\mathbb{Z}^n$ (resp. A^n,) (cf. I.7,) est engendré par la famille $\varepsilon_i\,,_{1\leq i\leq n}$ où

$$\varepsilon_i = (0,\dots,0,1,0,\dots,0) \text{ ou encore } \varepsilon_i(j) = \delta_i^j \ \forall 1 \leq i \leq n,\ \forall 1 \leq j \leq n, \ .$$

d) Dans l'anneau $A[X]$ des polynômes à une indéterminée et à coefficients dans A,

$$\text{la famille } X^n\,,_{n\,\in\,\mathbb{N}}$$

est une famille génératrice (cf. III.2.5.v).a).)

Définition II.1.5 (Groupe abélien (resp. Module) de type fini) Un groupe abélien (resp. A-module,) X est *de type fini* s'il possède une partie génératrice finie.

Exemple II.1.6 a) On constate sur l'exemple II.1.4.a) que $\mathbb{Z}$ est un groupe abélien de type fini et sur l'exemple II.1.4.b) que A est un A-module de type fini. De même l'exemple II.1.4.c) montre que $\mathbb{Z}^n$ (resp. A^n,) est un groupe abélien (resp. un A-module) de type fini.

b) En revanche la famille $X^n\,,_{n\,\in\,\mathbb{N}}$ de $A[X]$ n'est pas finie. On pourrait cependant se demander s'il n'existe pas une famille génératrice finie du A-module $A[X]$ (que A soit un corps $\mathbb{K}$ ou non.) L'exercice A.8.4 apporte une réponse à cette question.

Définition II.1.7 (Groupe monogène) Pour X un groupe abélien (resp. A-module,) et $x \in X$, le sous-groupe (resp. sous- A-module,)

$$< \{x\} > = \{a \cdot x \ , \ a \in \mathbb{Z} \text{ (resp. } A)\} \, ,$$

engendré par $\{x\}$ est usuellement noté

$$\mathbb{Z} \cdot x \text{ (resp. } A \cdot x, \text{)}$$

ou même simplement

$$\mathbb{Z}x \text{ (resp. } Ax \text{ .)}$$

En particulier pour $a \in A$, l'idéal engendré par $\{a\}$ est noté Aa. Cette notation rappelle celle utilisée pour les $\mathbb{K}$-espaces vectoriels et qui consiste à noter $\mathbb{K}v$ la droite engendrée par le vecteur v.

Si $X = < \{x\} >$ on dit que X est *monogène*.

Lemme II.1.8 *Étant donnés un groupe abélien (resp. un A-module,) X, un entier $n \in \mathbb{N}^*$ et un n-uplet $x_i \, , 1 \leq i \leq n} \in X$ d'éléments de X, il existe un morphismes de groupes (resp. de A-modules,)*

$$\phi \ : \ \mathbb{Z}^n (\text{resp. } A^n) \ \to \ X \ , \ \varepsilon_i \ \mapsto \ x_i$$

(où les éléments $\varepsilon_i \, , 1 \leq i \leq n$ sont les éléments introduits en II.1.4.c).) La généralisation de ce lemme donnée en II.2.10 assure même que ϕ est unique.

Preuve *: Si un tel morphisme existe,*

$$\forall a_i \, , 1 \leq i \leq n \in \mathbb{Z}^n (\text{resp. } A^n), \ \phi\big(\sum_{i=1}^{n} a_i \varepsilon_i\big) \ = \ \sum_{i=1}^{n} a_i \cdot x_i \ .$$

Il est tout à fait élémentaire de voir que cette formule définit bien un morphisme.

Proposition II.1.9 *Étant donné un groupe abélien (resp. A-module,) X, les assertions suivantes sont équivalentes :*

a) X est de type fini.

b) Il existe un entier $r \in \mathbb{N}$, et un morphisme surjectif

$$p \ : \ \mathbb{Z}^r (\text{resp. } A^r) \ \to \ X \ .$$

c) Il existe un groupe abélien (resp. A-module,) de type fini Y et un morphisme surjectif $p \ : \ Y \ \to \ X$.

Preuve *:*

*i) **(a)** $\Rightarrow$ **b)***

Si X est de type fini, il possède une partie génératrice fini $S := \{s_1, \ldots, s_r\}$. Il existe alors, en vertu du lemme II.1.8 un morphisme de groupes (resp. A-modules,)

$$\phi \ : \ A^r \ \to \ X \ , \ \varepsilon_i \ \mapsto \ s_i \, , 1 \leq i \leq r$$

(où ε_i) et défini comme dans l'exemple II.1.4.c). Il résulte alors du lemme II.1.3.i), que ϕ est surjectif.

ii) ***(b)*** $\Rightarrow$ ***c))***
(cf. II.1.4.c).)

iii) ***(c)*** $\Rightarrow$ ***a))***
Si Y est de type fini, il existe une partie génératrice finie S de Y. Si $p : Y \to X$ est un morphisme surjectif, il résulte du lemme II.1.3.i) que $p(S)$ est une partie génératrice de X finie qui plus est.

Remarque II.1.10 On constate avec la proposition ci-dessus qu'il est presque tautologique qu'un quotient d'un groupe abélien
(resp. A-module,) de type fini est de type fini mais qu'on n'a rien affirmé concernant les sous-groupes (resp. sous-A-modules.) Ceci semble d'autant plus contre intuitif qu'on sait depuis longtemps que la dimension est croissante pour les $\mathbb{K}$-espaces vectoriels. Des résultats positifs seront cependant exposés au paragraphe II.4.

Proposition II.1.11 *Étant donné deux groupes abéliens (resp. A-modules,) de type fini X_1 et X_2,*

i) le groupe abélien (resp. A-module,) $X_1 \times X_2$ est de type fini ;

ii) si X_1 et X_2 sont des sous-groupes (resp. sous-A-modules,) d'un groupe abélien (resp. A-module,) X tels que $X = X_1 + X_2$, X est de type fini ;

iii) si X est un groupe abélien (resp. A-module,) tel qu'il existe une suite exacte

$$0 \to X_1 \xrightarrow{i} X \xrightarrow{p} X_2 \to 0$$

X est de type fini.

Preuve *: Étant donnée une partie génératrice finie de X_2, on note X_2 un ensemble de relèvement de ces générateurs dans X. Alors X_2 est une partie finie de X, et si l'on note $Y_2 := < X_2 >$ le sous-groupe (resp. sous- A-moduled)e X engendré par X_2, tout élément de X_2 possède un relèvement dans Y_2. Ainsi, pour tout $x \in X$, $p(x)$ possède un relèvement $y \in Y_2$. Il en résulte que*

$$p(x - y) = p(x) - p(y) = 0,$$

c'est-à-dire que $x - y \in i(X_1)$.
Il s'ensuit que $X = Y_2 + i(X_1)$ (cette somme n'ayant aucune raison d'être directe en général.)
Il suffit donc d'aplliquer le point ii).

II.2 . −Groupes abéliens (resp. A-modules) libres

Définition II.2.1 (Famille libre) Une partie $L \subset X$ d'un groupe abélien (resp. A-module,) est *libre* si, pour tout entier n, tout n-uplet $\lambda_{i\ ,1\leq i\leq n} \in L$ d'éléments deux à deux distincts de L, tout n-uplet $a_{i\ ,1\leq i\leq n}$ d'éléments de $\mathbb{Z}$ (resp. A,)

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

Remarque II.2.2 Dans la définition II.2.1 ci-dessus, il revient au même de dire que

$$< L > = \sum_{\lambda \in L} \mathbb{Z} \cdot \lambda (\text{resp. } A \cdot \lambda \text{ est une somme directe (cf. I.4.8.ii) (resp. A.4.6.ii).))}$$

Lemme II.2.3 *Soit X un groupe abélien (resp. A-module.)*

i) si $f : X \to Y$ est un morphisme injectif de groupe abéliens (resp. A-modules) l'image de toute partie libre de X est une partie libre de Y.

ii) Pour toute partie libre L de X tout sous-ensemble de L est libre.

Exemple II.2.4 Dans l'anneau $A[[X]]$ (cf. III.1,) (ainsi d'ailleurs que dans le groupe abélien (resp. A-module,) $A[X]$,) la famille $X^{n}{}_{,n\ \in\ \mathbb{N}}$ est libre.

Définition II.2.5 (Base) Une partie $\mathcal{B}$ d'un groupe abélien (resp. A-module,) X est une *base* de X si c'est une partie libre et génératrice.

Exemple II.2.6 a) Dans les exemples II.1.4.b) à II.1.4.d) les partie génératrices qu'on a mises en évidence sont en fait des bases.

b) Si $A = \mathbb{Z}x = < x >$ est un groupe monogène (cf. II.1.7,) $\{x\}$ est tautologiquement une partie génératrice de A, cependant, contrairement à ce qui se passe dans le cas des espaces vectoriels, il ne suffit pas que $x \neq 0$ pour que x soit une base de A. Les paragraphes II.5 et A.7 précisent cette question en introduisant la notion d'éléments *de torsion*.

Si $X = x_{i\ ,1\leq i\leq r}$ est une partie finie de X, le sous-groupe (resp. sous- A-module,) $< X >$ de X engendré par X est (cf. I.4.8(resp. A.4.6,))

$$< X > = \sum_{i=1}^{r} A \cdot x_i\ .$$

Là encore il est difficile de donner, en toute généralité, des conditions dans lesquelles cette somme est directe.

Remarque II.2.7 La définition d'une base donnée ci-dessus n'est en rien différente de celle donnée pour les $\mathbb{K}$-espaces vectoriels. Plus précisément encore, une base d'un $\mathbb{K}$-espace vectoriel E est une base de E en tant que $\mathbb{K}$-module.

Si, comme nous allons le voir, les bases des groupes abéliens (resp. A-modules) bénéficient de bonnes propriétés, leur plus grand défaut est, contrairement à la situation rencontrée pour les $\mathbb{K}$-espaces vectoriels, de ne pas toujours exister. Dans le groupe abélien ($\mathbb{Z}$-module) $\mathbb{Z}/n\mathbb{Z}$, par exemple, $n\cdot\alpha = 0$ pour tout $\alpha \in \mathbb{Z}/n\mathbb{Z}$. Aucune famille de $\mathbb{Z}/n\mathbb{Z}$ n'est donc libre.

Certains groupes abéliens (modules,) ne possédant donc pas de base, on est motivé à donner la définition suivante :

Définition II.2.8 (Groupe abélien (resp. A-module,) libre) On dira qu'un groupe abélien (resp. A-module,) X est *libre* s'il admet une base.

Pour un groupe abélien il revient au même d'être libre au sens ci-dessus ou d'être libre en tant que $\mathbb{Z}$-module.

Exemple II.2.9 Ainsi les modules considérés dans les exemples II.1.4.b) à II.1.4.d) sont des modules libres.

Bien entendu, si $\mathbb{K}$ est un corps un $\mathbb{K}$-espace vectoriel est un $\mathbb{K}$-module libre.

Lemme II.2.10 *Étant donné un groupe abélien (resp. A-module,) X possédant une base $\mathcal{B} := \beta_{i\ ,1\leq i\leq n}$, pour tout groupe abélien (resp. A-module,) Y et tout n-uplet $\gamma_{i\ ,1\leq i\leq n} \in Y$ d'éléments de Y, il existe un unique morphisme de groupes (resp. A-modules,)*

$$\phi\ :\ X\ \to\ Y\ ,\ \beta_k i\ \mapsto\ \gamma_{i\ ,1\ \leq\ i\ \leq\ n}\ .$$

Preuve *: Pour tout $x \in X$, il existe, puisque $\mathcal{B}$ est une base de X, $a_{i\ ,1\leq i\leq n} \in A$, tel que $x = \sum_{i=1}^{n} a_i\beta_i$. Si donc ϕ existe, nécessairement,*

$$\phi(x)\ =\ \phi\big(\sum_{i=1}^{n} a_i\beta_i\big)\ =\ \sum_{i=1}^{n} a_i\phi(\beta_i)\ =\ \sum_{i=1}^{n} a_i\gamma_i\ .$$

Ceci établit l'unicité de ϕ.

Reste à voir que la formule ci-dessus définit bien, sans ambiguïté un morphisme de groupes abélienss (resp. A-modules.)

Remarque II.2.11 i) Le lemme II.2.10 est bien connu dans le cas des espaces vectoriels, et la preuve donnée ici n'est pas sensiblement différente de celle qu'on peut donner pour les espaces vectoriels et les applications linéaires. Une fois encore dès que l'on dispose d'une base pour un groupe abélien (resp. A-module,) un certain nombre de résultats établis dans le cas des espaces vectoriels peuvent se transposer aisément au cas des groupes abéliens (resp. modules.) Mais outre que l'on ne dispose pas toujours d'une base, un certain nombre de résultats ne s'étendront pas au cas des groupes abéliens (resp. A-modules.)

ii) Dans le lemme II.2.10 on n'est pas obligé de supposer que la base $\mathcal{B}$ est de cardinal fini mais c'est essentiellement la situation que nous allons rencontrer (cf. II.12.2 pour un résultat plus général.)

Lemme II.2.12 *Si $f : X \cong Y$ est un isomorphisme de groupes, entre groupes abéliens (resp. A-modules,) pour toute base $\mathcal{B}$ de X, $f(\mathcal{B})$ est une base de Y.*

II.3 . −Groupes abéliens (resp. A-modules,) libres de type fini

Proposition II.3.1 (Modules libres de type fini) *Pour un groupe abélien (resp. A-module,) X, les conditions suivantes sont équivalentes :*

a) X possède une base de cardinal fini $n \in \mathbb{N}^*$.

b) Il existe un isomorphisme

$$X \cong \mathbb{Z}^n (\text{resp. } A^n)$$

(cf. II.1.6.a).)

c) X est un groupe abélien (resp. A-module,) à la fois libre et de type fini.

***Preuve** :*

*i) (**a)** $\Rightarrow$ **b**))*
Soit $\mathcal{B} := \beta_{i\ ,1\leq i\leq n}$ une base de X et $\varepsilon_{i\ ,1\leq i\leq n}$ la base de $\mathbb{Z}^n$ (resp. A^n) introduite dans l'exemple II.1.4.c). En vertu du lemme II.2.10, il existe un unique couple de morphismes de groupes (resp. A-modules,)

$$\begin{aligned} & \phi \ : \ X \ \to \ \mathbb{Z}^n (\text{resp. } A^n) \ , \ \beta_i \ \mapsto \ \varepsilon_{i\ ,1 \leq i \leq n} \\ \text{et} \quad & \psi \ : \ \mathbb{Z}^n (\text{resp. } A^n) \ \to \ X \ , \ \varepsilon_i \ \mapsto \ \beta_{i\ ,1 \leq i \leq n} \quad . \end{aligned}$$

Comme

$$\forall 1 \leq i \leq n, \ \psi(\phi(\beta_i)) \ = \ \beta_i \ = \ \mathrm{Id}_X(\beta_i)$$

le lemme II.1.8 assure encore que

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

Le même argument assure que

$$\phi \ \circ \ \psi \ = \ \mathrm{Id}_{\mathbb{Z}^n (\text{resp. } A^n)} \ .$$

*ii) (**b)** $\Rightarrow$ **a**))*
Il suffit d'appliquer le lemme II.2.12.

*iii) (**a)** $\Rightarrow$ **c**))*
Est tautologique.

*iv) (**c)** $\Rightarrow$ **a**))*
Soit $\mathcal{B}$ une base de X et $S := \{s_1, \ldots, s_r\}$ une famille génératrice finie de X. Puisque $\mathcal{B}$ est une base, pour tout $1 \leq i \leq r$ il existe une partie finie $\mathcal{B}_i$ de $\mathcal{B}$ et une application

$$a_i \ : \ \mathcal{B}_i \ \to \ \mathbb{Z} (\text{resp. } A)$$

tels que

$$s_i \ = \ \sum_{\beta \ \in \ \mathcal{B}_i} a_i(\beta)\beta \ .$$

Or S étant une famillle génératrice de X, pour tout $x \in X$, il existe un

$$r - \text{uplet } x_{i\ ,1\leq i\leq r} \ \in \ \mathbb{Z} (\text{resp. } A),$$

d'éléments de $\mathbb{Z}$ (resp. A,) tel que

$$x \ = \ \sum_{i=1}^{r} x_i s_i \ .$$

Il en résulte que

$$x \ = \ \sum_{i=1}^{r} \sum_{\beta \ \in \ \mathcal{B}_i} x_i a_i(\beta)\beta \ .$$

Cela signifie exactement que $\bigcup_{i=1}^{r} \mathcal{B}_i$ est une famille génératrice de X. Comme c'est une union finie d'ensemble finis c'est un ensemble fini. Comme de plus c'est un sous-ensemble de $\mathcal{B}$ c'est une famille libre en vertu du lemme II.2.3.ii). C'est donc une base de cardinal fini de X.

Définition II.3.2 (Groupe abélien (resp. A-Module,) libre de type fini) Un groupe abélien (resp. A-module,) X vérifiant les assertions équivalentes de la proposition II.3.1 est dit *libre de type fini*.

Proposition II.3.3 *Étant donné un groupe abélien (resp. un A-module,) X, les assertions II.1.9.a) à II.1.9.c) sont encore équivalente au fait qu'il existe un groupe abélien (resp. A-module,) libre de type fini L et un morphisme surjectif $f \ : \ L \ \to \ X$.*

Proposition II.3.4 *Soient $(r, s) \ \in \ \mathbb{N} \times \mathbb{N}$ il existe un isomorphisme*

$$\phi \ : \ \mathbb{Z}^r \ \cong \ \mathbb{Z}^s \ (\textit{resp.}\ \phi \ : \ A^r \ \cong \ A^s$$

si et seulement si $r \ = \ s$.

***Preuve** : (cf. TD n° III, exercice B.)*

Corollaire II.3.5 *Si X est un groupe abélien (resp. A-module,) libre de type fini, il existe un entier $r \ \in \ \mathbb{N}$ et un isomorphisme*

$$X \ \cong \ \mathbb{Z}^r (\textit{resp.}\ A^r) \ .$$

L'entier r est alors uniquement déterminé par X.

Définition II.3.6 (Rang d'un groupe abélien (resp. A-module,) libre de type fini) Si X est un groupe abélien
(resp. A-module,) libre de type fini, l'entier r donné par le corollaire II.3.5 est appelé le *rang* de X noté $\mathrm{rg}(X)$. Il est égal au nombre d'éléments d'une base de X.

Remarque II.3.7 Il serait tentant ici encore de faire jouer au rang d'un groupe abélien (resp. A-module,) libre de type fini le rôle de la dimension d'un $\mathbb{K}$-espace vectoriel mais le rang n'a malheureusement pas d'aussi bonnes propriétés : par exemple deux groupes abéliens (resp. A-modules,) $Y \ \subset \ X$ de même rang ne sont pas nécessairement égaux (cf. II.12.3.question 3).)

Remarque II.3.8 On pourrait penser que les groupes abéliens (resp. A-modules,) libres de type fini ont tendance à se comporter comme des espaces vectoriels. Cependant même sous l'hypothèse *libre de type fini* un certains nombre de résultats ne se transposent pas du contexte des espaces vectoriels à celui des groupes abéliens (resp. A-modules :)

i) Une famille libre maximale n'et pas nécessairement une base (cf. II.12.3.question 1).)

ii) Un sous-groupe (resp. sous-A-module,) d'un groupe abélien (resp. A-module,) libre de type fini n'a pas nécessairement un supplémentaire (cf. II.12.3.question 2).)

iii) Une famille libre ne peut pas nécessairement se compléter en une base.

Les résultats positifs que nous pouvons cependant donner sont les suivants :

Proposition II.3.9 *Étant donné un groupe abélien (resp. A-module,) libre de type fini L, toute suite exacte*

$$0 \to Y \xrightarrow{i} X \xrightarrow{p} L \to 0$$

de groupes (resp. A-modules,) est scindée, (cf. I.9.11.i);) ce qui entraîne en particulier que Y possède un suplémentaire dans X isomorphe à L.

Preuve *: Soit $\lambda_{i\ ,1\leq i\leq r}$ une base de L. Le morphisme p étant surjectif, pour tout $1 \leq i \leq r$ il existe $\mu_i \in X$, tel que $p(\mu_i) = \lambda_i$. En vertu du lemme II.2.10, il existe un unique morphisme de groupes (resp. A-modules,)*

$$s : L \to X\ ,\ \lambda_i \mapsto \mu_{i\ ,1\leq i\leq r}\ .$$

Comme,

$$\forall 1 \leq i \leq r,\ p(s(\lambda_i)) = p(\mu_i) = \lambda_i = \mathrm{Id}_L(\lambda_i),$$

l'énoncé d'unicité dans le lemme II.2.10 assure que

$$p \circ s = \mathrm{Id}_L\ .$$

On laisse alors le lecteur établir, à partir des résultats du paragraphe I.9 que l'on a un isomorphisme

$$X \cong i(Y) \oplus s(L)\ .$$

Proposition II.3.10 *Soient L_1 et L_2 des groupes abéliens (resp. A-modules,) libres de rangs respectifs r_1 et r_2.*

i) $L_1 \times L_2$ est libre de rang $r_1 + r_2$.

ii) Si

$$0 \to L_1 \longrightarrow L \longrightarrow L_2 \to 0$$

est une suite exacte courte de groupes (resp. A-modules,) L est un groupe abélien (resp. A-module,) libre de rang $r_1 + r_2$.

iii) Soit L un groupe abélien (resp. A-module,) tel que $L = L_1 \oplus L_2$. Alors L est libre de rang $r_1 + r_2$.

Preuve *: On laisse le soin au lecteur de vérifier que les arguments qu'il connaît bien dans le cas des espaces vectoriels pour établir les points i) et iii) s'adaptent sans presque de modification au cas des groupes abéliens (resp. A-modules.)*

On déduit ii) de i), dans la mesure où, dès qu'on a une suite exacte $0 \to L_1 \longrightarrow L \longrightarrow L_2 \to 0$, L_2 étant libre celle-ci sera scindée, en vertu de la proposition II.3.9. Dans ce cas, en appliquant la proposition I.9.13, on disposera d'un isomorphisme $L \cong L_1 \times L_2$ permettant de conclure graçe à i).

Remarque II.3.11 L'énoncé II.3.10.ii) est sans doute l'énoncé le plus proche du théorème du rang que l'on puisse envisager. Si $f : X \to Y$ est un morphisme de groupes, il s'en déduit une suite exacte

$$0 \to \mathrm{Ker}\, f \longrightarrow X \longrightarrow \mathrm{Im}\, f \to 0\,.$$

Or si X et Y sont des groupes abéliens libres de type fini :
— $\mathrm{Ker}\, f$ est un groupe abélien libre de type fini comme sous-groupe de X (cf. II.4.6 ;)
— $\mathrm{Im}\, f$ est un groupe abélien libre de type fini comme sous-groupe de Y.
Il résulte alors de II.3.10.ii) que

$$\mathrm{rg}(X) = \mathrm{rg}(\mathrm{Ker}\, f) + \mathrm{rg}(\mathrm{Im}\, f)\,. \qquad \text{II.3.11.1}$$

Si bien entendu X et Y sont des $\mathbb{K}$-espaces vectoriels pour $\mathbb{K}$ un corps, l'égalité ci-dessus n'est autre que le théorème du rang.

Remarque II.3.12 (Attention ! !) Si le théorème du rang semble valoir encore pour des groupes abéliens (resp. A-modules,) libres de type fini, il faut prendre garde que ses corollaires fréquemment utilisés en algèbre linéaire ne sont plus tous valables dans le cas des groupes abéliens (resp. A-modules,) même libre de type fini.

i) (**Morphisme surjectif**)
Si $f : X \to X$ est un endomorphisme surjectif (ou même $f : X \to Y$ un morphisme entre groupes abéliens libres de même rang) l'égalité II.3.11.1 assure que $\mathrm{rg}(\mathrm{Ker}\, f) = 0$, et donc que f est injectif (cf. TD n° III, exercice A, question 2), b).)

ii) (**Morphisme injectif**)
Il n'est pas vrai en revanche qu'un endomorphisme

$$f : X \to X \text{ injectif}$$

(ou même un morphisme $f : X \to Y$ entre groupes abéliens (resp. A-modules,) libres de même rang) est nécessairement surjectif. L'égalité II.3.11.1 entraîne, en effet, que $\mathrm{rg}(\mathrm{Im}\, f) = \mathrm{rg}(Y)$, mais ce qui n'assure en aucun cas que $\mathrm{Im}\, f$ soit égal à Y (cf. TD n° III, exercice A, question 2), a).)

Nous avons déjà remarqué (cf. II.3.7,) que deux groupes abéliens (resp. A-moduleS,) libres de type fini, emboîtés, fussent-ils de même rang, ne sont pas nécessairement égaux. Les paragraphes II.11 et C expliquent complètement quelles peuvent être les positions relatives de deux objets dans ce cas.

II.4 . −Sous-groupe (resp. sous-A-module,) d'un groupe abélien (resp. A-module,) libre de type fini

Si l'on veut, dans ce paragraphe (II.4,) tenir compte des généralisations des énoncés sur les groupes abéliens, aux A-modules, il faut nécessairement supposer que A est un anneau *principal* (cf. I.12.2.) On pourrait juste penser que c'est une hypothèse de confort et qu'on pourrait éventuellement l'affaiblir. La preuve du lemme II.4.1 montre déjà qu'on aurait du mal à s'en passer mais la remarque II.4.9 et surtout la proposition II.4.10 assurent définitivement qu'il n'en est pas question !

Lemme II.4.1 *Si L est un groupe abélien (resp. A-module,) libre de rang 1 (cf. II.3.6,) et M un sous-groupe (resp. sous- A-module,) de L, alors M est un groupe abélien (resp. A-module,) libre de rang plus petit que* 1.

Preuve *: On dispose, en vertu du corollaire II.3.5, d'un isomorphisme*

$$\phi \,:\, \mathbb{Z}(\text{resp. } A) \,\cong\, L\,.$$

Pour tout sous-groupe (resp. sous-A-module,) $M \subset L$, puisque ϕ est un morphisme, en particulier surjectif, $M = \phi[\phi^{-1}(M)]$.

En outre $\phi(M)$ est un sous-groupe de $\mathbb{Z}$ (cf. I.5.1.ii),) (resp. sous-A-module de A (cf. A.5.1.ii).))

Or un sous-groupe de $\mathbb{Z}$ est un idéal de $\mathbb{Z}$ (resp. un sous-A-module de A un idéal de A (cf. A.3.2.b).)) Il existe donc $a \in \mathbb{Z}(\text{resp. } A)$ tel que

$$\phi^{-1}(M) \,=\, a\mathbb{Z}(\text{resp. } aA\,.)$$

Il s'ensuit que $\phi(a)$ est une base de M si $a \neq 0$. Ainsi soit $M = \{0\}$ soit M est le sous-groupe (resp. sous- A-module,) de L de base $\phi(a)$ donc de rang 0 ou 1.

Remarque II.4.2 Une fois établi le lemme II.4.1 ci-dessus, on imagine qu'on pourra obtenir un résultat analogue pour des groupes abéliens (resp. A-modules,) libres de rang quelconque par un argument de récurrence sur le rang.

Rappelons cependant que, si L est un groupe abélien (resp. A-module,) libre de rang $r+1$, (r étant un entier), muni d'une base $\lambda_i\,,_{0\leq i\leq r}$, que D désigne le sous groupe (resp. sous-A-module,) de L engendré par $\{\lambda_0\}$, et H le sous-groupe (resp. sous-A-module,) engendré par $\{\lambda_1, \ldots, \lambda_r\}$,) D et H sont bien entendu supplémentaires dans L. Cependant, pour un sous-groupe (resp. sous-A-module,) $X \subset L$, il n'est pas du tout certain, et même faux en général, que X soit somme directe de $X \cap D$, et $X \cap H$. Ce résultat est déjà faux dans le cas des espaces vectoriels même si dans ce dernier cas, on peut adapter la situation en choisissant D convenablement, c'est-à-dire en choisissant une famille libre que l'on complètera convenablement. On ne dispose pas, dans le cas des groupes abéliens (resp. A-modules,) (même libres de type fini) d'un équivalent du théorème de la base incomplète et le mieux qu'on pourra espérer, dans le cas déjà très particulier des anneaux principaux, est exposé aux paragraphe II.11 et C.

Sans choix particulier de la base $\lambda_i\,,_{0\leq i\leq r}$ de L, le « découpage » $L = D \oplus H$, permet cependant d'obtenir un « découpage » de tout sous-groupe abélien (resp. A-module,) X qui nous permettra de metre en œuvre un argument de récurrence :

Notation II.4.3 Soit $r \in \mathbb{N}^*$, un entier et L un groupe abélien (resp. A-module,) libre de rang $r+1$ et de base $\lambda_i\,,_{0\leq i\leq r}$. Soit D le sous-groupe (resp. sous-A-module,) de L engendré par $\{\lambda_0\}$ et H par $\{\lambda_1 \ldots, \lambda_r\}$.

Lemme II.4.4 *Avec les notations ci-dessus on a deux suites exactes (cf. I.9.1,) de groupes (resp. A-modules,) scindées :*

$$0 \to D \xrightarrow{i} L \xrightarrow{p} H \to 0 \qquad \text{II.4.4.1}$$

et

$$0 \to H \xrightarrow{j} L \xrightarrow{q} D \to 0\,. \qquad \text{II.4.4.2}$$

Preuve *: Il suffit de remarquer que, par construction, $L = D \oplus H$, et d'appliquer le théorème I.9.15.*

Remarque II.4.5 On pourrait utiliser indifféremment l'une ou l'autre des suites exactes II.4.4.1 ou II.4.4.2 pour établir le théorème II.4.6 et l'on choisira de développer la construction à partir de II.4.4.1. Néanmoins une relecture attentive du paragraphe I.9 montrerait que ces deux suites exactes sont en fait deux formulations d'un même résultat, à savoir que $L = D \oplus H$ et peuvent se déduire l'une de l'autre.

Théorème II.4.6 *Étant donné un groupe abélien (resp. A-module,) L libre de rang $r \in \mathbb{N}$, tout sous-groupe (resp. sous-A-module,) M de L est libre de rang s avec $s \leq r$.*

Preuve *: On raisonne par récurrence sur l'entier r. Si $r = 0, L = \{0\}$ et $M = \{0\}$, si bien que la conclusion est immédiate.*

Pour $r \in \mathbb{N}$ si L est libre de rang $r+1$, il existe un isomorphisme

$$L \cong \mathbb{Z}^{r+1} (\text{resp. } A^{r+1})$$

ou, ce qui revient au même (cf. II.3.1,) une base $\lambda_{i\ ,0\leq i\leq r}$ de L. On reprend les notations II.4.3 et l'on considère la suite exacte II.4.4.1. Étant donné un sous-groupe abélien (resp. A-module,) M de L, $P := p(M)$ est un sous-groupe (resp. sous-A-module,) de H. Le groupe abélien (resp. A-module,) H étant libre de rang r, on peut, par hypothèse de récurrence, supposer que P est un groupe abélien (resp. A-module,) libre de rang s avec $s \leq r$. Soit donc $\rho_{i\ ,1\leq i\leq s}$ une base de P.

Choisissons des antécédents des $\rho_{i\ ,1\leq i\leq s}$ dans M i.e. $\sigma_{i\ ,1\leq i\leq s}$ des éléments de M tels que

$$\forall 1 \leq i \leq s,\ p(\sigma_i) = \rho_i$$

(on dit parfois des relèvements des ρ_i.) Puisque l'image par p de la famille $\sigma_{i\ ,1\leq i\leq s}$ est une base de P, donc une famille libre, la famille $\sigma_{i\ ,1\leq i\leq s}$ est une famille libre. Le sous-groupe (resp. sous-A-module,) S de M engendré par $\{\sigma_1 \ldots, \sigma_s\}$ est donc un sous-groupe (resp. sous-A-module,) libre de rang s de M et de L.

Le groupe abélien (resp. A-module,) $E := M \cap D$ est un sous-groupe (resp. A-module,) de D. Puisque D est un groupe abélien (resp. A-module,) de rang 1, il résulte du lemme II.4.1 que E est un groupe abélien (resp. A-module,) libre de rang ≤ 1.

Si donc on établit (ce qui va être fait dans le lemme II.4.6.1,) que

$$M = E \oplus S,$$

il résulte de la proposition II.3.10.iii), que M est un groupe abélien (resp. A-module,) libre de rang inférieur ou égale à $s+1 \leq r+1$.

Lemme II.4.6.1

$$M = E \oplus S\,.$$

Preuve : *Pour tout* $x \in M$, $p(x) \in P$ *si bien qu'il existe* a_i ,$1 \leq i \leq s$ *tel que* $p(x) = \sum_{i=1}^{s} a_i \rho_i$ *si bien que :*

$$\begin{aligned} & p(x) - \sum_{i=1}^{s} a_i \rho_i = 0 \\ \Leftrightarrow \quad & p(x) - \sum_{i=1}^{s} a_i p(\sigma_i) = 0 \\ \Leftrightarrow \quad & p\big(x - \sum_{i=1}^{s} a_i \sigma_i\big) = 0 \\ \Leftrightarrow \quad & x - \sum_{i=1}^{s} a_i \sigma_i \in \operatorname{Ker} p = D . \end{aligned}$$

Pour tout $x \in M$, *il existe donc* $y \in S$ *tel que* $z := x - y \in D$. *Or* $x \in M$, $y \in S \subset M$ *donc*

$$z \in M \cap D = E .$$

Il est immédiat de voir que

$$S \cap E \subset S \cap D = \{0\}$$

si bien que

$$M = S \oplus E .$$

Remarque II.4.7 Une lecture attentive de la preuve du théorème II.4.6 et plus particulièrement de la preuve du lemme II.4.6.1 permettra de se rendre compte, qu'un certain nombre d'arguments donnés ici semblent l'avoir déjà été, en particulier dans les preuves des propositions II.3.9 et I.9.13 ; ce qui pourrait laisser penser que l'on peut rédiger la preuve du théorème II.4.6 de manière plus concise en faisant appel à ces résultats antérieurs :

En effet, en reprenant les notations de la preuve, considérons la restrictions $q := p_{|M}$ de p à M à valeurs dans $P := p(M)$. Le noyau de q est $E = M \cap D$ et l'on a donc une suite exacte

$$0 \to E \longrightarrow M \xrightarrow{q} P \to 0 . \qquad \text{II.4.7.1}$$

Le lemme II.4.1 dont il est bien entendu inenvisageable de se passer, assure alors que E est un groupe abélien (resp. A-module,) libre de rang inférieur ou égal à 1. Le groupe abélien (resp. A-module,) H étant libre de rang r et P un sous-groupe abélien (resp. A-module,) de H, l'hypothèse de récurrence assure que P est libre de rang inférieur ou égal à r. Il suffit alors d'appliquer la proposition II.3.9 pour conclure.

Corollaire II.4.8 (du théorème II.4.6) *i) Tout sous-groupe (resp. sous-*A*-module,)* Y *d'un groupe abélien (resp.* A*-module,) de type fini* X *est de type fini.*

Preuve : *Si* X *est de type fini il existe (cf. II.3.3,) un groupe abélien (resp.* A*(-module,) libre de type fini* L *et un morphisme surjectif* $p : L \to X$. *Alors l'image inverse* $p^{-1}(Y)$ *de* Y *dans* L *est un sous-groupe (resp. sous-* A*-module,) de* L. *Ce dernier étant libre de type fini,* $p^{-1}(Y)$ *est encore libre de type fini en vertu du théorème II.4.6. Or la restriction*

$$p_{|p^{-1}(Y)} : p^{-1}(Y) \to N$$

est un morphisme surjectif ce qui entraîne, en vertu de la proposition II.1.9 que Y *est de type fini.*

ii) Étant donnée une suite exacte de groupes abéliens (resp. A-modules,)

$$0 \to N \longrightarrow X \longrightarrow Q \to 0,$$

X est de type fini si et seulement si N et Q le sont.

***Preuve** : Si X est de type fini, Q l'est ausssi en vertu de la proposition II.1.9 et N en vertu du point i). L'assertion réciproque a été montrée dans la proposition II.1.11.iii).*

Remarque II.4.9 On pourrait donner une réciproque au théorème II.4.6 dont nous n'aurons pas d'usage particulier dans ce cours. Cependant soit A un anneau tel que tout sous-A-module d'un A-module libre de rang r est un A-module libre de rang inférieur ou égal à r. L'anneau A lui-même étant un A-module libre de rang 1, tout idéal de A étant un sous-A-module de A il est libre de rang plus petit que 1 ce qui signifie exactement qu'il est principal.

On peut même donner un énoncé plus fort :

Proposition II.4.10 *Réciproquement, si A est un anneau intègre tel que tout sous-A-module d'un A-module libre de type fini est libre de type fini, alors A est principal.*

***Preuve** : Considérons en effet un idéal $\mathfrak{I} \subset A$ de A. En tant que sous-A-module de A lui-même il est donc libre de type fini c'est-à-dire qu'il possède une base ε_i ,$1 \leq i \leq d$. Si $d > 1$,*

$$\varepsilon_1 \varepsilon_2 - \varepsilon_2 \varepsilon_1 = 0$$

ce qui contredit le fait que $\{\varepsilon_1, \varepsilon_2\}$ soit libre et entraîne donc $d \leq 1$ c'est-à-dire $\mathfrak{I}$ principal.

II.5 . −Ordre d'un élément,, exposant d'un groupe (cf. IV.2, A.7)

Dans tout ce paragraphe (II.5,) $(A,+)$ **est un groupe abélien. On note toujours** $\cdot\ :\ \mathbb{Z}\times A\ \to\ A$ **la loi externe définie en I.6.6, et qui donne à** A **sa structure de** $\mathbb{Z}$**-module (cf. A.1.11.i).)**

Lemme II.5.1 ((cf. IV.2.1, A.7.1)) *Pour tout*

$$x\ \in\ A\,\text{et}\,m\ \in\ \mathbb{Z},$$

il est équivalent que $nx\ =\ 0$, *ou que le morphisme de groupes*

$$\mathbb{Z}\ \to\ A\ ,\ m\ \mapsto\ mx \qquad \textit{II.5.1.1}$$

se factorise en un morphisme

$$\begin{array}{ccc} & & \mathbb{Z} \\ & & \downarrow \qquad \searrow_{m\mapsto mx} \\ \mathbb{Z}/n\mathbb{Z} & \to & A\ . \end{array} \qquad \textit{II.5.1.2}$$

Définition II.5.2 ((cf. IV.2.2, A.7.2)) i) (**Élément de torsion**)
Si x et n vérifient les conditions équivalentes du lemme II.5.1 ci-dessus, on dit que x est de n-*torsion*.
On dit que $x\ \in\ A$ est *de torsion* s'il existe $n\ \in\ \mathbb{Z}\,n\ \neq\ 0$, tel que x soit de n-torsion, *i.e.* tel que $nx\ =\ 0$.

ii) (**Partie de** n**-torsion**)
Pour tout $n\ \in\ \mathbb{N}^*$, on note

$$A[n]\ :=\ \{x\ \in\ A\ ;\ nx\ =\ 0\}$$

le sous-ensemble de A formé des éléments de n-torsion de A.
On appellera $A[n]$ la *partie de* n*-torsion* de A.
On dira que A est *de* n*-torsion* si $A\ =\ A[n]$.

iii) (**Ordre d'un élément**)
Pour tout $x\ \in\ A$, on dit que x est d'*ordre* n si le morphisme

$$\mathbb{Z}/n\mathbb{Z}\ \to\ A\ ,\ \overline{m}\ \mapsto\ mx\ \text{(cf. II.5.1.2)}$$

est injectif ou, ce qui revient au même, si $n\mathbb{Z}$ est le noyau $\mathrm{Ann}_{\mathbb{Z}}(x)$ du morphisme II.5.1.1.
Si x est d'ordre $n\ \neq\ 0$, n est aussi le nombre d'éléments de l'image du morphisme IV.2.1.2 qui est encore l'image du morphisme II.5.1.1 ou bien encore le sous-groupe $<\ x\ >$ de A engendré par x.

iv) (**Exposant d'un groupe**)
L'ensemble

$$\mathrm{Ann}_{\mathbb{Z}}(A)\ :=\ \bigcap_{x\ \in\ A}\mathrm{Ann}_{\mathbb{Z}}(x)\ =\ \{n\ \in\ \mathbb{Z}\,;\ \forall x\in A,\ n\cdot x\ =\ 0\}$$

est un sous-groupe, ou de manière équivalente un idéal de $\mathbb{Z}$ dont le générateur positif est usuellement appelé *exposant* du groupe A.

v) (**Partie de torsion**)
On note

$$\mathrm{Tor}_{\mathbb{Z}}(A)\ \text{ou tout simplement}\ \mathrm{Tor}\,(A)\ :=\ \bigcup_{n\ \in\ \mathbb{N}^*}A[n]$$

l'ensemble des éléments de torsion de A qu'on appelle la *partie de torsion* de A.

vi) (**Groupe de torsion**)
On dit que A est *de torsion* si

$$A \;=\; \mathrm{Tor}(A)\;.$$

vii) (**Groupe sans torsion**)
On dit que A est *sans torsion* si

$$\mathrm{Tor}(A) \;=\; \{0\}\;.$$

Proposition II.5.3 (Ordre et exposant (cf. IV.2.3, A.7.3)) *i) L'exposant du groupe A est le **Ppcm** des ordres des éléments de A. Il s'ensuit, en vertu du théorème de* LAGRANGE*, que si A est de cardinal fini, ce dernier est un multiple de l'exposant de A.*

ii) Un entier m est l'exposant du groupe abélien A, si et seulement si $m\mathbb{Z}$ est le noyau du morphisme naturel

$$\mathbb{Z} \;\to\; \mathrm{End}_{\mathbf{Gr}}(A)\;.\ \textit{(cf. I.6.8 .)}$$

iii) Pour A et B des groupes abéliens, si $A \;\subset\; B$, l'exposant de A divise celui de B.

iv) Pour tout morphisme de groupes $f \;:\; A \;\to\; B$ et tout $x \;\in\; A$, l'ordre de $f(x)$ dans B divise l'ordre de x dans A avec égalité si f est injectif.
Il s'ensuit que l'exposant de $f(A)$ divise l'exposant de A avec égalité si f est injectif.

Proposition II.5.4 (Propriétés de $A[n]$ (cf. IV.2.4, A.7.4)) *i) Pour tout $n \;\in\; \mathbb{N}$, $A[n]$ est un sous-groupe de A.*

***Preuve** : (cf. TD n° I, exercice A, question 1).)*

ii) Pour B un groupe abélien, $f \;:\; A \;\to\; B$ un morphisme de groupes, et tout $n \;\in\; \mathbb{N}$,

$$f(A[n]) \;\subset\; B[n] \text{ et } f[n] \;:=\; f_{|A[n]} \;:\; A[n] \;\to\; B[n]$$

est un morphisme de groupes, qui est un isomorphisme dès que f en est un.

***Preuve** : (cf. TD n° I, exercice A, question 2).)*

iii) Pour tout $(p,q) \;\in\; \mathbb{Z}\times\mathbb{Z}$ si p et q sont premiers entre eux

$$A[pq] \;=\; A[p] \;\oplus\; A[q]\;.$$

***Preuve** : (cf. TD n° I, exercice A, question 3).)*

iv) Si de plus A est d'exposant pq alors $A[p]$ (resp. $A[q]$,) est d'exposant p (resp. q.)

Proposition II.5.5 (Propriétés de la partie de torsion cf. A.7.5) *i) L'ensemble $\mathrm{Tor}(A)$ est un sous-groupe de A.*

***Preuve** : (cf. TD n° I, exercice A, question 1).)*

ii) Le quotient $A/\mathrm{Tor}(A)$ et sans torsion.

***Preuve** : (cf. TD n° I, exercice A, question 4).)*

iii) Pour tout groupe abélien B et tout morphisme $f : A \to B$,

$$f(\mathrm{Tor}(A)) \subset \mathrm{Tor}(B) \text{ et } f_{|\mathrm{Tor}(A)} : \mathrm{Tor}(A) \to \mathrm{Tor}(B)$$

est un morphisme de groupes qui est un isomorphisme dès que f en est un.

***Preuve** : (cf. TD n° I, exercice A, question 2).)*

iv) Si A est d'exposant strictement positif (i.e. $\mathrm{Ann}_{\mathbb{Z}}(a) \neq \{0\}$,) A est de torsion.

Remarque II.5.6 La réciproque du point II.5.5.iv) n'est en revanche pas vraie en général : Par exemple pour tout $\frac{a}{b} \in \mathbb{Q}/\mathbb{Z}$, $b\frac{a}{b} \in \mathbb{Z}$ c'est-à-dire que $b\frac{a}{b} = 0$ dans $\mathbb{Q}/\mathbb{Z}$. Cependant pour tout $n \in \mathbb{N}^*$, $a \in \mathrm{Ann}_{\mathbb{Z}}(\frac{1}{n})$ si et seulement si $a \in n\mathbb{Z}$, ce qui entraîne que

$$\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) \subset \bigcap_{n \in \mathbb{N}^*} n\mathbb{Z} = \{0\}\,.$$

En revanche si A est de type fini, on a la proposition suivante :

Proposition II.5.7 ((cf. IV.2.5, A.7.6)) *Si A est de type fini (cf. II.1.5,) A est de torsion si et seulement si A est d'exposant strictement positif.*

Proposition II.5.8 (cf. IV.2.6) *Un groupe abélien est de type fini et de torsion si et seulement s'il est fini.*

***Preuve** : (cf. TD n° III, exercice D.)*

II.6 . −Structure des groupes abéliens de type fini (cf. B.1)

Proposition II.6.1 ((cf. B.1.1)) *Un groupe abélien libre (cf. II.2.8,) est sans torsion (cf. II.5.2.vii).)*

Preuve *: Soit L un groupe abélien libre de base $\mathcal{B}$. Pour tout $x \in L, x \neq 0, a \in \mathrm{Ann}_{\mathbb{Z}}(x)$, (i.e. $a \cdot x = 0$.) Or il existe une partie finie $\mathcal{B}_x \subset \mathcal{B}$ et une application $\xi : \mathcal{B}_x \to \mathbb{Z}$ non identiquement nulle, tels que*

$$x = \sum_{\beta \in \mathcal{B}_x} \xi(\beta)\beta \, .$$

Il s'ensuit que $ax = 0$ entraîne

$$\sum_{\beta \in \mathcal{B}_x} a\xi(\beta)\beta = 0 \, .$$

Or $\mathcal{B}_x$ est une partie d'une famille libre donc est libre (cf. II.2.3.ii).) Il s'ensuit que

$$\forall \beta \in \mathcal{B}_x, \; a\xi(\beta) = 0 \, .$$

L'élément x n'étant pas nul il existe $\beta \in \mathcal{B}_x$ tel que $\xi(\beta) \neq_0$. Puisque $\mathbb{Z}$ est intègre, $a\xi(\beta) = 0$ entraîne $a = 0$ et finalement

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{0\}$$

ce qui assure que L est sans torsion.

On peut enfin donner la réciproque attendue, dans le cas des anneaux principaux à la proposition II.6.1 :

Théorème II.6.2 ((cf. B.1.2)) *Un groupe abélien A de type fini (cf. II.1.5,) est libre (cf. II.2.8,) si et seulement s'il est sans torsion (cf. II.5.2.vii).)*

Preuve *: Le fait qu'un groupe abélien libre est sans torsion découle de la proposition II.6.1.*

Réciproquement, soit A un groupe abélien de type fini et sans torsion. Il existe une partie génératrice finie $\alpha_{i\,,1\leq i\leq m}$ de A. Par ailleurs pour tout $a \in \mathbb{Z}$, $a\alpha_i = 0$ entraîne $a = 0$, puisque A est sans torsion. L'ensemble des parties libres de $\alpha_{i\,,1\leq i\leq m}$, est donc non vide puisque $\{\alpha_i\}$ est libre pour tout i. Il existe donc une partie libre maximale de $\alpha_{i\,,1\leq i\leq m}$ qu'on peut noter, quite à renuméroter $\alpha_{i\,,1\leq i\leq n}$ $n \leq m$.

Notons $B := \mathrm{Vect}\{\alpha_{i\,,1\leq i\leq n}\}$ le sous-groupe de A engendré par $\{\alpha_1, \ldots, \alpha_n\}$ qui est un groupe abélien libre de rang n.

Lemme II.6.2.1 *Pour tout $n < k \leq m$, il existe*

$$a_k \in \mathbb{Z} \setminus \{0\} \text{ tel que } a_k\alpha_k \in B \, .$$

Preuve (du lemme II.6.2.1)*: Pour tout $n < k \leq m$, la famille $\{\alpha_{i\,,1\leq i\leq n}\} \cup \{\alpha_k\}$ est liée par maximalité de $\alpha_{i\,,1\leq i\leq n}$. Il existe donc $a_{i\,,1\leq i\leq n} \in A$ et $a_k \in A$ non tous nuls, tels que $\sum_{i=1}^{n} a_i\alpha_i + a_k\alpha_k = 0$. Or puisque $\alpha_{i\,,1\leq i\leq n}$ est libre, $a_k \neq 0$. De plus*

$$a_k\alpha_k = -\sum_{i=1}^{n} a_i\alpha_i \in B \, .$$

Soit

$$a := \prod_{i=n+1}^{m} a_i \text{ et} \lambda : A \to A\,,\ x \mapsto a \cdot x$$

(où les a_i ,$n+1 \leq i \leq m$ sont définis par le lemme II.6.2.1.) Notons que si $n = m$, la démonstration est déjà terminée puisque $A = B$, mais qu'on peut n'en pas tenir compte en posant dans ce cas $a = 1$ et poursuivre comme nous allons le faire.

Lemme II.6.2.2 *L'application λ définie ci-dessus est un morphisme injectif de groupes à valeurs dans B.*

***Preuve** (**du lemme II.6.2.2**): D'abord il est clair que λ est un morphisme.*

Ensuite $\lambda(x) = 0 \Leftrightarrow ax = 0$. Comme A est sans torsion et que $a \neq 0, \operatorname{Ker}\lambda = \{0\}$.

Enfin pour tout $x \in A$, il existe x_i ,$1 \leq i \leq m \in A$ tel que $x = \sum_{i=1}^{m} x_i\alpha_i$. Il s'ensuit que :

$$\begin{aligned} \lambda(x) &= ax \\ &= \sum_{i=1}^{m} ax_i\alpha_i \\ &= a\sum_{i=1}^{n} x_i\alpha_i + \sum_{i=n+1}^{m} x_i a\alpha_i\ . \end{aligned}$$

Or $a\sum_{i=1}^{n} x_i\alpha_i \in B$ par définition et $\sum_{i=n+1}^{m} x_i a\alpha_i \in B$ en vertu du lemme II.6.2.1. Il s'ensuit que $\lambda(x) \in B$.

D'après le lemme ci dessus, λ induit donc un isomorphisme de A sur $\operatorname{Im}\lambda \subset B$. Or B étant un groupe abélien libre de type fini, le théorème II.4.6, entraîne qu'il en est de même de $\operatorname{Im}\lambda$ et donc de A.

Proposition II.6.3 ((cf. B.1.3)) *Soit A un groupe abélien de type fini et $\operatorname{Tor}(A)$ son sous-groupe de torsion (cf. II.5.5.i),) et $p : A \to L := A/\operatorname{Tor}(A)$ la surjection canonique. Alors :*

i) Le sous-groupe $\operatorname{Tor}(A)$ de A est de type fini.

***Preuve** : (cf. II.4.8.i).)*

ii) Le groupe abélien L est libre de type fini.

***Preuve** : Le groupe L est de type fini en vertu de la proposition II.1.9, est sans torsion grâce à la proposition II.5.5.ii) et donc libre, de type fini, en vertu du théorème II.6.2.*

iii) La suite exacte

$$0 \to \operatorname{Tor}(A) \longrightarrow A \xrightarrow{p} L \to 0$$

est sindée (cf. I.9.11.i),) si bien que p définit un isomorphisme

$$A \cong \operatorname{Tor}(A) \oplus L\ .$$

***Preuve** : Puisque L est un groupe abélien libre en vertu de ii), la suite exacte*

$$0 \to \operatorname{Tor}_A(M) \longrightarrow M \xrightarrow{p} L \to 0$$

est sindée en vertu de la proposition II.3.9. L'isomorphisme $A \cong \operatorname{Tor}(A) \oplus L$ provient alors de la proposition I.9.13.

Théorème II.6.4 (Structure des groupes abéliens de type fini (cf. B.1.4)) *Soit A un groupe abélien de type fini (cf. II.1.5.)*

i) Il existe un groupe abélien T de type fini et de torsion (cf. II.5.2.vi),) (i.e. en vertu de II.5.8 un groupe abélien fini,) et un groupe abélien libre de type fini (cf. II.3.2,) L tels que

$$A \cong T \times L .$$

***Preuve** : (cf. II.6.3.iii).)*

ii) Le couple (T, L) est unique au sens où T est isomorphe au sous-groupe de torsion $\mathrm{Tor}(A)$ de A et s'il existe L_1 et L_2 tels que

$$A \cong T \times L_1 \cong T \times L_2$$

L_1 et L_2 sont isomorphe et ont donc en particulier même rang.

***Preuve** : Soit T un groupe abélien de type fini et de torsion, L un groupe abélien libre de type fini et*

$$f : T \times L \cong A \text{ un isomorphisme } .$$

$*$) (***Construction d'un morphisme** $g : L \to A/\mathrm{Tor}(A)$)*

Le sous-groupe $T \subset T \times L$ (cf. I.7.6,) est de torsion dans $T \times L$, son image $f(T)$ est donc un sous-groupe de $\mathrm{Tor}(A)$ en vertu du lemme II.5.5.iii). Si $p : A \to A/\mathrm{Tor}(A)$ désigne la surjection canonique $\mathrm{Ker}\, p = \mathrm{Tor}(A)$, si bien que $p \circ f$ se factorise en un morphisme

$$g : (T \times L)/T \to A/\mathrm{Tor}(A) .$$

Or le produit $T \times L$ donne lieu, en vertu de la proposition I.7.6 ou de sa reformulation dans le théorème I.9.15, à une suite exacte

$$0 \to T \longrightarrow T \times L \xrightarrow{q} \to 0L$$

rendant isomorphes L et $T \times L/T$. On peut donc considérer qu'on a un morphisme

$$g : L \to A/\mathrm{Tor}(A) \text{ tel que } g \circ q = p \circ f .$$

†) (***Un « morphisme de suites exactes »**)*

En notant $h := f_{|T}$, la restriction de f à T, nous pouvons récapituler les informations dont nous disposons dans le diagramme commutatif à lignes exactes suivant :

$$\begin{array}{ccccccccc} 0 \to & T & \xrightarrow{j} & T \times L & \xrightarrow{q} & L & \to 0 & & \\ & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & [2] & (1) \\ 0 \to & \mathrm{Tor}(A) & \xrightarrow{i} & A & \xrightarrow{p} & A/\mathrm{Tor}(A) & \to 0 . & & \end{array}$$

‡) (*g **est surjectif et** h **injectif**)*

Or $p \circ f$ étant surjectif et $g \circ q = p \circ f$, g est surjectif. De même $i \circ h = f \circ j$ et $f \circ j$ étant injectif, h est injectif.

2. Il est d'usage d'appeler un tel diagramme un *morphisme de suites exactes* mais il n'est vraiement pas nécessaire, dans l'immédiat tout du moins, de s'encombrer l'esprit avec une pareille terminologie.

§) (g ***est injectif***)

Pour tout $x \in L$, il existe $y \in T \times L$ tel que $x = q(y)$. Il s'ensuit que $g(x) = 0$ entraîne $g[q(y)] = 0$ c'est-à-dire que $p[f(y)] = 0$ donc

$$f(y) \in \operatorname{Ker} p = \operatorname{Tor}(A) .$$

Il s'ensuit que (cf. II.5.5.iii),) $y = f^{-1}[f(y)]$ est de torsion dans $T \times L$. Il en résulte, toujours en vertu de loc. cit., que $x = q(y)$ est de torsion dans L. Or L étant libre il est sans torsion (cf. II.6.1,) si bien que $x = 0$. On en conclut que g est injectif.

¶) (h ***est surjectif***)

Quiconque connaîtrait le lemme du serpent conclurait immédiatement du fait que g est injectif et f surjectif, que h est surjectif[3].

Soit donc $x \in \operatorname{Tor}(A)$, et $i(x)$ qu'on peut continuer à noter x son image dans A. Autrement dit, soit x un élément de torsion de A. Son image $f^{-1}(x)$ dans $T \times L$ est encore un élément de torsion ce qui entraîne que $q[f^{-1}(x)]$ est de torsion dans L qui est sans torsion. Il s'ensuit donc que $q[f^{-1}(x)] = 0$, c'est-à-dire que

$$f^{-1}(x) \in \operatorname{Ker} q = T$$

c'est-à-dire que $f^{-1}(x)$ est un antécédent pour x par h ce qui assure que h est surjectif.

‖) (***Conclusion***)

Il résulte de ce qui précède que g et h sont des isomorphismes ; ce qui prouve le résultat.

3. On ne supposera pas acquis ce résultat.

II.7 . −Rang d'un groupe abélien de type fini

On a défini le *rang* d'un groupe abélien (resp. A-module,) libre de type fini en II.3.6. On peut étendre cette définition au groupe abéliens de type fini en général. Les résultats du présent paragraphe (II.7,) s'appliqent également aux A-modules de type fini en prenant bien soint de faire l'hypothèse que A est un anneau principal. Ce qui suit s'appuyant essentiellement sur le théorème II.6.4, si on en veut l'analogue pour les A-modules de type fini, il faut utiliser le théorème B.1.4.

Définition II.7.1 (Rang d'un groupe abélien (resp. A-module,) de type fini) L'énoncé d'unicité II.6.4.ii) (resp. B.1.4.ii),) permet de définir le rang d'un groupe abélien (resp. A-module,) de type fini X comme le rang au sens de la définition II.3.6, de sa partie libre $\mathcal{L}(X) := X/\mathrm{Tor}(X)$ et l'on notra

$$\mathrm{rg}(X) := \mathrm{rg}(\mathcal{L}(X)) .$$

On déduit de ce qui précède, une nouvelle caractérisation des groupe abéliens (resp. A-modules,) de torsion (cf. II.5.2.vi) (resp. A.7.2.vi) :))

Corollaire II.7.2 (du théorème II.6.4 (resp. B.1.4)) *Un groupe abélien (resp. A-module,) X de type fini, est de torsion si et seulement si* $\mathrm{rg}(X) = 0$.

La définition II.7.1 ne prend tout son sens que si on dispose d'un énoncé similaire à la proposition II.3.10, or :

Proposition II.7.3 *Soient X_1 et X_2 deux groupes abéliens (resp. A-modules,) de type fini.*

*i) (**(cf. II.3.10.i),**)*
On a :

$$\mathrm{rg}(X_1 \times X_2) = \mathrm{rg}(X_1) + \mathrm{rg}(X_2) .$$

***Preuve** : Écrivons*

$$X_1 = T_1 \times L_1 \text{ et } X_2 = T_2 \times L_2$$

grâce à II.6.4.i) (resp. B.1.4.i) avec T_i de type fini et de torsion et L_i libre de type fini (pour $i = 1$ ou 2.) On a alors

$$X_1 \times X_2 = (L_1 \times L_2) \times (T_1 \times T_2)$$

où $L_1 \times L_2$ est libre de rang

$$\mathrm{rg}(L_1) + \mathrm{rg}(L_2) = \mathrm{rg}(X_1) + \mathrm{rg}(X_2)$$

d'après la proposition II.3.10.i), et $T_1 \times T_2$ est de torsion. Le résultat d'unicité II.6.4.ii) (resp. B.1.4.ii),) permet de conclure.

*ii) (**cf. II.3.10.iii)**)*
Si X_1 et X_2 sont des sous-groupes (resp. sous-A-modules,) d'un groupe abélien (resp. A-module,) X tels que

$$X = X_1 \oplus X_2,$$
$$\mathrm{rg}(X) = \mathrm{rg}(X_1) + \mathrm{rg}(X_2)\,.$$

***Preuve** : Il suffit d'utiliser l'isomorphisme*

$$X \cong X_1 \times X_2$$

donné par le théorème I.9.15, pour conclure grâce au point i).

On aimerait également avoir l'analogue du point II.3.10.ii), ce qui sera obtenu dans la proposition II.7.9. On introduit d'abord quelques notations (cf. II.7.4,) puis on énonce et on démontre les lemmes II.7.6 à II.7.8, qui sont des cas particuliers de la proposition qu'on veut obtenir mais entrent également comme ingrédients dans sa preuve.

Notation II.7.4 Pour un groupe abélien (resp. A-module,) X de type fini, on note toujours $\mathrm{Tor}(X)$ sa partie de torsion et l'on notera $\mathcal{L}(X) := X/\mathrm{Tor}(X)$ qui est un groupe abélien (resp. A-module,) libre de type fini. Le théorème II.6.4 (resp. B.1.4,) assure alors qu'on a toujours une suite exacte :

$$0 \to \mathrm{Tor}(X) \xrightarrow{j_X} X \xrightarrow{p_X} \mathcal{L}(X) \to 0 \qquad \text{II.7.4.1}$$

où $j_X = \mathrm{Id}_{X|\mathrm{Tor}(X)}$ est l'inclusion naturelle et p_X la surjection canonique.
Dans la suite on suppose que X est un groupe abélien (resp. A-module,) tel qu'il existe une suite exacte :

$$0 \to N \xrightarrow{i} X \xrightarrow{q} Q \to 0 \text{ avec } N \text{ et } Q \text{ de type fini.} \qquad \text{II.7.4.2}$$

Si N et Q sont de type fini X l'est aussi en vertu de la proposition II.1.11.iii).
Le lemme II.5.5.iii) (resp. A.7.5.iii),) donne le carré commutatif

$$\begin{array}{ccc} \mathrm{Tor}(N) & \xrightarrow{\mathrm{Tor}(i)} & \mathrm{Tor}(X) \\ {\scriptstyle j(N)}\downarrow & & \downarrow{\scriptstyle j(X)} \\ N & \xrightarrow{i} & X \end{array} \qquad \text{II.7.4.3}$$

qui donnent par factorisation un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Tor}(N) & \xrightarrow{j_N} & N & \xrightarrow{p_N} & \mathcal{L}(N) & \to & 0 \\ & & {\scriptstyle \mathrm{Tor}(i)}\downarrow & & {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \mathcal{L}(i)} & & \\ 0 & \to & \mathrm{Tor}(X) & \xrightarrow{j_X} & X & \xrightarrow{p_X} & \mathcal{L}(X) & \to & 0 \end{array} \qquad \text{II.7.4.4}$$

Lemme II.7.5 *Le morphisme $\mathcal{L}(i)$ dans le diagramme II.7.4.4 est injectif.*

Preuve : *Pour tout* $x \in \mathcal{L}(N)$ *il existe* $y \in N$ *tel que* $p_N(y) = x$. *Alors*

$$\mathcal{L}(i)[p_N(y)] = 0 \Leftrightarrow p_X[i(y)] = 0$$

i.e.

$$i(y) \in \operatorname{Ker} p_X = \operatorname{Im} j_X .$$

Il existe donc $z \in \operatorname{Tor}(X)$ *tel que* $i(y) = j_X(z)$. *Or* $z \in \operatorname{Tor}(X)$ *c'est-à-dire que* z *est de torsion i.e.*

$$\exists a \in \mathbb{Z} \setminus \{0\} (\textit{resp. } A \setminus \{0\}),\ az = 0 .$$

Il s'ensuit que

$$i(ay) = ai(y) = aj_X(z) = j_X(az) = 0 .$$

Puisque i *est injectif,* $ay = 0$ *i.e.* y *est de torsion i.e.*

$$\exists w \in \operatorname{Tor}(N),\ y = j_N(w) .$$

Finalement

$$x = p_N(y) = p_N[j_N(w)] = 0 .$$

Lemme II.7.6 *Sous les conditions II.7.4.2, si* N *et* X *sont libres et* Q *de torsion,*

$$\operatorname{rg}(X) = \operatorname{rg}(N) .$$

Preuve : *Puisque* X *est libre de type fini, choisissons une base* $x_i\,,1\leq i\leq r}$ *de* X. *Puisque* Q *est de torsion,*

$$\forall 1 \leq i \leq r,\ \exists a_i \in \mathbb{Z} \setminus \{0\} (\textit{resp. } A \setminus \{0\}),\ a_i q(xm_i) = 0 .$$

Il s'ensuit que $q(a_i x_i) = 0$, *i.e.*

$$\forall 1 \leq i \leq r,\ a_i x_i \in N .$$

Puisque $x_i\,,1\leq i\leq r}$ *est une partie libre de* X, $a_i x_i\,,1 \leq i \leq r}$ *est encore une partie libre de* X. *Le sous-module* P *qu'elle engendre est donc libre de rang* r. *Or*

$$P \subset N \subset X$$

ce qui entraîne, en vertu du théorème II.4.6, que

$$r = \operatorname{rg}(P) \leq \operatorname{rg}(N) \leq \operatorname{rg}(X) = r$$

d'où finalement

$$\operatorname{rg}(X) = \operatorname{rg}(N) .$$

Lemme II.7.7 *Sous les conditions de II.7.4.2, si Q est de torsion*

$$\mathrm{rg}(X) \;=\; \mathrm{rg}(N)\;.$$

Preuve : *D'après le lemme II.7.5, $\mathcal{L}(i) \;:\; \mathcal{L}(N) \;\to\; \mathcal{L}(X)$ est injectif ; notons donc*

$$R \;:=\; \mathcal{L}(X)/\mathcal{L}(N) \text{ et } r \;:\; \mathcal{L}(X) \;\to\; R \text{ la surjection canonique}$$

si bien qu'on a une suite exacte :

$$0 \;\to\; \mathcal{L}(N) \xrightarrow{\mathcal{L}(i)} \mathcal{L}(N) \xrightarrow{\;r\;} R \;\to\; 0\;. \qquad \textit{II.7.7.1}$$

Or

$$r \circ p_X \circ i \;=\; r \circ \mathcal{L}(i) \circ p_N \;=\; 0$$

si bien qu'il existe un morphisme

$$t \;:\; Q \;\to\; R \text{ tel que } t \circ q \;=\; r \circ p_X\;;$$

en d'autres termes qu'on a le diagramme commutatif suivant à lignes exactes :

$$\begin{array}{ccccccccc}
0 & \to & N & \xrightarrow{\;i\;} & X & \xrightarrow{\;q\;} & Q & \to & 0 \\
 & & {\scriptstyle p_N}\downarrow & & {\scriptstyle p_X}\downarrow & & \downarrow{\scriptstyle t} & & \\
0 & \to & \mathcal{L}(N) & \xrightarrow{\mathcal{L}(i)} & \mathcal{L}(X) & \xrightarrow{\;r\;} & R & \to & 0\;.
\end{array}$$

Cette dernière condition entraîne, puisque $r \circ p_X$ est surjectif, que r est surjectif. Ceci entraîne que R est de torsion.

On peut alors appliquer le lemme II.7.6 à la suite II.7.7.1 qui donne alors

$$\mathrm{rg}\big(\mathcal{L}(X)\big) \;=\; \mathrm{rg}\big(\mathcal{L}(N)\big)$$

c'est-à-dire

$$\mathrm{rg}(X) \;=\; \mathrm{rg}(N)\;.$$

Lemme II.7.8 *Sout les conditions de II.7.4.2, si Q est libre (de type fini,)*

$$\mathrm{rg}(X) \;=\; \mathrm{rg}(N) \;+\; \mathrm{rg}(Q)\;.$$

Preuve : *Si Q est libre, la suite exacte*

$$0 \;\to\; N \xrightarrow{\;i\;} X \xrightarrow{\;q\;} Q \;\to\; 0 \textit{ (cf. II.7.4.2 ,)}$$

est scindée (cf. II.3.9 ;) on a donc un isomorphisme

$$X \;\cong\; N \;\oplus\; Q$$

et le résulta découle alors du point II.7.3.ii).

Proposition II.7.9 *Soit X un groupe abélien (resp. A-module,) tel qu'on ait une suite exacte*

$$0 \to N \xrightarrow{i} X \xrightarrow{q} Q \to 0 \text{ (cf. II.7.4.2 ,)}$$

où N et Q sont des groupes abéliens (resp. A-moduless) de type fini, alors X est de type fini et

$$\mathrm{rg}(X) = \mathrm{rg}(N) + \mathrm{rg}(Q)\,.$$

Preuve *: Écrivons une décomposition de*

$$0 \to \mathrm{Tor}(Q) \xrightarrow{j_Q} Q \xrightarrow{p_Q} \mathcal{L}(Q) \to 0 \text{ (cf. II.7.4.1)}$$

où $\mathcal{L}(Q)$ est libre et $\mathrm{Tor}(Q)$ de torsion. Cette suite étant scindée on peut en fait écrire une suite exacte

$$0 \to \mathcal{L}(Q) \xrightarrow{\ell} Q \xrightarrow{t} \mathrm{Tor}(Q) \to 0 \text{ (cf. I.9.9 .)}$$

Notons alors $P := q^{-1}[\ell(\mathcal{L}(Q))]$ si bien que $q_{|P}$ donne un morphisme surjectif $p : P \to \mathcal{L}(Q)$ de noyau N (cf. I.8.16.)

On a donc un diagramme commutatif à lignes et colonnes exactes :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & N & \xrightarrow{j} & P & \xrightarrow{p} & \mathcal{L}(Q) & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_N}\downarrow & & {\scriptstyle \mathrm{Id}_{X\,|P}}\downarrow & & \downarrow{\scriptstyle \ell} & & \\
0 & \to & N & \xrightarrow{i} & X & \xrightarrow{q} & Q & \to & 0 \\
 & & {\scriptstyle 0}\downarrow & & {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle t} & & \\
 & & 0 & \to & R & \to & \mathrm{Tor}(Q) & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \qquad \text{II.7.9.1}$$

où l'isomorphisme $R \cong \mathrm{Tor}(Q)$ n'est autre que celui du corollaire I.8.15.iii).

En appliquant le lemme II.7.7 à la suite exacte verticale centrale dans le diagramme II.7.9.1, puisque R est de torsion, on obtient

$$\mathrm{rg}(X) = \mathrm{rg}(P)\,.$$

En appliquant alors le lemme II.7.8 à la ligne horizontale du haut dans le diagramme II.7.9.1, puisque $\mathcal{L}(Q)$ est libre, on obtient

$$\mathrm{rg}(X) = \mathrm{rg}(P) = \mathrm{rg}(N) + \mathrm{rg}\big(\mathcal{L}(Q)\big) = \mathrm{rg}(N) + \mathrm{rg}(Q)\,.$$

II.8 . –Décomposition p-primaire (cf. IV.3, B.2)

Notation II.8.1 (cf. B.2.1) Pour un groupe abélien A, $p \in \mathbb{P}$ et $n \in \mathbb{N}$, on note

$$A[p^n] = \{x \in A \,;\, p^n x = 0\} \text{ sa partie de } p^n \text{ torsion (cf. II.5.2.v) ,)}$$

Définition II.8.2 (Composante p-primaire (cf. IV.3.1, B.2.2)) Pour A un groupe abélien et $p \in \mathbb{P}$, la *composante p-primaire* de A est

$$A[p^\infty] := \bigcup_{n \in \mathbb{N}} A[p^n]$$

qui est un sous-groupe de A en vertu de la proposition I.3.12.iii).

Théorème II.8.3 (de décomposition primaire (cf. IV.3.2, B.2.3)) *Étant donné un groupe abélien fini de cardinal n et d'exposant m (cf. II.5.2.iv),)*

$$\forall p \in \mathbb{P},\ A[p^\infty] = A[p^{v_p(m)}] = A[p^{v_p(n)}] \,; \qquad \textit{II.8.3.1}$$

de plus, on a des isomorphismes naturels (donnés par l'inclusion des sous-groupes :)

$$\bigoplus_{p \in \mathcal{S}(m)} A[p^\infty] \cong A \,; \qquad \textit{II.8.3.2}$$

$$\bigoplus_{p \in \mathcal{S}(n)} A[p^\infty] \cong A \,. \qquad \textit{II.8.3.3}$$

Preuve *: (cf. TD n° I, exercice A, question 10).)*

Corollaire II.8.4 (cf. B.2.5) *Étant donné un groupe abélien fini A d'exposant m, pour tout $p \in \mathcal{S}(m)$, il existe $x \in A$ d'ordre $p^{v_p(m)}$.*

Preuve *: Puisque $A[p^{v_p(m)}]$ s'injecte dans A, en vertu du théorème II.8.3, et que l'ordre se conserve par injection (cf. II.5.3.iv),) on peut supposer que $A = A[p^{v_p(m)}]$.*

On remarque alors que, pour tout $x \in A$ l'ordre de x est p^k avec $k \leq v_p(m)$. L'exposant de A étant le ***Ppcm*** *des ordres des éléments de A (cf. II.5.3.i),) il s'ensuit qu'il existe $x \in A$ d'ordre $p^{v_p(m)}$.*

II.9 . −Groupes cycliques (cf. IV.4, B.3)

Proposition II.9.1 (Groupes cycliques (cf. IV.4.1, B.3.1)) *Soit A un groupe abélien. Les assertions suivantes sont équivalentes :*

a) A est fini et $\#(A)$ est l'exposant de A (cf. II.5.2.iv).)

ii) A est fini et il existe $a \in A$ d'ordre $\#(A)$;

c) Le groupe A est monogène et fini.

d) Le groupe A est monogène (cf. II.1.7,) engendré par un élément d'ordre $d \in \mathbb{N}^*$ (cf. II.5.2.i).)

e) Il existe $d \in \mathbb{N}^*$ et un isomorphisme
$$\mathbb{Z}/d\mathbb{Z} \cong A .$$

f) Le groupe abéllien A est d'exposant $m \neq 0$ et isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

***Preuve** : Cet énoncé étant l'exact analogue de la proposition IV.4.1, certains arguments de preuve seront donnés ici tandis que d'autres seront donnés dans la preuve de IV.4.1 laissant le lecteur faire le parallèle entre ces deux preuves et les compléter.*

*i) (**a)** $\Rightarrow$ **ii)**)*
(cf. IV.4.1.)

*ii) (**ii)** $\Rightarrow$ **c)**)*
(cf. IV.4.1.)

*iii) (**c)** $\Rightarrow$ **d)**)*
Immédiat.

*iv) (**d)** $\Rightarrow$ **e)**)*
(cf. IV.4.1.)

*v) (**e)** $\Rightarrow$ **a)**)*
Découle du fait que $1_{\mathbb{Z}/d\mathbb{Z}}$ est précisément d'ordre d.

*vi) (**f)** $\Leftrightarrow$ **e)**)*
Est immédiat.

Définition II.9.2 (Groupes cycliques (cf. IV.4.2, B.3.2)) Un groupe vérifiant les assertions équivalentes de la proposition II.9.1 est un *groupe cyclique*. Un tel groupe est nécessairement abélien.

Proposition II.9.3 (Sous-groupe cyclique (cf. IV.4.5, B.3.5)) *Un groupe abélien A possède un sous-groupe cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$ si et seulement si A contient un élément d'ordre d.*

Proposition II.9.4 (Théorème chinois des restes (cf. IV.4.6, B.3.6)) *Si A est un groupe cyclique d'exposant m avec $m = pq$, p et q premier entre eux alors*

$$A \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} .$$

Remarque II.9.4.1 C'est exactement le théorème II.8.3 dans le cas cyclique.

Corollaire II.9.5 ((cf. IV.4.7, B.3.7)) *Soit A un groupe abélien $(x, y) \in A \times A$ d'ordres respectifs p et q avec p et q premiers entre eux, alors il existe $z \in A$ d'ordre pq.*

Preuve *: On a des morphismes injectifs*

$$\begin{array}{ccc} \mathbb{Z} & & \\ {\scriptstyle \pi_p}\downarrow & \searrow_{n\mapsto nx} & \\ \mathbb{Z}/p & \xrightarrow[\pi_p]{} & A \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{Z} & & \\ {\scriptstyle \pi_q}\downarrow & \searrow_{n\mapsto ny} & \\ \mathbb{Z}/q & \xrightarrow[\pi_q]{} & A \end{array} \qquad \textit{(cf. II.9.3 .)}$$

Le morphisme

$$\mathbb{Z} \times \mathbb{Z} \to A\ ,\ (m, n) \mapsto mx + ny$$

se factorise donc en un morphisme

$$\phi\ :\ \mathbb{Z}/p \times \mathbb{Z}/q \to A\ .$$

Or :

$$\begin{array}{lrcl} \forall (\alpha, \beta) = (\pi_p(m), \pi_q(n)) \in \mathbb{Z}/p \times \mathbb{Z}/q, & \phi(\alpha, \beta) & = & 0 \\ \Leftrightarrow & mx + ny & = & 0\ . \end{array}$$

Or

$$x \in A[p] \text{ et } y \in A[q]\ .$$

Comme $A[p]$ et $A[q]$ sont en somme directe (cf. II.5.4.iii),)

$$\begin{array}{rrcl} & mx + ny & = & 0 \\ \Leftrightarrow & mx = 0 & \text{et} & ny = 0 \\ \Leftrightarrow & p|m & \text{et} & q|n \\ \Leftrightarrow & \alpha = 0 & \text{et} & \beta = 0\ ; \end{array}$$

si bien que ϕ est injectif.

Enfin on dispose d'après le théorème chinois des restes, d'un isomorphisme

$$\gamma\ :\ \mathbb{Z}/(pq) \cong \mathbb{Z}/p \times \mathbb{Z}/q\ .$$

Le composé $\phi \circ \gamma$ est donc un morphisme injectif

$$\mathbb{Z}/(pq) \hookrightarrow A$$

ce qui donne, grâce encore à II.9.3 un élément d'ordre pq dans A.

II.10 . –Théorème de structure des groupes abéliens finis (cf. IV.11, B.6)

Notation II.10.0 ((cf. IV.11.0, B.6.0)) Dans tout ce paragraphe (II.10,) A est un groupe abélien fini d'exposant m. Rappelons (cf. II.5.8,) qu'il revient au même de demander que A soit de type fini (cf. II.1.5,) et de torsion (cf. II.5.2.vi).) En particulier A est d'exposant $m > 0$ (cf. II.5.7.)

Proposition II.10.1 (Existence d'un élément d'ordre maximal m (cf. IV.11.1, B.6.3)) *Il existe un élément*

$$a \in A \text{ d'ordre } m$$

i.e. un sous-groupe de A isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Preuve : *On a :*

$$A \cong \bigoplus_{p \in \mathcal{S}(m)} A[p^{v_p(m)}] \text{ (cf. II.8.3.2 .)}$$

On sait en outre, grâce au corollaire II.8.4, que, pour tout $p \in \mathcal{S}(m)$, il existe $x_p \in A$ d'ordre $p^{v_p(m)}$. Puisque $\mathcal{S}(m)$ est un ensemble fini, un argument de récurrence et le corollaire II.9.5 permettent de conclure.

Notation II.10.2 ((cf. IV.11.2, B.6.4)) Soit $C \subset A$ un sous-groupe cyclique de A isomorphe à $\mathbb{Z}/m\mathbb{Z}$ et construit grâce à la proposition II.10.1 ci-dessus. On note $Q := A/C$ si bien qu'on a une suite exacte :

$$0 \to C \xrightarrow{i} A \xrightarrow{q} Q \to 0 \,. \qquad \text{II.10.2.1}$$

Proposition II.10.3 (cf. IV.11.3) *Dans la suite exacte II.10.2.1, si Q et cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$, la surjection canonique q possède une section (cf. I.9.11.i),) i.e. il existe un morphisme de groupes*

$$s : Q \to A \text{ tel que } q \circ s = \mathrm{Id}_Q \,.$$

On déduit alors naturellement (cf. I.9.15,) de la suite exacte $0 \to C \xrightarrow{i} A \xrightarrow{q} Q \to 0$ un isomorphisme

$$A \cong C \times Q \,.$$

Preuve : *Soit y un générateur de Q (par example l'image de 1 par la surjection canonique*

$$\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \,.)$$

Soit $x \in A$ tel que $q(x) = y$, si bien que $q(x)$ est d'ordre d. Notons n l'ordre de x. On a alors :

$$d|n|m \,. \qquad \text{II.10.3.1}$$

Par ailleurs, $q(dx) = dq(x) = 0$, c'est-à-dire que

$$dx \in \mathrm{Ker}\, q = i(C) \cong \mathbb{Z}/m\mathbb{Z} \,.$$

Soit donc z un générateur de $\mathrm{Ker}\, q$, il existe $a \in \mathbb{Z}$ tel que

$$dx = az \,.$$

Or $x \in M$, *si bien que* $mx = 0$. *Il résulte alors de II.10.3.1 qu'il existe*

$$k \in \mathbb{Z} \text{ tel que } m = dk .$$

Il s'ensuit que

$$0 = mx = kdx = kaz .$$

Comme z *est d'ordre* m,

$$kaz = 0 \Rightarrow m|ka,$$

c'est-à-dire que $dk|ka$, *d'où finalement*

$$d|a .$$

Il existe donc $b \in \mathbb{Z}$ *tel que* $a = db$.
Soit alors $w := x - bz$. *Il en résulte que*

$$dw = dx - dbz = dx - az = 0 \text{ et donc que}$$

l'ordre de w *divise* d.
Le morphisme $\mathbb{Z} \to A$, $1 \mapsto w$ *se factorise donc en un morphisme*

$$s : Q \to A , y \mapsto w .$$

Or

$$q(s(y)) = q(w)\, q(x - bz) = q(x) = y$$

d'où puisque y *est un générateur de* Q,

$$q \circ s = \mathrm{Id}_Q .$$

Proposition II.10.4 (cf. IV.11.4) *Dans la suite exacte II.10.2.1, si*

$$Q \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z}$$

est isomorphe à un produit de groupes cycliques alors la surrjection canonique $q : A \to Q$ *possède une section* s, *qui induit un isomorphisme*

$$A \cong C \times Q \cong \mathbb{Z}/m\mathbb{Z} \times \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} .$$

Preuve : *Supposons donc qu'il existe*

$$r \in \mathbb{N} \text{ et } d_k \text{ ,} 1 \le k \le r \text{ , tels que } Q \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} .$$

Notons allors

$$\begin{array}{lrcl} \forall 1 \le k \le r, & & & \\ i_k : & \mathbb{Z}/d_k\mathbb{Z} & \longrightarrow & Q \\ & y & \longmapsto & (0, \dots, 0, y, 0, \dots, 0) \\ (\text{resp. } \chi_k : & Q & \longrightarrow & \mathbb{Z}/d_k\mathbb{Z} \\ & (0, \dots, 0, x, 0, \dots 0) & \longmapsto & x ,) \end{array}$$

le morphisme injectif (resp. surjectif) défini par la structure de produit de Q comme en I.7.6. On constate alors presque immédiatement que

$$\sum_{k=1}^{r} i_k \circ \chi_k \;=\; \mathrm{Id}_Q \;. \qquad \textit{II.10.4.1}$$

Soit

$$A_k \;:=\; q^{-1}[i_k(\mathbb{Z}/d_k\mathbb{Z})],$$

d'où un diagramme commutatif :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C & \xrightarrow{j_k} & A_k & \xrightarrow{q_k} & \mathbb{Z}/d_k\mathbb{Z} & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_C}\downarrow & & {\scriptstyle \mathrm{Id}_{A\,|\,A_k}}\downarrow & & \downarrow{\scriptstyle i_k} & & \\
0 & \to & C & \xrightarrow{i} & A & \xrightarrow{q} & Q & \to & 0
\end{array}$$

Puisque

$$C \;\subset\; A_k \;\subset\; A,$$

l'exposant m de C divise l'exposant de A_k divisant lui-même l'exposant de A encore égal à m ; si bien que m est encore l'exposant de A_k.

On peut donc appliquer la proposition II.10.3 à la suite exacte

$$0 \;\to\; C \xrightarrow{j_k} A_k \xrightarrow{q_k} \mathbb{Z}/d_k\mathbb{Z} \;\to\; 0$$

du diagramme ci-dessus. Pour tout $1 \;\leq\; k \;\leq\; r$ il existe donc un morphisme

$$s_k \;:\; \mathbb{Z}/d_k\mathbb{Z} \;\to\; A_k \text{ tel que } q_k \;\circ\; s_k \;=\; \mathrm{Id}_{\,\mathbb{Z}/d_k\mathbb{Z}} \;.$$

On définit alors :

$$s \;:=\; \sum_{k=1}^{r} s_k \circ \chi_k \;:\; Q \;\to\; A \;.$$

Il s'ensuit que :

$$\begin{aligned}
q \circ s \;&=\; q \circ \big(\sum_{k=1}^{r} s_k \circ \chi_k\big) \\
&=\; \sum_{k=1}^{r} q \circ s_k \circ \chi_k \\
&=\; \sum_{k=1}^{r} i_k \circ q_k \circ s_k \circ \chi_k \\
&=\; \sum_{k=1}^{r} i_k \circ \chi_k \\
&=\; \mathrm{Id}_Q \;,
\end{aligned}$$

la dernière égalité étant II.10.4.1.

Théorème II.10.5 (de structure des groupes abéliens finis (cf. IV.11.5, B.6.13)) *Étant donné un groupe abélien fini A, il existe un unique entier $r \in \mathbb{N}$ et un unique r-uplet $d_{k\ ,1\leq k\leq r} \in \mathbb{N}$ tels que*

$$A \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z},\ d_1 > 1 \text{et } \forall 1 \leq k \leq r-1,\ d_k | d_{k+1}\ .$$

Remarque II.10.5.1 Il est immédiat de constater que si les conditions ci-dessus sont satisfaites, d_r est l'exposant de A.

Preuve *:*

i) ***(Existence)***
Si $A = \{0\}, r = 0$ convient.
Le groupe abélien A étant fini, on peut appliquer la proposition II.10.1 qui donne la suite exacte

$$0 \to C \xrightarrow{\ i\ } A \xrightarrow{\ q\ } Q \to 0 \text{ (cf. II.10.2.1 ,)}$$

où $C \cong \mathbb{Z}/m\mathbb{Z}$ est un groupe cyclique.
Bien entendu, si $Q = \{0\}, C \cong A$ et le résultat est établi.
Sinon, il résulte du téhorème I.9.19 que

$$\#(Q) < \#(A)\ .$$

On peut alors faire lh'ypothèse de récurrence qu'il existe

$$r \in \mathbb{N}\ ,\ d_{k\ ,1\leq k\leq r} \in \mathbb{N}\ ,\ d_1 > 1 \text{ tels que } Q \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} \text{ et } \forall 1 \leq k \leq r-1,\ d_k | d_{k+1}\ .$$

La proposition II.10.4 permet alors d'écrire

$$A \cong Q \times C \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\ .$$

Le lemme II.5.3.iv) assure alors que $d_r | m$ ce qui achève la preuve.

ii) ***(Unicité)***
(cf. TD n° IV, exercice A, TD n° IV, exercice B)

Remarque II.10.5.3 Bien entendu le théorème II.10.5 peut être vu comme un corollaire du théorème B.6.13 puisque les arguments utilisés dans la preuve de ce dernier s'appliquent sans restriction aux groupes abéliens considérés comme $\mathbb{Z}$-modules.

On s'aperçoit néanmoins qu'ici, comme ce sera le cas en IV.11.5, un certain nombre d'argument est simplifié grâce notamment à des résultats come le théorème I.9.19.

Définition II.10.6 (Facteurs invariants (cf. IV.11.9, B.6.14)) Pour un groupe abélien fini A, les entiers

$$d_{k\ ,1\leq k\leq r} \text{ donnés par le théorème II.10.5}$$

ci-dessus sont appelés les *facteurs invariants* de A.

Il est d'usage de dire que lorsqu'on écrit alors

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

on a mis A sous sa *forme canonique*.

Corollaire II.10.7 ((cf. IV.11.10, B.6.15)) *i) Deux groupes abéliens finis sont isomorphes si et seulement si ils ont mêmes facteurs invariants.*

Preuve *: Soient A et B deux groupes abéliens finis. En vertu du théorème II.10.5.i), il existe*

$$r \in \mathbb{N} \text{ et } d_k\,,_{1\leq k\leq r} \text{ tels que } A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \text{ et } \forall 1 \leq k \leq r-1,\ d_{k+1}|d_k\ .$$

Un isomorphisme $B \cong A$ donne par composition un isomorphisme

$$B \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}\ .$$

Les $d_k\,,_{1\leq k\leq r}$ sont alors les facteurs invariants de B grâce à l'énoncé d'unicité B.6.13.2).

Réciproquement si $r \in \mathbb{N}$, $d_k\,,_{1\leq k\leq r}$, sont simultanément les facteurs invariants de A et B, les isomorphismes

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \text{ et } B \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

donne un isomorphisme

$$B \cong A$$

grâce à la proposition I.4.9 par exemple.

ii) Deux groupes abéliens de type fini sont isomorphes si et seulement si ils ont même rang (cf. II.7.1) et mêmes facteurs invariants.

Preuve *: Écrivons, grâce au théorème II.6.4,*

$$A = \mathrm{Tor}(A) \oplus \mathcal{L}(A) \text{ et } B = \mathrm{Tor}(B) \oplus \mathcal{L}(B)$$

où $\mathrm{Tor}(A)$ et $\mathrm{Tor}(B)$ (resp. $\mathcal{L}(A)$ et $\mathcal{L}(B)$) sont de type fini et de torsion (resp. libres de type fini.)

Si $\phi : A \cong B$ est un isomorphisme

$$\mathrm{Tor}(\phi) : \mathrm{Tor}(A) \cong \mathrm{Tor}(B) \text{ (cf. II.5.4.ii) ,)}$$

est un isomorphisme, ce qui assure, d'après le point i) que A et B ont les mêmes facteurs invariants.

Les isomorphismes

$$A \cong B \text{ et } \mathrm{Tor}(A) \cong \mathrm{Tor}(B)$$

assurent, graçe au théorème B.1.4.ii) que $\mathcal{L}(A)$ et $\mathcal{L}(B)$ sont isomorphes, c'est-à-dire que A et B ont même rang.

Réciproquement si A et B ont les mêmes facteurs invariants il résulte de i) qu'il existe un isomorphisme $\psi : \mathrm{Tor}(A) \cong \mathrm{Tor}(B)$. Si $\mathcal{L}(A)$ et $\mathcal{L}(B)$ sont libres de type fini et ont même rang, n ils sont tous les deux isomorphes à $\mathbb{Z}^n$ ce qui done, par composition, un isomorphisme

$$\phi : \mathcal{L}(A) \cong \mathcal{L}(B)\ .$$

On vérifie facilement que le morphisme

$$\psi + \phi : A = \mathrm{Tor}(M) \oplus \mathcal{L}(A) \to B = \mathrm{Tor}(B) \oplus \mathcal{L}(B)\ ,\ (x+y) \mapsto \psi(x) + \phi(y)$$

est un isomorphisme.

Exemple II.10.8 a) Bien évidemment, étant donnés des entiers naturels $a \neq b$, $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$ ne sont pas isomorphes parce qu'il n'ont pas le même nombre d'éléments et c'est le plus élémentaire des invariant qui se conserve par isomorphisme.

b) Il n'est nul besoin des résultats donnés ci-dessus pour établir non plus que $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes, puisqu'il y a un élément d'ordre 4 dans le premier et qu'il n'y en a pas dans le second et que l'ordre se conserve par isomorphismes (cf. II.5.3.iv).) On pourrait aussi remarquer, ce qui revient un peu au même, que ces deux groupes n'ont pas même exposant.

c) Il commence à devenir délicat, en s'abstenant d'utiliser le corollaire II.10.7.i), de déterminer si $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ sont ou non isomorphes. Il n'est pas impossible qu'en analysant finement le nombre d'éléments d'ordre respectifs 2 et 4 dans chacun d'entre eux on arrive finalement à les discriminer. Se faisant, cela revient à analyser la 2^n-torsion dans chacun de ces groupes et du coup à redémontrer (partiellement peut-être) dans un cas particulier le théorème II.10.5.

Bien entendu, le premier groupe ayant pour facteurs invariants $(2, 2, 4)$ et le second $(4, 4)$ il ne sont pas isomorphes.

d) Il se peut qu'on ait affaire à des groupes qui ne sont pas donnés sous forme canonique : par exemple $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Le premier groupe n'est pas donné sous forme canonique alors que le second l'est. En appliquant itérativement le théorème chinois des restes on peut remettre ce groupe sous forme canonique ici : $\mathbb{Z}/12\mathbb{Z}$. Les facteurs invariants du premier groupe sont donc (12) tandis que ceux du second sont $(2, 6)$. Ces groupes ne sont donc pas isomorphes (à noter qu'ici en réalité l'argument de b) s'appliquait sans qu'on ait besoin d'avoir recours à des arguments sophistiqués.

e) (cf. TD n° IV, exercice C, II.12.5.)

II.11 . –Le théorème de la base adaptée et lalgorithme d'EUCLIDE–GAUSS (cf. C)

Le théorème II.4.6 assure qu'étant donné un groupe abélien (resp. A-module,) libre de type fini L (A étant bien entendu toujours un anneau principal,) tout sous-groupe (resp. sous- A-module,) M de L est libre de type fini et de rang inférieur à celui de L. En revanche on n'a encore donné aucune réponse quant au fait de savoir dans quel(s) cas M pourrait posséder un supplémentaire dans L, ou de manière équivalente à quelle(s) condition(s) une base de M pourrait se compléter en une base de L. On a parfois néanmoins abordé ces questions à travers des exemples (cf. TD n° III, exercice C, question 1), c), TD n° III, exercice C, question 2), TD n° III, exercice C, question 3).)

Le théorème II.11.12, dit de la *base adaptée* assure qu'un couple $M \subset L$ de groupes abéliens, où L est supposé libre de type fini, possède une base adaptée au sens de la définition II.11.1. Le théorème II.11.12 peut être démontré sans préalablement supposer que le théorème II.4.6 a été établi, et dans ce cas il en redonne en fait une preuve.

Nous allons cependant, dans ce paragraphe (II.11,) démontrer le théorème II.11.12 de la base adaptée, uniquement dans le cas des groupes abéliens ou à tout le moins dans le cas de A-modules lorsque A est un *anneau euclidien* I.13.6.1. La contrepartie à cette restriction concernant les anneaux, est que, la preuve qu'on va donner ici du théorème II.11.12, est algorithmique et donne un moyen de construire effectivement une base adaptée (cf. II.11.9.)

On constatera (cf. II.11.3,) que l'existence d'une base adaptée pour un couple $M \subset L$ de A-modules (donc en particulier de groupes abéliens,) n'est pas indépendante de l'existence des *facteurs invariants* pour le groupe quotient L/M. L'interaction entre ces deux questions sera développée davantage dans l'appendice C où l'on traitera la question d'existence d'une base adaptée pour un couple $M \subset L$ de A-modules où A est un anneau principal quelconque.

Définition II.11.1 (BAse adaptée) On dit qu'un couple $M \subset L$ de groupes abéliens (resp. A-modules,) libres de type fini (cf. II.3.2,) admet une *base adaptée*, s'il existe une base $\lambda_{i\ ,1\leq i\leq r}$ de L, un entier $s \leq r$, des éléments

$$d_{i\ ,1\leq i\leq s} \in \mathbb{Z}(\text{resp. } A) \text{ tel que } d_i\lambda_{i\ ,1\leq i\leq s} \text{ soit une base de } M$$

et

$$\forall 1 \leq i \leq s-1,\ d_{i+1}|d_i\ .$$

Remarque II.11.2 Si $\mathfrak{I} \subset A$ est un idéal, puisque A est principal, il existe $a \in A$ tel que $\mathfrak{I} = Aa$. Si $\mathfrak{I} \neq \{0\}, a \neq 0$ est une base de $\mathfrak{I}$. Comme 1 est une base de A, c'est une base adaptée pour $\mathfrak{I} \subset A$. On peut donc trouver une base adaptée dans cette situation.

Proposition II.11.3 *Si un couple $M \subset L$, possède une base adaptée*

$$\left(\lambda_{i\ ,1\leq i\leq r}\ , d_{i\ ,1\leq i\leq s}\right)_{,s\leq r} \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i,$$

les éléments d_i non inversibles sont les facteurs invariants de L/M (cf. II.10.6, B.6.14.)

Preuve : *Soit $P := \mathbb{Z}^{-s}(\text{resp. } A^{r-s},)$ muni de sa base canonique (cf. II.1.4.c),) $\varepsilon_{i\ ,s+1\leq i\leq r}$. Soit*

$$Q := A/d_1 \times \ldots \times A/d_s \times P\ .$$

Il résulte du théorème II.6.4 (resp. B.1.4,) que

$$\mathrm{Tor}_A(Q) \;=\; A/d_1 \;\times\; \ldots \;\times\; A/d_s \text{ et } \mathrm{rg}(Q) \;=\; r-s\;.$$

Définissons un $\mathbb{Z}$(resp. A)-morphisme :

$$\begin{array}{rccl} \phi: & L & \longrightarrow & Q \\ & \lambda_i & \longmapsto & 1_{A/d_i}\;,\; \forall 1 \leq i \leq s, \\ & \lambda_i & \longmapsto & \varepsilon_i\;,\; \forall s+1 \leq i \leq r,\;\; . \end{array}$$

Alors :

Lemme II.11.3.1 *Le morphisme ϕ est surjectif et M est son noyau.*

Il découle alors du lemme II.11.3.1 ci-dessus et du théorème de factorisation des morphismes (cf. I.8.11,) qu'il existe un isomorphisme

$$\psi \;:\; L/M \;\cong\; Q \text{ tel que } \psi \;\circ\; \pi \;=\; \phi \text{ où } \pi \;:\; L \;\to\; L/M \text{ est la surjection canonique }\;.$$

Puisque

$$\forall 1 \leq i \leq s-1,\; d_{i+1} | d_i,$$

il existe un unique $1 \;\leq\; t \;\leq\; s$ tel que

$$d_i \;\in\; \mathbb{Z}^\times (\text{resp. } A^\times) \;\Leftrightarrow\; i \geq t\;.$$

Comme pour $i \;\geq t$, $A/d_i \;=\; \{0\}$, on en déduit que

$$\mathrm{Tor}_A(Q) \;=\; A/d_1 \;\times\; \ldots \;\times\; A/d_t\;.$$

La condition $d_{i+1}|d_i$ assure l'unicité de cette décomposition dans le théorème II.10.5.ii) (resp. B.6.13.2),) si bien que les d_i ,$_{1\leq i\leq t}$ sont bien les facteurs invariant de L/M.

***Preuve** (**du lemme II.11.3.1**):*

*i) (**Surjectivité de** ϕ)*
Pour tout $\alpha \;\in\; Q$, il existe un unique couple (α_t, α_l),

$$\alpha_t \;\in\; \prod_{i=1}^{s} A/d_i \text{ et } \alpha_l \;\in\; P \text{ tel que } \alpha \;=\; \alpha_t \;+\; \alpha_l\;.$$

Or

$$\exists a_i\,,_{1\leq i\leq s} \;\in\; A,\; \alpha_t \;=\; \big(a_1 1_{A/d_1}, \ldots, a_s 1_{A/d_s}\big) \text{ et } \exists a_i\,,_{s+1\leq i\leq r} \;\in\; A,\; \alpha_l \;=\; \sum_{i=s+1}^{r} a_i \varepsilon_i\;.$$

On vérifie alors que :

$$\begin{array}{rcl} \phi\big(\sum_{i=1}^{r} a_i\lambda_i\big) & = & \phi\big(\sum_{i=1}^{s} a_i\lambda_i\big) + \phi\big(\sum_{i=s+1}^{r} a_i\lambda_i\big) \\ & = & \alpha_t + \alpha_l \\ & = & \alpha\;. \end{array}$$

ii) ***(Le noyau de*** ϕ***)***
Pour tout

$$x \ := \ \sum_{i=1}^{r} a_i \lambda_i \ \in \ M,$$

$\phi(x) \ = \ 0$ *entraîne que*

$$\phi\big(\sum_{i=1}^{s} a_i \lambda_i\big) \ = \ 0 \text{ et } \phi\big(\sum_{i=s+1}^{r} a_i \lambda_i\big) \ = \ 0$$

puisque $Q \ = \ \mathrm{Tor}_A(Q) \ \oplus \ P$.

La seconde égalité entraîne $\sum_{i=s+1}^{r} a_i \varepsilon_i \ = \ 0$ *qui entraîne*

$$\forall i \leq s+1 \leq r, \ a_i \ = \ 0$$

puisque $\varepsilon_{i \ ,1 \ \leq \ s+1 \ \leq \ i}$ *est une base de* P.

Par ailleurs $\phi\big(\sum_{i=1}^{s} a_i \lambda_i\big) \ = \ 0$, *équivaut à*

$$\forall 1 \leq i \leq s, \ a_i 1_{A/d_i} \ = \ 0$$

ce qui équivaut encore à

$$\forall 1 \leq i \leq s, \ d_i | a_i$$

qui équivaut finalement à

$$\forall i \leq 1 \leq s, \ a_i \lambda_i \ \in \ M \ .$$

Corollaire II.11.4 *Si* $M \ \subset \ L$ *possède une base adaptée*

$$\big(\lambda_{i \ ,1 \leq i \leq r} \, , d_{i \ ,1 \leq i \leq s}\big)_{,s \leq r} \forall 1 \leq i \leq s-1, \ d_{i+1} | d_i,$$

le s*-uplet* $d_{i \ ,1 \leq i \leq s}$ *est unique (à association près.)*

Preuve *: C'est bien entendu une conséquence de l'identification faite entre les* $d_{i \ ,1 \leq i \leq s}$ *et les facteurs invariants dans la proposition II.11.3 et l'énoncé d'unicité dans le théorème II.10.5.ii) (resp. B.6.13.2).)*

Notation II.11.5 Pour deux entiers naturels n et p, on note $\mathcal{M}_{n,p}(A)$ l'ensemble des matrices à n lignes et p colonnes à coefficients dans A et $\mathcal{M}_n(A) \ := \ \mathcal{M}_{n,p}(A)$ pour $p \ = \ n$ l'ensemble des matrices à n lignes et n collonnes à coefficients dans A.

Pour tous $(m,n,p) \ \in \ \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, $(M,N) \ \in \ \mathcal{M}_{m,n}(A) \ \times \ \mathcal{M}_{n,p}(A)$, le produit $M \cdot N$ est défini de manière usuelle.

En particulier $(\mathcal{M}_n(A), +, \cdot)$ a une structure d'anneau (non commutatif en général) et on note $\mathrm{GL}_n(A)$ le groupe des élément inversibles de $\mathcal{M}_n(A)$ qu'on apelle ordinairement le *groupe linéaire*.

On notera

$$O_{1,n} \ \in \ \mathcal{M}_{1,n}(A) (\text{resp. } O_{n,1} \ \in \ \mathcal{M}_{n,1}(A) \ )$$

la matrice dont tous les coefficients sont nuls.

Lemme II.11.6 *Étant donné un A-module L libre de type fini et de rang n, muni d'une base λ_i ,$1\leq i\leq n$ l'application qui à tout endomorphisme*

$$f \in \mathrm{End}_A(L) = \mathrm{Hom}_A(L,L)$$

de L associe la matrice $M(f)$ définie par

$$\forall 1\leq j\leq n,\ f(\lambda_j) = \sum_{i=1}^{n} M(f)_{i,j}\lambda_i$$

est un isomorphisme d'anneaux.

En particulier pour tout $f \in \mathrm{End}_A(L)$ f est un automorphisme si et seulement si sa matrice $M(f)$ est inversible i.e.

$$f \in \mathrm{Aut}_A(L) \Leftrightarrow M(f) \in \mathrm{GL}_n(A)\ .$$

Notation II.11.7 Soit $n \in \mathbb{N}^*$ un entier et L un A-module libre de rang n rapporté à une base λ_i ,$1\leq i\leq n$. On note $I_n \in \mathcal{M}_n(A)$ la matrice identité. Pour $M \in \mathcal{M}_{n,p}(A)$:

i) $((\mathrm{Ligne}_i(M) \leftrightarrow \mathrm{Ligne}_j(M)))$

l'opération sur les lignes de M symboliquement notée $(\mathrm{Ligne}_i(M) \leftrightarrow \mathrm{Ligne}_j(M))$ consistant à échanger la $i^{\text{ième}}$ et la $j^{\text{ième}}$ ligne, correspond à la multiplication à gauche par la matrice $P_{i,j}^{(n)}$ obtenue à partir de la matrice I_n en appliquant la permutation des lignes $\mathrm{Ligne}_i(I_n)$ et $\mathrm{Ligne}_j(I_n)$, qui correspond (par l'isomorphisme construit dans le lemme II.11.6,) à l'automorphisme de L défini par

$$\lambda_i \mapsto \lambda_j\ ,\ \lambda_j \mapsto \lambda_i\ ,\ \forall 1\leq k\leq n,\ k\neq i\ ,\ k\neq j\ ,\ \lambda_k \mapsto \lambda_k\ ;$$

ii) $((\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M)))$

l'opération sur les lignes de m symboliquement notée $(\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M))$ consistant à remplacer la $i^{\text{ième}}$ ligne par une combinaison linéaire de cette dernière et d'une autre ligne, correspond à la multiplication à gauche par la matrice $T_{i,j}^{(n)}(a)$, *matrice de transvection* obtenue à partir de I_n par application de la transvection $(\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M))$, correspondant à l'automorphisme de L défini par

$$\lambda_j \mapsto \lambda_j + a\lambda_i\ ,\ \forall 1\leq k\leq n,\ k\neq j\ ,\ \lambda_k \mapsto \lambda_k\ ;$$

iii) les opérations sur les colonnes correspondent, elles, à des multiplications à droite par les matrices $P_{i,j}^{(p)}$ et ${}^tT_{i,j}^{(p)}(a)$.

Remarque II.11.8 Les matrices $P_{i,j}^{(n)}$ et $T_{i,j}^{(n)}(a)$ introduites en II.11.7.i) et II.11.7.ii) correspondant à des automorphismes de L, sont donc inversibles.

II.11.9 . –Description de l'algorithme

L'algorithme consiste à transformer une matrice $M \in \mathcal{M}_{n,p}(A)$ par des opérations élémentaire sur les lignes et les colonnes. Seules les opérations suivantes sont autorisées :

—

les permutations de lignes $(\mathrm{Ligne}_i(M) \leftrightarrow \mathrm{Ligne}_j(M))$

ou de colonnes $(\mathrm{Colonne}_i(M) \leftrightarrow \mathrm{Colonne}_j(M))$,

—

les transvections de lignes $(\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M)\ ,\ i,j\ \in\ \{1,\dots,n\}\ ,\ a\ \in\ A)$

ou de colonnes $(\mathrm{Colonne}_i(M) \leftarrow \mathrm{Colonne}_i(M) + a\mathrm{Colonne}_j(M)\ ,\ i,j\ \in\ \{1,\dots,p\}\ ,\ a\ \in\ A)$.

—

La multiplication d'une ligne et d'une colonne par -1 .

$$(\mathrm{Ligne}_i(M) \leftarrow -\mathrm{Ligne}_i(M)) \text{ et } (\mathrm{Colonne}_j(M) \leftarrow -L\mathrm{Colonne}_j(M)) .$$

Comme dans l'algorithme de Gauss habituel, les opérations élémentaires correspondent à la multiplication par des matrices inversibles dans l'anneau $\mathcal{M}_n(A)$ (respectivement $\mathcal{M}_p(A)$). Une suite finie d'opérations élémentaires autorisées transforment donc la matrice M en une matrice de la forme PMQ où $P\ \in\ \mathrm{GL}_n(A)$ et $Q\ \in\ \mathrm{GL}_p(A)$

Très précisément, il s'agit, par une suite finie d'opérations élémentaires autorisées, de transformer la matrice non nulle

$$M\ :=\ (m_{i,j})_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ p}}\ \in\ \mathcal{M}_{n,p}(A) \qquad \text{II.11.9.1}$$

en une matrice de la forme (quasi-diagonale)

$$D\ =\ \begin{pmatrix} d_1 & 0 & & & 0\\ 0 & d_2 & 0 & & \\ & & \ddots & & \\ & & & d_s & 0\\ 0 & & & & 0 \end{pmatrix} \text{ où :} \qquad \text{II.11.9.2}$$

$$1\ \leq\ s\ \leq\ \min(n,p)\ ,\quad d_{i\ ,1\leq i\leq s}\ \in\ A\quad d_1|d_2|\dots|d_s\ .$$

Tous les autres coefficients de D sont nuls.

Notation II.11.9.3 L'anneau A étant euclidien on note

$$\mathbf{v}\ :\ A\ \setminus\ \{0\}\ \to\ \mathbb{N}$$

le *stathme euclidien* (cf. I.13.6.1.)

$$\text{si } A\ =\ \mathbb{Z}\ ,\ \forall n \in \mathbb{Z}\ \setminus \{0\},\ \mathbf{v}(n)\ =\ |n|\ ;$$

$$\text{si } A\ =\ \mathbb{K}[X]\ ,\ \forall P \in \mathbb{K}[X]\ \setminus\ \{0\},\ \mathbf{v}(P)\ =\ \deg(P)\ .$$

Pour toute matrice

$$M\ :=\ (m_{i,j})_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ p}}\ \in\ \mathcal{M}_{n,p}(A),$$

on note

$$\mathbf{v}(M)\ :=\ \min_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ p}, m_{i,j}\ \neq\ 0} \left(m_{i,j}\right) .$$

À chaque étape de l'algorithme, l'entier strictement positif $\mathbf{v}(M)$ décroît strictement, ce qui assure la finitude de l'algorithme.

Définition II.11.9.4 (Pivot) Un coefficient $m_{i,j}$ de M tel que $\mathbf{v}(m_{i,j})\ =\ \mathbf{v}(M)$ s'appelle un *pivot*.

II.11.10 . –Les étapes de l'algorithme

i) (**Première étape**)

a) On choisit un pivot $m_{i,j}$ que l'on amène à la position $(1,1)$ grâce aux transpositions

$$\mathrm{Ligne}_1(M) \leftrightarrow \mathrm{Ligne}_i(M) \text{ et } \mathrm{Colonne}_1(M) \leftrightarrow \mathrm{Colonne}_j(M) \ .$$

b) Pour j de 2 à p et pour i de 2 à n on effectue les divisions euclidiennes

$$m_{1,j} \ = \ q_j m_{1,1} \ + \ r_j \text{ et } m_{i,1} \ = \ q'_i m_{1,1} \ + \ r'_i \ ;$$

puis les transvections

$$\mathrm{Colonne}_j(M) \leftarrow \mathrm{Colonne}_j(M) - q_j \mathrm{Colonne}_1(M) \text{et } \mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) - a\mathrm{Ligne}_1(M) \ .$$

c) On a alors

$$\mathbf{v}(m_{1,j}) \ < \ \mathbf{v}(m_{1,1}) \text{ et } \mathbf{v}(m_{i,1}) \ < \ \mathbf{v}(m_{1,1}) \ \forall j > 1 \text{ et } i > 1 \ .$$

Si tous les $m_{1,j}$ et $m_{i,1}$ sont nuls, on passe à la deuxième étape ii).

Sinon on choisit l'un de ces coefficient non nul, on le place en position $(1,1)$ par une transposition, et on recommence b).

Puisque $\mathbf{v}(m_{1,1})$ diminue strictement à chaque étape le processus s'arrête, et on arrive à une matrice de la forme

$$\begin{pmatrix} m_{1,1} & O_{1,p-1} \\ \\ O_{n-1,1} & M' \end{pmatrix} \text{ où } M' \ \in \ \mathcal{M}_{n-1,p-1}(A) \ . \qquad 1$$

ii) (**Deuxième étape**)

Si $m_{1,1}$ divise tous les coefficients de M', on passe à la troisième étape iii). Sinon, on choisit un coefficient $m_{i,j}$ qui n'est pas divisible par $m_{1,1}$ et on effectue l'opération $\mathrm{Ligne}_1(M) \ \leftarrow \ \mathrm{Ligne}_1(M) + \mathrm{Ligne}_j(M)$. (Notons que le coefficient $m_{1,1}$ n'est pas modifié). On recommence alors la première étape i) à partir de i).b) : divisions euclidiennes, transvections, transposition. On arrive à une matrice de la forme i).c).1 mais avec une nouvelle valeur de $\mathbf{v}(m_{1,1})$ strictement plus petite.

Comme à chaque fois la valeur de $\mathbf{v}(m_{1,1})$ diminue strictement, on arrive à une matrice de la forme

$$\begin{pmatrix} m_{1,1} & O_{1,p-1} \\ \\ O_{n-1,1} & M' \end{pmatrix} \text{ où } M' \ \in \ \mathcal{M}_{n-1,p-1}(A) \qquad 1$$

et où $m_{1,1}$ divise tous les coefficients de M'.

iii) (**Troisième étape**)

On applique les étapes i) et ii) à la matrice M', ce qui ne modifie pas la première ligne et la première colonne. En répétant un nombre fini de fois le processus, on arrive à la forme quasi-diagonale II.11.9.2 souhaitée.

Proposition II.11.11 *Étant donnés deux entiers n et p la donnée d'une matrice M comme en II.11.9.1 équivaut à se donner les coordonnées de p vecteurs de A^n (ou d'un A-module libre de rang n, rapporté à une base.) Soit B le sous-A-module de A^n engendré par ces p vecteurs. Les multiplications autorisée à gauche de la matrice M correspondent à des changements de base dans A^n tandis que les multiplications autorisées à droite de M changent les générateurs de B en une autre famille de générateurs.*

Il s'ensuit, qu'au terme des transformations effectuées, le sous-A-module engendré par les colonnes de la matrice D (II.11.9.2) est encore B. Ces colonnes constituent alors manifestement une famille libre i.e. une base de B et cette base est évidemment adaptée à $B \subset A^n$ (cf. II.11.1.)

Si donc les étapes de l'algorithme ne sont pas uniques, si même les matrices P et Q telles que $D = PMQ$, ne le sont pas non plus le s-uplet $d_i\,,_{1\leq i\leq s}$ constituant les éléments diagonaux de D, est quant à lui unique en vertu du théorème II.11.12. aux termes de la proposition II.11.3, ce sont mêmes des générateurs des facteurs invariants (cf. II.10.6,) du quotient A^n/B.

Théorème II.11.12 (de la base adaptée) *Si $M \subset L$ sont des groupes abéliens, et L est libre de type fini (cf. II.3.2,) alors M est libre de type fini et le couple*

$$(L, M) \text{ possède une base adaptée } \left(\lambda_i\,,_{1\leq i\leq r}\,, d_i\,,_{1\leq i\leq s}\right),_{s\leq r} \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i\ ,$$

(ce qui contient en particulier le fait que $\mathrm{rg}(M) \leq \mathrm{rg}(L)$.) De plus le s-uplet $d_i\,,_{1\leq i\leq s}$ est unique.

Preuve *: D'abord le théorème II.4.6 assure que M est libre de type fini et $\mathrm{rg}(M) \leq \mathrm{rg}(L)$.*

Ensuite, l'existence d'une base adaptée est assurée par la proposition II.11.11.

L'unicité est finalement assurée par le corollaire II.11.4.

Exemple II.11.13 (Vecteur primitif) Soit $M := \begin{pmatrix}6 & 10 & 30\end{pmatrix}$ On effectue une suite d'opérations sur les colonnes :

$$\begin{array}{rcl} & & \begin{pmatrix}6 & 10 & 30\end{pmatrix} \\ \mathrm{Colonne}_3(M) \leftarrow \mathrm{Colonne}_3(M) - 5\mathrm{Colonne}_1(M), & & \\ \mathrm{Colonne}_2(M) \leftarrow \mathrm{Colonne}_2(M) - \mathrm{Colonne}_1(M) & \to & \begin{pmatrix}6 & 4 & 0\end{pmatrix} \\ \mathrm{Colonne}_1(M) \leftarrow \mathrm{Colonne}_1(M) - \mathrm{Colonne}_2(M) & \to & \begin{pmatrix}2 & 4 & 0\end{pmatrix} \\ \mathrm{Colonne}_2(M) \leftarrow \mathrm{Colonne}_2(M) - 2\mathrm{Colonne}_1(M) & \to & \begin{pmatrix}2 & 0 & 0\end{pmatrix} = D\,. \end{array}$$

On obtient la matrice Q en appliquant la suite d'opérations élémentaires à la matrice I_3 :

$$Q = \begin{pmatrix}2 & -5 & -5\\ -1 & 3 & 0\\ 0 & 0 & 1\end{pmatrix}$$

On a donc

$$\begin{pmatrix}2 & 0 & 0\end{pmatrix} = \begin{pmatrix}6 & 10 & 30\end{pmatrix}\begin{pmatrix}2 & -5 & -5\\ -1 & 3 & 0\\ 0 & 0 & 1\end{pmatrix}\,.$$

On a aussi

$$Q^{-1} = \begin{pmatrix}3 & -5 & -15\\ 1 & 2 & 5\\ 0 & 0 & 1\end{pmatrix}$$

et donc

$$\begin{pmatrix}6 & 10 & 30\end{pmatrix} = \begin{pmatrix}2 & 0 & 0\end{pmatrix}\begin{pmatrix}3 & -5 & -15\\ 1 & 2 & 5\\ 0 & 0 & 1\end{pmatrix}\,.$$

Remarque II.11.14 Comparer l'exemple ci-dessus au corollaire C.1.4.

Exemple II.11.15 Trouver une base de $\mathbb{Z}^3$ adaptée au sous-groupe (sous-$\mathbb{Z}$-module) F engendré par les vecteurs

$$y_1 := \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \text{ et } y_2 := \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}.$$

On a ici $Y = \begin{pmatrix} 1 & 2 \\ 1 & -1 \\ -1 & 0 \end{pmatrix}$ et en appliquant l'algorithme d'EUCLIDE–GAUSS, on voit que la suite d'opérations élémentaires

$$\begin{gathered} \mathrm{Colonne}_2(Y) \leftarrow \mathrm{Colonne}_2(Y) - 2\mathrm{Colonne}_1(Y)\,, \\ \mathrm{Ligne}_2(Y) \leftarrow \mathrm{Ligne}_2(Y) - \mathrm{Ligne}_1(Y)\,, \\ \mathrm{Ligne}_3(Y) \leftarrow \mathrm{Ligne}_3(Y) + \mathrm{Ligne}_1(Y)\,, \\ \mathrm{Ligne}_2(Y) \leftarrow \mathrm{Ligne}_2(Y) + \mathrm{Ligne}_3(Y)\,, \\ \mathrm{Ligne}_3(Y) \leftarrow \mathrm{Ligne}_3(Y) + 2\mathrm{Ligne}_1(Y) \end{gathered}$$

transforment la matrice Y en la matrice $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 0 \end{pmatrix}$. On en déduit que

$$Y = P^{-1}DQ \text{ avec } P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \text{ et } Q = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

On a alors $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & -1 \\ -1 & -2 & 1 \end{pmatrix}$. La base

$$\left\{ e_1 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 \\ 3 \\ -2 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\}$$

est donc adaptée au sous-groupe F : c'est une base de $\mathbb{Z}^3$ et $(e_1, -e_2)$ est une base de F.

Exemple II.11.16 (Résolution d'un système $\mathbb{Z}$-linéaire) Soit

$$A := (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{Z}) \text{ et } B := \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{Z})\,.$$

On cherche à résoudre le système linéaire $AX = B$, avec $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$.

i) (**Cas d'un système homogène**)

L'ensemble F de ses solutions est un sous-module de $\mathbb{Z}^p$. Il est libre, de rang $p - k$ où k est le rang de la matrice A. On écrit A sous la forme $A = PDQ^{-1}$ où D (cf. II.11.9.2.) Le système s'écrit alors $PDQ^{-1}X = 0$, c'est à dire $DY = 0$ où

$$Y = Q^{-1}X = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}.$$

L'ensemble des solutions du système $DY = 0$ est le sous $\mathbb{Z}$-module dont une base est $(Y_{k+1}, \ldots, Y_p)$ où Y_j est le vecteur colonne dont toutes les coordonnées sont nulles, sauf la coordonnée d'indice j qui vaut 1. Les vecteurs $X_j = QY_j$ $(k+1 \leq j \leq p)$ forment donc une $\mathbb{Z}$-base de F. Si l'on préfère une représentation paramétrique on peut écrire :

$$F = \left\{ \sum_{j=k+1}^{p} t_j X_j \ , \mid (t_{k+1}, \ldots t_p) \in \mathbb{Z}^{p-k} \right\} .$$

ii) (**Cas général**)
Le système s'écrit alors sous la forme

$$DY = C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} ,$$

où $C = P^{-1}B$.

Pour que le système soit compatible il faut et il suffit que

$$\begin{cases} d_1 | c_1, \ldots, d_k | c_k \\ c_{k+1} = \ldots = c_n = 0 . \end{cases}$$

Les solutions du système $DY = C$ sont de la forme

$$\begin{pmatrix} c_1/d_1 \\ \vdots \\ c_k/d_k \\ t_{k+1} \\ \vdots \\ t_p \end{pmatrix}$$

où $t_{k+1,\ldots t_p}$ sont des entiers arbitraires. Les solutions du système $AX = B$ sont alors de la forme

$$(c_1/d_1)X_1 + \ldots + (c_k/d_k)X_k + t_{k+1}X_{k+1} + \ldots + t_pX_p$$

où $t_{k+1}, \ldots, t_p$ sont arbitraires dans $\mathbb{Z}$. On retrouve bien, comme dans le cas des espaces vectoriels" la structure de "sous-module affine" de l'ensemble des solutions. (On parle plus volontiers, dans ce cas, d'*espace principal homogène*).

iii) On peut traiter ici, à titre d'exemple, la résolution de l'équation $a_1x_1 + \ldots + a_px_p = b$. où $a_1, \ldots, a_p$ sont des entiers premiers entre eux.

II.12 . −Exercices

Exercice II.12.1 Démontrer les points II.1.11.i) et II.1.11.ii).

Exercice II.12.2 Soit M un A-module et $\mathcal{B}$ une base de M. Pour tout A-module N, définir une bijection entre l'ensemble des applications de $\mathcal{B}$ dans N et l'ensemble $\mathrm{Hom}_A(M,N)$ des morphismes de A-modules de M dans N.

Exercice II.12.3 Soit $n \in \mathbb{Z}$ un entier strictement plus grand que 1.

1) Montrer que $\{n\}$ est une partie libre maximale du $\mathbb{Z}$-module $\mathbb{Z}$ mais n'est pas une base.

2) Montrer que le sous-$\mathbb{Z}$-module $n\mathbb{Z}$ de $\mathbb{Z}$ n'a pas de supplémentaire dans $\mathbb{Z}$.

3) Montrer que $\mathbb{Z}$ et $n\mathbb{Z}$ sont des $\mathbb{Z}$-module libre de type fini et de rang 1.

Exercice II.12.4 [Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$]

1) Étant donnée une application $f : E \to F$, rappeler rapidement pourquoi, si f est surjective,

$$\forall A \subset F \; f(f^{-1}(A)) = A \, .$$

2) Soit G un groupe abélien, H un sous-groupe de G, et $\pi : G \to G/H$ la projection canonique. Notons $\mathcal{E}$ (resp. $\mathcal{F}$,) l'ensemble des sous-groupes de G contenant H, (resp. l'ensemble des sous-groupes de G/H.)

Montrer que les applications

$$\pi_* : \mathcal{E} \to \mathcal{F} \, , \; K \mapsto \pi(K) \text{ et } \pi^* : \mathcal{F} \to \mathcal{E} \, , \; L \mapsto \pi^{-1}(L)$$

sont bien définies et inverses l'une de l'autre.

3) Soit $n \in \mathbb{N}^*$,

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \, , \; x \mapsto x \, mod \, n$$

la projection canonique et L un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer qu'il existe un unique $d \in \mathbb{N}$, tel que

$$d|n \text{ et } L = \pi(d\mathbb{Z}) \, .$$

b) Construire un isomorphisme

$$\mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/L \, .$$

On note $n = de$.

c) Construire un isomorphisme

$$\mathbb{Z}/e\mathbb{Z} \cong L \, .$$

Exercice II.12.5 [cf. IV.12.1]

1) Parmi les groupes suivants, lesquels sont isomorphes (justifier) :

$$G_1 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}, G_2 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}, G_3 = (\mathbb{Z}/27\mathbb{Z})^\times \times \mathbb{Z}/25\mathbb{Z},$$
$$G_4 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

Lesquels sont cycliques ?

2) Déterminer les classes d'isomorphisme de groupes abéliens d'ordre 32, puis les classes d'isomorphisme de groupes abéliens d'ordre 18.

3) Un groupe abélien G a un élément d'ordre 11×2^4 et au moins 26 éléments d'ordre 11. Quel est le plus petit ordre possible du groupe ? Donner alors la structure (ou les structures possibles) pour cet ordre.

4) Déterminer à isomorphisme près les groupes abéliens de cardinal 300.

5) Les groupes abéliens

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \text{ et } \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$$

sont-ils isomorphes ?

6) (**Groupes abéliens à** 144 **éléments**)
Donner les classes d'isomorphismes de groupes abéliens de cardinal 144.

7) **Soit** A **le groupe abélien** $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.
Trouver les entiers $k \geq 1$ et d_i ,$1 \leq i \leq k \geq 2$ tels que :
— pour tout $1 \leq i < k$, $d_{i+1} | d_i$ et
—

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} .$$

8) Soit $G = \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Donner les invariants du groupe abélien fini G. Combien y a-t-il de sous-groupes d'exposant 5 dans G ?

9) **On pose**

$$A := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} , \ B := \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} , C := \mathbb{Z}/5\mathbb{Z} .$$

Trouver les entiers $k \geq 1$ et $d_i \geq 2$ pour $1 \leq i \leq k$ tels que d_{i+1} divise d_i pour tout $1 \leq i < k$ et tels que

$$A \times B \times C = \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} .$$

10) On admet que le groupe multiplicatif de l'anneau $\mathbb{Z}/p^r\mathbb{Z}$ est cyclique quand p est un nombre premier impair. Trouver les entiers $k \geq 1$ et $d_i \geq 2$ pour $1 \leq i \leq k$ tels que d_{i+1} divise d_i pour tout $1 \leq i < k$ et tels que $(\mathbb{Z}/91\mathbb{Z})^\times \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_k\mathbb{Z}$.

11) **a)** On rappelle/admet que si p est un nombre premier impair et $n \geq 1$, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$ est cyclique. Donner son cardinal.

b) Soit $G = (\mathbb{Z}/6615\mathbb{Z})^\times$. Ecrire G sous la forme $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ avec s un entier positif et d_i des entiers positifs et $d_{i+1}|d_i$ pour $1 \leq i \leq s-1$.

12) Soient p, q, r trois nombres premiers distincts. Combien y a-t-il de classes d'isomorphismes de groupes abéliens d'ordre $p \times q^3 \times r^4$?

Donner la structure en termes d'entiers d_i avec $d_{i+1}|d_i$ de tous ceux possédant de plus un sous-groupe d'ordre r^3 et d'exposant r.

13) **a)** On rappelle/admet que si p est un nombre premier impair et $n \geq 1$, $(\mathbb{Z}/p^n\mathbb{Z})^\times$ (groupe des éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$) est cyclique. Donner son cardinal.

b) Soit $G = (\mathbb{Z}/(49 \times 18 \times 17)\mathbb{Z})^\times$. Ecrire G sous la forme $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ avec s un entier positif et d_i des entiers positifs tels que $d_{i+1}|d_i$ pour $1 \leq i \leq s-1$.

Errata :

1. À la fin de la preuve de la proposition II.10.3
   il faut lire « Le morphisme $\mathbb{Z} \to A\ ,\ 1 \mapsto w$ se factorise donc »
   et non « Le morphisme $A \to M\ ,\ 1 \mapsto w$ se factorise donc » .
2. La référence B.7 au paragraphe II.11 est en fait C.

III . −Les anneaux de polynômes

Dans tout ce chapitre (III), $(A, +_A, *_A, 0_A, 1_A)$ **est un anneau (commutatif) (cf. I.1.8,) qu'on supposera même assez vite intègre (cf. I.1.14,) et l'on ne finira même par considérer, au paragraphe III.5 que le cas où** A **est un corps.**

III.1 . −L'anneau des séries formelles à coefficients dans A

On ne construit, dans ce paragraphe (III.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.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.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.1.2 On rappelle que l'ensemble des suites à valeurs dans A est usuellement noté $A^{\mathbb{N}}$. 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 :

$$(\alpha +_{A^{\mathbb{N}}} \beta)_n := \alpha_n +_A \beta_n \qquad \text{III.1.2.1}$$

et

$$(\alpha *_{A^{\mathbb{N}}} \beta)_n := \sum_{k=0}^{n} \alpha_k *_A \beta_{n-k}\ . \qquad \text{III.1.2.2}$$

Proposition III.1.3 *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* $*_{A^{\mathbb{N}}}$.

Preuve *: Il s'agit, en premier lieu , de montrer que* $(A, +_{A^{\mathbb{N}}})$ *est un groupe abélien, ce qui est fait dans l'exercice III.7.1 et résulte également de la proposition I.6.1.i).*

On montre ensuite dans l'exercice III.7.2 que $(A, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ *est un anneau commutatif.*

Définition III.1.4 (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.1.5 Pour tout $a \in A$, on définit l'élément $i(a)$ de $A^{\mathbb{N}}$ par :

$$i(a)_0 := a \text{ et } \forall n \in \mathbb{N},\ n > 0 \Rightarrow i(a)_n = 0\,. \qquad \text{III.1.5.1}$$

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

$$p(\alpha) := \alpha_0\,. \qquad \text{III.1.5.2}$$

Proposition III.1.6 *i)*

$$p \circ i = \mathrm{Id}_A\,.$$

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

***Preuve** : Découle du point précédent.*

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

***Preuve** : Le fait que i est un morphisme d'anneaux est démontré dans le III.7.5. La vérification du fait que p est aussi un morphisme est très simple et laissée en exercice.*

Notation III.1.7 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.1.8 *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$_4$)

$$1_A \cdot \alpha = \alpha\,.$$

Preuve : *Ce n'est qu'un jeu d'écriture sur le fait que i est un morphisme d'anneaux.*

Remarque III.1.9 Si A était un corps les propriétés III.1.8.Mod$_1$) à III.1.8.Mod$_4$) assureraient que $A^{\mathbb{N}}$ est un *A-espace vectoriel*. Cependant dans le cas où A est simplement un anneau on parle de *A-module* (cf. A.1.1.) Le morphisme $i : A \to A^{\mathbb{N}}$ fait même de $A^{\mathbb{N}}$ une A-algèbre (cf. A.1.6e)t sa structure de A-module n'est autre que celle induite par sa structure de A-algèbre (cf. A.1.8.b).)

Notation III.1.10 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 $\varepsilon_0 = \upsilon$.

Lemme III.1.11 *Pour tout $j \in \mathbb{N}$,*

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

et par conséquent

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

Preuve : *C'est un exercice.*

Notation III.1.12 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 $(\alpha_n)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$ 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.

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

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

Proposition III.1.13 *i) Pour tout $(\alpha_n)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$, $\alpha \neq \zeta$, il existe un entier naturel $\mathrm{val}(\alpha)$ tel que*

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

Preuve : *Voir l'exercice III.7.4.question 2).*

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.

Preuve : *Voir l'exercice III.7.4.question 3).*

iii)

$$\forall(\alpha,\beta)\in(A^{\mathbb{N}}\setminus\{\zeta\})\ \times\ (A^{\mathbb{N}}\setminus\{\zeta\}),\ \mathrm{val}(\alpha+_{A^{\mathbb{N}}}\beta)\ \geq\ \min\big(\mathrm{val}(\alpha)\ ,\ \mathrm{val}(\beta)\big)$$

avec égalité dans le cas où $\mathrm{val}(\alpha)\ \neq\ \mathrm{val}(\beta)$.

Preuve *: Voir l'exercice III.7.4.question 5).*

Définition III.1.14 (Valuation) Pour tout $\alpha\ \in\ A^{\mathbb{N}}\setminus\{\zeta\}$, on appellera *valuation X-adique* ou simplement de α, l'entier $\mathrm{val}(\alpha)$.

Remarque III.1.15 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. La définition de valuation donnée en III.1.14 est alors à rapprocher de la notion de valuation p-adique donnée en I.13.5.5, 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 :

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

Sit 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 III.1.13.ii) et III.1.13.iii) sont vérifiés pour tout $(\alpha,\beta)\ \in\ A^{\mathbb{N}}\ \times\ A^{\mathbb{N}}$.

Proposition III.1.16 *Si A est un anneau commutatif intègre il en est de même de $A^{\mathbb{N}}$.*

Preuve *: Voir l'exercice III.7.4.question 4).*

III.2 . −Anneau des polynômes à une indéterminée

On reprend les notations du paragraphe III.1.

Notation III.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 $\big(\alpha_n\big)_{,n\in\mathbb{N}}\ \in\ A^{\mathbb{N}}$ 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.2.2 *i) Pour tout $\big(\alpha_n\big)_{,n\in\mathbb{N}}\ \in\ A^{\mathbb{N},0}$, $\alpha\ \neq\ \zeta$, il existe un unique entier naturel $\deg(\alpha)$ tel que*

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

Preuve *: Voir l'exercice III.7.6.question 1).*

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.

Preuve *: Voir l'exercice III.7.6.question 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 $\deg(\alpha)\ \neq\ \deg(\beta)$.

Preuve *: Voir l'exercice III.7.6.question 3).*

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

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

Preuve *: Voir l'exercice III.7.6.question 6).*

Définition III.2.3 (Degré) Pour tout $\alpha\ \in\ A^{\mathbb{N},0}\ \setminus\ \{\zeta\}$, l'entier $\deg(\alpha)$ sera appelé *degré* de α.

Remarque III.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.1.15.b).) Les assertions III.2.2.ii) et III.2.2.iii) sont alors vérifiées pour tout $(\alpha,\beta)\ \in\ A^{\mathbb{N},0}\ \times\ A^{\mathbb{N},0}$.

Proposition III.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 est intègre.)*

Preuve *: Voir l'exercice III.7.6.question 4).*

ii) Le morphisme $i\ :\ A\ \to\ A^{\mathbb{N}}$ étant celui défini en III.1.5.1, l'image de i est incluse dans $A^{\mathbb{N},0}$ et l'on a

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

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

Preuve *: Voir l'exercice III.7.6.question 7).*

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

Preuve *: Voir l'exercice III.7.6.question 8).*

iv) La loi externe $\cdot$ définie en III.1.7 se restreint à $A^{\mathbb{N},0}$ et vérifie encore les axiomes III.1.8.Mod$_1$) à III.1.8.Mod$_4$).

***Preuve** : Est une conséquence presque immédiate du point ii).*

v) La famille $X^n\,,_{n\in\mathbb{N}}$ est une base 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

$$\alpha = \sum_{j=0}^{d} a_j \cdot X^j;$$

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

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

***Preuve** :*

a) 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) Exercice.

Notation III.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.1.12,) 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.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.2.8 Dans l'anneau $A := \mathbb{Z}/p^2\mathbb{Z}$, pour p un nombre premier, les éléments

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

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

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

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

Proposition III.2.9 (Propriété universelle de l'anneau des polynômes) *Soient*

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

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.1.5.1.)
Ceci entraîne en particulier que :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow \phi_b(\alpha) = \sum_{k=0}^{\deg(\alpha)} f(\alpha_k) *_B b^k . \qquad \text{III.2.9.1}$$

***Preuve** :*

*i) (**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,

$$\phi_b(1_{A[X]} = 1_B \Rightarrow \phi_b(\upsilon) = 1_B \Rightarrow \phi_b(X^0) = 1_B$$

d'où il résulte finalement :

$$\forall n \in \mathbb{N}, \phi_b(X^n) = b^n . \qquad 1$$

Par ailleurs si on note $\cdot$ la loi externe définie en III.1.7, $\phi_b \circ i = f$ 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 1, ϕ_b est nécessairement unique.

*ii) (**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 I.2.4.Ann$_5$) est satisfait.

Par ailleurs :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k$$

$$\forall \beta \in A[X], \beta = \sum_{k=0}^{\deg(\beta)} \beta_k X^k \quad \phi_b(\alpha *_{A^{\mathbb{N}}} \beta) = \sum_{k=0}^{\deg(\alpha)+\deg(\beta)} \Big(\sum_{\ell+m=k} \alpha_\ell \beta_m \Big) \cdot X^k$$

$$= \sum_{k=0}^{\deg(\alpha)+\deg(\beta)} f\Big(\sum_{\ell+m=k} \alpha_\ell \beta_m \Big) *_B b^k$$

$$= \Big(\sum_{k=0}^{\deg(\alpha)} f(\alpha_k) *_B b^k \Big) *_B \Big(\sum_{k=0}^{\deg(\beta)} f(\beta_k) *_B b^k \Big)$$

$$= \phi_b(\alpha) *_B \phi_b(\beta)$$

ce qui prouve que ϕ_b vérifie l'axiome I.2.4.Ann$_6$).

Il est enfin clair que l'axiome I.2.4.Ann$_7$) est satisfait.

Notation III.2.10 Avec les hypothèses et notations de la proposition III.2.9 ci-dessus, on notera $A[b]$ l'image de $A[X]$ dans B par le morphisme ϕ_b.

Corollaire III.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 :

$$\forall \alpha \in A[X], \alpha := \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow f[X](\alpha) = \sum_{k=0}^{\deg(\alpha)} f(\alpha_k) X^k . \qquad \textit{III.2.11.1}$$

***Preuve** : Il suffit d'appliquer la proposition III.2.9 au morphisme d'anneaux $i_B \circ f : A \to B[X]$ et à l'élément $X \in B[X]$.*

Exemple III.2.12 Le corollaire III.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 l'exemple 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 corrollaire III.2.11 pour en déduire un morphisme

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

en vertu de III.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 du paragraphe III.5

Corollaire III.2.13 (Polynômes à plusieurs indéterminées) *Soit A un anneau commutatif et $A[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans A. Puisque $A[X]$ est un anneau, on peut construire $(A[X])[Y]$ l'anneau des polynômes à une indéterminée et à coefficients dans $A[X]$ qu'on va simplement noter $A[X][Y]$. C'est également une notation temporaire, qu'on va pouvoir encore simplifier au vu de ce qui suit.*

En effet, la suite d'inclusions

$$A \xrightarrow{i_A} A[X] \xrightarrow{i_{A[X]}} A[X][Y]$$

permet de considérer A comme un sous-anneau de $A[X][Y]$. Il existe donc, grâce à la proposition III.2.9, un unique morphisme d'anneaux

$$A[X] \to A[X][Y] , \ X \mapsto Y$$

respectant les inclusions ci-dessus. Ce dernier morphisme, permet, toujours grâce à la proposition III.2.9, de construire un morphisme

$$A[X][y] \to A[X][Y] , \ (X, Y) \mapsto (Y, X) .$$

On laisse le soin au lecteur de montrer que ce dernier morphisme est un isomorphisme d'anneaux. Cela justifie la notation $A[X, Y] := A[X][Y]$.

On peut dès lors définir par récurrrence

$$A[X_1, \dots X_{n+1}] := A[X_1, \dots, X_n][X_{n+1}] .$$

Pour ne nécessiter que des arguments plutôt formels pour être définis, les anneaux de polynômes à plusieurs indéterminées nécessitent cependant des outils un peu plus élaborés pour être étudiés que les anneaux à une indéterminée et en particulier quand A est un corps.

III.3 . −Évaluation et fonctions polynômes

Dans cette section (III.3) A est un anneau.

Proposition III.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 :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow \mathrm{ev}_a(\alpha) = \sum_{k=0}^{\deg(\alpha)} \alpha_k * a^k . \qquad \textit{III.3.1.1}$$

Preuve *: Il suffit d'appliquer la proposition III.2.9 à l'identité de A et à l'élément a de A.*

Notation III.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 .

Lemme III.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 :*

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

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

Preuve *: Voir la proposition I.6.1.ii)*

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 III.1.8.Mod$_1$) à III.1.8.Mod$_4$).

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.3.4 *Considérons l'ensemble A^A des applications de A dans lui-même muni de la structure $+, *$ définie en III.3.2 et III.3.3.*

i) Il existe un unique morphisme d'anneaux :

$$\phi : A[X] \to A^A , X \mapsto \mathrm{Id}_A \mid \phi \circ i_A = j_A \qquad 1$$

et l'on a alors :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k , \phi(\alpha) = x \mapsto \sum_{k=0}^{\deg(\alpha)} \alpha_k x^k . \qquad 2$$

Preuve *: Il suffit d'appliquer la proposition III.2.9 au morphisme j_A et à $\mathrm{Id}_A \in A^A$.*

ii) Si $\cdot$ désigne la loi externe définie en III.1.7 (resp. la loi externe définie en III.3.3.ii).1), selon le contexte :

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

***Preuve** : Vérification sans difficulté.*

iii)

$$\forall a \in A,\ \forall \alpha \in A[X], \mathrm{ev}_a(\alpha) \ = \ \phi(\alpha)(a) \ = \ \sum_{k=0}^{\deg(\alpha)} \alpha_k a^k \qquad 1$$

qu'on notera bien évidemment $\alpha(a)$.

***Preuve** : Idem.*

Définition III.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.3.6 (Fonctions polynômes) On appelle *ensemble des fonctions polynômes* l'image du morphisme ϕ défini en III.3.4.i).1, dans A^A et *fonction polynôme* un élément de cette image.

Remarque III.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 en III.3.4.i).1 est injectif c'est-à-dire que si deux polynômes définisssent la même fonction polynôme ils sont égaux.

b) En revanche 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 en III.2.1.

III.4 . −Le théorème de la division euclidienne

Dans ce paragraphe (III.4,) $\mathbb{K}$ est un corps et l'on s'intéresse à l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$.

Proposition III.4.1

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

***Preuve** : Résulte de III.2.2.ii).*

Théorème III.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*

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

Preuve *: (cf. III.7.7.)*

Remarque III.4.3 a) On peut faire ici la même observation que dans le cas des entiers relatifs 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. III.2.2.iii).) On a déjà mentionné et on rappelle encore que cet énoncé d'unicité n'est pas nécessaire pour établir que l'anneau $\mathbb{K}[X]$ est principal . et qu'elle n'est pas vérifiée, par exemple, par le stathme euclidien de l'anneau des entiers de GAUSS qui n'en jouit pas moin de toute les propriétés des anneaux principaux.

b) Les termes de *dividende*, *diviseur*, *quotient* et *reste* introduits en I.13.6.1 sont bien entendu, utilisés dans le cas de l'anneau $\mathbb{K}[X]$ et l'on peut même, en vertu de a), parler du reste et du quotient.

Théorème III.4.4 (Structure des idéaux de $\mathbb{K}[X]$) *Une partie $\mathfrak{I} \subset \mathbb{K}[X]$ est un idéal (cf. I.3.5,) de $\mathbb{K}[X]$ si et seulement si :*

$$\exists P \in \mathbb{K}[X],\ \mathfrak{I} = P\mathbb{K}[X] = \{P * Q\ ;\ Q \in \mathbb{K}[X]\} \qquad \textit{III.4.4.1}$$

c'est-à-dire que l'anneau $\mathbb{K}[X]$ est un anneau principal (cf. I.12.2.)

Preuve *:*

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

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

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 . 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.4.5 Dans la proposition précédente, et partant dans le théorème III.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.4.4.1.

III.5 . −Propriétés arithmétiques de l'anneau $\mathbb{K}[X]$

Dans tout ce paragraphe (III.5,) $\mathbb{K}$ est un corps et l'anneau $\mathbb{K}[X]$ est l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ introduit au paragraphe III.2. Son élément neutre que nous avons jusqi'ci noté ζ (resp. son élément unité υ) seront dorénavant noté 0 (resp. 1.)

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.4.2 et son corollaire le théorème III.4.4.

On aurait pu, pour ce paragraphe (III.5,) se contenter d'établir l'existence d'une *division euclidienne* pour l'anneau $\mathbb{K}[X]$ (cf. III.4.2,) la proposition I.13.6.4 assurant alors que l'anneau $\mathbb{K}[X]$ est un anneau principal. Dès lors, tous les résultats dévelopés au paragraphe I.13 et relatifs à l'arithmétique des anneaux principaux s'appliquent à $\mathbb{K}[X]$.

Nous allons cependant passé de nouveau en revue ces résultats en donnant le cas échéant des arguments de preuve particuliers à l'anneau $\mathbb{K}[X]$:

l'existence de PGCD et de PPCM (cf. I.13.1 III.5.1 ;)
le théorème de BÉZOUT (cf. I.13.2.1 III.5.2.1 ;)
le lemme de GAUSS (cf. I.13.2.3 III.5.2.3 ;)
le lemme d'Euclide (cf. I.13.2.6 III.5.2.4 ;)
les applications à l'arithmétique modulaire (cf. I.13.2.8 III.5.3.1 ;)
le théorème chinois des restes (cf. I.13.4.4 III.5.4.1 ;)
le théorème fondamental de l'arithmétique (cf. I.13.5.3 III.5.5.1.)

III.5.0 . −Quelques remarques préliminaires

Certaines notions introduites dans le cadre général des anneaux principaux au paragraphe I.13, revêtent un aspect particulier dans le cas de l'anneau $\mathbb{K}[X]$, elle peuvent en fait être précisées et explicitées :

Remarque III.5.0.1 (Éléments inversibles) L'ensemble $\mathbb{K}[X]^\times$ des éléments inversibles de l'anneau $(\mathbb{K}[X],+,*)$ s'identifie au groupe $\mathbb{K}^\times$ des inversibles de $\mathbb{K}$ lui-même (cf. III.2.5.iii).)

Remarque III.5.0.2 (Éléments associés) Par conséquent, deux éléments P et Q de $\mathbb{K}[X]$ sont *associés* (cf. I.11.2,) si et seulement s'il existe $u \in \mathbb{K}^\times$ tel que $P = u * Q$.

III.5.1 . −PGCD et PPCM dans $\mathbb{K}[X]$

Proposition III.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. I.10.13.)

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 :

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

(voir la proposition I.13.1.3 .)

Définition III.5.1.2 (Identité de BÉZOUT) La formule III.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.5.1.3 L'hypothèse que A est fini dans la proposition III.5.1.1 n'est pas indispensable et l'on peut tout à fait s'en passer comme le montre la preuve de la proposition I.13.1.3

Proposition III.5.1.4 *Toute famille de polynômes admet un PPCM. (voir la proposition I.13.1.6 .)*

III.5.2 . −Théorème de BÉZOUT,

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

Théorème III.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. I.10.11.)*

b) $\bigwedge A = 1$.

c) Il existe un n-uplet de polynômes $U_{i\ ,1\leq i\leq n}$ tel que

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

(voir le théorème I.13.2.1 .)

Remarque III.5.2.2 Le théorème de BÉZOUT III.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 le théorème III.5.4.1 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.5.6.1.)

Théorème III.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 $P|R$.*
(voir le théorème I.13.2.3 .)

Théorème III.5.2.4 (lemme d'Euclide) *Dans l'anneau de polynômes $\mathbb{K}[X]$ tous les éléments irréductibles (cf. I.10.6,) sont premiers (cf. I.10.5.)*
(voir le théorème I.13.2.6 .)

Remarque III.5.2.5 (Éléments irréductibles) Le théorème III.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.5.2.6 *Pour tout $P \in \mathbb{K}[X]$ $\deg(P) = 1$ entraîne P irréductible.*

Preuve *: 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 III.2.2.ii) et III.2.2.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 de III.5.2.5.ii).1 entraîne Q ou R inversible et donc P irréductible.

Remarque III.5.2.7 (Polynômes irréductibles) Nous venons de montrer en III.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. (cf. TD n° V, exercice D et III.7.13.)

III.5.3 . −Arithmétique modulaire sur $\mathbb{K}[X]$

Proposition III.5.3.1 *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible (ou premier non nul ce qui revient au même en vertu du lemme d'Euclide (cf. III.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*.*

Preuve *: (Voir aussi le TD n° V, exercice B.) 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

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

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* $\mathbb{K}[X]/P$*.*

III.5.4 . −Théorème chinois des restes sur $\mathbb{K}[X]$

Théorème III.5.4.1 (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 en I.7.3, 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 :

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

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

Preuve *: (cf. III.7.8.)*

Remarque III.5.4.2 Bien entendu le résultat du théorème III.5.4.1 ci-dessus peut s'étendre à une famille finie de polynômes deux à deux premiers entre eux (cf. TD n° II, exercice B, question 5).)

III.5.5 . −Théorème fondamental de l'arithmétique

Théorème III.5.5.1 (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*

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

III.5.6 . −Algorithme d'Euclide sur $\mathbb{K}[X]$

Proposition III.5.6.1 (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

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

(voir la proposition I.13.6.5 .)

***Preuve** : Seul le point i) de cette proposition nécessite des arguments nouveaux par rapport à ceux donnés pour l'anneau $\mathbb{Z}$. ou dans le cas général pour les anneaux euclidiens dans la proposition I.13.6.5.*

Pour $n \geq 2$, si $P_n \neq 0$, $\deg(P)_n < \deg(P)_{n-1}$ (cf. III.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 . −Étude des racines d'un polynôme

Dans cette section (III.6,) $\mathbb{K}$ est un corps si bien que tou les résultat du paragraphe (III.5,) peuvent être utilisés.

Certain résultat du paragraphe III.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.6.1 *Pour tout polynôme $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ est une racine de P (cf. III.3.5,) si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P \;=\; (X - a) *_{\mathbb{K}[X]} Q$.*

***Preuve** :*

*i) (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.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.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.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 $P \;=\; (X - a) *_{\mathbb{K}[X]} Q$.

ii) ($X - a | P$)

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

Corollaire III.6.2 (Nombre de racines d'un polynôme) *Un polynôme $P \in \mathbb{K}[X]$ non nul possède au plus $\deg(P)$ racines.*

***Preuve** :*

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. III.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.6.3 (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*
$card\Gamma_d \leq d$.

***Preuve** : Le fait que $\#(\Gamma_d) \leq d$ est une conséquence immédiate du corollaire III.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.6.4 (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.

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

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

***Preuve** :*

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

ii) C'est une vérification très élémentaire.

Proposition III.6.5 (Polynômes à racines simples) *Pour tout polynôme $P \in \mathbb{K}[X]$ si P et P' sont premiers entre eux les racines de P sont simples.*

***Preuve** : 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. III.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 $(X-a)^kQU + [k(X-a)^{k-1}Q + (X-a)^kQ']V$ 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 . −Exercices

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 $n \in \mathbb{N}$. On reprends les notations données en III.1.2.

Exercice III.7.1 [Addition]
Pour tout $(a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, on définit l'élément $a +_{A^{\mathbb{N}}} b \in A^{\mathbb{N}}$ par $(a +_{A^{\mathbb{N}}} b)_n := a_n + b_n$.
Montrer que $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}})$ ainsi construit est un groupe abélien dont on précisera l'élément neutre z.
Dorénavant on notera simplement $+$ pour $+_{A^{\mathbb{N}}}$ si aucune confusion n'est à craindre.

Exercice III.7.2 [Multiplication]
Pour tout $(a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, on définit $a *_{A^{\mathbb{N}}} b$ par

$$(a *_{A^{\mathbb{N}}} b)_n := \sum_{k=0}^{n} a_k * b_{n-k} .$$

Montrer que :

1) l'élément $v \in A^{\mathbb{N}}$ défini par

$$v_0 := 1 \text{ et } \forall n \in \mathbb{N},\ n \geq 1 \Rightarrow v_n := 0,$$

est un élément neutre pour $*_{A^{\mathbb{N}}}$;

2)

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} b = b *_{A^{\mathbb{N}}} a ;$$

3)

$$\forall (a, b, c) \in A^{\mathbb{N}} \times A^{\mathbb{N}} \times A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} (b +_{A^{\mathbb{N}}} c) = a *_{A^{\mathbb{N}}} b +_{A^{\mathbb{N}}} a *_{A^{\mathbb{N}}} c .$$

De même on notera $*$ au lieu de $*_{A^{\mathbb{N}}}$ si aucune confusion n'est à craindre.

Exercice III.7.3 [Anneau] Énoncer et démontrer les propriétés de $+_{A^{\mathbb{N}}}$ et $*_{A^{\mathbb{N}}}$ qui font de

$$(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}) \text{ un anneau commutatif .}$$

Exercice III.7.4 [Valuation]

1) Rappeler ce que signifie que l'anneau A est intègre.

On suppose, dans toute la suite de la III.7.4 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.7.5 [Morphisme structural]

Pour tout $a \in A$, **on définit l'élément** $i(a)$ **de** $A^{\mathbb{N}}$ **par**

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

Montrer que l'application $i : A \to A^{\mathbb{N}}$ ainsi définie est un morphisme injectif d'anneaux.

On note désormais

$$\mathcal{P} := \{a \in A^{\mathbb{N}}\ ;\ \exists n \in \mathbb{N},\ \forall p \in \mathbb{N},\ p \geq n \Rightarrow a_p = 0\}$$

le sous-ensemble de $A^{\mathbb{N}}$ **des suites « presque nulles » autrement dit dont le terme est nul à partir d'un certain rang.**

Exercice III.7.6 [degré]

On suppose encore 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 III.7.4.question 6).)

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 défini à la III.7.5, est contenue dans $\mathcal{P}$ et que i est donc un morphisme injectif d'anneaux de A dans $\mathcal{P}$. Caractériser les éléments de $\mathrm{Im}\, i$ par leur degré.

8) Montrer que la restriction $i^{\times}\ :=\ i_{|A^{\times}}$ de i à l'ensemble $A^{\times}$ des éléments inversibles de A est un morphisme bijectif de groupes 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.7.7 [Division euclidienne]

1) Rappeler ce que signifie l'assertion : A est un corps.

On suppose, jusqu'à la fin de III.7.7 que A est un corps.
Soit $b\ \in\ \mathcal{P}, b\ \neq\ \zeta$.

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

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

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

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

4) Montrer finalement que, pour tout $a\ \in\ \mathcal{P}$ il existe un unique $(q,r)\ \in\ \mathcal{P}\ \times\ \mathcal{P}$ tel que :

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

Exercice III.7.8 [Théorème chinois des restes dans $\mathbb{K}[X]$]

Cet exercice particularise, au cas des anneaux de polynômes sur un corps, les résultats obtenus pour des anneaux généraux au TD n° II, exercice B, question 3), ou encore pour les anneaux principaux, dont $\mathbb{K}[X]$ est un cas particulier, en I.13.4.

Dans tout cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur 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 :**

$$\begin{aligned}(\alpha_1, \alpha_2) + (\beta_1, \beta_2) &:= (\alpha_1 + \beta_1, \alpha_2 + \beta_2)\\ (\alpha_1, \alpha_2) * (\beta_1, \beta_2) &:= (\alpha_1 * \beta_1, \alpha_2 * \beta_2)\ .\end{aligned}$$

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

$$\begin{array}{rccc}\phi: & \mathbb{K}[X] & \to & \mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2\\ & Q & \mapsto & (Q \bmod P_1, Q \bmod P_2)\end{array}$$

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.7.9 [Division euclidienne, applications]

1) (**Division euclidienne de polynômes**)

a) Effectuer la division euclidienne de $X^5 + 13X^4 + 11X^3 + 7X^2 + 5X + 3$ par $X^2 + 1$.

b) Calculer le PGCD de $X^6 + 2X^5 + 3X^4 + 5X^3 + 7X^2 + 11X$ et $13X^3 + 17X^2 + 19$.

2) Soient $k \in \mathbb{N}^*$ et $P \in \mathbb{C}[X]$.

a) Montrer qu'il existe

$$P_{j\ ,0\le j\le k-1} \in \mathbb{C}[X]\ |\ P(X^k)\ =\ P_0(X^k)\ +\ XP_1(X^k)\ +\ \ldots\ +\ X^{k-1}P_{k-1}(X^k)\ .$$

b) En déduire le reste de la division de P par $X^k - a, a \in \mathbb{C}$.

c) (**Exemple**)
Déterminer le reste de la division de $X^{38} - X^7 + X^4 - 1$ par $X^5 - 1$.

3) a) (Cours)
Soit $\mathbb{K}$ un corps. Énoncer (sans démonstration) le théorème de division euclidienne dans $\mathbb{K}[X]$.
Soit maintenant $P \in \mathbb{K}[X]$. **Soient** $a, b \in \mathbb{K}$ **distincts et notons** $\alpha := P(a), \beta := P(b)$.

b) Exprimer le reste de la division euclidienne de P par $(X-a)(X-b)$, en fonction de a, b, α et β.

c) Dans $\mathbb{C}[X]$ ou $\mathbb{R}[X]$, donner le reste de la division euclidienne de $(\cos\theta + X\sin\theta)^n$ par X^2+1.

Exercice III.7.10 [**Pgcd** et **Ppcm** de polynômes]

1) (PGCD)
On considère les polynômes à coefficients réels

$$A := X^5 + X^4 - X^3 - 2X^2 - 2X \text{ et } B := X^3 + 4X^2 + 4X + 3\,.$$

a) Déterminer le PGCD D de A et B, et trouver deux polynômes U et V tels que $UA + VB = D$.

b) Factoriser A en facteurs irréductibles, dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.

2) (PGCD de polynômes)
On considère le polynôme à coefficients réels

$$A := X^4 - 4X^3 + 2X^2 + 8X - 8\,.$$

a) Déterminer le PGCD D de A et du polynôme dérivé A', et trouver deux polynômes U et V tels que $UA + VA' = D$.

b) Factoriser A en facteurs irréductibles, dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.

c) Soit $B := (X-1)^2(X^3-3)$.

a) Factoriser B en facteurs irréductibles, dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$ (*on peut admettre, sans le démontrer, que* $X^3 - 3$ *n'a pas de racine dans* $\mathbb{Q}$*).*

b) Donner le PGCD de B et B' *(avec une phrase d'explication, mais sans long calcul).*

3) Soient

$$m \geq 1 \quad n \geq 1 \text{ et } d := m \wedge n$$

des entiers.

a) a) Soit $z \in \mathbb{C}$, montrer que

$$\left(z^m = 1 \text{ et } z^n = 1 \right) \Rightarrow z^d = 1\,.$$

b) En déduire que

$$X^m - 1 \wedge X^n - 1 = X^d - 1\,.$$

b) On suppose $m \geq n$ et on note r le reste de la division euclidienne de m par n.

a) Montrer que le reste de la division de $X^m - 1$ par $X^n - 1$ est $X^r - 1$.

b) Retrouver le résultat de la première question.

c) Soit $P \in \mathbb{C}[X]$.

a) Quel est le PGCD de $P^m - 1$ et $P^n - 1$?

b) Montrer que, si m et n sont premiers entre eux, $(P^m - 1)(P^n - 1)$ divise $(P - 1)(P^{mn} - 1)$.

d) Soit $q \in \mathbb{N}^*$. Donner une condition pour que $1 + X^m + \ldots + X^q$ divise $1 + X^m + \ldots + X^{qm}$.

4) Dans cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ désigne l'anneau des polynômes à une indéterminée sur $\mathbb{K}$.

a) Montrer que l'intersection de deux idéaux de $\mathbb{K}[X]$ est encore un idéal de $\mathbb{K}[X]$.

b) Pour deux polynômes P et Q non nuls, on note M un générateur de $P * \mathbb{K}[X] \cap Q * \mathbb{K}[X]$.

a) Montrer que $P|M$, $Q|M$ et que pour tout $R \in \mathbb{K}[X]$ tel que $P|R$ et $Q|R$, $M|R$.

b) En déduire que $\deg(M)$ est minimal parmi les multiples communs de P et Q.
On dira qu'un élément $\mu \in \mathbb{K}[X]$ est un PPCM de P et Q s'il vérifie les conditions de a).

c) Montrer que $\mu \in \mathbb{K}[X]$ est un PPCM de P et Q si et seulement si μ est un générateur de $P * \mathbb{K}[X] \cap Q * \mathbb{K}[X]$.

d) Que peut-on dire de deux PPCM μ et μ' de P et Q ?

Exercice III.7.11 []
Posons :

$$\forall P \in \mathbb{Q}[X],\ P := \sum_{i=0}^{\delta} a_i X^i\ ,\ \forall p \in \mathcal{P},$$

si $P \neq 0$

$$\begin{aligned} V_p(P) &:= \min_{i=0}^{\delta}(v_p(a_i)) \\ \mathcal{S}(P) &:= \{p \in \mathbb{P}\,;\, V_p(P) \neq 0\} \end{aligned}$$

si $P = 0$

$$\begin{aligned} V_p(P) &:= (+\infty) \\ \mathcal{S}(P) &:= \mathcal{P}\,. \end{aligned}$$

On note encore v_p la *valuation p-adique* (cf. I.13.5.5, I.14.9.) On peut, dans cet exercice, encore remplacer $\mathbb{Z}$ par n'importe quel anneau principal A et $\mathbb{Q}$ par son corps des fractions $\mathbb{K}$.

1) Pour tout $P \in \mathbb{Q}[X] \setminus \{0\}$, vérifier que :

Val$[X]_1$)

$$\forall P \in \mathbb{Q}[X],\ P \in \mathbb{Z}[X] \Leftrightarrow V_p(P) \geq 0\, \forall\, p \in \mathcal{P}\,.$$

Val$[X]_2$) L'ensemble $\mathcal{S}(P)$ est fini.

Soient

$$P \ := \ \sum_{i=0}^{\deg(P)} a_i X^i \text{ et } Q \ := \ \sum_{i=0}^{\deg(Q)} b_i X^i$$

des éléments de $\mathbb{Q}[X] \setminus \{0\}$ **et** $p \in \mathcal{P}$.

2) Montrer que

$$\forall (P,Q) \in \big(\mathbb{Q}[X] \setminus \{0\}\big)^2, \ \forall p \in \mathbb{P}, \ V_p(PQ) \ = \ V_p(P) \ + \ V_p(Q) \, .$$

3) (**Contenu d'un polynôme**)

On définit un invariant numérique associé à un polynôme $P \ := \ \sum_{i=0}^{\deg(P)} a_i X^i \ \in \ \mathbb{Z}[X] \setminus \{0\}$ appelé *contenu du polynôme* P et noté $C(P)$ comme le PGCD des $a_{i \ , 0 \leq i \leq \deg(P)}$. Montrer qu'alors

$$\forall (P,Q) \in \big(\mathbb{Z}[X] \setminus \{0\}\big)^2, \ C(PQ) \ = \ C(P)C(Q) \, .$$

Exercice III.7.12 [Irréductibilité des polynômes à coefficients entiers]

On note encore v_p **la *valuation* p*-adique* (cf. I.13.5.5, I.14.9) et** $V_p(\cdot)$ **la valuation** p**-adique d'un polynôme (cf. III.7.11.) On peut, dans cet exercice, encore remplacer** $\mathbb{Z}$ **par n'importe quel anneau principal** A **et** $\mathbb{Q}$ **par son corps des fractions** $\mathbb{K}$**.Soit** $P \in \mathbb{Z}[X] \setminus \{0\}$. **On suppose qu'il existe**

$$(Q,R) \ \in \ \big(\mathbb{Q}[X] \setminus \mathbb{Q}\big)^2 \mid P \ = \ QR \, .$$

1) Pour tout $p \in \mathcal{P}$, montrer qu'il existe $a \in \mathbb{Z} \setminus \{0\}$, tel que :

i) soit

$$V_p(aQ) \ \geq \ 0 \text{ et } V_p(\frac{1}{a}R) \ \geq \ 0,$$

ii) soit

$$V_p(aR) \ \geq \ 0 \text{ et } V_p(\frac{1}{a}Q) \ \geq \ 0 \, .$$

2) En déduire qu'il existe

$$(Q_1,R_1) \ \in \ \big(\mathbb{Z}[X] \setminus \{-1;1\}\big)^2 \mid P \ = \ R_1Q_1 \, .$$

3) Établir finalement qu'un polynôme $P \in \mathbb{Z}[X] \setminus \{0\}$ unitaire est irréductible dans $\mathbb{Z}[X]$ si et seulement si il l'est dans $\mathbb{Q}[X]$.

Exercice III.7.13 [Polynômes irréductibles de $\mathbb{Q}[X]$]

Soient $a_1, a_2, \ldots, a_n, n \geq 1$ **des entiers deux à deux distincts,**

$$H \ := \ (X - a_1) \ldots (X - a_n) - 1 \, .$$

1) Montrer que H est irréductible dans $\mathbb{Q}[X]$.

2) En déduire qu'il existe une infinité de polynômes de degré n, irréductibles dans $\mathbb{Q}[X]$.

IV . −Réduction des endomorphismes

Dans tout ce chapitre (IV,) $\mathbb{K}$ **est un corps,** E **un** $\mathbb{K}$**-espace vectoriel,** $u \in \mathrm{End}_{\mathbb{K}}(E)$ **un endomorphisme** $\mathbb{K}$**-linéaire de** E **et** $\mathbb{K}[X]$ **l'anneau des polynômes à une indéterminée et à coefficients dans** $\mathbb{K}$.

IV.1 . −Le formalisme des $\mathbb{K}[X]$-modules

Rappel IV.1.1 Soient E un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme κ-linéaire de E. Pour tout polynôme $P \in \mathbb{K}[X]$, l'endomorphisme $P(u) \in \mathrm{End}_{\mathbb{K}}(E)$ est l'image de P par l'unique morphisme d'anneaux

$$\mathbb{K}[X] \to \mathrm{End}_{\mathbb{K}}(E)\ ,\ X \mapsto u \text{ (cf. III.2.9 ;)}$$

c'est-à-dire, pour

$$P = \sum_{i=1}^{r} a_i X^i\ ,\ p(u) = \sum_{i=1}^{r} a_i u^i\ .$$

Le morphisme $\mathbb{K}[X] \to \mathrm{End}_{\mathbb{K}}(E)$ ci-dessus est, en particulier un morphisme $\mathbb{K}[X] \to \mathrm{End}_{\mathbf{Gr}}(E)$ qui définit, en vertu de la proposition A.1.4, une structure de $\mathbb{K}[X]$-module sur E. On constate qu'alors, la structure de $\mathbb{K}[X]$-module est donnée par :

$$\forall P \in \mathbb{K}[X],\ \forall x \in E,\ P \cdot x = P(u)(x)\ . \qquad \text{IV.1.1.1}$$

Il est d'usage de noter $\mathbb{K}[u]$ l'image du morphisme $\mathbb{K}[X] \to \mathrm{End}_{\mathbf{Gr}}(E)$ ci-dessus, qui est un sous-anneau de $\mathrm{End}_{\mathbf{Gr}}(E)$ et même de $\mathrm{End}_{\mathbb{K}}(E)$.

On montre dans le paragraphe (IV.1,) qui suit, qu'il y a en fait correspondance (bijective) entre les $\mathbb{K}[X]$-modules et les couples (E, u) où E est un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. Ce formalisme qu'il n'est pas indispensable d'utiliser dans un premier temps au moins, puisque nous nous attacherons à formuler les énoncés principaux sans y recourir, permet néanmoins d'envisager les résultats des paragraphe qui suivent, dans la perspective de l'appendices B et ainsi de les rapprocher des énoncés obtenus dans le chapitre II

Proposition IV.1.2 *i) Un ensemble E est un $\mathbb{K}[X]$-module si et seulement si E est un $\mathbb{K}$-espace vectoriel muni d'un endomorphisme $u \in \mathrm{End}_{\mathbb{K}}(E)$ tel que pour tout $v \in E$,*

$$X \cdot v = u(v) \text{ (cf. TD n° V, exercice E, question 1) .)}$$

ii) Une application $f : E \to F$ est un morphisme de $\mathbb{K}[X]$-modules si et seulement si E (resp. F,) est un $\mathbb{K}$-espace vectoriel muni d'un endomorphisme $\mathbb{K}$-linéaire

$$u \in \mathrm{End}_{\mathbb{K}}(E)\ ,\ (mathrespv \in \mathrm{End}_{\mathbb{K}}(F)\ ,)$$

$f \in \mathrm{Hom}_{\mathbb{K}}(E, F)$ est une application $\mathbb{K}$-linéaire telle que

$$f \circ u = v \circ f \text{ (cf. TD n° V, exercice E, question 2) .)}$$

iii) Étant donné un $\mathbb{K}[X]$-module E une partie $F \subset E$ est un sous-$\mathbb{K}[X]$-module de E si et seulement si F est un sous-$\mathbb{K}$-espace vectoriel de E stable par l'endomorphisme $u \in \mathrm{End}_{\mathbb{K}}(E)$ définissant la structure de $\mathbb{K}[X]$-module de E (cf. i),) i.e.

$$u(F) \subset F \text{ (cf. TD n° V, exercice E, question 3), a) .)}$$

iv) Un morphisme de $\mathbb{K}[X]$-modules $q : E \to Q$ est un quotient du $\mathbb{K}[X]$-module E c'est-à-dire que q est un morphisme surjectif de $\mathbb{K}[X]$-modules (cf. I.9.4.i),) si et seulement si $\operatorname{Ker} q$ est stable par l'endomorphisme $u \in \operatorname{End}_{\mathbb{K}}(E)$ définissant la structure de E si et seulement si il existe un endomorphisme $v \in \operatorname{End}_{\mathbb{K}}(E)$ tel que

$$v \circ q = q \circ u .$$

***Preuve** : Notons $K := \operatorname{Ker} q$ si bien qu'on a une suite exacte de $\mathbb{K}[X]$-modules :*

$$0 \to K \longrightarrow E \xrightarrow{q} Q \to 0 . \qquad 1$$

La suite 1 est encore une suite exacte de $\mathbb{K}$-espaces vectoriels puisque les notions de noyau et d'image ne concernent que les groupes abéliens sous-jacents.

Pour tout $(x, y) \in E \times E$,

$$y - x \in K \Rightarrow u(x - y) \in K \text{ (cf. iii) ,)}$$

puisque K est un sous-$\mathbb{K}[X]$-module de E. Il en résulte que

$$\forall (x, y) \in E \times E,\ (y - x) \in K \Rightarrow q[u(x)] = q[u(y)] \text{ puisque } \operatorname{Ker} q = K .$$

Pour tout $\alpha \in Q$ on peut donc définir

$$v(\alpha) := q[u(x)] \forall x \in E, \text{ tel que } q(x) = \alpha$$

et l'on a alors

$$v \circ q = q \circ u .$$

On vérifie aisément la réciproque.

Définition IV.1.3 i) Étant donné un $\mathbb{K}[X]$-module, E on parlera du $\mathbb{K}$-*espace vectoriel sous-jacent* qu'on notera $E_{/\mathbb{K}}$ pour désigner E uniquement muni de sa structure de $\mathbb{K}$-espace vectoriel comme en IV.1.2.i). On pourrra désigner l'endomorphisme u défini par l'action de X sur E sous le terme d'*endomorphisme de structure*.

ii) De même pour un morphisme de $\mathbb{K}[X]$-modules $f : E \to F$, on pourra ddésigner sous le terme d'*application linéaire sous-jacente* et noter $f_{/\mathbb{K}}$, le morphisme de $\mathbb{K}$-espaces vectoriels induit par f comme en IV.1.2.ii).

Lemme IV.1.4 *Si $(u, u') \in \operatorname{End}_{\mathbb{K}}(E) \times \operatorname{End}_{\mathbb{K}}(E)$ est tel que $u \circ u' = u' = u' \circ u$ (i.e. u et u' commutent,) pour tout $P \in \mathbb{K}[X]$, $\operatorname{Ker} P(u')$ est stable par u.*

***Preuve** : C'est un résultat bien connu d'algèbre linéaire et que le lecteur aura certainement déjà démontré. Il peut se reformuler en constatant que la condition de commutation entre u et u' a, en particulier pour conséquence, que l'inclusion naturelle $\operatorname{Ker} P(u') \hookrightarrow E$ est un morphisme de $\mathbb{K}[X]$-modules (cf. IV.1.2.ii),) si bien que $\operatorname{Ker} P(u')$ apparaît comme un sous-$\mathbb{K}[X]$-module de E (cf. IV.1.2.iii),) et est donc stable par u. La structure de $\mathbb{K}[X]$-module sur E (et ses sous-modules) est donnée par u.*

Notation IV.1.5 Étant donnés un $\mathbb{K}$-espace vectoriel E et un endomorphisme $\mathbb{K}$-linéaire $u \in \operatorname{End}_{\mathbb{K}}(E)$ on dira que (E, u) (ou simplement E si ce n'est pas ambigu) est monogène engendré par $x \in E$ s'il existe

$$x \in E \text{ tel que } E = \operatorname{Vect}\big\{\{u^n(x)\}, n \in \mathbb{N}\big\} .$$

À noter que cela signifie exactement que (E, u) est monogène au sens des $\mathbb{K}[X]$-modules (cf. II.1.7.)

IV.2 . −Polynômes annulateurs (cf. II.5, A.7)

Les polynômes annulateurs, polynômes minimaux d'un endomorphisme ont déjà été étudiés en algèbre linéaire. On aimerait cependant insister dans ce paragraphe (IV.2,) sur le parallèle entre ces notions et celles d'ordre d'un éléments dans un groupe abéliens et d'exposant d'un groupe abélien étudiées au paragraphe II.5. Ce parallèle est bien entendu beaucoup plus que formel puisque l'on s'apercevra que les objet étudiés ici et ceux respectivement étudiés pour les groupes sont des cas particuliers de ceux introduits pour les A-modules au paragraphe A.7. **Dans ce paragraphe (IV.2,) E est un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E, si bien que (E, u) est muni de la structure de $\mathbb{K}[X]$-module étudiée au paragraphe IV.1.**

Lemme IV.2.1 ((cf. II.5.1, A.7.1)) *Pour tout*

$$x \in E \text{ et } P \in \mathbb{K}[X],$$

il est équivalent que $P \cdot x = 0$, *ou* $P(u)(x) = 0$, *ou que le morphisme de* $\mathbb{K}[X]$*-modules*

$$\mathbb{K}[X] \to E\ ,\ Q \mapsto Q \cdot x = Q(u)(x) \qquad \textit{IV.2.1.1}$$

se factorise en un morphisme

$$\begin{array}{rcl} & & \mathbb{K}[X] \\ & & \downarrow \qquad \searrow_{Q \mapsto Q\cdot x\, =\, Q(u)(x)} \\ \mathbb{K}[X]/P\mathbb{K}[X] & \to & E\ . \end{array} \qquad \textit{IV.2.1.2}$$

Définition IV.2.2 ((cf. II.5.2, A.7.2)) i) (**Élément de torsion**)

Si x et P vérifient les conditions équivalentes du lemme IV.2.1 ci-dessus, on dit que x est de P*-torsion*.

On dit que $x \in E$ est *de torsion* s'il existe $P \in \mathbb{K}[X]$ $P \neq 0$, tel que x soit de P-torsion, *i.e.* tel que

$$P \cdot x = P(u)(x) = 0\ .$$

ii) (**Partie de P-torsion**)

Pour tout polynôme $P \in \mathbb{K}[X]$, on note

$$E[P] := \mathrm{Ker}\, P(u) = \{x \in E\ ;\ P(u)(x) = 0\} = \{x \in E\ ;\ P \cdot x = 0\}$$

le sous-ensemble de E formé des éléments de P-torsion. On appelle $E[P]$ la *partie de P-torsion* de E.

iii) (**Polynôme minimal en x**)

Pour tout $x \in E$, on dit que $P \in \mathbb{K}[X]$ est un *polynôme minimal en x* si le morphisme

$$\mathbb{K}[X]/P\mathbb{K}[X] \to E\ ,\ \overline{P} \mapsto P \cdot x = P(u)(x) \text{ (cf. IV.2.1.2)}$$

est injectif ou, ce qui revient au même, si $P\mathbb{K}[X]$ est le noyau $\mathrm{Ann}_{\mathbb{K}[X]}(x)$ du morphisme IV.2.1.1.

Il est usuel d'appeler le *polynôme minimal en x* qu'on note $P^x_{\min u}$ le représentant unitaire de la classe d'association des polynômes minimaux en x.

Le degré de $P^x_{\min u}$ est la dimension (en tant que $\mathbb{K}$-espace vectoriel) de l'image du morphisme IV.2.1.2 qui est encore l'image du morphisme IV.2.1.1 (cf. TD n° V, exercice C.)

iv) (**Polynôme minimal**)
L'ensemble

$$\begin{aligned}\mathrm{Ann}_{\mathbb{K}[X]}(E) & \\ &:= \{P \in \mathbb{K}[X]\,;\, \forall x \in E,\ P(u)(x) = 0\} \\ &= \{P \in \mathbb{K}[X]\,;\, \forall x \in E,\ P \cdot x = 0\} \\ &= \bigcap_{x \in E} \mathrm{Ann}_{\mathbb{K}[X]}(x)\end{aligned}$$

est un idéal de $\mathbb{K}[X]$ (qui n'est autre que l'idéal annulateur $\mathrm{Ann}_{\mathbb{K}[X]}((E,u))$ du $\mathbb{K}[X]$-module (E,u),) dont un générateur unitaire est appelé *polynôme minimal* de u et usuellement noté $P_{\min u}$.
Un élément de $\mathrm{Ann}_{\mathbb{K}[X]}(E)$ est appelé *polynôme annulateur* de u.

v) (**Partie de torsion**)
On note

$$\mathrm{Tor}_{\mathbb{K}[X]}(E) \text{ ou tout simplement } \mathrm{Tor}(E) := \bigcup_{P \in \mathbb{K}[X] \setminus \{0\}} E[P] = \bigcup_{P \in \mathbb{K}[X] \setminus \{0\}} \mathrm{Ker}\, P(u)$$

l'ensemble des éléments de torsion de E qu'on appelle la *partie de torsion* de E.

vi) On dit que E est *de torsion* si

$$E = \mathrm{Tor}(E)\,.$$

vii) On dit que E est *sans torsion* si

$$\mathrm{Tor}(E) = \{0\}\,.$$

Proposition IV.2.3 (Polynômes minimaux (cf. II.5.3, A.7.3)) *i) Le polynôme minimal*

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

ii) L'idéal

$$\begin{aligned}P_{\min u}\mathbb{K}[X] &= \mathrm{Ann}_{\mathbb{K}[X]}((E,u)) \\ &= \{P \in \mathbb{K}[X]\,;\, \forall x \in E,\ P(u)(x) = 0\} \\ &= \{P \in \mathbb{K}[X]\,;\, \forall x \in E,\ P \cdot x = 0\}\end{aligned}$$

est le noyau du morphisme d'anneaux

$$\mathbb{K}[X] \to \mathrm{End}_{\mathbb{K}}(E)\,,\ X \mapsto u\,.$$

iii) Si F est un sous-$\mathbb{K}$-espace vectoriel de E stable par u (i.e. un sous $\mathbb{K}[X]$-module de $(E?u)$, (cf. IV.1.2.iii),)

$$P_{\min u_{|F}} | P_{\min u}\,.$$

iv) Si F est un $\mathbb{K}$-espace vectoriel, $v \in \mathrm{End}_{\mathbb{K}}(F)$ un endomorphisme κ-linéaire de F et $f : E \to F$ une application $\mathbb{K}$-linéaire telle que $v \circ f = f \circ u$, (i.e. un morphisme de $\mathbb{K}[X]$-modules (cf. IV.1.2.ii),)) alors

$$\forall x \in E,\ P^{f(x)}_{\min v} | P^{x}_{\min u}$$

avec égalité si f est injective.

De plus, si f est surjective,

$$P_{\min v} | P_{\min u}$$

avec égalité si f est injective.

Proposition IV.2.4 ((cf. II.5.4, A.7.4)) *i) Pour tout $P \in \mathbb{K}[X]$, $\mathrm{Ker}\, P(u) = E[P]$ est un sous-$\mathbb{K}$-espace vectoriel de E stable par u i.e. un sous-KkX-module (cf. IV.1.2.iii),) de (E, u).*

ii) Étant donnés un $\mathbb{K}$-espace vectoriel F muni d'un endomorphisme v, un morphisme de $\mathbb{K}$-espaces vectoriels (i.e. une application linéaire) $f : E \to F$ vérifiant $v \circ f = f \circ u$ (i.e. définissant un morphisme de $\mathbb{K}[X]$-modules $(E, u) \to (F, v)$ (cf. IV.1.2.ii),)) pour tout

$$P \in \mathbb{K}[X] f(\mathrm{Ker}\, P(u)) = f(E[P]) \subset \mathrm{Ker}\, P(v) = F[P]$$

si bien que f définit un morphisme (de $\mathbb{K}$-espace vectoriels mais encore de $\mathbb{K}[X]$-modules et même de $\mathbb{K}[X]/P$-modules)

$$f[P] := f_{|E[P]} : E[P] \to F[P]\,.$$

Ce dernier morphisme est un isomorphisme dès que f en est un.

*iii) (**lemme des noyaux**)*

Étant donnés des polynômes P, Q et R dans $\mathbb{K}[X]$ tels que $P = QR$ et Q et R sont premiers entre eux,

$$\mathrm{Ker}\, P(u) = \mathrm{Ker}\, Q(u) \oplus \mathrm{Ker}\, R(u)$$

et de plus, les projections

$$\pi_Q : \mathrm{Ker}\, P(u) \to \mathrm{Ker}\, Q(u) \text{ et } \pi_R : \mathrm{Ker}\, P(u) \to \mathrm{Ker}\, R(u) \text{ sont des polynômes en } u\,.$$

***Preuve** : Puisque Q et R sont premiers entre eux, il existe, d'après le théorème de* BÉZOUT,

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

Il s'ensuit que :

$$\forall v \in E,\ (AQ)(u)(v) + (BR)(u)(v) = v, \qquad 1$$

puis que :

$$\begin{array}{lrcl} \forall v \in \mathrm{Ker}\,(PQ)(u), & (AQ)(u) \circ (AQ)(u)(v) & = & (AQ)(u) \circ (AQ + BR)(u)(v) \\ & & = & (AQ)(u)(v) \\ \big(\textit{resp.} & (BR)(u) \circ (BR)(u)(v) & = & (BR)(u) \circ (AQ + BR)(u)(v) \\ & & = & (BR)(u)(v)\ .\big)\,. \end{array} \qquad 2$$

En posant

$$\pi_Q := (BR)(u) : \mathrm{Ker}\, P(u) \to \mathrm{Ker}\, Q(u) \text{ et } \pi_R := (AQ)(u) : \mathrm{Ker}\, P(u) \to \mathrm{Ker}\, R(u),$$

π_Q et π_R sont, par définition des polynômes en u. Le calcul 2 ci-dessus montre que π_Q et π_R sont des projecteurs. Enfin l'égalité 1 assure que

$$\pi_Q + \pi_R = \mathrm{Id}_{\mathrm{Ker}\, P(u)}$$

ce qui achève la preuve.

iv) De plus si $R = P_{\min u}$ *est le polynôme minimal de* u *sur* E,

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

v) S'il existe $(x, y) \in E \times E$ *de polynômes minimaux respectifs* P *et* Q

$$(\textit{i.e.}\ ,\ P^x_{\min u} = P \ \mathrm{et}\ P^y_{\min u} = Q\ ,)$$

il existe $z \in E$ *dont le polynôme minimal local est le* ***Ppcm*** *de* P *et* Q.

Proposition IV.2.5 ((cf. II.5.7, A.7.6)) *Si* E *est de dimension finie,* (E, u) *est de torsion si et seulement si* $P_{\min u} \neq 0$ *(i.e.* $\mathrm{Ann}_{\mathbb{K}[X]}(E) \neq \{0\}$*.)*

Proposition IV.2.6 (cf. II.5.8) *Les assertions suivantes sont équivalentes :*

a) Le $\mathbb{K}[X]$*-module* E *est de type fini et de torsion*

b) Le $\mathbb{K}[X]$*-module* E *est de type fini et* $P_{\min u} \neq 0$.

c) Le $\mathbb{K}$*-espace vectoriel sous-jacent* $E_{/\mathbb{K}}$ *est de dimension finie.*

Preuve *:*

i) ***(a)*** $\Leftrightarrow$ ***b))***
Est pour ainsi dire tautologique.

ii) ***(c)*** $\Rightarrow$ ***b))***
Ce résultat peut, bien entendu, être vu comme une conséquence du théorème IV.7.2 (de CAYLEY–HAMILTON*,) mais ce dernier, outre qu'il done un énoncé beaucoup plus précis, fait appel à des constructions nettement plus élaborées que celles dont on a besoin ici.*

En effet, si $\dim_{\mathbb{K}} E = n$, $\dim_{\mathbb{K}} \mathrm{End}_{\mathbb{K}}(E) = n^2$. *Le sous-ensemble* $\{u^i\}_{,i \leq 0 \leq n^2}$ *est donc une partie liée du* $\mathbb{K}*$*-espace vectoriel* $\mathrm{End}_{\mathbb{K}}(E)$. *Il existe donc* $a_{i\ ,0 \leq i \leq n^2} \in \mathbb{K}$ *non tous nuls tels que*

$$\sum_{i=0}^{n^2} a_i u^i = 0$$

ce qui assure l'existence d'un polynôme annulateur non nul.

iii) ***(a)*** $\Rightarrow$ ***c))***
(cf. TD n° V, exercice E, question 4).)

IV.3 . −Sous-espaces caractéristiques (cf. II.8, B.2)

Définition IV.3.1 (Espaces caractéristiques (cf. II.8.2, B.2.2)) Si P est un facteur irréductible de $P_{\min u}$, il existe un plus grand entier α (la valuation P-adique de $P_{\min u}$,) tel que $P^\alpha | P_{\min u}$. On a alors

$$\operatorname{Ker} P^\alpha(u) \;=\; \bigcup_{n\in\mathbb{N}} \operatorname{Ker} P^n(u)$$

qui n'est autre que la composante P-primaire du $\mathbb{K}[X]$-module E et qu'on appelle *sous-espaces caractéristiques* de u associé au facteur P^α du polynôme minimal $P_{\min u}$ de u ou simplement à l'élément irréductible P.

Théorème IV.3.2 ((cf. II.8.3, B.2.3)) *Si $P_{\min u} \;=\; \prod_{i=1}^{r} P_i^{\alpha_i}$ avec P_i irréductible, P_i et P_j premiers entre eux si $i \neq j$, (autrement dit si on a décomposé $P_{\min u}$ en produits d'irréductibles dans l'anneau principal $\mathbb{K}[X]$ (cf. I.13.5.3,)) on note*

$$E_i \;:=\; \operatorname{Ker} P_i^{\alpha_i}(u) \;=\; E[P_i^{\alpha_i}],$$

alors :

i)

$$E \;=\; \bigoplus_{i=1}^{r} E_i \;;$$

***Preuve** : On peut bien entendu appliquer le lemme des noyaux IV.2.4.iii) qui, joint à un argument de récurrence, donne ce résultat. On peut également le considérer comme une conséquence, dans le cas particulier des $\mathbb{K}[X]$-modules du théorème B.2.3.*

ii) pour tout $1 \;\leq\; i \;\leq\; r$ E_i est stable par u ;

***Preuve** : C'est une conséquence du lemme IV.1.4 ou bien du fait que la décomposition donnée en i) $E \;=\; \bigoplus_{i=1}^{r} E_i$ est en fait une décomposition en somme directe de $\mathbb{K}[X]$-modules.*

iii) le polynôme minimal de $u_{|E_i}$ est $P_i^{\alpha_i}$;

***Preuve** : C'est exactement l'énoncé B.2.3.iii).*

iv)

$$\pi_i \;:\; E \;\to\; E_i \text{ est un polynôme en } u \;.$$

***Preuve** : C'est encore une conséquence de la proposition IV.2.4.iii).*

Remarque IV.3.3 Dans le théorème ci-dessus on s'aperçoit qu'on a seulement l'analogue de l'isomorphisme II.8.3.2 puisque le polynôme minimal $P_{\min u}$ est l'analogue de l'exposant du groupe abélien, *i.e.* un générateur de l'idéal annulateur. Cependant, on ne dispose pas encore à ce point, d'un analogue du cardinal du groupe. Le *polynôme caractéristique* (cf. IV.6.1,) aura tendance à jouer ce rôle, surtout au vu du théorème de CAYLEY–HAMILTON (cf. IV.7.2,) qui pourrait alors s'interpréter comme un analogue du théorème de LAGRANGE.

Exemple IV.3.4 Soit u un projecteur, $u^2 \;=\; u$;

$$P_{\min u} \;=\; X^2 - X \;=\; X(X-1) \text{ d'où } E \;=\; \operatorname{Ker} u \;\oplus\; \operatorname{Ker} u - \operatorname{Id}_E \;.$$

IV.4 . −Endomorphismes cycliques, vecteurs cycliques, ($\mathbb{K}[X]$-modules cycliques) (cf. II.9, B.3)

Proposition IV.4.1 (Espaces cycliques (cf. II.9.1, B.3.1)) *Soient E un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. Alors les assertions suivantes sont équivalentes :*

a)

$$E \text{ est de dimension finie } \dim_{\mathbb{K}} E = \deg(P_{\min u}) \text{ (cf. IV.2.2.iv) .)}$$

b)

$$E \text{ est de dimension finie et } \exists x \in E, \text{ tel que } \dim_{\mathbb{K}} E = \deg(P^x_{\min u}) .$$

c) (E, u) *est monogène et le $\mathbb{K}$-espace vectoriel E est de dimension finie.*

d) (E, u) *est monogène, engendré par $x \in E$ et $P^x_{\min u} \neq 0$ (cf. IV.2.2.i).)*

e) Il existe $P \in \mathbb{K}[X]$, $P \neq 0$, tel que le morphisme d'anneaux

$$\mathbb{K}[X] \to \mathrm{End}_{\mathbb{K}}(E) , \ X \mapsto u$$

induise un isomorphisme (aussibien de $\mathbb{K}$-espaces vectoriels que de $\mathbb{K}[X]$-modules,)

$$\mathbb{K}[X]/P\mathbb{K}[X] \cong E .$$

f) Le $\mathbb{K}[X]$-module (E, u) est isomorphe à $\mathbb{K}[X]/\mathrm{Ann}_{\mathbb{K}[X]}((E, u)) = \mathbb{K}[X]/P_{\min u}\mathbb{K}[X]$ et $P_{\min u}\mathbb{K}[X] = \mathrm{Ann}_{\mathbb{K}[X]}((E, u)) \neq \{\}0$.

g) Il existe un entier $d \in \mathbb{N}$ et un $\mathbb{K}[X]$-morphisme

$$\phi : \mathbb{K}[X] \to (E, u) \text{ tels que } \{\phi(1), \phi(X), \ldots, \phi(X^{d-1})\}$$

est une $\mathbb{K}$-base du $\mathbb{K}$-espace vectoriel E.

h) Il existe un entier $d \in \mathbb{N}$ et un élément $x \in E$ tels que $\{x, u(x), \ldots, u^{d-1}(x)\}$ est une base du $\mathbb{K}$-espace vectoriel E.

i) Le $\mathbb{K}$-vectoriel E est de dimension finie et

$$\dim_{\mathbb{K}} E = \deg(P_{\min u}) .$$

j) Il existe une base du $\mathbb{K}$-espace vectoriel E dans laquelle la matrice de u est :

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix} \qquad 1$$

Preuve : *Cet énoncé étant l'exact analogue de la proposition II.9.1, certains arguments de preuve seront donnés ici tandis que d'autres seront donnés dans la preuve de II.9.1 laissant le lecteur faire le parallèle entre ces deux preuves et les compléter.*

i) ***(a) $\Rightarrow$ b))***
Notons $d := \dim_{\mathbb{K}} E = \deg(P_{\min u})$ *et* $\varepsilon_i\,, 1 \leq i \leq d$ *une base de* E. *Pour tout*

$$1 \leq i \leq d P^{\varepsilon_i}_{\min u} | P_{\min u}$$

si bien que si on note μ *le* ***Ppcm*** *des* $P^{\varepsilon_i}_{\min u}\,, 1 \leq i \leq d$, $\mu | P_{\min u}$.
Or :

$$\forall y \in E,\ \exists a_i\,, 1 \leq i \leq d \in \mathbb{K}^n,\ y = \sum_{i=1}^{d} a_i \varepsilon_i$$

si bien que :

$$\begin{aligned} \mu(u)(y) &= \mu(u)\big(\sum_{i=1}^{d} a_i \varepsilon_i\big) \\ &= \sum_{i=1}^{d} a_i \mu(u)(\varepsilon_i) \\ &= 0 \end{aligned}$$

ce qui entraîne donc que $P_{\min u} | \mu$ *et donc finalement*

$$\mu = P_{\min u}\ .$$

De plus, il résulte de IV.2.4.v) que

$$\exists x \in E,\ \text{tel que } P^x_{\min u} = \mu = P_{\min u}\ .$$

Donc

$$\dim_{\mathbb{K}} E = \deg(P^x_{\min u})\ .$$

ii) ***(b) $\Rightarrow$ c))***
Soit $x \in E$ *tel que* $\dim_{\mathbb{K}} E = \deg(P^x_{\min u})$ *et* $F := \mathrm{Vect}\big\{\{u^n(x)\}\,, n \in \mathbb{N}\big\}$ *le sous-espace monogène de* E *engendré par* x. *Alors :*

$$\dim_{\mathbb{K}} F = \deg(P^x_{\min u}) = \dim_{\mathbb{K}} E \text{ (cf. TD n° V, exercice C ;)}$$

d'où $F = E$.

iii) ***(c) $\Rightarrow$ d))***
Immédiat.

iv) ***(d) $\Rightarrow$ e))***
(cf. TD n° V, exercice C.)

v) ***(f) $\Leftrightarrow$ e))***
Est immédiat.

*vi) (**f**) $\Rightarrow$ **g**))*
Notons

$$\psi \,:\, (E,u) \,\cong\, \mathbb{K}[X]/P_{min\,u}\mathbb{K}[X] \,=\, \mathbb{K}[X]/\mathrm{Ann}_{\mathbb{K}[X]}((E,u))\,,\ \pi \,:\, \mathbb{K}[X] \,\to\, \mathbb{K}[X]/P_{min\,u}\mathbb{K}[X]$$

et

$$\phi \,:=\, \pi \,\circ\, \psi\,.$$

Or $\mathbb{K}[X]/P_{min\,u}\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel de dimension $\deg(P_{min\,u})$ dont

$$\big(\pi(1), \pi(X), \ldots, \pi(X^{\deg(P_{min\,u})-1})\big) \text{ est une base (cf. TD n° V, exercice C, question 2).}$$

*vii) (**g**) $\Rightarrow$ **h**))*
Il suffit de prendre l'image de la base

$$\{1 \bmod P, \ldots, X^{\deg(P)-1} \bmod P\}$$

par l'isomorphisme

$$(E,u) \,\cong\, \mathbb{K}[X]/P_{min\,u}\mathbb{K}[X] \,=\, \mathbb{K}[X]/\mathrm{Ann}_{\mathbb{K}[X]}((E,u))\,.$$

*viii) (**h**) $\Rightarrow$ **c**))*
Immédiat.

*ix) (**h**) $\Rightarrow$ **a**))*
L'ensemble $\{x, u(x), \ldots, u^{d-1}(x)\}$ est une base il existe donc un unique d-uplet

$$a_{i\ ,0\le i\le d-1} \text{ tel que } u^d(x) \,=\, \sum_{i=0}^{d-1} a_i u^i(x)\,.$$

Notons

$$P \,:=\, X^d - \sum_{i=0}^{d-1} a_i X^i \,\in\, \mathbb{K}[X]\,.$$

Alors :

$$\begin{aligned}
\forall 0 \le k \le d-1,\ P\cdot u^k(x) \quad &=\quad P(u)[u^k(x)] \\
&=\qquad [u^d - \sum_{i=0}^{d-1} a_i u^i][u^k(x)] \\
&=\qquad [u^{d+k} - \sum_{i=0}^{d-1} u^{i+k}](x) \\
&=\qquad u^k[\big(u^d - \sum_{i=0}^{d-1} a_i u^i\big)(x)] \\
&=\qquad 0\,.
\end{aligned}$$

Il s'ensuit, puisque $\{u^k(x)\}_{,1\,\le\, k\,\le\, d-1}$ est une base de E, que $P(u) \,=\, 0$ (i.e. est l'endomorphisme nul de E.) Le polynôme P est donc un polynôme annulateur de u. Par ailleurs si

$$Q \,:=\, \sum_{i=0}^{r} b_i X^i \text{ est un polynôme annulateur de } u,$$

$$\forall y \in E,\ Q(u)(y) \,=\, 0\,.$$

En particulier :

$$\begin{aligned} & Q(u)(x) &=& \ 0 \\ \Leftrightarrow \quad & \sum_{i=0}^{r} b_i u^i(x) &=& \ 0 \end{aligned}$$

ce qui entraîne

$$r \ \geq d \text{ ou } \forall 0 \leq i \leq r,\ b_i \ = \ 0$$

puisque $\{u^k(x)\}\,,1 \leq k \leq d-1$ *est une partie libre de* E. *Ceci assure que* P *est le polynôme minimal de* u *et donc que*

$$\deg(P_{\min u}) \ = \ \dim_{\mathbb{K}} E\,.$$

*x) **(f)** $\Leftrightarrow$ **i))***
(cf. TD n° V, exercice C.)

*xi) **(h)** $\Leftrightarrow$ **j))***
(cf. DOC n° III, n° III.1.exercice A.)

Définition IV.4.2 (Espaces cycliques (cf. II.9.2, B.3.2)) Si un couple (E,u) vérifie les assertions équivalentes de la proposition IV.4.1, on dit que :

i) (E,u) est un *espace cyclique* ; ce qui équivaut en fait au fait que (E,u) est un $\mathbb{K}[X]$-module cyclique au sens de la définition B.3.2.

ii) On dit aussi que u est un *endomorphisme cyclique*.

iii) Si (E,u) est un espace cyclique, un élément $x \in E$ tel que $E \ = \ \mathrm{Vect}\big\{\{u^n(x)\}\,,n \in \mathbb{N}\big\}$ est un *vecteur cyclique*.

Remarque IV.4.3 Il se peut qu'on trouve des définitions moins restrictives de vecteurs cyclique, typiquement que la partie $\{u^n(v)\}_{n \in \mathbb{N}}$ soit génératrice sans exiger qu'une partie finie le soit. Cela permet de tenir compte du cas où $\mathrm{Ann}_{\mathbb{K}[X]}(M) \ = \ \{0\}$, que nous avons exclu dans le cas des modules cycliques.

Définition IV.4.4 (Matrice compagnon) Une matrice comme en IV.4.1.j).1 s'appelle *matrice compagnon* du polynôme minimal

$$P_{\min u} \ = \ X^d + \sum_{i=0}^{d-1} a_i X^i \text{ de } u\,.$$

Proposition IV.4.5 (Sous-espace cyclique (cf. II.9.3, B.3.5)) *Soient*

$$E \text{ un } \mathbb{K}-\text{espace vectoriel et } u \ \in \ \mathrm{End}_{\mathbb{K}}(E) \text{ un endomorphisme } \mathbb{K}-\text{linéaire de } E\,.$$

Pour tout polynôme $P \ \in \ \mathbb{K}[X]$, *les données suivantes sont équivalentes :*

a) Un sous-$\mathbb{K}$*-espace vectoriel* $F \ \subset \ E$ *stable par* u *(i.e. un sous-*$\mathbb{K}[X]$*-module de* (E,u)*,) tel que* $(F, u_{|F})$ *soit cyclique avec* $P_{\min u_{|F}} \ = \ P$.

b) Un élément $x \ \in \ E$ *de polynôme minimal* $P^x_{\min u}$ *égal à* P.

Proposition IV.4.6 (Théorème chinois des restes (cf. II.9.4, B.3.6)) *Si (E, u) est un espace cyclique de polynôme minimal*

$$PQ \text{ avec } (P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \text{ premiers entre eux ,}$$

alors

$$E = \operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u) = E[P] \oplus E[Q]$$

et

$$\operatorname{Ker} P(u) (\text{resp. } \operatorname{Ker} Q(u)) \text{ est cyclique de polynôme minimal } P \text{ (resp. } Q \text{ .)}$$

Réciproquement si F et G sont deux sous-espaces cycliques de E de polynomes minimaux respectifs P et Q premiers entre eux, la sommes $F + G$ et directe et le sous-espace $F \oplus G$ est cyclique de polynômes minimal PQ.

Preuve *: (cf. TD n° VI, exercice C,) sachant que cet énoncé n'est autre en fait que le théorème chinois des restes.*

Remarque IV.4.6.1 C'est exactement le théorème IV.3.2 dans le cas cyclique.

Corollaire IV.4.7 ((cf. II.9.5, B.3.7)) *Soient $(x, y) \in E \times E$ de polynômes annulateurs respectifs P et Q premiers entre eux. Alors il existe $z \in E$ de polynôme annulateur PQ.*

IV.5 . −Valeurs propres, vecteurs propres, espaces propres

Lemme IV.5.1 *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 $X - \lambda = P_{\min u} x$ soit le polynôme minimal de u en x (cf. IV.2.2.iii) ;)

d)

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

***Preuve** :*

*i) (**a**) $\Leftrightarrow$ **b**))*
Est tautologique.

*ii) (**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

$$P^x_{\min u} = X - \lambda \ .$$

*iii) (**c**) $\Rightarrow$ **d**))*
(cf. IV.2.3.i).)

*iv) (**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 de la proposition IV.2.4.iii) 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

$$(u - \lambda \mathrm{Id}_E)^\ell \neq 0 \text{ et } (u - \lambda \mathrm{Id}_E)^{\ell+1} (w) = 0 \ .$$

Posant

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

Définition IV.5.2 (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 IV.5.1. Il est usuel de noter $\mathrm{Sp}(u)$ et d'appeler *spectre* de u l'ensemble des valeurs propres de u.

ii) (**Vecteur propre**)
Un vecteur $x \in E$ vérifiant (de manière équivalente) IV.5.1.b) ou IV.5.1.c) 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 $\{0\}$.)

Remarque IV.5.3 i) Bien entendu pour λ une valeur propre de u, l'espace propre associé à λ est un sous-espace (stable par u) du sous-espace caractéristique associé à $X - \lambda$ (cf. IV.3.1.)

ii) Il se peut tout à fait que le spectre d'un endomorphisme u soit vide. En effet, le spectre de u est en bijection avec les facteurs irréductibles de degré 1 de $P_{\min u}$ (cf. IV.5.1.d).) Or, quitte à définir u comme l'endomorphisme associé à une matrice compagnon arbitraire (cf. IV.4.4,) on peut fixer arbitrairement le polynôme minimal de u.

Si donc on sait construire des polynômes irréductibles de degré > 1, on sait construire des endomorphismes sans valeurs propres.

Ceci n'arrive jamais dans $\mathbb{C}[X]$ (où un polynôme est irréductible si et seulement si il est de degré 1 – théorème de D'ALEMBERT–GAUSS –,) et par conséquent, tout endomorphisme d'un $\mathbb{C}$-espace vectoriel possède toujours des valeurs propres.

En revanche on sait qu'il existe des polynômes de degré 2 irréductibles dans $\mathbb{R}[X]$. On a même montré au TD n° V, qu'il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

iii) Pour peu qu'on l'ait défini, on peut encore donner une caractérisation des valeurs propres en termes du polynôme caractéristique de u IV.6.2.

Définition IV.5.4 On dit que u est *diagonalisable* si E est somme directe des espaces propres de u.

Proposition IV.5.5 *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 si et seulement si pour tout $1 \leq i \leq r$, la restriction $u_{|E_i}$ au sous-espace caractéristique (cf. IV.3.1,) est diagonalisable, si et seulement si les sous-espaces propres de u sont ses sous-espaces caractéristiques.

Définition IV.5.6 On dit que u est trigonalisable s'il existe une base dans laquelle la matrice de u est triangulaire supérieure.

Proposition IV.5.7 *L'endomorphisme u est trigonalisable si et seulement si $P_{\min u}$ est scindé.*

IV.6 . −Polynôme caractéristique

Définition IV.6.1 (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 IV.6.2 *Un élément $\lambda \in \mathbb{K}$ est une valeur propre de u (cf. IV.5.2.i),) si et seulement si $P_{car\, u}(\lambda) = 0$ i.e. λ est une racine de $P_{car\, u}$.*

Preuve *: 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 IV.5.1.a) des valeurs propres.*

Lemme IV.6.3 *i)*

$$\deg(P_{car\, u}) = \dim_{\mathbb{K}} E .$$

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

$$a_{d-1} = -\mathrm{Tr}(u) \text{ et } a_0 = (-1)^d \det(u) .$$

iii) Si $E = F \oplus G$ avec F et G stables par u,

$$P_{car\, u} = P_{car\, u_{|F}} \cdot P_{car\, u_{|G}} .$$

Preuve *: (cf. D.18.1.)*

Proposition IV.6.4 *Si (E, u) est un espace cyclique (cf. IV.4.2,)*

$$P_{car\, u} = P_{min\, u} .$$

Preuve *: (cf. DOC n° III, n° III.1.exercice C.)*

IV.7 . –Théorème de CAYLEY–HAMILTON

Remarque IV.7.1 On va démontrer, dans ce paragraphe (IV.7,) le théorème de CAYLEY–HAMILTON qui assure que le polynome minimal $P_{\min u}$ d'un endomorphisme u d'un $\mathbb{K}$-espace vectoriel E de dimension finie (cf. IV.2.2.iv),) divise son polynôme caractéristique $P_{\text{car } u}$. (cf. IV.6.1.) Ceci peut encore s'exprimer par le fait que le polynôme $P_{\text{car } u}$ est un polynôme annulateur de u.

i) On verra au paragraphe IV.11 qu'on peut déduire le théorème de CAYLEY–HAMILTON du théorème IV.11.5 de réduction de FROBENIUS. Nous allons cependant en donner ici une preuve qui n'utilise pas le résultat précité (cf. IV.7.2.)

ii) (**Le cas des espaces cycliques**)

Dans le cas où (E, u) est un espace cyclique (cf. IV.4.2.i),) le théorème est une conséquence immédiate de la proposition IV.6.4 ; cette dernière étant d'ailleurs un ingrédient essentiel de la preuve du théorème de CAYLEY–HAMILTON à partir de la réduction de FROBENIUS.

iii) On a vu que pour tout $\lambda \in \mathbb{K}$, λ est valeur propre de u si et seulement si $(X, \lambda)|P_{\min u}$ (cf. IV.5.1.d).) On a également vu en IV.6.2 que λ est valeur propre de u si et seulement si $(X, -\lambda)|P_{\text{car } u}$. Il en résulte que $P_{\min u}$ et $P_{\text{car } u}$ ont les même facteurs irréductibles de degré 1 dans une décomposition en produit de facteurs irréductibles.

Cependant il se peut que ces polynômes possèdent également des facteurs irréductibles qui ne sont pas de degré 1 dont on ne peut rien dire à ce stade.

Il se peut également, et même dans le cas où les facteurs irréductibles seraient tous de degré 1, pour $\mathbb{K} = \mathbb{C}$ par exemple, que les facteurs irréductibles de degré 1 soient affectés d'un exposant sur lequel on n'a encore guère de contrôle ici.

Dans le cas ttrès très particulier où $P_{\min u}$ est scindé à racines simples *i.e.* produit de polynôme de degré 1 deux à deux premiers entre eux, le théorème de CAYLEY–HAMILTON peut résulter des considérations précédentes : c'est le cas oùù u est diagonalisable (cf. IV.5.4.)

Théorème IV.7.2 (de CAYLEY–HAMILTON) *Pour tout $\mathbb{K}$-espace vectoriel de dimension finie E, et tout endomorphisme $\mathbb{K}$-linéaire $u \in \mathrm{End}_{\mathbb{K}}(E)$, $P_{\text{car } u}(u) = 0$ c'est-à-dire que $P_{\text{car } u}$ est un polynôme annulateur de u ou encore*

$$P_{\min u} | P_{\text{car } u} \ .$$

Preuve *: (cf. DOC n° III, n° III.1.exercice D.)*

Corollaire IV.7.3 *Pour tout $P \in \mathbb{K}[X]$ irréductible,*

$$P | P_{\min u} \ \Leftrightarrow \ P | P_{\text{car } u} \ .$$

On retrouve ici en particulier que les facteurs de degré 1 de $P_{\min u}$ sont exactement ceux de $P_{\text{car } u}$, ce qu'on avait déjà remarqué en IV.7.1.iii).

Corollaire IV.7.4 *Il découle du théorème IV.7.2 ci-dessus et du lemmme IV.6.3.i) que pour tout endomorphisme $u \in \mathrm{End}_{\mathbb{K}}(E)$,*

$$-\infty < \deg(P_{\min u}) \leq \deg(P_{\text{car } u}) = \dim_{\mathbb{K}} E \ .$$

Corollaire IV.7.5 *Le polynôme $P_{\min u}$ est scindé si et seulement si $P_{\text{car } u}$ est scindé.*

Corollaire IV.7.6 *La proposition IV.5.7 peut alors se reformuler en disant que u est trigonalisable si et seulement si $P_{\min u}$ est scindé, si et seulement si $P_{\text{car } u}$ est scindé.*

Définition IV.7.7 (Multiplicité des valeurs propres) Pour tout $\lambda \in \mathbb{K}$ si λ est valeur propre de u, il existe un unique

$$(m_\lambda, Q) \in \mathbb{N}^* \times \mathbb{K}[X] \text{ tel que } P_{\text{car } u} = (X-\lambda)^{m_\lambda} Q \text{ , } X-\lambda \text{ et } Q \text{ premiers entre eux } .$$

L'entier m_λ est apelé la *multiplicité de la valeur propre* λ.

Proposition IV.7.8 *L'endomorphisme u est diagonalisable si et seulement si $P_{\text{car } u}$ (ou de manière équivalente $P_{\min u}$) est sindé et*

$$\forall \lambda \in \mathrm{Sp}(u),\ m_\lambda = \dim_{\mathbb{K}} \mathrm{Ker}\, u - \lambda \mathrm{Id}_E \ .$$

Preuve *: Exercice.*

IV.8 . −Blocs de JORDAN, endomorphismes nilpotents

Définition IV.8.1 (Endomorphisme nilpotent) Un endomorphisme $u \in \mathrm{End}_{\mathbb{K}}(E)$ de E est *nilpotent*

$$\text{s'il existe } n \in \mathbb{N}, \text{ tel que } u^n = 0 .$$

On dit que u est *nilpotent d'échelon* d si d est le plus petit entier n tel que $u^n = 0$.

Lemme IV.8.2 *Soit $u \in \mathrm{End}_{\mathbb{K}}(E)$.*

i) u est nilpotent d'échlon d si et seulement si $P_{\min u} = X^d$.

ii) u est nilpotent d'échelon d et cyclique (cf. IV.4.2.ii),) si et seulement si

$$u \text{ est cyclique et } \dim_{\mathbb{K}} e = d .$$

iii) u est nilpotent d'échlon d si et seulement si u est nilpotent de rang $d-1$.

***Preuve** : (cf. TD n° VII, exercice A.)*

Proposition IV.8.3 *Pour $\lambda \in \kappa$, les assertions suivantes sont équivalentes :*

a) (E,u) est un espace cyclique de polynôme minimal $(X-\lambda)^{\dim_{\mathbb{K}} E}$, (on rappelle (cf. IV.4.1.i),) que le degré du polynôme minimal d'un espace cyclique est la dimension de cet espace ;)

b) $u - \lambda \mathrm{Id}_e$ est nilpotent d'échelon $\dim_{\mathbb{K}} E$ (ou de manière équivalente de rang $\dim_{\mathbb{K}} E - 1$;)

c) il existe une base de E dans laquelle la matrice de u est :

$$J_{\dim_{\mathbb{K}} E}(\lambda) = \begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{pmatrix} ; \qquad 1$$

d) il existe

$$\alpha \in \mathbb{N}^* \text{ tel que } P_{\min u} = (X-\lambda)^{\alpha} \text{ et } \dim_{\mathbb{K}} \mathrm{Ker}\,(u - \lambda \mathrm{Id}_E) = 1 .$$

***Preuve** :*

*i) **(a) $\Leftrightarrow$ b))***
Est immédiat.

ii) ***(b)*** $\Rightarrow$ ***c))***
Si $\nu \ := \ u - \lambda \mathrm{Id}_E$ *est nilpotent d'échelon* $\dim_{\mathbb{K}} E$, *il existe un éléments*

$$x \ \in \ E \text{ tel que } \nu^{\dim_{\mathbb{K}} E-1}(x) \ \neq \ 0 \text{ et } \nu^{\dim_{\mathbb{K}} E}(x) \ = \ 0 \, .$$

Dès lors

$$\left\{\nu^{\ell}(x)\right\} , 0 \leq \ell \leq \dim_{\mathbb{K}} E-1$$

est une famillle libre de E *et partant une base, dans laquelle*

$$\text{la matrice de } \nu \text{ est } \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} , \qquad 1$$

si bien que la matrice de

$$u \ = \ \lambda \mathrm{Id}_E \ + \ \nu \text{ est } J_{\dim_{\mathbb{K}} E}(\lambda) \ = \ \begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{pmatrix} \text{ dans cette même base } .$$

iii) ***(c)*** $\Rightarrow$ ***b))***
Laissé en exercice.

Définition IV.8.4 (Bloc de JORDAN) i) On pourra dire que le $\mathbb{K}$-espace vectoriel E est de JORDAN de paramètre λ s'il vérifie les conditions équivalentes de la proposition IV.8.3.

ii) On appellera *bloc de* JORDAN de paramètre λ et d'échelon d une matrice $J_d(\lambda)$ comme en IV.8.3.c).1.

iii) On note usuellement $J_d \ := \ J_d(0)$ un bloc de JORDAN de paramètre 0.

Corollaire IV.8.5 *Si* (E, u) *est un espace de* JORDAN *de paramètre* λ :

i) E *est un* $\mathbb{K}$*-espace vectoriel de dimension finie.*

ii) $\lambda \ \in \ \mathrm{Sp}(u)$ *est une valeur propre de* u.

Lemme IV.8.6 *Soit* (E, u) *un espace de* JORDAN.

i) L'espace (E, u) *est de paramètre* 0 *et d'échelon* d *si et seulement si* u *est nilpotent d'échelon* d.

ii) Si (E,u) *est de paramètre* λ *et d'échelon* d*, en notant*

$$\delta \ := \ \lambda \mathrm{Id}_E \ , \ \nu \ := \ u - \delta \ :$$

— δ *est diagonale ;*
— ν *est nilpotent d'échelon* d ;
—

$$u \ = \ \delta + \nu \ ;$$

—

$$\delta \circ \nu \ = \ \nu \circ \delta \ .$$

C'est la décomposition IV.9.3, de DUNFORD *dans le cas particulier où* (E,u)

Proposition IV.8.7 *Soient* E *et* F *des* $\mathbb{K}$*-espaces vectoriels*

$$E_{i\ ,1\leq i\leq k} \ \subset \ E \text{ et } F_{i\ ,1\leq i\leq k} \ \subset \ F \ \textit{tels que} \ E \ = \ \bigoplus_{i=1}^{k} E_i \text{ et } F \ = \ \bigoplus_{i=1}^{k} F_i \ .$$

i) Si

$$\forall 1 \leq i \leq k, \ \exists f_i \ : \ E_i \ \to \ F_i \ \textit{une application } \mathbb{K}\textit{-linéaire}$$

il existe une unique application $\mathbb{K}$*-linéaire*

$$f \ : \ E \ \to \ F \ \textit{telle que} \ \forall 1 \leq i \leq k, \ f_{|E_i} \ = \ f_i \ .$$

On notera

$$f \ = \ \bigoplus_{i=1}^{k} f_i \ .$$

Matriciellement cela correspond exactement à l'écriture par blocs de la matrice de f *; autrement dit, si chacun des* E_i *est rapporté à une base* $\mathcal{B}_i$*, dans laquelle la matrice de* f_i *est* M_i*, du fait de la décomposition de* E *en somme directe* $E \ = \ \bigoplus_{i=1}^{r} E_i$*,* $\mathcal{B} \ := \ \bigcup_{i=1}^{r} \mathcal{B}_i$ *est une base de* E *dans laquelle la matrice de* f *est*

$$M \ = \ \begin{pmatrix} M_1 & 0 & 0 & \dots & 0 \\ 0 & M_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & M_r \end{pmatrix} \ .$$

Preuve *: (cf. A.4.7, I.14.7.)*

ii) Si l'on suppose de plus donnés un endomorphisme (une structure de $\mathbb{K}[X]$*-module (cf. IV.1.2.i),))*

$$u \ \in \ \mathrm{End}_{\mathbb{K}}(E) \ (\textit{resp.} \ v \ \in \ \mathrm{End}_{\mathbb{K}}(F) \ ) \ \textit{tel que} \ \forall 1 \leq i \leq k,$$

— E_i *est stable par* u *(resp.* F_i *est stable par* v*,)*
—

$$f_i \ \circ \ u_{|E_i} \ = \ v_{|F_i} \ \circ \ f_i \ ,$$

alors l'application linéaire f *construite comme en i) vérifie* $f \ \circ \ u \ = \ v \ \circ \ f$ *(i.e. est un morphisme de* $\mathbb{K}[X]$*-modules (cf. IV.1.2.ii)).))*

Preuve *: (cf. I.14.8.)*

iii) Dans le cas particulier où $E = F$, *si*

$$\forall 1 \leq i \leq k,\ f_i \text{ est nilpotent d'échelon } d_i \ (\text{resp. diagonalisable})$$

$f = \bigoplus_{i=1}^{k} f_i$ *est nilpotent d'échelon* $\max_{1 \leq i \leq k}(d_i)$ *(resp. diagonalisable.)*

Preuve *: (cf. IV.12.2.)*

IV.9 . –Décomposition de DUNFORD

Définition IV.9.1 (Décomposition de DUNFORD) On appellera *décomposition de Dunford* de (E, u)

$$\text{un couple } (\delta, \nu) \in \mathbb{K}[u] \times \mathbb{K}[u] \text{ vérifiant :}$$

Dun_1)
$$\delta \circ \nu = \nu \circ \delta ;$$

Dun_2) l'endomorphisme δ est diagonalisable ;

Dun_3) l'endomorphisme ν est nilpotent ;

Dun_4)
$$u = \delta + \nu .$$

Proposition IV.9.2 *Pour $\lambda \in \mathbb{K}$, si $X - \lambda | P_{\min u}$ (c'est-à-dire (cf. IV.5.1.d),) si λ est valeur propre de u,) on note E_λ le sous-espace caractéristique (cf. IV.3.1,) associé à $X - \lambda$. Alors*

$$u_{|E_\lambda} = \lambda \mathrm{Id}_{E_\lambda} + \nu$$

où ν est nilpotent i.e. $u_{|E_\lambda}$ a une décomposition de DUNFORD.

Preuve *: Par définition même de λ, il existe $k \in \mathbb{N}^*$ et $Q \in \mathbb{K}[X]$ tel que $P_{\min u} = (X - \lambda)^k Q$ avec $X - \lambda$ et Q premiers entre eux. Par définition ensuite de E_λ on a*

$$(u_{|E_\lambda} - \lambda \mathrm{Id}_{E_\lambda})^k = 0 .$$

Théorème IV.9.3 (de décomposition de DUNFORD) *Pour tout $u \in \mathrm{End}_{\mathbb{K}}(E)$, si (de manière équivalente) $P_{\min u}$ ou $P_{\mathrm{car}\, u}$ est scindé, (E, u) admet une unique décomposition de* DUNFORD.

Preuve *: Écrivons*

$$P_{\min u} = \prod_{i=1}^{r} P_i^{\alpha_i}$$

où les P_i ,$1 \leq i \leq r$ sont des polynômes irréductibles deux à deux premiers entre eux. On en déduit une décomposition de E en somme directe d'espaces caractéristiques :

$$E = \bigoplus_{i=1}^{r} E_i \text{ avec } E_i = \mathrm{Ker}\, P_i^{\alpha_i}(u) = E[P_i^{\alpha_i}] \text{ (cf. IV.3.2 .)}$$

Comme, par hypothèse, $P_{\min u}$ est scindé, chacun des P_i l'est, c'est-à-dire qu'il existe

$$\lambda_i \,, 1 \leq i \leq r \in \mathbb{K} \text{ tel que } \forall 1 \leq i \leq r,\ P_i = X - \lambda_i .$$

On remarque alors que, pour tout $1 \leq i \leq r$, $\left(u_{|E_i} - \lambda_i \mathrm{Id}_{E_i}\right)^{\alpha_i} = 0$, i.e. est nilpotent d'échelon α_i, tandis que λ_i
IdE_i est diagonal. L'existence d'un couple (δ_i, ν_i) satisfaisant l'énoncé du théorème est donc établi pour chacune des restrictions de u aux sous-espaces caractéristiques de u.

Alors, en vertu de la proposition IV.8.7 $\bigoplus_{i=1}^{r}\delta_i$ *est diagonalisable tandis que* $\bigoplus_{i=1}^{r}\nu_i$ *est nilpotent. Néanmoins, en les construisant de cette manière, il n'est pas immédiat qu'on obtienne des polynômes en* u.

En revanche, si

$$\pi_i \ : \ E \ \to \ E_i \text{ est la projection de } E \text{ sur } E_i \text{ parallèlement à la somme } \bigoplus_{1 \ \leq \ j \ \leq \ r \ , \ j \neq i} E_j,$$

il découle de IV.3.2.iv), que π_i *est un polynôme en* u. *Il s'ensuit donc que*

$$\delta \ := \ \sum_{i=1}^{r} \lambda_i \pi_i \ \in \ \mathbb{K}[u] \ .$$

Comme chaque E_i *est stable par* π_i *et que* π_i *étant un projecteur,* $\pi_{i\,|E_i} \ = \ \mathrm{Id}_{E_i}$, *on a en fait*

$$\delta \ = \ \bigoplus_{i=1}^{r} \lambda_i \mathrm{Id}_{E_i}$$

ce qui assure, en vertu du lemme IV.8.7, que δ *est diagonalisable.*

Posons alors $\nu \ := \ u - \delta$ *ce qui assure immédiatement que* $\nu \ \in \ \mathbb{K}[u]$. *Par ailleurs il est presque immédiat de montrer que*

$$\nu \ = \ \bigoplus_{i=1}^{r} (u_{|E_i} - \lambda_i \mathrm{Id}_{E_i})$$

ce qui assure que ν *est nilpotent d'échelon* $\max_{i \ \leq \ 1 \ \leq \ r}(\alpha_i)$.

Comme δ *et* ν *sont des polynômes en* u, *on a* $\delta \ \circ \ \nu \ = \ \nu \ \circ \ \delta$.

L'unicité vient du fait qu'un endomorphisme simultanément diagonalisable et nilpotent est nul.

Corollaire IV.9.4 *Pour tout* $v \ \in \ \mathrm{End}_{\mathbb{K}}(E)$,

$$u \ \circ \ v \ = \ v \ \circ \ u \ (\Rightarrow \ v \ \circ \ \delta \ = \ \delta \ \circ \ v \text{ et } v \ \circ \ \nu \ = \ \nu \ \circ \ \delta \ .$$

Exemple IV.9.5 $\begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}$ est diagonalisable et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est nilpotent.

$$\begin{pmatrix} 3 & 1 \\ 0 & 5 \end{pmatrix} \ = \ \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} \ + \ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

n'est pas la décomposition de dunford de $\begin{pmatrix} 3 & 1 \\ 0 & 5 \end{pmatrix}$. La décomposition de Dunford de $\begin{pmatrix} 3 & 1 \\ 0 & 5 \end{pmatrix}$ est $\begin{pmatrix} 3 & 1 \\ 0 & 5 \end{pmatrix} + 0$.

Remarque IV.9.6 Le théorème IV.9.3 nécessite que $P_{\min u}$ ou $P_{\mathrm{car}\, u}$ soit scindé. Si $\mathbb{K} \ = \ \mathbb{C}$ le théorème s'applique. Si $\mathbb{K} \ = \ \mathbb{R}$, l'endomorphisme u_θ donné par la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ (rotation dans $\mathbb{R}^2$) ne vérifie pas $u_\theta \ = \ \delta \ + \ \nu$.

IV.10 . −Réduction de JORDAN

Dans ce paragraphe (IV.10,) on suppose que E est de dimension finie. Tout comme pour le théorème de CAYLEY–HAMILTON (cf. IV.7.2,) on dispose des outils nécessaire pour établir l'existence d'une réduction de JORDAN dans le cas des espaces cycliques (cf. IV.4.2.)

Ici encore, le théorème IV.11.5 de réduction de FROBENIUS permettra de déduire le théorème IV.10.10 de la proposition IV.10.3 tout comme on pouvait déduire le théorème IV.7.2 de la proposition IV.6.4.

Définition IV.10.1 (Réduction de JORDAN) On dit qu'un

$$\text{endomorphisme } u \in \mathrm{End}_{\mathbb{K}}(E) \text{ (ou même le couple } (E,u)\text{)}$$

admet une *réduction de* JORDAN s'il existe

$$\text{des sous espaces } E_i\ ,1\leq i\leq k \text{ de } E \text{ et des éléments } \lambda_i\ ,1\leq i\leq k \in \mathbb{K} \text{ de } \mathbb{K}$$

tels que :

J$_1$)
$$E = \bigoplus_{i=1}^{k} E_i\ ;$$

J$_2$) $\forall 1\leq i\leq k,\ E_i$ est stable par u ;

J$_3$)
$$\forall 1\leq i\leq k,\ u_{|E_i} \text{ est de JORDAN de paramètre } \lambda_i \text{ et d'échelon } \dim_{\mathbb{K}} E_i\ .$$

Le point J$_3$) équivaut à dire qu'il existe une base dans laquelle la matrice de $u_{|E_i}$ est un bloc de JORDAN $J_{\dim_{\mathbb{K}} E_i}(\lambda_i)$. Par conséquent u admet une réduction de JORDAN si et seulement si il existe une base de E dans laquelle la matrice de u s'écrit par blocs :

$$\begin{pmatrix} J_{d_1}(\lambda_1) & 0 & 0 & \dots & 0 \\ 0 & 0 & J_{d_2}(\lambda_2) & \dots & 0 \\ 0 & 0 & 0 & \dots & J_{d_k}(\lambda_k)\ . \end{pmatrix}\ .$$

On dira qu'une telle matrice est une *réduite de* JORDAN. On dira que $J \in \mathcal{M}_n(\mathbb{K})$ est une *réduite de* JORDAN pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$ si A et J sont conjuguées *i.e.* si

$$\exists P \in \mathrm{GL}_n(\mathbb{K}),\ A = PJP^{-1}\ .$$

On pourra écrire

$$(E,u) = \bigoplus_{i=1}^{k} (E_i,\theta_i)$$
où $\forall 1\leq i\leq k,\quad \theta_i : E_i \to E_i$ est de JORDAN de paramètre λ_i et d'échelon $\dim_{\mathbb{K}} E_i$. IV.10.1.1

Notation IV.10.2 Il r'ésulte immédiatement du corollaire IV.8.5 que, si (E,u) possède une réduction de JORDAN comme en IV.10.1.1 $\forall 1\leq i\leq k,\ ,\ \lambda_i$ est une valeur propre de u et que le couple (E_i,θ_i) est uniquement caractérisé par λ_i et $\dim_{\mathbb{K}} E_i$.

Étant donnée une réduction de JORDAN de (E,u) on notera, pour tout $\lambda \in \mathrm{Sp}(u)$, $D(\lambda)$ le uplet des dimension $\dim_{\mathbb{K}} E_i$ tels que $\lambda = \lambda_i$ dans la décomposition IV.10.1.1 ; c'est-à-dire le uplet des échelons (taille des matrices) des blocs de JORDAN de paramètre λ. On pourra supposer les éléments de $D(\lambda)$ rangés par ordre décroissant. On pourra même supposer, que pour tout $\lambda \in \mathrm{Sp}(u)$ les $D(\lambda)$ ont tous même nombre d'éléments r, quitte à donner la valeur 0 aux derniers éléments. On dira que

$$\{(\lambda, D(\lambda))\}\ ,\lambda \in \mathrm{Sp}(u)$$

est l'*ensemble de paramètres de la réduction*.

Par exemple si u a pour réduite de JORDAN

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

l'ensemble de paramètre de cette réduction est

$$\{(1,(2,1))(2,(2,0))(3,(1,0))\}\ .$$

Proposition IV.10.3 (Existence dans le cas cyclique) *Si (E,u) est un espace cyclique de polynôme minimal (ou caractéristique (cf. IV.6.4,)) scindé,*

$$P_{car\,u} \;=\; P_{min\,u} \;=\; \prod_{\lambda \,\in\, \mathrm{Sp}(u)} (X-\lambda)^{d_\lambda},$$

(E,u) possède une réduction de JORDAN *d'ensemble de paramètres*

$$\{\lambda \in \mathrm{Sp}(u)\ ;\ (\lambda,(d_\lambda))\}\ .$$

Preuve *: Il découle de la proposition IV.4.6, que*

$$E \;=\; \bigoplus_{\lambda \,\in\, \mathrm{Sp}(u)} \mathrm{Ker}\,((u-\lambda \mathrm{Id}_E)^{d_\lambda})$$

où

$$\big(\mathrm{Ker}\,((u-\lambda \mathrm{Id}_E)^{d_\lambda}), u_{|\mathrm{Ker}\,((u-\lambda \mathrm{Id}_E)^{d_\lambda})}\big) \text{ est cyclique de polynôme minimal } (X-\lambda)^{d_\lambda}$$

c'est-à-dire de JORDAN *de paramètre λ et d'échelon d_λ.*

Définition IV.10.4 (Réduction de FROBENIUS) On dit que (E,u) a une *réduction de* FROBENIUS s'il existe $r \in \mathbb{N}$ des sous-$\mathbb{K}$-espaces vectoriels $E_j\ ,1\leq j\leq r}$ de E et des polynômes $\mu_j\ ,1\leq j\leq r} \in \mathbb{K}[X]$ tels que :

Frob$_1$)

$$\forall 1 \leq j \leq r,\ E_j \text{ est stable par } u\ .$$

Frob$_2$)

$$\forall 1 \leq j \leq r,\ (E_j, u_{|E_j}) \text{ est cyclique de polynôme minimal } \mu_j\ .$$

Frob$_3$)

$$E \ = \ \bigoplus_{j=1}^{r} E_j \ .$$

Frob$_4$)

$$\forall 1 \leq j \leq r-1, \ \mu_{j+1} | \mu_j \ .$$

Les polynômes $\mu_j \, , 1 \leq j \leq r}$ s'appellent les *invariants de similitude* de (E,u) ou simplement de u (cf. IV.11.9.) On constate immédiatement sur cette définition que

$$P_{\min u} \ = \ \mu_1 \ .$$

Remarque IV.10.5 i) Il faudra se reporter au théorème IV.11.5 de réduction de FROBENIUS pour garantir qu'une telle réduction existe toujours pour un couple (E,u), cette dernière étant même unique.

ii) Néanmoins si (E,u) est cyclique, il est pour ainsi dire tautologique qu'il est sa propre réduction de FROBENIUS.

iii) Il est tout aussi immédiat de constater, que dans le cas où (E,u) est cyclique, la proposition IV.10.3, signifie en fait qu'une réduction de FROBENIUS détermine l'existance d'une réduction de JORDAN dans le cas où le polynôme minimal est scindé. Ce résultat se généralise comme suit (proposition IV.10.6.

Proposition IV.10.6 *Supposons que (E,u) possède une réduction de* FROBENIUS $\left(E_j \, , 1 \leq j \leq r} \, , \mu_j \, , 1 \leq j \leq r} \right)$ *et que $\mu_1 \ = \ P_{min \, u}$ soit scindé. Alors (E,u) possède une réduction de* JORDAN *d'ensemble de paramètres*

$$\{ (\lambda, d_{\lambda,j} \, , 1 \leq j \leq r \,) \} \, , \lambda \in \mathrm{Sp}(u)$$

où

$$\forall 1 \leq j \leq r, \ \mu_j \ = \ \prod_{\lambda \, \in \, \mathrm{Sp}(u)} (X-\lambda)^{d_{\lambda,j}} \ .$$

Preuve *: Il suffit d'appliquer la proposition IV.10.3 à chaque $(E_j, u_{|E_j})$ qui est cyclique ; et de constater que la condition IV.10.4.Frob$_4$) entraîne que $\forall \lambda \in \mathrm{Sp}(u), \ d_{\lambda,j}$ est une fonction décroissante de j.*

Remarque IV.10.7 On remarque dans la construction ci-dessus (proposition IV.10.6 que

$$\forall 1 \leq j \leq r, \ , d_{\lambda,j} \text{ n'est autre que la valuation } (X-\lambda) - \text{adique de } \mu_j$$

au sens où elle a été définie en toute généralité pour les anneaux principaux en I.13.5.5, ou plus précisément pour le cas particulier des anneaux de polynôme en III.5.5.

Proposition IV.10.8 *Supposons que (E,u) possède une réduction de* JORDAN *d'ensemble de paramètres*

$$\{ (\lambda, d_{\lambda,j} \, , 1 \leq j \leq r \,) \} \, , \lambda \in \mathrm{Sp}(u) \ .$$

Alors si l'on note $D_{\lambda,j}$ le sous-espace de JORDAN *de E correspondant à $(\lambda, d_{\lambda,j})$ dans la réduction de* JORDAN,

$$E_j \ := \ \bigoplus_{\lambda \, \in \, \mathrm{Sp}(u)} E_{\lambda,j} \text{ et } \mu_j \ = \ \prod_{\lambda \, \in \, \mathrm{Sp}(u)} (X-\lambda)^{d_{\lambda,j}},$$

$\left(E_j \, , 1 \leq j \leq r} \, , \mu_j \, , 1 \leq j \leq r} \right)$ *est une réduction de* FROBENIUS *de (E,u).*

Preuve *: Le fait que les sous-$\mathbb{K}$-espaces $E_j \, , 1 \leq j \leq r}$ soient cycliques est encore une conséquence de la proposition IV.4.6.*

Les $\nu_j \, , 1 \leq j \leq r}$ satisfont à IV.10.4.Frob$_4$) puisque $d_{\lambda,j}$ est décroissante en j.

Proposition IV.10.9 (réduction de JORDAN, réduction de FROBENIUS et isomorphisme) *Soient*

$$E \text{ et } F \text{ des } \mathbb{K}\text{-espaces vectoriels de dimension finie}$$

et

$$u \in \mathrm{End}_{\mathbb{K}}(E) \text{ (resp. } v \in \mathrm{End}_{\mathbb{K}}(F)) \text{ un endomorphisme } \mathbb{K}\text{-linéaire de } E \text{(resp. } F \text{ .)}$$

On suppose que (E, u) *(resp.* (F, v)*,) possède une réduction de* JORDAN *de paramètres*

$$P_E := \{(\lambda, (d_{u,\lambda,1}, \ldots, d_{u,\lambda,r}))\}_{,\lambda \in \mathrm{Sp}(u)} \text{ (resp. } P_F := \{(\lambda, (d_{u,\lambda,1}, \ldots, d_{u,\lambda,s}))\}_{,\lambda \in \mathrm{Sp}(u)} .$$

Alors les assertions suivantes sont équivalentes :

a) *Les espaces* (E, u) *et* (F, v) *ont même ensemble de paramètres de* JORDAN *i.e.* $P_E = P_F$.

b) *Il existe un isomorphisme de* $\mathbb{K}$*-espaces vectoriels*

$$\phi : E \to F \text{ tel que } \phi \circ u = v \circ \phi ;$$

c'est-à-dire, dans le formalisme dévelopé au paragraphe IV.1, et plus particulièrement en IV.1.2.ii), un isomorphisme de $\mathbb{K}[X]$*-modules*

$$\phi : (E, u) \cong (F, v) .$$

c) *Les espaces* (E, u) *et* (F, v) *ont même réduction de* FROBENIUS *i.e. ont mêmes invariants de similitude et leur polynôme minimal commun est scindé.*

Preuve *:*

i) ***(a)*** $\Rightarrow$ ***b))***
Si $P_E = P_F$*, on a en particulier* $r = s$*. Notons alors* r *le nombre commun d'éléments de*

$$D(\lambda)_{,\lambda \in \mathrm{Sp}(u)} \text{ (resp. } D(\lambda)_{,\lambda \in \mathrm{Sp}(v)} .)$$

Notons encore

$$E_{\lambda,k} \text{ (resp. } F_{\lambda,k})$$

le bloc de JORDAN *de paramètre* λ *et de taille* $d_{u,\lambda,k}$ *(resp.* $d_{v,\lambda,k}$*) dans la réduction de* JORDAN *de* (E, u) *(resp.* (F, v) *;) ces blocs pouvant éventuellement être* $\{0\}$ *; ce qui permet néanmoins d'écrire :*

$$\begin{aligned} E &= \bigoplus_{\lambda \in \mathrm{Sp}(u)} \bigoplus_{k=1}^{r} E_{\lambda,k} \\ (\text{resp. } F &= \bigoplus_{\lambda \in \mathrm{Sp}(v)} \bigoplus_{k=1}^{r} F_{\lambda,k} .) \end{aligned}$$

L'assertion a) entraîne en particulier que $\mathrm{Sp}(u) = \mathrm{Sp}(v)$ *et de plus que*

$$\forall \lambda \in \mathrm{Sp}(u) = \mathrm{Sp}(v),\ \forall 1 \leq k \leq r,\ d_{u,\lambda,k} = d_{v,\lambda,k} .$$

Les sous-espaces $E_{\lambda,k}$ *(resp.* $F_{\lambda,k}$*) étant cycliques, par définition même d'une réduction de* JORDAN*, il existe*

$$\begin{array}{ll} & x_{\lambda,k} \in E_{\lambda,k} \\ (\text{resp.} & y_{\lambda,k} \in F_{\lambda,k}) \\ \text{tel que} & (x_{\lambda,k}, \ldots, u^{d_{u,\lambda,k}-1}(x_{\lambda,k})) \\ (\text{resp.} & (y_{\lambda,k}, \ldots, v^{d_{v,\lambda,k}-1}(y_{\lambda,k}))\ ) \\ \text{est une base de} & E_{\lambda,k} \\ (\text{resp.} & F_{\lambda,k}\ ) \end{array} \quad \textit{(cf. IV.4.1)}$$

Puisque, par hypothèse, $d_{u,\lambda,k} = d_{v,\lambda,k}$ *on peut définir*

$$\begin{array}{rrcl} \phi_{\lambda,k} : & E_{\lambda,k} & \longrightarrow & F_{\lambda,k} \\ & u^i(x_{\lambda,k}) & \longmapsto & v^i(y_{\lambda;k})_{0 \leq i \leq d_{x,\lambda,k}-1} \\ (\textit{resp. } \psi_{\lambda,k} : & F_{\lambda,k} & \longrightarrow & E_{\lambda,k} \\ & v^i(y_{\lambda,k}) & \longmapsto & u^i(x_{\lambda;k})_{0 \leq i \leq d_{y,\lambda,k}-1} \ .) \end{array}$$

On a alors, par construction

$$\begin{array}{rcl} \phi_{\lambda,k} \circ \psi_{\lambda,k} & = & \mathrm{Id}_{F_{\lambda,k}} \ , \\ \psi_{\lambda,k} \circ \phi_{\lambda,k} & = & \mathrm{Id}_{E_{\lambda,k}} \ , \\ \phi_{\lambda,k} \circ u_{|E_{\lambda;k}} & = & v_{|F_{\lambda,k}} \circ \psi_{\lambda,k} \ ; \end{array} \qquad 1$$

(cf. Problème n° II, exercice D, question 4), b)pour une justification complète de la dernière égalité.)

Il existe alors, d'après la proposition IV.8.7.ii), un unique morphisme $\mathbb{K}$*-linéaire*[4]

$$\begin{array}{rrcl} & \phi : E \to F & & \\ (\textit{resp.} & \psi : F \to E \ ) & & \\ \textit{tel que } \forall \lambda \in & \mathrm{Sp}(u) & = & \mathrm{Sp}(v), \\ \forall 1 \leq k \leq r, & \phi_{|E_{\lambda,k}} & = & \phi_{\lambda,k} \\ (\textit{resp.} & \psi_{|F_{\lambda,k}} & = & \psi_{\lambda;k} \ .) \end{array}$$

Il résulte alors de 1 que

$$\phi \circ \psi = \mathrm{Id}_F \ , \ \psi \circ \phi = \mathrm{Id}_E \ , \ \phi \circ u = v \circ \psi \ .$$

ii) ***(b)*** $\Rightarrow$ ***c))***

L'existence d'une réduction de JORDAN *pour* (E, u) *(resp.* (F, v)*,) donne, grâce à la proposition IV.10.8 une réduction de* FROBENIUS *de* (E, u) *(resp.* (F, v)*,) d'invariants de similitude*

$$\begin{array}{rrcl} \forall 1 \leq j \leq r, & \mu_{E,j} & = & \displaystyle\prod_{\lambda \in \mathrm{Sp}(u)} (X - \lambda)^{d_{u,\lambda,j}} \\ (\textit{resp. } \forall 1 \leq j \leq s, & \mu_{F,j} & = & \displaystyle\prod_{\lambda \in \mathrm{Sp}(v)} (X - \lambda)^{d_{v,\lambda,j}} \ .) \end{array}$$

Ceci assure déjà que

$$P_{\textit{min } u} = \mu_{E,1} \ (\textit{resp. } P_{\textit{min } v} = \mu_{F,1} \ ,) \textit{ est scindé.}$$

Le point b) et le corollaire IV.11.10 assurent alors que

$$r = s \text{ et } \forall 1 \leq j \leq r, \ \mu_{E,j} = \mu_{F,j} \ .$$

iii) ***(c)*** $\Rightarrow$ ***a))***

Comme ci-dessus une réduction de JORDAN *permet de construire, graçe à la proposition IV.10.8 une réduction de* FROBENIUS*. L'unicité dans la décomposition en produit de facteurs irréductibles (cf. I.13.5.3,) assure alors que*

$$\mathrm{Sp}(u) = \mathrm{Sp}(v) \text{ et } \forall 1 \leq j \leq r, \ \forall \lambda \in \mathrm{Sp}(u), \ d_{u,\lambda,j} = d_{v,\lambda,j} \ .$$

4. En observant bien les énoncés précités, on s'apercevrait qu'il s'agit même d'un $\mathbb{K}[X]$-morphisme.

Théorème IV.10.10 (de réduction de JORDAN) *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$, $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E tel que son polynôme minimal $P_{min\,u}$ (ou de manière équivalente son polynôme caractéristique $P_{car\,U}$) est scindé. Alors :*

1) L'endomorphisme u admet une réduction de JORDAN.

***Preuve** : Le théorème IV.11.5 assure de l'existence d'une réduction de* FROBENIUS *pour (E, u). La proposition IV.10.6 permet alors de construire une réduction de* JORDAN.

2) (E, u) possède une unique réduction de JORDAN *au sens des équivalences de la proposition IV.10.9.*

Remarque IV.10.10.3 L'unicité dans le théorème de réduction IV.10.10 est a rapprocher de la remarque B.6.13.3. Les blocs de JORDAN dans la décomposition de JORDAN ne sont en effet rien d'autres que les *diviseurs élémentaires* (cf. B.6.10,) dans le cas particulier où les facteurs irréductibles de l'annulateur sont des polynômes scindés.

Corollaire IV.10.11 *Si E est un $\mathbb{K}$-espace vectoriel de dimension finie, on peut grâce au théorème IV.3.2, écrire E comme somme directe de ses sous-espaces caractéristiques*

$$E \;=\; \bigoplus_{i=1}^{k} E[P_i],$$

où les P_i ,$1 \leq i \leq k \in \mathbb{K}[X]$ sont les facteurs irréductibles du polynôme minimal $P_{min\,u}$ (aussibien que du polynôme caractéristique $P_{car\,u}$.) Il n'y a en toute généralité aucune raison que les $E[P_i]$ soient cycliques. Cependant le théorème IV.11.5 permet de décomposer chacun des $E[P_i]$ comme une somme directe d'espaces cycliques

$$E[P_i] \;=\; \bigoplus_{j=1}^{r_i} E_{i,j}$$

où $E_{i,j}$ est cyclique de polynôme minimal $\mu_{i,j}$ avec $\mu_{i,1} \;=\; P_i$.

Si l'on suppose, de plus que $P_{min\,u}$ est scindé,

$$\forall 1 \leq i \leq k,\ \exists \lambda_i \in \mathbb{K},\ \exists d_{i,1} \in \mathbb{N}^*,\ \mu_{i,1} \;=\; P_i \;=\; (X - \lambda_i)^{d_{i,1}}\ .$$

Il s'ensuit, en vertu de IV.10.4.Frob$_4$), que

$$\forall 1 \leq i \leq k,\ \forall 1 \leq j \leq r_i,\ \exists d_{i,j} \in \mathbb{N}^*,\ \mu_{i,j} \;=\; (X - \lambda_i)^{d_{i,j}}\ .$$

Il en résulte que les sous-espaces $E_{i,j}$,$1 \leq i \leq k$, $1 \leq j \leq r_i$ sont de JORDAN. *L'énoncé IV.10.10.2) d'unicité assure alors qu'il s'agit de la réduction de* JORDAN *de (E, u).*

Remarque IV.10.12 Le corollaire IV.10.11 ci-dessus confronté à la proposition IV.10.6 fait apparaître qu'on peut déterminer la réduction de JORDAN de (E, u), pour peu qu'elle existe *i.e.* que le polynôme minimal soit scindé, de deux manières différentes :

i) Soit on applique le théorème IV.11.5 de réduction de FROBENIUS à (E, u) puis le théorème IV.3.2 de décomposition en sous-espaces caractéristiques à chacun des sous-espaces stables de la réduction de FROBENIUS. On peut d'ailleurs dans ce cas, se contenter de la proposition IV.4.6.

C'est la manière dont nous avons procédé dans la proposition IV.10.6.

ii) On peut d'abord décomposer l'espace (E,u) en une somme directe de sous-espaces caractéristiques, grâce au théorème IV.3.2 ; et décomposer ensuite chacun d'eux en sommes directe de sous-espaces cycliques, grâce au théorème IV.11.5.

C'est la manière dont nous avons procédé dans le corollaire IV.10.11.

L'énoncé IV.10.10.2) d'unicité assure cependant que les constructions i) et ii) déterminent l'unique réduction de JORDAN de (E,u).

Corollaire IV.10.13 (du théorème IV.10.10 : Conséquences matricielles) *Soit $n \in \mathbb{N}^*$.*

i) La proposition IV.10.9 assurent que deux réduites de JORDAN *J et $K \in \mathcal{M}_n(\mathbb{K})$ ayant mêmes paramètres, sont conjuguées i.e.*

$$\exists P \in \mathrm{GL}_n(\mathbb{K}),\ K = PJP^{-1}\,.$$

ii) Pour tout $(A,B) \in \mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$, A et B sont conjuguées si et seulement si elles ont même réduite de JORDAN *(i.e. des réduites de* JORDAN *ayant les mêmes paramètres.)*

iii) Si le polynôme minimal $P_{min\,u} = \mu_1$ de u est de la forme $(X-\lambda)^{d_{\lambda,1}}$ autrement dit siμ_1 a un unique facteur irréductible qui est de degré 1,

$$\forall 2 \leq j \leq r,\ \mu_j = (X-\lambda)^{d_{\lambda,j}}\ ,\ d_{\lambda,j} \leq d_{\lambda,j-1}$$

où μ_j ,$1\leq j\leq r$ sont les invariants de similitude donnés par la réduction de FROBENIUS *(cf. IV.10.4.) Alors les sous-espaces cycliques E_j qui leur sont associés, sont de* JORDAN *et la réduction de* FROBENIUS *est déjà une réduction de* JORDAN*. Le polynôme minimal de E_j est*

$$\mu_j = (X-\lambda)^{d_{\lambda,j}} = \sum_{\ell=1}^{d_{\lambda,j}} (-1)^{d_{\lambda,j}-\ell} \binom{\ell}{d_{\lambda,j}} \lambda^{d_{\lambda,j}-\ell} X^\ell\,.$$

La matrice compagnon qui lui est associée est alors :

$$C_j = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & (-1)^{d_{\lambda,j}-1}\lambda^{d_{\lambda,j}} \\ 1 & 0 & 0 & \dots & 0 & (-1)^{d_{\lambda,j}-2} d_{\lambda,j}\lambda^{d_{\lambda,j}} \\ 0 & 1 & 0 & \dots & 0 & (-1)^{d_{\lambda,j}-3}\binom{2}{d_{\lambda,j}}\lambda^{d_{\lambda,j}-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \end{pmatrix}\,. \qquad 1$$

Cette matrice est celle de $u_{|E_j}$ dans une base $\big(x, u(x), \dots, u^{d_{\lambda,j}-1}(x)\big)$.
En vertu de la proposition IV.8.3, un bloc de JORDAN

$$J_j = \begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{pmatrix} \qquad 2$$

qui correspond à une base $\big(y, u(y)-\lambda y, \dots (u-\lambda \mathrm{Id}_{E_j})^{d_{\lambda,j}-1}(y)\big)$.
On constate néanmoins que si x est un vecteur cyclique alors

$$(u-\lambda)^k(x) = 0 \Rightarrow (X-\lambda)^{d_{\lambda,j}} | (X-\lambda)^k$$

puisque précisément, si x est cyclique

$$P^v_{\min u_{|E_j}} \;=\; P_{\min u_{|E_j}} \;.$$

La base

$$\big(x, u(x) - \lambda x, \dots, (u - \lambda \mathrm{Id}_{E_i})^{d_{\lambda,j}-1}(x)\big)$$

est alors une base dans laquelle la matrice de $u_{|E_j}$ est J_j.

On peut ainsi déterminer un changement de base permettant de passer de C_j à J_j.

iv) Dans le cas où $\lambda = 0$, i.e. u est nilpotent, la matrice compagnon (iii).1) C_j et le bloc de JORDAN *(iii).2) coïncident sans qu'il soit nécessaire de changer de base.*

IV.11 . −Théorème de réduction de FROBENIUS (cf. II.10, B.6)

On démontrera dans ce paragraphe (IV.11,) le théorème IV.11.5 dit de *réduction de* FROBENIUS.
Une formulation beaucoup plus concrète de ce résultat est donnée au corollaire IV.11.7 :

Théorème 1 Étant donnée une matrice $M \in \mathcal{M}_n(\mathbb{K})$ (carrée de taille n à coefficients dans un corps $\mathbb{K}$,) il existe une matrice inversible $P \in \mathrm{GL}_n(\mathbb{K})$ telle que :

$$P^{-1}MP = \begin{pmatrix} C_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & C_2 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & C_r \end{pmatrix}$$

où pour tout $1 \leq i \leq k$, C_i est une matrice dite *compagnon i.e.* une matrice de la forme

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

L'entier r qui apparaît dans l'écriture ci-dessus est exactement celui qui apparaît dans le théorème de réduction de FROBENIUS, à savoir le nombre de sous-modules cycliques dans la décomposition.

Il est possible, à travers l'identification entre $\mathbb{K}[X]$-modules et $\mathbb{K}$-espaces vectoriels munis d'un endomorphisme faite au paragraphe IV.1, de voir le théorème de réduction de FROBENIUS comme un avatar du théorème des *facteurs invariants* (cf. B.6.13.) un tel point de vue pourrait certes être suffisant pour obtenir un résultat du type du corollaire IV.11.10 qui n'est qu'une reformulation du corollaire B.6.15. Cependant, le caractère abstrait de ce point de vue ne permet pas d'en tirer directement de méthode pour construire la réduite de FROBENIUS d'un endomorphisme qui serait concrètement donné par sa matrice par exemple. Nous allons donc, dans ce paragraphe (IV.11,) adopter un point de vue spécifique aux $\mathbb{K}$-espaces vectoriels de dimension finie.

Notation IV.11.0 ((cf. II.10.0, B.6.0)) Dans tout ce paragraphe (IV.11,) $\mathbb{K}$ est un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-Linéaire. Rappelons (cf. IV.2.6,) qu'il revient au même de demander que (E, u) soit un $\mathbb{K}[X]$-module de type fini (cf. II.1.5,) et de torsion (cf. IV.2.2.vi).) En particulier (cf. IV.2.6,) le polynôme minimal $P_{\min u}$ est non nul.

Proposition IV.11.1 (Existence d'un vecteur cyclique maximal (cf. II.10.1, B.6.3)) *Soient*

$$E \text{ un } \mathbb{K}\text{-espace vectoriel de dimension finie}$$

et

$$u \in \mathrm{End}_{\mathbb{K}}(E) \text{ un endomorphisme } \mathbb{K}\text{-linéaire de } E\,.$$

Alors il existe $x \in E$ tel que le polynôme minimal de u en x $P^x_{\min u}$ (cf. IV.2.2.iii),) soit le polynôme minimal $P_{\min u}$ de u. Il s'ensuit que $C := \mathrm{Vect}\big\{\{u^n(x)\}, n \in \mathbb{N}\big\}$ est un sous-espace de E stable par u et cyclique de polynôme minimal $P_{\min u}$ (i.e. un sous-$\mathbb{K}[X]$-module cyclique de (E, u).)

Preuve *: (cf. TD n° VI, exercice D.)*

On pourrait à ce point utiliser un analogue de la proposition II.10.4, puisque, comme dans le cas des groupes abéliens finis on dispose d'un invariant qui décroît strictement dans les suites exactes. Plus précisément la proposition IV.11.1 assure qu'on a dès lors une suite exacdte comme en II.10.2.1 ou B.6.4.1. La suite des $\mathbb{K}$-espaces vectoriels sous-jacents est alors exacte en vertu du point IV.1.2. On peut donc lui applicquer le *principe d'Euler-Poincaré* (cf. I.9.19,) à savoir que la dimension du quotient dans la suite exacte est strictement inférieure à la dimension du terme central. On pourrait alors montrer que cette suite est scindée.

On peut cependant ici employer un argument propre à la structure sous-jacente de $\mathbb{K}$-espaces vectoriels des $\mathbb{K}[X]$-modules :

Notation IV.11.2 ((cf. II.10.2, B.6.4)) Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphismes $\mathbb{K}$-linéaire de E de polynôme minimal $P_{\min u}$. Soit

$$\begin{array}{ll} & C \subset E \text{ un sous-}\mathbb{K}\text{-espace vectoriel de } E \text{ stable par } u \\ (\textit{i.e.} & \text{un sous-}\mathbb{K}[X]\text{-module de } (E,u),) \text{ cyclique de polynôme minimal } P_{\min u}\ . \end{array} \qquad \text{IV.11.2.1}$$

On a donné dans la proposition IV.4.1 un certain nombre de caractérisations équivalentes des espaces cycliques. En particulier,

$$\exists x \in C,\ C = \mathrm{Vect}\big\{\{u^n(x)\}\,,n \in \mathbb{N}\big\}$$

ce qui signifie de manière équivalente que le morphisme de $\mathbb{K}$-espaces vectoriels

$$\mathbb{K}[X] \to E\,,\ X \mapsto X\cdot x = u(x),$$

est surjectif, à valeurs dans C et de noyau

$$P^x_{\min u}\mathbb{K}[X] = P_{\min u}\mathbb{K}[X] = \mathrm{Ann}_{\mathbb{K}[X]}(x)\ .$$

On a donc un isomorphisme

$$\mathbb{K}[X]/P^x_{\min u}\mathbb{K}[X] = \mathbb{K}[X]/P_{\min u}\mathbb{K}[X] = \mathbb{K}[X]/\mathrm{Ann}_{\mathbb{K}[X]}(x) \cong C\ .$$

En vertu de la proposition IV.4.1, C est alors de dimension

$$d := \deg(P^x_{\min u}) = \deg(P_{\min u}) \qquad \text{IV.11.2.2}$$

en tant que $\mathbb{K}$-espace vectoriel et $\{x, u(x), \dots, u^{d-1}(x)\}$ en est une base.

On complète cette base en une base

$$e_i\,,1\le i\le \dim_{\mathbb{K}} E \text{ avec } \forall 1 \le i \le d,\ e_i = u^{i-1}(x)\ . \qquad \text{IV.11.2.3}$$

Notons $e_i^*\,,1\le i\le \dim_{\mathbb{K}} E$ sa base duale, si bien qu'on a, en particulier,

$$\forall a_i\,,0\le i\le d-1 \in \mathbb{K},\ e_d^*\Big(\sum_{i=0}^{d-1} a_i u^i(x)\Big) = a_{d-1}\ . \qquad \text{IV.11.2.4}$$

Soit enfin

$$S := \{y \in E\,;\ \mathbb{K}[X]\cdot y \subset \mathrm{Ker}\, e_d^*\}\ ; \qquad \text{IV.11.2.5}$$

c'est-à-dire que S est l'ensemble des $y \in E$ tels que

$$\forall P \in \mathbb{K}[X],\ P(u)(y) \in \mathrm{Ker}\, e_d^*\ .$$

On va montrer que S est un supplémentaire de C en tant que $\mathbb{K}$-espace vectoriel stable par u ; ce qui revient en fait à montrer que c'est un supplémentaire de C en tant que $\mathbb{K}[X]$-module.

Proposition IV.11.3 (cf. II.10.3) *i) L'ensemble S (cf. IV.11.2.5,) est un sous-$\mathbb{K}$-espace vectoriel de E stable par u (i.e. un sous-$\mathbb{K}[X]$-module de (E,u).*

Preuve *: Bien entendu $0 \in S$ si bien que $S \neq \emptyset$. Pour tout*

$$(y_1,y_2) \in S\times S\ ,\ \text{tout}\ (A_1,A_2)\in \mathbb{K}[X]\times\mathbb{K}[X]\ ,\ \text{tout}\ P\in\mathbb{K}[X],$$

$$\begin{aligned} e_d^*\big(P\cdot(A_1\cdot y_1+A_2\cdot y_2)\big) &= e_d^*\big((PA_1)\cdot y_1+(PA_2)\cdot y_2\big)\\ &= e_d^*[(PA_1)\cdot y_1]+e_d^*[(PA_2)\cdot y_2]\\ &= 0\ ; \end{aligned}$$

si bien que

$$A_1\cdot y_1+A_2\cdot y_2\in S$$

assurant que S est un sous-$\mathbb{K}[X]$-module de E.

ii) Les espaces C et S étant come en IV.11.2.1, (resp. IV.11.2.5,)

$$C\cap S=\{0\}\ .$$

Preuve *: Soit $y\in S\cap C$. En particulier $y\in C$ si bien qu'il existe*

$$a_{i\ ,1\le i\le d}\in\mathbb{K}\ \text{tel que}\ y=\sum_{i=1}^d a_ie_i=\sum_{i=1}^d a_iu^{i-1}(y)\ .$$

Par ailleurs, puisque $y\in S$, pour tout $n\in\mathbb{N}$,

$$e_d^*(X^n\cdot y)=0\ .$$

Alors :

$$\begin{aligned} \forall 0\le j\le d-1,\quad 0 &= e_d^*(X^j\cdot y)\\ &= e_d^*\big(u^j[\sum_{i=1}^d a_iu^{i-1}(v)]\big)\\ &= e_d^*\big(\sum_{i=1}^d a_iu^{i+j-1}(v)\big)\\ &= a_{d-j}\ . \end{aligned}$$

Il s'ensuit que $y=0$.

iii) L'application

$$\phi\ :\ \mathbb{K}[X]\ \to\ E^*\ ,\ P\ \mapsto\ e_d^*\circ P(u)$$

est un morphisme $\mathbb{K}$-linéaire dont le noyau est $\mathbb{K}[X]P_{\min u}$.

Preuve *:*

$*$) (ϕ **est** $\mathbb{K}$**-linéaire**)

Puisque u *est un endomorphisme* $\mathbb{K}$*-linéaire de* E*, pour tout* $P \in \mathbb{K}[X]$*,* $P(u)$ *est encore un endomorphisme* $\mathbb{K}$*-linéaire de* E *et*

$$\phi(P) := e_d^* \circ P(u)$$

est donc bien une forme $\mathbb{K}$*-linéaire sur* E *i.e. un élément de* E^**.*

$\forall (P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$,
$\forall (a,b) \in \mathbb{K} \times \mathbb{K}$,
$\forall y \in E$,

$$\begin{aligned} \phi(aP+bQ)(y) &= e_d^*\big((aP+bQ)(u)(y)\big) \\ &= e_d^*\big((aP(u)+bQ(u))(y)\big) \\ &= e_d^*\big(aP(u)(y)+bP(u)(y)\big) \\ &= a(e_d^* \circ P(u))(y) + b(e_d^* \circ Q(u))(y) \\ &= a\phi(P)(y) + b\phi(Q)(y) \end{aligned}$$

d'où il résulte que

$$\phi(aP+bQ) = a\phi(P) + b\phi(Q)\,.$$

†) ($\mathbb{K}[X]P_{\min u} \subset \operatorname{Ker}\phi$)

En outre, pour tout $P \in \mathbb{K}[X]P_{\min u}$*,* $P_{\min u}|P$ *si bien que* $P(u) = 0$*, ce qui entraîne*

$$\phi(P) = e_d^* \circ P(u) = 0$$

et donc

$$\mathbb{K}[X]P_{\min u} \subset \operatorname{Ker}\phi\,.$$

Soit $P \in \operatorname{Ker}\phi$*.*

‡) ($P(u)(e_i) = P \cdot E_i \in \operatorname{Ker} e_d^*$)

$e_d^* \circ P(u) = 0$*. En particulier, pour tout* $1 \le i \le d$*,*

$$e_d^*\big(P(u)[e_i]\big) = 0\,.$$

Or $e_i \in C$*, et* C *est stable par* u *donc* $P(u)(e_i) \in C$*, si bien que*

$$\forall 1 \le i \le d,\ P \cdot e_i = P(u)(e_i) \in C \cap \operatorname{Ker} e_d^*\,. \qquad 1$$

§) ($P \cdot e_i \in S$)

Or pour tout $j \in \mathbb{N}$

$$X.j \cdot e_i = u^j(e_i) \in C$$

puisque C *est stable sous* u*, si bien qu'il existe*

$$a_{i,j\,,1 \le j \le d} \in \mathbb{K} \text{ tel que } X^j \cdot e_i = \sum_{1=j}^{d} a_{i,j} e_j\,.$$

Par conséquent :

$$\begin{aligned} e_d^*\big(X^j \cdot P(u)(e_i)\big) &= e_d^*\big((X^j P) \cdot e_i\big) \\ &= e_d^*\big(P \cdot [X^j \cdot e_i]\big) \\ &= e_d^*\big(P \cdot [\sum_{j=1}^{d} a_{i,j} e_j]\big) \qquad 1 \\ &= \sum_{j=1}^{d} a_{i,j} e_d^*[P \cdot e_j] \\ &= 0 \text{ d'après ‡).1}\,. \end{aligned}$$

Puisque $\operatorname{Ker} e_d^*$ *est un* $\mathbb{K}$*-espace vectoriel, il découle de 1 que, pour tout* $Q \in \mathbb{K}[X]$,

$$Q \cdot (P \cdot e_i) \in \operatorname{Ker} e_d^*$$

c'est-à-dire que

$$\mathbb{K}[X] \cdot (P \cdot e_i) \subset \operatorname{Ker} e_d^* .$$

Il s'ensuit que $P \cdot e_i \in S$.

¶) $(P(u)_{|C} = 0)$
Or $P \cdot e_i \in C$, *et d'après ii),* $C \cap S = \{0\}$. *Donc*

$$P(u)(e_i) = P \cdot e_i = 0 . \qquad 1$$

Comme $e_{i\,,1\leq i\leq d}$ *est une base de* C, *il s'ensuit que* $P(u)_{|C} = 0$.

‖) $(P_{\mathbf{min}\,u}|P)$
Il s'ensuit que

$$P_{min\,u_{|C}}|P .$$

Or C *est précisément construit de sorte que*

$$P_{min\,u} = P_{min\,u_{|C}}$$

ce qui termine la preuve.

iv) Le morphisme ϕ *étant construit comme dans le lemme iii) il existe un unique morphisme* $\mathbb{K}$*-linéaire injectif* $\overline{\phi}$ *tel que le diagramme suivant, où la flèche vertical est la surjection canonique, soit commutatif :*

$$\begin{array}{rcl} \mathbb{K}[X] & \xrightarrow{\phi} & E^* \\ \downarrow & \nearrow \overline{\phi} & \\ \mathbb{K}[X]/(\mathbb{K}[X]P_{min\,u}) & & \end{array}$$

Preuve *: Remarquons que* $\mathbb{K}[X]P_{min\,u}$ *est un idéal de* $\mathbb{K}[X]$ *donc un sous-*$\mathbb{K}[X]$*-module de* KkX *lui-même. C'est donc aussi (cf. IV.1.2.iii),) un sous-*$\mathbb{K}$*-espace vectoriel de* $\mathbb{K}[X]$ [5]*. Ceci peut également se déduire du fait, que dans iii), on a identifié*
$\mathbb{K}[X]P_{min\,u}$ *au noyau d'une application* $\mathbb{K}$*-linéaire.*
Il suffit désormais d'appliquer la factorisation des morphismes de κ*-espaces vectoriels à* ϕ.

5. Ni l'un ni l'autre d'ailleurs n'étant de $\mathbb{K}$-dimension finie alors qu'ils sont de type fini come $\mathbb{K}[X]$-modules.

v) Notons

$$F \ := \ \mathrm{Im}\,\overline{\phi} \ \subset \ E^* \ \textit{(cf. iv) ;)}$$

le sous-espace S étant comme en IV.11.2.5 :

$$S \ = \ F^{\perp} \ = \ \{y \ \in \ E \, ; \, \forall f \in F, \ f(y) \ = \ 0\} \, .$$

Preuve *:*

$*$) ($S \ \subset \ F^{\perp}$)
Pour tout $y \ \in \ S$, par définition $\mathbb{K}[X] \cdot y \ \subset \ \mathrm{Ker}\, e_d^*$ c'est-à-dire que pour tout $P \ \in \ \mathbb{K}[X]$, $P \cdot y \ \in \ \mathrm{Ker}\, e_d^*$ c'est-à-dire que

$$e_d^*(P \cdot y) \ = \ 0 \ \Leftrightarrow \ e_d^*[P(u)(y)] \ = \ 0 \ \Leftrightarrow \ \phi(P)(y) \ = \ 0$$

c'est-à-dire que

$$S \ \subset \ ({}^{\perp}\mathrm{Im}\,\phi) \ = \ ({}^{\perp}\mathrm{Im}\,\overline{\phi}) \ = \ F^{\perp} \, .$$

†) ($F^{\perp} \ \subset \ S$)
Pour tout $y \ \in \ F^{\perp}$, pour tout $P \ \in \ \mathbb{K}[X]$, $\phi(P)(y) \ = \ 0$ c'est-à-dire que $e_d^*[P(u)(y)] \ = \ 0$ ou encore $P \cdot y \ \in \ \mathrm{Ker}\, e_d^*$ ou encore, de manière équivalente $y \ \in \ S$, ce qui achève la preuve.

vi) Les espaces C et S étant come en IV.11.2.1, (resp. IV.11.2.5,)

$$\dim_{\mathbb{K}} S \ + \ \dim_{\mathbb{K}} C \ = \ \dim_{\mathbb{K}} E \, .$$

Preuve *: On déduit de iv) que*

$$\dim_{\mathbb{K}} \mathrm{Im}\,\overline{\phi} \ = \ \dim_{\mathbb{K}} \mathbb{K}[X]/\mathbb{K}[X]P_{\textit{min}\,u} \, .$$

Or $\mathbb{K}[X]/\mathbb{K}[X]P_{\textit{min}\,u}$ est un $\mathbb{K}[X]$-module cyclique au sens de la définition IV.4.2, si bien qu'en vertu de la proposition IV.4.1,

$$\dim_{\mathbb{K}} \mathbb{K}[X]/\mathbb{K}[X]P_{\textit{min}\,u} \ = \ \deg(P_{\textit{min}\,u}) \ = \ d \ = \ \dim_{\mathbb{K}} C \, .$$

C'est un résultat connu de dualité dans les espaces vectoriels que

$$\dim_{\mathbb{K}} F \ + \ \dim_{\mathbb{K}} F^{\perp} \ = \ \dim_{\mathbb{K}} E$$

et qui permet de conclure.

Proposition IV.11.4 (cf. II.10.4) *Étant donnés un $\mathbb{K}$-espace vectoriel E de dimension finie, un endomorphisme $u \ \in \ \mathrm{End}_{\mathbb{K}}(E)$ Kkk-linéaire de E, C un sous-espace de E stable par u et cyclique de polynôme minimal $P_{\textit{min}\,u}$, C possède un supplémentaire stable par u.*

Preuve *: On construit un supplémentaire S de C comme en IV.11.2.5, puis on applique IV.11.3.ii) et IV.11.3.vi) pour montrer que C et S sont supplémentaire.*

Théorème IV.11.5 (de réduction de FROBENIUS (cf. II.10.5, B.6.13)) *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $K k$-linéaire de E. Alors :*

*1) (**Existence**)*

Le couple (E,u) possède une réduction de FROBENIUS *au sens où nous l'avons déjà définie en IV.10.4 et que nous rappelons ici : Il existe un entier $r \in \mathbb{N}$, E_j ,$1\leq j\leq r$ des sous-$\mathbb{K}$-espaces vectoriels de E, et des polynômes μ_j ,$1\leq j\leq r$ $\in \mathbb{K}[X]$ tels que :*

Frob$_1$)

$$\forall 1 \leq j \leq r,\ E_j \text{ est stable par } u\ .$$

Frob$_2$)

$$\forall 1 \leq j \leq r,\ (E_j, u_{|E_j}) \text{ est cyclique de polynôme minimal } \mu_j\ .$$

Frob$_3$)

$$E\ =\ \bigoplus_{j=1}^{r} E_j\ .$$

Frob$_4$)

$$\forall 1 \leq j \leq r-1,\ \mu_{j+1} | \mu_j\ .$$

***Preuve** : On a vu IV.2.6 que u possède un polynôme minimal $P_{\min u} \in \mathbb{K}[X]$ non nul.*

La proposition IV.11.1 assure alors qu'il existe un sous-espace cyclique C de E de polynôme minimal $P_{\min u}$ ce qui signifie un sous-$\mathbb{K}$-espace vectoriel C de E, stable par u et de dimension $\deg(P_{\min u})$.

La proposition IV.11.4 assure alors que C possède un supplémentaire S dans E, tel que S est stable par u. Le $\mathbb{K}$-espace vectoriel S étant de dimension strictement inférieure à celle de E, on peut faire l'hypothèse de récurrence que $(S, u_{|S})$ possède une réduction de FROBENIUS.

Il existe donc S_2 ,$j\leq 2\leq r$ des sous-$\mathbb{K}$-espaces vectoriels de S stables par u cycliques de polynômes minimaux respectifs μ_j ,$2\leq j\leq r$ avec

$$S\ =\ \bigoplus_{2=j}^{r} S_i \text{ et } \forall 2 \leq j \leq r-1,\ \mu_{j+1} | \mu_j\ .$$

On montre le résultat en posant

$$E_1\ :=\ C \text{ et } \forall 2 \leq j \leq r,\ E_j\ :=\ S_j$$

pour peu qu'on montre que $\mu_2 | P_{\min u}$. Or par hypothèse de récurrence, μ_2 est le polynôme minimal $P_{\min u_{|S_2}}$ de la restriction de u à S_2. Or, par définition du polynôme minimal de u

$$\forall x \in E,\ P_{\min u}(u)(x)\ =\ 0$$

donc

$$\forall x \in E_2,\ P_{\min u}(u)(x)\ =\ 0\ \Leftrightarrow\ \forall x \in E_2,\ P_{\min u}(u_{|E_2})(x)\ =\ 0$$

ce qui prouve que

$$\mu_2 | P_{\min u}\ .$$

*2) (**Unicité**)*
L'entier r et le r-uplet μ_j ,$_{1\leq j\leq r}$ sont uniques et ne dépendent que de l'endomorphisme u.

***Preuve** : On suppose*

$$E \;=\; \bigoplus_{i=1}^{r} E_i \;=\; \bigoplus_{j=1}^{s} F_j$$

avec E_i, F_j stables par u et $u_i \;=\; u_{|E_i}$, $v_j \;=\; u_{|F_j}$ cycliques ;

$$\begin{array}{rcl} \mu_i & := & P_{\min u_i} \text{ vérifie } \forall 1 \leq i \leq r-1,\ \mu_{i+1}|\mu_i \\ \text{et} \quad \nu_j & := & P_{\min v_j} \text{ vérifie } \forall 1 \leq j \leq s-1,\ \nu_{j+1}|\nu_j \ , \end{array}$$

c'est-à-dire que

$$(E_i, \mu_i)\,,_{1\,\leq\, i\,\leq\, r} \text{ et } (F_j, \nu_j)\,,_{1\,\leq\, j\,\leq\, s}$$

sont des réduction de FROBENIUS *de (E, u).*
On a alors, d'après la proposition IV.4.1 :

$$\sum_{i=1}^{r} \dim_{\mathbb{K}} E_i \;=\; \sum_{j=1}^{s} \dim_{\mathbb{K}} F_j \text{ donc} \sum_{i=1}^{r} \deg(\mu_i) \;=\; \sum_{j=1}^{s} \deg(\nu_j)\ . \qquad 1$$

Supposons que

$$\mu_i\,,_{1\leq i\leq r} \;\neq\; \nu_j\,,_{1\leq j\leq s}\ .$$

Alors il existe i tel que $\mu_i \;\neq\; \nu_i$ et notons t le plus petit entier tel que $\mu_t \;\neq\; \nu_t$.
Alors $t > 1$; en effet

$$\mu_1 \;=\; P_{\min u} \;=\; \nu_1\ .$$

Lemme 2).2

$$\forall 1 \leq k \leq t-1,\ \operatorname{rg}\big(\mu_t(u)_{|F_k}\big) \;=\; \operatorname{rg}\big(\mu_t(u)_{|E_k}\big)\ .$$

Lemme 2).3

$$\forall k \;\geq t\ ,\ \mu_t(u)_{|E_k} \;=\; \mu_t(u)_{|F_k} \;=\; 0\ .$$

En particulier $\mu_t\big(u_{|F_t}\big) \;=\; 0$. Or $P_{\min u_{|F_t}} \;=\; \nu_t$, donc

$$\nu_t|\mu_t\ .$$

On échange les rôles de μ_i et ν_i pour obtenir

$$\mu_t|\nu_t$$

Finalement $\mu_t \;=\; \nu_t$ ce qui contredit l'hypothèse et assure donc que

$$\mu_i\,,_{1\leq i\leq r} \;=\; \nu_j\,,_{1\leq j\leq s}\ .$$

IV.11.6 . −Preuves des lemmes IV.11.5.2).2).2 et IV.11.5.2).2).3

Preuve (**du lemme IV.11.5.2).2).2**): Par hypothèse sur t

$$\mu_k \;=\; \nu_k \;=\; X^d - \sum_{\ell=0}^{d-1} a_\ell X^\ell \,.$$

D'après la proposition IV.4.1, il existe $x \in E_k$ (resp. $y \in F_k$) tel que

$$\{u_k^\ell(x)\}\,,0 \leq \ell \leq d-1 \;\text{ (resp. } \{v_k^\ell(y)\}\,,0 \leq \ell \leq d-1 \;)$$

est une base de E_k (resp. F_k)

$$u_k^d(x) \;=\; \sum_{\ell=0}^{d-1} a_\ell u_k^\ell(x) \text{ et } v_k^d(y) \;=\; \sum_{\ell=0}^{d-1} a_\ell v_k^\ell(y)\,.$$

Il résulte de cette relation que, si l'on définit

$$\phi \;:\; E_k \;\to\; F_k \;,\; u_k^\ell(x) \;\mapsto\; v_k^\ell(y),$$

ϕ est un isomorphisme de $\mathbb{K}$-espaces vectoriels (puisqu'il envoie une base sur une base) et de plus

$$\forall z \in E_k,\; \phi[u_k(z)] \;=\; v_k[\phi(z)]\,.$$

On peut réécrire cette dernière identité, puisque

$$u_k \;=\; u_{|E_k} \text{ et } v_k \;=\; u_{|F_k},$$

$$\forall z \in E_k,\; \phi[u(z)] \;=\; u[\phi(z)]$$

(ce qu'on pourrait résumer par le fait que ϕ est en fait un isomorphisme de $\mathbb{K}[X]$-modules (cf. IV.1.2.ii).))

Il s'ensuit que

$$\phi \circ \mu_{t|E_k} \;=\; \mu_{t|F_k} \circ \phi$$

ce qui prouve le résultat.

Preuve (**du lemme IV.11.5.2).2).3**): tout d'abord

$$\forall t \leq k \leq r,\; \mu_k | \mu_t$$

et μ_k est le polynôme minimale de $u_k \;=\; u_{|E_k}$ si bien que :

$$\mu_t(u)_{|E_k} \;=\; \mu_t(u_{|E_k}) \;=\; \mu_t(u_k) \;=\; 0\,. \qquad \text{IV.11.6.1}$$

Puisque les $E_i\,,_{1\leq i\leq r}$ et $F_j\,,_{1\leq j\leq s}$ sont stables par u donc par $\mu_t(u)$,

$$\mu_t(E) \;=\; \bigoplus_{i=1}^{r} \mu_t(E_i) \;=\; \bigoplus_{j=1}^{s} \mu_t(F_j)$$

d'où il résulte que

$$\mathrm{rg}(\mu_t(u)) \;=\; \sum_{i=1}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big) \;=\; \sum_{j=1}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\,.$$

Ceci se réécrit, en vertu du lemme IV.11.5.2).2).2,

$$\sum_{i=t}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big) \;=\; \sum_{j=t}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\;.$$

En utilisant IV.11.6.1, il vient

$$\sum_{j=t}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big) \;=\; 0$$

ce qui assure

$$\forall t \leq k \leq s,\; \mu_t(u)_{|F_j} \;=\; 0\;.$$

Le corrollaire qui suit reformule l'énoncé d'existence IV.11.5.1) en termes de réduction de matrices :

Corollaire IV.11.7 *Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$ un entier et $M \in \mathcal{M}_n(\mathbb{K})$ une matrice carré de taille n. Alors il existe une matrice carré inversibles de taille n, $P \in \mathrm{GL}_n(\mathbb{K})$ telle que*

$$P^{-1}MP \;=\; \begin{pmatrix} C_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & C_2 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & C_r \end{pmatrix}$$

où pour tout $1 \;\leq\; i \;\leq\; k$, C_i est une matrice compagnon i.e. une matrice de la forme

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix} \text{ (cf. IV.4.1.j).1 .)}$$

Preuve *: Considérons la matrice M comme la matrice d'un endomorphisme $\mathbb{K}$-linéaire u de $E \;:=\; \mathbb{K}^n$. Le théorème IV.11.5.1) donne une décomposition de E en somme directe*

$$E \;=\; \bigoplus_{i=1}^{r} E_i$$

de sous-$\mathbb{K}$-espaces vectoriels stables par u ce qui correspond à une écriture de la matrice de u par blocs. Chaque bloc est la matrice d'un endomorphisme cyclique de E_i et l'on peut donc trouver, (cf. IV.4.1.j),)une base dans laquelle c'est une matrice compagnon.

Le corollaire qui suit est une conséquence de l'énoncé d'unicité IV.11.5.2) et correspond presque mot pour mot au corollaire B.6.15 (voir aussi le corollaire II.10.7.)

Corollaire IV.11.8 *Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$ un entier et $(M, N) \in \mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$ un couple de matrices carrées de tail n. Les matrices M et N sont semblables*

$$(\textit{i.e.} \exists P \in \mathrm{GL}_n(\mathbb{K}),\; M \;=\; P^{-1}NP\;)$$

si et seulement si le r-uplet de polynômes $\mu_i\,,_{1\leq i\leq r}$ défini par le théorème IV.11.5 est le même pour M et N.

Définition IV.11.9 (Invariants de similitude (cf. II.10.6, B.6.14)) Le corollaire ci-dessus conduit a nomer

$$\text{le } r-\text{uplet } \mu_i\ ,1\leq i\leq r\ \in\ \mathbb{K}[X]$$

les *invariants de similitude* d'un endomorphisme ou d'une matrice.

Ces invariants ne sont ni plus ni moins que les facteurs invariants dans la décomposition d'un module de torsion (cf. B.6.14.)

Corollaire IV.11.10 ((cf. II.10.7, B.6.15)) *Étant donnés des $\mathbb{K}$-espaces vectoriels E et F de dimension finie*

$$u\ \in\ \mathrm{End}_{\mathbb{K}}(E)\ (\textit{resp. } v\ \in\ \mathrm{End}_{\mathbb{K}}(F)\ )\ \textit{un endomorphisme } \mathbb{K}\textit{-linéaire de } E\ (\textit{resp. } F\ ,)$$

et

$$f\ :\ E\ \to\ F\ \textit{tel que}\ f\ \circ\ u\ =\ v\ \circ\ f,$$

(i.e. un morphisme de $\mathbb{K}[X]$-modules (cf. IV.1.2.ii),)) f est un isomorphisme (de $\mathbb{K}$-espaces vectoriels aussibien que de $\mathbb{K}[X]$-modules) si et seulement si (E,u) et (F,v) ont les mêmes invariants de similitude.

Corollaire IV.11.11 (de la proposition IV.6.4) *Soient $\mu_i\ ,1\leq i\leq r$ les invariants de similitude de u (cf. IV.11.9,) alors :*

$$P_{\mathit{car}\,u}\ =\ \prod_{i=1}^{r}\mu_i\ .$$

Preuve *: Le théorème IV.11.5 de réduction de* FROBENIUS *permet d'écrire*

$$E\ =\ \bigoplus_{i=1}^{r}E_i$$

où les $E_i\ ,1\leq i\leq r$ sont stables par u et cycliques de polynômes minimal respectif μ_i.

En appliquant la proposition IV.6.4 à chacun des sous-espaces cycliques E_i, on obtient

$$\forall 1\leq i\leq r,\ P_{\mathit{car}\,u_{|E_i}}\ =\ P_{\mathit{min}\,u_{|E_i}}\ =\ \mu_i\ .$$

Il résulte alors du lemme IV.6.3.iii) que :

$$P_{\mathit{car}\,u}\ =\ \prod_{i=1}^{r}P_{\mathit{car}\,u_{|E_i}}\ =\ \prod_{i=1}^{r}P_{\mathit{min}\,u_{|E_i}}\ =\ \prod_{i=1}^{r}\mu_i\ . \qquad \textit{IV.11.11.1}$$

Remarque IV.11.12 Lorsqu'on considère (E,u) muni de sa structure de $\mathbb{K}[X]$-module, l'inclusion IV.5.3.i) correspond à l'inclusion $E[X-\lambda]\ \subset\ E[(X-\lambda)^k]$. On a vu, au paragraphe B.6, l'importance du rôle joué par $E[P]$ lorsque P est un élément irréductible. Dans ce cas, en effet, si $\kappa\ :=\ \mathbb{K}[X]/(\mathbb{K}[X]P)$ est le corps résiduel en P, $E[P]$ est un κ-espace vectoriel de dimension finie.

Si $P\ =\ X-\lambda$

$$\kappa\ =\ \mathbb{K}[X]/(\mathbb{K}[X](X-\lambda))\ =\ \mathbb{K}$$

et alors $\dim_\kappa\cdot\ =\ \dim_{\mathbb{K}}\cdot$ s'interprète comme la dimension sur $\mathbb{K}$ de l'espace vectoriel sous-jacent. Dans le cas où le polynôme minimal $P_{\min u}$ de u est scindé, la proposition B.6.11 se réinterprète comme suit (cf. IV.11.13.)

La difficulté, dans le cas où $P_{\min u}$ n'est pas scindé, provient de ses facteurs irréductibles ou plus exactement des corps résiduels $\kappa\ :=\ \mathbb{K}[X]/(\mathbb{K}[X]P)$. Cependant si $\mathbb{K}\ =\ \mathbb{R}$, un facteur irréductible de $P_{\min u}$ qui n'et pas de degré 1 sera de degré 2, et l'on aura alors

$$\kappa\ =\ \mathbb{K}[X]/(\mathbb{K}[X]P)\ \cong\ \mathbb{C}\ .$$

Proposition IV.11.13 *Si le polynôme minimal $P_{\min u}$ de u est scindé, l'entier r donné par la réduction de Frobenius (cf. IV.11.5,) est le maximaum des dimension des sous-espaces propres de u.*

IV.12 . −Exercices

Exercice IV.12.1 [cf. II.12.5]

1) Soient P_1, P_2, P_3 trois polynômes irréductibles distincts sur un corps K.

Combien y a-t-il de classes de similitude de matrices à coefficients dans K ayant comme polynôme minimal $P_1P_2^2P_3$ et comme polynôme caractéristique $P_1^2P_2^4P_3^3$?

Pour chacune d'elles, donner les invariants de similitude.

Exercice IV.12.2 Soient E un $\mathbb{K}$-espace vectoriel et E_i ,$1\leq i\leq k$ des sous-espaces de E tels que $E = \bigoplus_{i=1}^{k} E_i$. Soit

$$\forall 1 \leq i \leq k,\ f_i\ :\ E_i\ \rightarrow\ E_i \text{ un endomorphisme de } E_i \text{ et } f\ := \bigoplus_{i=1}^{k} f_i\ .$$

Montrer que si

$$\forall 1 \leq i \leq k,\ f_i \text{ est nilpotent d'échelon } d_i \text{ (resp. diagonalisable)}$$

f est nilpotent d'échelon $\max_{1\ \leq\ i\ \leq\ k}(d_i)$ (resp. diagonalisable.)

Appendices

A . – A-modules, A-algèbres

A.0 . – Introduction

Dans tout ce paragraphe (A), A est un anneau commutatif. (cf. I.1.8.)

Si l'on confronte
- les propriétés I.6.6.1 à I.6.6.4 ;
- les propriétés I.6.14.1 à I.6.14.4 ;
- les propriétés III.1.8.Mod$_1$) à III.1.8.Mod$_4$) ;
- et éventuellement les souvenir qu'on peut (ou qu'on doit sans doute) avoir de l'axiomatique des espaces vectoriels,

on s'aperçoit que, dans la forme au moins les diverses situations mentionnées ci-dessus sont régies par une axiomatique très voisine.

Cela ne suffit pas nécessairement à motiver l'introduction d'une définition générale dont le seul mérite serait d'englober les définitions particulières précédentes dans un cadre commun. Si en effet, cette définition générale n'était pas de nature à produire des résultats par elle-même mais nécessitait de revenir aux situations particulières pour justifier le moindre énoncé, elle s'avérerait d'une utilité finalement assez médiocre.

La notion de A-module que nous allons introduire ici n'est ni tout à fait de la première espèce qui ferait découler la totalité des résultat sur les groupes abéliens, les espaces vectoriels et les idéaux de résultats généraux sur les A-modules, ni de la seconde espèce, c'est-à-dire absoluement stérile et inopérante.

Ni miraculeuse ni vaine, cette définition donne un cadre confortable pour formuler un certain nombre d'énoncés.

Conceptuellement les A-modules et leurs morphismes ne sont pas très différents des espaces vectoriels et applications linéaires. On ne dispose cependant pas pour les A-modules lorsque A est un anneau quelconque des résultats de classification relatifs aux $\mathbb{K}$-espaces vectoriels. En particulier l'un des premiers invariants de l'algèbre linéaire, à savoir la dimension, qui dans le cas des $\mathbb{K}$-espaces vectoriels de dimension finie caractérise (à isomorphisme près) un $\mathbb{K}$-espace vectoriel, n'a que de très vagues analogues dans le cas des A-modules, tout comme des résultat tels que les théorèmes de la base incomplète ou du rang ...

On conseil de revenir à cette remarque une fois qu'on aura établi les résultats du cours qui suit. En effet quand on aura constaté l'ampleur du travail nécessaire à donner un théorème de structure des A-modules, ne serait-ce que lorsque A est un anneau principal, on aura mesuré, du moins je l'espère, combien, s'il n'y a aucune crainte à avoir quant à la définition de A-module, il faut en revanche être précautionneux quant au énoncés que l'ont peut établir concernant ces objets.

On ne doit pas non plus céder au découragement, en découvrant qu'on a été capable de ne produire des énoncés que relativement aux anneaux principaux qui, comme chacun sait, ne sont qu'une partie des anneaux qu'on est amené à rencontrer même en arithmétique. Les anneaux de corps de nombres en particulier ne sont pas tous principaux et l'on pourrait trouver particulièrement décevant de ne même pas disposer, à la fin de ce cours, des outils susceptibles d'aborder ces objets, pourtant usuels pour les arithméticiens. On peut néanmoins garder quelque optimisme quant à ce sujet dans la mesure où le pas qu'il faudrait franchir, ce que nous ne ferons pas dans ce cours, consiste à passer des anneaux principaux aux *anneaux de Dedekind*. Des théorèmes de structures des A-modules pour A un anneau de Dedekind existent encore, et peuvent se déduire des résultats sur les anneaux principaux qui constituent l'essence de ce cours. La marche qui permet de passer de l'un à l'autre n'est pas si haute que cela en définitive, pour peu qu'on ait soigneusement étudié les anneaux de Dedekind et leurs propriétés.

On aurait pu passer sous silence les définitions et propriétés élémentaires des A-algèbres. Cependant puisqu'on va voir que l'axiomatique des A-modules correspond « à remplacer » les coefficients entiers relatifs dans

la construction de la proposition I.6.6 par des coefficients dans un anneau arbitraire, on se doute bien que les résultats établis pour les anneaux notamment en I.6.13.1 doivent avoir leurs analogues lorsqu'on remplace $\mathbb{Z}$ par un anneau arbitraire. On pourrrait dire que « les A-algèbres sont aux anneaux ce que les A-modules sont aux groupes abéliens » ; cette formulation un peu vague étant précisée notamment en A.1.11, A.2.11, A.3.10, A.4.9,

A.1 . $-A$-modules, A-algèbres (cf. I.1)

Définition A.1.1 (A-module) Étant donné un anneau commutatif A, un *A-module* est un triplet

$$(M, +_M, \cdot_M) \text{ (simplement noté } (M, +, \cdot) \text{ ou même } M, \ )$$

tel que :

Mod_0) Le couple $(M, +)$ est un groupe abélien (cf. I.1.3 ;)
$\cdot \ : \ A \times M \ \to \ M$, appelée *application de structure* vérifie :

Mod_1)
$$\forall (a, x, y) \in A \times M \times M, \ a \cdot x + y \ = \ a \cdot x + a \cdot y \ ;$$

Mod_2)
$$\forall (a, b, x) \in A \times A \times M, \ a + b \cdot x \ = \ a \cdot x + b \cdot x \ ;$$

Mod_3)
$$\forall (a, b, x) \in A \times A \times M, \ a * b \cdot x \ = \ a \cdot (b \cdot x) \ ;$$

Mod_4)
$$\forall x \in M, \ 1 \cdot x \ = \ x \ .$$

On dira aussi que les lois $+$ et $\cdot$ *munissent M d'une structure de A-module*.
On dira souvent que $(M, +)$ est le *groupe abélien sous-jacent* au A-module M.

Exemple A.1.2 Les remarque faites en introductions (cf. A.0,) attestent qu'on a déjà rencontré des exemples de A-modules, sans nécessairement avoir axiomatisé la notion :

a) (**$\mathbb{K}$-espace vectoriel**)
Si $\mathbb{K}$ est un corps, un $\mathbb{K}$-module n'est rien d'autre qu'un $\mathbb{K}$-espace vectoriel.

b) (**Anneau**)
Un anneau A possède une structure naturelle de A module données par

$$\cdot \ : \ A \times A \ \to \ A \ , \ (a, x) \ \mapsto \ a \cdot x \ := \ a * x$$

qui est la même construction qui fait de tout corps $\mathbb{K}$ un $\mathbb{K}$-espace vectoriel.

c) (**Idéal**)
Pour la même structure que ci-dessus, tout idéal de A est également un A-module (cf. I.6.14.)

d) Les propositions I.0.2.7 et I.6.1.i) sétendent aux A-modules au sens où, pour un A-module M et un ensemble E, l'ensemble M^E est muni d'une structure naturelle de groupe (cf. I.0.2.7.ii)) (au sens où c'est la seule telle que $f \ \mapsto \ f(x)$ soit un morphisme.) De même on constate que la loi externe donnée par

$$\forall (a, f, x) \in A \times M^E \times E, \ (a \cdot f)(x) \ = \ a \cdot f(x)$$

est la seule qui fasse de $f \ \mapsto \ f(x)$ un morphisme de A-modules pour tout x.

e) On a déjà remarqué en III.1.8 que pour un anneau A, l'anneau $A[[X]]$ des séries formelles est un A-module. On a montré un résultat analogue pour l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A en III.2.5.iv). Cet exemple et en fait un cas particulier de la construction envisagée en A.1.8.b).

Notation A.1.3 Pour un groupe abélien M, on notera $\mathrm{End}_{\mathbf{Gr}}(M)$ (cf. I.2.8,) l'ensemble des endomorphismes de groupes de M, *i.e.* l'ensemble des morphismes de groupes de M dans lui-même.

On rappelle que $\big(\mathrm{End}_{\mathbf{Gr}}(M), +, \circ\big)$ a une structure d'anneau (cf. I.6.3,) (qui n'est pas commutatif en général.)

La proposition A.1.4 qui suit généralise le corollaire I.6.8.

Proposition A.1.4 *i) Étant donné un A-module $(M, +, \cdot)$, $(M, +)$ est un groupe abélien et l'on a vu (cf. I.6.3,) qu'alors $\mathrm{End}_{\mathbf{Gr}}(M)$ a une structure naturelle d'anneau (non commutatif.) À la structure de A-module sur M on associe un morphisme d'anneaux*

$$\phi_{(M,+,\cdot)} \,:\, A \,\to\, \mathrm{End}_{\mathbf{Gr}}(M)$$

de A à valeurs dans l'anneau $(\mathrm{End}_{\mathbf{Gr}}(M), +, \circ)$, en posant, pour tout $a \,\in\, A$,

$$\begin{array}{rccc} \phi_{(M,+,\cdot)}(a) : & M & \to & M \\ & x & \mapsto & a \cdot x \,. \end{array}$$

***Preuve** : Posons*

$$\phi \,:=\, \phi_{(M,+,\cdot)} \,:\, A \,\to\, \mathrm{End}_{\mathbf{Gr}}(M) \,,\; a \,\mapsto\, (x \mapsto a \cdot x) \,.$$

L'axiome A.1.1.Mod$_1$) assure que $\phi(a)$ est un morphisme de groupes. L'application ϕ ainsi définie est donc bien à valeurs dans $\mathrm{End}_{\mathbf{Gr}}(M)$.

L'axiome A.1.1.Mod$_2$) assure que

$$\phi \,:\, (A, +) \,\to\, (\mathrm{End}_{\mathbf{Gr}}(M), +)$$

est un morphisme de groupes c'est-à-dire que ϕ satisfait l'axiome I.2.4.Ann$_5$).

Enfin l.axiome A.1.1.Mod$_3$) (resp. A.1.1.Mod$_4$),) assure que ϕ satisfait à l'axiome I.2.4.Ann$_6$) (resp. I.2.4.Ann$_7$).)

ii) Réciproquement, étant donné un groupe abélien $(M, +)$ muni d'un morphisme

$$\phi \,:\, (A, +, *) \,\to\, (\mathrm{End}_{\mathbf{Gr}}(M), +, \circ),$$

il existe une unique structure de A-module $\cdot_{\phi,M}$ sur M telle que

$$\phi_{(M,+,\cdot_{\phi,M})} \,=\, \phi \,.$$

***Preuve** : Réciproquement supposons donné un groupe abélien $(M, +)$ et un morphisme d'anneaux*

$$\phi \,:\, (A, +, *) \,\to\, (\mathrm{End}_{\mathbf{Gr}}(M), +, \circ) \,.$$

Supposons qu'il existe une structure de module $\cdot$ sur M telle que

$$\psi \,:=\, \phi_{(M,+,\cdot)} \,=\, \phi \,.$$

Pour tout $a \,\in\, A$, et tout $x \,\in\, M$,

$$a \cdot x \,=\, \psi(a)(x) \,=\, \phi(a)(x) \,.$$

La structure $\cdot$ existe et est donc uniquement déterminée. Reste à prouver qu'elle vérifie bien les axiomes A.1.1.Mod$_1$) à A.1.1.Mod$_4$). On peut dégager de la preuve de i) le tableau suivant, mettant en correspondance les axiomes :

$$\begin{array}{rcl} \cdot & \text{« } \Leftrightarrow \text{ »} & \phi \\ \textit{A.1.1.Mod}_1) & \text{« } \Leftrightarrow \text{ »} & \phi \textit{ est à valeurs dans } \mathrm{End}_{\mathbf{Gr}}(M) \\ \textit{A.1.1.Mod}_2) & \text{« } \Leftrightarrow \text{ »} & \textit{I.2.4.Ann}_5) \\ \textit{A.1.1.Mod}_3) & \text{« } \Leftrightarrow \text{ »} & \textit{I.2.4.Ann}_6) \\ \textit{A.1.1.Mod}_4) & \text{« } \Leftrightarrow \text{ »} & \textit{I.2.4.Ann}_7) \end{array} \qquad 1$$

iii) Si $(M,+,\cdot)$ est un A-module

$$\cdot_{\phi_{(M,+,\cdot)},M} \;=\; \cdot\,.$$

***Preuve** : Est tout à fait formel en considérant le tableau ii).1.*

Remarque A.1.5 i) Si M est un A-module, pour tout $x \in M$, on a :

$$0_A \cdot x \;=\; 0_M\,.$$

Grâce à la proposition A.1.4, ceci est immédiat car l'image de 0_A dans $(\mathrm{End}_{\mathbf{Gr}}(M),+)$ est nécessairement l'application nulle (cf. I.2.3.i).)

On peut aussi donner une démonstration directe de ce fait, qui reprend évidemment l'argument utilisé pour prouver I.2.3.i) : On a en effet, pour tout $x \in M$,

$$\begin{array}{rcl} 0_A \cdot x & = & (0_A +_A 0_A)\cdot x \\ & = & 0_A \cdot x + 0_A \cdot x\,. \end{array}$$

Le fait que l'on puisse "simplifier" l'égalité $0_A \cdot x + 0_A \cdot x = 0_A \cdot x$ par $0_A \cdot x$, vient de ce que $(M,+)$ est un groupe.

ii) De même pour tout $x \in M$,

$$(-1_A)\cdot x \;=\; -x\,,$$

(où -1_A désigne l'opposé de 1_A dans le groupe $(A,+_A)$ et $-x$ l'opposé de x dans le groupe $(M,+)$.)

iii) Enfin pour tout $a \in A$,

$$a \cdot 0_M \;=\; 0_M\,;$$

ce qui découle du fait qu'on peut, grâce à la proposition A.1.4, voir a comme une homothétie de M et donc comme un endomorphisme du groupe abélien $(M,+)$.

Définition A.1.6 (A-algèbre) Si $f : A \to B$ est un morphisme d'anneaux (cf. I.2.4) on dit que B ou le couple (B,f) ou même le morphisme f est une *A-algèbre*. Le morphisme f est appelé *morphisme structural*.

Si B est un anneau commutatif on dit de B, (B,f) ou f que c'est une *algèbre commutative*.

On peut ici encore, si l'on oublie le morphisme structural parler de

$$\text{l'}\textit{anneau sous-jacent}\text{ à l'algèbre } f : A \to B\,.$$

Exemple A.1.7 (Exemples de A-algèbres) a) Pour tout anneau A, l'identité de A donne à A une structure de A-algèbre *i.e.* (A,Id_A) est une A-algèbre.

b) La proposition I.6.11 assure que tout anneau A est une $\mathbb{Z}$-algèbre et ce d'une seule manière.

c) Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension finie.

Le corps $\mathbb{K}$ s'identifie "naturellement" à l'ensemble des homothéties de E, c'est-à-dire qu'à tout $\lambda \in \mathbb{K}$, on associe l'endomorphisme de E défini par $x \mapsto \lambda x$ pour tout $x \in E$. On définit ainsi une structure "naturelle" de $\mathbb{K}$-algèbre sur $\mathrm{End}(E)$.

Exemple A.1.8 a) L'exemple A.1.2.b) peut être réinterprété à la lumière de la proposition A.1.4. En effet un anneau commutatif $(A, +, *)$ est, en particulier, un groupe abélien et, pour tout $a \in A$, l'application

$$A \to A\,,\ x \mapsto a * x$$

est un endomorphisme du groupe abélien $(A, +)$ (cf. I.6.13,) *i.e.* un élément de $\mathrm{End}_{\mathbf{Gr}}((A, +))$.

On vérifie que l'application

$$A \to \mathrm{End}_{\mathbf{Gr}}((A, +))\,,\ a \mapsto (x \mapsto a * x)$$

est un morphisme d'anneaux. On définit ainsi une structure de A-module sur A dont on vérifie aisément que c'et exactement celle définie en A.1.2.b).

b) Plus généralement si $f : A \to B$ est un morphisme d'anneaux, (on dit alors que (B, f) est une A-algèbre (cf. A.1.6,)) le morphisme $B \to \mathrm{End}_{\mathbf{Gr}}(B)$ défini comme ci-dessus composé avec le morphisme f est un morphisme d'anneaux $A \to \mathrm{End}_{\mathbf{Gr}}(B)$ qui donnt donc à B, en vertu de la proposition A.1.4, une structure de A-module.

Plus explicitement, on constate sans difficulté, que celle-ci est donnée par la loi externe

$$\cdot : A \times B \to B,\ \text{définie par } a \cdot b := f(a) *_B b\,.$$

On remarquera que l'exemple a) est un cas particulier de ce qui précède en prenant

$$B = A \,\text{et}\, f = \mathrm{Id}_A : A \to A\,.$$

c) Un cas particulier de l'exemple b) est celui où $\mathfrak{I} \subset A$ est un idéal de A et $B = A/\mathfrak{I}$. La surjection canonique $\pi : A \to B$ fait, bien entendu de B une A-algèbre, mais on se limitera souvent, à considérer la structure de A-module sur B.

Dans le cas où $A = \mathbb{Z}$ est l'anneau des entiers relatifs, et $n \in \mathbb{Z}$ cela revient à ne considérer $\mathbb{Z}/n\mathbb{Z}$, que comme un groupe abélien, en oubliant sa structure d'anneau.

d) Si $f : A \to B$ est un morphisme d'anneaux (ou ancore une A-algèbre,) et $(M, +, \cdot^B)$ un B-module, M est muni d'une structure naturelle de A-module $\cdot^A$ définie pour tout $a \in A$ et tout $x \in M$ par :

$$a \cdot^A x := f(a) \cdot^B x\,.$$

Elle provient du morphisme $A \to \mathrm{End}_{\mathbf{Gr}}(M)$ obtenu en composant le morphisme

$B \to \mathrm{End}_{\mathbf{Gr}}(M)$ définissant la structure de B-module sur M et le morphisme d'anneaux f .

La proposition suivante permet de donner une description alternative et peut-être plus habituelle que celle donnée en A.1.6, des A-algèbres. Elle fait également le lien avec l'exemple A.1.8.b).

Proposition A.1.9 *i) Soit B un anneau commutatif muni d'une loi de composition externe*

$$\cdot_B \ : \ A \times B \ \to \ B$$

telle que $(B, +_B, \cdot_B)$ soit un A-module.

Alors il existe un unique morphisme d'anneaux $f \ : \ A \ \to \ B$ tel que

$$f \ : \ (A, +_A, \cdot_A) \ \to \ (B, +_B, \cdot_B)$$

soit aussi un morphisme de A-modules (où A est vu comme A-module à travers l'identité Id_A (cf. A.1.2.)

***Preuve** : S'il existe un morphisme d'anneaux $f \ : \ A \ \to \ B$, nécessairement $f(1_A) \ = \ 1_B$. Pour tout $a \ \in \ A$,*

$$\begin{aligned} f(a) &= f(a *_A 1_A) \\ &= f(a \cdot_A 1_A) \\ &= a \cdot_B f(1_A) \\ &= a \cdot_B 1_B \ . \end{aligned}$$

Ceci définit bien une unique application $f \ : \ A \ \to \ B$. Reste à prouver que c'est bien un morphisme ; ce qui est laissé en exercice.

ii) Une A-algèbre $f \ : \ A \ \to \ B$ a une structure canonique de A-module, donnée, pour tout $(a, b) \ \in \ A \times B$, par :

$$a \cdot_B b \ := \ f(a) *_B b \ .$$

Avec cette structure,

$$f \ : \ (A, +_A, \cdot_A) \ \to \ (B, +_B, \cdot_B)$$

est un morphisme de A-modules, (où A est vu comme A-module à travers l'identité Id_A,

***Preuve** : (cf. A.1.8.b).)*

Les procédé i) et ii) sont inverses l'un de l'autre .

Remarque A.1.10 Nous avons alors envisagé les algèbres comme des anneaux bénéficiant d'une structure supplémentaire, à savoir un morphisme structural ; on peut aussi considérer les A-algèbres comme des A-modules (cf. A.1.8.b),) munis d'une structure supplémentaire, à savoir une structure d'anneau compatible, en un certain sens, à la structure de A-module. Avant d'expliquer comment ces deux constructions se déduisent l'une de l'autre et comment en réalité elles recouvrent la même notion, remarquons que ainsi définies de deux manières différentes, pourrait se poser pour les algèbres la question de la cohérence de certaines définitions. Le noyau par exemple d'un morphisme d'algèbre pourrait être vu comme le noyau au sens des morphismes d'anneaux, tout comme le noyau au sens des morphismes de A-modules et il ne serait pas certain, a priori, que le terme noyau désigne alors le même objet. En réalité dans ce cas particulier la notion n'est autre que celle héritée de la structure de groupe abélien sous-jacente.

Tout d'abord, étant donné un anneau commutatif A, un ensemble B est une A-algèbre si, de manière équivalente :

i) Il existe un morphisme d'anneaux $f \ : \ A \ \to \ B$ (ce qui entraîne implicitement que B est un anneau ;)

ii) B est un anneau qui possède une structure de A-module ;

On dira que le morphisme structural i) et la loi externe ii) *se déduisent l'un de l'autre*.

Remarque A.1.11 i) La proposition I.6.6 assure en fait qu'un groupe abélien a une structure naturelle (*i.e.* unique) de $\mathbb{Z}$-module.

ii) Tout anneau A est canoniquement une $\mathbb{Z}$-algèbre, *i.e.*

$$\text{il existe un unique morphisme de structure } f : \mathbb{Z} \to A .$$

Preuve : Voir la proposition I.6.11.

iii) Les proposition A.1.9 ci-dessus et A.1.4 conduisent à une exact analogue de la remarque I.6.13.

Si $\phi : A \to B$ est le morphisme structural de B, $\psi : A \to \mathrm{End}_{\mathbf{Gr}}(B)$ le morphisme donnant la structure de A-module et $\mu : B \to \mathrm{End}_{\mathbf{Gr}}(B)$ défini comme en I.6.13, on a encore un diagramme commutatif de morphismes d'anneaux :

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ & \searrow^{\psi} & \downarrow \mu \\ & & \mathrm{End}_{\mathbf{Gr}}(B) . \end{array} \qquad 1$$

iv) Il se peut qu'on ait déjà rencontré la notion de $\mathbb{K}$-algèbre dans le cas où $\mathbb{K}$ est un corps qu'on aura alors vraisemblablement définie comme un anneau ayant une structure de $\mathbb{K}$-espace vectoriel. Ceci correspond exactement aux remarques faites ci-dessus.

A.2 . −Morphismes (cf. I.2)

Définition A.2.1 Étant donnés deux A-modules $(M, +_M, \cdot_M)$ et $(N, +_N, \cdot_N)$ on appelle *morphisme (homomorphisme) de A-modules* (ou simplement *morphisme* si le contexte est clair, ou même *application linéaire*) une application $f : M \to N$, telle que :

Mod$_5$) $f : (M, +_M) \to (N, +_N)$ est un morphisme de groupes (cf. I.2.1 ;)

Mod$_6$) pour tout $a \in A$ et tout $x \in M$,

$$f(a \cdot_M x) = a \cdot_N f(x) .$$

De manière équivalente, $f : M \to N$ est un morphisme de A-modules si et seulement si pour tout $(a, b) \in A \times A$ et tout $(x, y) \in M \times M$,

$$f(a \cdot_M x +_M b \cdot_M y) = a \cdot_N f(x) +_N b \cdot_N f(y) .$$

On pourrait noter $\mathrm{Hom}_{A-\mathbf{mod}}(M, N)$ l'ensemble des morphismes de A-modules de M dans N, néanmoins la notation la plus utilisée est encore $\mathrm{Hom}_A(M, N)$.

Définition A.2.2 (Morphisme de A-algèbres) Soit A un anneau

$$f : A \to B \text{ et } g : A \to C \text{ deux } A\text{-algèbres} .$$

Un morphisme d'anneaux (cf. I.2.4) $u : B \to C$ est un *morphisme de A-algèbres* si $u \circ f = g$ autrement dit, si l'on a un triangle commutatif de morphismes d'anneaux :

$$\begin{array}{ccc} A & & \\ {\scriptstyle f}\downarrow & \searrow {\scriptstyle g} & \\ B & \xrightarrow{u} & C . \end{array}$$

On note $\mathrm{Hom}_{A-\mathbf{alg}}(B, C)$ l'ensemble des homomorphismes de A-algèbres de B dans C.

Lemme A.2.3 ((cf. I.2.5)) *Étant donnés un anneau A,*

i) Pour tout A-module (resp. toute A-algèbre) X, l'identité Id_X, de X est un morphisme de A-modules (resp. de A-algèbres) de X dans lui-même.

ii) Pour

$$f : X \to Y \text{ et } g : Y \to Z$$

des morphismes de A-modules, (resp. de A-algèbres,) le composé $g \circ f$ est un morphisme de A-modules (resp. de A-algèbres,) de X à valeurs dans Z.

Définition A.2.4 (Isomorphisme (cf. I.2.6)) Étant donné un anneau A, un morphisme $f : X \to Y$ de A-modules (resp. de A-algèbres) est un *isomorphisme* s'il existe un morphisme (de A-modules (resp. de A-algèbres,)) $g : Y \to Z$ tel que :

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

On notera

$\mathrm{Isom}_{A-\mathbf{mod}}(X,Y)$ (resp. $\mathrm{Isom}_{A-\mathbf{alg}}(X,Y)$) (ou simplement $\mathrm{Isom}_A(X,Y)$ ou même $\mathrm{Isom}(X,Y)$

si le contexte est clair) l'ensemble des isomorphismes de X dans Y.

Proposition A.2.5 (Morphisme bijectif (cf. I.2.7)) *Étant donnés deux A-modules (resp. A-algèbres) X et Y, une application $f : X \to Y$ est un isomorphisme de A-modules (resp. A-algèbres) si et seulement si c'est un morphisme bijectif.*

Preuve *: Si f est un isomorphisme, f est évidemment une bijection.*

Réciproquement, supposons que f est une bijection. Il existe alors une bijection ensembliste réciproque $g : Y \to X$, i.e. une application telle que

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

Puisque f est dans tous les cas un morphisme de groupes, il en est de même de g grâce à la proposition I.2.7. Si f est un morphisme d'algèbres, donc en particulier d'anneaux, la proposition loc. cit. assure encore qu'il en est de même de g. Ne reste donc qu'à vérifier :

*i) (A-**module**)*

Si f est un morphisme de A-modules :

$$\begin{array}{rcl} \forall a \in A,\ \forall y \in Y, \quad g(a \cdot y) & = & g(a \cdot f(g(y))) \\ & = & g(f(a \cdot g(y))) \\ & = & a \cdot g(y) \,; \end{array}$$

ce qui assure que g est un morphisme de A-modules.

*ii) (A-**algèbres**)*

Si f est un morphisme de A-algèbres, notons alors $u : A \to X$ et $v : A \to Y$ les morphismes structuraux respectifs de X et Y. On a alors, puisque f est un morphisme $f \circ u = v$, si bien que

$$g \circ v = g \circ f \circ u = u \,;$$

ce qui assure que g est un morphisme d'Algèbres.

Définition A.2.6 (Endomorphisme/Automorphisme (cf. I.2.8)) Pour un A-module (resp. une A-algèbre,) X,

i) (**Endomorphismes**)

Un morphisme $f : X \to X$ de X dans lui-même est appelé *endomorphisme*.

On note

$\mathrm{End}_{A-\mathbf{mod}}(X)$ (resp. $\mathrm{End}_{A-\mathbf{alg}}(X)$) (ou simplement $\mathrm{End}_A(X)$ ou même $\mathrm{End}(X)$)

l'ensemble des endomorphismes de X.

ii) (**Automorphisme**)

Un morphisme $f : X \to X$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition A.2.5, de dire que f est un endomorphisme bijectif.

On note

$$\mathrm{Aut}_{A-\mathbf{mod}}(X) \text{ (resp. } \mathrm{Aut}_{A-\mathbf{alg}}(X) \text{) (ou simplement } \mathrm{Aut}_A(X) \text{ ou même } \mathrm{Aut}(X) \text{)}$$

l'ensemble des automorphismes de X.

Exemple A.2.7 a) Pour un A-module M, l'identité Id_M est un automorphisme.

b) Pour tout A-module M et tout $a \in A$, l'application de M dans lui-même $x \mapsto a \cdot x$ (qu'on pourrait appeler *homothétie de rapport* a) est un endomorphisme de M qui est même un automorphisme si et seulement si $a \in A^\times$ est inversible. L'identité Id_M n'est autre que l'homothétie de rapport 1.

Exemple A.2.8 (Automorphismes de A-algèbres) a) Pour une A-algèbre $f : A \to B$, l'identité Id_B est un automorphisme.

b) L'inclusion du corps $\mathbb{R}$ des nombres réels dans le corps $\mathbb{C}$ des nombres complexes fait de $\mathbb{C}$ une $\mathbb{R}$-algèbre. La conjugaison complexe est un automorphisme de la $\mathbb{R}$-algèbre $\mathbb{C}$.

c) La situation ci-dessus peut être vue come un cas particulier d'une question plus générale consistant à étudier les automorphismes d'une K-algèbre L où K et L sont des corps et $K \subset L$. Cette construction sera abondamment étudiée dans le cadre de la théorie de Galois notamment mais pas dans le cadre de ce cours.

Proposition A.2.9 *Étant donné un anneau A et des A-algèbres (B, f) et (C, g), une application $u : B \to C$ est un morphisme de A-algèbre au sens de la définition A.2.2 si et seulement si u est un morphisme de A-modules et un morphisme d'anneaux pour la structure qui lui correspond par la proposition A.1.9.*

Preuve *: Notons $f : A \to B$ et $g : A \to C$ les morphismes structuraux des A-algèbres B et C. L'application u est un morphisme d'algèbres au sens de la définition A.2.2, si u est un morphisme d'anneaux et si, de plus, $u \circ f = g$. Notons $\cdot_B$ (resp. $\cdot_C$) la loi externe sur B (resp. C) déduite de f (resp. g.) Alors pour tout $(x, y) \in B \times B$, et tout $(a, b) \in A \times A$,*

$$\begin{aligned} u(a \cdot_B x +_B b \cdot_B y) &= u(f(a) *_B x +_B f(b) *_B y) \\ &= u[f(a)] *_C u(x) +_C u[f(b)] *_C y \\ &= g(a) *_C x +_C g(b) *_C y \\ &= a \cdot_C x +_C b \cdot_C y \end{aligned}$$

ce qui prouve que u est bien un morphisme de A-modules.

Réciproquement si $\cdot_B$ (resp. $\cdot_C$) désigne la structure de A-module sur B (resp. C,) on note $f : A \to B$ (resp. $g : A \to C$) le morphisme d'anneaux qui s'en déduit par la proposition A.1.9. Si u est un morphisme de A-modules, u est, en particulier, un morphisme de groupes

$$(B, +_B) \to (C, +_C) .$$

C'est aussi un morphisme d'anneaux par hypothèse. La seule chose à vérifier est donc la compatibilité aux morphismes structuraux. Or, pour tout $a \in A$:

$$\begin{aligned} u[f(a)] &= u[f(a) *_B 1_B] \\ &= u[a \cdot_B 1_B] \\ &= a \cdot_C u(1_B) \\ &= a \cdot_C 1_C \\ &= g(a) *_C 1_C \\ &= g(a) \end{aligned}$$

ce qui prouve que $u \circ f = g$ *et achève la preuve.*

Même si nous n'en ferons sans doute pas un usage immodéré dans ce cours, il est bon, dans un souci de cohérence, de mentionner que les constructions que nous avons faites à partir des algèbres dans l'exemple A.1.8.b) s'étendent aux morphismes :

Proposition A.2.10 *Étant donné un morphisme de* A*-algèbres*

$$u : (B, f) \to (C, g)$$

(cf. A.2.2,) c'est un morphisme de A*-modules pour les structures définies en A.1.8.b).*

C'est même un isomorphisme de A*-algèbres si et seulement si c'est un morphisme de* A*-algèbre et un isomorphisme de* A*-modules.*

Remarque A.2.11 i) De même qu'on a vu en A.1.11.i) qu'il n'y a aucune différence entre groupes abéliens et $\mathbb{Z}$-modules la proposition I.6.10 établit qu'il n'y a en fait aucune différence non plus entre leurs morphismes, autrement dit qu'un morphisme de ghroupes entre groupes abéliens n'est rien d'autre qu'un morphisme de $\mathbb{Z}$-modules.

ii) Étant donnés deux anneaux A et B, $u : A \to B$ est un morphisme d'anneaux si et seulement si u est un morphisme de $\mathbb{Z}$-algèbres.

Preuve : Soient A et B deux anneaux dont on notera f_A et f_B les structures canoniques de $\mathbb{Z}$-algèbres dont l'existence et l'unicité ont été établies en A.1.11.ii).

Soit $u : A \to B$ un morphisme d'anneaux. Alors

$$u \circ f_A : \mathbb{Z} \to B$$

est un morphisme d'anneaux de $\mathbb{Z}$ à valeurs dans B. Or d'après A.1.11.ii), un tel morphisme est unique il s'ensuit que

$$u \circ f_A = f_B ;$$

ce qui prouve que u est un morphisme de $\mathbb{Z}$-algèbres.

Réciproquement un morphisme $u : A \to B$ de $\mathbb{Z}$-algèbres est, par définition, un morphisme d'anneaux.

Proposition A.2.12 *i) Pour M et N des A-modules, l'ensemble*

$$\mathrm{Hom}_A(M,N) \text{ des morphismes de } A\text{-modules de } M \text{ dans } N$$

a une structure naturelle de A-module.

Preuve *: On sait que $\mathrm{Hom}_A(M,N)$ a déjà une structure de groupe abélien : en effet M et N sont par définition des groupes abéliens (cf. A.1.1.Mod$_0$)) et tout morphisme de A-modules de M dans N, est en particulier un morphisme de groupes (cf. A.2.1.Mod$_5$).)*

On rappelle que la loi $+$ est donnée sur $\mathrm{Hom}_A(M,N)$ par $(f+g)(x) = f(x) +_N g(x)$. On définit maintenant une loi externe

$$\cdot : A \times \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N)$$

par

$$(a \cdot f)(x) := a \cdot_N f(x) .$$

On laisse le soin au lecteur de constater qu'on définit bien ainsi une structure de A-module.

ii) Étant donné un morphisme de A-modules $f : M \to N$, on définit pour tout A-modules P des applications :

$$\begin{array}{rccc} \mathrm{Hom}_A(f,P): & \mathrm{Hom}_A(N,P) & \longrightarrow & \mathrm{Hom}_A(M,P) \\ & u & \longmapsto & u \circ f \\ \mathrm{Hom}_A(P,f): & \mathrm{Hom}_A(P,M) & \longrightarrow & \mathrm{Hom}_A(P,N) \\ & v & \longmapsto & f \circ v . \end{array}$$

qui sont des morphismes de A-modules.

iii) Pour tout A-module M l'application

$$\mathrm{Hom}_A(A,M) \to M , \ f \mapsto f(1)$$

est un isomorphisme de A-modules.

Notation A.2.13 Pour un A-module M on voudra peut-être parfois noter $M^* := \mathrm{Hom}_A(M,A)$ (où A est muni de sa structure de A module définie en A.1.2.b) ou de manière équivalente en A.1.8.a).)

On sera tenter d'appler M^* le *dual* de M ; puisque dans le cas où A est un corps et M par conséquent un espace vectoriel on retrouve effectivement la construction de l'espace vectoriel dual. Les éléments de M^* seront aussi usuellement appelés *formes linéaires*. Il faudrait cependant bien se garder de croire que le A-module M^* jouit des mêmes agréables propriétés que dans le cas des espaces vectoriels (cf. TD n° I, exercice B.)

Pour un morphisme de A-modules $f : M \to N$, on notera

$$f^* := \mathrm{Hom}_A(f,A) : N^* = \mathrm{Hom}_A(N,A) \to M^* = \mathrm{Hom}_A(M,A)$$

(la notation $\mathrm{Hom}_A(f,P)$ bien que tout à fait explicite n'en restant pas moins assez lourde !)

A.3 . −Sous-modules, sous-algèbres (cf. I.3)

Définition A.3.1 (Sous-module) Étant donné un A-module $(M, +_M, \cdot_M)$ on appelle *sous-A-module* (ou simplement sous-module) de M un sous-ensemble K de M tel que les lois $+_M$ et

$\cdot_M$ définissent une structure de A-module sur K. Autrement dit la loi $+_M$ (resp. $\cdot_M$) se restreint à $K \times K$ (resp ; $A \times K$,) donnant à $(K, +_{M|K\times K}, \cdot_{M|A\times k})$ une structure de A-module.

En particulier $(K, +_{M|K\times K})$ est un sous-groupe de $(M, +)$ (cf. I.3.1.)

Exemple A.3.2 a) Étant donné un A-module M, les parties $\{0\}$ et M de M sont des sous-modules de m.

b) On rappelle (cf. A.1.2.b),) qu'un anneau A possède une structure naturelle de A-module sur lui-même. Une partie $\mathfrak{I}$ de A est alors un sous-A-module de A si et seulement si c'est un idéal (cf. I.3.5.)

c) Si $\mathbb{K}$ est un corps, une partie $\mathfrak{I}$ de l'anneau $\mathbb{K}[X]$ est un sous-$\mathbb{K}[X]$-module de $\mathbb{K}[X]$ si et seulement si c'est un idéal de $\mathbb{K}[X]$ si et seulement s'il existe un polynôme $P \in$ '$\mathbb{K}[X]$ tel que $\mathfrak{I} = P\mathbb{K}[X]$.

d) Si $f : a \to B$ est une A-algèbre (cf. A.1.6,) toute sous-A-algèbre $g : A \to C$ de B est naturellement un sous-A-module de B pour les structures considérées dans l'exemple A.1.8.b).

e) (cf. TD n° V, exercice E, question 3), a),) pour une description des sous-KkX-modules d'un $\mathbb{K}[X]$-module quelconque.

Définition A.3.3 (Sous-algèbre) Étant donnés un anneau A et une A-algèbre $f : A \to B$, on dit qu'une partie C
$subset$ B de A est une *sous-A-algèbre* de B si C est un sous-anneau de B (cf. I.3.3,) et si le morphisme structural f est à valeurs dans C.

Il revient au même de demander que l'inclusion canonique $C \hookrightarrow B$ *i.e.* la restriction de $res\mathrm{Id}_B C$ de Id_B à C soit un morphisme d'algèbres.

Par extension (cf. I.3.3,) si $i : B \to C$ est un morphisme injectif de A-algèbres on dira parfois aussi, par abus de langage, que C est une sous-A-algèbre de B.

Exemple A.3.4 (Exemples de sous-algèbres) L'anneau $\mathbb{Q}$ (resp. $\mathbb{R}$) est une sous-algèbre de $\mathbb{R}$ (resp. $\mathbb{C}$) même si l'injection étant l'inclusion canonique on omet presque toujours de la noter.

Proposition A.3.5 (Sous-algèbre/sous-module) *Une partie $C \subset B$ de B est une sous-A-algèbre de B au sens de la définition A.3.3, si et seulement si c'et à la fois un sous-anneau au sens de la définition I.3.3 et un sous-module au sens de la définition A.3.1.*

Proposition A.3.6 (Caractérisation des sous-modules (cf. I.3.9)) *Étant donné un A-module M et K un sous-ensemble, de M, les assertions suivantes sont équivalentes :*

a) K est un sous-A-module de M.

b) K est un sous-ensemble non vide de M tel que pour tout $(a, b) \in A \times A$ et tout $(x, y) \in K \times K$,

$$a \cdot_M x +_M b \cdot_M y \in K .$$

c) La restriction

$$\mathrm{Id}_{M|K} : K \to M$$

de l'identité Id_M à K est un morphisme de A-modules. Ceci signifie implicitement que K possède une structure de A-module.

Remarque A.3.7 On exprimera usuellement la propriété A.3.6.b) en disant que K est *stable par combinaisons linéaires à coefficients dans* Ace qui est une terminologie déjà bien connue dans le cas où A est un corps, M par conséquent un A-espace vectoriel et K un sous-espace vectoriel de M.

Exemple A.3.8 a) Si N est un sous-A-module de M et P un sous-A-module de N alors P est un sous-A-module de M.

b) Si N et P sont deux sous-A-modules d'un module M, $N \cap P$ est un sous-A-module de M. Noter qu'en général, $N \cup P$ n'est pas un sous-A-module de M (cf. A.3.9.iii).)

Proposition A.3.9 (Le treillis des sous-modules (cf. I.3.12)) *Étant donnés deux sous-A-modules (resp. sous-A-algèbres)*

$$Y \subset X \text{ et } Z \subset X \text{ d'un } A\text{-module (resp. d'une } A\text{-algèbre) } X :$$

i) $Y \cap Z$ *est un sous-module (resp. une sous-algèbre) de* X ;

ii) Plus généralement pour $\mathcal{Y}$ *un ensemble non vide de sous-modules (resp. de sous-algèbres) de* X, $\bigcap_{\mathcal{Y}} Y$ *est un sous-module (resp. une sous-algèbre) de* X.

iii) $Y \cup Z$ *est un sous-module (resp. une sous-algèbre) de* X *si et seulement si* $Y \subset Z$ *ou* $Z \subset Y$.

iv) Si $\left(Y_n\right)_{,n\in\mathbb{N}}$ *est une suite de sous-modules (resp. de sous-algèbres) de* X *telle que*

$$\forall (p,q) \in \mathbb{N}\times\mathbb{N},\ \exists r \in \mathbb{N},\ Y_p \subset Y_r \text{ et } Y_q \subset Y_r,$$

alors $\bigcup_{n\in\mathbb{N}} Y$ *est un sous-module (resp. une sous-algèbre) de* X.

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

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p \leq q \Rightarrow Y_p \subset Y_q$$

car alors

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ Y_p \subset Y_{\max(p,q)} \text{ et } Y_q \subset Y_{\max(p,q)} .$$

Remarque A.3.10 i) (**Sous-groupe**)

Une partie $\mathfrak{I}$ de $\mathbb{Z}$, est un sous-$\mathbb{Z}$-module si et seulement si c'est un idéal de $\mathbb{Z}$ si et seulement si c'est un sous-groupe de $\mathbb{Z}$ si et seulement si il existe $d \in \mathbb{Z}$ tel que $\mathfrak{I} = d\mathbb{Z}$.

Plus généralement pour tout groupe abélien A, une partie $B \subset A$ de A est un sous-groupe de A si et seulement si c'est un sous-$\mathbb{Z}$-module de A.

ii) (**Sous-$\mathbb{Z}$-algèbres**)

Étant donné un anneau A, (ou de manière équivalente, en vertu de A.1.11.ii), une $\mathbb{Z}$-algèbre,) une partie B de A est un sous-anneau si et seulement si c'et une sous-$\mathbb{Z}$-algèbre.

A.4 . −Intersection, somme, engendrement (cf. I.4)

Corollaire A.4.1 (de la proposition A.3.9 (cf. I.4.1)) *Étant donnés un anneau commutatif A, un A-module (resp. une A-algèbre) X, et $S \subset X$ une partie de X, l'ensemble $\mathcal{Y}$ des sous-modules (resp. sous-algèbres) de X contenant S possède un plus petit élément*

$$< S >= \bigcap_{Y \in \mathcal{Y}} Y \, .$$

Définition A.4.2 (Sous-module (resp. sous-algèbre) engendré (cf. I.4.2)) Avec les notations du corollaire A.4.1, le sous-module (resp. la sous-algèbre) $< S >$ s'appelle le *sous-module engendré*, (resp. la *sous-algèbre engendrée*,) par S. On dit que S est une *partie génératrice* de $< S >$.

Exemple A.4.3 ((cf. I.4.3)) a) $< \emptyset >= \{0\}$.

b) Pour tout sous-module N de M,

$$< N >= N \, .$$

c) Tout sous-$\mathbb{Z}$-module de $\mathbb{Z}$, (resp. sous-$\mathbb{K}[X]$-module de $\mathbb{K}[X]$ (cf. III.5,)) *i.e.* tout idéal de $\mathbb{Z}$ (resp. $\mathbb{K}[X]$,) est engendré par un seul élément *i.e.* est *principal*.

d) Si $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel, pour tout $S \subset E$, $< S >$ n'est autre que le sous-espace vectoriel engendré par S usuellement noté $\mathrm{Vect}\big\{S\big\}$ dans le cadre de l'algèbre linéaire.

Il se peut également que pour un A-module M avec A un anneau qu'i n'est pas nécessairement un corps, et $S \subset M$, on note $\mathrm{Vect}\big\{S\big\} := < S >$.

Lemme A.4.4 (descriptions du sous-module engendré (cf. I.4.6)) *Étant donné un A-module M, pour tout $X \subset M$, tout $x \in M$, $x \in < X >$ si et seulement s'il existe $r \in \mathbb{N}$, $x_i \, , 1 \leq i \leq r \in X$, et $a_i \, , 1 \leq i \leq r \in A$ tels que*

$$x \; = \; \sum_{i=1}^{r} a_i \cdot x_i \, . \qquad \textit{A.4.4.1}$$

Lemme A.4.5 (Somme (cf. I.4.7)) *Étant donné un A-module M et $\mathcal{X}$ un ensemble de sous-modules de M,*

$$< \bigcup_{X \in \mathcal{X}} X >= \left\{ r \in \mathbb{N} \, ; \, \sum_i 1 r s_i \, , \, \forall 1 \leq i \leq r, \, \exists X \in \mathcal{X}, \, s_i \in X \right\} . \qquad \textit{A.4.5.1}$$

Autrement dit :

$$\forall x \in M, \; x \in < \bigcup_{X \in \mathcal{X}} X > \; \Leftrightarrow \; \exists r \in \mathbb{N}, \, \forall 1 \leq i \leq r, \, \exists X_i \in \mathcal{X}, \, \exists x_i \in X_i, \, x \; = \; \sum_{i=1}^{r} x_i \, . \qquad \textit{A.4.5.2}$$

Définition A.4.6 (Somme (cf. I.4.8)) Avec les notations du lemme A.4.5 :

i) (**Somme**)
$(\bigcup_{X \in \mathcal{X}} Y)$ s'appelle la *somme* des X pour X appartenant à $\mathcal{X}$ qu'on notera $\sum_{X \in \mathcal{X}} X$.

ii) (**Somme directe**)

On dit qu'on a une *somme directe* si dans la décomposition A.4.5.2 l'entier r, les X_i et les $x_i \neq 0$, sont uniques. On notera alors

$$\bigoplus_{X \in \mathcal{X}} X := < \bigcup_{X \in \mathcal{X}} > .$$

iii) (**Supplémentaires**)

Pour un A-module M et deux sous-modules N et P, si $M = N \oplus P$, on dit que N et P sont *supplémentaires* l'un de l'autre.

Proposition A.4.7 (Propriété universelle des sommes directes (cf. I.4.9)) *Étant donnée un a-module M et $\mathcal{N}$ une famille de sous-modules telle que la somme $\sum_{N \in \mathcal{N}} N = \bigoplus_{N \in \mathcal{N}} N$ est directte, pour tout ensemble de morphismes*

$$\{f_N : N \to P\}_{,N \in \mathcal{N}},$$

où P est un A-module, il existe un unique morphisme

$$f : \bigoplus_{N \in \mathcal{N}} N \to P \text{ tel que } \forall N \in \mathcal{N},\ f_{|N} = f_N .$$

Remarque A.4.8 ((cf. I.4.10)) i) De même que dans le cas des groupes abéliens, pour M un A-module, N et P des sous-modules,N et P sont en somme directe ou encore supplémentaires l'un de l'autre si et seulement si

$$M = N + P \text{ et } N \cap P = \{0\} .$$

ii) Pour deux sous-modules N et P de M, le sous-module $N + P$ engendré par $N \cup P$ est l'ensemble des $x + y$ avec $x \in N$ et $y \in P$.

iii) Plus généralement, pour $N_{i\ ,1 \leq i \leq r}$ ($r \in \mathbb{N}^*$) un r-uplet de sous-modules de M, Notons

$$S := \sum_{i=1}^{r} N_i = N_1 + \ldots + N_r .$$

Alors pour tout $x \in M$, $x \in S$ si et seulement s'il existe un r-uplet

$$x_{i\ ,1 \leq i \leq r}\ ,\ \forall 1 \leq i \leq r,\ x_i \in N_i \text{ tel que } x = \sum_{i=1}^{r} x_i .$$

iv) Étant donné un A-module M et $\mathcal{N}$ un ensemble de sous-modules de M, on note $S := \sum_{N \in \mathcal{N}} N$. Alors pour tout $x \in M$, $x \in S$ si et seulement s'il existe un entier $r \in \mathbb{N}$, un r-uplet $N_{i\ ,1 \leq i \leq r} \in \mathcal{N}$ de sous-modules appartenant à $\mathcal{N}$, un r-uplet

$$x_{i\ ,1 \leq i \leq r}\ ,\ \forall 1 \leq i \leq r,\ x_i \in N_i \text{ tel que } x = \sum_{i=1}^{r} x_i .$$

Il convient de bien remarquer que, même si l'ensemble $\mathcal{N}$ n'est pas fini, la somme $\sum_{N \in \mathcal{N}} N$ est l'ensemble des sommes finies d'éléments des $N \in \mathcal{N}$.

Ainsi, par exemple la famille $X^{n}{}_{,n \in \mathbb{N}}$ est génératrice pour l'anneau $\mathbb{K}[X]$ vu comme $\mathbb{K}$-module (cf. III.2,) mais ne l'est pas pour l'anneau $\mathbb{K}[[X]]$ des séries formelles, toujours vu comme $\mathbb{K}$-module (cf. III.1.)

v) Ici encore l'existence d'un supplémentaire pour un sous-module N d'un A-module M n'est pas assurée en général ; puisqu'en particulier elle n'est déjà pas assurée dans le cas des $\mathbb{Z}$-modules (cf. I.4.10.ii).) Ici encore le théorème I.9.15 établit l'équivalence entre existence d'un supplémentaire de N et d'une section de la surjection canonique $M \to M/N$.

vi) (**Espaces vectoriels**)
Bien entendu, on sait que dans le cas où A est un corps un A-module M est un espace vectoriel. Dans le cas où M est de dimension finie, on connaît bien le théorème de la base incomplète qui assure en particulier que tout sous-espace vectoriel de M admet un supplémentaire.

Remarque A.4.9 i) Si $(A, +)$ est un groupe abélien et $S \subset A$ une partie de A, le sous-groupe de A engendré par S au sens de la définition I.4.2 est exactement le sous-$\mathbb{Z}$-module de A engendré par S au sens de la définition A.4.2.

ii) De même si $(A, +, *)$ est un anneau commutatif et $S \subset A$ une partie de A, l'idéal engendré par S au sens de la définition I.4.2 est exactement le sous-A-module de A engendré par S au sens de la définition A.4.2. On comparera notamment les formules I.4.6.2 et A.4.4.1.

iii) La *somme* (resp. *somme directe*) d'un ensemble de sous-$\mathbb{Z}$-modules définie en A.4.6 est exactement la somme (resp. la somme directe) définie pour les sous-groupes en I.4.8. la définition

A.5 . –Images directes, images réciproques, noyaux (cf. I.5)

Proposition A.5.1 (Image directe/réciproque (cf. I.5.1)) *Soit*

$$f \,:\, X \,\to\, Y \text{ un morphisme de } A\text{-modules (resp. de } A\text{-algèbres)}$$

i) ***(Image réciproque)***
Pour tout sous-module (resp. idéal,) Z de Y, l'image réciproque

$$f^{-1}(Z') \,=\, \{x \,\in\, X \,;\, f(x) \,\in\, Z\}$$

est un sous-module (resp. un idéal) de X.

ii) ***(Image directe)***
Pour tout sous-module (resp. sous-algèbre) Z de X, l'image directe de Z

$$f(Z) \,=\, \{y \,\in\, Y \,;\, \exists x \,\in\, Z,\ ,\ y \,=\, f(x)\}$$

est un sous-module (resp. une sous-algèbre,) de Y.

Définition A.5.2 (Noyau/Image (cf. I.5.2)) Étant donné un morphisme de A-modules (resp. de A-algèbres,) $f \,:\, X \,\to\, Y$, on appellera *noyau* (resp. *image*) de f

$$\mathrm{Ker}\, f \,:=\, \{x \,\in\, X \,\mid\, f(x) = 0_N\} \,=\, f^{-1}(\{0_N\}) \text{ resp. } (\mathrm{Im}\, f \,:=\, \{f(x)\,,\, x \,\in\, X\} \,=\, f(X)\,.)$$

Remarque A.5.3 (Noyau/Image (cf. I.5.3)) i) **(Image)**
La notion d'image d'un morphisme a été définie pour les groupes et les anneaux (cf. I.5.2.ii),) ainsi que pour les A-modules et les A-algèbres (cf. A.5.2.) Un A-module (resp. une A-algèbre,) étant, en particulier un groupe abélien (resp. un anneau,) il conviendrait de se demander si toutes ces définitions sont compatibles entre elles. En réalité il est immédiat de constater QUE l'image d'un morphisme de quelques sorte que ce soit, est en fait li'mage au sens ensembliste de l'application sous-jacente et qu'elle ne dépend donc pas du type de morphisme considéré. En revanche cette image peut jouir de propriétés différentes suivant le morphisme auquel on a affaire, voir à ce propos les propositions I.5.1 et A.5.1.

ii) De la même manière la notion de *noyau* est définie en I.5.2.i) et en A.5.2 et l'on pourrait se demander si toutes ces définitions sont compatibles. Il faut encore constater que toutes les structures algébriques considérées (anneaux, modules, algèbres,) sont en particulier des structures de groupes et leurs morphismes des morphismes de groupes. Les diverses définitions de noyaux n'en sont alors qu'une seule et même corresponddant à la définition de noyau d'un morphisme de groupe.

Corollaire A.5.4 (de la proposition A.5.1 : noyau/image) *Pour un morphisme de A-modules $f \,:\, M \,\to\, N$, le noyau (resp. l'image) de f est un sous-module de M (resp. N.)*

Proposition A.5.5 (Injectivité/surjectivité (cf. I.5.4)) *Un morphisme de*

$$A\text{-modules } (\text{resp. de } A\text{-algèbres }) \, f \,:\, X \,\to\, Y$$

est injectif (resp. surjectif) si et seulement si

$$\mathrm{Ker}\, f \,=\, \{0\} \,(\text{resp. } .\mathrm{Im}\, f \,=\, Y\,.)$$

Définition A.5.6 Si

$$i : N \to M \text{ est un morphisme de modules injectif, il induit un isomorphisme } N \cong \operatorname{Im} i ;$$

si bien que N est isomorphe à un sous-module de M. On dira parfois même par abus de langage que N (ou même (N, i) pour plus de précision) est lui-même un sous-module de M.

A.6 . $-\mathbb{Z}$-modules, $\mathbb{K}[X]$-modules

Dans le cadre de ce cours les exemples fondamentaux de A-modules sont constitués par les $\mathbb{Z}$-modules, qui sont exactement les groupes abéliens et par les $\mathbb{K}[X]$-modules. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ étant principaux on disposera, pour ces objets (et leurs morphismes) des théorèmes notamment exposés dans l'appendice B et qui peuvent se particulariser pour les groupes abéliens (resp. $\mathbb{K}[X]$-modules,) comme aux chapitres II et IV.

Exemple A.6.1 (Le cas des groupes abéliens) i) Tout groupe abélien $(G, +_G)$ est canoniquement un $\mathbb{Z}$-module, *i.e.* il existe une unique structure de $\mathbb{Z}$-module $\cdot_G$ sur $(G, +_G)$.

Preuve : (cf. I.6.6.)

ii) Étant donnés deux groupes abéliens G et H, une application $f : G \to H$ est un morphisme de groupes si et seulement si f est un morphisme de $\mathbb{Z}$-modules.

Preuve : (cf. I.6.10 ;)

iii) Si G est un groupe abélien une partie H de G est un sous-groupe si et seulement si c'est un sous-$\mathbb{Z}$-module.

Preuve : (cf. A.3.10.i) ;)

iv) Étant donnés des groupes abéliens G, K, et H et des applications

$$i : K \to H \text{ et } p : G \to H,$$

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

est une suite exacte courte au sens de la définition I.9.1 si et seulement si

$$0 \to K \xrightarrow{i} G \xrightarrow{p} H \to 0$$

est une suite exacte courte au sens des $\mathbb{Z}$-modules.

Exemple A.6.2 (Le cas des $\mathbb{K}[X]$-modules) Voir le paragraphe IV.1.

A.7 . −Torsion, annulateurs (cf. II.5, IV.2)

Dans ce paragraphe (A.7,) A est un anneau intègre et M un a-module.

Lemme A.7.1 ((cf. II.5.1, IV.2.1)) *Pour tout*

$$x \in M \text{ et } a \in A,$$

il est équivalent que $a \cdot x = 0$ *ou que le morphisme de* A*-modules*

$$A \to M\ ,\ b \mapsto b \cdot x \qquad \text{A.7.1.1}$$

se factorise en un morphisme

$$\begin{array}{ccc} A & & \\ \downarrow & \searrow_{b \mapsto b \cdot x} & \\ A/a & \to & M\ . \end{array} \qquad \text{A.7.1.2}$$

Définition A.7.2 ((cf. II.5.2, IV.2.2)) i) (**Élément de torsion**)

Si x et a vérifient les conditions équivalentes du lemme A.7.1 ci-dessus, on dit que x est de a*-torsion*.

On dit que $x \in M$ est *de torsion* s'il existe $a \in A\ a \neq 0$, tel que x soit de a-torsion, *i.e.* tel que $a \cdot x = 0$.

ii) Pour $T \subset A$, la *partie de* T*-torsion* de M notée $M[T]$ est le sous-ensemble de M défini par

$$M[T] := \{x \in M\ ;\ \forall a \in T,\ ax = 0\}\ ;$$

M est *de* T*-torsion* si $M = M[T]$.

Pour $a \in A$, on parlera simplement de la *partie de* a*-torsion* qu'on notera $M[a]$ au lieu de $M[\{a\}]$ de M pour la partie de $\{a\}$-torsion et on dira simplement que M est *de* a*-torsion* pour $\{a\}$-torsion.

iii) (**Idéal annulateur**)

Pour tout $x \in M$, on appelle *idéal annulateur* de x et on note

$$\mathrm{Ann}_A(x) := \{a \in A\ ;\ ax = 0\}$$

le noyau du morphisme A.7.1.1.

iv) Plus généralement pour toute partie $P \subset M$, (pas nécessairement un sous-module,) on appelle *idéal annulateur* de P et on note

$$\mathrm{Ann}_A(P) := \{a \in A\ ;\ \forall x \in P,\ ax = 0\} = \bigcap_{x \in P} \mathrm{Ann}_A(x)\ .$$

Avec cette définition

$$\mathrm{Ann}_A(x) = \mathrm{Ann}_A(\{x\})\ .$$

$\mathrm{Ann}_A(M)$ est appelé *idéal annulateur* de M.

v) (**Partie de torsion**)

On note

$$\mathrm{Tor}_A(M) := \{x \in M\ ;\ \mathrm{Ann}_A(x) \neq \{0\}\} = \bigcup_{a \in A \setminus \{0\}} M[a]$$

i.e. l'ensemble des éléments de torsion de M qu'on appelle la *partie de torsion de* M.

vi) (**Module de torsion**)
On dit que M est *de torsion* si

$$M \ = \ \mathrm{Tor}_A(M) \ .$$

vii) (**Module sans torsion**)
On dit que M est *sans torsion* si

$$\mathrm{Tor}_A(M) \ = \ \{0\} \ .$$

Proposition A.7.3 (Idéaux annulateurs (cf. II.5.3, IV.2.3)) *0) Pour tout $x \in M$, $\mathrm{Ann}_A(x)$ est un idéal de A. Pour toute partie $P \subset M$, $\mathrm{Ann}_A(P)$ étant une intersection d'idéaux, c'est encore un idéal. C'est pourquoi on rencontrera le terme d'idéal annulateur aussi bien pour un élément x, une partie P ou M lui-même.*

i)

$$\mathrm{Ann}_A(M) \ = \ \bigcap_{x \ \in \ M} \mathrm{Ann}_A(x)$$

est un idéal et an particulier

$$\forall x \in M, \ \mathrm{Ann}_A(M) \ \subset \ \mathrm{Ann}_A(x) \ .$$

ii) Pour un A-module M, $\mathrm{Ann}_A(M)$ est le noyau du morphisme

$$A \ \to \ \mathrm{End}_{\mathbf{Gr}}(M) \ \textit{(cf. A.1.4 ,)}$$

définissant la structure de A-module de M.

iii) Pour des parties $P \subset N \subset M$ de M,

$$\mathrm{Ann}_A(N) \ \subset \ \mathrm{Ann}_A(P) \ .$$

iv) Pour tout morphisme de A-modules $f \ : \ M \ \to \ P$ et toutes partie $Q \subset M$ de M,

$$\mathrm{Ann}_A(Q) \ \subset \ \mathrm{Ann}_A(f(Q))$$

avec égalité si f est injectif.

v) Tout A-module M est un $A/\mathrm{Ann}_A(M)$-module.

vi) Pour toute partie $P \subset M$, si $< P >$ est le sous-A-module de M engendré par P,

$$\mathrm{Ann}_A(< P >) \ = \ \mathrm{Ann}_A(P)$$

et la structure de A-module sur $< P >$ se factorise à travers $A/\mathrm{Ann}_A(P)$. En particulier,

$$\forall x \in M, \ \mathrm{Ann}_A(x) \ = \ \mathrm{Ann}_A(Ax) \ .$$

vii) Pour toutes parties $P \subset M$ *et* $N \subset M$,

$$\mathrm{Ann}_A(P \cup N) = \mathrm{Ann}_A(P) \cap \mathrm{Ann}_A(N) \text{ et } \mathrm{Ann}_A(P) + \mathrm{Ann}_A(N) \subset \mathrm{Ann}_A(P \cap N) .$$

En particulier si

$$N \subset M \text{ et } P \subset M$$

sont des sous-A*-modules de* M,

$$\mathrm{Ann}_A(N + P) = \mathrm{Ann}_A(N) \cap \mathrm{Ann}_A(P) .$$

Plus généralment, pour tout ensemble $\mathcal{N}$ *de sous-modules de* M,

$$\mathrm{Ann}_A(\sum_{N \in \mathcal{N}} N) = \bigcap_{N \in \mathcal{N}} \mathrm{Ann}_A(N) .$$

Proposition A.7.4 (Propriétés de la torsion (cf. II.5.4, IV.2.4)) *i) Pour tout* $T \subset A$, $M[T]$ *est un sous-*A*-module de* M.

ii) Pour toutes parties $T \subset U \subset A$,

$$M[U] \subset M[T] .$$

iii) Pour tous $T \subset A$ *et* $U \subset A$,

$$M[T \cup U] = M[T] \cap TrspMU = (M[U])[T] \text{ et } M[T] + M[U] \subset M[T \cap U] .$$

iv) Pour tout $T \subset A$, *si* (T) *désigne l'idéal engendré par* T,

$$M[T] = M[(T)]$$

et la structure de A*-module sur* $M[T]$ *se factorise en une structure de* $A/(T)$*-module.*

v) Pour tout idéal $\mathfrak{I} \subset A$, *l'application qui à tout morphisme* $f : A \to M$ *associe* $f(1)$ *induit un isomorphisme de* A*-modules*

$$\mathrm{Hom}_A(A/\mathfrak{I}, M) \cong M[\mathfrak{I}] \text{ (cf. A.8.6.question 2), a) .)}$$

vi) Pour tout morphisme de A*-module* $f : M \to P$, *et toute partie* $T \subset A$, *la restriction de* f *à* $M[T]$ *est à valeurs dans* $P[T]$ *et définit un morphisme de* A*-modules (et même un morphisme de* $A/(T)$*-modules)*

$$f[T] := f_{|M[T]} : M[T] \to P[T] .$$

En particulier, si f *est un isomorphisme*

$$f[T] : M[T] \cong P[T]$$

est un isomorphisme.

vii) Pour toute partie $T \subset A$ *de* A,

$$T \subset \mathrm{Ann}_A(M[T])$$

ce qui entraîne encore, puisque l'annulateur de M *est un idéal, que*

$$(T) \subset \mathrm{Ann}_A(M[T]) .$$

viii) Pour toute partie $P \subset M$,

$$P \subset M[\mathrm{Ann}_A(P)]$$

ce qui entraîne encore, puisque $M[\mathrm{Ann}_A(P)]$ *est un sous-*A*-module de* M,

$$< P > \subset M[\mathrm{Ann}_A(P)] .$$

ix) Si $\mathfrak{I}$ *et* $\mathfrak{J}$ *sont comaximaux, on a un isomorphisme naturel*

$$M[\mathfrak{I} \cap \mathfrak{J}] \cong M[\mathfrak{I}] \oplus M[\mathfrak{J}] .$$

Preuve *: (cf. A.8.6.question 1).)*

x) Si de plus, $\mathrm{Ann}_A(M) = \mathfrak{I} \cap \mathfrak{J}$

$$\mathfrak{I} = \mathrm{Ann}_A(M[\mathfrak{I}]) \text{ et } \mathfrak{J} = \mathrm{Ann}_A(M[\mathfrak{J}]) .$$

Preuve *: (cf. B.7.1.)*

Proposition A.7.5 (Propriétés de la partie de torsion cf. II.5.5) *i)* $\mathrm{Tor}_A(M)$ *est un sous-*A*-module de* M.

Preuve *: Ici on a besoin de l'hypothèse* A *intègre : Comme on a toujours*

$$0 \in \mathrm{Tor}_A(M), \mathrm{Tor}_A(M) \neq \emptyset .$$

Pour tout $(x, y) \in \mathrm{Tor}_A(m) \times \mathrm{Tor}_A(M)$, *et tout* $(a, b) \in A \times A$, *il existe* $(c, d) \in (A \setminus \{0\}) \times (A \setminus \{0\})$, *tel que*

$$c \cdot x = d \cdot y = 0 .$$

Il s'ensuit que

$$cd(ax + by) = adcx + bcdy = 0$$

c'est-à-dire que $cd \in \mathrm{Ann}_A(ax + by)$. *Or* A *étant intègre*

$$cd \neq 0,$$

ce qui entraîne que

$$\mathrm{Ann}_A(ax + by) \neq \{0\}$$

si bien que

$$ax + by \in \mathrm{Tor}_A(M) .$$

ii) Le quotient $M/\mathrm{Tor}_A(M)$ est sans torsion.

***Preuve** : Notons $p : M \to Q := M/\mathrm{Tor}_A(M)$ la surjection canonique. Pour tout $(a, y) \in A \times Q$, il existe $x \in M$ tel que $y = p(x)$. Ainsi $ay = 0$, si et seulement si*

$$p(ax) = ap(x) = 0$$

si et seulement si

$$ax \in \mathrm{Ker}\, p = \mathrm{Tor}_A(M) .$$

Il existe donc $b \in A \setminus \{0\}$, tel que $abx = 0$.

Si $a \neq 0, ab \neq 0$ (A est intègre,) si bien que

$$x \in \mathrm{Tor}_A(M) = \mathrm{Ker}\, p$$

ce qui entraîne

$$y = p(x) = 0 .$$

Il s'ensuit que Q est sans torsion.

iii) Pour $f : M \to P$ un morphisme de A-modules, la restriction de f à $\mathrm{Tor}_A(M)$ est à valeurs dans $\mathrm{Tor}_A(P)$ si bien que f se restreint en un morphisme de A-modules

$$\mathrm{Tor}_A(f) := f_{|\mathrm{Tor}_A(M)} : \mathrm{Tor}_A(M) \to \mathrm{Tor}_A(P) .$$

En particulier si f est un isomorphisme,

$$\mathrm{Tor}_A(f) : \mathrm{Tor}_A(M) \cong \mathrm{Tor}_A(P)$$

est un isomorphisme.

iv) Si $\mathrm{Ann}_A(M) \neq \{0\}$, M est de torsion.

***Preuve** : En effet, d'après A.7.4.viii) $M \subset M[\mathrm{Ann}_A(M)]$. Par ailleurs $M[\mathrm{Ann}_A(M)] \subset \mathrm{Tor}_A(M)$. Comme par définition, $\mathrm{Tor}_A(M) \subset M$,*

$$M = \mathrm{Tor}_A(M) .$$

Proposition A.7.6 ((cf. II.5.7, IV.2.5)) *Si M est de type fini, M est de torsion si et seulement si*

$$M = M[\mathrm{Ann}_A(M)] = \mathrm{Tor}_A(M)$$

si et seulement si $\mathrm{Ann}_A(M) \neq \{0\}$.

***Preuve** : La première équivalence est immédiate et le sens réciproque de la seconde vrai sans hypothèse sur M et établi en A.7.5.iv).*

Supposons donc $M = < S >$ de type fini où $S \subset M$ est un ensemble fini. Or il découle de A.7.3.iii), que

$$\mathrm{Ann}_A(M) = \mathrm{Ann}_A(S) = \bigcap_{s \in S} \mathrm{Ann}_A(s) .$$

De plus pour tout $s \in S$, $s \in M = \mathrm{Tor}_A(M)$ si bien que $\mathrm{Ann}_A(s) \neq \{0\}$. Il existe donc

$$a_s \in \mathrm{Ann}_A(s) , \ a_s \neq 0 .$$

Puisque A est intègre,

$$a := \prod_{s \in S} a_s \neq 0 \text{ et } a \in \bigcap_{s \in S} \mathrm{Ann}_A(s) = \mathrm{Ann}_A(M) .$$

A.8 . –Exercices

Exercice A.8.1 Dans le contexte de l'exemple A.3.2.d), tout sous-A-module de B est-il nécessairement une sous-A-algèbre de B ?

Exercice A.8.2 Compléter la preuve de la proposition A.3.6.

Exercice A.8.3 Soient A un anneau comutatif, M un A-module et $\left(M_n\right)_{,n\in\mathbb{N}}$ une suite de sous-modules de M ayant la propriété suivante : Pour tout $(p,q) \in \mathbb{N}\times\mathbb{N}$, il existe $r \in \mathbb{N}$ tel que

$$M_p \subset M_r \text{ et } M_q \subset M_r .$$

Montrer qu'alors

$$\bigcup_{M\in\mathbb{N}} n$$

est un sous-A-module de M.

Exercice A.8.4 Soit S une partie finie de $A[X]$ et $< S >$ le sous-A-module de $A[X]$ engendré par S. Montrer qu'il existe un entier $n \in \mathbb{N}$, tel que, pour tout $P \in < S >$, $\deg(P) \leq n$. En déduire que $A[X]$ n'est pas un A-module de type fini.

Exercice A.8.5 [Homomorphismes]

1) Étant donné un morphisme de A-modules $f : M \to N$, et P un A-module vérifier que

$$f^* : \mathrm{Hom}_A(N,P) \to \mathrm{Hom}_A(M,P)\ ,\ u \mapsto u\circ f$$

est un morphisme de A-modules.

2) Étant donnée une suite exacte de A-modules

$$0 \to N \xrightarrow{\ i\ } M \xrightarrow{\ p\ } Q \to 0,$$

pour tout A-module P, on définit

$$\begin{array}{rrcl} p^* : & \mathrm{Hom}_A(Q,P) & \longrightarrow & \mathrm{Hom}_A(M,P) \\ & u & \longmapsto & u\circ p \\ \text{et } i^* : & \mathrm{Hom}_A(M,P) & \longrightarrow & \mathrm{Hom}_A(N,P) \\ & v & \longmapsto & u\circ i \end{array}$$

comme ci-dessus. Montrer qu'alors la suite

$$0 \to \mathrm{Hom}_A(Q,P) \xrightarrow{\ p^*\ } \mathrm{Hom}_A(M,P) \xrightarrow{\ i^*\ } \mathrm{Hom}_A(N,P)$$

est une suite exacte de A-modules. Donner une condition suffisante pour que

$$0 \to \mathrm{Hom}_A(Q,P) \xrightarrow{\ p^*\ } \mathrm{Hom}_A(M,P) \xrightarrow{\ i^*\ } \mathrm{Hom}_A(N,P) \to 0$$

soit une suite exacte courte.

3) Soient M, N, P des A-modules.

a) En notant

$$p \,:\, M \times N \,\to\, M \,,\, (x,y) \,\mapsto\, x \text{ et } q \,:\, M \times N \,\to\, N \,,\, (x,y) \,\mapsto\, y$$

les projections montrer que

$$\mathrm{Hom}_A(P, M \times N) \,\to\, \mathrm{Hom}_A(P,M) \times \mathrm{Hom}_A(P,N) \,,\, f \,\mapsto\, (p \circ f, q \circ f)$$

est un isomorphisme de A-modules.

b) En notant

$$i \,:\, M \,\to\, M \times N \,,\, x \,\mapsto\, (x,0) \text{ et } j \,:\, N \,\to\, M \times N \,,\, x \,\mapsto\, (0,x)$$

montrer que

$$\mathrm{Hom}_A(M \times N, P) \,\to\, \mathrm{Hom}_A(M,P) \times \mathrm{Hom}_A(N,P) \,,\, f \,\mapsto\, (f \circ i, f \circ j)$$

est un isomorphisme de A-modules.

Exercice A.8.6 [Torsion]
Soit A un anneau commutatif et M un A-module. Pour tout $T \subset A$, on rappelle que

$$M[T] \,=\, \{x \,\in\, M \,;\, \forall a \in T,\, ax \,=\, 0\} \,.$$

1) Étant donnés deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A, montrer que $\mathfrak{I} + \mathfrak{J} \,=\, A$ entraîne

$$M[\mathfrak{I} \cap \mathfrak{J}] \,=\, M[\mathfrak{I}] \,\oplus\, M[\mathfrak{J}] \,.$$

2) **a)** Soit $\mathfrak{I} \subset A$ un idéal et M un A-module. Montrer que l'application

$$\mathrm{Hom}_A(A, M) \,\to\, M \,,\, f \,\mapsto\, f(1)$$

induit un isomorphisme

$$\mathrm{Hom}_A(A/\mathfrak{I}, M) \,\cong\, M[\mathfrak{I}] \,.$$

b) Réinterpréter le résultat ci-dessus dans le cas des groupes abéliens *i.e.* $A \,=\, \mathbb{Z}$.

c) Peut-on redémontrer question 1) en utilisant la a) et l'A.8.5 ?

Exercice A.8.7 [Le « lemme du serpent »] Dans cet exercice les ensembles considérés sont des groupes abéliens ou des $\mathbb{K}$-espaces vectoriels ($\mathbb{K}$ étant un corps) ou même des A-modules. Les morphismes sont des morphismes pour la structure considérée. La notation

$$0 \to N \xrightarrow{i} M \xrightarrow{p} Q \to 0$$

que l'on appellera *suite exacte*signifie que :
— $i : N \to M$ est injectif ;
— $p : M \to Q$ est surjectif ;
— $\operatorname{Ker} p = \operatorname{Im} i$.
Dire que le carré :

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\ P & \xrightarrow{g} & Q \end{array}$$

est *commutatif* signifiera que $g \circ u = v \circ f$.

1) Vérifier que dans la situation d'une suite exacte

$$0 \to N \xrightarrow{i} M \xrightarrow{p} Q \to 0$$

on a un isomorphisme naturel $M/\operatorname{Im} i \cong Q$ qu'on abrègera généralement en $Q = M/N$ en identifiant N à l'image de i.

Soit le diagramme

$$(*) : \quad \begin{array}{ccccccccc} 0 \to & N_1 & \xrightarrow{i_1} & M_1 & \xrightarrow{p_1} & Q_1 & \to 0 \\ & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & \\ 0 \to & N_2 & \xrightarrow{i_2} & M_2 & \xrightarrow{p_2} & Q_2 & \to 0 \end{array}$$

où tous les carrés sont commutatifs.

Notons

$$I := \operatorname{Ker} f \,,\ J := \operatorname{Ker} g \text{ et } K := \operatorname{Ker} h \,.$$

2) Montrer qu'il existe des morphismes

$$u : I \to J \text{ et } v : J \to K \text{ tels que } k \circ v = p_1 \circ j \text{ et } j \circ u = i_1 \circ i \,.$$

le diagramme $(*)$ **se complète en un diagramme :**

$$(**) : \quad \begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 \to & I & \xrightarrow{u} & J & \xrightarrow{v} & K & & & \\ & {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle k} & & & \\ 0 \to & N_1 & \xrightarrow{i_1} & M_1 & \xrightarrow{p_1} & Q_1 & \to 0 & & \\ & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & & \\ 0 \to & N_2 & \xrightarrow{i_2} & M_2 & \xrightarrow{p_2} & Q_2 & \to 0 & & \end{array}$$

où tous les carrés sont commutatifs.

On note

$$c : N_2 \to C := N_2/\operatorname{Im} f \,,\ d : M_2 \to D := M_2/\operatorname{Im} g \text{ et } e : Q_2 \to E := Q_2/\operatorname{Im} h$$

les surjections canoniques.

3) Montrer qu'il existe des morphismes

$$w \,:\, C \,\to\, D \text{ et } x \,:\, D \,\to\, E \text{ tels que } w \circ c \,=\, d \circ i_2 \text{ et } x \circ d \,=\, e \circ p_2 \,.$$

le diagramme $(**)$ se complète en un diagramme :

$$(***)\ :\quad \begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 \to & I & \xrightarrow{u} & J & \xrightarrow{v} & K & & & \\
 & {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle k} & & & \\
0 \to & N_1 & \xrightarrow{i_1} & M_1 & \xrightarrow{p_1} & Q_1 & \to 0 & & \\
 & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & & \\
0 \to & N_2 & \xrightarrow{i_2} & M_2 & \xrightarrow{p_2} & Q_2 & \to 0 & & \\
 & {\scriptstyle c}\downarrow & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle e} & & & \\
 & C & \xrightarrow{w} & D & \xrightarrow{x} & E & \to 0 & & \\
 & \downarrow & & \downarrow & & \downarrow & & & \\
 & 0 & & 0 & & 0 & & &
\end{array}$$

où tous les carrés sont commutatifs.

4) Montrer qu'il existe un morphisme $\delta \,:\, K \,\to\, C$ tel que

$$\operatorname{Ker}\delta \,=\, \operatorname{Im} v \text{ et } \operatorname{Im}\delta \,=\, \operatorname{Ker} w \,.$$

B . −Modules de type fini sur un anneau principal

B.0 . −Introduction

Dans ce paragraphe (B) A est encore un anneau principal.

Notation B.0.1 Dans la suite, A étant un anneau principal, pour tout élément $a \in A$, on notera A/a l'anneau quotient A/Aa de A par l'idéal principal Aa. On notera $\pi_a : A \to A/a$ la surjection canonique.

Rappel B.0.2 (Éléments associés) On rappelle (cf. I.11.2,) que deux éléments a et b d'un anneau intègre A sont *associés* si

$$a|b \text{ et } b|a$$

si et seulement si ils engendrent le même idéal ***i.e.***

$$Aa = Ab,$$

si et seulement si

$$\exists (u,v) \in A^\times \times A^\times,\ a = bu \text{ et } b = av\ .$$

La relation d'association est une relation d'équivalences dont les classes correspondent bijectivement aux idéaux principaux de A et donc aux idéaux de A si A est principal.

On sait que les **Ppcm** et **Pgcd** en particulier sont définis comme des classes d'association.

Notation B.0.3 (Éléments irréductibles) On note $\mathbb{P}_A$ (ou simplement $\mathbb{P}$) un ensemble d'éléments irréductibles de A tel que $\mathbb{P}_A$ contienne un et un seul représentant de chaque classe d'association.

— Dans le cas où A est l'anneau $\mathbb{Z}$ des entiers relatifs il est usuel de prendre pour $\mathbb{P}_\mathbb{Z}$ l'ensemble des nombres premiers.

— Dans le cas où A est l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans un corps $\mathbb{K}$, il est usuel de prendre pour $\mathbb{P}_\mathbb{K}[X]$ l'ensemble des polynômes irréductibles unitaires.

Notation B.0.4 (Valuations p-adiques) Pour tout irréductible

$$p \in \mathbb{P} \text{ et tout } a \in A, \text{ on note } v_p(a)$$

sa valuation p-adique (cf. I.13.5.5.) On note encore

$$\mathcal{S}(a) := \{p \in \mathbb{P}\ ;\ v_p(a) \neq 0\}$$

dont on rapelle que c'est un ensemble fini.

On remarque que :

i) Pour deux irréductibles p et q associés, et tout $a \in A$, $v_p(a) = v_q(a)$; autrement dit, la valuation p-adique ne dépend pas du choix d'un représentant de la classe d'association de l'élément irréductible p. Ainsi en notant $\mathfrak{p}$ l'idéal engendré par n'importe quelle élément de cette classe on pourrait noter $v_\mathfrak{p}$ en lieu et place de v_p.

ii) Un élément $u \in A$, est inversible si et seulement si

$$\forall p \in \mathbb{P},\ v_p(u) = 0\ .$$

iii) Plus généralement deux éléments a et b sont associés si et seulement si

$$\forall p \in \mathbb{P},\ v_p(a) \ = \ v_p(b)\ .$$

Dans un anneau principal un idéal $\mathfrak{I}$ correspondant à une classe d'association d'élément de A, on peut tout à fait noter $v_p(\mathfrak{I})$ et parler de la valuation p-adique d'un idéal comme celle de n'importe laquelle de ses bases. On pourait montrer qu'il s'agit en fait de la plus grande puissance de l'idéal $\mathfrak{p}$ contenant $\mathfrak{I}$.

Notation B.0.5 (Décomposition en produit d'irréductibles) Pour tout $a \in A \setminus \{0\}$, on a

$$a \ = \ u \prod_{p \in \mathbb{P}} p^{v_p(a)} \ = \ \prod_{p \in \mathcal{S}(a)} p^{v_p(a)}\ ,\ u \in A^\times \text{ (cf. I.13.5.3 ;)}$$

le produit ci-dessus étant en fait fini puisque $v_p(a) \neq 0$ pour un nombre fini de $p \in \mathbb{P}$ seulement.

Notation B.0.6 (Corps résiduel) Soit p un élément irréductible de A, ce qui signifie, dans le cas où $A = \mathbb{Z}$, un nombre premier p. On note $\kappa_p := A/p$ (ou simplement κ s'il n'y a pas d'ambiguïté sur l'élément p,) qui est un corps (cf. I.13.3.1,) et même le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ dans le cas où $A = \mathbb{Z}$.

Il est d'usage d'appeler κ_p le *corps résiduel en* p.

B.1 . −Modules de type fini sur un anneau principal (cf. II.6)

Proposition B.1.1 ((cf. II.6.1)) *Si A est un anneau intègre, un A-module libre est sans torsion.*

Preuve *: Même preuve que pour II.6.1.*

Dans le théorème qui suit (B.1.2,) l'hypothèse A principal est absolument indispensable puisque la preuve fait apparaître que c'est un corollaire du théorème II.4.6 pour lequel on n'a constaté ne pas pouvoir se passer de l'hypothèse A principal.

Théorème B.1.2 ((cf. II.6.2)) *Si A est un anneau principal et M un A-module de type fini (cf. II.1.5,) M est libre (cf. II.2.8,) si et seulement s'il est sans torsion (cf. A.7.2.vii).)*

Preuve *: On peut sans presqu'aucune modification adapter la preuve du théorème II.6.2 en remplaçant les coefficients dans $\mathbb{Z}$ par des coefficients dans l'anneau A. On remarquera que l'utilisation, à la fin de la preuve, du théorème II.4.6, est déterminante et requiert l'hypothèse que A soit principal.*

Proposition B.1.3 ((cf. II.6.3)) *Soient A un anneau principal et M un A-module de type fini, $\mathrm{Tor}_A(M)$ son sous-module (cf. A.7.5.i),) de torsion et $p\ :\ M \to L := M/\mathrm{Tor}_A(M)$ la surjection canonique. Alors :*

i) $\mathrm{Tor}_A(M)$ *est un A-module de type fini.*

Preuve *: (cf. II.4.8.i).)*

ii) L est un A-module libre de type fini.

Preuve *: La preuve est, mutatis mutandis la même que celle de II.6.3.ii).*

iii) La suite exacte de A-module

$$0 \to \mathrm{Tor}_A(M) \longrightarrow M \xrightarrow{p} L \to 0$$

est scindée d'où il résulte qu'il existe un isomorphisme

$$M \cong \mathrm{Tor}_A(M) \oplus L\,.$$

***Preuve** : La preuve est, mutatis mutandis la même que celle de II.6.3.iii).*

Théorème B.1.4 (Structure des A-module de type fini sur un anneau principal (cf. II.6.4)) *Soit A un anneau principal. Étant donné un A-module M de type fini,*

i) Il existe un A-module de type fini et de torsion T et un A-module libre de type fini L tels que

$$M \cong T \times L\,.$$

***Preuve** : (cf. B.1.3.iii).)*

ii) Le couple (T, L) est unique au sens où T est isomorphe au sous module de torsion $\mathrm{Tor}_A(M)$ de M et s'il existe L_1 et L_2 tels que

$$M \cong T \times L_1 \cong T \times L_2$$

L_1 et L_2 sont isomorphe et ont donc en particulier même rang.

***Preuve** : Il suffit d'adapter la preuve de II.6.4.ii).*

Proposition B.1.5 *Soit M un A-module de type fini. Toute suite $\left(M_n\right)_{,n\in\mathbb{N}}$ croissante de sous-modules de M est stationnaire à partir d'un certain rang ; c'est-à-dire qu'il existe $p \in \mathbb{N}$ tel que pour tout $q \geq p, M_q = M_p$.*

***Preuve** : Étant donnée une suite $\left(M_n\right)_{,n\in\mathbb{N}}$ croissante de sous-A-modules de M, la proposition A.3.9.iv) assure que*

$$\tilde{M} := \bigcup_{n \in \mathbb{N}} M_n$$

est un sous-A-module de M. Or, d'après le corollaire II.4.8.i),$\tilde{M}$ est de type fini. Il existe donc une partie $m_{i\,,1\leq i\leq r} \in \tilde{M}$ génératrice de $\tilde{M}$. Pour tout $1 \leq i \leq r$ il existe donc $n_i \in \mathbb{N}$ tel que $m_i \in M_{n_i}$. Notons $s := \max_{1 \leq i \leq r}(n_i)$. Puisque la suite $\left(M_n\right)_{,n\in\mathbb{N}}$ est croissante,

$$\forall 1 \leq i \leq r,\ M_{n_i} \subset M_s$$

si bien que

$$\forall 1 \leq i \leq r,\ m_i \in M_s\,.$$

Il s'ensuit que $\tilde{M} \subset M_s$. On a donc, pour tout $t \geq s$,

$$\tilde{m} \subset M_s \subset M_t \subset \tilde{M}$$

ce qui prouve le résultat.

Remarque B.1.6 On dit usuellement d'un module qui possède la propriété démontrée ci-dessus pour les A-modules de type fini sur un anneau principal, qu'il est *noethérien*. Cette propriété est vraie pour des classes d'anneaux plus générales mais ce sont des résultats dont nous n'aurons pas besoin dans ce cours.

On peut remarquer que le résultat, établi pour un A-module de type fini quelconque, dans la proposition B.1.5, l'a déjà été pour l'anneau A lui-même (vu comme A-module) (cf. I.13.5.2.) On dit, dans ce cas, que l'anneau A est *noethérien*. Il y a bien d'autres aneaux noethériens que les anneaux principaux et leur étude est tout à fait pertinente, mais également tout à fait au-delà du cadre de ce cours.

B.2 . −Décomposition p-primaire (cf. II.8, IV.3)

Notation B.2.1 (cf. II.8.1) Étant donné un A-module M et $p \in \mathbb{P}$, on note :

i)
$$\mathbf{p} : M \to M , x \mapsto px$$
la *multiplication par* p qui est un endomorphisme du A-module M ;

ii)
$$\forall n \in \mathbb{N},\ M[p^n] := M[\{p^n\}] = M[Ap^n]$$
qu'on pourra appeler la partie de p^n-torsion de M (cf. A.7.2.ii) ;)

On constate immédiatement que
$$M[p] = \operatorname{Ker} \mathbf{p}$$
et plus généralement, pour tout $n \in \mathbb{N}$,
$$M[p^n] = \operatorname{Ker} \mathbf{p}^n$$
où $\mathbf{p}^n$ est la composée de n applications égales à $\mathbf{p}$.

Définition B.2.2 (Composante p-primaire (cf. II.8.2, IV.3.1)) Pour M un A-module et tout $p \in \mathbb{P}$, on appelle *composante p-primaire* de M le sous-module de M
$$M[p^\infty] := \bigcup_{n \in \mathbb{N}} M[p^n] .$$

Théorème B.2.3 (de décomposition p-primaire (cf. II.8.3, IV.3.2)) *Soit M un A-module de type fini et de torsion. On note $\operatorname{Ann}_A(M)$ son idéal annulateur (cf. A.7.2.iv).) On sait (cf. A.7.6,) que $\operatorname{Ann}_A(M) \neq 0$ et pour tout $p \in \mathbb{P}$, on note $v_p(\operatorname{Ann}_A(M))$ sa valuation p-adique (cf. B.0.4.) Alors :*

i)
$$\forall p \in \mathbb{P},\ M[p^\infty] = M[p^{v_p(\operatorname{Ann}_A(M))}] ;$$

ii)
$$M = \coprod_{p \in \mathbb{P}} M[p^{v_p(\operatorname{Ann}_A(M))}] ;$$

iii)
$$\forall p \in \mathbb{P},\ \operatorname{Ann}_A(v_p(\operatorname{Ann}_A(M))[p^\cdot] = Ap^{v_p(\operatorname{Ann}_A(M))} .$$

Preuve : *Soit ω_M un générateur de l'idéal $\mathrm{Ann}_A(M)$. Alors*

$$\forall p \in \mathbb{P},\ v_p(\mathrm{Ann}_A(M)) \ = \ v_p(\omega_M)\ .$$

De plus l'ensemble

$$\mathcal{S}(\mathrm{Ann}_A(M)) \ := \ \mathcal{S}(\omega_M) \ = \ \{p \ \in \ \mathbb{P}\,;\ v_p(\omega_M) \ \neq \ 0\}$$

est fini et l'on a :

$$\begin{array}{rcl} \omega_M & = & u \displaystyle\prod_{p \ \in \ \mathcal{S}(\mathrm{Ann}_A(M))} p^{v_p(\omega_M)} \\ \mathrm{Ann}_A(M) & = & \displaystyle\bigcap_{p \ \in \ \mathcal{S}(\mathrm{Ann}_A(M))} Ap^{v_p(\omega_M)}\ . \end{array} \qquad \textit{B.2.3.1}$$

On peut donc raisonner par récurrence sur le nombre d'éléments de $\mathcal{S}(\mathrm{Ann}_A(M))$.
$\#(\mathcal{S}(\mathrm{Ann}_A(M))) \ = \ 1$ Dans ce cas il existe $p \ \in \ \mathbb{P}$ et $k \ \in \ \mathbb{N}^*$ tels que $\omega_M \ = \ p^k$. Comme on a toujours

$$M \ \subset \ M[\mathrm{Ann}_A(M)] \textit{ (cf. A.7.4.viii) ,)}$$

et que, par définition $M[\mathrm{Ann}_A(M)] \ \subset \ M$, on a :

$$M \ = \ M[\mathrm{Ann}_A(M)] \ = \ M[p^k] \ = \ M[p^{v_p(\mathrm{Ann}_A(M))}]$$

ce qui prouve ii) dans ce cas. Le point iii) est alors tautologique ou presque.
$\#(\mathcal{S}(\mathrm{Ann}_A(M))) \ > \ 1$ Soient

$$p \ \in \ \mathcal{S}(\mathrm{Ann}_A(M)) \text{ et } \omega_{(p)} \ := \ \frac{\omega_M}{p^{v_p(\omega_M)}} \ = \ \prod_{q \ \in \ \mathcal{S}(\mathrm{Ann}_A(M))\setminus\{p\}} q^{v_q(\omega_M)}\ .$$

Comme on a toujours $M \ = \ M[\mathrm{Ann}_A(M)]$, que p et $\omega_{(p)}$ sont premiers entre eux, (i.e. les idéaux $A\omega_{(p)}$ et $Ap^{v_p(\mathrm{Ann}_A(M))}$ sont comaximaux,) on a :

$$M \ = \ M[\mathrm{Ann}_A(M)] \ = \ M[A\omega_{(p)}p^{v_p(\mathrm{Ann}_A(M))}] \ = \ M[A\omega_{(p)} \ \cap \ Ap^{v_p(\mathrm{Ann}_A(M))}]\ .$$

Il résulte alors de la proposition A.7.4.ix) que

$$M \ = \ M[\omega]_{(p)} \ \oplus \ M[p^{v_p(\mathrm{Ann}_A(M))}]$$

et de la proposition A.7.4.x), que

$$\mathrm{Ann}_A(M[\omega]_{(p)}) \ = \ A\omega_{(p)} \text{ et } \mathrm{Ann}_A(M[p^{v_p(\mathrm{Ann}_A(M))}]) \ = \ Ap^{v_p(\mathrm{Ann}_A(M))}$$

ce qui permet d'appliquer l'hypothèse de récurrence à $M[\omega_{(p)}]$ et de conclure.

Remarque B.2.4 i) La some

$$M \ = \ \coprod_{p \ \in \ \mathbb{P}} M[p^{v_p(\mathrm{Ann}_A(M))}]$$

dans l'énoncé du théorème B.2.3 ci-dessus est finie puisque

$$\{p \ \in \ \mathbb{P}\,;\ v_p(\mathrm{Ann}_A(M)) \ \neq \ 0\}$$

est un ensemble fini.

ii) On aurait pu, écrire la preuve du théorème ci-dessus, en remarquant d'abord que

$$M \;=\; M[\mathrm{Ann}_A(M)] \text{ (cf. A.7.6 ;)}$$

qui donne alors, grâce à la proposition A.7.4.v) un isomorphisme

$$M \;\cong\; \mathrm{Hom}_A(A/\mathrm{Ann}_A(M), M)\,.$$

Ce dernier isomorphisme donne encore, en vertu du théorème chinois des restes (cf. I.13.4,) un isomorphisme$\frac{1}{2}$

$$M \;\cong\; \mathrm{Hom}_A(\prod_{p\,\in\,\mathbb{P}} A/p^{v_p(\mathrm{Ann}_A(M))}, M)\,.$$

C'est à ce point de la preuve, que l'on fait appell une première fois à un argument de récurrence, qui pourrait sans cela paraître escamoté.

On peut ensuite utiliser le A.8.5.question 3), b), en remarquant bien qu'on a ici affaire à un produit fini, pour écrire :

$$M \;\cong\; \prod_{p\,\in\,\mathbb{P}} \mathrm{Hom}_A(A/p^{v_p(\mathrm{Ann}_A(M))}, M)\,.$$

On peut alors, à nouveau appliquer la proposition A.7.4.v) pour conclure.

Corollaire B.2.5 (cf. II.8.4) *Pour un module M de type fini et de torsion, pour tout $p \in \mathbb{P}$, il existe $x \in M$, tel que*

$$\mathrm{Ann}_A(x) \;=\; Ap^{v_p(\mathrm{Ann}_A(M))}\,.$$

Preuve *: Si $v_p(\mathrm{Ann}_A(M)) = 0$,*

$$\mathrm{Ann}_A(0) \;=\; A\,.$$

Si $v_p(\mathrm{Ann}_A(M)) \neq 0$, on peut chercher $x \in M[p^{v_p(\mathrm{Ann}_A(M))}]$ grâce à B.2.3.ii) et donc supposer que

$$\mathrm{Ann}_A(M) \;=\; Ap^{v_p(\mathrm{Ann}_A(M))}$$

grâce à B.2.3.iii).

Alors, pour tout $x \in M$, $\mathrm{Ann}_A(M) \subset \mathrm{Ann}_A(x)$, c'est-à-dire qu'il existe

$$\omega(x) \text{ tel que } \mathrm{Ann}_A(x) \;=\; A\cdot\omega(x) \text{ et } \omega(x)|p^{v_p(\mathrm{Ann}_A(M))}$$

c'est-à-dire qu'il existe

$$k(x) \;\leq\; v_p(\mathrm{Ann}_A(M)) \text{ tel que } \mathrm{Ann}_A(x) \;=\; A\cdot p^{k(x)}\,.$$

Or $M = < M >$ c'est-à-dire que

$$M \;=\; \sum_{x\,\in\,M} A\cdot x$$

ce qui entraîne, d'après la proposition A.7.3.vii),

$$\begin{aligned} A\cdot p^{v_p(\mathrm{Ann}_A(M))} &= \mathrm{Ann}_A(M)\\ &= \bigcap_{x\,\in\,M} \mathrm{Ann}_A(A\cdot x)\\ &= \bigcap_{x\,\in\,M} \mathrm{Ann}_A(x)\\ &= A\cdot \mathrm{PPCM}_{x\,\in\,M}(x \in M)\\ &= A\cdot p^{\max_{x\,\in\,M}\left(k(x)\right)} \end{aligned}$$

d'où il d'écoule que $\max_{x \in M}\big(k(x)\big) = v_p(\mathrm{Ann}_A(M))$, *ce qui prouve qu'il existe*

$$x \in M \text{ tel que } \mathrm{Ann}_A(x) = A \cdot p^{v_p(\mathrm{Ann}_A(M))} .$$

Proposition B.2.6 *Si* M *est un* A*-module de type fini et de torsion, pour tout*

$$n \in \mathbb{N}, n \geq v_p(\mathrm{Ann}_A(M)) \Rightarrow M[p^n] = M[p^{v_p(\mathrm{Ann}_A(M))}] .$$

Preuve *:* *Pour* $n \geq v_p(\mathrm{Ann}_A(M))$,

$$M[p^{v_p(\mathrm{Ann}_A(M))}] \subset M[p^n] \subset M \text{ (cf. A.7.4.ii) .)}$$

Il s'ensuit que

$$\mathrm{Ann}_A(M) \subset \mathrm{Ann}_A(M[p^n]) \subset \mathrm{Ann}_A(M[p^{v_p(\mathrm{Ann}_A(M))}]) .$$

Or d'après le théorème B.2.3.iii), $\mathrm{Ann}_A(M[p^{v_p(\mathrm{Ann}_A(M))}]) = Ap^{v_p(\mathrm{Ann}_A(M))}$. *Il en résulte que*

$$\mathrm{Ann}_A(M[p^n]) = Ap^{v_p(\mathrm{Ann}_A(M))},$$

ce qui entraîne

$$M[p^n] \subset M[p^{v_p(\mathrm{Ann}_A(M))}] .$$

Corollaire B.2.7 *Si* M *est de type fini et de torsion*

$$M[p^\infty] = M[p^{v_p(\mathrm{Ann}_A(M))}] \text{ et } M = \coprod_{p \in \mathbb{P}} M[p^\infty] .$$

Preuve *:* *C'est une conséquence de la proposition B.2.6 et du théorème B.2.3.ii).*

B.3 . $-A$-modules cycliques (cf. II.9, IV.4)

Proposition B.3.1 (A**-modules cycliques (cf. II.9.1, IV.4.1))** *Étant donné un* A*-module* C*, les assertions suivantes sont équivalentes :*

a) C *est de type fini engendré par un singleton* $\{x\}$ *avec* x *de torsion (cf. A.7.2.i).)*

b) Il existe un isomorphisme

$$A/\mathrm{Ann}_A(C) \cong C \text{ et } \mathrm{Ann}_A(C) \neq 0 .$$

c) Il existe un idéal $\mathfrak{I} \subset A$ *de* A, $\mathfrak{I} \neq \{0\}$ *et un isomorphisme de* A*-modules*

$$A/\mathfrak{I} \cong C .$$

Preuve *:*

i) ***(a)*** $\Rightarrow$ ***b))***
Si C *est engendré par* $\{C\}$*, par définition le morphisme*

$$f \,:\, A \,\to\, C\,,\; a \,\mapsto\, ax$$

est surjectif. Son noyau est, par définition $\mathrm{Ann}_A(x)$ *ce qui donne un isomorphisme de* A*-modules*

$$A/\mathrm{Ann}_A(x) \,\cong\, C\,.$$

Or $\mathrm{Ann}_A(C) \,=\, \mathrm{Ann}_A(x)$ *en vertu de A.7.3.iii).*

ii) ***(b)*** $\Rightarrow$ ***c))***
Est immédiat.

iii) ***(c)*** $\Rightarrow$ ***a))***
Le A*-module* $A/\mathfrak{I}$ *est engendré par l'image de* 1*, ce qui donne un générateur de* C *par isomorphisme.*

Définition B.3.2 (*A*-Modules cycliques (cf. II.9.2, IV.4.2)) Un A-module vérifiant les assertions équivalentes de la proposition B.3.1 est un *A-module cyclique*.

Remarque B.3.3 On remarque que, dans le cas où

$$A \,=\, \mathbb{Z} \,(\text{resp. } \mathbb{K}[X])$$

est l'anneau des entiers relatifs, (resp. des polynômes à une indéterminée à coefficients dans $\mathbb{K}$,) un A-module cyclique est exactement un groupe cyclique (cf. II.9.2,) (resp. un espace cyclique (cf. IV.4.2.))

Lemme B.3.4 *Un module cyclique* C *est de torsion si et seulement si* $\mathrm{Ann}_A(C) \,\neq\, \{\,\}0$.

Proposition B.3.5 (Sous-module cyclique (cf. II.9.3, IV.4.5)) *Un* a*-module* M *possède un sous-module cyclique isomorphe à* $A/\mathfrak{I}$ *si et seulement si*

$$\exists x \,\in\, M,\; \mathrm{Ann}_A(x) \,=\, \mathfrak{I}\,.$$

Proposition B.3.6 (Théorème chinois des restes (cf. II.9.4, IV.4.6)) *Soit* A *un anneau principal. Étant donné un élément* $d \,\in\, A$

$$A/d \,\cong\, \prod_{p \,\in\, \mathbb{P}} A/p^{v_p(d)}\,.$$

Remarque B.3.6.1 C'est exactement le théorème B.2.3 dans le cas cyclique ; c'est-à-dire le cas où le morphisme $A/(\mathfrak{I} \cap \mathfrak{J}) \,\hookrightarrow\, M$ est injectif et définit donc, grâce au théorème chinois des restes un morphisme injectif $A/\mathfrak{I} \times A/\mathfrak{J} \,\hookrightarrow\, M$.

Corollaire B.3.7 ((cf. II.9.5, IV.4.7)) *Soit* M *un* A*-module de type fini et de torsion avec*

$$\mathrm{Ann}_A(M) \,=\, A\omega_M\,.$$

Soit $(a, b) \,\in\, A \times A$ *premiers entre eux, tels que*

$$ab \,=\, \omega_M\,.$$

alors : Si

$$\exists (x,y) \in M \times M,\ \mathrm{Ann}_A(x) = Aa \text{ et } \mathrm{Ann}_A(y) = Ab$$

il existe

$$z \in M \text{ tel que } \mathrm{Ann}_A(z) = Aab\ .$$

Preuve : *Les arguments donnés dans la preuve du corollaire II.9.5 s'adaptent mutatis mutandis puisque l'argument essentiel est en fait le théorème chinois des restes.*

Proposition B.3.8 *Soient A un anneau principal et $a \in A$, $a \neq 0$. Pour deux A-modules N et Q, les conditions suivantes sont équivalentes :*

a) Il existe une suite exacte courte

$$0 \to N \xrightarrow{\ i\ } A/a \xrightarrow{\ p\ } Q \to 0\ .$$

b) Il existe

$$(b,c) \in A \times A \text{ tel que } bc = a\ ,\ N \cong A/b\ ,\ Q \cong A/c\ .$$

Le sous$-A$-module $i(N)$ de A/a est alors le sous-A-module engendré par $\pi_a(c)$. C'est aussi le noyau du morphisme

$$A/a \to A/a\ ,\ x \mapsto bx$$

c'est-à-dire $A/a[Ab]$.

Preuve : *Les arguments donnés pour le cas où $A = \mathbb{Z}$, dans l'exercice II.12.4 s'adaptent mutatis mutandis au cas d'un anneau principal quelconque. On redonne cependant ici les arguments essentiels :*

*i) **(a)** $\Rightarrow$ **b)***

En confondant, à isomorphisme près, N et $i(N)$, N est un sous-A-module de A/a. La surjection canonique $\pi_a : A \to A/a$ étant un morphisme surjectif, $N = \pi_a[\pi_a^{-1}(N)]$ et $\pi_a^{-1}(N)$ est un sous-A-module (un idéal) de A. Il existe donc $c \in A$, tel que $\pi_a^{-1}(N) = Ac$. Il en résulte que :

$$i(N) = \pi_a(Ac)\ . \qquad 1$$

Puisque $\{0\} \subset N$,

$$Aa = \mathrm{Ker}\,\pi_a = \pi_a^{-1}(\{0\}) \subset \pi_a^{-1}(N) = Ac$$

si bien que $c|a$ et que :

$$\exists b \in A,\ ,\ bc = a\ . \qquad 2$$

Le noyau $\mathrm{Ker}\, p \circ \pi_a$ du morphisme surjectif $p \circ \pi_a : A \to Q$ est

$$\begin{aligned} \mathrm{Ker}\, p \circ \pi_a &= \{x \in A\ ;\ p[\pi_a(x)] = 0\} \\ &= \{x \in A\ ;\ \pi_a(x) \in \mathrm{Ker}\, p\} \\ &= \{x \in A\ ;\ \pi_a(x) \in i(N)\} \\ &= \pi_a^{-1}(N) \\ &= Ac\ . \end{aligned}$$

Il suffit désormais d'appliquer à $p \circ \pi_a$ *le corollaire I.8.13 pour obtenir un isomorphisme :*

$$Q \cong A/c \,. \tag{3}$$

Considérons le morphisme

$$\gamma : A \to A \,,\ x \mapsto cx \,. \tag{4}$$

Alors

$$\pi_a \circ \gamma : A \to N$$

est un morphisme surjectif. Son noyau est donné par :

$$\begin{array}{rcl} \operatorname{Ker} \pi_a \circ \gamma & = & \{x \in A \,;\, \gamma(x) \in \operatorname{Ker} \pi_a\} \\ & = & \{x \in A \,;\, cx \in Aa\} \\ & = & \{x \in A \,;\, \exists y \in A,\ ,\ cx = ay\} \\ & = & \{x \in A \,;\, \exists y \in A,\ ,\ cx = bcy\} \\ & = & \{x \in A \,;\, \exists y \in A,\ ,\ x = by\} \\ & = & Ab \,. \end{array} \tag{5}$$

En appliquant, cette fois au morphisme $\pi_a \circ \gamma$*, le corollaire I.8.13, on obtient un isomorphisme :*

$$N \cong A/b \,. \tag{6}$$

Les points 1, 2, 3 et 6 prouvent le résultat demandé.

ii) ***(b)*** $\Rightarrow$ ***a))***

Supposons donnés trois éléments a*,* b *et* c *de* A *tels que* $a \neq 0$ *et* $bc = a$*. Le morphisme* γ *déjà considéré en i).4 est tel que* $\operatorname{Ker} \pi_a \circ \gamma = Ab$ *(cf. i).5.) On an déduit, grâce à la proposition I.8.11, un morphisme injectif*

$$i : A/b \to A/a \text{ tel que } i \circ \pi_b = \pi_a \circ \gamma \,.$$

Notons alors

$$p : A/a \to (A/a)/i(A/b)$$

la surjection canonique. On laisse le soin au lecteur de montrer que le noyau du morphisme surjectif $p \circ \pi_a$ *est* Ac*, ce qui entraîne, grâce au corollaire I.8.13, que*

$$A/c \cong (A/a)/i(A/b) \,.$$

Proposition B.3.9 *L'anneau* A *étant toujours principal, Avec les notations de la proposition B.3.8, la suite est scindée si et seulement si* b *et* c *sont premiers entre eux.*

Preuve *: Si* b *et* c *sont premiers entre eux, l'existence d'une section (d'ailleurs unique) est établie dans au B.7.2.*

B.4 . $-p$-gradué

Lemme B.4.1 (Propriétés de $M[p^n]$**)** *Soit* M *un* A*-module. Pour tout élément irréductible* $p \in \mathbb{P}$ *:*

i) Pour tout $n \in \mathbb{N}$*,* $M[p^n]$ *est un sous-*A*-module de* M *(cf. A.7.4.i).) C'est même un* A/p^n*-module, et en particulier,* $M[p]$ *est un* A/p*-module, c'est-à-dire un* A/p*-espace vectoriel puisque* A/p *est un corps.*

ii) Pour tout $(m,n) \in \mathbb{N}\times\mathbb{N}$,

$$m \leq n \Rightarrow M[p^m] \subset M[p^n]$$

(cf. A.7.4.ii).)

iii)

$$\forall (m,n)\in\mathbb{N}\times\mathbb{N},\ (M[p^n])[p^m] = M[p^{\min(m,n)}] \text{ (cf. A.7.4.iii) .)}$$

iv) Pour tout morphisme de A*-modules* $f : M \to P$ *et tout* $n \in \mathbb{N}$, f *définit par restriction un morphisme de* A*-modules*

$$f[p^n] : M[p^n] \to P[p^n] \text{ (cf. A.7.4.vi) ,)}$$

qui est un isomorphisme dès que f *en est un.*

*v) (**Torsion et annulateur**)*

$$v_p(\mathrm{Ann}_A(M)) = 0 \Rightarrow \forall n\in\mathbb{N},\ M[p^n] = \{0\}\,.$$

***Preuve** : On a toujours* $Ap^n \subset \mathrm{Ann}_A(M[p^n])$, *si* d *est un générateur de* $\mathrm{Ann}_A(M[p^n])$, *il s'ensuit que*

$$d|p^n \text{ i.e. } d = p^\ell\,,\ \ell \leq n\,.$$

Or si $M[p^n] \neq \{0\}, \mathrm{Ann}_A(M[p^n]) \neq A$, *c'est-à-dire* $d \notin A^\times$, *ou encore* $\ell = v_p(d) > 0$.
Or

$$\mathrm{Ann}_A(M) \subset \mathrm{Ann}_A(M[p^n]) = Ap^\ell$$

si bien que

$$\ell = v_p(p^\ell) \leq v_p(\mathrm{Ann}_A(M))$$

ce qui entraîne le résultat par contraposée.

vi) S'il existe deux sous-A*-modules* N *et* P *tels que* $M = N \oplus P$, *alors, pour tout* $n \in \mathbb{N}$,

$$M[p^n] = N[p^n] \oplus P[p^n]\,;$$

s'il existe des A*-modules* N *et* P *tels que* $M = N \times P$,

$$\forall n\in\mathbb{N},\ M[p^n] \cong N[p^n] \times P[p^n]\,.$$

***Preuve** : Puisque* $\cdot[p^m]$ *est le noyau de* $\mathbf{p}^m$, *ceci résulte de la proposition I.9.18.i).*

Notation B.4.2 Étant donné un A-module M, un élément irréductible $p \in \mathbb{P}$ et un entier $n \in \mathbb{N}^*$, on note $\mathrm{gr}_{n,p}(M)$ (ou même $\mathrm{gr}_n(M)$ s'il ne peut y avoir de doute quant à p,) le module quotient

$$\mathrm{gr}_{n,p}(M) \ := \ M[p^n]/M[p^{n-1}]$$

qu'on appelle parfois le *gradué associé à la filtration* $M[p^\ell]\,,_{\ell \in \mathbb{N}}$.

Remarque B.4.3 En fait nous n'utiliserons, la plupart du temps que $\mathrm{gr}_{1,p}(M)$, (qui n'est autre que $M[p]$,) hormis dans des énoncés comme la proposition B.6.12, dont on peut d'ailleurs se passer dans le cas des groupes abéliens et des $\mathbb{K}[X]$-modules. Dans ce contexte on peut donc également se passer du lemme B.4.4 et se contenter de B.4.1.

Lemme B.4.4 (Propriétés de $\mathrm{gr}_{n,p}(M)$) *Soit M un A-module et $p \in \mathbb{P}$ un élément irréductible.*

i) Pour tout $n \in \mathbb{N}^*$, $\mathrm{gr}_{n,p}(M) := M[p^n]/M[p^{n-1}]$ est un κ_p-espace vectoriel, qui est de dimension finie si M est de type fini.

***Preuve** : Il suffit de remarquer que, pour tout*

$$x \in \mathrm{gr}_{n,p}(M)\,,\ px = 0\,,\ \text{si bien que le morphisme } A \to \mathrm{End}(\mathrm{gr}_{n,p}(M))$$

définissant la structure de module sur $\mathrm{gr}_{m,p}(M)$ se factorise à travers $\kappa_p = A/p$.

ii)

$$\forall (m,n) \in \mathbb{N}^* \times \mathbb{N}^*,\ n \leq m \Rightarrow \mathrm{gr}_{n,p}(M) = \mathrm{gr}_{n,p}(M[p^m])\ \textit{(cf. B.4.1.iii) .)}$$

iii) Pour tout morphisme de A-modules $f : M \to P$, et tout $n \in \mathbb{N}^*$, f induit un morphisme de κ_p-espaces vectoriels

$$\mathrm{gr}_{n,p}(f) : \mathrm{gr}_{n,p}(M) \to \mathrm{gr}_{n,p}(P)$$

plus précisément, $\mathrm{gr}_{n,p}(f)$ est l'unique morphisme rendant commutatif le diagramme :

$$\begin{array}{ccccccccc} 0 & \to & M[p^{n-1}] & \longrightarrow & M[p^n] & \longrightarrow & \mathrm{gr}_{n,p}(M) & \to & 0 \\ & & {\scriptstyle f[p^{n-1}]}\downarrow & & {\scriptstyle f[p^n]}\downarrow & & \downarrow{\scriptstyle \mathrm{gr}_{n,p}(f)} & & \\ 0 & \to & P[p^{n-1}] & \longrightarrow & P[p^n] & \longrightarrow & \mathrm{gr}_{n,p}(P) & \to & 0 \end{array} \qquad 1$$

Si f est un isomorphisme, $\mathrm{gr}_{n,p}(f)$ est aussi un isomorphisme.

***Preuve** : Il résulte du lemme B.4.1.ii) et B.4.1.iv) qu'on a un carré commutatif dont les morphismes horizontaux sont injectifs :*

$$\begin{array}{ccc} M[p^{n-1}] & \xrightarrow{\ i\ } & M[p^n] \\ {\scriptstyle f[p^{n-1}]}\downarrow & & \downarrow{\scriptstyle f[p^n]} \\ P[p^{n-1}] & \xrightarrow{\ j\ } & P[p^n]\,. \end{array}$$

En notants $q : P[p^n] \to \mathrm{gr}_{n,p}(P)$ la surjection canonique, on constate immédiatement que

$$q \circ f[p^n] \circ i = q \circ j \circ f[p^{n-1}] = 0$$

si bien que $q \circ Trsppfn$ se factorise à travers $\mathrm{gr}_{n,p}(M) = M[p^n]/M[p^{n-1}]$ c'est-à-dire qu'il existe un morphisme de A-modules

$$\mathrm{gr}_{n,p}(f) : \mathrm{gr}_{n,p}(M) \to \mathrm{gr}_{n,p}(P)$$

tel que le diagramme 1 soit commutatif. Il n'est pas difficile de constater que $\mathrm{gr}_{n,p}(f)$ est aussi un morphisme de κ_p-espaces vectoriels.

iv)

$$v_p(\mathrm{Ann}_A(M)) \;=\; 0 \;\Rightarrow\; \forall n \in \mathbb{N}^*,\ \mathrm{gr}_{n,p}(M) \;=\; \{0\}\ \textit{(cf. B.4.1.v) .)}$$

v) ***(gradué et somme directe/produit)***

Si M est un A-module tel qu'il existe deux sous-A-modules N et P tels que $M \;=\; N \,\oplus\, P$, alors, pour tout élément irréductible $p \;\in\; A$ et tout $n \;\in\; \mathbb{N}^*$, il existe un isomorphisme naturel

$$\mathrm{gr}_{n,p}(M) \;\cong\; \mathrm{gr}_{n,p}(N) \;\times\; \mathrm{gr}_{n,p}(P)\,.$$

***Preuve** : Pour $n \;\in\; \mathbb{N}^*$, notons $q \;:\; M[p^n] \;\to\; \mathrm{gr}_{n,p}(M)$ la surjection canonique dont le noyau est $M[p^{n-1}]$. Pour $X \;=\; N$ ou P, $q(X[p^n])$ est isomorphe à*

$$X[p^n]/(\mathrm{Ker}\, q \cap X[p^n]) \;\cong\; X[p^n]/(M[p^{n-1}] \cap X[p^n]) \;\cong\; X[p^n]/X[p^{n-1}] \;\cong\; \mathrm{gr}_n(X)\,. \qquad 1$$

Pour tout $x \;\in\; \mathrm{gr}_{n,p}(M)$, il existe $u \;\in\; n[p^M]$ tel que $q(u) \;=\; x$. D'après B.4.1.vi), il existe $(v,w) \;\in\; N[p^n] \;\times\; P[p^n]$ tel que $u \;=\; v + w$ si bien que $x \;=\; q(v) + q(w)$. On a ainsi montré que :

$$\mathrm{gr}_{n,p}(M) \;=\; q(N[p^n]) \;+\; q(P[p^n]) \qquad 2$$

ou encore, ce qui revient au même, grâce aux isomorphismes 1 que le morphisme

$$\mathrm{gr}_{n,p}(N) \times \mathrm{gr}_{n,p}(P) \;\to\; \mathrm{gr}_{n,p}(m)M\ ,\ (v,w) \;\mapsto\; q(v) + q(w)$$

est surjectif.

Il revient au même de montrer que ce dernier morphisme est injectif ou que la somme 2 est directe. Pour tout $(v,w) \;\in\; N[p^n] \;\times\; P[p^n]$

$$q(v) + q(w) \;=\; 0 \;\Leftrightarrow\; q(v+w) \;=\; 0 \;\Leftrightarrow\; v + w \;\in\; \mathrm{Ker}\, q \;=\; M[p^{n-1}]\,.$$

Il s'ensuit que

$$p^{n-1}(v+w) \;=\; 0 \;\Leftrightarrow\; p^{n-1}v \;+\; p^{n-1}w \;=\; 0\,.$$

Or $v \;\in\; N[p^n]$ (resp. $w \;\in\; P[p^n]$,) donc $p^{n-1}v \;\in\; N[p^n]$ (resp. $p^{n-1}w \;\in\; P[p^n]$.) La décomposition de $M[p^n]$ en somme directe B.4.1.vi), et $p^{n-1}v + p^{n-1}w \;=\; 0$ entraînent

$$p^{n-1}v \;=\; 0 \,\text{et}\, p^{n-1}w \;=\; 0$$

c'est-à-dire

$$v \;\in\; N[p^n] \;\cap\; M[p^{n-1}] \,\text{et}\, w \;\in\; P[p^n] \;\cap\; M[p^{n-1}],$$

qui équivaut à

$$v \;\in\; N[p^{n-1}] \,\text{et}\, w \;\in\; P[p^{m-1}],$$

qui entraîne finalement

$$q(v) \;=\; q(w) \;=\; 0\,.$$

Proposition B.4.5 *Soit $C := A/d$ un A-module cyclique (cf. B.3.2.)*

i) Si $d = p^\ell, \ell \in \mathbb{N}^*$, il résulte de la proposition B.3.8, que :

$$\begin{array}{rcl} \forall n \in \mathbb{N}^*, \quad n \leq \ell & \Rightarrow & C[p^n] \cong A/p^n \\ n > \ell & \Rightarrow & C[p^n] \cong C\,; \end{array} \qquad 1$$

il s'ensuit que :

$$\begin{array}{rcl} \forall n \in \mathbb{N}^*, \quad n \leq \ell & \Rightarrow & \mathrm{gr}_{n,p}(C) \cong \kappa_p \\ n > \ell & \Rightarrow & \mathrm{gr}_{n,p}(C) \cong \{0\}\,. \end{array}$$

ii) Il résulte alors des énoncés, B.4.1.vi) et B.4.4.v), des énoncés B.4.1.v) et B.4.4.iv) ainsi que du lemme B.3.6 que, pour $d \in A$ quelconque :

$$\begin{array}{l} \forall n \in \mathbb{N}^*, \\ \forall p \in \mathbb{P}, \quad \begin{array}{rcl} n \leq v_p(d) & \Rightarrow & C[p^n] \cong A/p^n \\ n > v_p(d) & \Rightarrow & C[p^n] \cong A/p^{v_p(d)}\,; \end{array} \end{array} \qquad 1$$

et il en résulte que :

$$\begin{array}{l} \forall n \in \mathbb{N}^*, \\ \forall p \in \mathbb{P}, \quad \begin{array}{rcl} n \leq v_p(d) & \Rightarrow & \mathrm{gr}_{n,p}(C) \cong \kappa_p \\ n > v_p(d) & \Rightarrow & \mathrm{gr}_{n,p}(C) \cong \{0\}\,. \end{array} \end{array} \qquad 2$$

B.5 . $-A/d$-modules injectifs

Lemme B.5.1 (A-modules, A/d-modules) *Soit $d \in A, d \neq 0$.*

i) Si

M est un A/d-modules, c'est en particulier un A-module à travers le morphisme structural $\pi_d : A \to A/d$ (cf. A.1.8.d) ,)

la loi étant donnée par $a \cdot x = \pi_d()a \cdot x$.

ii) Si $f : M \to N$ est un A/d-morphisme c'est un A-morphisme si M et N sont munis des structures de A-module décrites en i).

iii) Si M est un A/d-module de type fini il est aussi de type fini en tant que A-module (avec la structure décrite ci-dessus) : En effet si M est un A/d-module de type fini, il existe un entier $r \in \mathbb{N}$ et un A/d-morphisme surjectif $A/d^r \to M$. Ce dernier est également un A-morphisme qui composé avec le A-morphisme (déduit de $\pi_d\, \pi_d^r : A^r \to A/d^r$ donne un A-morphisme $A^r \to M$.

iv) Si M est un A/d-module tout sous-A/d-module de M est un sous-A-module de M.

v) Il découle alors du point iv) ci-dessus et de la proposition B.3.8 qu'un idéal de A/d est isomorphe à A/a avec $a|d$ et que le quotient $A/d/A/a$ est isomorphe à A/b avec $ab = d$.

Lemme B.5.2 *Soit $d \in A$, $d \neq 0$, $a \in A$ avec $a|d$. On considère A/a comme A/d-module graçe à sa structure de A/d-algèbre $A/d \to A/a$ (cf. A.1.8.b).) Pour tout $b \in A$ avec $b|a$, le morphisme naturel $A/b \hookrightarrow A/a$ doné par la proposition B.3.8 est aussi un A/d-morphisme qui fait de A/b un sous-A/d-module de A/a.*

Alors pour tout A/d-morphisme $f : A/b \to A/d$, il existe un morphisme

$$g : A/a \to A/d \text{ tel que } g_{|A/b} = f .$$

***Preuve** : On peut écrire $a = bc$, et l'on a alors, d'après la proposition, B.3.8, la suite exacte*

$$0 \to A/b \longrightarrow A/a \longrightarrow A/c \to 0 . \qquad \text{B.5.2.1}$$

La construction qui suit va en fait nous permettre de nous ramener au cas où $A/a = A/d$ en « remplaçant » en quelque sorte la suite B.5.2.1 par la colonne centrale du diagramme B.5.2.3. Notons $p : A/d \to A/a$ la surjection. L'image réciproque de A/b par ce morphisme est un sous-A/d-module de A/d donc en fait un sous-A-module de A/d qui, toujours d'après la proposition B.3.8 est de la forme A/b' avec $b'|d$. De plus la flèche induite $q : A/b' \to A/b$ étant encore surjective, $b|b'$. Le noyau de ces deux flèches est le même (cf. I.8.16,) égal à A/a'. On en déduit un isomorphisme sur les quotients A/c. On a les relations de divisibilité

$$aa' = d , ba' = b' , bc = a \text{ et } b'c = d . \qquad \text{B.5.2.2}$$

On peut synthétiser la construction précédente, qui n'est autre que celle donnée en I.8.15.iii), dans le diagramme à lignes et colonnes exactes suivan :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A/a' & \to & A/b' & \xrightarrow{q} & A/b & \to & 0 \\
 & & \downarrow \mathrm{Id} & & \downarrow j & & \downarrow i & & \\
0 & \to & A/a' & \to & A/d & \xrightarrow{p} & A/a & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \to & A/c & \xrightarrow{\mathrm{Id}} & A/c & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \qquad \text{B.5.2.3}$$

La donnée du morphisme $f : A/b \to A/d$ donne un morphisme $f' := f \circ q : A/b' \to A/d$ qui s'annule sur A/a (ou en d'autres termes vérifie $A/a \subset \operatorname{Ker} f'$.)

Il découle de la proposition B.3.8, que A/b' est engendré (tant comme sous-A-module que comme sous-A/d-module) de A/d par $\pi_d(c)$. Or A/b' est précisément l'annulateur $\operatorname{Ann}_{A/d}(\pi_d(b'))$ de $\pi_d(b')$ dans A/d. Puisque f' est un A/d-morphisme,

$$\pi_d(c) \in \operatorname{Ann}_{A/d}(\pi_d(b')) \Rightarrow f'(\pi_d(c)) \in \operatorname{Ann}_{A/d}(\pi_d(b')) .$$

Il existe donc $\alpha \in A/d$ tel que

$$f'(\pi_d(c)) = \alpha\pi_d(c) .$$

Il existe un unique A/d-morphisme

$$g' : A/d \to A/d , 1 \mapsto \alpha .$$

Il est immédiat de constater que ${g'}_{|A/b'} = f'$ ce qui entraîne en particulier que $A/a \subset \operatorname{Ker} g'$. Il existe donc un unique A/d-morphisme

$$g : A/a \to A/d \text{ tel que } g \circ p = g' .$$

C'est finalement un exercice de montrer que $g_{|A/b} = f$.

Proposition B.5.3 *Soit $d \in A, d \neq 0$, alors pour tout A/d-module de type fini M et tout morphisme injectif de A/d-modules $i : A/d \to M$ il existe un morphisme de A/d-modules*

$$r : M \to A/d \text{ tel que } r \circ i = \mathrm{Id}_{A/d} .$$

Preuve *:*

i) ***(Construction d'une suite*** $\left(M_n\right)_{,n\in\mathbb{N}}$***)***

Soit donc donné un A/d-module de type fini M et un A/d-morphisme injectif $i : A/d \to M$. Le morphisme i définit un isomorphisme

$$i : A/d \cong M_0 := \mathrm{Im}(i)$$

dont on note r_0 le morphisme réciproque.

Supposons donnés

$$M_k \,,0\leq k\leq n \text{ des sous-}A/d\text{-modules de } M$$

et

$$r_k \,,0\leq k\leq n \text{ des morphismes } M_k \to A/d$$

tels que

$$\forall 0 \leq k \leq n-1,\ M_k \subset M_{k+1}\ ,\ r_{k+1|M_k} = r_k \text{ et } r_{k+1} \circ i = \mathrm{Id}_{A/d}\ ;$$

(M_0, r_0) étant construit comme précédemment. S'il existe $x \in M \setminus M_n$, et un A/d-morphisme

$$r_{n+1} : M_n + A/dx \to A/d \text{ tel que } r_{n+1|M_n} = r_n \text{ et } r_{n+1} \circ i = \mathrm{Id}_{A/d},$$

on pose

$$M_{n+1} := M_n + A/dx \text{ sinon } M_{n+1} = M_n .$$

ii) ***(La suite*** $\left(M_n\right)_{,n\in\mathbb{N}}$ ***stationne)***

La suite $\left(M_n\right)_{,n\in\mathbb{N}}$ construite ci-dessus est croissante (c'est d'ailleurs une notion purement ensembliste qui ne concerne pas les éventuelles structures de modules.) Or on a remarqué en B.5.1.iii), que si M est de type fini comme A/d-module il l'est encore comme A-module. De plus, en vertu de B.5.1.iv), les $\left(M_n\right)_{,n\in\mathbb{N}}$ sont également des sous-A-modules de M. La proposition B.1.5 assure, puisque A est un anneau principal, que la suite $\left(M_n\right)_{,n\in\mathbb{N}}$ est stationnaire à partir d'un certain rang p.

iii) $(M_p = M)$

Si $M_p \neq M$, soit $x \in M \setminus M_p$ et $D := A/dx$ le sous-A/d-module de M engendré par x. Le noyau du A/d-morphisme

$$A/d \to M\ ,\ 1 \mapsto x$$

est l' annulateur $\mathrm{Ann}_{A/d}(x)$ de x dans A/d. On en déduit un A/d-isomorphisme

$$D \cong A/d/\mathrm{Ann}_{A/d}(x) .$$

Or $A/d/\mathrm{Ann}_{A/d}(x)$ est un certain quotient A/a de A/d (i.e. avec $a|d$) en vertu du point B.5.1.v). On a donc un A/d-isomorphisme $f : A/a \to D$. Or $D \cap M_p$ est un sous A/d-module de D dont l'image inverse par f est un sous-A/d-module de A/a et donc de la forme A/b avec $b|a$, toujours en vertu du point B.5.1.v).

Or le lemme B.5.2 assure que $f_{|A/b} \circ r_n$ se prolonge à A/a ce qui entraîne que r_n se prolonge à $M_p + D$ ce qui contredit que $M_p \neq M_{p+1}$ et finalement que $M_p \neq M$.

iv) Si $M_p \,=\, M$ on dispose sur M d'un A/d-morphisme

$$r_p \,:\, M \,\to\, A/d \text{ tel que } r_p \,\circ\, i \,=\, \mathrm{Id}_{A/d}\,.$$

B.6 . −Théorème de structure des A-modules de torsion (cf. II.10, IV.11)

Notation B.6.0 ((cf. II.10.0, IV.11.0)) Dans ce paragraphe (B.6,) A est un anneau principal.

Définition B.6.1 On dira dans cette section B.6 qu'un A-module M possède une *décomposition canonique* s'il existe un entier $r \,\in\, \mathbb{N}$, et des idéaux $\mathfrak{I}_{k\,,1\leq k\leq r}$ strictes (*i.e.* différents de A) et non nuls, de A, tels que

$$M \,\cong\, A/\mathfrak{I}_1 \,\times\, \ldots \,\times\, A/\mathfrak{I}_r \text{ et } \forall 1 \leq k \leq r-1,\; \mathfrak{I}_k \,\subset\, \mathfrak{I}_{k+1}\,.$$

On appellera r et le r-uplet $\mathfrak{I}_{k\,,1\leq k\leq r}$ les paramètres de la décomposition.

Remarque B.6.2 i) Dans la définition ci-dessus, si $d_{k\,,1\leq k\leq r}$ désigne des éléments de A, tels que

$$\forall 1 \leq k \leq r,\; \mathfrak{I}_k \,=\, Ad_k,$$

la condition $\mathfrak{I}_k \,\subset\, \mathfrak{I}_{k+1}$ équivaut à $d_{k+1}|d_k$. En revanche sans hypothèse suplémentaire, on ne peut pas envisager d'énoncé d'unicité vraiement strict, puisqu'on comprend bien que d_k et ud_k pour n'impporte quel élément inversible $u \,\in\, A^\times$, jouent le même rôle.

ii) On remarque qu'un module M possédant une décomposition canonique est de type fini (cf. II.1.5,) puisque $\{1_{A/\mathfrak{I}_k}\}_{,1\,\leq\, k\,\leq\, r}$ est une famille génératrice de M.

iii) On remarque encore que, si M possède une décomposition canonique, $\forall x \in M,\; \mathfrak{I}_1 \,\subset\, \mathrm{Ann}_A(x)$ (ce qui s'écrit $d_1 x \,=\, 0$, si d_1 est un générateur de $\mathfrak{I}_1$.) Or

$$\mathrm{Ann}_A(M) \,=\, \bigcap_{x\,\in\, M} \mathrm{Ann}_A(x),$$

si bien que $\mathfrak{I}_1 \,\subset\, \mathrm{Ann}_A(M)$.

Finalement, $A/\mathfrak{I}_1 \,\subset\, M$ donne la suite d'inclusions

$$\mathfrak{I}_1 \,\subset\, \mathrm{Ann}_A(M) \,\subset\, \mathrm{Ann}_A(A/\mathfrak{I}_1) \,=\, \mathfrak{I}_1$$

le dernier module étant cyclique (cf. B.3.2.)

Il en résulte que M est de torsion (cf. A.7.2.vi),) et d'idéal annulateur

$$\mathrm{Ann}_A(M) \,=\, \mathfrak{I}_1\,.$$

iv) Dans le cas où $M \,=\, \{0\}$, M possède une décomposition canonique de paramètres $r \,=\, 0$, qui est une convention cohérente avec le reste des énoncés.

v) Dans le cas où G est un groupe abélien, une décomposition canonique s'écrira

$$G \,\cong\, \mathbb{Z}/d_1\mathbb{Z} \,\times\, \ldots \,\times\, \mathbb{Z}/d_r\mathbb{Z}\,.$$

Les points ii), et iii) entraînent alors que G est fini d'exposant d_1.

Voir le paragraphe IV.11 pour une interprétation de ces résultats en termes de $\mathbb{K}[X]$-modules.

Le but de ce paragraphe (B.6) est d'établir le théorème B.6.13 qui constitue une réciproque aux points B.6.2.ii) et B.6.2.iii) de la remarque ci-dessus.

Le cas du A-module nul, $\{0\}$ ayant été traité en B.6.2.iv), on peut supposer, dans la suite, que M est un A-module non nul, de type fini (cf. II.1.5,) et de torsion (cf. A.7.2.vi).)

La première étape de la démonstration consiste à construire un sous-module cyclique (cf. B.3.2,) C de M isomorphe à $A/\mathrm{Ann}_A(M)$, où ce qui revient au même à construire un élément $x \in M$ tel que $\mathrm{Ann}_A(x) = \mathrm{Ann}_A(M)$. C'est la proposition B.6.3.

Dans le cas des groupes abéliens cela signifie qu'on met en évidence dans M un élément dont l'ordre est exactement l'exposant de M.

Proposition B.6.3 (Existence d'un sous-module cyclique maximal (cf. II.10.1, IV.11.1)) *Pour M un A-module non nul de type fini et de torsion, il existe un A-morphisme injectif $i : A/\mathrm{Ann}_A(M) \to M$ ou ce qui revient au même un élément*

$$x \in M \text{ tel que } \mathrm{Ann}_A(x) = \mathrm{Ann}_A(M)\,.$$

Preuve *: En notant*

$$\mathcal{Q} := \{p \in \mathcal{P}\,;\, v_p(\mathrm{Ann}_A(M)) \neq 0\},$$

en vertu du corollaire B.2.5, pour tout $setinp\mathcal{Q}$, il existe $x_p \in M$ tel que

$$\mathrm{Ann}_A(x_p) = Ap^{v_p(\mathrm{Ann}_A(M))}\,.$$

Le corollaire B.3.7 et un argument de récurrence sur le nombre d'éléments de $\mathcal{S}(\mathrm{Ann}_A(M))$ (dont on rapelle que c'est un ensemble fini) permettent de conclure.

Notation B.6.4 ((cf. II.10.2, IV.11.2)) En vertu de la proposition B.6.3 ci-dessus, et en notant

$$C := A/\mathrm{Ann}_A(M) \text{ et } Q := M/C,$$

on dispose d'une suite exacte :

$$0 \to C \xrightarrow{\ i\ } M \xrightarrow{\ q\ } Q \to 0\,. \qquad \text{B.6.4.1}$$

Lemme B.6.5 *Si M est un A-module de type fini et de torsion, dans la suite exacte B.6.4.1 il en est de même pour Q.*

Preuve *: La proposition II.1.9 assure que Q est de type fini. Il découle du lemme A.7.3.iv) que $\mathrm{Ann}_A(Q) \neq \{0\}$ si bien que Q est de torsion.*

Remarque B.6.6 À l'inverse de ce qu'on a constaté dans le cas des groupes abéliens ($\mathbb{Z}$-modules) au paragraphe II.10 et dans le cas des $\mathbb{K}[X]$-modules au paragraphe IV.11, on ne dispose pas, dans le cas général, d'un argument « à la EULER–POINCARÉ » Il ne serait pas impossible, et ce peut être un exercice intéressant, de généraliser par exemple les proposition II.10.3 et II.10.4 au cas A-modules sur un anneau principal A. Cependant il manquerait un invariant (le cardinal dans le cas des groupes abéliens, la $\mathbb{K}$-dimension dans le cas des $\mathbb{K}[X]$-modules) qui prendrait une valeur sur le quotient Q dans la suite exacte B.6.4.1, strictement inférieure à celle qu'il prendrait sur M.

On disposera en fait d'un tel invariant (voir proposition B.6.8, mais bénéficiant d'une propriété plus faible, à savoir qu'on peut montrer qu'il prend une valeur sur Q strictement inférieure à celle qu'il prend sur M à la seule condition que la suite B.6.4.1 soit scindée ; autrement dit que

$$M \;\cong\; C \oplus Q\,.$$

On ne peut donc déduire ce résultat d'un argument de récurrence et l'on doit le montrer a priori ; ce qui est fait à la proposition B.6.7.

Proposition B.6.7 *Pour M un A-module de type fini et de torsion, la suite B.6.4.1 possède une rétraction c'est-à-dire qu'il existe un A-morphisme*

$$\rho \;:\; M \;\to\; C \text{ tel que } \rho \circ i \;=\; \mathrm{Id}_C$$

ce qui donne un isomorphisme

$$M \;\cong\; C \;\oplus\; Q\,.$$

Preuve *: Le A-module M étant de torsion c'est encore un $A/\mathrm{Ann}_A(M)$-module et il en est de même du A-module C dans la suite exacte B.6.4.1. On constate qu'alors i est un $A/\mathrm{Ann}_A(M)$-morphisme et il suffit d'appliquer la proposition B.5.3.*

Proposition B.6.8 *Si la suite B.6.4.1 est scindée, i.e.*

$$M \;\cong\; C \oplus Q \text{ alors } \max_{p\,\in\,\mathbb{P}}(\dim_{\kappa_p} Q[p]) \;<\; \max_{p\,\in\,\mathbb{P}}(\dim_{\kappa_p} M[p])\,.$$

Preuve *: Pour tout élément irréductible $p \in \mathbb{P}$, il résulte du lemme B.4.1.vi) que :*

$$M[p] \;\cong\; C[p] \;\times\; Q[p]\,. \qquad \textit{B.6.8.1}$$

Or $\mathrm{Ann}_A(M) \;=\; A\omega_M$, et il existe un ensemble fini $\mathcal{S}(\mathrm{Ann}_A(M))$ d'éléments irréductibles deux à deux non associés tel que

$$\omega_M \;=\; \prod_{p\,\in\,\mathcal{S}(\mathrm{Ann}_A(M))} p^{v_p(\mathrm{Ann}_A(M))}\,.$$

Puisque $C \;\cong\; A/\mathrm{Ann}_A(M) \;\cong\; A/\omega_M$, le théorème chinois des restes donne un isomorphisme

$$C \;\cong\; \prod_{p\,\in\,\mathcal{S}(\mathrm{Ann}_A(M))} A/p^{v_p(\mathrm{Ann}_A(M))}\,.$$

Il résulte alors, toujours du lemme B.4.1.vi), que pour tout irréductible $p \in \mathbb{P}$,

$$C[p] \cong \prod_{q \in \mathcal{S}(\mathrm{Ann}_A(M))} A/q^{v_q(\omega_M)}[p] .$$

Or

$$\forall (p,q) \in \mathbb{P} \times \mathbb{P},\ p \neq q \Rightarrow \forall n \in \mathbb{N},\ \forall m \in \mathbb{N},\ \mathrm{gr}_{n,p}(A/q^m) = 0 .$$

Il résulte alors du lemme B.4.5.i) :

$$\begin{array}{rcl} \forall p \in \mathbb{P}, \quad p \in \mathcal{S}(\mathrm{Ann}_A(M)) & \Rightarrow & \dim_{\kappa_p} C[p] = 1 \\ p \notin \mathcal{S}(\mathrm{Ann}_A(M)) & \Rightarrow & \dim_{\kappa_p} C[p] = 0 . \end{array} \qquad \textit{B.6.8.2}$$

En utilisant la décomposition p*-primaire de* M *(cf. B.2.3.ii)e)t le lemme B.4.1.vi),*

$$\forall p \in \mathbb{P},\ M[p] \cong \prod_{q \in \mathcal{S}(\mathrm{Ann}_A(M))} M[q^{v_q(\mathrm{Ann}_A(M))}][p]$$

d'où il découle que :

$$\forall p \in \mathbb{P},\ p \notin \mathcal{S}(\mathrm{Ann}_A(M)) \Rightarrow M[p] = \{0\} . \qquad \textit{B.6.8.3}$$

Il résulte alors de B.6.8.1, B.6.8.2 et B.6.8.3 que :

$$\begin{array}{rcl} \forall p \in \mathbb{P}, \quad p \in \mathcal{S}(\mathrm{Ann}_A(M)) & \Rightarrow & \dim_{\kappa_p} Q[p] = \dim_{\kappa_p} M[p] - 1 \\ p \notin \mathcal{S}(\mathrm{Ann}_A(M)) & \Rightarrow & \dim_{\kappa_p} Q[p] = \dim_{\kappa_p} M[p] . \end{array} \qquad \textit{B.6.8.4}$$

On en déduit finalement que :

$$\max_{p \in \mathbb{P}}(\dim_{\kappa_p} Q[p]) < \max_{p \in \mathbb{P}}(\dim_{\kappa_p} M[p]) . \qquad \textit{B.6.8.5}$$

Lemme B.6.9 *Soit* M *un* A*-module possédant une décomposition canonique de paramètres*

$$r \in \mathbb{N} \text{ et } \mathfrak{I}_{k\ ,1 \leq k \leq r} .$$

Alors il existe $p \in \mathbb{P}$ *tel que*

$$\forall 1 \leq k \leq r,\ \dim_{\kappa_p} A/\mathfrak{I}_k[p] = 1 .$$

Preuve *: On sait déjà, d'après le lemme B.4.5.ii).2, que*

$$\forall 1 \leq k \leq r,\ \dim_{\kappa_p} A/d_k[p] \leq 1 .$$

Or

$$\mathfrak{I}_r \neq 0 \text{ et } \mathfrak{I}_r \neq A \textit{ (cf. B.6.1 .)}$$

Il en résulte qu'il existe $p \in \mathbb{P}$ *tel que*

$$0 < v_p(\mathfrak{I}_r) < (+\infty) .$$

Puisque

$$\forall 1 \leq k \leq r-1,\ \mathfrak{I}_k \subset \mathfrak{I}_r,$$
$$\forall 1 \leq k \leq r,\ 0 < v_p(\mathfrak{I}_k) < (+\infty) .$$

Le résultat découle alors du lemme B.4.5.ii).1.

Définition B.6.10 (Diviseur élémentaires) Pour M un A-module de type fini, et $(r, \mathfrak{I}_k\ ,1\leq k\leq r\ )$ une décomposition canonique de $\mathrm{Tor}_A(M)$, les $p^{v_p(\mathfrak{I}_k)}$, $p\ \in\ \mathbb{P}$, non inversibles, sont appelés *diviseurs élémentaires* de M.

Proposition B.6.11 *Étant doné un A-module M possédant une décomposition canonique de paramètres*

$$r\ \in\ \mathbb{N}\,\text{et}\,\mathfrak{I}_k\ ,1\leq k\leq r\ \in,$$
$$r\ =\ \max_{p\ \in\ \mathbb{P}}(\dim_{\kappa_p} M[p])\ .$$

Preuve *: On a déjà remarqué (cf. B.6.2.ii), B.6.2.iii),) que sous ces hypothèses M est de type fini et de torsion et que $\mathrm{Ann}_A(M)\ =\ \mathfrak{I}_r$.*

Le théorème de décomposition B.2.3.ii) assure qu'il existe un sous-ensemble fini $\mathcal{S}(\mathrm{Ann}_A(M))\ \subset\ \mathbb{P}$ tel que pour tout $p\ \in\ \mathcal{S}(\mathrm{Ann}_A(M))$, $v_p(\mathrm{Ann}_A(M))\ \neq\ 0$, et

$$M\ =\ \prod_{p\ \in\ \mathcal{S}(\mathrm{Ann}_A(M))} M[p^{v_p(\mathrm{Ann}_A(M))}]$$

et pour tout $p\ \notin\ \mathcal{S}(\mathrm{Ann}_A(M))$, et tout $n\ \in\ \mathbb{N}$, $M[p^n]\ =\ \{0\}$. Il s'ensuit que

$$\max_{p\ \in\ \mathbb{P}}(\dim_{\kappa_p} M[p])\ =\ \max_{p\ \in\ \mathcal{S}(\mathrm{Ann}_A(M))}(\dim_{\kappa_p} M[p])\ . \qquad \textit{B.6.11.1}$$

Le lemme B.4.1.vi) permet alors d'écrire :

$$\max_{p\ \in\ \mathcal{S}(\mathrm{Ann}_A(M))}(\dim_{\kappa_p} M[p])\ =\ \max_{p\ \in\ \mathcal{S}(\mathrm{Ann}_A(M))}\big(\sum_{k=1}^{r}\dim_{\kappa_p} A/\mathfrak{I}_k[p]\big)\ .$$

Or d'après le lemme B.4.5.ii).2, $\dim_{\kappa_p} A/\mathfrak{I}_k[p]\ \leq\ 1$, si bien que :

$$\max_{p\ \in\ \mathbb{P}}(\dim_{\kappa_p} M[p])\ =\ \max_{p\ \in\ \mathcal{S}(\mathrm{Ann}_A(M))}(\dim_{\kappa_p} M[p])\ \leq\ r\ . \qquad \textit{B.6.11.2}$$

Or le lemme B.6.9 affirme qu'il existe $p\ \in\ \mathbb{P}$ tel que

$$\forall 1\leq k\leq r,\ \dim_{\kappa_p} A/\mathfrak{I}_k[p]\ =\ 1$$

ce qui achève la preuve.

Proposition B.6.12 *Étant doné un A-module M possédant une décomposition canonique de paramètres*

$$r\ \in\ \mathbb{N}\,\text{et}\,\mathfrak{I}_k\ ,1\leq k\leq r\ \in,$$

alors

$$\forall p\in\mathbb{P},\ \forall n\in\mathbb{N}^*,\ \dim_{\kappa_p}\mathrm{gr}_{n,p}(M)\ =\ \#\big(\{k\ \in\ [1;r]\ ;\ v_p(d_k)\ \leq\ n\}\big)$$

ou bien encore

$$\forall p\in\mathbb{P},\ \forall n\in\mathbb{N}^*,\ \dim_{\kappa_p}\mathrm{gr}_{n+1,p}(M)-\dim_{\kappa_p}\mathrm{gr}_{n,p}(M)\ =\ \#\big(\{k\ \in\ [1;r]\ ;\ v_p(d_k)\ =\ n\}\big)\ .$$

Preuve *: C'est une conséquence du lemme B.4.4.v) qui permet d'écrire*

$$\forall p\in\mathbb{P},\ \forall n\in\mathbb{N}^*,\ \mathrm{gr}_{n,p}(M)\ =\ \prod_{k=1}^{r}\mathrm{gr}_{n,p}(A/\mathfrak{I}_k)$$

et du lemme B.4.5.ii).2.

Théorème B.6.13 (de structure des A-modules de torsion (cf. II.10.5, IV.11.5)) *Soit M un A-module de type fini (cf. II.1.5,) et de torsion (cf. A.7.2.vi).)*

1) Il existe un entier $r \in \mathbb{N}$, et des idéaux strictes, non égaux à A, et non égaux à $\{0\}$ $\mathfrak{I}_k$,$1 \leq k \leq r$ de A, tels que M est isomorphe, en tant que A-module au produit

$$A/\mathfrak{I}_1 \times \ldots \times A/\mathfrak{I}_r \text{ et } \forall 1 \leq k \leq r-1,\ \mathfrak{I}_k \subset \mathfrak{I}_{k+1}\ .$$

2) L'entier r et le r-uplet d'idéaux $\mathfrak{I}_k$,$1 \leq k \leq r$ satisfaisant aux conditions de 1) sont uniques.

***Preuve** :*

*1) (**Existence**)*

On rappelle que si $M = \{0\}$ on prendra $r = 0$.

Si M est un A-module non nul, de type fini et de torsion, on peut appliquer la proposition B.6.3 qui donne la suite exacte

$$0 \to C \xrightarrow{i} M \xrightarrow{q} Q \to 0 \text{ (cf. B.6.4.1 ,)}$$

où $C \cong A/\mathrm{Ann}_A(M)$ est un A-module cyclique.

Bien entendu, si $Q = \{0\}$, $C \cong M$ et le résultat est prouvé. Sinon, on sait, en vertu de la proposition B.6.7, que la suite ci-dessus est rétractée. Il s'ensuit que

$$M \cong C \times Q\ .$$

Il en résulte, en vertu de la proposition B.6.8, que

$$\max_{p \in \mathbb{P}}(\dim_{\kappa_p} Q[p]) < \max_{p \in \mathbb{P}}(\dim_{\kappa_p} M[p])\ .$$

En raisonnant par récurrence sur $\max_{p \in \mathbb{P}}(\dim_{\kappa_p} \cdot[p])$, on peut donc supposer le résultat établi pour Q et conclure, pour peu qu'on se convainque, que si $\max_{p \in \mathbb{P}}(M[p]) = 1$, l'énoncé découle du théorème B.2.3 et du théorème chinois des restes.

*2) (**Unicité**)*

La proposition B.6.11 caractérise complètement l'entier r dans une décomposition canonique en termes du A-mùodule M lui-même.

La proposition B.6.12 permet pour tout $p \in \mathbb{P}$ et tout $1 \leq k \leq r$, de déterminer $v_p(\mathfrak{I}_k)$ ce qui détermine complètement les idéaux $\mathfrak{I}_k$,$1 \leq k \leq r$.

Remarque B.6.13.3 L'unicité de la décomposition du A-module M consiste en fait, une fois l'entier r déterminé grâce à la proposition B.6.11, à décomposer chacun des $A/\mathfrak{I}_k$ grâce au théorème chinois des restes. Il est alors nécessaire et suffisant d'établir l'unicité des diviseurs élémentaires (cf. B.6.10,) $v_p(\mathfrak{I}_k)$ qui sont bien déterminés grâce à la proposition B.6.12. On constatera en IV.10.10.3 que dans le cas des $\mathbb{K}[X]$-modules ces diviseurs élémentaires ne sont rien d'autres que les blocs de JORDAN et qu'on a alors d'autres arguments pour prouver leur unicité.

Dans le cas des $\mathbb{K}[X]$-module l'unicité des facteurs invariants peut être établie a priori et l'unicité des diviseurs élémentaires en découle.

Dans le cas général envisagé dans ce paragraphe, on procède en fait dans l'ordre inverse et c'est l'unicité des diviseurs élémentaires qui entraîne l'unicité des facteurs invariants.

Définition B.6.14 (Facteurs invariants (cf. II.10.6, IV.11.9)) Pour un A-module de type fini M, les idéaux $\mathfrak{I}_k$,$1\leq k\leq r$ donnés par le téhorème B.6.13 et tels que

$$\mathrm{Tor}_A(M) \;\cong\; A/\mathfrak{I}_1 \;\times\; \ldots \;\times A/\mathfrak{I}_r$$

s'appellent les *facteurs invariants*de M.

Lorsqu'il existe un choix « canonique » de générateurs des idéaux $\mathfrak{I}_k$,$1\leq k\leq r$ (dans $\mathbb{Z}$ des entiers > 1, dans $\mathbb{K}[X]$ des polynômes unitaires,) ces générateurs sont, par abus de langage, appelés *facteurs invariants* de M.

Corollaire B.6.15 ((cf. II.10.7, IV.11.10)) *i) Deux A-modules de type fini et de torsion M et P sont isomorphes si et seulement si ils ont les mêmes facteurs invariants.*

ii) Deux A-modules de type fini M et P sont isomorphes si et seulement si ils ont même rang et mêmes facteurs invariants.

Preuve *: Adapter la preuve du corollaire II.10.7.*

Remarque B.6.16 Étant donné un A-module $M \;=\; \mathcal{L}(M) \;\oplus\; \mathrm{Tor}(M)$, on pourrait étendre la définition de *facteurs invariants* à la partie libre $\mathcal{L}(M)$ de M. En effet si $\mathrm{rg}(M) \;=\; n$, on a

$$\mathcal{L}(M) \;\cong\; A^n \;\cong\; (A/\{0\})^n\,.$$

En autorisant les facteurs invariants à être nuls. Si $\mathrm{Tor}(M)$ a r facteurs invariants on obtient une suite de $n+r$ idéaux

$$\mathfrak{I}_k\,,1\leq k\leq n+r \text{ telle que } \forall 1\leq k\leq n,\; \mathfrak{I}_k \;=\; \{0\} \text{ et } \forall 1\leq k\leq n+r-1,\; \mathfrak{I}_k \;\subset\; \mathfrak{I}_{k+1}\,.$$

On peut alors déduire du corollaire B.6.15 et du théorème B.1.4, que deux A-module de type fini sont isomorphes si et seulement si ils ont mêmes facteurs invariants avec la définition étendue donnée ci-dessus.

B.7 . −Exercices

Exercice B.7.1 [Annulateur]

On rappelle que l'annulateur $\mathrm{Ann}_A(P)$ **pour** $P \;\subset\; M$, **est lidéal défini par**

$$\mathrm{Ann}_A(P) \;=\; \{a \;\in\; A\,;\; \forall x\in P,\; ax \;=\; 0\}\,.$$

Soient $\mathfrak{I}$ **et** $\mathfrak{J}$ **des idéaux de** A.

1) Montrer que

$$\mathfrak{I} \;\subset\; \mathrm{Ann}_A(M[\mathfrak{I}]) \text{ et } \mathfrak{J} \;\subset\; \mathrm{Ann}_A(M[\mathfrak{J}])\,.$$

On suppose désormais que $\mathfrak{I}$ **et** $\mathfrak{J}$ **sont comaximaux *i.e.*** $\mathfrak{I}+\mathfrak{J} \;=\; A$.

2) Montrer qu'alors

$$A \;=\; \mathfrak{I}+\mathfrak{J} \;=\; \mathrm{Ann}_A(M[\mathfrak{I}]) \;+\; \mathrm{Ann}_A(M[\mathfrak{J}])\,.$$

On suppose de plus désormais que $\mathrm{Ann}_A(M) \;=\; \mathfrak{I}\cap\mathfrak{J}$.

3) Montrer que

$$M \;=\; M[\mathrm{Ann}_A(M)] \;=\; M[\mathfrak{I}\cap\mathfrak{J}] \;=\; M[\mathfrak{I}] \;\oplus\; M[\mathfrak{J}]\,.$$

4) Montrer que

$$\mathfrak{I} \cap \mathfrak{J} \;=\; \mathrm{Ann}_A(M[\mathfrak{I}]) \;\cap\; \mathrm{Ann}_A(M[\mathfrak{J}])\,.$$

5) Conclure finalement que

$$\mathfrak{I} \;=\; \mathrm{Ann}_A(M[\mathfrak{I}]) \text{ et } \mathfrak{J} \;=\; \mathrm{Ann}_A(M[\mathfrak{J}])\,.$$

Exercice B.7.2 [Suites exactes]
Supposons donnée une suite exacte

$$0 \;\to\; \mathbb{Z}/a \xrightarrow{\;i\;} A \xrightarrow{\;p\;} \mathbb{Z}/b \;\to\; 0\,.$$

1) Que vaut $\#(A)$?

2) Montrer que pour tout $x \in A$, $abx = 0$ (on pourra chercher à donner deux arguments distincts.)

3) Étant données deux sections s et $t : \mathbb{Z}/b \to A$ de p, montrer que $s-t$ définit un morphisme $\mathbb{Z}/b \to \mathbb{Z}/a$; et en déduire que si a et b sont premier entre eux, p possède au plus une section.

4) On suppose désormais que a et b sont premiers entre eux et on note $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ un couple d'entiers tel que $au + bv = 1$.

a) Montreer que

$$\underline{b} : A \to A\,,\; x \mapsto bvx$$

est un projecteur à valeurs dans $i(\mathbb{Z}/a)$ et en déduire une rétraction $r : A \to \mathbb{Z}/a$ de i. Que peut-on dire d'une autre rétraction r' de i ?

b) En déduire un isomorphisme de groupes

$$A \;\cong\; \mathbb{Z}/a \;\times\; \mathbb{Z}/b\,.$$

Exercice B.7.3 Considérons l'anneau $A := \mathbb{Z}/6\mathbb{Z}$ et M le A-module A lui-même (cf. A.1.2.b).) Déterminer $\mathrm{Tor}_A(M)$, est-ce un sous-A-module de M ?

Exercice B.7.4 [Résolution d'un groupe commutatif de type fini]

1) Soit K un corps et E un K-espace vectoriel admettant une famille génératrice finie. Montrer qu'il existe alors un unique entier $n \in \mathbb{N}$ tel que $K^n \simeq E$.

2) Soit G un groupe commutatif admettant une famille génératrice finie.

a) Existe-t-il nécessairement un entier $n \in \mathbb{N}$ tel que $\mathbb{Z}^n$ soit isomorphe à G ?

b) Montrer qu'il existe un couple d'entiers $(n, m) \in \mathbb{N}^2$ tel que la suite courte

$$0 \longrightarrow \mathbb{Z}^m \longrightarrow \mathbb{Z}^n \longrightarrow G \longrightarrow 0$$

soit exacte.

c) Le couple d'entiers (n, m) de la question précédente est-il unique ? Donner une condition nécessaire et suffisante sur $(n, m) \in \mathbb{N}^2$ pour qu'il existe une suite exacte courte

$$0 \longrightarrow \mathbb{Z}^m \longrightarrow \mathbb{Z}^n \longrightarrow G \longrightarrow 0.$$

Soit A un anneau commutatif et M un A-module.

3) a) Montrer que les $\mathbb{Z}$-modules sont les groupes commutatifs et que les K-modules sont les K-espaces vectoriels si K est un corps.

b) Reformuler les résultats des deux premières questions dans le langage des A-modules.

c) Montrer qu'il existe un anneau commutatif A et un module M admettant une famille génératrice finie tel qu'il n'existe pas de couple d'entiers $(n, m) \in \mathbb{N}^2$ tel que la suite

$$0 \longrightarrow A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$$

soit exacte (on pourra étudier $A = \mathbb{Q}[x, y]$ et M le $\mathbb{Q}[x, y]$-module $\mathbb{Q}$ muni de l'action induite par $xm = 0$ et $ym = 0$ pour tout $m \in M$).

C . −Théorème de la base adaptée. (cf. II.11)

C.0 . −Introduction

On a établi, au paragraphe II.11 l'existence d'une *base adaptée* pour un couple de A-module $M \subset L$ dans le cas où A est un *anneau euclidien* (cf. I.13.6.1,) et où L est un A-module libre de type fini (cf. II.3.2.) Rappelons d'abord (cf. II.11.1,) que

Définition C.0.1 (base adaptée) On dit qu'un couple de A-modules $M \subset L$ admet une *base adaptée*, s'il existe une base $\lambda_i\,,1\leq i\leq r}$ de L, un entier $s \leq r$, des éléments

$$d_i\,,1\leq i\leq s} \in A \text{ tel que } d_i\lambda_i\,,1 \leq i \leq s} \text{ soit une base de } M$$

et

$$\forall 1 \leq i \leq s-1,\ d_{i+1}|d_i\ .$$

Dans toute la suite de cet appendice (C,) on supposera que A est un anneau principal.

On démontre (théorème C.1.8,) le théorème dit de la base adaptée dans le cas d'un anneau principal quelconque, sans faire,, comme au paragraphe II.11 l'hypothèse que A est un anneau euclidien. Le résultat obtenu ici, est donc, en un certain sens, plus général que celui obtenu en II.11.12. Cependant on ne donne ici aucun procédé algorithmique (contrairement à II.11.9) permettant de construire une base adaptée.

On a déjà mentionné au paragraphe II.11 que le théorème de la base adaptée précise en fait le théorème II.4.6 en caractérisant de quelle manière son disposés deux A-modules emboîtés $M \subset L$ pour peu que L soit libre de type fini. Cepandant en observant atentivement la preuve du théorème C.1.8 et notamment la proposition C.1.6 et le lemme C.1.7, qui en sont les ingrédients principaux, on constate qu'on ne fait jamais l'hypothèse que M est libre et même de type fini. Il s'ensuit qu'on obtient de cette manière une preuve alternative du théorème II.4.6. On obtient également un résultat plus précis que l'on connaissait cependant déjà dans le cas où $\mathrm{rg}(L) = 1$ grâce au lemme II.4.1.

On a également mis en évidence à la proposition II.11.3 le lien qui existe entre une base adaptée pour le couple $M \subset L$ et les *facteurs invariants* du quotient L/M. On précisera encore davantage ce lien au paragraphe C.2.

On continuera, dans ce chapitre à utiliser les notations déjà utilisées dans les chapitres précédents.

Notation C.0.2 A étant un anneau principal, pour tout élément $a \in A$, on notera A/a l'anneau quotient A/Aa de A par l'idéal principal Aa.

On notera $\pi_a : A \to A/a$ la surjection canonique.

De même pour tout $n \in \mathbb{Z}$, on aura tendance à noter $\mathbb{Z}/n$ pour $\mathbb{Z}/n\mathbb{Z}$ et $\pi_n : \mathbb{Z} \to \mathbb{Z}/n$ la surjection canonique.

Notation C.0.3 Étant donné un A-module M,

i) On appellera *formes A-linéaires* ou même tout simplement *formes linéaires* sur M un morphisme de A-modules $f : M \to A$. Dans le cas où $A = \mathbb{Z}$ est l'anneau des entiers relatifs, on emploira parfois le terme de *formes linéaires entières*.

ii) On notera

$$M^* := \mathrm{Hom}_A(M, A) \text{ (cf. A.2.13 ,)}$$

l'ensemble des formes linéaires sur M.

On rappelle que M^* a une structure naturelle de A-module (cf. A.2.12.)

On pourra appeler M^* le *module dual* de M.

iii) Pour L un A-module libre de rang r et de base $\lambda_{i\ ,1\leq i\leq r}$, pour tout $1 \leq j \leq r$ on notera $\lambda_j^* : L \to A$ l'unique morphisme (cf. II.1.8,) défini par

$$\forall 1 \leq i \leq r,\ \lambda_j^*(\lambda_i) = \delta_i^j .$$

Bien entendu, par analogie avec la situation des espaces vectoriels, on peut appeler $\lambda_{i\ ,1\leq i\leq r}^*$ la *base duale* de $\lambda_{i\ ,1\leq i\leq r}$.

C.1 . −Existence et unicité d'une base adaptée

Dans tout ce paragraphe (C.1,) A est un anneau principal.

Lemme C.1.1 *Soient L un A-module libre de type fini et $x \in L \setminus \{0\}$. Les conditions suivantes sont écquivalentes :*

a) Ax a un supplémentaire dans L.

b) Il existe une forme linéaire

$$f : L \to A \text{ telle que } f(x) = 1 .$$

c) L'élément x peut être complété en une base de L.

d) L'élément x est indivisible i.e.

$$\exists (y, d) \in L \times A,\ x = dy \Rightarrow d \in A^\times .$$

e) Le module L/Ax est sans torsion.

***Preuve** :*

*i) **(a) ⇔ c))***

Il suffit de remarquer que L étant libre (sans torsion suffirait), x n'est pas un élément de torsion et est donc une base de Ax. Si cette base se complète en une base $\mathcal{B}$ de L, $\mathrm{Vect}\big(\mathcal{B} \setminus \{x\}\big)$ est évidemment un supplémentaire de Ax.

Réciproquement si Ax possède un suplémentaire M, ce dernier est un sous-A-module de L. Si L est libre de type fini, il en est de même de M (cf. II.4.6 ;) puisque A est un anneau principal. Si $\mathcal{B}$ est une base de M, $\mathcal{B} \cup \{x\}$ est clairement une base de L.

*ii) **(c) ⇒ b))***

Si x se complète en une base de L, il existe une unique application linéaire $f : L \to A$ telle que $f(x) = 1$ et $f(\beta) = 0\ \forall \beta \in \mathcal{B}$, où l'on a complété x de sorte que $\mathcal{B} \cup \{x\}$ est une base de L.

iii) ***(b) ⇒ a))***

La forme linéaire $f : L \to A$ *est alors surjective : en effet pour tout* $a \in A$,

$$f(ax) = af(x) = a\,.$$

En notant $K := \operatorname{Ker} f$, *on a une suite exacte courte*

$$0 \to K \longrightarrow L \xrightarrow{f} A \to 0\,.$$

Comme A *est un* A*-module libre de type fini, cette suite est scindée (cf. II.3.9,) i.e. il existe*

$$^{M}orsAL \text{ tel que } f \circ s = \mathrm{Id}_A\,.$$

On peut même ici choisir s *définie par* $s(1) := x$. *D'où il suit que* $s(A) = Ax$. *Il résulte alors du théorème I.9.15 que*

$$M = K \oplus Ax\,.$$

iv) ***(e) ⇒ a))***

On a une suite exacte

$$0 \to Ax \longrightarrow L \xrightarrow{p} L/Ax \to 0\,.$$

Puisque L/Ax *est sans torsion il est libre d'après le théorème B.1.2. La suite exacte ci-dessus est donc scindée en vertu de la proposition II.3.9. Il existe donc un morphisme*

$$s : L/Ax \to L \text{ tel que } p \circ s = \mathrm{Id}_{L/Ax},$$

et d'après le théorème I.9.15,

$$L = Ax \oplus s(L/Ax)\,.$$

v) ***(a) ⇒ e))***

si Ax *possède un supplémentaire* S, *il résulte du théorème I.9.15, qu'on a une suite exacte*

$$0 \to Ax \longrightarrow L \xrightarrow{p} S \to 0$$

Si $\pi : L \to L/Ax$ *est la surjection canonique,*

$$\operatorname{Ker}\pi = \operatorname{Ker} p,$$

si bien que p *se factorise en un morphisme injectif*

$$^{M}or\phi L/AxS \text{ tel que } \phi \circ \pi = p\,.$$

Or S *est un supplémentaire de* Ax *donc un sous-*A*-module de* L, *donc libre de type fini en vertu du théorème II.4.6. Puisque* ϕ *est injectif,* L/Ax *est isomorphe à un sous-*A*-module de* S *qui, en vertu du théorème loc. cit. est encore libre de type fini, donc sans torsioN.*

*vi) (**e**) $\Rightarrow$ **d**))*
Soit $p : L \to L/Ax$ la surjection canonique. Soient $(d, y) \in A \times L$ tel que $x = dy$. Il s'ensuit alors que

$$dp(y) = p(dy) = p(x) = 0 .$$

Or $x \neq 0$, donc $d \neq 0$. Il s'ensuit, L/Ax étant sans torsion, que $p(y) = 0$ i.e. $y \in Ax$. Il existe donc $u \in A$ tel que $y = ux$, d'où il découle que

$$y = duy \Leftrightarrow y(1 - du) = 0 .$$

Or

$$x \neq 0 \Rightarrow y \neq 0$$

et comme L est libre, donc sans torsion,

$$1 - du = 0$$

c'est-à-dire que d est inversible.

*vii) (**d**) $\Rightarrow$ **e**))*
Laissé en exercice.

Remarque C.1.2 L'hypothèse, *libre de type fini* faite sur L dans le lemme C.1.1, n'est pas indispensable pour montrer l'équivalence entre C.1.1.a) et C.1.1.b). Il suffit de supposer que L est sans torsion.

Définition C.1.3 (Vecteur primitif) Si $x \in L$ vérifie les assertions équivalentes du lemme C.1.1, on dit que x est un *vecteur primitif* du A-module libre de type fini L.

Corollaire C.1.4 *Soient L un A-module libre de type fini et de rang r,*

$$\lambda_{i\ ,1\leq i\leq r} \text{ une base de } L\ ,\ a_{i\ ,1\leq i\leq n} \in A\ ,\ \text{ premiers entre eux dans leur ensemble,}$$

alors il existe une base de l dont

$$\sum_{i=1}^{r} a_i\lambda_i \text{ est le premier vecteur } .$$

Remarque C.1.5 Soit $M \subset L$ un couple de A-module libres de type fini possédant une base adaptée

$$\left(\lambda_{i\ ,1\leq i\leq r}\ , d_{i\ ,1\leq i\leq s}\right)_{,s\leq r} \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i \text{ . (cf. C.0.1 ,)}$$

Soit $f : L \to A$ un morphisme de A-modules, *i.e.* une forme linéaire dans ce cas particulier (cf. A.2.13.) Alors pour tout $x \in M$, $d_s|f(x)$. En effet, $x \in M$ si et seulement si

$$\exists a_{i\ ,1\leq i\leq s} \in A,\ x = \sum_{i=1}^{s} a_i d_i \lambda_i\ ;$$

ce qui entraîne que

$$f(x) = \sum_{i=1}^{s} a_i d_i f(\lambda_i) .$$

Or, par définition de la base adaptée

$$\left(\lambda_{i\ ,1\leq i\leq r}\ , d_{i\ ,1\leq i\leq s}\right)_{,s\leq r} \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i,$$

$$\forall 1 \leq i \leq s,\ d_s | d_i$$

d'où il résulte que $d_s | f(x)$.

L'élément d_s est donc un minorant de l'ensemble $E := \{f(x), x \in M\ ,\ f \in L^*\}$. C'est même un plus petit élément puisque la forme linéaire f définie sur L par

$$f(\lambda_s) := 1\ ,\ \forall 1 \leq i \leq r,\ i \neq s\ ,\ f(\lambda_i) := 0,$$

vérifie $f(d_s \lambda_s) = d_s$.

L'élément $d_s \in E$ est en particulier un élément minimal pour la divisibilité. Cela signifie que pour tout $a \in E$, si $a | d_s$, alors $d_s | a$ *i.e.* d_s et a sont associés (à défaut d'être égaux.) Bien, entendu, qui peut le plus peut le moins, et être un plus petit élément entraîne bien évidemment d'être un élément minimal pour la divisibilité. En revanche il est techniquement possible de montrer que E possède des éléments minimaux pour la divisibilité, quand il serait nettement plus délicat de montrer qu'il possède un plus petit élément. Finalement l'existence d'élément minimaux pour la divisibilité, plus facile à atteindre que celle de plus petit élément, sera suffisante pour la construction que nous avons en vue dans ce paragraphe.

Proposition C.1.6 *Soient $M \subset L$ des A-modules et*

$$E := \{f(x)\ ,\ x \in M\ ,\ f \in L^*\}\ .$$

Alors E est un sous-ensemble de A possédant des éléments minimaux pour la divisibilité.

Preuve *: Pour tout $f \in L^*$, $f(M)$ est un sous-A-module de A, c'est-à-dire un idéal de A. Choisissons un élément $f_0 \in L^*$. L'idéal $\mathfrak{I}_0 := f_0(M)$ est principal et donc engendré par un élément $f_0(x_0)$, $x_0 \in M$.*

Si $f_0(x_0)$ n'est pas minimal dans E, il existe $\{f_1\} L^*$ et $x \in M$ tels que $f_1(x)$ divise strictement $f_0(x_0)$; autrement dit $f_1(x) | f_0(x_0)$ et $f_1(x)$ et $f_0(x_0)$ ne sont pas associés ou encore n'engendrent pas le même idéal. Il existe alors $x_1 \in M$ tel que

$$\mathfrak{I}_1 := f_1(M) = A f_1(x_1)\ .$$

Si $f_0(x_0)$ est minimal on pose $\mathfrak{I}_1 := \mathfrak{I}_0$.

On peut ainsi construire, par récurrence, une suite $\left(\mathfrak{I}_n\right)_{,n \in \mathbb{N}}$ d'idéaux : supposant construits

$$\mathfrak{I}_{k\ ,0 \leq k \leq n} \text{ des idéaux tels que } \mathfrak{I}_k = A f_k(x_k)\ ,\ f_k \in L^*\ ,\ x_k \in M,$$

avec $\mathfrak{I}_k \subset \mathfrak{I}k + 1$ et $\mathfrak{I}_{k+1} = \mathfrak{I}_k$ si et seulement si $f_k(x_k)$ est minimal dans E. Alors si $f_n(x_n)$ est minimal dans E, on pose

$$f_{n+1} := f_n\ ,\ x_{n+1} := x_n \text{ et } \mathfrak{I}_{n+1} := \mathfrak{I}_n\ .$$

Sinon il existe $f_{n+1} \in L^*$ et $x \in M$, tel que $f_{n+1}(x)$ divise strictement $f_n(x_n)$ et l'on posera alors

$$\mathfrak{I}_{n+1} := f_{n+1}(M)\ .$$

On constate qu'alors

$$f_{n+1}(x_{n+1}) | f_{n+1}(x) | f_n(x_n)$$

ce qui entraîne

$$\mathfrak{I}_n \subset \mathfrak{I}_{n+1}$$

l'inclusion étant stricte dès que $f_{n+1}(x)$ divise strictement $f_n(x_n)$.

La suite $\left(\mathfrak{I}_n\right)_{,n \in \mathbb{N}}$ ainsi construite est donc une suite croissante d'idéaux. Alors :

Lemme C.1.6.1 *La suite $\left(\mathfrak{I}_n\right)_{,n \in \mathbb{N}}$ est stationnaire à partir d'un certain rang, c'est-à-dire qu'il existe $\ell \in \mathbb{N}$ tel que pour tout $m \geq \ell$, $\mathfrak{I}_m = \mathfrak{I}_\ell$.*

La manière dont on a construit $\left(\mathfrak{I}_n\right)_{,n \in \mathbb{N}}$ assure alors que $f_\ell(x_\ell)$ est minimal dans E.

***Preuve** (**du lemme C.1.6.1**): C'est un cas particulier de la proposition B.1.5 et un résulta qu'on a déjà établi en I.13.5.2.*

On peut encore justifier ce résultat en constatant que, la suite $\left(\mathfrak{I}_n\right)_{,n\in\mathbb{N}}$ étant croissante

$$\mathfrak{I} := \bigcup_{n\,\in\,\mathbb{N}} \mathfrak{I}_n$$

est un idéal. Comme A est principal, il existe $a \in A$ tel que $\mathfrak{I} = Aa$. Or il existe $n \in \mathbb{N}$, tel que $a \in \mathfrak{I}_n$. Il en résulte, puisque $\mathfrak{I}_n$ est un idéal, que $\mathfrak{I} \subset \mathfrak{I}_n$. On a donc

$$\forall \ell \in \mathbb{N},\ \ell \geq n, \mathfrak{I}_n \subset \mathfrak{I}_\ell \subset \mathfrak{I} \subset \mathfrak{I}_n\ .$$

Lemme C.1.7 *Soient $M \subset L$ des A-modules,*

$$E := \{f(x)\ ,\ x \in M\ ,\ f \in L^*\}$$

et $(f, x) \in L^* \times M$ tel que $d := f(x)$ est minimal dans E.

i) Pour tout $g \in L^*$,

$$f(x)|g(x)\ .$$

***Preuve** : L'ensemble*

$$\mathfrak{J} := \{g(x)\ ,\ g \in L^*\}$$

est un idéal de A. En effet, pour tout couple $(g, h) \in L^* \times L^*$ de formes linéaires sur L, et tout couple $(a, b) \in A \times A$, $ag + bh$ est encore une forme linéaire sur L et

$$(ag + bh)(x) = ag(x) + bh(x)$$

ce qui prouve, $\mathfrak{J}$ étant non vide ($f(x) \in \mathfrak{J}$,) que $\mathfrak{J}$ est un idéal de A. Puisque A est principal, il existe un élément

$$g(x)\ ,\ (g, x) \in L^* \times M \text{ tel que } \mathfrak{J} = Ag(x)\ .$$

Or si $g(x)$ divise strictement $f(x)$ la minimalité de $f(x)$ est contredite. $f(x)$ et $gg(x)$ sont donc associés i.e. $f(x)$ est générateur de $\mathfrak{J}$.

ii) Pour tout $y \in M$,

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

***Preuve** : L'ensemble*

$$\mathfrak{I} := \{f(y)\ ,\ y \in M\},$$

est un idéal de A qui n'est autre que $f(M)$. On a en fait déjà établi dans la preuve de la proposition C.1.6 que $f(x)$ est un générateur de $\mathfrak{I}$. Cependant si $f(y)$ est un générateur de $\mathfrak{I}$, ($\mathfrak{I}$ est principal,) alors $f(y)|f(x)$. Mais $f(y)$ ne peut diviser strictement $f(x)$ sans quoi ce dernier ne serait pas minimal dans E.

iii) Si L est libre de type fini et $M \neq \{0\}$, il existe $y \in L$ tel que $x = dy$ et par conséquent $f(y) = 1$, y est un vecteur primitif au sens de C.1.3.

***Preuve** : Soit $\lambda_{i\ ,1\leq i\leq r}$ une base de L. Pour tout $1 \leq i \leq r$ notons*

$$\lambda_i^* \ : \ L \ \to \ A \ , \ \lambda_j \ \mapsto \ \delta_i^j$$

qu'on pourrait appeler la base dual de $\lambda_{i\ ,1\leq i\leq r}$ moyennant de vérifier que c'est bien une base de L^* (ce qui n'est pas forcément nécessaire pour prouver ce lemme.)

On peut écrire

$$x \ = \ \sum_{i=1}^{r} x_i \lambda_i \ , \ x_{i\ ,1\leq i\leq r} \ \in \ A \ .$$

Il vient alors

$$\forall 1 \leq i \leq r, \ \lambda_i^*(x) \ = \ x_i$$

et par conséquent

$$x \ = \ \sum_{i=1}^{r} \lambda_i^*(x) \lambda_i \ .$$

Or d'après le point i),

$$\forall 1 \leq i \leq r, \ d | \lambda_i^*(x) \ .$$

Il existe donc

$$y_{i\ ,1\leq i\leq r} \ \in \ A \text{ tel que } \forall 1 \leq i \leq r, \ x_i \ = \ \lambda_i^*(x) \ = \ dy_i \ .$$

En posant

$$y \ := \ \sum_{i=1}^{r} y_i \lambda_i,$$

on a bien évidemment $x = dy$.

Si $M \neq \{0\}$, $d \neq 0$, (il existe au moins une forme linéaire prenant une valeur non nul sur M, l'un des λ_i^* en particulier.) On a alors

$$d \ = \ f(x) \ = \ f(dy) \ = \ df(y)$$

qui entraîne, puisque A est intègre

$$f(y) \ = \ 1 \ .$$

Théorème C.1.8 (de la base adaptée) *Soit $M \subset L$ un couple de A-modules avec L libre de type fini et de rang $r \in \mathbb{N}$.*

1) Il existe une base adaptée

$$\left(\lambda_{i\ ,1\leq i\leq r} \ , d_{i\ ,1\leq i\leq s}\right)_{,s\leq r} \forall 1 \leq i \leq s-1, \ d_{i+1} | d_i$$

pour $M \subset L$.

2) Les données $(s, d_{i\ ,1\leq i\leq s})$ sont uniquement (à association près) déterminées par les facteurs invariants du module quotient L/M.

Preuve : *Le point 2) n'est autre que le corollaire II.11.4.*

Nous allons prouver l'existence d'une base adaptée par récurrence sur le rang r de L.

$r = 0$ $L = M = \{0\}$, et le résultat est établi.

— *Soient $r \in \mathbb{N}$, L de rang $r+1$ et $M \subset L$. Si $M = \{0\}$, $\emptyset$ est la seule base de M et le résultat est établi.*

Si $M \neq \{0\}$, notons

$$E := \{f(x)\,,\ f \in L^*\,,\ x \in M\}\,.$$

D'après la proposition C.1.6, E possède un élément minimal

$$d = f(x)\,,\ f \in L^*\,,\ x \in M\,.$$

Il résulte alors du lemme C.1.7.iii) qu'il existe $y \in L$ tel que $x = dy$ et tel que y soit un vecteur primitif (cf. C.1.3.)

Remarquons alors que $f : L \to A$ est surjective et qu'en notant $K := \mathrm{Ker}\, f$ son noyau, on dispose d'une suite exacte courte :

$$0 \to K \longrightarrow L \xrightarrow{f} A \to 0\,.\ \textit{(cf. C.1.1.iii) .)}$$

On dispose même d'une section

$$\sigma : A \to L\,,\ a \mapsto ay\,.$$

Il en résulte que :

$$L = Ay \oplus K\,. \qquad \textit{C.1.8.1}$$

Le lemme qui suit permet de terminer la preuve :

Lemme C.1.8.2

$$M = Ax \oplus (M \cap K)\,.$$

Or on sait, puisque y est un vecteur primitif, que K est un A-module libre de rang r. En posant $N := M \cap K$, on peut faire l'hypothèse de récurrence que $N \subset K$ possède une base adaptée

$$\left(\kappa_i\,,_{1\leq i\leq r}\,, d_i\,,_{1\leq i\leq s}\right),_{s\leq r}\ ,\ \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i\,.$$

Alors $(\kappa_i\,,_{1\leq i\leq r}\,, y)$ est une base de L. En posant :

$$\begin{array}{lrcl} \forall 1 \leq i \leq s, & \lambda_i & := & \kappa_i \\ & \lambda_{s+1} & := & y \\ & d_{s+1} & := & d \\ \forall s+2 \leq i \leq r+1, & \lambda_i & := & \kappa_{i-1'} \end{array}$$

on a construit une base adaptée pour $M \subset L$ moyennant de montrer que :

Lemme C.1.8.3

$$d = d_{s+1}|d_s\ ;$$

***Preuve** (**du lemme C.1.8.2**): Montrons d'abor que*

$$\sigma \circ f \ : \ M \ \to \ Ax$$

est un projecteur (surjectif[6].) En effet on a bien $(\sigma \circ f)^2 \ = \ \sigma \circ f$. *Par ailleurs il découle du lemme C.1.7.ii) que,*

$$\forall z \in M, \ f(x) \ = \ d|f(z)$$

d'où il découle que

$$\sigma[f(z)] \ \in \ Ady \ = \ Ax \ .$$

Comme par ailleurs $x \ \in \ M$ *et* $\sigma[f(x)] \ = \ X$, *on en déduit que*

$$\sigma[f(M)] \ = \ Ax \ .$$

Le lemme I.9.8 permet de conclure.

Preuve** (**du lemme C.1.8.3**): Notons* $e \ := \ d_{s+1} \ \wedge \ d_s$ *un* ***Pgcd*de* $d \ = \ d_{s+1}$ *et* d_s. *Il existe donc un couple de coefficients de* BÉZOUT $(u, v) \ \in \ A \times A$ *tel que*

$$d_{s+1}u \ + \ d_s v \ = \ e \ , \ e|d \text{ et } e|d_s \ .$$

Par construction

$$d_s\lambda_s \ \in \ M \text{ et } d_{s+1}\lambda_{s+1} \ \in \ M$$

d'où

$$d_{s+1}u\lambda_{s+1} \ + \ d_s v\lambda_s \ \in \ M \text{ et } \lambda^*_{s+1} + \lambda^*_s \ \in \ L^* \ .$$

Or :

$$\begin{array}{rcl}(\lambda^*_{s+1} + \lambda^*_s)(d_{s+1}u\lambda_{s+1} + d_s v\lambda_s) & = & \lambda^*_{s+1}(d_{s+1}u\lambda_{s+1} + d_s v\lambda_s) + \lambda^*_s(d_{s+1}u\lambda_{s+1} + d_s v\lambda_s) \\ & = & d_{s+1}u\lambda^*_{s+1}(\lambda_{s+1}) + d_s v\lambda^*_s(\lambda_s) \\ & = & d_{s+1}u + d_s v \\ & = & e \ .\end{array}$$

Il en résulte que $e \ \in \ E$. *Par minimalité de* d, $e|d$ *entraîne* $d|e$, *et comme* $e|d_s$, *il vient finalement*

$$d|d_s \ .$$

Remarque C.1.9 Le cas où $\mathrm{rg}(L) \ = \ 1$ dans le théorème C.1.8 ci-dessus était déjà traité dans le lemme II.4.1. On n'en a cependant pas besoin pour l'argument de récurrence. On constatera d'ailleurs que la preuve du théorème C.1.8 consiste à affiner celle du théorème II.4.6.

6. C'est le genre d'argument qu'on a déjà donné dans la preuve de la proposition I.9.9 par exemple.

C.2 . –Une autre preuve du théorème de la base adaptée C.1.8

Étant donné un A-module Q de type fini et de torsion on peut montrer (cf. B.7.4q)u'il existe des A-modules libres de type fini tels qu'on ait une suite exacte

$$0 \to M \longrightarrow L \longrightarrow Q \to 0$$

où Q apparaît comme le quotient L/M. La proposition II.11.3 assure alors que si l'on connaît une base adaptée

$$\left(\lambda_{i\ ,1\leq i\leq r}\ , d_{i\ ,1\leq i\leq s}\right)_{,s\leq r} \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i$$

de $M \subset L$, les $d_{i\ ,1\leq i\leq s}$ sont des générateurs des facteurs invariants de Q. Le théorème C.1.8 donne donc une preuve alternative de l'énoncé d'existence B.6.13.1) par un procédé différent.

On peut donc légitimement se demander si l'on ne peut pas à l'inverse établir l'existence d'une base adaptée pour un couple $M \subset L$ avec L libre de type fini, connaissant le théorème de structure des A-modules de type fini et de torsion B.6.13. C'est ce que nous allons montrer dans ce paragraphe, à titre de curiosité certes, parce qu'il n'est pas totalement indispensable de disposer de plusieurs preuves d'un même résultat. D'autant que le paragraphe II.11 peut tout à fait lui-même donner une preuve algorithmique du théorème C.1.8.

Notation C.2.1 Dans la suite L est un A-module libre de type fini (cf. II.3.2,) et M un sous-A-module de L. On note $Q := L/M$, le quotient de L par M si bien qu'on a une suite exacte courte :

$$0 \to M \xrightarrow{i} L \xrightarrow{q} Q \to 0 \qquad \text{C.2.1.1}$$

(où $i := \mathrm{Id}_{L|M}$ et $q : L \to L/M$ est la surjection canonique.)

Notons

$$r := \mathrm{rg}(L) \in \mathbb{N}\,.$$

Lemme C.2.2 *Si $Q \cong A/d$ est cyclique, il existe une base $\lambda_{i\ ,1\leq i\leq r}$ de L telle que $q(\lambda_1)$ est un élément inversible de l'anneau A/d.*

Preuve *: Puisque $q : L \to Q$ est surjectif, il existe $\xi \in L$ tel que $q(\xi) = 1_{A/d}$. Dans une base $\mu_{i\ ,1\leq i\leq r}$ de L, ξ s'écrit*

$$\xi = \sum_{i=1}^{r} x_i\mu_i\ .$$

*Soient a un **Pgcd** des x_i,*

$$y_{i\ ,1\leq i\leq r} \text{ tel que } \forall 1 \leq i \leq r,\ x_i = ay_i \text{ et } \eta := \sum_{i=1}^{r} y_i\mu_i\ .$$

Il s'ensuit que $\xi = a\eta$, ce qui entraîne

$$1_A/d = q(\xi) = aq(\eta)\,. \qquad \text{C.2.2.1}$$

Les coordonnées de η dans la base $\mu_{i\ ,1\leq i\leq r}$ sont première entre elles dans leur ensemble ce qui entraîne (cf. C.1.4,) que η peut être complété en une base

$$(\lambda_1 := \eta, \lambda_2, \ldots, \lambda_r) \text{ de } L\ .$$

L'égalité C.2.2.1 assure bien que $q(\lambda_1)$ est inversible dans A/d.

Lemme C.2.3 *Le A-module $Q \cong A/d$ étant toujours cyclique et la base $\lambda_{i\ ,1\leq i\leq r}$ étant construite comme dans le lemme C.2.2 :*

i)

$$\forall 2 \leq i \leq r,\ \exists a_i \in A,\ \mu_i := \lambda_i - a_i\lambda_1 \in M\ .$$

Preuve *: Puisque $q(\lambda_1)$ est inversible dans A/d,*

$$\forall 2 \leq i \leq r,\ \exists a_i \in A,\ q(\lambda_i) = a_i q(\lambda_1)$$

Il s'ensuit que

$$\forall 2 \leq i \leq r,\ q(\lambda_i - a_i\lambda_1) = 0 \Leftrightarrow \lambda_i - a_i\lambda_1 \in M\ .$$

ii) En posant $\mu_1 := \lambda_1$, $\mu_{i\ ,1\leq i\leq r}$ est une base de L.
Il existe donc une base $\mu_{i\ ,1\leq i\leq r}$ de L, telle que $q(\mu_1)$ est inversible dans A/d et

$$\forall 2 \leq i \leq r,\ \mu_i \in M\ .$$

Preuve *: La famille $\mu_{i\ ,1\leq i\leq r}$ est libre : Soit $b_{i\ ,1\leq i\leq r} \in A$,*

$$\begin{aligned} & \sum_{i=1}^{r} b_i\mu_i = 0 \\ \Leftrightarrow \quad & (b_1 - \sum_{i=2}^{r} b_i a_i)\lambda_1 + \sum_{i=2}^{r} b_i\lambda_i = 0\ . \end{aligned}$$

Puisque $\lambda_{i\ ,1\leq i\leq r}$ est une famille libre, on en déduit que

$$\forall 2 \leq i \leq r,\ b_i = 0 \text{ et } (b_1 - a\sum_{i=2}^{r} b_i a_i) \Rightarrow \forall 1 \leq i \leq r,\ b_i = 0\ .$$

La famille $\mu_{i\ ,1\leq i\leq r}$ est manifestement génératrice de L.

Lemme C.2.4 *Si $Q \cong A/d$ est cyclique, la base $\mu_{i\ ,1\leq i\leq r}$ construite au lemme C.2.3 est adaptée (cf. C.0.1,) pour $M \subset L$.*

Preuve *: Pour tout $\xi \in M$, on écrit*

$$\xi = \sum_{i=1}^{r} x_i\mu_i\ .$$

Or :

$$\begin{aligned} 0 &= q(\xi) \\ &= \sum_{i=1}^{r} x_i q(\mu_i) \\ &= x_1 q(\mu_1)\ . \end{aligned}$$

Or $q(\mu_1)$ est inversible dans l'anneau A/d, si bien que

$$x_1 q(\mu_1) = 0 \Rightarrow d|x_1\ .$$

Il en résulte que $(d\mu_1, \mu_2, \ldots, \mu_r)$ est une base de M ce qui prouve que $\mu_{i\ ,1\leq i\leq r}$ est adaptée à $M \subset L$.

Proposition C.2.5 *On suppose que le module $Q = L/M$ dans la suite exacte C.2.1.1 est de torsion. Comme L est de type fini, Q est également de type fini et l'on a :*

$$Q \cong A/d_1 \times \ldots \times A/d_{s+1}$$

où les d_i ,$1 \leq i \leq s+1$ sont des générateurs des facteurs invariants donnés par le théorème B.6.13.

Écrivons une suite exacte :

$$0 \to R \xrightarrow{j} Q \xrightarrow{t} A/d_1 \to 0 \qquad \text{C.2.5.1}$$

où l'on a naturellement

$$R \cong \prod_{i=2}^{s+1} A/d_i \, . \qquad \text{C.2.5.2}$$

i) Soit $P := q^{-1}[j(R)]$. La restriction

$$p := q_{|P} : P \to R \text{ de } q \text{ à } P$$

est un morphisme surjectif de noyau M. On obtient un diagramme à lignes et colonnes exactes :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M & \xrightarrow{\mathrm{Id}_{L|M}} & P & \xrightarrow{p} & R & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_M}\downarrow & & {\scriptstyle \mathrm{Id}_{L|P}}\downarrow & & \downarrow{\scriptstyle j} & & \\
0 & \to & M & \xrightarrow{i} & L & \xrightarrow{q} & Q & \to & 0 \\
 & & {\scriptstyle 0}\downarrow & & {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle t} & & \\
 & & 0 & \to & A/d & \cong & A/d & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \qquad 1$$

Preuve *: Le corrollaire I.8.16 assure que la suite horizontale du haut est exacte. Lisomorphisme en bas à droite entre les quotients est donné par le corollaire I.8.15.*

ii) Il existe une décomposition

$$L = H \oplus D \, , \; P = H \oplus d_1 D \, .$$

Preuve *: On l'obtient en appliquant le lemme C.2.4 à la suite verticale du centre dans le diagramme i).1.*

iii) Si on pose

$$K := M \cap H \text{ alors } M = K \oplus d_1 D \, .$$

Preuve : *On a* $d_1Q = 0$. *Notons* δ *une base de* D. *Alors*

$$q(d_1\delta) = d_1 q(\delta) = 0$$

c'est-à-dire que

$$d_1\delta \in \operatorname{Ker} q = M .$$

Pour tout $\xi \in M$, *puisque* $\xi \in P$, *il existe un unique couple* $(\psi, \eta) \in d_1D \times H$ *tel que* $\xi = \psi + \eta$. *Or*

$$\eta = \xi - \psi \Rightarrow \eta \in M$$

si bien que

$$\eta \in K = H \cap M .$$

iv) On a une suite exacte :

$$0 \to K \longrightarrow H \longrightarrow R \to 0 . \qquad 1$$

Preuve : *Les décompositions*

$$P = H \oplus d_1D \text{ (cf. ii) ,)}$$

et

$$M = K \oplus d_1D \text{ (cf. iii) ,)}$$

ainsi que la suite horizontale du haut dans le diagramme i).1, donnent un diagramme à lignes et colonnes exactes dans lequel les deux colonnes de gauche sont scindées :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & K & \longrightarrow & H & \xrightarrow{v} & S & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_{M\,|\,K}}\downarrow & & {\scriptstyle \mathrm{Id}_{P\,|\,H}}\downarrow & & \downarrow{\scriptstyle w} & & \\
0 & \to & M & \xrightarrow{\mathrm{Id}_{L\,|\,M}} & P & \xrightarrow{p} & R & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & d_1D & \cong & D_1D & \to & 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Puisque $K \subset M = \operatorname{Ker} p$, p *se factorise à travers* $S := H/K$, *ce qui donne le morphisme* $w : S \to R$ *vérifiant* $w \circ v = p$. *Cette dernière condition, entraînant, puisque* p *est surjectif, que* w *l'est aussi. Puisque le morphisme sur la ligne du bas du diagramme ci-dessus est un isomorphisme, le lemme du serpent assurerait automatiquement que* w *est injectif. Cependant on peut le montrer « à la main » : En effet, pour tout* $\xi \in S$, *il existe* $\psi \in H$ *tel que* $\xi = v(\psi)$. *Alors* $w(\xi) = 0$, *équivaut à*

$$w[v(\psi)] = 0$$

qui équivaut encore à $p(\psi) = 0$. *Il s'ensuit que*

$$\psi \in \operatorname{Ker} p = M .$$

Or $\psi \in H$, *d'où*

$$\psi \in K = M \cap H$$

i.e.

$$\xi \;=\; v(\psi) \;=\; 0\,.$$

On en déduit que

$$w \;:\; S \;\cong\; R$$

ce qui donne la suite exacte demandée.

v) Le couple $M \subset L$ possède une base adaptée (cf. C.0.1.)

***Preuve** : On raisonne par récurrence sur le nombnre de facteurs invariants du quotient $Q = L/M$.*

Dans le cas où Q n'a qu'un facteur invariant, i.e. est cyclique le résulta est le lemme C.2.4.

Si on suppose L de rang $r+1$, puisque $L/P \cong A/d$ (cf. i).1,) il découle de la proposition II.7.9 et même du lemme II.7.7 que $\mathrm{rg}(P) = \mathrm{rg}(L) = r+1$. Il découle alors de la décomposition ii)

$$P \;=\; H \;\oplus\; d_1 D$$

que $\mathrm{rg}(H) = r$.

Pour $s \in \mathbb{N}$, si Q a $s+1$, facteurs invariants, le A-module R défini en C.2.5.2 a s facteurs invariants. L'hypothèse de récurrence appliquée à la suite exacte construite en iv).1 permet de construire une base $\lambda i 2r+1$ de H tels que $(d_2\lambda_2, \ldots, d_{s+1}\lambda_{s+1})$ soit une base de K.

Soit alors λ_1 une base de D, la décomposition

$$L \;=\; D \;\oplus\; H \text{ (cf. ii) ,)}$$

assure que λ_i ,$1 \leq i \leq r+1$ est une base de L.

Enfin la décomposition

$$M \;=\; d_1 d \;\oplus\; K \text{ (cf. iii) ,)}$$

assure que

$$(d_1\lambda_1, d_2\lambda_2, \ldots, d_{s+1}\lambda_{s+1}$$

est une base de M.

Proposition C.2.6 *Dans le cas général i.e. où Q est quelconque (de type fini bien sûr) mais pas nécessairement de torsion, on a une décomposition de Q en partie libre et partie de torsion donnée par le théorème B.1.4 :*

$$0 \;\to\; \mathrm{Tor}(Q) \xrightarrow{\;j\;} Q \xrightarrow{\;\ell\;} \mathcal{L}(Q) \;\to\; 0 \qquad \textit{C.2.6.1}$$

(où $\mathrm{Tor}(Q)$ est de torsion et $\mathcal{L}(Q)$ est libre.)

On note enfin :

$$P \;:=\; q^{-1}[j(\mathrm{Tor}(Q))]\;,\; p \;:=\; q_{|P} \;:\; P \;\to\; \mathrm{Tor}(Q)\,. \qquad \textit{C.2.6.2}$$

i) On a alors le diagramme à lignes et colonnes exactes suivant :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M & \xrightarrow{\mathrm{Id}_{L|P}} & P & \xrightarrow{\;p\;} & \mathrm{Tor}(Q) & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_N}\downarrow & & {\scriptstyle \mathrm{Id}_{L|P}}\downarrow & & \downarrow{\scriptstyle j} & & \\
0 & \to & M & \xrightarrow{\;i\;} & L & \xrightarrow{\;q\;} & Q & \to & 0 \\
 & & \downarrow & & {\scriptstyle k}\downarrow & & \downarrow{\scriptstyle \ell} & & \\
 & & 0 & \to & \mathcal{L}(Q) & \cong & \mathcal{L}(Q) & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \qquad \textit{1}$$

Preuve : *Le corrollaire I.8.16 assure que la suite horizontale du haut est exacte. Lisomorphisme en bas à droite entre les quotients est donné par le corollaire I.8.15.*

ii) Le couple $M \subset L$ *a une base adaptée (cf. C.0.1.)*

Preuve : *La suite exacte verticale centrale dans le diagramme i).1 est scindée puisque le dernier terme* $\mathcal{L}(Q)$ *est libre de type fini. On peut donc écrire*

$$L = P \oplus \mathcal{L}(Q) .$$

Or dans la suite exacte horizontale du diagramme i).1, le quotient $P/M \cong \mathrm{Tor}(Q)$ *est de torsion, ce qui permet d'appliquer le résultat C.2.5.v) qui donne une base adaptée pour le couple* $M \subset P$*. Elle ce complète (en prenant une base arbitraire de* $\mathcal{L}(Q)$*) en une base adaptée pour* $M \subset L$*.*

D . −Rappels sur les formes linéaires alternées et les déterminants

Ce paragraphe a essentiellement pour but de rappler certaines notations et convention concernant les déterminants permettant d'en user librement dans le paragraphe IV.6 consacré à l'étude du polynôme caractéristique d'un endomorphisme. La plupart des résultats rappelés ici est certainement connue du lecteur, aussi les preuves ont-elles été omises. **Dans toute cette section, E est un $\mathbb{K}$-espace vectoriel de dimension finie $d \in \mathbb{N}^*$, où $\mathbb{K}$ est un corps de caractéristique différente de 2. On note $\mathcal{S}_d$ le groupe des permutations sur l'ensemble $[1;d] \subset \mathbb{N}$.**

Définition D.1 (Forme d-linéaire alternée) On appelle *forme d-linéaire alternée* sur E une application

$$f \,:\, E^d \,:=\, E \times \ldots \times E \,\to\, \mathbb{K}\,,$$

telle que pour tout d-uplet $(v_1,\ldots,v_d)$ d'éléments de E, tout entier $1 \,\leq\, i \,\leq\, d$, tout élément $v'_{i\,\in\,E}$ et tout couple $(\lambda,\lambda') \,\in\, \mathbb{K}\times\mathbb{K}$,

$$f(v_1,\ldots,\lambda v_i+\lambda' v'_i,\ldots,v_d) \,=\, \lambda f(v_1,\ldots,v_i,\ldots,v_d) \,+\, \lambda' f(v_1,\ldots,v'_i,\ldots,v_d)\,; \qquad \text{D.1.1}$$

et pour toute permutation $s \,\in\, \mathcal{S}_d$,

$$f(v_{s(1)},\ldots,v_{s(d)}) \,=\, \sigma(s) f(v_1,\ldots,v_d)\,, \qquad \text{D.1.2}$$

(où $\sigma(s)$ désigne la signature de la permutation s.)

On notera $\mathcal{A}^d\,E$ l'ensemble des formes d-linéaires alternées sur E.

Remarque D.2 Si $d \,=\, 1$, on remarque immédiatement que

$$\mathcal{A}^d\,E \,\cong\, E^*\,.$$

On supposera, dans toute la suite de ce paragraphe (D), que $d \geq 2$.

Lemme D.3 *Soit $f \,\in\, \mathcal{A}^d\,E$, et $(v_1,\ldots,v_d)$ un d-uplet d'éléments de E tel qu'il existe $1 \leq i < j \leq d$ tels que $v_i \,=\, v_j$. Alors*

$$f(v_1,\ldots,v_d) \,=\, 0\,.$$

Proposition D.4 *L'ensemble $\mathcal{A}^d\,E$ est un $\mathbb{K}$-espace vectoriel et*

$$\dim_{\mathbb{K}} \mathcal{A}^d\,E \,=\, 1\,. \qquad \textit{D.4.1}$$

Proposition D.5 *Étant donnés deux $\mathbb{K}$-espaces vectoriels E et F de même dimension d, on note*

$$\mathcal{A}^d \,:\, \mathrm{Hom}_{\mathbb{K}}(E,F) \,\to\, \mathrm{Hom}_{\mathbb{K}}(\mathcal{A}^d\,F,\mathcal{A}^d\,E)$$

l'application définie par $u \mapsto \mathcal{A}^d\,(u)$ où

$$\forall f \in \mathcal{A}^d\,F,\ \forall (v_1,\ldots,v_d) \in E^d,\ [(\mathcal{A}^d\,(u))(f)](v_1,\ldots,v_d) \,:=\, f(u(v_1),\ldots,u(v_d))\,, \qquad \textit{D.5.1}$$

ii) Cette application vérifie pour E,F,G des $\mathbb{K}$-espaces vectoriels de même dimension d et

$$u \,:\, E \,\to\, F\,,\ v \,:\, F \,\to\, G \text{ des morphismes :}$$
$$\mathcal{A}^d\,(v\circ u) \,=\, \mathcal{A}^d\,(u) \,\circ\, \mathcal{A}^d\,(v)\,.$$

iii) Avec les notations précédentes, si v est l'inverse de u, alors $\mathcal{A}^d(u)$ est inversible et

$$\mathcal{A}^d(v) \;=\; \mathcal{A}^d(u)^{-1}\,.$$

iv) Pour tout morphisme $u : E \to F$, $\mathcal{A}^d(u)$ est un morphisme (application linéaire) de $\mathcal{A}^d F$ dans $\mathcal{A}^d E$.

Remarque D.6 On pourrait simplement noter $\mathcal{A}^d(u) = f \circ u$ si cette notation n'était abusive pour $d \neq 1$, et si cela ne pouvait conduire à des confusions. Cette notation peut cependant aider à comprendre le comportement de $\mathcal{A}^d(u)$ vis-à-vis de la composition et de l'inverse notamment, très analogue à celui de u^* .

En revanche, il faut bien prendre garde au fait que en général $\mathcal{A}^d(u+v) \neq \mathcal{A}^d(u) + \mathcal{A}^d(v)$!

Définition D.7 (Déterminant d'un endomorphisme) Pour tout

$$u : E \to F \text{ avec } \dim E = \dim F = d,$$

on appelle *déterminant de u* l'application

$$\mathcal{A}^d(u) : \mathcal{A}^d F \to \mathcal{A}^d E\,.$$

Proposition D.8 *i) Si $u : E \to E$ est un endomorphisme alors $\mathcal{A}^d(u)$ est un endomorphisme de $\mathcal{A}^d E$ qui est de dimension 1. L'application $\mathcal{A}^d(u)$ est donc une homothétie uniquement caractérisée par son rapport $k \in \mathbb{K}$. Le scalaire k est aussi appelé déterminant de u et noté $\det(u)$.*

ii) Si u et v sont des endomorphismes de E la proposition D.5.ii) a pour conséquence que

$$\det(v \circ u) \;=\; \det(u)\det(v) \;=\; \det(u \circ v)\,.$$

De même, la proposition D.5.iii) a pour conséquence que, si u est un automorphisme de E (i.e. un endomorphisme inversible,)

$$\det(u^{-1}) \;=\; (\det(u))^{-1}\,.$$

Il s'ensuit que la restriction de l'application $\det(\cdot)$ au groupe linéaire $\mathrm{GL}(E)$ définit un morphisme à valeurs dans le groupe $(\mathbb{K}^\times, *)$.

Remarque D.9 Attention : Il faut bien noter que le déterminant d'un endomorphisme u de E est indépendant du choix de toute base sur E.

Définition D.10 (Déterminant d'un système de vecteurs) Une base

$$(e_1, \ldots, e_d) \text{ de } E \text{ étant fixée,}$$

à tout d-uplet $(v_1, \ldots, v_d)$ de vecteurs de E, on peut associer un unique endomorphisme u de E défini par :

$$u(e_i) \;:=\; v_i\,,\, 1 \leq i \leq d\,.$$

On appellera *déterminant du système de vecteurs* $(v_1, \ldots, v_d)$ dans la base $(e_1, \ldots, e_d)$ et on notera

$$\det_{e_1,\ldots,e_d}(v_1, \ldots, v_d) \;:=\; \det(u)$$

le déterminant de u au sens de la définition D.7.

Remarque D.11 i) Il s'ensuit immédiatement que pour tout endomorphisme u de E,

$$\det(u) \;=\; \det_{(e_1,\ldots,e_d)}(u(e_1), \ldots, u(e_d))\,.$$

ii) L'identité D.5.ii) a pour conséquence que, si

$$(e_1, \dots, e_d) \text{ et } (e'_1, \dots, e'_d) \text{ sont deux bases de } E,$$

et $(v_1, \dots, v_d)$ un système de vecteurs quelconque,

$$\det_{(e_1,\dots,e_d)}(v_1, \dots, v_d) \;=\; \det_{(e_1,\dots,e_d)}(e'_1, \dots, e'_d) \;\cdot\; \det_{(e'_1,\dots,e'_d)}(v_1, \dots, v_d)\,.$$

Remarque D.12 (Attention :) Le déterminant d'un système de vecteurs, en revanche, n'a de sens que par rapport à une base donnée.

Lemme D.13 *Pour tout d-uplet*

$$x \;:=\; (x_1, \dots, x_d)$$

d'éléments de E et tout d-uplet

$$y \;:=\; (y_1, \dots, y_d)$$

d'éléments de E^*, on pose

$$\delta(x, y) \;:=\; \sum_{s \,\in\, \mathcal{S}_d} \sigma(s) \prod_{i \,\in\, [1;d]} \langle x_{s(i)}, y_i \rangle \qquad \text{D.13.1}$$

$$(\text{où } \forall (x, y) \in E \times E^*,\; \langle x, y \rangle \;:=\; y(x)\,.)$$

Alors pour tout (x, y) comme ci-dessus, δ vérifie les propriétés suivantes :

ii)

$$\delta(x, y) \;=\; \sum_{s \,\in\, \mathcal{S}_d} \sigma(s) \prod_{i \,\in\, [1;d]} \langle x_i, y_{s(i)} \rangle\,.$$

iii) Pour y fixé, $\delta(\cdot, y)$ est une forme d-linéaire alternée sur E.

iv) Pour x fixé, $\delta(x, \cdot)$ est une forme d-linéaire alternée sur E^*.

v) Pour tout endomorphisme u de E,

$$\delta(u(x), y) \;=\; \det(u)\delta(x, y) \text{ (où } u(x) \;:=\; (u(x_1), \dots, u(x_d))\,.)$$

vi) Pour tout endomorphisme v de E^*,

$$\delta(x, v(y)) \;=\; \det(v)\delta(x, y) \text{ (où } v(y) \;:=\; (v(y_1), \dots, v(y_d))\,.)$$

vii) Pour tout endomorphisme u de E (resp. v de E^*,)

$$\delta(u(x), y) \;=\; \delta(x, u^*(y)) \text{ resp. } \delta(x, v(y)) \;=\; \delta(v^*(x), y)\,.)$$

viii) Si x est une base de E et y sa base duale $\delta(x, y) \;=\; 1$.

ix) Si x (resp. y) est un système lié,

$$\delta(x, y) \;=\; 0\,.$$

x) Si $x := (x_1, \dots, x_d)$ *est un* d*-uplet de vecteurs de* E *et* $b := (b_1, \dots, b_d)$ *une base de* E,

$$\det_b(x) = \delta(x, b^*) ,$$

(où b^* *est la base duale de* b.)

Corollaire D.14 *Étant donnée une base* b *de* E *et l'application qui à tout système* d*-uplet d'éléments de* E, v *associe* $\det_b(v)$ *est une forme* d*-linéaire alternée sur* E.

Corollaire D.15 *Étant donné un endomorphisme* u *de* E,

$$\det(u) = \det(u^*) , \qquad \textit{D.15.1}$$

(où u^* *désigne le dual de* u *,) pour toute base* $\mathcal{B}$ *de* E, *si*

$$M := (m_{i,j}) \frac{1 \leq i \leq d}{1 \leq j \leq d}$$

est la matrice de u *dans la base* $\mathcal{B}$:

$$\det(M) := \det(u) = \sum_{s \in \mathcal{S}_d} \sigma(s) \prod_{i \in [1;d]} M_{i,s(i)} = \det({}^t M) \qquad \textit{D.15.2}$$

Corollaire D.16 *i) Un endomorphisme* u *de* E *est inversible si et seulement si* $\det(u) \neq 0$.

ii) Étant donnée une base $(e_1, \dots, e_d)$ *de* E, *un système* $(v_1, \dots, v_d)$ *de vecteurs de* E *est une base si et seulement si*

$$\det_{(e_1,\dots,e_d)}(v_1, \dots, v_d) \neq 0 .$$

Proposition D.17 *Supposons donnée sur* E *une forme bilinéaire non dégénérée* ϕ. *Alors tout endomorphisme* u *de* E ϕ*-orthogonal vérifie*

$$\det(u)^2 = 1 .$$

D.18 . −Exercices

Exercice D.18.1 [Déterminants par blocs]
Pour tout $n \in \mathbb{N}^*$, **on note** $I_n \in \mathcal{M}_n(\mathbb{K})$ **la matrice identité. Dans la suite** p **et** q **sont dans** $\mathbb{N}^*$.

1) Soient

$$A \in \mathcal{M}_p(\mathbb{K}) \text{ et } B \in \mathcal{M}_q(\mathbb{K}) .$$

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 $\det(\begin{pmatrix} A & \\ 0 & B \end{pmatrix})$ en fonction de $\det(A)$ et $\det(B)$.

Indication : *Utiliser la multiplicativité du déterminant.*

2) Soient

$$A \in \mathcal{M}_p(\mathbb{K}) \, , \; B \in \mathcal{M}_q(\mathbb{K}) \, \text{et} \, C \in \mathcal{M}_{p,q}(\mathbb{K}) \, .$$

a) Calculer $\det(\begin{pmatrix} A & C \\ 0 & I_q \end{pmatrix})$ en fonction de $\det(A)$.

b) Pour

$$M := \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \in \mathcal{M}_{p+q}(\mathbb{K}),$$

calculer $\det(M)$ en fonction de $\det(A)$ et $\det(B)$.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

TD n° I

Groupes abéliens

Exercice A : (Torsion dans un groupe abélien)
Soit A un groupe abélien noté additivement. Pour tout entier $n \geq 1$, on note

$$A[n] := \{x \in A\,;\, nx = 0\} \text{ et } \mathrm{Tor}(A) := \bigcup_{n\geq 1} A[n]\,.$$

1) Montrer que les

$$A[n]\,, n \in \mathbb{N} \text{ et } \mathrm{Tor}(A)$$

sont des sous-groupes de A.

2) Soit $f : A \to B$ un homomorphisme de groupes. Montrer que pour tout $n \geq 1$,

$$f(A[n]) \subset B[n] \text{ puis que } f(\mathrm{Tor}(A)) \subset f(\mathrm{Tor}(B))$$

avec égalité si f est un isomorphisme.

3) Si p et q sont des entiers premiers entre eux, montrer que tout élément de $A[pq]$ s'écrit de manière unique comme somme d'un élément de $A[p]$ et d'un élément de $A[Q]$; autrement dit que

$$A[pq] = A[p] \oplus A[q]\,.$$

4) Montrer que $A/\mathrm{Tor}(A)$ est sans torsion ***i.e.***

$$\forall (n,x) \in \mathbb{N} \times A/\mathrm{Tor}(A),\ n \cdot x = 0 \Leftrightarrow n = 0 \text{ ou } x = 0\,.$$

On suppose désormais que A est fini, on note n le cardinal de A et $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ la décomposition de n en facteurs irréductibles (donc $e_i \geq 1$ pour tout $i = 1, \cdots, r$).

5) Pour tout entier $m \in \mathbb{N}$, si $v_p(m)$ dénote la valuation p-adique de m, alors

$$A[m] = \bigoplus_{p|m} A[p^{v_p(m)}]\,.$$

Si p est un nombre premier, on note $A[p^\infty]$ le sous-ensemble de A des éléments dont l'ordre est une puissance de p.

$$A[p^\infty] = \{a \in A\,;\, \exists s \in \mathbb{N},\ ,\ |<a>_A| = p^s\}\,.$$

6) Montrer que $A[p^\infty]$ est un sous-groupe de A.

7) Montrer que $A[p^\infty] \neq \{0\}$ si et seulement si p est l'un des p_i.

8) Plus généralement, montrer que $A[p^\infty]$ est l'unique p-Sylow de A. En déduire le cardinal de $A[p^\infty]$.
Soit

$$\begin{array}{rccc} \pi : & \bigoplus_p A[p^\infty] & \longrightarrow & A \\ & (x_p)_p & \longmapsto & \sum_p x_p. \end{array}$$

9) a) Soit $(x_p)_p \in \mathrm{Ker}\,\pi$ et soit q un nombre premier. Montrer qu'il existe $k \in \mathbb{N}$ tel que $x_q \in A[q^k]$ et k' premier à q tel que $x_q \in A[k']$.

b) En déduire que π est injective.

10) Montrer que π est surjective et en déduire que

$$A \cong \bigoplus_{i=1}^{r} A[p_i^\infty]$$

Exercice B : Soient A et B deux groupes abéliens et $\mathrm{Hom}(A,B)$ l'ensemble des morphismes de A dans B.

1) Vérifier rapidement que $\mathrm{Hom}(A,B)$ a une structure de groupe abélien.

2) Montrer que

$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A) \cong A[m] := \{a \in A\,;\, ma = 0\}$$

(on donnera explicitement un isomorphisme.)

3) Montrer que

$$\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z} \text{ où } d = (p \wedge q)\,.$$

4) Montrer que $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = 0$.

5) Montrer que $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

6) Si

$$A = \prod_{i=1}^{k} A_i \text{ et } B = \prod_{j=1}^{\ell} B_j$$

sont des groupes abéliens, montrer que $\mathrm{Hom}(A, \prod_{j=1}^{\ell} B_j)$ est isomorphe à $\prod_{j=1}^{\ell} \mathrm{Hom}(A, B_j)$ et que $\mathrm{Hom}(\prod_{i=1}^{k} A_i, B)$ est isomorphe à $\prod_{i=1}^{k} \mathrm{Hom}(A_i, B)$.

Indication : *On pourra se borner à le montrer pour deux facteurs.*

Exercice C : 1) Comment l'exercice B permet-il de retrouver le résultat de l'exercice A, question 3) ?

2) De quel énoncé connu peut-on rapprocher ce dernier résultat ?

Exercice D : Soient

$$0 \to N \xrightarrow{i} M \xrightarrow{p} Q \to 0$$

une suite exacte courte de groupes abéliens, R un groupe abélien et $f : R \to Q$ un morphisme de groupes.

On note

$$r : R \times M \to R\,,\ (x,y) \mapsto x \text{ et } q : R \times M \to M\,,\ (x,y) \mapsto y\,.$$

Enfin on note

$$P := \{(x,y) \in R \times M\,;\, f[r(x,y)] = p[q(x,y)]\}\,.$$

1) $R \times M$ étant muni de sa structure produit, montrer que P en est un sous-groupe.

2) Montrer que, si f est injectif,

$$q_{|P} : P \to M$$

induit un isomorphisme

$$P \cong p^{-1}[f(R)]\,.$$

3) Montrer que $r_{|P}$ est un morphisme surjectif de noyau isomorphe à N et qu'on a donc une suite exacte

$$0 \to N \longrightarrow P \xrightarrow{r_{|P}} R \to 0\,.$$

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

TD n° II

Anneaux idéaux

Exercice A : (Rappels et compléments sur les idéaux)
Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux.

1) On suppose que f est surjectif.

a) Montrer que si $\mathfrak{I} \subset A$ est un idéal de A alors $f(\mathfrak{I})$ est un idéal de B.

b) Montrer que si $\mathfrak{I}$ est un idéal de A contenant$\mathrm{Ker}\, f$ alors

$$f^{-1}(f(\mathfrak{I})) = \mathfrak{I}\,.$$

c) En déduire que l'application $\mathfrak{I} \mapsto f(\mathfrak{I})$ réalise une bijection croissante entre l'ensemble des idéaux de A contenant $\mathrm{Ker}\, f$ et l'ensemble des idéaux de B.

2) On ne suppose plus que f est surjectif.

a) Si $\mathfrak{I} \subset A$ est un idéal de A, le sous-ensemble $f(\mathfrak{I}) \subset B$ est-il toujours un idéal de B ?

b) Soit $\mathfrak{J}$ un idéal de B. Montrer que $f^{-1}(\mathfrak{J}) \subset A$ est un idéal de A et que $A/f^{-1}(\mathfrak{J})$ s'identifie à un sous-anneau de $B/\mathfrak{J}$.

c) En déduire que si $\mathfrak{J}$ est un idéal premier de B, alors $f^{-1}(\mathfrak{J})$ est un idéal premier de A.

d) Si $\mathfrak{J} \subset B$ est un idéal maximal de B, le sous-ensemble $f^{-1}(\mathfrak{J}) \subset A$ est-il nécessairement un idéal maximal de A ?

Exercice B : (Autour du théorème chinois)
Soit A un anneau commutatif. Si $\mathfrak{I}, \mathfrak{J} \subset A$ sont des idéaux de A, on pose :

$$\mathfrak{I} + \mathfrak{J} := \{a + b \mid a \in \mathfrak{I} \text{ et } b \in \mathfrak{J}\} \text{ et } \mathfrak{I}\mathfrak{J} := \{a_1 b_1 + \cdots + a_k b_k \mid a_i \in \mathfrak{I} \text{ et } b_j \in \mathfrak{J}\}\,.$$

1) Montrer que si $\mathfrak{I}, \mathfrak{J}$ sont des idéaux de A alors $\mathfrak{I} + \mathfrak{J}$, $\mathfrak{I}\mathfrak{J}$ et $\mathfrak{I} \cap \mathfrak{J}$ sont des idéaux de A.

2) Soient $\mathfrak{I}, \mathfrak{J}$ des idéaux de A.

a) Montrer que $\mathfrak{I}\mathfrak{J} \subset \mathfrak{I} \cap \mathfrak{J}$

b) On suppose que $\mathfrak{I} + \mathfrak{J} = A$. Montrer que $\mathfrak{I}\mathfrak{J} = \mathfrak{I} \cap \mathfrak{J}$.

c) Donner un contre-exemple à cette égalité si $\mathfrak{I} + \mathfrak{J} \neq A$. (On pourra choisir $A = \mathbb{Z}$).

d) Soient $\mathfrak{K}$ et $\mathfrak{L}$ des idéaux tels que

$$\mathfrak{I} \subset \mathfrak{K}\,,\ \mathfrak{J} \subset \mathfrak{L}\,,\ \mathfrak{K} \cap \mathfrak{L} \subset \mathfrak{I} \cap \mathfrak{J} \text{et } \mathfrak{K} + \mathfrak{L} \subset \mathfrak{I} + \mathfrak{J}\,.$$

Montrer qu'alors

$$\mathfrak{I} = \mathfrak{K} \text{ et} \mathfrak{J} = \mathfrak{L}\,.$$

3) Soient $\mathfrak{I}$ et $\mathfrak{J}$ des idéaux de A. On note

$$p_{\mathfrak{I}} : A \to A/\mathfrak{I} \text{ et } p_{\mathfrak{J}} : A \to A/\mathfrak{J}$$

les surjections canoniques et

$$q : A \to A/\mathfrak{I} \times A/\mathfrak{J}\,,\ x \mapsto \big(p_{\mathfrak{I}}(x), p_{\mathfrak{J}}(x)\big)\,.$$

a) Vérifier que q est un morphisme d'anneaux ; montrer qu'il existe un unique morphisme d'anneaux

$$i : A/(\mathfrak{I} \cap \mathfrak{J}) \to A/\mathfrak{I} \times A/\mathfrak{J} \text{ tel que } i \circ p_{\mathfrak{I}\cap\mathfrak{J}} = q$$

et que i est injectif.

b) Montrer qu'il existe un unique morphisme d'anneaux

$$q_{\mathfrak{I}} \,:\, A/\mathfrak{I} \,\to\, A/(\mathfrak{I}+\mathfrak{J}) \text{ tel que } q_{\mathfrak{I}} \circ p_{\mathfrak{I}} \,=\, p_{\mathfrak{I}+\mathfrak{J}} \text{ (resp. } q_{\mathfrak{J}} \,:\, A/\mathfrak{J} \,\to\, A/(\mathfrak{I}+\mathfrak{J}) \text{ tel que } q_{\mathfrak{J}} \circ p_{\mathfrak{J}} \,=\, p_{\mathfrak{I}+\mathfrak{J}} \text{)}$$

et que $q_{\mathfrak{I}}$ et $q_{\mathfrak{J}}$ sont surjectifs.

Soit

$$p \,:\, A/\mathfrak{I} \times A/\mathfrak{J} \,\to\, A/(\mathfrak{I}+\mathfrak{J}) \,,\, (\alpha,\beta) \,\mapsto\, q_{\mathfrak{I}}(\alpha) - q_{\mathfrak{J}}(\beta) \,.$$

c) Montrer que p est un morphisme surjectif de A-modules.

d) Comparer $\mathrm{Ker}\, p$ et $\mathrm{Im}\, i$ et conclure.

e) Que devient la conclusion de d) si $\mathfrak{I}+\mathfrak{J} \,=\, A$? Montrer qu'on a alors un isomorphisme

$$A/\mathfrak{I}\mathfrak{J} \,\cong\, A/\mathfrak{I} \times A/\mathfrak{J} \,.$$

4) Reformuler les résultats des questions précédentes dans le cas où A est un anneau principal.

5) Soient $\mathbb{K}$ un corps et $P \,\in\, \mathbb{K}[X]$. On écrit la décomposition de P en facteurs premiers dans $\mathbb{K}[X]$, $P \,=\, P_1^{e_1} \cdots P_\ell^{e_\ell}$ avec $e_i \geq 1$ pour $i \leq \ell$. Montrer que

$$\mathbb{K}[X]/(P) \,\cong\, \mathbb{K}[X]/(P_1^{e_1}) \times \cdots \times \mathbb{K}[X]/(P_\ell^{e_\ell}) \,.$$

Exercice C : (L'anneau $\mathbb{Z}[j]$ des entiers d'EISENSTEIN)

On note

$$\sigma \,:\, \mathbb{C} \,\to\, \mathbb{C} \,,\, a+ib \,\mapsto\, a-ib$$

la conjugaison complexe. On note

$$j \,:=\, e^{\dfrac{2i\pi}{3}} \,\in\, \mathbb{C}$$

qui vérifie

$$j^3 \,=\, 1 \,,\, 1+j+j^2 \,=\, 0 \text{ et } \sigma(j) \,=\, j^2 \,.$$

1) Montrer que si le polynôme $1+X+X^2 \,\in\, \mathbb{Q}[X]$ a une racine dans $\mathbb{Q}$ celle-ci est entière et en déduire que j n'est pas rationnel.

2) On note $\mathbb{Z}[j]$ le sous-anneau de $\mathbb{C}$ défini par

$$\mathbb{Z}[j] \,:=\, \{a+bj \,,\, (a,b) \,\in\, \mathbb{Z}\times\mathbb{Z}\}$$

muni des lois d'addition et de multiplication induites par celles de $\mathbb{C}$.

Montrer que $\mathbb{Z}[j]$ est un $\mathbb{Z}$-module (groupe abélien) libre de rang 2 et en donner une base.

3) Soit

$$N \,:\, \mathbb{C} \,\to\, \mathbb{R} \,,\, z \,\mapsto\, z\cdot\sigma(z) \,.$$

Montrer que N se restreint en une application encore notée $N \,:\, \mathbb{Z}[j] \,\to\, \mathbb{N}$ vérifiant

$$\forall \alpha \in \mathbb{Z}[j]\setminus\{0\},\; N(\alpha) \,\geq\, 1 \text{ et } \forall(\alpha,\beta)\in\mathbb{Z}[j]\times\mathbb{Z}[j],\; N(\alpha\beta) \,=\, N(\alpha)N(\beta) \,.$$

4) Déterminer le groupe $U \,:=\, \mathbb{Z}[j]^\times$ des éléments inversibles de $\mathbb{Z}[j]$.

On admettra dans la suite que, pour tout $z \,\in\, \mathbb{C}$ il existe $\alpha \,\in\, \mathbb{Z}[j]$ tel que $N(z-\alpha) \,<\, 1$.

5) Montrer que l'anneau $\mathbb{Z}[j]$ est principal.

6) Soit $\rho \,:=\, 1-j \,\in\, \mathbb{Z}[j]$.

Montrer que ρ est irréductible dans $\mathbb{Z}[j]$ et divise 3.

Indication : *on pourra calculer* $N(\rho)$.

7) On note $\kappa \,:=\, \mathbb{Z}[j]/(\mathbb{Z}[j]\rho)$.

Que peut-on dire de l'anneau κ ? Montrer que la composée du morphisme

$$\mathbb{Z} \,\to\, \mathbb{Z}[j] \,,\, a \,\mapsto\, a+0j \text{ et de la surjection canonique } \mathbb{Z}[j] \,\to\, \mathbb{Z}[j]/(\mathbb{Z}[j]\rho)$$

se factorise en un isomorphisme

$$\mathbb{F}_3 \,:=\, \mathbb{Z}/3\mathbb{Z} \,\cong\, \kappa \,.$$

8) Pour tout $\alpha \,\in\, \mathbb{Z}[j]$, on notera désormais $v(\alpha)$ sa valuation ρ-adique *i.e.* le plus grand entier naturel k tel que $\rho^k|\alpha$.

Rappeler rapidement pourquoi

$$\forall(\alpha,\beta)\in\mathbb{Z}[j]\times\mathbb{Z}[j],\; v(\alpha\beta) \,=\, v(\alpha) \,+\, v(\beta) \text{ et } v(\alpha+\beta) \,\geq\, \min(v(\alpha),v(\beta)) \,.$$

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

TD n° III

Groupes abéliens libres, groupes abéliens de torsion

Exercice A : (**Partie libre/génératrice**)
Soit M un groupe abélien (ou un A-module pour A un anneau principal) de type fini.

1) **a)** Une partie libre maximale de M est-elle génératrice ?

b) Une partie génératrice minimale de M est-elle une base ?

2) Un endomorphisme $f : M \to M$,

a) injectif est-il toujours surjectif ?

b) surjectif est-il toujours injectif ?

Exercice B : (**Rang d'un groupe abélien libre de type fini**)
Soient $r \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ des entiers

$$A \cong \mathbb{Z}^r \text{ et } B \cong \mathbb{Z}^s \textbf{ des groupes abéliens libres de type fini ;}$$

On suppose donné un isomorphisme $\phi : A \cong B$ dont on pourra noter $\psi : B \cong A$ l'isomorphisme réciproque.
Soit enfin $p \in \mathbb{P}$ un nombre premier et

$$\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, *) \textbf{ le corps à } p \textbf{ éléments.}$$

1) Montrer que

$$A' := \{px\,,\ x \in A\} \text{ (resp. } B' := \{px\,,\ x \in B\}\ )$$

est un sous-groupe de A (resp. B.)

2) Montrer que

$$A'' := A/A' \text{ (resp. } B'' := B/B'\ ) \text{ est un } \mathbb{F}_p\text{-espace vectoriel}$$
$$\text{isomorphe à } {\mathbb{F}_p}^r \text{ (resp. } {\mathbb{F}_p}^s\ .)$$

3) en notant

$$\pi_A : A \to A'' \text{ (resp. } \pi_B : B \to B''\ ) \text{ la surjection canonique ,}$$

montrer qu'il existe un unique $\phi'' : A'' \to B''$ et un unique $\psi'' : B'' \to A''$ morphismes de $\mathbb{F}_p$-espaces vectoriels (*i.e.* applications $\mathbb{F}_p$-linéaires) rendant les carrés suivants commutatifs :

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A'' & \xrightarrow{\phi''} & B'' \end{array} \qquad \text{et} \qquad \begin{array}{ccc} B'' & \xrightarrow{\psi} & A \\ \downarrow & & \downarrow \\ B'' & \xrightarrow{\psi''} & A''\ . \end{array}$$

4) Montrer que ϕ'' et ψ'' sont des isomorphismes inverses l'un de l'autre et en déduire que $r = s$.

Exercice C : (**Groupes abéliens libres et $\mathbb{Q}$-espaces vectoriels**)

1) Soit $f : \mathbb{Z}^n \to \mathbb{Z}^m$ un morphisme de groupes.

a) Montrer que $\mathrm{Ker}\, f$ et $\mathbb{Z}^n/\mathrm{Ker}\, f$ sont des groupes abéliens libres.

b) Soit $f_{|\mathbb{Q}} : \mathbb{Q}^n \to \mathbb{Q}^m$ l'application $\mathbb{Q}$-linéaire dont la restriction à $\mathbb{Z}^n$ est f. Montrer que $\mathrm{rg}(\mathrm{Ker}\, f) = \dim_{\mathbb{Q}} \mathrm{Ker}\,(f_{|\mathbb{Q}})$ et que $\mathrm{rg}(\mathbb{Z}^n/\mathrm{Ker}\, f) = \dim_{\mathbb{Q}} \mathrm{Im}\,(f_{|\mathbb{Q}})$.

c) Montrer que $\mathrm{Ker}\, f$ admet un supplémentaire dans $\mathbb{Z}^n$.

2) Soit

$$G := \left\{x \in \mathbb{Z}^4 \,;\, x+2y+3z = 0 \text{et } 2y+5t = 0\right\} .$$

Montrer que G est un groupe abélien libre de rang 2. Déterminer une base de G ainsi qu'un supplémentaire de G dans $\mathbb{Z}^4$.

3) Soit

$$H := \left\{x \in \mathbb{Z}^3 \,;\, 2x+y+5z = 0 \text{et } 4x+3y = 0\right\} .$$

Montrer que H est un groupe abélien libre de rang 1. Déterminer une base de H ainsi qu'un supplémentaire de H dans $\mathbb{Z}^3$.

Exercice D : (Groupes abéliens de type fini et de torsion)

1) Rappeler pourquoi un groupe abélien fini est de type fini et de torsion.
Soit G un groupe abélien de type fini et de torsion. Soit $S := \{s_1, \ldots, s_r\}$ une partie génératrice de G.

2) Rappeler pourquoi, pour tout $1 \leq i \leq r$ s_i est d'ordre fini d_i.

3) Montrer que le morphisme

$$\mathbb{Z}^r \to G\,,\ (n_1, \ldots n_r) \mapsto \sum_{i=1}^{r} n_i s_i$$

induit un morphisme surjectif

$$\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \to G\,.$$

4) En déduire que G est fini.

Exercice E : (Groupes abéliens de type fini)
Soit A un groupe abélien.

1) Prouver que, si A est de type fini, tout quotient de A est encore un groupe abélien de type fini.

2) Prouver que, si A est de type fini, tout sous-groupe de A est encore un groupe abélien de type fini.

3) Étant donnée une suite exacte courte

$$0 \to B \longrightarrow A \longrightarrow C \to 0$$

où B et C sont des groupes abéliens de type fini, montrer qu'il en est de même de A.

Exercice F : Dans le cours, la proposition suivante a été démontrée.

Proposition F.1 *Soit G un groupe commutatif fini de type fini et H un sous-groupe de G. Alors H est de type fini.*

L'objectif de cet exercice est de faire remarquer que la généralisation de cette proposition aux groupes non-commutatifs n'est pas vraie. Pour cela, on introduit la notion suivante.

Définition F.2 Un groupe G (non-nécessairement commutatif) est de type fini s'il admet une partie génératrice de cardinal fini ; c'est-à-dire s'il existe une famille $(g_i)_{i\in I}$ de cardinal fini telle que $G = < g_i | i \in I >_G$.

Soit $\mathfrak{S}(\mathbb{Z})$ le groupe des bijections de $\mathbb{Z}$ dans $\mathbb{Z}$. Soit $\mathfrak{S}_c(\mathbb{Z})$ le sous-groupe de $\mathfrak{S}(\mathbb{Z})$ des bijections de support fini ; c'est-à-dire l'ensemble des bijections f telles qu'il existe $N \in \mathbb{N}$ tel que $f(x) = x$ si $x \notin [-N, N]$. Si $f \in \mathfrak{S}_c(\mathbb{Z})$, on appelle support de f le plus petit entier N vérifiant la propriété ci-dessus.

1) En considérant le plus grand des supports d'une famille de cardinal fini d'éléments de $\mathfrak{S}_c(\mathbb{Z})$, montrer que $\mathfrak{S}_c(\mathbb{Z})$ n'est pas de type fini.
Soit G le sous-groupe de $\mathfrak{S}(\mathbb{Z})$ engendré par $\mathfrak{S}_c(\mathbb{Z})$ et par le décalage $d : n \longmapsto n+1$.

2) Pour tout $N \in \mathbb{N}$, montrer que l'ensemble des bijections de support $[-N, N]$ est engendré par les permutations de la forme $(n, n+1)$ pour $-N \leq n \leq N-1$.

3) Montrer que pour tout $n \in \mathbb{N}$, $(n, n+1)$ appartient à $< d, (0,1) >_G$.

4) En déduire que G est de type fini mais que son sous-groupe $\mathfrak{S}_c(\mathbb{Z})$ n'est pas de type fini.

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

TD n° IV

Facteurs invariants et bases adaptées

Exercice A : (Décomposition canonique des p-groupes abéliens)
Soit p un nombre premier, et G un p-groupe abélien de cardinal p^k $k \in \mathbb{N}^*$.

1) Rappeler pourquoi il existe $r \in \mathbb{N}$ et $a_{k\ ,1\leq k\leq r}$ tels que

$$G \cong \mathbb{Z}/p^{a_1} \times \ldots \times \mathbb{Z}/p^{a_r} \text{ et } \forall 1 \leq k \leq r-1,\ a_{k+1} \leq a_k\ .$$

On dira que G admet une « décomposition canonique » $(r, a_{k\ ,1\leq k\leq r}\ )$.
On notera

$$\underline{p} : G \to G\ ,\ x \mapsto p \cdot x$$

la multiplication par p dans G. On suppose désormais que G a deux décompositions canoniques

$$(r, a_{k\ ,1\leq k\leq r}\ ) \text{ et } (s, b_{k\ ,1\leq k\leq s}\ )\ ,\ (r \textbf{ n'étant pas nécessairement égal à } s\ .)$$

Soient

$$u := \#\big(\{i \in [1;r]\ ;\ a_i = 1\}\big) \text{ et } v := \#\big(\{i \in [1;s]\ ;\ b_i = 1\}\big)\ .$$

2) Montrer que $\#(\operatorname{Im}\underline{p}) < \#(G)$.

3) Écrire des décompositions canoniques de $\operatorname{Im}\underline{p}$ données par $(r, a_{k\ ,1\leq k\leq r}\ )$ et $(s, b_{k\ ,1\leq k\leq s}\ )$.

4) Montrer que

$$p^u \cdot \prod_{1\ \leq\ i\ \leq\ r, a_i>1} p^{a_i} = p^v \cdot \prod_{1\ \leq\ i\ \leq\ w, b_i>1} p^{b_i}\ .$$

5) Montrer finalement par récurrence sur $\#(G)$ qu'un p-groupe abélien G possède une unique décomposition canonique.

Exercice B : (Décomposition canonique pour un groupe abélien fini quelconque)
Soit G un groupe abélien fini.

1) Rappeler pourquoi il existe

$$r \in \mathbb{N} \text{ et } n_{k\ ,1\leq k\leq r} \text{ tels que } G \cong \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_r\ ,\ \forall 1 \leq k \leq r-1,\ n_k | n_{k+1}\ .$$

On dit alors qu'on a une décomposition canonique de G $: (r, n_{k\ ,1\leq k\leq r}\ )$.
Dans la suite, on suppose donnée une décomposition canonique $(r, n_{k\ ,1\leq k\leq r}\ )$ pour G.

2) Soit p un nombre premier tel que $p|n_1$ ($v_p(n_1) > 0$.) Montrer que l'entier r peut être caractérisé en terme de la décomposition canonique du p-groupe $G[p^\infty]$ et utiliser les résultats de l'exercice A pour montrer que r ainsi que les $v_p(n_k)\ ,1 \leq k \leq r$ sont uniquement déterminés par G.

3) En déduire l'unicité d'une décomposition canonique pour un groupe abélien G fini quelconque.

Exercice C : (Structure des groupes finis(cf. TD n° VII, exercice C.))

1) Parmi les groupes suivants, lesquels sont isomorphes (vous devez justifier votre réponse) :

$$\begin{aligned} G_1 &= \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \\ G_2 &= \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ G_3 &= \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ G_4 &= (\mathbb{Z}/25\mathbb{Z})^\times \times \mathbb{Z}/5\mathbb{Z} \end{aligned}$$

Lesquels sont cycliques ?

2) Combien y a-t-il de classes d'isomorphismes de groupes abéliens de cardinal 1400 et possédant au moins un sous-groupe non cyclique d'ordre une puissance de 2 ? Donner leurs invariants (ou diviseurs élémentaires).

3) Soient r, s et t trois entiers positifs. On désire calculer en fonction de r, s et t les invariants $(d_1, d_2, \ldots, d_k)$ du groupe abélien

$$A \ := \ \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z} \, .$$

a) Que vaut d_1 ?

b) Calculer de deux manières le nombre d'éléments d'ordre divisant d_k et montrer que $k \leq 3$ et que d_3 est le **Pgcd** de r, s et t.

c) Montrer que

$$d_2 \ = \ \mathrm{PPCM}\big((r \wedge s), (s \wedge t), (t \wedge r)\big) \, .$$

4) Montrer que si A et B sont des groupes abéliens finis et

$$A \times A \ \cong \ B \times B, \text{ alors } \ \cong \ AB \, .$$

Exercice D : Soient

$$v_1 \ := \ (1,4,2,5) \, , \ v_2 \ := \ (3,7,11,6) \, , \ v_3 \ := \ (4,13,10,2) \, , \ v_4 \ := \ (5,11,9,7)$$

des éléments de $\mathbb{Z}^4$.

Déterminer le sous-groupe A de $\mathbb{Z}^4$ engendré par les éléments v_i ,$1 \leq i \leq 4$ c'est-à-dire donner une base adaptée pour A.

Exercice E : Déterminer à isomorphisme près les groupes abéliens de cardinal 300.

Exercice F : Cet exercice reprend les étapes de l'étude des sous-groupes d'un groupe abélien libre de type fini de manière effective.

Soit A le groupe abélien libre $\mathbb{Z}^2$ et B le sous-groupe de A engendré par les éléments $b_1 \ = \ (-4, 12)$ et $b_2 \ = \ (-8, 12)$. On désire calculer les facteurs invariants (diviseurs élémentaires) de A/B.

1) Donner un homomorphisme f de A dans $\mathbb{Z}$ tel que l'image de B soit maximale.

2) On note d un générateur de $f(B)$. Donner un élément a_2 de A tel que da_2 soit dans B et tel que $f(a_2) \ = \ 1$.

3) Calculer une base a_1 du noyau de f. Calculer l'intersection B' du noyau de f avec B et exprimer un générateur de B' d'une part en fonction de a_1 et d'autre part dans le système générateur de B.

4) Calculer les facteurs invariants de A/B.

Exercice G : **1)** Soit $A = \mathbb{Z}^2$ et B le sous-groupe de A engendré par $b_1 = (14, 2)$ et $b_2 = (2, 4)$. Calculer une base de A adaptée à B. Donner la structure du quotient A/B.

2) Soit G un groupe abélien (noté additivement) et possédant deux générateurs a et b tels que

$$14a \ + \ 2b \ = \ 0_G \text{ et } 2a \ + \ 4b \ = \ 0_G \, .$$

Montrer que G est isomorphe à un quotient d'un groupe d'ordre 52 dont on donnera la structure.

Exercice H : Soit $e_1 = (a_1, \ldots, a_n)$ un élément de $\mathbb{Z}^n$ tel que le **Pgcd** des a_i vaille 1 [7]

Montrer qu'il existe une base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$ dont le premier vecteur est e_1.

Que peut-on dire du quotient $\mathbb{Z}^n/\mathbb{Z}e_1$?

Adapter l'exercice en ne supposant plus que le **Pgcd** vaut 1.

7. Un tel vecteur est dit *primitif* et un certain nombre d'autres propriétés des vecteurs primitifs sont étudiées dans le cours en C.1.3.

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

TD n° V

Anneau de polynômes

Exercice A : Soit A un anneau commutatif intègre.

1) Montrer que A est un corps si et seulement si $A[X]$ est principal.

2) En déduire que $A[X,Y]$ et $\mathbb{Z}[X]$ ne sont pas principaux.

Exercice B : (Idéaux maximaux, polynômes irréductibles)
Soit A un anneau commutatif.

1) Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme à une indéterminée à coefficients dans $\mathbb{K}$. Montrer que l'idéal $P\mathbb{K}[X] := \{P * Q\ ,\ Q \in \mathbb{K}[X]\}$ est maximal si et seulement si P est irréductible.

2) Montrer que le résultat de la question 1) se généralise à n'importe quel anneau principal, à savoir que si A est un anneau principal, un idéal $\mathfrak{I}$ de A est maximal si et seulement s'il existe un élément irréductible $p \in A$ tel que $\mathfrak{I} = Ap$.

3) Dans cette question $A := \mathbb{Z}[X]$ l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{Z}$.

a) Déterminer l'ensemble $A^\times$ des éléments inversibles de A.

b) Vérifier que le polynôme $X^2+1 \in A$ est irréductible.

c) Montrer que, pour tout $P \in A$, il existe un unique couple $(Q,R) \in A \times A$ tel que

$$P = Q*(X^2+1) + R \text{ et } \deg(R) \leq 1\,.$$

Dans la suite on a toujours $A = \mathbb{Z}[X]$, p est un nombre premier,

$$I := (X^2+1)*A = \{(X^2+1)*P\ ,\ P \in A\}\ ,\ J := \{(X^2+1)*P + p*Q\ ,\ (P,Q) \in A \times A\}\,.$$

4) et l'on suppose de plus que $p = 7$. On note alors $\mathbb{F}_7 := (\mathbb{Z}/7\mathbb{Z},+,*)$ le corps à 7 éléments et $\mathbb{F}_7[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{F}_7$.

a) Montrer que le polynôme X^2+1 est irréductible dans $\mathbb{F}_7[X]$.

b) On note $k := \mathbb{F}_7[X]/(X^2+1)*\mathbb{F}_7[X]$. Montrer qu'on a un isomorphisme

$$A/J \cong k$$

et en déduire que J est maximal dans A.

Exercice C : (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

$$\pi : \mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X] \text{ la surjection canonique.}$$

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)

$$\text{par conséquent } \dim_{\mathbb{K}} \mathbb{K}[X]/P\mathbb{K}[X] \;=\; \deg(P)\;.$$

Exercice D : (**Le critère d'Eisenstein**)

Soit A un anneau principal et p un élément irréductible de A. On note $\pi \;:\; A \;\to\; \kappa \;:=\; A/p$ la surjection canonique et $\pi[X] \;:\; A[X] \;\to\; \kappa[X]$ le morphisme entre les anneaux de polynômes qui s'en déduit (qui consiste à réduire les coefficients modulo p.) On note $\mathbb{K}$ le corps des fractions de A. On pourra ne considérer que le cas où $A \;=\; \mathbb{Z}$ et $\mathbb{K} \;=\; \mathbb{Q}$.

Soit $P \;:=\; X^n + a_{n-1}X^{n-1} + \cdots a_1.X + a_0 \;\in\; A[X]$ un polynôme unitaire non constant à coefficients dans A.

On note v_p les valuations p-adiques (cf. I.14.9,'III.7.11.)

On dit que P est *p-Eisenstein* si les deux conditions suivantes sont vérifiées :

i) Pour tout $i \leq n-1$, p divise a_i (*i.e.* $v_p(a_i) > 0$.)

ii) p^2 ne divise pas a_0 (*i.e.* $v_p(a_0) \;=\; 1$.)

1) Montrer que pour tout $P \;\in\; A[X]$, tout $Q \;\in\; A[X]$, P est p-Eisenstein et $Q|P$ entraîne $\pi[X](Q) \;=\; \pm X^{\deg(Q)}$.

2) Pour tout

$$P \in A[X]\;,\; Q \;:=\; \sum_{i=0}^{\deg(Q)} b_i X^i \in A[X]\;,\; R \;:=\; \sum_{i=0}^{\deg(R)} c_i X^i \in A[x],$$

montrer que $P \;=\; Q * R$, P est p-Eisenstein $\deg(Q) > 0, \deg(R) > 0$ entraîne $v_p(b_0) \;>\; 0$ et $v_p(c_0) \;>\; 0$.

3) Déduire de ce qui précède que pour $P \;\in\; A[X]$, P est p-Eisenstein entraîne P est irréductible.

4) Montrer finalement qu'il existe des polynômes irréductibles de tout degré dans $\mathbb{K}[X]$.

Exercice E : ($\mathbb{K}[X]$**-modules**)

Soit $\mathbb{K}$ un corps.

1) Montrer que E est un $\mathbb{K}[X]$-module si et seulement si, E est un $\mathbb{K}$-espace vectoriel muni d'un endomorphisme u tel que pour tout $v \;\in\; E$, $X \cdot v \;=\; u(v)$.

On parlera pour E du $\mathbb{K}$-*espace vectoriel sous-jacent*.

2) Décrire les morphismes de $\mathbb{K}[X]$-modules (en termes d'applications $\mathbb{K}$-linéaires.)

3) Étant donné un $\mathbb{K}[X]$-module E, décrire :

a) Les sous-$\mathbb{K}[X]$-modules de E,

b) Les quotients de E.

c) Les suites exactes courtes

$$0 \;\to\; N \xrightarrow{\;i\;} E \xrightarrow{\;p\;} Q \;\to\; 0\;.$$

4) Montrer qu'un $\mathbb{K}[X]$-module E est de type fini et de torsion si et seulement si le $\mathbb{K}$-espace vectoriel E est de dimension finie.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

TD n° VI

Lemme des noyaux, espaces cycliques

L'exercice A est un exercices d'application du théorème de décomposition de DUNFORD (cf. cours IV.9.3 ;) l'exercice B permet à nouveau de mettre en œuvre des méthodes utilisées dans le DOC n° V ; l'exercice C et l'exercice D permettent de prouver un certain nombre de résultats qui seront utiles pour établir les derniers théorèmes de réduction de ce cours à savoir le théorème de réduction de FROBENIUS (cf. cours IV.11.5,) et le théorème de réduction de JORDAN (cf. cours IV.10.10.) L'exercice D permet, en particulier d'établir la proposition IV.11.1 qui est l'exacte analogue des propositions II.10.1 et B.6.3 lesquelles constituent la première étape de la preuves des théorèmes IV.11.5 II.10.5 et B.6.13 respectivement.

Exercice A : (Décomposition de DUNFORD)

1) Soit A la matrice

$$A := \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 2 \end{pmatrix}$$

et f l'endomorphisme de $\mathbb{R}^3$ associé.

a) Factoriser le polynôme caractéristique de A.

b) Déterminer les sous-espaces propres et caractéristiques de A.

c) Démontrer qu'il existe une base de $\mathbb{R}^3$ dans laquelle la matrice de f est

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

et trouver une matrice P inversible telle que $A = PBP^{-1}$.

d) Écrire la décomposition de DUNFORD de B (justifier).

e) Pour $t \in \mathbb{R}$, calculer $\exp tB$.

f) Donner les solutions des systèmes différentiels

$$Y' = BY \text{ et } X' = AX .$$

2) Trouver la décomposition de DUNFORD de la matrice/endomorphisme

$$u = \begin{pmatrix} \alpha & x & z \\ 0 & \alpha & y \\ 0 & 0 & \beta \end{pmatrix} .$$

Exercice B : $(P(u) = \sum P(\lambda_i)u_i)$
Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathrm{End}_{\mathbb{K}}(E)$.

1) On suppose u diagonalisable et on note $\lambda_1, \ldots, \lambda_p$ ses valeurs propres supposées deux à deux distinctes.

a) Montrer qu'il existe des endomorphismes $u_1, \ldots, u_p$ tels que pour tout polynôme $P \in \mathbb{K}[X]$, on ait :

$$P(u) = \sum_{i=1}^{p} P(\lambda_i)u_i . \qquad 1$$

b) Montrer que pour tout $1 \leq i \leq p$, il existe un polynôme P_i tel que $u_i = P_i(u)$.

2) Réciproquement, soit $u, u_1, \ldots, u_p \in \mathrm{End}_{\mathbb{K}}(E)$ et $\lambda_1, \ldots, \lambda_p \in \mathbb{K}$ tels que

$$\forall P \in \mathbb{K}[X],\ P(u) = \sum_{i=1}^{p} P(\lambda_i) u_i \,.$$

Montrer que u est diagonalisable et

$$\mathrm{Sp}(u) \subset \{\lambda_1, \ldots, \lambda_p\} \,.$$

Exercice C : Soit E un espace vectoriel de dimension finie et u un endomorphisme de E. Soit F (resp. G) un sous-espace cyclique de E pour u de polynôme minimal P (resp. Q). On suppose que P et Q sont premiers entre eux.

Montrer que F et G sont en somme directe et que la somme $F \oplus G$ est cyclique. Quel est son polynôme minimal ?

Exercice D : (Sous-espace cyclique)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme de E. Si x est un élément de E, on appelle *polynôme minimal de f en x* (cf. cours IV.2.2.iii),) le polynôme unitaire $P^x_{\min f} \in \mathbb{K}[X]$ de plus petit degré tel que $P^x_{\min f}(f)(x) = 0$.

1) Montrer que pour tout $x \in E$, il existe un unique polynôme minimal en x et que $P^x_{\min f}$ divise le polynôme minimal $P_{\min f}$ de f.

2) On suppose dans cette question que $\mathbb{K}$ est infini.

a) Montrer que si $F_1, \cdots, F_n$ sont des sous-espaces vectoriels de E tels que $E = \bigcup_i F_i$ alors il existe $1 \leq i \leq n$ tel que $F_i = E$.

b) En déduire qu'il existe $x \in E$ tel que $P^x_{\min f}$ soit le polynôme minimal $P_{\min f}$ de f.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

TD n° VII

Réduction de FROBENIUS

Exercice A : (**Endomorphismes nilpotents**)
Soit $u \in \mathrm{End}_{\mathbb{K}}(E)$.
Montrrer que :

1) u est nilpotent d'échlon d si et seulement si $P_{\min u} = X^d$.

2) u est nilpotent d'échelon d et cyclique si et seulement si

$$u \text{ est cyclique et } \dim_{\mathbb{K}} E = d\,.$$

3) u est nilpotent d'échelon d si et seulement si u est nilpotent de rang $d-1$.

Exercice B : Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que $V = \oplus_{i=1}^{4} V_i$ où les sous-espaces vectoriels V_i sont des sous-espaces stables par u, cycliques pour u de polynôme minimal respectif x, x, $x(x-1)$, $(x-1)^2$.

1) Quelle est la dimension de V ?

2) Donner les invariants de similitude de V et écrire une décomposition de FROBENIUS de u.

Exercice C : 1) Soient P_1, P_2, P_3, P_4 des polynômes unitaires de $\mathbb{Q}[x]$ irréductibles et distincts deux à deux.
Donner le nombre de classes de similitude des matrices à coefficients dans $\mathbb{Q}$

$$\text{de polynôme caractéristique } P_{\text{car}} = \pm P_1^7 P_2^6 P_3^7 P_4^4$$

(décomposition de P en facteurs irréductibles) et

$$\text{de polynôme minimal } P_{\min} = P_1^6 P_2^2 P_3^3 P_4^3\,.$$

On justifiera en énonçant en particulier le théorème utilisé sur les invariants des classes de similitude.

2) Soient P_1, P_2, P_3 trois polynômes irréductibles distincts sur un corps K.

a) Combien y a-t-il de classes de similitude de matrices à coefficients dans K ayant comme polynôme minimal $P_1P_2^2P_3^2$ et comme polynôme caractéristique $P_1^3P_2^3P_3^4$? Pour chacune d'elles, donner les invariants de similitude.

b) On prend $K = \mathbb{Q}$ et $P_1 = x^2+1$, $P_2 = x+1$ et $P_3 = x-1$. Parmi les classes de similitudes précédentes, quelles sont celles pour lesquelles la dimension de l'espace propre associé à la valeur propre 1 est supérieure ou égale à 3 ?
Donner la matrice de Frobenius associée à une telle décomposition de Frobenius
Indication : *il ne doit donc apparaître que des matrices compagnons.*

Exercice D : (**Endomorphismes anti-involutif**)
Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme de E anti-involutif ; c'est-à-dire vérifiant $f^2 = -\mathrm{Id}$.

1) Donner un exemple d'un tel endomorphisme sur $\mathbb{R}^2$.

2) Montrer que f n'admet pas de valeurs propres réelles. En déduire que la dimension de E est paire.

3) Montrer que pour tout $x \in E$, le sous-espace vectoriel $\mathrm{Vect}\{x, f(x)\}$ est stable par f.

4) Montrer que si $F \subset E$ est un sous-espace vectoriel de E stable par f et si x est un élément de E tel que $\mathrm{Vect}\{x, f(x)\} \cap F \neq \{0\}$, alors $x \in F$.

5) En déduire que si $\dim E = 2n$, il existe des vecteurs $e_1, \cdots, e_n$ de E tels que $(e_1, f(e_1), \cdots, e_n, f(e_n))$ soit une base de E. Quelle est la matrice de f dans cette base ?

Exercice E : Soit $\mathbb{K}$ un corps commutatif.

1) Combien y a-t-il de classes de similitude de matrices de $\mathcal{M}_8(\mathbb{K})$ telles que $\mathrm{Im}\, A = \mathrm{Ker}\, A$?

2) Combien y a-t-il de classes de similitude de matrices nilpotentes de $A \in \mathcal{M}_5(\mathbb{K})$ telles que le rang de A^2 soit 2 ?

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

TD n° VIII

Réduction de JORDAN

Exercice A : Déterminer les invariants de similitude des matrices sous forme réduite de JORDAN suivantes :

$$A := \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; B := \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \text{ et } C := \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Exercice B : Soit V un espace vectoriel de dimension finie et u un endomorphisme dont la matrice est la suivante dans une base $\mathcal{B} = (e_1, \cdots, e_{14})$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Répondre aux questions suivantes dans l'ordre désiré (en justifiant et en limitant les calculs) :

1) Calculer le polynôme minimal de u.

2) Écrire la décomposition de FROBENIUS de $(V, u) : V =$
$dspoplusi1'V_i$ en précisant la valeur de r et la valeur des polynômes minimaux de la restriction de u à V_i.

3) Calculer la dimension des noyaux de u^s pour s entier.

Exercice C : (Réduite de JORDAN lorsque P_{car} est connu)

1) Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que le polynôme caractéristique de u est $\pm(X-2)^4(X+3)$ et que le noyau de $u - 2\mathrm{Id}$ est un plan.

Quelles sont les formes possibles de la réduite de JORDAN ?

2) Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que le polynôme caractéristique de u est $\pm(X-1)^3(X+1)^2$ et que le noyau de $u - \mathrm{Id}$ est un plan.

Quelles sont les formes possibles de la réduite de JORDAN ?

3) Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que le polynôme caractéristique de u est $\pm(X+1)^4(X^2-1)^2$ et que le noyau de $u + \mathrm{Id}$ est de dimension 3.

Quelles sont les formes possibles de la réduite de JORDAN ? Donner les invariants de similitude pour chacune.

Exercice D : (Matrice semblable à son double)
Soit $A \in \mathcal{M}_n(\mathbb{C})$.

1) Montrer que si A est semblable à $2A$ alors A est une matrice nilpotente.

2) Montrer que pour tout $k \in \mathbb{N}$, le bloc de JORDAN J_k est semblable à $2J_k$.

3) En déduire qu'une matrice est nilpotente si et seulement si elle est semblable à son double.

Exercice E : (Matrice semblable à sa transposée)
On va montrer que toute matrice $A \in \mathcal{M}_n(\mathbb{C})$ est semblable à sa transposée.

1) Montrer qu'il suffit de vérifier le résultat pour les matrices avec une unique valeur propre.

2) Montrer qu'il suffit de vérifier le résultat pour les matrices nilpotentes.

3) Démontrer le résultat pour les matrices nilpotentes.

Exercice F : On considère les endomorphismes u et v de $\mathbb{C}^3$ dont les matrices dans la base canonique sont respectivement

$$A := \begin{pmatrix} 8 & -16 & -9 \\ 7 & -15 & -9 \\ -7 & 16 & 10 \end{pmatrix} \text{ et } B := \begin{pmatrix} 2 & 2 & -3 \\ 5 & 1 & -5 \\ -3 & 4 & 0 \end{pmatrix} .$$

1) Montrer que $P_{\text{car } A} = P_{\text{car } B} = (X-1)^3$.

2) Montrer que l'ensemble des matrices M de $\mathcal{M}_3(\mathbb{C})$ vérifiant $(M - \mathrm{Id})^3 = 0$ est constitué de 3 classes de similitudes dont on déterminera les réduites de JORDAN associées.

3) Déterminer la réduite de JORDAN de u ainsi qu'une base de $\mathbb{C}^3$ dans laquelle la matrice de u est sa réduite de JORDAN.

4) Déterminer la réduite de JORDAN de v ainsi qu'une base de $\mathbb{C}^3$ dans laquelle la matrice de v est sa réduite de JORDAN.

Exercice G : (Racine carrée)
Soit $A \in \mathcal{M}_n(\mathbb{C})$. On appelle *racine carrée de* A, toute matrice M de $\mathcal{M}_n(\mathbb{C})$ vérifiant $M^2 = A$.

1) On suppose que A est diagonalisable. Montrer que A admet une racine carrée.

2) Dans cette question, on traite le cas où A est nilpotente.

a) Soit $B \in \mathcal{M}_n(\mathbb{C})$ une matrice nilpotente.
Déterminer le tableau de YOUNG associé à B^2 en fonction du tableau de YOUNG associé à B.

b) Étant donnée une matrice nilpotente A dont le tableau de YOUNG est

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix} , \text{ (resp. } \begin{pmatrix} * & * \\ * & * \\ * & \end{pmatrix}) , \text{ (resp. } \begin{pmatrix} * & * & * \\ * & * & \end{pmatrix})$$

trouver une matrice B telle que $B^2 = A$.

c) En déduire que si A est une matrice nilpotente alors A admet une racine carrée si et seulement si le tableau de YOUNG associé à A ne contient pas deux colonnes consécutives de même longueur impaire. En particulier le bloc de JORDAN

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

n'a pas de racine carrée.

3) Dans cette question, on traite le cas où A est inversible.

a) Montrer que si B est une matrice nilpotente alors $I + B$ admet une racine carrée (où I est la matrice identité.)
Indication : *On pourra utiliser le développement en série entière de $x \mapsto \sqrt{1+x}$ au voisinage de 0.*

b) En déduire que toute matrice inversible admet une racine carrée.

4) Donner une condition nécessaire et suffisante pour que A admette une racine carrée.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Problème n° I

Les résultat du TD n° II, exercice C peuvent bien entendu être utilisés dans ce problème, qui en constitue une suite naturelle possible.

L'équation $\alpha^3 + \beta^3 + \gamma^3 = 0$**)**

Dans la suite on considère

$$(\alpha, \beta, \gamma) \in \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que } \alpha^3 + \beta^3 + \gamma^3 = 0\,.$$

Dans cette question, l'élément $\rho \in \mathbb{Z}[j]$ **est défini comme à la TD n° II, exercice C, question 6).**

1) Montrer que ρ divise l'un des trois facteurs

$$(\alpha + \beta)\,,\ (\beta + \gamma) \text{ ou } (\gamma + \alpha)$$

Indication : *on pourra vérifier que*

$$(\alpha + \beta + \gamma)^3 = 3(\alpha + \beta)(\beta + \gamma)(\gamma + \alpha)\,.$$

On suppose dans la suite que $\rho|(\alpha + \beta)$**. On suppose de plus que** $\alpha, \beta,$ **et** γ **sont deux à deux premiers entre eux.**

2) i) Montrer que l'on peut supposer que

$$\alpha \equiv 1\ [\rho] \text{ et } \beta \equiv -1\ [\rho]$$

Indication : *on pourra utiliser la TD n° II, exercice C, question 7).*

ii) En écrivant $\alpha = 1 + \lambda\rho$ et en étudiant les congruences possibles de λ modulo ρ, montrer que,

$$\alpha \equiv 1\ [\rho^2] \text{ ou } j\alpha \equiv 1\ [\rho^2] \text{ ou } j^2\alpha \equiv 1\ [\rho^2]\,;$$

on admettra sans refaire les calculs, qu'un résultat analogue vaut pour β, *i.e.*

$$\beta \equiv -1\ [\rho^2] \text{ ou } j\beta \equiv -1\ [\rho^2] \text{ ou } j^2\beta \equiv -1\ [\rho^2]\,.$$

iii) Montrer que

$$v(\alpha\beta\gamma) = v(\gamma) > 0\,.$$

3) Montrer qu'il existe

$$(\alpha_1, \beta_1, \gamma_1) \in \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que}$$

i)

$$\alpha_1 \equiv 1\ [\rho^2]\,,\ \beta_1 \equiv -1\ [\rho^2]\,;$$

ii)

$$\alpha_1^3 + \beta_1^3 + \gamma_1^3 = 0\,;$$

iii)

$$v(\alpha_1\beta_1\gamma_1) = v(\alpha\beta\gamma) > 0$$

iv) α_1, β_1 et γ_1 sont deux à deux premiers entre eux.

4) Montrer qu'il existe

$$(A,B,C) \in \mathbb{Z}[j]\times\mathbb{Z}[j]\times\mathbb{Z}[j] \text{ tel que } \begin{array}{rcl} \alpha_1 + j\beta_1 &=& A\rho, \\ j\alpha_1 + \beta_1 &=& B\rho \\ \text{et } j^2(\alpha_1+\beta_1) &=& C\rho\,. \end{array}$$

5) Montrer que :

i) A et B sont premiers entre eux

Indication : *on pourra calculer*

$$\rho(Bj^2 - Aj) \text{ et } \rho(Aj^2 - Bj)\,;$$

Un calcul tout à fait similaire et qu'on ne demande pas de faire montre que A et C (resp. B et C,) sont également premiers entre eux.

ii) $A + B + C = 0\,;$

iii)

$$A \equiv 1\,[\rho]\,,\ B \equiv -1\,[\rho] \text{ et } C \equiv 0\,[\rho]\,;$$

iv)

$$\rho^3 ABC = -\gamma_1^3\,.$$

6) Montrer qu'il existe

$$(u,\alpha_2,\beta_2,\gamma_2) \in \mathbb{Z}[j]^\times\times\mathbb{Z}[j]\times\mathbb{Z}[j]\times\mathbb{Z}[j] \text{ tel que } u\alpha_2^3 = A\,,\ u\beta_2^3 = B \text{ et } u\gamma_2^3 = C\,.$$

7) Montrer que

$$v(\gamma_2) = v(\gamma) - 1$$

et en déduire que

$$v(\alpha_2\beta_2\gamma_2) = v(\alpha\beta\gamma) - 1\,.$$

8) (**Bonus**)
Montrer qu'il n'existe pas d'entiers $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ non nuls tels que

$$a^3 + b^3 = c^3\,.$$

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Problème n° II

pour le 20 avril 2020 **Ce problème et totalement ou partiellement facultatif. Cependant l'exercice A, l'exercice B, l'exercice C, l'exercice D sont des exercices relativement élémentaires qui ont été posés lors d'examens au cours des années passées. Il peuvent donc être considérés comme des sujets d'annales et nous en donnerons un corrigé détaillé. L'exercice E reste tout à fait dans l'esprit de ce qui précède et tire profit des différents invariants introduits précédemment afin de déterminer dans quelle mesure on peut fixer arbitrairement la suite des noyaux itérés d'un endomorphisme nilpotent. L'exercice F, l'exercice G et l'exercice H permettent d'étudier l'ensemble des matrices nilpotentes de $\mathcal{M}_n(\mathbb{C})$ sous des aspects géométriques et combinatoires. Ils sont cependant plus difficiles que les précédents et à la limite du programme. L'exercice I traite un sujet assez différent à savoir les liens qui existent entre polynôme minimal et polynôme caractéristique d'un endomorphisme, au-delà de ce qu'établit déjà le théorème IV.7.2 de CAYLEY–HAMILTON. Les résultats obtenus dans l'exercice I, pourraient également l'être grâce au théorème IV.11.5 de réduction de FROBENIUS ou plus exactement à son corollaire IV.11.11, qui est en fait une version plus précise du théorème de CAYLEY–HAMILTON. Cependant on développera dans l'exercice I des méthodes tout à fait différentes et qui peuvent présenter un intérêt en soi. On y construit notamment une *division euclidienne* (cf. exercice I, question 6),) dans un cadre plus général que celui habituellement envisagé ; et qui pourrait avoir des applications à $\mathbb{Z}[X]$ en particulier. Cet exercice reste néanmoins tout à fait marginal en regard du programme du cours. Il est recommandé de connaître l'énoncé du théorème IV.10.10 de réduction de JORDAN ; même s'il n'est pas absolument nécessaire d'approfondir, dans un premier temps au moins, les éléments de sa preuve.**

Exercice A : (La suite des noyaux itérés)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et}\, f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \text{ on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

Cet exercice peut être traité de manière tout à fait élémentaire et ne nécessite l'usage ni du théorème IV.10.10 de JORDAN ni du théorème IV.11.5 de réduction de FROBENIUS.

1) Montrer qu'il existe un vecteur $x \in E$ tel que la famille $\{f^i(x)\}_{,0 \leq i \leq \varepsilon-1}$ est libre.

2) (**polynôme minimal**)
Quel est le polynôme minimal de f ? Qu'en déduit-on sur ε et n ?

3) Montrer que la suite

$$\{0\} \subset \mathrm{Ker}\, f \subset \ldots \subset \mathrm{Ker}\, f^{\varepsilon-1} \subset \mathrm{Ker}\, f^{\varepsilon} = E$$

est strictement croissante ; et constante lorsque $k \geq \varepsilon$.

4) Montrer qu'il existe une base de E dans laquelle la matrice de f est triangulaire supérieure stricte.

5) Dans le cas où $\varepsilon = n$, montrer qu'il existe une base où la matrice de f est

$$J_n(0) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix} .$$

6) Quand $\varepsilon = n$, décrire complètement la suite $\dim_{\mathbb{K}} N_i\,,_{i\in\mathbb{N}}$.

Exercice B : (Injection de FROBENIUS)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N},\ \textbf{on note}\ N_k := \mathrm{Ker}\, f^k \,\mathrm{et}\, n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

On note

$$\forall i \in \mathbb{N}^*,\ d_i := \dim_{\mathbb{K}} N_i - \dim_{\mathbb{K}} N_{i-1}\ .$$

Il est vraisemblable que nombre des énoncés de cet exercice peuvent être obtenus comme corollaires du théorème IV.10.10 de réduction de JORDAN, mais on va chercher à les établir ici par des méthodes plus élémentaires.

1) Étant donnés un $\mathbb{K}$-espace vectoriel V de dimension finie et $W \subset V$ un sous-espace de V, , rappeler ce que vaut $\dim_{\mathbb{K}} V/W$ en fonction de $\dim_{\mathbb{K}} V$ et $\dim_{\mathbb{K}} W$.

2) Montrer que

$$\forall i \in \mathbb{N},\ d_i \geq 0\ .$$

3) Vérifier que, pour tout $i \in \mathbb{N}$, la restriction $f_{|N_{i+1}}$ de f à N_{i+1} est à valeurs dans N_i.

Pour tout $i \in \mathbb{N}$, on note

$$p_i : N_{i+1} \to N_{i+1}/N_i \textbf{ la surjection canonique}\ .$$

4) Montrer que, pour tout $i \in \mathbb{N}$, il existe un unique morphisme

$$f_i : N_{i+2}/N_{i+1} \to N_{i+1}/N_i tq\ f_i \circ p_{i+1} = p_i \circ f_{|N_{i+2}}\ .$$

5) Montrer que

$$\forall i \in \mathbb{N},\ f_i \text{ est injective}\ .$$

On l'appellera l'*injection de* FROBENIUS.

6) Déduire de ce qui précède que $d_{\cdot}$ est décroissante.

Exercice C : (Tableaux de YOUNG)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N},\ \textbf{on note}\ N_k := \mathrm{Ker}\, f^k \,\mathrm{et}\, n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

1) Justifier, en citant précisément le théorème que vous utilisez, mais sans le redémontrer bien entendu, qu'il existe un entier $m \in \mathbb{N}^*$, des entiers strictement positifs $r_j\,,_{1\leq j\leq m}$ et des sous espaces $E_j\,,_{1\leq j\leq m}$ tels que :

J_1)

$$E = \bigoplus_{j=1}^{m} E_j\ ;$$

J$_2$) $\forall 1 \leq j \leq m,\ E_j$ est stable par f ;

J$_3$)
$$\forall 1 \leq j \leq m-1,\ r_j \ \geq \ r_{j+1}\ ;$$

J$_4$) le sous-espace $(E_j, f_{|E_j})$ est cyclique de polynômes minimal X^{r_j}.

2) Que vaut $\displaystyle\sum_{j=1}^{m} r_j$?

On peut donc trouver une base de E dans laquelle la matrice de f est J :

Pour tout $r \leq n$, soit

$$J_r \ := \ \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} \ \in \ \mathcal{M}_r(\mathbb{C})$$

le bloc de JORDAN "élémentaire".

La matrice J est donc de la forme

$$J \ = \ \textbf{diag}\,(J_{r_1}, J_{r_2}, \cdots, J_{r_m}) \ = \ \begin{pmatrix} J_{r_1} & 0 \cdots & \cdots & 0 \\ 0 & J_{r_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{r_m} \end{pmatrix}$$

pour un certain entier m .

3) (**Décomposition des noyaux**)
Notons
$$\forall 1 \leq i \leq m,\ f_i \ := \ f_{|E_i}\ .$$
Pour tout $k \ \in \ \mathbb{N}$ et tout $1 \ \leq \ i \ \leq \ m$, donnez une relation entre les $n_{i,k} \ := \ \dim \mathrm{Ker}\, f_i^k$ et n_k .

4) Établir la valeur de $n_{i,k}$ en fonction de k et de r_i.

5) En déduire que
$$n_1 \ := \ \dim \mathrm{Ker}\, f \ = \ m \text{ et } n_k \ = \ \sum_{i=1}^{m} \min(k, r_i)\ .$$

On définit le *tableau de* YOUNG de (E, f) comme le tableau constitué de m lignes, alignées sur la gauche et tel que la $j^{\text{ième}}$ ligne comporte r_j cases. Par exemple si $m \ = \ 3, (r_1, r_2, r_3) \ = \ (5, 4, 1)$, le tableau de YOUNG est

$$Y(E,f) \ = \ \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix}\ .$$

6) Montrer que pour tout $j \ \in \ \mathbb{N}^*$, $d_j \ := \ \dim_{\mathbb{K}} N_j - \dim_{\mathbb{K}} N_{j-1}$ est la hauteur (le nombre de cases) de la $j^{\text{ième}}$ colonne du tableau de YOUNG $Y(E, f)$.

7) **a)** Donner les invariants de similitudes de f nilpotent dont le tableau de YOUNG est

$$Y(E,f) \ = \ \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix}\ .$$

b) Quelle est la dimension de E ?

c) Quels sont le tableau de YOUNG de f^2 et ses invariants de similitude.

Exercice D : (Commutant)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie n et $u \in \mathrm{End}_{\mathbb{K}}(E)$. On appelle *commutant de* u et on note

$$\mathrm{Com}(u) := \{v \in \mathrm{End}_{\mathbb{K}}(E) \,;\, u \circ v = v \circ u\} \subset \mathrm{End}_{\mathbb{K}}(E)$$

l'ensemble des endomorphismes de E qui commutent avec u. On rappelle que $\mathbb{K}[u] \subset \mathrm{End}_{\mathbb{K}}(E)$ est l'ensemble des polynômes en u *i.e.* l'image de $\mathbb{K}[X]$ par le morphisme $X \mapsto u$.

1) Montrer que $\mathrm{Com}(u)$ est un sous espace vectoriel de $\mathrm{End}_{\mathbb{K}}(E)$.

2) On suppose dans cette question que u est cyclique et que $x_0 \in E$ est un vecteur cyclique pour u.

a) En considérant l'application

$$\varphi : \mathrm{Com}(u) \to E \,,\, v \mapsto v(x_0),$$

montrer que l'on a $\dim_{\mathbb{K}} \mathrm{Com}(u) \leqslant n$.

b) Montrer que $\dim \mathbb{K}[u] \geq n$ et que

$$\mathrm{Com}(u) = \mathbb{K}[u] \,.$$

On pourra remarquer, en particulier que si u est nilpotent d'échelon n (cf. cours IV.8.1,)

$$\mathrm{Com}(u) \cong \mathbb{K}[u] \,.$$

3) Supposons que $E = \bigoplus_{i=1}^{r} E_i$ avec E_i stable par u. Comparer

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \text{ et } \sum_{i=1}^{r} \dim_{\mathbb{K}} \mathrm{Com}(u_{|E_i}) \,.$$

4) On suppose que $E = E_1 \oplus E_2$, où E_i est stable par u, cyclique de polynôme minimal μ_i avec $\mu_2 | \mu_1$.

a) Montrer qu'il existe une base $\mathcal{B}$ de E telle que :

$$M_{\mathcal{B}}(u) = \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix}$$

où pour tout polynôme $R \in \mathbb{K}[X]$, C_R désigne la matrice compagnon de R.

b) En déduire qu'il existe un endomorphisme $v \in \mathrm{Com}(u) \setminus \{0\}$ dont la matrice dans la base $\mathcal{B}$ est de la forme

$$M_{\mathcal{B}}(v) = \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix} .$$

c) Montrer que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) > n \,.$$

5) Déduire de ce qui précède que, si u n'est pas cyclique $\dim_{\mathbb{K}} \mathrm{Com}(u) > n$; puis que $\dim_{\mathbb{K}} \mathrm{Com}(u) = n$ si et seulement si u est cyclique.

Exercice E : (Une question réciproque)

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie n .

On cherche dans ce problème à savoir s'il existe des endomorphismes nilpotents de E dont la dimension des noyaux itérés est arbitrairement fixée. Si c'est le cas, on essayera de les déterminer, au moins à conjugaison près. Il est recommandé de traiter l'exercice C avant le présent exercice. On y a, en effet étudié certains invariants liés à la suite des noyaux itérés en grand détail ; ce qui pourra s'avéré très utile pour traiter les questions qui suivent.

L'objectif de cet exercice est de déterminer quelles sont les suites finies d'entiers n_k ,$0 \leq k \leq n$, $n_k \leq n$, pour lesquelles il existe un endomorphisme nilpotent $f \in \mathrm{End}_{\mathbb{C}}(E)$ de E tel que

$$\forall 1 \leq k \leq n, \ , \ \dim \mathrm{Ker}\, f^k \ = \ n_k \ . \qquad \textbf{1}$$

Soit donc donnée, dans toute cette partie, une suite n_k satisfaisant les hypothèses ci-dessus. On suppose qu'il existe f nilpotent vérifiant la condition 1 et l'on cherche à en tirer un certain nombre de conséquences.

On cherche au moins à déterminer la classe de conjugaison de f comme ci-dessus et, par conséquent, on peut se placer dans une base $\mathcal{B}$ dans laquelle la matrice de f est une réduite de JORDAN notée J .

Pour tout $r \leq n$, soit

$$J_r \ := \ \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} \ \in \ \mathcal{M}_r(\mathbb{C})$$

le bloc de JORDAN "élémentaire".

La matrice J est donc de la forme

$$J \ = \ \textbf{diag}\,(J_{r_1}, J_{r_2}, \cdots, J_{r_m}) \ = \ \begin{pmatrix} J_{r_1} & 0 \cdots & \cdots & 0 \\ 0 & J_{r_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{r_m} \end{pmatrix}$$

pour un certain entier m .

1) Pour toute permutation σ de l'ensemble $[1; m]$, montrer que les matrices J et

$$J_\sigma \ := \ \mathrm{diag}\,(J_{r_{\sigma(1)}}, J_{r_{\sigma(2)}}, \ \cdots \ , J_{r_{\sigma(m)}})$$

obtenue en permutant les blocs de JORDAN, sont conjuguées, c'est-à-dire qu'il existe une matrice inversible

$$P_\sigma \ \in \ \mathcal{M}_r(\mathbb{C}) \ \text{ telle que } \ J \ = \ P_\sigma \ J_\sigma \ P_\sigma^{-1} \ ,$$

ou encore qu'il existe une autre base $\mathcal{B}_\sigma$ dans laquelle la matrice de f est également une réduite de JORDAN.

2) (Pentes)

Pour tout

$$k \ \in \ \mathbb{N}^* \textbf{ on note encore } \ d_k \ := \ n_k \ - \ n_{k-1} \ . \textbf{ (cf. exercice C, question 6) .)}$$

Montrer qu'alors d_k est le nombre d'indice j tel que $r_j \ \geq k$.

3) (Nombre de blocs)

En déduire que pour tout $k \geq 0$, $d_k - d_{k+1}$ est exactement le nombre d'indices $1 \ \leq \ j \ \leq \ m$ tels que $r_j \ = \ k$. Remarquer qu'on obtient à nouveau ainsi l'énoncé de décroissance établi à l'exercice B, question 6) sans avoir recours à l'injection de FROBENIUS et par un argument particulièrement élémentaire. Qu'en pensez-vous ?

On suppose que $n \ = \ 25$, on donne la suite

$$n_1 \ = \ 7 \ , \ n_2 \ = \ 14 \ , \ n_3 \ = \ 20 \ , \ n_4 \ = \ 23 \ , \ n_5 \ = \ 25 \ .$$

Un endomorphisme f vérifiant 1 pour cette suite est donc nilpotent d'échelon 5 .

4) (Polygône)

On note $M_k \ := \ (k, n_k)$,$0 \ \leq \ k \ \leq 5$. Tracez le graphe obtenu en reliant M_k et M_{k+1} par un segment de droite.

5) a) Interpréter géométriquement dans ce cas les d_k de la question 2).

b) Montrer que le graphe correspond à une fonction concave.

c) À quoi correspondent les points anguleux de ce graphe ?

6) Montrer l'existence d'un endomorphisme nilpotent d'échelon 5 vérifiant 1 pour la suite n_k donnée dans cette question. Que peut-on dire de tous les endomorphismes solutions du problème ?

7) Dans le cas général (n quelconque,) quelles conditions (nécessaires et suffisantes) doit satisfaire la suite n_k pour qu'il existe un endomorphisme f nilpotent vérifiant 1 ?

Exercice F : (Géométrie du cône nilpotent)

On regarde dans $\mathcal{M}_n(\mathbb{C})$ l ensemble $\mathcal{N}$ des matrices nilpotentes, comme espace topologique. On l'appelle le *cône nilpotent*. (En fait on pourrait considérer n'importe quel corps, même si pour la suite il faudrait préciser les topologies, ce qu'est une variété etc..)

1) $\mathcal{N}$ est-il un espace vectoriel ?

2) Même si ce n'est pas le cas, on va montrer que $\mathcal{N}$ est une sous-variété de $\mathcal{M}_n(\mathbb{C})$ et déterminer sa dimension.

a) Montrer que $\mathcal{N}$ est fermé.

b) Supposons dans cette question que $n = 2$.

i) Montrer qu'une matrice nilpotente est de trace nulle.

ii) Donner deux équations définissant $\mathcal{N}$ dans $\mathcal{M}_2(\mathbb{C})$ (ou une seule équation dans $\{M \in \mathcal{M}_2(\mathbb{C}) ; \mathrm{Tr}(M) = 0\}$).

iii) Quelle est cette surface ?

Indication : *on pourra effectuer le changement de variables linéaire $x = x', y = y' + z'$ et $z = y' - z'$.*

iv) Montrer que $\mathcal{N}$ s'identifie à une surface dans $\mathbb{C}^3$, mais a un point singulier en 0.

Indication : *On pourra considérer l'espace tangeant en la matrice nulle, et montrer qu'il est de dimension 3.*

c) Montrer que les matrices nilpotentes de rang $n-1$ (*i.e.*d'échelon n (cf. cours IV.8.1,)) forment un ouvert, dense, de $\mathcal{N}$.

Indication : *On pourra considérer N sous forme de Jordan, et regarder $N + \frac{1}{k}J_n$.*

d) Montrer que toutes les matrices nilpotentes de rang $n-1$ sont conjuguées.

e) Soit N une telle matrice. Montrer que l'ensemble des matrices P qui commutent à N est isomorphe à $\mathbb{C}^n$

Indication : *on pourra supposer que N est sous forme normale de Jordan disons sous-diagonale (pourquoi ?* , et regarder l image par P de e_1).

f) (Difficile)

Montrer que l'ensemble des matrices de rang exactement $n-1$ est de dimension $n(n-1)$. On pourra construire un $\mathcal{C}^\infty$-difféomorphisme explicite entre $\mathcal{N}_n$, l'ensemble des matrices nilpotentes d'ordre exactement n, et

$$S = \left\{ M = \begin{pmatrix} 1 & \star & \dots & \star \\ 0 & & & \\ \vdots & \vdots & & \vdots \\ 0 & \star & & \star \end{pmatrix} \mid M \in \mathrm{GL}_n(\mathbb{C}) \right\},$$

en utilisant ce qui précède.

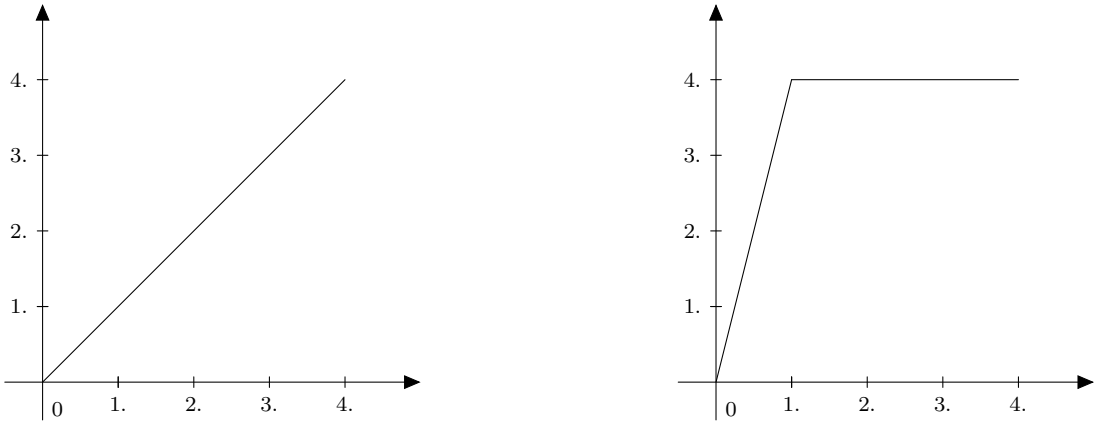
Exercice G : (Partitions, tableaux de YOUNG, polygônes concaves)

On appelle partition de n une suite $d_1 \geq d_2 \geq \dots d_n \geq 0$ telle que $d_1 + \dots + d_n = n$ (on autorise à avoir des répétitions et des zéros). On note $\mathcal{P}art(n)$ leur ensemble. On note $\mathcal{P}ol$ l'ensemble des polygones croissants, concaves, à abscisses de rupture entières tels que $P(0) = 0$ et $P(n) = n$ et pour tout $0 \leq k \leq n, P(k) \in \mathbb{N}$.

On note $\mathcal{Y}$ l'ensemble des diagrammes de Young à n cases (https://fr.wikipedia.org/wiki/Tableau_de_Young).

1) Montrer que l'on a des bijections (naturelles) entre $\mathcal{P}art(n)$, $\mathcal{P}ol$, et $\mathcal{Y}$.

FIGURE 1 – Deux exemples de polygônes dans $\mathcal{P}ol$ pour $n = 4$



2) Construire une application naturelle $\nu : \mathcal{N} \to \mathcal{P}art(n)$ telle qu'une matrice d'échelon n est envoyée sur la partition $1 + 1 + .. + 1 = n$, et la matrice nulle est envoyée sur $n + 0 + \cdots + 0 = n$.

3) Quel polygone est alors associé à une matrice de rang $n - 1$? De rang 0 ?

4) Montrer que deux matrices de $\mathcal{N}$ sont semblables ssi leurs ν sont égaux (vu comme polygones, partition ou diagramme, au choix).

Pour toute partition (ou polygone, ou diagramme) p, on note $\mathcal{N}_p$ l ensemble des matrices envoyées sur p.

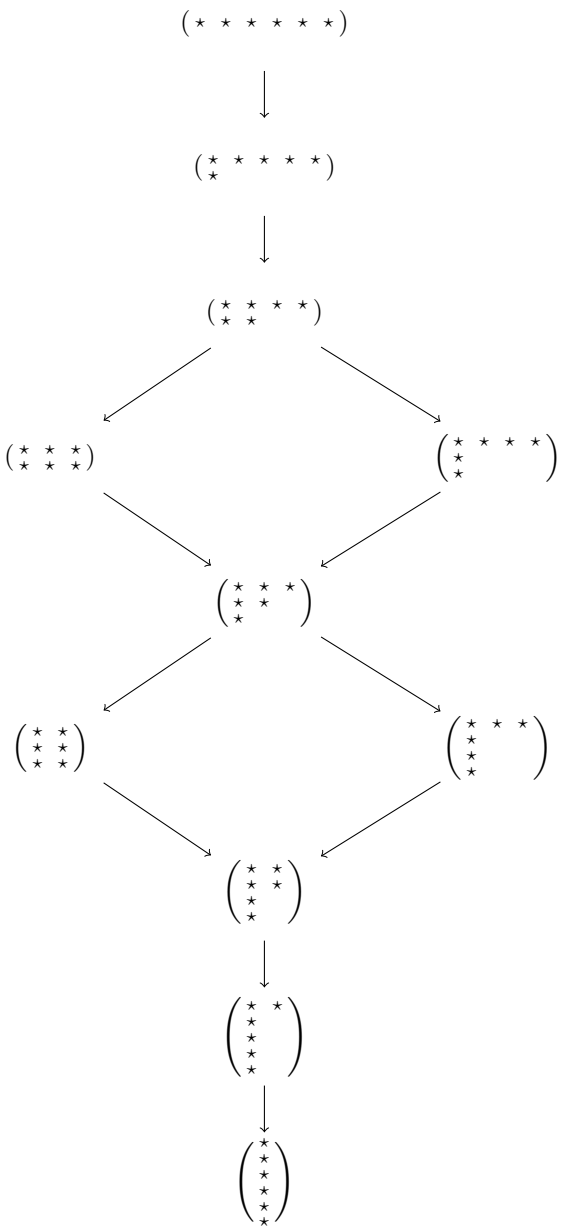
5) Pourquoi $\mathcal{N}_p$ est-il une classe de conjugaison ? Donner pour $n = 8$, un représentant de la classe de conjugaison de la partition $3 + 2 + 2 + 1 = 8$.

6) (**Difficile**)
Montrer que $\mathcal{N}_{p'}$ est dans l'adhérence de $\mathcal{N}_p$ si et seulement si le polygone de p est en dessous du polygone de p'.

Exercice H : (**Un graphe**)

1) Pour $n = 6$, donner le graph orienté dont les sommets sont les classes de similitudes de matrices nilpotentes, et les arêtes sont orientées $M \longrightarrow M$ s il existe une suite de matrices dans la classe de conjugaison de M dont la limite est dans la classe de conjugaison de M (on enlevera les arêtes ayant même sommet de départ et d arrivée, et lorsque l'on a des arrêtes $M \longrightarrow M' \longrightarrow M''$ on ne fera pas apparaitre l'arrête $M \longrightarrow M''$).

Solution :



2) Ce graph, vu comme graphe orienté, a t'il des cycles ? Et si on oublie l'orientation ?

Exercice I : (Facteurs irréductibles du polynôme minimal et du polynôme caractéristique)

On va chercher, dans ce problème, a comparer la décomposition en produit d'irréductibles du polynôme minimal et du polynôme caractéristique d'un endo morphisme.

À noter immédiatement que le corollaire IV.7.3 du théorème IV.7.2 de CAYLEY–HAMILTON est abusif. En effet du théorème de CAYLEY–HAMILTON assurant que

$$P_{\textbf{min}\ u} | P_{\textbf{car}\ u}$$

il résulte immédiatement que, tout facteur irréductible de $P_{\textbf{min}\ u}$ est un facteur irréductible de $P_{\textbf{car}\ u}$, mais rien ne permet à ce point d'affirmer que, réciproquement un facteur irréductible de $P_{\textbf{car}\ u}$ soit un facteur irréductible de $P_{\textbf{min}\ u}$ (hormis si toutefois il est de degré 1 mais ceux-ci jouent un rôle particulier (cf. question 1).))

En fait, dans la présentation qui est faite dans le cours, le corollaire IV.7.3 devrait apparaître comme un corollaire du corollaire IV.11.11. Ce dernier est lui-même un corollaire de la proposition IV.6.4 (cf. DOC n° III, n° III.1.exercice C) et bien entendu du théorème IV.11.5 de réduction de FROBENIUS. C'est précisément le recours à ce dernier résultat, qui est l'un des plus techniques de ce cours, qui pourrait inciter à donner un argument alternatif ; ce que nous allons faire dans ce qui suit.

Dans tout cet exercice, $\mathbb{K}$ est un corps, $n \in \mathbb{N}^*$, E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. On note $P_{\textbf{car}\ u}$ (resp. $P_{\textbf{min}\ u}$,) le *polynôme caractéristique* (cf. cours IV.6.1,) (resp. le *polynôme minimal* (cf. cours IV.2.2.iv).))

1) (**Les facteurs de degré** 1)
Rappeler pourquoi

$$\forall \lambda \in \mathbb{K},\ (X-\lambda)|P_{\min u} \ \Leftrightarrow\ (X-\lambda)|P_{\text{car } u}$$

et en déduire que si $\mathbb{K}$ est algébriquement clos,

$$P_{\text{car } u}|(P_{\min u})^n\ .$$

On sait déjà, grâce au théorème IV.7.2 de CAYLEY–HAMILTON, que

$$P_{\textbf{min } u}|P_{\textbf{car } u}\ .$$

On va montrer, (cf. question 7), c),) que

$$P_{\textbf{car } u}|[P_{\textbf{min } u}]^n\ .$$

L'élément technique principal pour prouver l'énoncé de divisibilité ci-dessus est la possibilité de faire la division euclidienne d'un polynôme à coefficients dans un anneau de matrices par un autre (cf. question 6).) La dificulté réside alors dans le fait de pouvoir justifier une telle construction. Si $A[X]$ et en effet un anneau de polynômes à une indéterminée, nous n'avons formellement établi un théorème de la *division euclidienne* que dans le cas où A est un corps (cf. cours III.4.2 ;) sans compter que nous n'avons même défini les anneaux de polynôme que dans le cas où A est un anneau commutatif (cf. cours III,) et que nous nous sommes bornés à ne donner la plupart des résultat que dans le cas où A est intègre. Or si l'on veut considérer l'anneau $\mathcal{M}_n(\mathbb{K})$ on sait de longue date qu'il n'est ni intègre ni commutatif. Qui plus est, on risque d'être amené, comme on l'a déjà fait (cf. DOC n° III, n° III.1.exercice D,) à identifier les deux anneaux

$$\big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ et } \mathcal{M}_n(\mathbb{K}[X]) \textbf{ (cf. question 3) .)}$$

On rappelle que, pour un anneau commutatif A, on note $\mathcal{M}_n(A)$ l'anneau des matrices carrées de taille $n\times n$ à coefficients dans A. On rapelle que cet anneau est isomorphe à l'anneau $\mathrm{End}_{A-\mathbf{mod}}(A^n)$ des endomorphismes du A-module libre A^n ; cet isomorphisme n'étant pas canonique mais donné par le choix d'une base de A^n.

2) (**L'anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$**)
Notons $\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathcal{M}_n(\mathbb{K})$. On va définir l'anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ des polynômes à une indéterminée à coefficients dans l'anneau $\mathcal{M}_n(\mathbb{K})$ des matrices $n\times n$ comme le sous anneaux des éléments presques nuls de l'anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ des séries formelles à coefficients dans $\mathcal{M}_n(\mathbb{K})$ dont on rappelle brièvement la construction ci-après. On suit en cela le même schéma que celui exposé dans le chapitre III du cours pour les annaux commutatifs.

i) (Addition : groupe abélien)
Puisque $(\mathcal{M}_n(\mathbb{K}),+)$ est un groupe abélien, $\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}$ a une structure naturelle de groupe abélien donnée par l'addition terme à terme (cf. cours I.6.1.i) ;) pour laquelle l'élément neutre est la suite nulle de valeur constante égale à $0_{\mathcal{M}_n(\mathbb{K})}$ et pour laquelle l'opposé d'une suite $\big(M_k\big)_{,k\in\mathbb{N}}$ est la suite $\big(-M_k\big)_{,k\in\mathbb{N}}$.

ii) (Multiplication : anneau)
Comme dans le cas où A est un anneau commutatif, on définira le *produit de* CAUCHY sur $\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}$ (cf. cours III.1.2.2,)

$$\forall (M,P)\in\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}\times\mathcal{M}_n(\mathbb{K})^{\mathbb{N}},\ (M*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}P)_k\ :=\ \sum_{i=0}^{k} M_i *_{\mathcal{M}_n(\mathbb{K})} P_{k-i}\ .$$

Il faut d'ores et déjà remarquer que $*_{\mathcal{M}_n(\mathbb{K})}$ n'étant pas commutative, $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ ne le sera pas davantage. Il est cependant toute à fait élémentaire de vérifier que $\big(U_k\big)_{,k\in\mathbb{N}}$ définie par

$$U_0\ :=\ I\ =\ 1_{\mathcal{M}_n(\mathbb{K})} \text{ et } \forall k\in\mathbb{N}^*,\ U_k\ :=\ 0_{\mathcal{M}_n(\mathbb{K})},$$

est un élément neutre pour $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ qu'on notera abusivment I ou même 1 dans la suite, et que

$$\begin{array}{lll}\forall (M,P,Q)\in\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}\times\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}\times\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}, & (M+P)*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}Q & = \ M*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}Q+P*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}Q \\ \text{et} & M*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}(P+Q) & = \ M*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}P+M*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}Q\ ;\end{array}$$

c'est-à-dire que $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ est distributive sur $+$.
On notera $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ l'anneau ainsi construit.

iii) (Anneau des polynômes)

On s'intéressera cependant surtout au sous-anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ de $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ constitué des suites presque nulles, *i.e.* des suites $\big(M_k\big)_{,k\in\mathbb{N}}$ pour lesquels il existe $p \in \mathbb{N}$ tel que pour tout $q \geq p, M_q = 0_{\mathcal{M}_n(\mathbb{K})}$.

Il est fastidieux mais sans grande difficulté de vérifier que

$$\big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ est effectivement un sous-anneau de } \big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$$

ce qui signifie (cf. cours I.3.3,) que $\big(\big(\mathcal{M}_n(\mathbb{K})\big)[X],+\big)$ est un sous-groupe de $\big(\big(\mathcal{M}_n(\mathbb{K})\big)[X],+\big)$, que $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ est stable par le produit de CAUCHY $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ et que l'élément unité I est dans $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$.

Il ne s'agit rien moins, mais rien de plus non plus que de vérifier que la somme et le produit de deux suites presque nulle est encore une suite presque nulle ; les arguments étant alors exactement de même nature que dans le cas d'un anneau commutatif.

iv) (Degré et valuation)

On peut encore définir la *valuation* $\mathrm{val}(\cdot)$ d'un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ (cf. cours III.1.14,) ou de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ et le *degré* $\deg(\cdot)$ d'un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ (cf. cours III.2.3.) Cependant il convient de s'arrêter un instant sur leurs propriétés (cf. b).)

v) (Morphisme structural)

L'application

$$\iota : \mathcal{M}_n(\mathbb{K}) \to \big(\mathcal{M}_n(\mathbb{K})\big)[[X]], \ M \mapsto (M,0,0,\ldots,0,\ldots)$$

est encore un morphisme injectif d'anneaux qui est en fait à valeurs dans $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$; identifiant $\mathcal{M}_n(\mathbb{K})$ à un sous-anneau de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$; si bien que, pour tout $M \in \mathcal{M}_n(\mathbb{K})$ on notera simplement M pour la série formelle (resp. le polynôme) dont le terme de rang 0 est M et les autres termes sont nuls.

Il est encore clair que l'image $\mathrm{Im}\,\iota$ de ι est l'ensemble des éléments de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ de degré 0.

vi) (Loi externe, structure de $\mathcal{M}_n(\mathbb{K})$-module)

Pour tout

$$(A,M) \in \mathcal{M}_n(\mathbb{K}) \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]$$

on peut définir $A \cdot M := A *_{\big(\mathcal{M}_n(\mathbb{K})\big)[X]} M$, en considérant A comme un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ à travers ι.

vii) (Base)

En X l'élément $(0,1,0,\ldots,0,\ldots) \in \big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$, on constate que c'est en fait un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$, et que

$$\forall k \in \mathbb{N},\ X^k := X *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} \cdots *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} X$$

est la suite dont le $i^{\text{ième}}$ terme est $\delta_{k,i}$. Comme dans le cas commutatif il n'est pas dificile de montrer que $\{X^k\}_{,k\in\mathbb{N}}$ est une $\mathcal{M}_n(\mathbb{K})$-base de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$.

a) $(n = 1)$

Que dire de $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ et $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ lorsque $n = 1$?

b) (Valuation et degré)

Soit $(P,Q) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]$, que peut-on dire de :

$$\begin{aligned} &\mathrm{val}(P+Q),\\ &\mathrm{val}(P*Q),\\ &\deg(P+Q)\\ \text{et}\quad &\deg(P*Q)\,. \end{aligned}$$

Bien qu'on n'ait pas, en général, $P*Q = Q*P$, aurait-on cependant

$$\deg(P*Q) = \deg(Q*P)\ ?$$

3) Montrer qu'il existe un unique morphisme d'anneau $\mathcal{M}_n(\mathbb{K})$-linéaire :

$$\begin{array}{rccl} \phi: & \big(\mathcal{M}_n(\mathbb{K})\big)[X] & \longrightarrow & \mathcal{M}_n(\mathbb{K}[X]) \\ & X & \longmapsto & M_1 := \begin{pmatrix} X & 0 & \ldots & 0 & 0 \\ 0 & X & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & X & 0 \\ 0 & 0 & \ldots & 0 & X \end{pmatrix} \end{array}$$

et que de plus ϕ est un isomorphisme.

Indication : *On pourra noter*

$$\forall i \in \mathbb{N},\ M_i := M_1^i$$

et remarquer que M_i commute avec tous les éléments de $\mathcal{M}_n(\mathbb{K}[X])$.

L'isomorphisme ϕ ci-dessus permet donc d'identifier (en tant qu'anneau) les polynômes dont les coefficients sont des matrices $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ au matrices dont les coefficients sont des polynômes $\mathcal{M}_n(\mathbb{K}[X])$. On se placera donc, dans la suite, sous l'un ou l'autre point de vue, selon ce qui sera le plus commode. En particulier on oubliera la notation M_i pour lui préférer X^i, dont on gardera bien à l'esprit que c'est une matrice qui commute avec n'importe quel élément de $\mathcal{M}_n(\mathbb{K}[X])$. On notera I l'unité de ces anneaux qui est la matrice identité de $\mathcal{M}_n(\mathbb{K})$.

4) (Valuation et degré)

Pour $M \in \big(\mathcal{M}_n(\mathbb{K})\big)[X]$ comparer la valuation et le degré de M définis en question 2), iv) et les valuations et degré respectifs des coefficients de la matrice $\phi(M)$.

5) (Éléments inversibles)

Puisque $\mathcal{M}_n(\mathbb{K})$ est un sous-anneau de $\phi : \big(\mathcal{M}_n(\mathbb{K})\big)[X] \cong \mathcal{M}_n(\mathbb{K}[X])$, tout inversible de $\mathcal{M}_n(\mathbb{K})$ est encore inversible dans $\mathcal{M}_n(\mathbb{K}[X])$. En revanche il n'est pas tout à fait immédiat de déterminer exactement ce qu'est $(\mathcal{M}_n(\mathbb{K}[X]))^\times$; ce dont d'ailleurs nous n'aurons pas explicitement besoin. On peut cependant remarquer :

a) (Matrice de carré nul)

Montrer que si $A \in \mathcal{M}_n(\mathbb{K})$ vérifie $A^2 = 0$, $I - AX$ est inversible.

b) (Matrices nilpotentes)

Plus généralement montrer que si $A \in \mathcal{M}_n(\mathbb{K})$ est tel que $A^n = 0$, (nilpotente d'échelon n (cf. cours IV.8.1,)) $I - AX$ est inversible.

6) (Division euclidienne)

Pour tout $(M, P) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]$ tel que

$$P = \sum_{i=0}^{d} P_i X^i \text{ avec } P_d \in \mathcal{M}_n(\mathbb{K})^\times \text{ inversible,}$$

montrer qu'il existe

$$(Q, R) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ tel que } M = P * Q + R \text{ et } \deg(R) < \deg(P) .$$

Indication : *On pourra adapter la méthode utilisée dans le III.7.7.*

7) (Facteurs irréductibles)

Soit

$$A \in \mathcal{M}_n(\mathbb{K}) \text{ et } M := P_{\textbf{min } A} I \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \cong \mathcal{M}_n(\mathbb{K}[X]) .$$

a) (Division euclidienne)

Montrer qu'il existe

$$(Q, R) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ tel que } M = (A - IX) * Q + R \text{ et } \deg(R) < 1 .$$

b) Montrer que $R = 0$.

c)

$$P_{\text{car } A} | [P_{\text{min } A}]^n .$$

d) (Facteurs irréductible)

En déduire que tout facteur irréductible de $P_{\text{car } A}$ est un facteur irréductible de $P_{\text{min } A}$.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Corrigé du Problème n° II

Exercice A : (La suite des noyaux itérés)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \text{ on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

Cet exercice peut être traité de manière tout à fait élémentaire et ne nécessite l'usage ni du théorème IV.10.10 de JORDAN ni du théorème IV.11.5 de réduction de FROBENIUS.

1) () Montrer qu'il existe un vecteur $x \in E$ tel que la famille $\{f^i(x)\}_{,0 \leq i \leq \varepsilon-1}$ est libre.

Solution : *Puisque, par hypothèse $f^{\varepsilon-1} \neq 0$,*

$$\exists x \in E,\ f^{\varepsilon-1}(x) \neq 0\,.$$

Il s'ensuit immédiatement que

$$\forall 0 \leq i \leq \varepsilon - 1,\ f^i(x) \neq 0\,.$$

Par ailleurs, bien entendu

$$\forall k \in \mathbb{N},\ k \geq \varepsilon \Rightarrow f^k(x) = 0\,.$$

Il s'ensuit que pour tout

$$\begin{array}{lll} a_{i\,,0\leq i\leq \varepsilon-1} \in \mathbb{K} & \sum_{i=0}^{\varepsilon-1} a_i f^i(x) & = 0 \\ \Rightarrow & f^{\varepsilon-1}\big(\sum_{i=0}^{\varepsilon-1} a_i f^i(x)\big) & = 0 \\ \Rightarrow & \sum_{i=0}^{\varepsilon-1} a_i f^{i+\varepsilon-1}(x) & = 0 \\ \Rightarrow & a_0 f^{\varepsilon-1}(x) & = 0 \\ \Rightarrow & a_0 & = 0\,. \end{array}$$

On établit ainsi que

$$\forall 0 \leq i \leq \varepsilon - 1,\ a_i = 0\,.$$

2) () **(polynôme minimal)**

Quel est le polynôme minimal de f ? Qu'en déduit-on sur ε et n ?

Solution : *Par définition, X^{ε} est un polynôme annulateur de f ; si bien que $P_{\mathrm{min}\,f} | X^{\varepsilon}$. Le polynôme X étant irréductible dans $\mathbb{K}[X]$, $\exists k \in \mathbb{N},\ P_{\mathrm{min}\,f} = X^k$. Puisque $f^{\varepsilon-1} \neq 0$ par hypothèse*

$$P_{\mathrm{min}\,f} = \varepsilon\,.$$

Or on a montré (cf. question 1),) qu'il existe alors une famille libre à ε éléments dans E ; ce qui entraîne

$$\varepsilon \leq n\,.$$

Bien entendu on pouvait obtenir l'inégalité ci-dessus grâce au gthéorème IV.7.2 de CAYLEY–HAMILTON *puisque*

$$\varepsilon = \deg(P_{\mathrm{min}\,f}) \leq \deg(P_{\mathrm{car}\,f}) = n\,;$$

néanmoins l'argument de question 1) est beaucoup plus élémentaire.

3) () Montrer que la suite

$$\{0\} \subset \operatorname{Ker} f \subset \ldots \subset \operatorname{Ker} f^{\varepsilon-1} \subset \operatorname{Ker} f^{\varepsilon} = E$$

est strictement croissante ; et constante lorsque $k \geq \varepsilon$.

Solution : *Soit $k \in \mathbb{N}$ tel que $N_k = N_{k+1}$. Alors*

$$\begin{array}{lrcl} \forall p \in \mathbb{N},\ \forall x \in N_{k+1+p}, & f^{k+1+p}(x) & = & 0 \\ \Leftrightarrow & f^{k+1}[f^p(x)] & = & 0 \\ \Leftrightarrow & f^p(x) & \in & N_{k+1} \\ \Leftrightarrow & f^p(x) & \in & N_k \\ \Leftrightarrow & f^{k+p}(x) & = & 0 \\ \Leftrightarrow & x & \in & N_{k+p}\ . \end{array}$$

4) () Montrer qu'il existe une base de E dans laquelle la matrice de f est triangulaire supérieure stricte.

Solution : *Cette assertion équivaut en fait à construire une fammille $E_{i\ ,0\leq i\leq n}$ de sous-$\mathbb{K}$-espaces vectoriels de E, tels que*

$$\forall 0 \leq i \leq n,\ \dim_{\mathbb{K}} E_i = i \text{ et } \forall 1 \leq i \leq n,\ E_{i-1} \subset E_i \text{ et } f(E_i) \subset E_{i-1}\ .$$

En effet E_1 est alors une ddroite dont on peut prendre une base e_1. $E_1 \subset E_2$ qui est un plan et dans lequel la base e_1 se complète en une base (e_1, e_2). On construit ainsi, de proche en proche, une base $\mathcal{B} := (e_1, \ldots, e_n)$. Or la condition $f(E_i) \subset E_{i-1}$ entraîne que $f(e_1) = 0$ et que pour $i > 1$, $f(e_i)$ s'exprime en fonction des $e_{j\ ,1\leq j\leq i-1}$; ce qui signifie exactement que la matrice de f dans la base $\mathcal{B}$ est triangulaire supérieure stricte.

Reste à construire le « drapeau » $E_{i\ ,0\leq i\leq n}$. On verra à la question 6) que dans le cas où $\varepsilon = n$, la suite $N_{i\ ,0\leq i\leq n\,=\,\varepsilon}$ des noyaux convient. Dans le cas général, on a montré (cf. question 3),) que cette suite est cependant strictement croissante. Il se pourrrrait que le « saut de dimension » entre deux noyaux successifs soit plus grand strictement que 1 [8]

On aura nécessairement

$$E_0 = \{0\} \text{ et } E_n = N_\varepsilon = E\ .$$

Supposons donc qu'on ait construit $E_{k\ ,i\leq k\leq n}$ avec

$$\dim_{\mathbb{K}} E_k = k\ ,\ E_{k-1} \subset E_k \text{ et } f(E_k) \subset E_{k-1}$$

tel que $E_i = N_j$.

Bien entendu si $N_j = N_0 = \{0\}$, on a terminé.

Sinon, soit

$$\dim_{\mathbb{K}} N_{j-1} = \dim_{\mathbb{K}} N_j - 1$$

et l'on pose

$$E_{i-1} = N_{j-1}\ ;$$

soit on « intercale » le nombre de E_k qu'il faut. Plus précisément il existe $E_{k\ ,i-(\dim_{\mathbb{K}} N_j - \dim_{\mathbb{K}} N_{j-1})\leq k\leq i}$ tel que

$$E_{i-(\dim_{\mathbb{K}} N_j - \dim_{\mathbb{K}} N_{j-1})} = N_{j-1}\ ,\ E_k \subset E_{k+1} \text{ et } \dim_{\mathbb{K}} E_k = k\ .$$

Comme par ailleurs $E_k \subset N_j$,

$$f(E_k) \subset f(N_j) \subset N_{j-1} \subset E_{k-1}\ .$$

5) () Dans le cas où $\varepsilon = n$, montrer qu'il existe une base où la matrice de f est

$$J_n(0) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}\ .$$

Solution : *Dans le cas où $\varepsilon = n$, la famille libre $f^i(x)_{\,,0\,\leq\, i\,\leq\, \varepsilon-1}$ (cf. question 1),) est une base de E dans laquelle la matrice de f est précisément* $\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$.

8. On pourra même calculer très précisément ces sauts (cf. exercice C, question 3), exercice C, question 4) ;) mais on a alors supposé qu'on disposait d'une réduite de JORDAN ce dont on peut se passer ici.

6) () Quand $\varepsilon = n$, décrire complètement la suite $\dim_{\mathbb{K}} N_{i\,,i\in\mathbb{N}}$.

Solution : *Choisissons une base $e_{i\,,0\le i\le n-1}$ donnée par un vecteur*

$$x \in E \text{ tel que } \{e_i := f^i(x)\}_{,0\le i\le \varepsilon-1} \text{ soit une base de } E \text{ (cf. question 1) .)}$$

Alors :

$$\begin{array}{rcl} \forall 1\le i\le n,\quad \forall 0\le j\le n-1-i,\ f^i(e_j) & = & e_{i+j} \\ \forall n-i\le j\le n-1,\ f^i(e_j) & = & 0\,. \end{array}$$

Il s'ensuit que

$$\begin{array}{ll} f_{|\mathrm{Vect}\left\{e_{j\,,0\le j\le n-1-i}\right\}} & \text{est injective} \\ f_{|\mathrm{Vect}\left\{e_{j\,,n-i\le j\le n-1}\right\}} & \text{est nulle .} \end{array}$$

Comme par ailleurs

$$E = \mathrm{Vect}\left\{e_{j\,,0\le j\le n-1-i}\right\} \oplus \mathrm{Vect}\left\{e_{j\,,n-i\le j\le n-1}\right\},$$

on en déduit que

$$\forall 0\le i\le n-1,\ N_i = \mathrm{Vect}\left\{e_{j\,,n-i\le j\le n-1}\right\} \Rightarrow \dim_{\mathbb{K}} N_i = i\,.$$

Enfin $f^n = 0$, si bien que

$$\forall i\in\mathbb{N},\ i \ge n = \dim_{\mathbb{K}} N_i = n\,.$$

Exercice B : (Injection de FROBENIUS)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \text{ et} f^{\varepsilon-1} \ne 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k\in\mathbb{N},\ \textbf{on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

On note

$$\forall i\in\mathbb{N}^*,\ d_i := \dim_{\mathbb{K}} N_i - \dim_{\mathbb{K}} N_{i-1}\,.$$

Il est vraisemblable que nombre des énoncés de cet exercice peuvent être obtenus comme corollaires du théorème IV.10.10 de réduction de JORDAN, mais on va chercher à les établir ici par des méthodes plus élémentaires.

1) (0.5points) Étant donnés un $\mathbb{K}$-espace vectoriel V de dimension finie et $W \subset V$ un sous-espace de V, , rappeler ce que vaut $\dim_{\mathbb{K}} V/W$ en fonction de $\dim_{\mathbb{K}} V$ et $\dim_{\mathbb{K}} W$.

Solution : *On a*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W$$

en application par exemple du théorème I.9.19 qui se déduit en fait du fait que V/W est isomorphe à n'importe qu'elle supplémentaire de W dans V.

2) (0.5points) Montrer que

$$\forall i\in\mathbb{N},\ d_i \ge 0\,.$$

Solution : *(cf. exercice A, question 3),) d'où l'on peut même déduire plus précisément que*

$$\forall 1\le i\le\varepsilon,\ d_i > 0 \text{ et } \forall k\in\mathbb{N},\ k > \varepsilon \Rightarrow d_k = 0\,.$$

3) (0.5points) Vérifier que, pour tout $i \in \mathbb{N}$, la restriction $f_{|N_{i+1}}$ de f à N_{i+1} est à valeurs dans N_i.

Solution :

$$\forall x\in N_{i+1},\ u^i[u(x)] = u^{i+1}(x) = 0 \Leftrightarrow u(x) \in N_i\,.$$

Pour tout $i \in \mathbb{N}$, **on note**

$$p_i : N_{i+1} \to N_{i+1}/N_i \textbf{ la surjection canonique} .$$

4) (1point) Montrer que, pour tout $i \in \mathbb{N}$, il existe un unique morphisme

$$f_i : N_{i+2}/N_{i+1} \to N_{i+1}/N_i tq\ f_i \circ p_{i+1} = p_i \circ f_{|N_{i+2}} .$$

Solution : *Considérons le diagramme commutatif :*

$$\begin{array}{ccc} N_{i+1} & \hookrightarrow & N_{i+2} \\ {\scriptstyle f_{|N_{i+1}}}\downarrow & & \downarrow{\scriptstyle f_{|N_{i+2}}} \\ N_i & \hookrightarrow & N_{i+1} \end{array}$$

dont les flèches horizontales sont injectives. On obtient, par factorisation un morphisme

$$f_i : N_{i+2}/N_{i+1} \to N_{i+1}/N_i$$

si bien qu'on a un morphisme de suites exactes (c'est-à-dire un diagramme commutatif à lignes exactes) :

$$\begin{array}{ccccccccc} 0 & \to & N_{i+1} & \longrightarrow & N_{i+2} & \xrightarrow{p_{i+1}} & N_{i+2}/N_{i+1} & \to & 0 \\ & & {\scriptstyle f_{|N_{i+1}}}\downarrow & & {\scriptstyle f_{|N_{i+2}}}\downarrow & & \downarrow{\scriptstyle f_i} & & \\ 0 & \to & N_i & \longrightarrow & N_{i+1} & \xrightarrow{p_i} & N_{i+1}/N_i & \to & 0 \end{array} .$$

5) (1point) Montrer que

$$\forall i \in \mathbb{N},\ f_i \text{ est injective} .$$

On l'appellera l'*injection de* FROBENIUS.

Solution :

$$\forall y \in N_{i+2}/N_{i+1},\ \exists x \in N_{i+2},\ \textit{tel que}\ p_{i+1}(x) = y .$$

Alors :

$$\begin{array}{rrcl} & f_i(y) & = & 0 \\ \Leftrightarrow & f_i[p_{i+1}(x)] & = & 0 \\ \Leftrightarrow & p_i[u(x)] & = & 0 \\ \Leftrightarrow & u(x) & \in & N_i \\ \Rightarrow & x & \in & N_{i+1} \\ \Rightarrow & p_{i+1}(x) & = & 0 \\ \Rightarrow & y & = & 0 . \end{array}$$

Ainsi f_i est injective.

6) (0.5points) Déduire de ce qui précède que $d.$ est décroissante.

Solution :

$$\begin{array}{rcll} \forall i \in \mathbb{N},\quad d_{i+1} - d_i & = & \big(\dim_{\mathbb{K}} N_{i+1} - \dim_{\mathbb{K}} N_i\big) & \\ & & -\big(\dim_{\mathbb{K}} N_i - \dim_{\mathbb{K}} N_{i-1}\big) & \textit{(cf. question 1) .)} \\ & = & \dim_{\mathbb{K}} N_{i+1}/N_i - \dim_{\mathbb{K}} N_i/N_{i-1} & \end{array}$$

Or f_{i-1} étant injectif (cf. question 5),)

$$\dim_{\mathbb{K}} N_{i+1}/N_i \leq \dim_{\mathbb{K}} N_i/N_{i-1}$$

ce qui conclut.

Exercice C : (Tableaux de YOUNG)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \ \textbf{on note} \ N_k := \mathrm{Ker}\, f^k \,\mathrm{et}\, n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

1) (0.5points) Justifier, en citant précisément le théorème que vous utilisez, mais sans le redémontrer bien entendu, qu'il existe un entier $m \in \mathbb{N}^*$, des entiers strictement positifs $r_{j\ ,1\leq j\leq m}$ et des sous espaces $E_{j\ ,1\leq j\leq m}$ tels que :

J$_1$)
$$E = \bigoplus_{j=1}^{m} E_j \ ;$$

J$_2$) $\forall 1 \leq j \leq m,\ E_j$ est stable par f ;

J$_3$)
$$\forall 1 \leq j \leq m-1,\ r_j \geq r_{j+1} \ ;$$

J$_4$) le sous-espace $(E_j, f_{|E_j})$ est cyclique de polynômes minimal X^{r_j}.

Solution : *Le polynôme minimal de f est X^{ε}. Il est sindé et n'a qu'un facteur irréductible, si bien que dans ce cas, aussibien le théorème IV.11.5 de réduction de* FROBENIUS *que le théorème IV.10.10 donne le résultat demandé.*

2) (0.5points) Que vaut $\displaystyle\sum_{j=1}^{m} r_j$?

Solution : *Puisque les sous-espaces $E_{j\ ,1\leq j\leq m}$ sont cycliques, on a :*

$$\forall 1 \leq j \leq m,\ \dim_{\mathbb{K}} E_j = \deg(P_{\mathit{min}\, f_{|E_j}}) = r_j \ \textit{(cf. IV.4.1 .)}$$

Or il résulte de question 1), J$_1$) que

$$n = \dim_{\mathbb{K}} E = \sum_{j=1}^{m} \dim_{\mathbb{K}} E_j = \sum_{j=1}^{m} r_j \ .$$

On peut donc trouver une base de E dans laquelle la matrice de f est J :

Pour tout $r \leq n$, soit

$$J_r := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} \in \mathcal{M}_r(\mathbb{C})$$

le bloc de JORDAN "élémentaire".

La matrice J est donc de la forme

$$J = \mathbf{diag}\,(J_{r_1}, J_{r_2}, \cdots, J_{r_m}) = \begin{pmatrix} J_{r_1} & 0 \cdots & \cdots & 0 \\ 0 & J_{r_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{r_m} \end{pmatrix}$$

pour un certain entier m .

3) (0.5points) (**Décomposition des noyaux**)
Notons

$$\forall 1 \leq i \leq m,\ f_i \ := \ f_{|E_i}\ .$$

Pour tout $k \ \in \ \mathbb{N}$ et tout $1 \ \leq \ i \ \leq \ m$, donnez une relation entre les $n_{i,k} \ := \ \dim \mathrm{Ker}\, f_i^k$ et n_k .

Solution : *Étant donné un endomorphisme u d'un espace vectoriel E tel que E soit somme directe des F_α ,$1 \leq \alpha \leq q$, stables par u, alors*

$$\mathrm{Ker}\, u \ = \ \bigoplus_{\alpha=1}^{q} \mathrm{Ker}\, u \cap F_\alpha\ .$$

De plus, $\mathrm{Ker}\, u \cap F_\alpha$ *est le noyau de la restriction u_α de u à F_α .*

En effet pour tout $x \in \mathrm{Ker}\, u$, il existe un unique q-uplet $(x_1, \ldots, x_q)$ $x_\alpha \in F_\alpha$, tel que $x \ = \ \sum_{\alpha=1}^{q} x_\alpha$. Par conséquent

$$\begin{aligned} & u(x) &=& \ 0 \\ \Leftrightarrow \quad & u\big(\sum_{\alpha=1}^{q} x_\alpha\big) &=& \ 0 \\ \Leftrightarrow \quad & \sum_{\alpha=1}^{q} u(x_\alpha) &=& \ 0\ . \end{aligned}$$

Or chacun des F_α étant stable par u, pour tout $1 \ \leq \ \alpha \ \leq \ q$, $u(x_\alpha) \in F_\alpha$. La décomposition de 0 étant unique sur les F_α, il en résulte que pour tout $1 \ \leq \ \alpha \ \leq \ q$, $u(x_\alpha) = 0$.

On vient donc de montrer que $\mathrm{Ker}\, u$ *est inclus dans la somme des* $\mathrm{Ker}\, u \cap F_\alpha$.

Cette dernière somme est directe car la décomposition de tout vecteur de E étant unique sur les F_α ceci est a fortiori vrai pour un élément de la somme des $\mathrm{Ker}\, u \cap F_\alpha$ *. Cette décomposition reste bien évidemment unique sur des sous-espaces des F_α .*

L'inclusion réciproque est claire.

Enfin si u_α désigne la restriction de u à F_α, pour tout $x \in F_\alpha$, $u_\alpha(x) = 0$ équivaut à $x \in F_\alpha$ et $u(x) = 0$, c'est-à-dire que $\mathrm{Ker}\, u \cap F_\alpha$ *est bien le noyau de la restriction de u à F_α .*

On applique le résultat précédent à $u \ := \ f^k$ et à la décomposition de E en somme directe des E_i ,$1 \ \leq \ i \ \leq \ m$, en ayant soin de remarquer que la restriction de f^k à E_i est bien f_i^k, et on en déduit que

$$n_k \ = \ \sum_{i=1}^{m} n_{i,k}\ .$$

4) (0.5points) Établir la valeur de $n_{i,k}$ en fonction de k et de r_i.

Solution : *Si $f_i \ := \ f_{|E_i}$ désigne, pour tout $1 \ \leq \ i \ \leq \ m$ la restriction de f à E_i, f_i est nilpotante d'échelon $r_i \ = \ \dim_{\mathbb{K}} E_i$.*
On a donc

$$\forall 0 \leq k \leq r_i,\ n_{i,k} \ = \ k \text{ et } \forall k \in \mathbb{N},\ k \ \geq \ r_i \ \Rightarrow \ n_{i,k} \ = \ r_i \text{ (cf. exercice A, question 6) ,)}$$

ce qui peut aussi s'écrire :

$$n_{i,k} \ = \ \min(k, r_i)\ .$$

5) (0.5points) En déduire que

$$n_1 \ := \ \dim \mathrm{Ker}\, f \ = \ m \text{ et } n_k \ = \ \sum_{i=1}^{m} \min(k, r_i)\ .$$

Solution : *Pour tout $1 \ \leq \ i \ \leq \ m$, on a $r_i \geq 1$, ce qui implique (cf. question 4),) que $n_{i,1} = 1$ et par conséquent $n_1 = m$.*

$$n_k \ = \ \sum_{i=1}^{m} n_{i,k} \ = \ \sum_{i=1}^{m} \min(r_i, k)\ .\ \text{(cf. question 3) , question 4))}$$

On définit le *tableau de* YOUNG de (E,f) comme le tableau constitué de m lignes, alignées sur la gauche et tel que la $j^{\text{ième}}$ ligne comporte r_j cases. Par exemple si $m = 3, (r_1,r_2,r_3) = (5,4,1)$, le tableau de YOUNG est

$$Y(E,f) = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix}.$$

6) (1.5points) Montrer que pour tout $j \in \mathbb{N}^*$, $d_j := \dim_{\mathbb{K}} N_j - \dim_{\mathbb{K}} N_{j-1}$ est la hauteur (le nombre de cases) de la $j^{\text{ième}}$ colonne du tableau de YOUNG $Y(E,f)$.

Solution : *Si l'on note h_j la hauteur de la $j^{\text{ième}}$ colonne du tableau de* YOUNG*, par construction*

$$h_j = \#\big(\{i \in \mathbb{N}\,;\, r_i \geq j\}\big).$$

Puisque le tableau de YOUNG *est construit en rangeant les r_i par ordre décroissant, on a*

$$\forall 1 \leq i \leq h_j,\ r_i \geq j \text{ et } \forall h_j + 1 \leq i \leq m,\ r_i < j\,.$$

Alors

$$\begin{array}{rcccccc} \forall 1 \leq i \leq h_j, & n_{i,j} & = & j & \text{et} & n_{i,j-1} & = & j-1 \\ \forall h_j + 1 \leq i \leq m, & n_{i,j} & = & r_j & \text{et} & n_{i,j-1} & = & r_j \end{array} \quad \textit{(cf. question 4) .)}$$

Il s'ensuit que :

$$\begin{aligned} d_j &= n_j - n_{j-1} \\ &= \sum_{i=1}^{m} n_{i,j} - n_{i,j-1} \\ &= \sum_{i=1}^{h_j} n_{i,j} - n_{i,j-1} + \sum_{i=h_j+1}^{m} n_{i,j} - n_{i,j-1} \\ &= \sum_{i=1}^{h_j} j - (j-1) + \sum_{i=h_j+1}^{m} r_j - r_j \\ &= h_j\,. \end{aligned}$$

7) (1.5points) **a)** (1.5points) Donner les invariants de similitudes de f nilpotent dont le tableau de YOUNG est

$$Y(E,f) = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix}.$$

Solution : *On a immédiatement*

$$m = 3\,,\ r_1 = 5\,,\ r_2 = 4 \text{ et } r_3 = 1\,.$$

b) (1.5points) Quelle est la dimension de E ?

Solution :

$$\dim_{\mathbb{K}} E = \sum_{i=1}^{m} r_i = 5 + 4 + 1 = 10\,. \textit{ (cf. question 2) .)}$$

c) (1.5points) Quels sont le tableau de YOUNG de f^2 et ses invariants de similitude.

Solution : *Cette question est l'une de celles qui met le mieux en évidence l'intérêt des tableaux de* YOUNG *dans l'études des endomorphismes nilpotents. En effet ces tableaux mettent en relation (leur lignes) les invariants de similitude r_i ,$1 \leq i \leq m$ d'un endomorphisme nilpotent et les sauts (les colonnes) dans la suite des noyaux itérés d_j ,$1 \leq j \leq r_1$. Comme chaque fois qu'on établit de telles correspondances il se peut que, suivant les situations, certains invariants soient plus facile à calculer ; ce qui permet de déterminer les autres.*

Typpiquement si l'on note $g := f^2$, on va constater que les sauts dans la suites des noyaux sont assez faciles à déterminer alors qu'il semble beaucoup moins immédiat de calculer les invariants de similitude. En effet,

$$\begin{aligned} \forall j \in \mathbb{N}^*,\quad \dim_{\mathbb{K}} \operatorname{Ker} g^j - \dim_{\mathbb{K}} \operatorname{Ker} g^{j-1} &= \dim_{\mathbb{K}} \operatorname{Ker} f^{2j} - \dim_{\mathbb{K}} \operatorname{Ker} f^{2j-2} \\ &= n_{2j} - n_{2j-2} \\ &= (n_{2j} - n_{2j-1}) + (n_{2j-1} - n_{2j-2})\,. \end{aligned}$$

Il faut donc « empiler l'une sur l'autre » (cf. question 6),) deux colonnes successives du tableau de f pour obtenir celui de g. Il en résulte, dans le cas particulier considéré ici que

$$Y(E,f^2) \;=\; Y(E,g) \;=\; \begin{pmatrix} * & * & * \\ * & * & \\ * & * & \\ * & * & \\ * & & . \end{pmatrix} .$$

Il an résulte que

$$m \;=\; 5\,,\; r_1 \;=\; 3\,,\; r_2 \;=\; r_3 \;=\; r_4 \;=\; 2 \;=\; r_5 \;=\; 1\,.$$

Exercice D : (**Commutant**)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie n et $u \in \mathrm{End}_{\mathbb{K}}(E)$. On appelle *commutant de* u et on note

$$\mathrm{Com}(u) \;:=\; \{v \in \mathrm{End}_{\mathbb{K}}(E)\,;\, u\circ v \;=\; v\circ u\} \subset \mathrm{End}_{\mathbb{K}}(E)$$

l'ensemble des endomorphismes de E qui commutent avec u. On rappelle que $\mathbb{K}[u] \subset \mathrm{End}_{\mathbb{K}}(E)$ est l'ensemble des polynômes en u *i.e.* l'image de $\mathbb{K}[X]$ par le morphisme $X \mapsto u$.

1) (0.5points) Montrer que $\mathrm{Com}(u)$ est un sous espace vectoriel de $\mathrm{End}_{\mathbb{K}}(E)$.

Solution : *Il est clair que l'application nulle et l'identité de E appartiennent à $\mathrm{Com}(u)$ qui est donc non vide. Par ailleurs pour v et w dans $\mathrm{Com}(u)$, a et b dans $\mathbb{K}$,*

$$\begin{aligned} u\circ(av+bw) &= u\circ av + u\circ bw \\ &= av\circ u + bw\circ u \\ &= (av+bw)\circ u \end{aligned}$$

c'est-à-dire que $av+bw \in \mathrm{Com}(u)$ ce qui prouve que $\mathrm{Com}(u)$ est un sous espace vectoriel de $\mathrm{End}_{\mathbb{K}}(E)$.

On peut également constater que l'application

$$\mathrm{End}_{\mathbb{K}}(E) \;\to\; \mathrm{End}_{\mathbb{K}}(E)\,,\; v \;\mapsto\; u\circ v \;-\; v\circ u$$

est linéaire et que $\mathrm{Com}(u)$ est son noyau.

2) (2points) **On suppose dans cette question que u est cyclique et que $x_0 \in E$ est un vecteur cyclique pour u.**

a) (1points) En considérant l'application

$$\varphi \;:\; \mathrm{Com}(u) \;\to\; E\,,\; v \;\mapsto\; v(x_0),$$

montrer que l'on a $\dim_{\mathbb{K}} \mathrm{Com}(u) \leqslant n$.

Solution : *Soit $v \in \mathrm{Com}(u)$ tel que $\phi(v) = 0$ c'est-à-dire que $v(x_0) = 0$. On en déduit alors que*

$$\forall 1 \leq k \leq n-1,\; v[u^k(x_0)] \;=\; u^k[v(x_0)] \;=\; u^k(0) \;=\; 0$$

c'est-à-dire que v s'annule sur une base de E et donc que $v = 0$.

Il s'ensuit que ϕ est injective ce qui entraîne

$$\dim \mathrm{Com}(u) \;\leq\; \mathrm{rg}(\phi) \;\leq\; \dim E \;\leq n\,.$$

b) (1point) Montrer que $\dim \mathbb{K}[u] \geq n$ et que

$$\mathrm{Com}(u) \;=\; \mathbb{K}[u]\,.$$

On pourra remarquer, en particulier que si u est nilpotent d'échelon n (cf. cours IV.8.1,)

$$\mathrm{Com}(u) \;\cong\; \mathbb{K}[u]\,.$$

Solution :

i) Considérons la famille $F_U := \{u^i\}_{,0 \leq i \leq n-1} \subset \mathbb{K}[u]$. *Pour tout* n*-uplet* $(a_0, \ldots, a_{n-1})$ *d'éléments de* $\mathbb{K}$,

$$\begin{aligned} \sum_{i=0}^{n-1} a_i u^i &= 0 \\ \Rightarrow \sum_{i=0}^{n-1} a_i u^i(x_0) &= 0 \\ \Rightarrow \qquad a_i &= 0 \; \forall 0 \leq i \leq n-1, \end{aligned}$$

puisque $\mathcal{B}$ *est une base de* E. *Il en résulte que* F_u *est une famille libre de cardinal* n *de* $\mathbb{K}[u]$ *qui est donc de dimension au moins* n.

On pourrait aussi voir que

$$\mathbb{K}[u] \cong \mathbb{K}[X]/P_{\min u}$$

qui est (cf. TD n° V, exercice C,) un espace vectoriel de dimension $\deg(P_{\min u})$. *Or* u *étant cyclique*

$$\deg(P_{\min u}) = n \text{ (cf. IV.4.1 .)}$$

ii) Pour tout $v \in \mathbb{K}[u]$, *il existe*

$$a_{i\,,0 \leq i \leq k} \in \mathbb{K} \text{ tel que } v = \sum_{i=0}^{k} a_i u^i \, .$$

Il s'ensuit que

$$\begin{aligned} u \circ v &= u \circ \big(\sum_{i=0}^{k} a_i u^i\big) \\ &= \sum_{i=0}^{k} a_i u^{i+1} \\ &= \big(\sum_{i=0}^{k} a_i u^i\big) \circ u \\ &= v \circ u \, . \end{aligned}$$

Il en résulte donc que $\mathbb{K}[u] \subset \mathrm{Com}(u)$ *ce qui combiné aux inégalités précédemment obtenues sur les dimensions donne finalement*

$$\mathbb{K}[u] = \mathrm{Com}(u) \, .$$

3) (0.5point) Supposons que $E = \bigoplus_{i=1}^{r} E_i$ avec E_i stable par u. Comparer

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \text{ et } \sum_{i=1}^{r} \dim_{\mathbb{K}} \mathrm{Com}(u_{|E_i}) \, .$$

Solution : *Notons* $\forall 1 \leq i \leq r, \; u_i := u_{|E_i}$. *Pour tout* $v_{i\,,1 \leq i \leq r} \in \mathrm{Com}(u_i)$ *notons* $v \in \mathrm{End}_{\mathbb{K}}(E)$ *l'unique endomorphisme de* E *défini par*

$$\forall x := \sum_{i=1}^{r} x_{i\,,x_i \in E_i} \in E, \; v(x) := \sum_{i=1}^{r} v_i(x_i) \, .$$

Notons que si l'on s'est donné des bases des sous-espaces E_i *dont la réunion forme une base de* E, *ce qui précède revient à écrire la matrice de* v *par blocs. De manière plus abstraite, c'est une conséquence de la proposition A.4.7.*

Alors :

$$\begin{aligned} \forall x \in E, \quad u[v(x)] &= u\big(\sum_{i=1}^{r} v(x_i)\big) \\ &= u\big(\sum_{i=1}^{r} v_i(x_i)\big) \\ &= \sum_{i=1}^{r} u[v_i(x_i)] \\ &= \sum_{i=1}^{r} u_i[v_i(x)] \\ &= \sum_{i=1}^{r} v_i[u_i(x_i)] \\ &= v\big(\sum_{i=1}^{r} u_i(x_i)\big) \\ &= v[u(x)] \, . \end{aligned}$$

On construit ainsi une application

$$\gamma \,:\, \prod_{i=1}^{r} \mathrm{Com}(u_i) \;\to\; \mathrm{Com}(u)\,.$$

C'est une vérification assez pénible mais sans grande difficulté que de montrer que γ est linéaire. De plus :

$$\begin{array}{lrcl} \forall v_i\,,1\leq i\leq r \in \prod_{i=1}^{r} \mathrm{Com}(u_i), & \gamma(v) & = & 0 \\ \Leftrightarrow \qquad \forall 1\leq i\leq r,\ \forall x\in E_i,\ & \gamma(v)(x) & = & 0 \\ \Leftrightarrow & v_i(x) & = & 0 \\ \Leftrightarrow & \forall 1\leq i\leq r,\ v_i & = & 0\,; \end{array}$$

c'est-à-dire que γ est injective ; d'où l'on déduit que

$$\sum_{i=1}^{r} \dim_{\mathbb{K}} \mathrm{Com}(u_i) \;=\; \dim_{\mathbb{K}}\big(\prod_{i=1}^{r} \mathrm{Com}(u_i)\big) \;\leq\; \dim_{\mathbb{K}} \mathrm{Com}(u)\,.$$

4) (2.5points) **On suppose que $E = E_1 \oplus E_2$, où E_i est stable par u, cyclique de polynôme minimal μ_i avec $\mu_2|\mu_1$.**

a) (0.5points) Montrer qu'il existe une base $\mathcal{B}$ de E telle que :

$$M_{\mathcal{B}}(u) \;=\; \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix}$$

où pour tout polynôme $R \in \mathbb{K}[X]$, C_R désigne la matrice compagnon de R.

Solution : *Par définition des espaces Cycliques (cf. cours IV.4.1.)*

b) (1.5point) En déduire qu'il existe un endomorphisme $v \in \mathrm{Com}(u) \setminus \{0\}$ dont la matrice dans la base $\mathcal{B}$ est de la forme

$$M_{\mathcal{B}}(v) \;=\; \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}.$$

Solution : *Si un tel v existe :*

$$\begin{array}{lrcl} & M_{\mathcal{B}}(u)M_{\mathcal{B}}(v) - M_{\mathcal{B}}(v)M_{\mathcal{B}}(u) & = & 0 \\ \Leftrightarrow \quad \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix}\cdot\begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}\cdot\begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix} & = & 0 \\ \Leftrightarrow \quad \begin{pmatrix} 0 & 0 \\ C_{\mu_2}A & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ AC_{\mu_1} & 0 \end{pmatrix} & = & 0 \\ \Leftrightarrow \quad C_{\mu_2}A - AC_{\mu_1} & = & 0\,. \end{array}$$

Une matrice non nulle $\begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}$ par blocs correspond à un morphisme $v : E_1 \to E_2$. La condition de commutation correspond à $v \circ u_1 = u_2 \circ v$ ce qui signifie exactement que v est un morphisme de $\mathbb{K}[X]$-modules (cf. cours IV.1.) Or $E_i = \mathbb{K}[X]/\mu_i$ avec $\mu_2|\mu_1$. On sait bien que dans ce cas, on a un morphisme naturel factorisant les projections canoniques :

$$\begin{array}{ccc} & \mathbb{K}[X] & \\ & \downarrow \quad \searrow & \\ \mathbb{K}[X]/\mu_1 & \to & \mathbb{K}[X]/\mu_2\,. \end{array}$$

Si l'isomorphisme $E_i \cong \mathbb{K}[X]/\mu_i$ est donné par un vecteur cyclique x_i, dans les identifications ci-dessus, v est l'unique morphisme

$$v \,:\, E_1 \to E_2\,,\; x_1 \mapsto x_2 \text{ et } v\circ u_1 = u_2 \circ v\,.$$

c) (0.5points) Montrer que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \;>\; n\,.$$

Solution : *Pour $i = 1$ ou 2, notons*

$$V_i \;:=\; \big\{v \in \mathrm{End}_{\mathbb{K}}(E)\,;\; E_j\,,_{j\,=\,1\text{ ou }2} \text{ est stable par } v\,,\; v_{|E_i} \in \mathrm{Com}(u_{|E_i})\,,\; v_{|E_{3-i}} = 0\big\}\,.$$

On a alors $V_i \cong \mathrm{Com}(u_{|E_i})$, $V_i \subset \mathrm{Com}(u)$ et la somme $V_1 + V_2$ est directe. On en déduit que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \;\geq\; \dim_{\mathbb{K}} V_1 + \dim_{\mathbb{K}} V_2 \;\geq\; \dim_{\mathbb{K}} E_1 + \dim_{\mathbb{K}} E_2$$

en utilisant les résultats de la question 2). Or l'endomorphisme v construit en b) n'appartient pas à $V_1 \oplus V_2$ ce qui rend strict l'inégalité précédente.

5) (1point) Déduire de ce qui précède que, si u n'est pas cyclique $\dim_{\mathbb{K}} \mathrm{Com}(u) > n$; puis que $\dim_{\mathbb{K}} \mathrm{Com}(u) = n$ si et seulement si u est cyclique.

Solution : *On a vu (cf. question 2), b),) que lorsque u est cyclique* $\dim_{\mathbb{K}} \mathrm{Com}(u) = n$.

Si u n'est pas cyclique, il existe en vertu du théorème IV.11.5 de réduction de FROBENIUS *une décomposition de*

$$E = \bigoplus_{i=1}^{r} E_i$$

en sous-espaces cycliques. L'énoncé d'unicité IV.11.5.2) dans le théorème loc. cit., assure alors que nécessairement $r \geq 2$. En appliquant alors un argument de récurrence sur r, on montre (cf. question 4),) que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) > n .$$

Exercice E : (**Une question réciproque**)

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie n .

On cherche dans ce problème à savoir s'il existe des endomorphismes nilpotents de E dont la dimension des noyaux itérés est arbitrairement fixée. Si c'est le cas, on essayera de les déterminer, au moins à conjugaison près. Il est recommandé de traiter l'exercice C avant le présent exercice. On y a, en effet étudié certains invariants liés à la suite des noyaux itérés en grand détail ; ce qui pourra s'avéré très utile pour traiter les questions qui suivent.

L'objectif de cet exercice est de déterminer quelles sont les suites finies d'entiers n_k ,$0 \leq k \leq n$, $n_k \leq n$, pour lesquelles il existe un endomorphisme nilpotent $f \in \mathrm{End}_{\mathbb{C}}(E)$ de E tel que

$$\forall 1 \leq k \leq n, \ , \ \dim \mathrm{Ker}\, f^k = n_k . \qquad \textbf{1}$$

Soit donc donnée, dans toute cette partie, une suite n_k satisfaisant les hypothèses ci-dessus. On suppose qu'il existe f nilpotent vérifiant la condition 1 et l'on cherche à en tirer un certain nombre de conséquences.

On cherche au moins à déterminer la classe de conjugaison de f comme ci-dessus et, par conséquent, on peut se placer dans une base $\mathcal{B}$ dans laquelle la matrice de f est une réduite de JORDAN notée J .

Pour tout $r \leq n$, soit

$$J_r := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} \in \mathcal{M}_r(\mathbb{C})$$

le bloc de JORDAN "élémentaire".

La matrice J est donc de la forme

$$J = \mathbf{diag}\,(J_{r_1}, J_{r_2}, \cdots, J_{r_m}) = \begin{pmatrix} J_{r_1} & 0 \cdots & \cdots & 0 \\ 0 & J_{r_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{r_m} \end{pmatrix}$$

pour un certain entier m .

1) (2pts) Pour toute permutation σ de l'ensemble $[1; m]$, montrer que les matrices J et

$$J_\sigma := \mathrm{diag}\,(J_{r_{\sigma(1)}}, J_{r_{\sigma(2)}}, \cdots, J_{r_{\sigma(m)}})$$

obtenue en permutant les blocs de JORDAN, sont conjuguées, c'est-à-dire qu'il existe une matrice inversible

$$P_\sigma \in \mathcal{M}_r(\mathbb{C}) \text{ telle que } J = P_\sigma\, J_\sigma\, P_\sigma^{-1} ,$$

ou encore qu'il existe une autre base $\mathcal{B}_\sigma$ dans laquelle la matrice de f est également une réduite de JORDAN.

Solution : *On peut donner deux arguments diférents :*

i) ***(Construction d'une matrice de permutation)***

Nous avons déjà remarqué que l'écriture de la matrice J de f par blocs signifie qu'on a une décomposition de l'espace vectoriel E en somme directe de sous-espaces E_i de dimension r_i stables par f . L'écriture par blocs de la matrice J signifie également qu'on a choisi une base $\mathcal{B}$ de E réunion de bases

$$\mathcal{B}_i := \{b_{ij} \,, 1 \leq j \leq r_i\} ,$$

où $\mathcal{B}_i$ est une base de E_i .

On construit une base

$$\mathcal{B}_\sigma \ := \ \{b_{\sigma,\alpha}\,,1\leq\alpha\leq n\,\}$$

de E de la manière suivante :

Pour tout $1 \leq \alpha \leq n$, il existe un unique $1 \leq i_\alpha \leq m$ tel que

$$\beta \ := \ \sum_{i<i_\alpha} r_{\sigma(i)} \ < \ \alpha \ \leq \ \sum_{i\leq i_\alpha} r_{\sigma(i)} \ .$$

Posons

$$b_{\sigma,\alpha} \ := \ b_{\sigma(i_\alpha),\alpha-\beta} \ .$$

Il n'est alors pas difficile de vérifier que la matrice de f dans la base $\mathcal{B}_\sigma$ est J_σ .

*ii) (**En utilisant les théorème de réduction (cf. cours IV.10 , IV.11**))*

En effet les matrices J et J_σ ont les mêmes paramètres de JORDAN *(cf. cours IV.10.2 ;) ce qui entraîne, en vertu du corollaire IV.10.13.i), que J et J_σ sont conjugués.*

De manière équivalente, dans le cas des matrices nilpotentes, (ou plus généralement n'ayant qu'une valeur propre) la réduction de JORDAN *est également la réduction de* FROBENIUS *et l'on constate que les matrices J et J_σ ont mêmes invariants de similitude (cf. cours IV.11.9 ;) ce qui assure en vertu du corollaire IV.11.8 qu'elles sont semblables.*

2) (3pts) (**Pentes**)

Pour tout

$$k \ \in \ \mathbb{N}^* \textbf{ on note encore } \ d_k \ := \ n_k \ - \ n_{k-1} \ . \textbf{ (cf. exercice C, question 6) .)}$$

Montrer qu'alors d_k est le nombre d'indice j tel que $r_j \ \geq k$.

Solution : *On a en fait déjà répondu à cette question (cf. exercice C, question 6).)En effet on a :*

$$\begin{array}{rcl} d_k & & n_k - n_{k-1} \\ & \overset{exercice\ C,\, question\ 3)}{=} & \displaystyle\sum_{i=1}^{m} n_{i,k} - n_{i,k-1} \\ & \overset{exercice\ C,\, question\ 4)}{=} & \displaystyle\sum_{i=1}^{m} \min(r_i,k) - \min(r_i,k-1) \ . \end{array}$$

Or $\min(r_i,k) - \min(r_i,k-1)$ vaut 1 si et seulement si $r_i \ \geq \ k$ et vaut 0 sinon. On en déduit que d_k est le nombre de blocs de dimension supérieure ou égale à k . En particulier que $d_1 \ = \ n_1$ est la dimension du noyau de f soit le nombre de blocs (de taille supérieure ou égale à 1 dans J .)

3) (2pt) (**Nombre de blocs**)

En déduire que pour tout $k \geq 0$, $d_k - d_{k+1}$ est exactement le nombre d'indices $1 \ \leq \ j \ \leq \ m$ tels que $r_j \ = \ k$. Remarquer qu'on obtient à nouveau ainsi l'énoncé de décroissance établi à l'exercice B, question 6) sans avoir recours à l'injection de FROBENIUS et par un argument particulièrement élémentaire. Qu'en pensez-vous ?

Solution : *C'est une conséquence immédiate de question 2). À noter qu'on a montré (cf. exercice B, question 6),) que $d.$ est décroissante. Il pourrait sembler surprenant qu'on ait dépensé tant d'énergie à établir ce résultat dans l'exercice B alors qu'il semble découler ici d'un simple argument de comptage très élémentaire. Si la différence $d_k - d_{k+1}$ représente en effet un cardinal fini, c'est par nature un entier positif. On remarquera qu'on n'a pas fait dans l'exercice B l'hypothèse que l'endomorphisme f possède une réduction de* JORDAN*. On conseillerait bien volontiers au lecteur de se reporter aux preuves des théorème IV.10.10 de réduction de* JORDAN *et IV.11.5 de réduction de* FROBENIUS *pour constater à quel point cette hypothèse n'est pas gratuite !*

On suppose que $n \ = \ 25$, on donne la suite

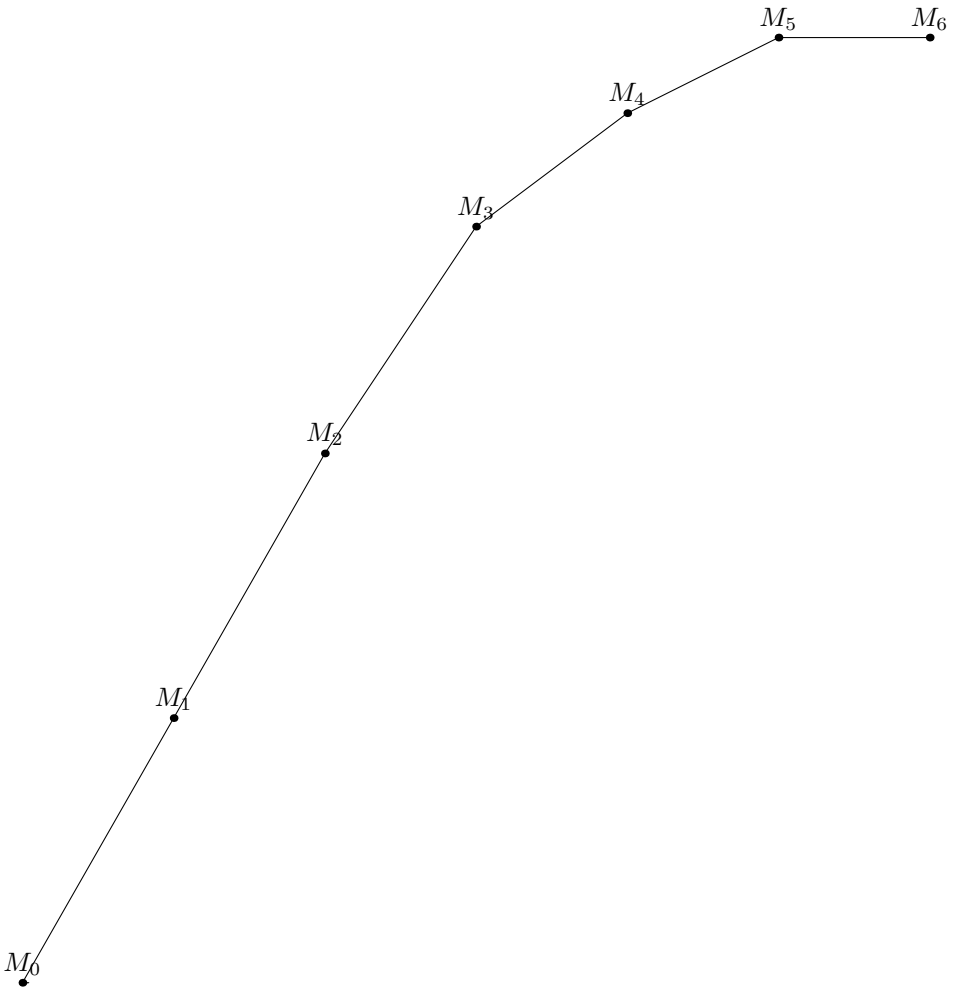
$$n_1 \ = \ 7 \ , \ n_2 \ = \ 14 \ , \ n_3 \ = \ 20 \ , \ n_4 \ = \ 23 \ , \ n_5 \ = \ 25 \ .$$

Un endomorphisme f vérifiant 1 pour cette suite est donc nilpotent d'échelon 5 .

4) (1pt) (**Polygône**)

On note $M_k \ := \ (k, n_k)\,,_{0 \ \leq \ k \ \leq \ 5}$. Tracez le graphe obtenu en reliant M_k et M_{k+1} par un segment de droite.

Solution :



5) (4pt) **a)** (1pt) Interpréter géométriquement dans ce cas les d_k de la question 2).

Solution :

$$\forall k \in \mathbb{N}^*,\ d_k \ = \ n_k - n_{k-1} \ = \ \frac{n_k - n_{k-1}}{k-(k-1)}$$

qui et donc la pente du segment $[M_{k-1}; M_k]$ ou de manière équivalente la dérivée de la fonction affine par morceaux définissant le graphe sur l'intervalle $]k-1; k[$.

b) (1pt) Montrer que le graphe correspond à une fonction concave.

Solution : *On a montré (cf. question 3),) ou (cf. exercice B, question 6),) que $d.$ est décroissante ; ce qui combiné avec l'identification précédente de $d.$ avec la pente du graphe, assure que ce dernier est concave.*

c) (2pt) À quoi correspondent les points anguleux de ce graphe ?

Solution : *Le point M_k du graphe est anguleux si et seulement si la pente "à gauche" de M_k (d_k) est différente de la pente "à droite" de M_k $(d_{k+1}\ ;)$ autrement dit si et seulement si $d_k - d_{k+1}$ est non nul. Or nous avons vu (cf. question 3),) que cette différence est précisément le nombre de blocs de* JORDAN *élémentaires de taille k dans la matrice de f . Il s'ensuit que le point M_k est anguleux si et seulement si la matrice de f comporte des blocs de taille k .*

6) (4pts) Montrer l'existence d'un endomorphisme nilpotent d'échelon 5 vérifiant 1 pour la suite n_k donnée dans cette question. Que peut-on dire de tous les endomorphismes solutions du problème ?

Solution :

*i) (**Conditions nécessaires**)*

On sait (cf. question 3),) que s'il existe un endomorphisme f vérifiant 1, nécessairement il existe une base de E dans laquelle sa matrice est sous forme de JORDAN *et comporte :*

$$\begin{array}{lllll} d_1 - d_2 & = & 2n_1 - n_2 & = & 0 \quad \textit{blocs de taille } 1 \\ d_2 - d_3 & = & 2n_2 - n_1 - n_3 & = & 1 \quad \textit{blocs de taille } 2 \\ d_3 - d_4 & = & 2n_3 - n_2 - n_4 & = & 3 \quad \textit{blocs de taille } 3 \quad . \\ d_4 - d_5 & = & 2n_4 - n_3 - n_5 & = & 1 \quad \textit{blocs de taille } 4 \\ d_5 - d_6 & = & 2n_5 - n_4 - n_6 & = & 2 \quad \textit{blocs de taille } 5\ . \end{array}$$

Il faut remarquer que, même s'il n'est pas donné, nécessairement $n_6 \;=\; 25$. *On constate que* $2+3*3+4+2*5 \;=\; 25$ *ce qui fait qu'on a bien réalisé une partition de* 25. *On choisit donc une base de* E *et l'on définit* f *comme l'endomorphisme de* E *défini par la matrice comportant* 1 *bloc de* JORDAN *élémentaire de taille* 2, 3 *blocs de* JORDAN *élémentaires de taille* 3, 1 *bloc de taille* 4 *et* 2 *blocs de taille* 5 :

$$J \;:=\; \left\{ \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&00&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix} \right\} . \qquad 1$$

ii) ***(Unicité à conjugaison près)***

Puisque la forme de JORDAN *de* f *répondant à 1 est fixée (à conjugaison près (cf. question 1),)) on sait que toute autre solution au problème aura une matrice semblable à* J.

iii) ***(Conditions suffisantes)***

On a rappelé en i), que la réduite de JORDAN *d'un endomorphisme dont la suite des noyaux itérés est*

$$n_{i\ ,1\leq i\leq 5} \;=\; (7,14,20,23,25)$$

comporte $m \;=\; 1+3+1+2 \;=\; 7$ *blocs de* JORDAN *dont les dimensions sont données par*

$$r_{i\ ,1\leq i\leq m\,=\,7} \;=\; (5,5,4,3,3,3,2)\,.$$

Cette réduction correspond également au tableau de YOUNG *(cf. exercice C :)*

$$\begin{pmatrix}
&&*&*&*\\
&&*&*&*\\
&&*&*&\\
&&*&&\\
&&*&&\\
&&*&&\\
&&&&
\end{pmatrix} . \qquad 1$$

Reste à vérifier, sinon à démontrer qu'un endomorphisme ayant une réduite de JORDAN *comme en i).1 ou de manière équivalente un tableau de* YOUNG *comme en 1 répond bien à la question.*

On pourra poser, pour rendre les notations plus commodes, mais néanmoins toujours cohérentes,

$$n_0 \;:=\; \dim \mathrm{Ker}\, f^0 \;=\; \dim \mathrm{Ker}\, \mathrm{Id} \;=\; 0\,.$$

On a alors,

$$\forall 1\leq k\leq 5,\; n_k - n_{k-1} \;=\; \sum_{i=1}^{7} \min(r_i,k) - \min(r_i,k-1)$$ *(cf. exercice C, question 3) , exercice C, question 4) , question 2).)*

Si donc la suite des paramètres de JORDAN *est* $r_{i\ ,1\leq i\leq m\ =\ 7}\ =\ (5,5,4,3,3,3,2)$, *correspondant au tableau de* YOUNG *1, on a :*

$$\begin{aligned} n_1 &= \sum_{i=1}^{7} \min(r_i,1) - \min(r_i,0) &= 7 \\ n_2 &= \sum_{i=1}^{7} \min(r_i,2) - \min(r_i,1) &= 14 \\ n_3 &= \sum_{i=1}^{7} \min(r_i,3) - \min(r_i,2) &= 20 \quad . \\ n_4 &= \sum_{i=1}^{7} \min(r_i,4) - \min(r_i,3) &= 23 \\ n_5 &= \sum_{i=1}^{7} \min(r_i,5) - \min(r_i,4) &= 25 \end{aligned}$$

7) (4pts) Dans le cas général (n quelconque,) quelles conditions (nécessaires et suffisantes) doit satisfaire la suite n_k pour qu'il existe un endomorphisme f nilpotent vérifiant 1 ?

Solution : *Soit donc* $\left(n_k\right)_{,k\in\mathbb{N}}$ *une suite d'entiers. On cherche ici à généraliser la construction faite à la question 6) ; c'est-à-dire plus précisément à déterminer à quelles conditions il est possible de construire un endomorphisme f nilpotent d'un $\mathbb{C}$-espace vectoriel E de dimension finie n dont la suite des noyaux itérés est la suite* $\left(n_k\right)_{,k\in\mathbb{N}}$. *Supposons donc qu'il existe (E,f) avec E un $\mathbb{C}$-espace vectoriel de dimension finie et $f\ \in\ \mathrm{End}_{\mathbb{C}}(E)$ un endomorphisme nilpotent de E.*

N_1) *La suite* $\left(n_k\right)_{,k\in\mathbb{N}}$ *est à valeurs entières.*

Puisque

$$n_0\ =\ \mathrm{Ker}\, f^0\ =\ \mathrm{Ker}\,\mathrm{Id}_E\ =\ 0,$$

N_2) $n_0\ =\ 0$.

Si f est un endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension n,

$$\forall k\in\mathbb{N},\ \mathrm{Ker}\, f^k\ \subset\ E\ \Rightarrow\ n_k\ =\ \dim_{\mathbb{C}}\mathrm{Ker}\, f^k\ \leq\ n,$$

ce qui entraîne que

N_3) *La suite* $\left(n_k\right)_{,k\in\mathbb{N}}$ *est bornée.*

Il est par ailleurs presque immédiat que

$$\forall k\in\mathbb{N},\ \mathrm{Ker}\, f^k\ \subset\ \mathrm{Ker}\, f^{k+1}\ \Rightarrow\ n_k\ \leq\ n_{k+1}\ ;$$

c'est-à-dire que :

N_4) *La suite* $\left(n_k\right)_{,k\in\mathbb{N}}$ *est croissante.*

Enfin on a montré (cf. exercice B, question 6),) ou (cf. question 3),) que :

N_5) *La suite* $\left(d_k\right)_{,k\ \in\ \mathbb{N}^*}\ d_k\ :=\ n_k - n_{k-1}$ *est décroissante ; c'est-à-dire que la fonction n_k est concave.*

Dès l'instant où la condition N_2) est satisfaite, puisque les suites $\left(n_k\right)_{,k\in\mathbb{N}}$ *et* $\left(d_k\right)_{,k\ \in\ \mathbb{N}^*}$ *sont reliées par la formule $d_k\ =\ n_k - n_{k-1}$, (« dérivation ») et la formule réciproque*

$$n_k\ =\ n_0\ +\ \sum_{i=1}^{k} d_k\ \text{ « intégration »} \qquad 1$$

l'une des deux suites est à valeurs entières si et seulement si l'autre l'est aussi.

La condition N_4) équivaut bien entendu à ce que la suite $\left(d_k\right)_{,k\ \in\ \mathbb{N}}$ *soit à valeurs positive. Quant aux conditions N_4) et N_3), elles équivalent à ce que n_k soit stationnaire à partir d'un certain rang, autrement dit qu'il*

$$\exists k\ \in\ \mathbb{N},\ \forall \ell\in\mathbb{N},\ \ell\ \geq\ k\ \Rightarrow\ n_\ell\ =\ n_k\ .$$

Ceci entraîne en particulier que $d_{k+1}\ =\ 0$; ce qui, sous l'hypothèse que d_k est positive et décroissante, équivaut à

$$\forall \ell\in\mathbb{N},\ \ell\ >\ k\ \Rightarrow\ d_\ell\ =\ 0\ .$$

Il s'ensuit que les conditions N_1) à N_5) sont encore équivalentes aux conditions suivantes pour une suite $\left(n_k\right)_{,k\in\mathbb{N}}$, *en notant $\forall k\in\mathbb{N}^*,\ d_k\ =\ n_k - n_{k-1}$:*

D_1) *La suite* $\left(d_k\right)_{,k\ \in\ \mathbb{N}^*}$ *est à valeurs entières i.e.à valeurs dans $\mathbb{N}$.*

D_2) $n_0 = 0$.

D_3) La suite $(d_k)_{,k \in \mathbb{N}^*}$ est décroissante.

D_4) Il existe $k \in \mathbb{N}$ tel que $d_k = 0$.

Avant de montrer (cf. 7).3,) que les conditions ci-dessus sont sufisantes à l'existence d'un couple (E, f) solution du problème, établissons la formule suivante qui nous servira à plusieurs reprises :

Lemme 7).1

$$\forall k \in \mathbb{N},\ \sum_{i=1}^{k} i\#\big(\{j \in [1;m]\,;\, r_j = i\}\big) = \sum_{i=1}^{k} i(d_i - d_{i+1}) = (1-k)n_k - kn_{k+1}\,.$$

***Preuve** : La première égalité est une conséquence de la question 3). Pour la seconde on calcule :*

$$\begin{aligned}
\sum_{i=1}^{k} i\#\big(\{j \in [1;m]\,;\, r_j = i\}\big) &= \sum_{i=1}^{k} i(d_i - d_{i+1}) \\
&= \sum_{i=1}^{k} id_i - \sum_{i=1}^{k} id_{i+1} \\
&= \sum_{i=1}^{k} id_i - \sum_{i=2}^{k+1} (i-1)d_i \\
&= \sum_{i=2}^{k} (i-(i-1))d_i - kd_{k+1} + d_1 \\
&= d_1 + \sum_{i=2}^{k} d_i - k(n_{k+1} - n_k) \\
&= \sum_{i=1}^{k} d_i - k(n_{k+1} - n_k) \\
&= \sum_{i=1}^{k} n_i - n_{i-1} - k(n_{k+1} - n_k) \\
&= n_k - kn_k + kn_{k+1} - n_0 \\
&= (1-k)n_k - kn_{k+1}
\end{aligned}$$

en se souvenant qu'on doit satisfaire à la condition N_2) ou D_2), i.e.$n_0 = 0$.

Remarque 7).2 On écrira souvent par la suite $\sum_{\ell=k}^{+\infty} d_\ell$ qui est en fait une somme finie, puisque la suite $(d_k)_{,k \in \mathbb{N}^*}$ est nulle à partir d'un certain rang (cf. D_4).)

Énonçons et prouvons le résulta suivant :

Proposition 7).3 *Étant donné une suite $(n_k)_{,k\in\mathbb{N}}$ vérifiant les conditions N_1) à N_5) ou de manière équivalentes les condition D_1) à D_4),*

*i) (**Existence**)*
il existe (E, f) avec E un $\mathbb{C}$-espace vectoriel de dimension finie et $f \in \mathrm{End}_{\mathbb{C}}(E)$ un endomorphisme nilpotent de E tel que

$$\forall k \in \mathbb{N},\ \dim_{\mathbb{C}} \mathrm{Ker}\, f^k = n_k\,.$$

*ii) (**Unicité à isomorphisme près**)*
De plus si (E, f) et (F, g) sont deux solutions au problème, il existe un

$$\mathbb{C}-\text{ isomorphisme } u : E \to F \text{ tel que } g \circ u = u \circ f\,.$$

Preuve *:*

i) D'après D_4) il existe des entiers k tels que $d_k = 0$. Soit donc ε le plus petit d'entre eux. Puisque d_k est décroissante (cf. D_3),) et à valeurs entières (cf. D_1),)

$$\forall k \in \mathbb{N},\ k \geq \varepsilon \Rightarrow d_k = 0\ .$$

Lemme i).1 *S'il existe un couple (E, f) solution au problème ε est l'échelon de nilpotence de f et n_ε la dimension de E.*

Preuve *:*

$$\forall k \in \mathbb{N},\ k \geq \varepsilon \Rightarrow n_k = n_\varepsilon + \sum_{i=\varepsilon+1}^{k} d_k = n_\varepsilon\ .$$

Or en vertu de N_4),

$$\forall k \in \mathbb{N},\ k \leq \varepsilon \Rightarrow n_k \leq n_\varepsilon\ .$$

Il en découle que

$$\forall k \in \mathbb{N},\ n_k = \dim_{\mathbb{C}} \operatorname{Ker} f^k \leq \dim_{\mathbb{C}} E \Rightarrow n_\varepsilon \leq \dim_{\mathbb{C}} E\ .$$

Cependant si f est nilpotent il existe k tel que $\operatorname{Ker} f^k = E$, i.e.$\dim_{\mathbb{C}} E = n_k$. Il s'ensuit que

$$\dim_{\mathbb{C}} E \leq \max_{k \in \mathbb{N}}(n_k) \leq n_\varepsilon\ .$$

Il en résulte donc que $\dim_{\mathbb{C}} E = n_\varepsilon$.

Notons donc désormais $n := n_\varepsilon$. On a déterminé à la question 3) quel devait être les paramètres de JORDAN $\left(m, r_{i\ ,1\leq i\leq m}\right)$ *d'un endomorphisme f de $\mathbb{C}^n$ nilpotent vérifiant*

$$\forall k \in \mathbb{N},\ \dim_{\mathbb{C}} \operatorname{Ker} f^k = n_k\ .$$

Lemme i).2 *Si*

$$\left(m, r_{i\ ,1\leq i\leq m}\right)$$

est l'ensemble de paramètre de JORDAN *construit comme en question 3),*

$$\sum_{i=1}^{m} r_i = n = n_\varepsilon\ .$$

Preuve *: Il faut constater qu'une bonne part du mystère possible de cette formule disparaît lorsqu'on réalise qu'il ne s'agit ni plus ni moins que d'égaler la somme suivant les lignes ou suivant les colonnes dans le tableau de* YOUNG *ou encore, pour ceux qui sauraient ce que sont ces objets, de considérer une partition et sa partition duale.*

Plus formellement, d'après la question 3), on a :

$$\begin{aligned}
\sum_{i=1}^{m} r_i &= \sum_{k=1}^{+\infty} k(d_k - d_{k+1}) \\
&= \sum_{k=1}^{\varepsilon} k(d_k - d_{k+1}) \\
&\overset{\text{(cf. 7).1)}}{=} (1-\varepsilon)n_\varepsilon + \varepsilon n_{\varepsilon+1} \\
&= n_\varepsilon
\end{aligned}$$

Ainsi, en vertu du lemme i).2 ci-dessus il existe un endomorphisme f de $\mathbb{C}^n$ dont la matrice est donnée par blocs, dans la base canonique par

$$J := \begin{pmatrix} J_{r_1} & 0 & 0 & \dots & 0 \\ 0 & J_{r_2} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 \dots & J_{r_m} & \end{pmatrix}\ .$$

Reste à montrer, pour conclure à l'existence de f que :

Lemme i).3

$$\forall k \in \mathbb{N},\ \dim_{\mathbb{C}} \operatorname{Ker} f^k = n_k\ .$$

Preuve *: on a*

$$\dim_{\mathbb{C}} \operatorname{Ker} f^k \;=\; \sum_{i=1}^{m} n_{i,k} \;=\; \sum_{i=1}^{m} \min(r_i, k) \text{ (cf. exercice C, question 3) , exercice C, question 4).)}$$

Il s'ensuit que :

$$\begin{aligned}
\dim_{\mathbb{C}} \operatorname{Ker} f^k &= \sum_{i=1}^{m} \min(r_i, k) \\
&= \sum_{1 \le i \le m \,,\, r_i \le k} r_i + \sum_{1 \le i \le m \,,\, r_i > k} k \\
&= \sum_{1 \le i \le m} \sum_{\ell=1}^{k} r_i \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big) + \sum_{1 \le i \le m} \sum_{\ell=k+1}^{+\infty} k \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big) \\
&= \sum_{\ell=1}^{k} r_i \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big) + \sum_{\ell=k+1}^{+\infty} k \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big) \\
&= \sum_{\ell=1}^{k} \ell \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big) + \sum_{\ell=k+1}^{+\infty} k \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big)
\end{aligned}$$

On peut encore calculer l'expression ci-dessus grâce à la question 3) :

$\dim_{\mathbb{C}} \operatorname{Ker} f^k$

$$\begin{aligned}
&= \sum_{\ell=1}^{k} \ell \#\big(\{i \in [1;m] \,;\, r_i = \ell\}\big) + \sum_{\ell=k+1}^{+\infty} k \#\big(\{i \in [1;m] \,;\, r_i = \ell\} \\
&= \sum_{\ell=1}^{k} \ell (d_\ell - d_{\ell+1}) + k \sum_{\ell=k+1}^{+\infty} (d_\ell - d_{\ell+1}) \\
&\overset{\text{(cf. 7).1)}}{=} (1-k) n_k + k n_{k+1} + k \sum_{\ell=k+1}^{+\infty} (d_\ell - d_{\ell+1}) \\
&(1-k) n_k + k n_{k+1} + k \left(\sum_{\ell=K+1}^{+\infty} d_\ell - \sum_{\ell=k+2}^{+\infty} d_\ell \right) \\
&= (1-k) n_k + k n_{k+1} + k d_{k+1} \\
&= (1-k) n_k + k n_{k+1} + k (n_k - n_{k+1}) \\
&= n_k \,.
\end{aligned}$$

ii) On a vu (cf. question 3),) que la suite $(d_k)_{,k \in \mathbb{N}^*}$ détermine complètement les paramètres de JORDAN *d'un couple (E, f) solution du problème. Pour peu que D_2) ou de manière équivalente N_2) les suites $(n_k)_{,k \in \mathbb{N}}$ et $(d_k)_{,k \in \mathbb{N}^*}$ se déterminent complètement l'une l'autre. Autrement dit les paramètre de* JORDAN *d'un couple (E, f) solution du problème sont entièrement déterminés par la suite $(n_k)_{,k \in \mathbb{N}}$. La solution du problème est alors unique à isomorphisme près en vertu de la proposition IV.10.9 du cours.*

Exercice F : (Géométrie du cône nilpotent)

On regarde dans $\mathcal{M}_n(\mathbb{C})$ l ensemble $\mathcal{N}$ des matrices nilpotentes, comme espace topologique. On l'appelle le *cône nilpotent*. (En fait on pourrait considérer n'importe quel corps, même si pour la suite il faudrait préciser les topologies, ce qu'est une variété etc..)

1) (6.5points) $\mathcal{N}$ est-il un espace vectoriel ?

Solution : *Il est claire que*

$$\forall N \in \mathcal{N},\ \forall a \in \mathbb{C},\ aN \in \mathcal{N} \,;$$

c'est-à-dire que $\mathcal{N}$ est au moins un cône i.e. une réunion de droites. Néanmoins, $\forall (N, M) \in \mathcal{N} \times \mathcal{N}$, il n'est pas du tout certain que $N + M$ soit encore nilpotent en particulier si N et M ne commutent pas. En particulier

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}) \text{ et } \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$$

sont nilpotentes mais leur somme $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *est de rang* 2*, et ne peut donc être nilpotente puisque une matrice nilpotente n'est jamais de rang maximal. On peut même voir explicitement que*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

2) (6.5points) Même si ce n'est pas le cas, on va montrer que $\mathcal{N}$ est une sous-variété de $\mathcal{M}_n(\mathbb{C})$ et déterminer sa dimension.

a) (6.5points) Montrer que $\mathcal{N}$ est fermé.
Solution : *Une matrice nilpotente dans* $\mathcal{M}_n(\mathbb{C})$ *est au maximaum d'échelon* n *(cf. exercice A, question 2).) Ainsi*

$$\forall N \in \mathcal{N},\ N^n = 0\,;$$

mais réciproquement si $N^n = 0$, N *est nilpotente si bien que*

$$\mathcal{N} = \{N \in \mathcal{M}_n(\mathbb{C})\,;\ N^n = 0\}\,.$$

Or l'application

$$\mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})\,,\ N \mapsto N^n \text{ est continue}$$

et $\mathcal{N}$ *est l'image réciproque du singleton* 0 *par cette application et est donc fermé.*

b) (6.5points) **Supposons dans cette question que** $n = 2$.

i) Montrer qu'une matrice nilpotente est de trace nulle.
Solution : *Si* $n = 2, \forall N \in \mathcal{M}_2(\mathbb{C}),$ *, le polynôme caractéristique* $P_{car\,N}$ *est*

$$P_{car\,N} = \det(XI - N) = X^2 - \mathrm{Tr}(N)X + \det(N)\,.$$

Or, en vertu du théorème IV.7.2 de CAYLEY–HAMILTON*, le polynôme minimal* $P_{min\,N}$ *divise* $P_{car\,N}$*. Si* N *est nilpotente,* $P_{min\,N} = X^k$, $k > 0$, *ce qui entraîne* $\det(N) = 0$ *; ce qu'on sait déjà d'ailleurs puisqu'une matrice nilpotente ne peut être de rang maximal. On sait également (cf. exercice I, ou IV.11.11) que* $P_{car\,N}$ *et* $P_{min\,N}$ *ont les même facteurs irréductibles ce qui force* $\mathrm{Tr}(N) = 0$.

ii) Donner deux équations définissant $\mathcal{N}$ dans $\mathcal{M}_2(\mathbb{C})$ (ou une seule équation dans $\{M \in \mathcal{M}_2(\mathbb{C})\,;\ \mathrm{Tr}(M) = 0\}$).
Solution : *On vient de voir ci dessus que si* $N \in \mathcal{M}_2(\mathbb{C})$ *est nilpotente alors*

$$\mathrm{Tr}(N) = \det(N) = 0\,.$$

Réciproquement si tel est le cas, $P_{car\,N} = X^2$*, si bien que, toujours en vertu du théorème de* CAYLEY–HAMILTON*,*

$$P_{min\,N} = X^k\,,\ 1 \leq k \leq 2\,;$$

i.e.N *est nilpotente. Ainsi :*

$$\begin{aligned} \mathcal{N} &= \{N \in \mathcal{M}_2(\mathbb{C})\,;\ \mathrm{Tr}(N) = 0 \text{ et } \det(N) = 0\} \\ &= \{N = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})\,;\ x + t = 0 \text{ et } xt - yz = 0\} \\ &= \{N = \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})\,;\ x^2 + yz = 0\}\,. \end{aligned}$$

iii) Quelle est cette surface ?
Indication : *on pourra effectuer le changement de variables linéaire* $x = x', y = y' + z'$ *et* $z = y' - z'$.
Solution : *En effectuant le changement de variable demandé l'équation* $x^2 + yz = 0$ *obtenue ci-dessus devient*

$$\begin{aligned} & x'^2 + (y' + z')(y' - z') = 0 \\ \Leftrightarrow \quad & x'^2 + y'^2 - z'^2 = 0\,. \end{aligned}$$

On constate qu'alors la courbe à z' *constant qu'on obtient est un cercle, ce qui caractérise un cône. À noter qu'en considérant la première forme de l'équation* $x^2 + yz = 0$*, on constate que la courbe obtenue à* X *constant est une hyperbole ce qui caractérise également un cône.*

On avait vérifié à la question 1) une propriété d'homogénéité qui assurait déjà que la variété $\mathcal{N}$ *est un cône.*

iv) Montrer que $\mathcal{N}$ s'identifie à une surface dans $\mathbb{C}^3$, mais a un point singulier en 0.

Indication : *On pourra considérer l'espace tangeant en la matrice nulle, et montrer qu'il est de dimension 3.*

Solution : *La différentielle df avec $f(x,y,z) = x^2+yz$ vaut $df = \begin{pmatrix}2x & z & y\end{pmatrix}$ et son rang ne chute qu'en 0.*

On peut aussi "tracer" des courbes sur $\mathcal{N}$, passant par $0 \in \mathcal{N}$ en $t=0$ et prendre le vecteur tangeant en 0 : l'espace tangeant en un point est l'ensemble de ces vecteurs tangeants, modulo équivalence. Soit alors

$$\gamma_1 : \begin{array}{ccc}[-1,1] & \longrightarrow & \mathcal{N} \\ t & \longmapsto & \begin{pmatrix}0 & T\\ 0 & 0\end{pmatrix}\end{array}, \quad \gamma_2 : \begin{array}{ccc}[-1,1] & \longrightarrow & \mathcal{N} \\ t & \longmapsto & \begin{pmatrix}0 & 0\\ t & 0\end{pmatrix}\end{array}, \quad \gamma_3 : \begin{array}{ccc}[-1,1] & \longrightarrow & \mathcal{N} \\ t & \longmapsto & \begin{pmatrix}t & -t\\ t & -t\end{pmatrix}\end{array},$$

qui sont clairement bien définies, et $\mathcal{C}^\infty$. Alors, l'espace (vectoriel) tangeant à $\mathcal{N}$ en 0 $T_0\mathcal{N}$ contient

$$d\gamma_1(0) = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, d\gamma_2(0) = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, d\gamma_3(0) + d\gamma_1(0) - d\gamma_2(0) = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

c'est donc $\mathfrak{sl}_2$, l'ensemble des matrices de taille 2 et trace nulle, de dimension 3.

c) (6.5points) Montrer que les matrices nilpotentes de rang $n-1$ (*i.e.*d'échelon n (cf. cours IV.8.1,)) forment un ouvert, dense, de $\mathcal{N}$.

Indication : *On pourra considérer N sous forme de Jordan, et regarder $N + \frac{1}{k}J_n$.*

Solution : *Supposons que J soit une matrice nilpotente sous forme de* JORDAN *: Pour tout $r \leq n$, soit*

$$J_r := \begin{pmatrix}0 & 0 & 0 & \dots & 0 & 0\\ 1 & 0 & 0 & \dots & 0 & 0\\ 0 & 1 & 0 & \dots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & 1 & 0\end{pmatrix} \in \mathcal{M}_r(\mathbb{C})$$

le bloc de JORDAN *"élémentaire".*

La matrice J est donc de la forme

$$J = diag\,(J_{r_1}, J_{r_2}, \cdots, J_{r_m}) = \begin{pmatrix}J_{r_1} & 0\cdots & \cdots & 0\\ 0 & J_{r_2} & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \cdots & 0 & J_{r_m}\end{pmatrix}$$

pour un certain entier m .

La suite $J+\frac{1}{k}J_n$ est formée de matrice nilpotentes puisque triangulaire inférieure stricte. On a montré en effet (cf. exercice A, question 4),) que cette condition était nécessaire, mais en considérant attentivement les arguments de la preuve on se convaincra facilement qu'elle est suffisante. Or les matrices $J + \frac{1}{k}J_n$ sont de rang n et donc d'échelon $n-1$.

Si $N \in \mathcal{N}$ n'est pas sous forme de JORDAN*, le théorème IV.10.10 de réduction de* JORDAN *qu'il existe une matrice J sous forme de* JORDAN *et une matrice P inversible telles que $N = PJP^{-1}$. Or $M \mapsto PMP^{-1}$ est continue de $\mathcal{M}_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})$ si bien que*

$$\lim_{k\to+\infty} J + \frac{1}{k}J_n = J \Rightarrow \lim_{k\to+\infty} P(J+\frac{1}{k}J_n)P^{-1} = N\,;$$

ce qui donne le résultat puisque le rang et l'échelon de nilpotence sont inchangés par conjugaison.

d) (6.5points) Montrer que toutes les matrices nilpotentes de rang $n-1$ sont conjuguées.

Solution : *Elle sont toute conjuguées à J_n. À noter que la combinatoire devient plus compliquée si on ne suppose pas le rang maximal et l'on est amené alors, pour déterminer les différentes classes de conjugaison à considérer des partitions du nombre n comme c'est fait dans l'exercice E ou dans l'exercice G.*

e) (6.5points) Soit N une telle matrice. Montrer que l'ensemble des matrices P qui commutent à N est isomorphe à $\mathbb{C}^n$

Indication : *on pourra supposer que N est sous forme normale de Jordan disons sous-diagonale (pourquoi ?* , et regarder l image par P de e_1).

Solution : *Si $N = J_n$ et $NP = PN$, on a $Pe_i = PNe_{i-1} = NPe_{i-1}$ donc par une récurrence immédiate, $Pe_i = N^{i-1}Pe_1$.*

Réciproquement, pour tout $v \in \mathbb{C}^n$ en posant $Pe_i = N^{i-1}v$, alors $NP = PN$. On a donc un isomorphisme entre $\mathbb{C}^n$ et $\mathrm{Com}(J_n)$, l'ensemble des matrices commutant à J_n. Si maintenant N n'est pas sous forme de Jordan, $N = QJ_nQ^{-1}$, et donc P commute à N si et seulement si

$$PQJ_nQ^{-1} = QJ_nQ^{-1}P \Leftrightarrow Q^{-1}PQJ_n = J_nQ^{-1}PQ,$$

si et seulement si $Q^{-1}PQ$ commute à J_n. Donc le commutant $\mathrm{Com}(N)$ de N est $Q^{-1}\mathrm{Com}(J_n)Q$, donc est aussi de dimension n.

Voir aussi l'exercice D.

f) (6.5points) (**Difficile**)

Montrer que l'ensemble des matrices de rang exactement $n-1$ est de dimension $n(n-1)$. On pourra construire un $\mathcal{C}^\infty$-difféomorphisme explicite entre $\mathcal{N}_n$, l'ensemble des matrices nilpotentes d'ordre exactement n, et

$$S = \left\{ M = \begin{pmatrix} 1 & \star & \dots & \star \\ 0 & & & \\ \vdots & \vdots & & \vdots \\ 0 & \star & & \star \end{pmatrix} \mid M \in \mathrm{GL}_n(\mathbb{C}) \right\},$$

en utilisant ce qui précède.

Solution : *Par ce qui précède, si $N = J_n$ et $NP = PN$, on a $Pe_i = PNe_{i-1} = NPe_{i-1}$ donc par une récurrence immédiate, $Pe_i = N^{i-1}Pe_1$. Donc si P commute à N et appartient à S, on a $Pe_1 = e_1$, et donc $P = \mathrm{Id}$.*

Essayons de donner un inverse à

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{C}) & \longrightarrow & \mathcal{N}_n \\ P & \longmapsto & PNP^{-1} \end{array}$$

qui est clairement C^∞, surjective, et injective restreinte à S. Réciproquement si $M = PNP^{-1}$, comment déduire P en fonction de M ? On calcule

$$Me_1 = PNP^{-1}e_1 \underbrace{=}_{P \in S} PNe_1 = Pe_2.$$

Plus généralement,

$$M^i e_1 = PN^i P^{-1} e_1 = PN^i e_1 = Pe_{i+1}.$$

Donc la matrice P est donnée en colonne par $e_1, Me_1, \dots, M^{n-1}e_1$ (qui est une base car M est de rang maximal). On en déduite un inverse à ϕ ;

$$\psi : \begin{array}{ccc} \mathcal{N}_n & \longrightarrow & S \\ M & \longmapsto & \mathit{Mat}(e_1, Me_1, \dots, M^{n-1}e_1) \end{array}$$

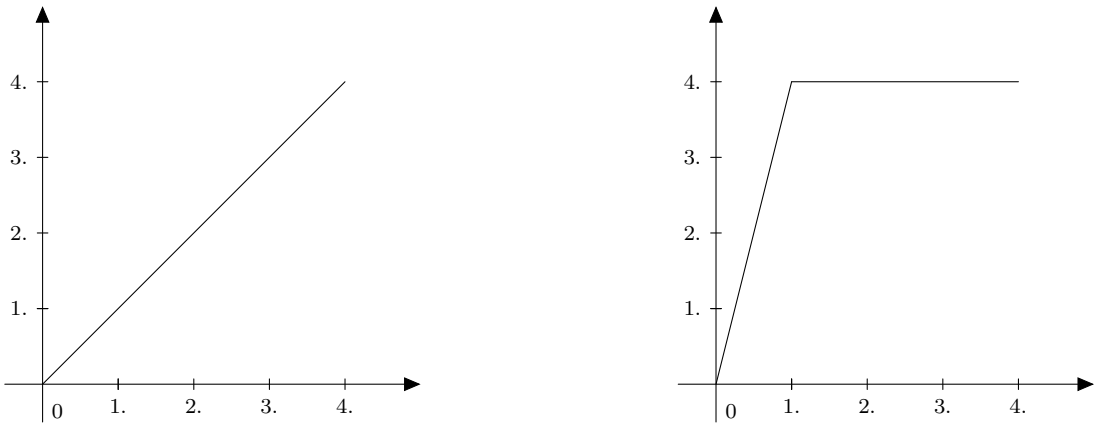
qui est clairement $\mathcal{C}^\infty$, puisque $M \mapsto Mx$ est C^∞ (linéaire en fait) de $\mathcal{M}_n(\mathbb{C}) \longrightarrow \mathbb{C}^n$.

Remarque 1 Si X est un fermé de $\mathbb{C}^N$, on peut définir la dimension de X comme le plus grand entier d tel qu'il existe un ouvert de X C^∞-difféomorphe à $\mathbb{C}^d$. Lorsque X est une variété différentiable, en particulier lisse, tous les ouverts de X ont même dimension (si X est connexe disons). Dans notre cas, $\mathcal{N}$ est connexe mais n'est pas lisse, et sa dimension est la dimension de $\mathcal{N}_n$, c'est donc $n(n-1)$.

Exercice G : (Partitions, tableaux de YOUNG, polygônes concaves)

On appelle partition de n une suite $d_1 \geq d_2 \geq \dots d_n \geq 0$ telle que $d_1 + \dots + d_n = n$ (on autorise à avoir des répétitions et des zéros). On note $\mathcal{P}art(n)$ leur ensemble. On note $\mathcal{P}ol$ l'ensemble des polygones croissants, concaves, à abscisses de rupture entières tels que $P(0) = 0$ et $P(n) = n$ et pour tout $0 \leq k \leq n, P(k) \in \mathbb{N}$.

FIGURE 2 – Deux exemples de polygônes dans $\mathcal{P}ol$ pour $n = 4$



On note $\mathcal{Y}$ l'ensemble des diagrammes de Young à n cases (https://fr.wikipedia.org/wiki/Tableau_de_Young).

1) (6.5points) Montrer que l'on a des bijections (naturelles) entre $\mathcal{P}art(n)$, $\mathcal{P}ol$, et $\mathcal{Y}$.

Solution : *Étant donné un polygône $p \in \mathcal{P}ol$, sa dérivée p' est une application constante sur les intervalles $]i-1; i[$, $1 \leq i \leq n$, et décroissante puisque p est concave. Si l'on note d_i la valeur de p' sur $]i-1; i[$, en intégrant p', on a bien évidemment*

$$\sum_{i=1}^{n} d_i \;=\; p(n) - p(0) \;=\; n\,.$$

Réciproquement une suite d_i ,$_{1\leq i\leq n}$ définit une application constante de valeur d_i sur les intervalles $]i-1;i[$, dont la primitive s'annulant en 0 est un élément de $\mathcal{P}ol$.

On associe en outre bijectivement à toute partition dans $\mathcal{P}art(n)$ un tableau de Young ayant d_i cases sur sa $i^{\text{ième}}$ colonne.

2) (6.5points) Construire une application naturelle $\nu : \mathcal{N} \to \mathcal{P}art(n)$ telle qu'une matrice d'échelon n est envoyée sur la partition $1+1+..+1=n$, et la matrice nulle est envoyée sur $n+0+\cdots+0=n$.

Solution : *Pour tout*

$$A \in \mathcal{N}\ ,\ \forall 1 \leq i \leq n,\ \nu(A)_i := \dim_{\mathbb{C}} \operatorname{Ker} A^i - \dim_{\mathbb{C}} \operatorname{Ker} A^{i-1}$$

convient. Le fait notamment que $\nu(A)_i$ est décroissante est établi dans l'exercice B, question 6). En outre les relations entre pentes du polygône, saut des dimensions des noyaux itérés et tableaux de YOUNG *on été étudiées notamment dans l'exercice C et l'exercice E. En particulier les entiers d_i introduit ici sont exactement ceux introduits dans l'exercice B et utilisés dans les exercices loc. cit..*

3) (6.5points) Quel polygone est alors associé à une matrice de rang $n-1$? De rang 0 ?

Solution : *Il suffit d'intégrer la formule ci-dessus autrement dit, si ν est défini comme ci-dessus, l'application π qui lui correspond par les isomorphismes (cf. exercice G,) est*

$$\pi : \mathcal{N} \to \mathcal{P}ol\ ,\ A \mapsto i \mapsto \dim_{\mathbb{C}} \operatorname{Ker} A^i\ .$$

Ainsi pour une matrice A de rang $n-1$, $\pi(A)$ est la première bissectrice, tandis que pour une matrice A de rang 0 i.e.la matrice nulle, $\pi(A)$ est la constante d'équation $y = n$.

4) (6.5points) Montrer que deux matrices de $\mathcal{N}$ sont semblables ssi leurs ν sont égaux (vu comme polygones, partition ou diagramme, au choix).

Solution : *Bien entendu, si A et B sont semblables elles ont même suites $\left(n_k\right)_{,k\in\mathbb{N}}$ de dimension de noyaux itérés $\forall k \in \mathbb{N},\ n_k = \dim_{\mathbb{K}} \operatorname{Ker} \cdot^k$. On peut se reporter à l'exercice C pour voir que cette suite détermine complètement le tableau de* YOUNG.

Réciproquement si deux matrices ont le même tableau de YOUNG *(le même polygône ou la même partition) elles ont même suite $\left(n_k\right)_{,k\in\mathbb{N}}$ de dimension des noyaux itérés, celle-ci étant en effet la primitive (qui s'annule en 0) de la suite d_k des pentes données par la partition ou le tableau de* YOUNG *:*

$$n_i = n_0 + \sum_{k=1}^{i} d_k$$

lorsque n_0 vaut nécessairement 0. On peut alors utiliser par exemple l'exercice E, question 7) pour assurer que la forme de JORDAN *correspondant aux données est alors uniquement déterminée ; et partant la classe de similitude de l'endomorphisme.*

Pour toute partition (ou polygone, ou diagramme) p, on note $\mathcal{N}_p$ l ensemble des matrices envoyées sur p.

5) (6.5points) Pourquoi $\mathcal{N}_p$ est-il une classe de conjugaison ? Donner pour $n=8$, un représentant de la classe de conjugaison de la partition $3+2+2+1=8$.

Solution : *On a vu ci-dessus q'avoir même polygône ou même tableau de* YOUNG *ou même partition revient à être semblable ce qui signifie précisément être conjugué par un élément du groupe linéaire $\mathrm{GL}_n(\mathbb{C})$.*

On se reporetera avec profit à l'exercice E pour les détails de la constructions d'une forme de JORDAN *dont on connaît par exemple les invariants numériques d_k. Ainsi pour la partition $(3,2,2,1)$ on sait que le*

$$\begin{array}{llllll} \textit{nombre de blocs de taille} & 1 & \textit{est} & 3-2 & = & 1 \\ \textit{nombre de blocs de taille} & 2 & \textit{est} & 2-2 & = & 0 \\ \textit{nombre de blocs de taille} & 3 & \textit{est} & 2-1 & = & 1 \\ \textit{nombre de blocs de taille} & 4 & \textit{est} & 1-0 & = & 1 \end{array}$$

ce qui donne la forme de JORDAN *(à permutation près :)*

$$J = \begin{pmatrix} 0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0 \end{pmatrix}.$$

6) (6.5points) (**Difficile**)

Montrer que $\mathcal{N}_{p'}$ est dans l'adhérence de $\mathcal{N}_p$ si et seulement si le polygone de p est en dessous du polygone de p'.

Solution : *On a déjà observé que la partition d_k associée à un endomorphisme nilpotent N est la « dérivée » de la suite $\big(n_k\big)_{,k\in\mathbb{N}}$ des dimension des noyaux itérés :*

$$n_k \;=\; \dim_{\mathbb{K}} \operatorname{Ker} N^k \text{ et } d_k \;=\; n_k - n_{k-1}\;.$$

Par semi continuité du rang (de N^i) on en déduit donc que si N_t est une suite de limite N_0 telle que N_t^i est de rang constant, alors

$$\operatorname{rg}(N_0^i) \;\leq\; \operatorname{rg}(N_t^i),$$

donc

$$\dim \operatorname{Ker} N_0^i \;\geq\; \dim \operatorname{Ker} N_t^i$$

donc

$$\sum_{k=1}^{i} d'_k \;\geq\; \sum_{k=1}^{i} d_k,$$

i.e. le polygône de p' est au dessus du polygone de p.

Réciproquement soit donc $N_0 \in \mathcal{N}_{p'}$ et montrons qu'on peut trouver une suite N_t, $t \in]0,1]$, telle que $N_t \in \mathcal{N}_p$ et $N_t \to N_0$. Tout d'abord on pourrait supposer $N_0 = J(p')$ (cf. exercice E, question 7),) la forme de Jordan standard associée à la partition p' : en effet si $N_t \to J(N_0)$, et $N_0 = PJ(p')P^{-1}$, alors PN_tP^{-1} convient. On suppose donc $N_0 = J(p')$.

Soit $d'_1 \geq \cdots \geq d'_n$ et $d_1 \geq \cdots \geq d_n$ les partitions p' et p. Par hypothèse, on a

$$d'_1 \geq d_1, \quad d'_1 + d'_2 \geq d_1 + d_2, \ldots, \sum_{k=1}^{i} d'_k \geq \sum_{k=1}^{i} d_k.$$

Soit i minimal tel que $\displaystyle\sum_{k=1}^{i} d'_k > \sum_{k=1}^{i} d_k$.

Soit $r \geq 1$ minimal tel que

$$N_0 : \underbrace{\operatorname{Ker} N^{i+r}/\operatorname{Ker} N^{i+r-1}}_{\dim = d_{i+r}} \longrightarrow \underbrace{\operatorname{Ker} N^{i+r-1}/\operatorname{Ker} N^{i+r-2}}_{\dim = d_{i+r-1}}$$

ne soit pas surjective. Soit alors $x = e_\ell \in \operatorname{Ker} N_0^{i+r-1}$ un vecteur de la base canonique qui n'est pas dans l'image précédente (on peut supposer que c'est un vecteur de la base canonique car $N_0 = J(p')$). Comme $d'_i = d'_{i+1} = \cdots = d'_{i+r-1} > d_i \geq \cdots \geq d_{i+r}$, il existe $j > r$ minimal tel que $d'_{i+j} < d'_{i+j+1}$, il existe donc $e_k \in \operatorname{Ker} N_0^{i+j+1}$ qui n'est pas dans l'image de N_0. On pose alors

$$N_t = N_0 + t\delta_{k,\ell}.$$

Autrement dit pour tout $i \neq \ell$, $N_t e_i = N_0 e_i$, et $N_t e_\ell = N_0 e_\ell + t e_k$. Notons $p'' = d''_i$ la partition associée à N_t.

On vérifie que,

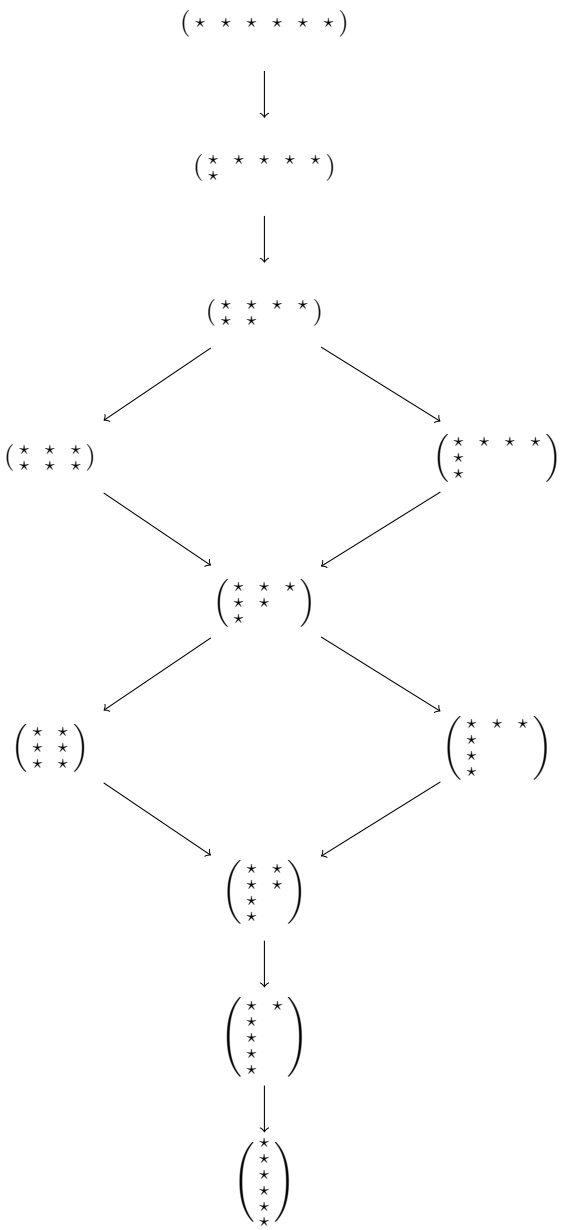
$$d''_s = d'_s, \quad \forall s \leq i + r - 1, \forall s \geq i + j + 1$$
$$d''_{i+r} = d'_{i+r} - 1,$$
$$d''_{i+j} = d'_{i+j} + 1,$$
$$d''_u = d'_u, \quad \forall i + r + 1 \leq u \leq i + j - 1$$

On a évidemment $N_t \to N_0$, et on vérifie facilement que $p' > p'' \geq p$ (en fait on a juste déplacé e_ℓ de $\operatorname{Ker} N^{i+r}$ vers $\operatorname{Ker} N^{i+j}$), donc par récurrence immédiate (sur les différences $\displaystyle\sum_{k=1}^{i} d'_k - d_k$), on en déduit l'existence d'une déformation N_t telle que $\nu(N_t) = p$.

Exercice H : (**Un graphe**)

1) (6.5points) Pour $n = 6$, donner le graph orienté dont les sommets sont les classes de similitudes de matrices nilpotentes, et les arêtes sont orientées $M \longrightarrow M$ s il existe une suite de matrices dans la classe de conjugaison de M dont la limite est dans la classe de conjugaison de M (on enlevera les arêtes ayant même sommet de départ et d arrivée, et lorsque l'on a des arrêtes $M \longrightarrow M' \longrightarrow M''$ on ne fera pas apparaitre l'arrête $M \longrightarrow M''$).

Solution :



2) (6.5points) Ce graph, vu comme graphe orienté, a t'il des cycles ?

Solution : *Evidemment le graphe précédent n'a pas de cycle comme graphe orienté : en terme de polygones (cf. exercice G, question 1) et exercice G, question 6)) une flèche est orientée vers un polygone plus bas, or, (cf. exercice G, question 4),) si deux classes de conjugaison ont le même polygone, elles sont égales : autrement dit, puisque l'on enlève les arrêtes ayant même sommet de départ et d'arrivée, le sommet d'arrivée d'une flèche a un polygone strictement en dessous de celui de départ : on ne peut donc pas avoir de cycle.*

Et si on oublie l'orientation ?

Solution : *Si par contre on oublie l'orientation des flèches, on voit que le graph précédent possède deux cycles.*

Exercice I : (**Facteurs irréductibles du polynôme minimal et du polynôme caractéristique**)

On va chercher, dans ce problème, a comparer la décomposition en produit d'irréductibles du polynôme minimal et du polynôme caractéristique d'un endo morphisme.

À noter immédiatement que le corollaire IV.7.3 du théorème IV.7.2 de CAYLEY–HAMILTON est abusif. En effet du théorème de CAYLEY–HAMILTON assurant que

$$P_{\textbf{min}\ u} | P_{\textbf{car}\ u}$$

il résulte immédiatement que, tout facteur irréductible de $P_{\textbf{min}\ u}$ est un facteur irréductible de $P_{\textbf{car}\ u}$, mais rien ne permet à ce point d'affirmer que, réciproquement un facteur irréductible de $P_{\textbf{car}\ u}$ soit un facteur irréductible de $P_{\textbf{min}\ u}$ (hormis si toutefois il est de degré 1 mais ceux-ci jouent un rôle particulier (cf. question 1).))

En fait, dans la présentation qui est faite dans le cours, le corollaire IV.7.3 devrait apparaître comme un corollaire du corollaire IV.11.11. Ce dernier est lui-même un corollaire de la proposition IV.6.4 (cf. DOC n° III, n° III.1.exercice C) et

bien entendu du théorème IV.11.5 de réduction de FROBENIUS. C'est précisément le recours à ce dernier résultat, qui est l'un des plus techniques de ce cours, qui pourrait inciter à donner un argument alternatif ; ce que nous allons faire dans ce qui suit.

Dans tout cet exercice, $\mathbb{K}$ est un corps, $n \in \mathbb{N}^*$, E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. On note $P_{\mathbf{car}\, u}$ (resp. $P_{\mathbf{min}\, u}$,) le *polynôme caractéristique* (cf. cours IV.6.1,) (resp. le *polynôme minimal* (cf. cours IV.2.2.iv).))

1) (6.5points) (**Les facteurs de degré** 1)
Rappeler pourquoi

$$\forall \lambda \in \mathbb{K},\ (X-\lambda)|P_{\min u} \ \Leftrightarrow\ (X-\lambda)|P_{\mathrm{car}\, u}$$

et en déduire que si $\mathbb{K}$ est algébriquement clos,

$$P_{\mathrm{car}\, u}|(P_{\min u})^n\ .$$

Solution : *Découle de l'équivalence entre IV.5.1.a) et IV.5.1.d).*

On sait déjà, grâce au théorème IV.7.2 de CAYLEY–HAMILTON, que

$$P_{\mathbf{min}\, u}|P_{\mathbf{car}\, u}\ .$$

On va montrer, (cf. question 7), c),) que

$$P_{\mathbf{car}\, u}|[P_{\mathbf{min}\, u}]^n\ .$$

L'élément technique principal pour prouver l'énoncé de divisibilité ci-dessus est la possibilité de faire la division euclidienne d'un polynôme à coefficients dans un anneau de matrices par un autre (cf. question 6).) La dificulté réside alors dans le fait de pouvoir justifier une telle construction. Si $A[X]$ et en effet un anneau de polynômes à une indéterminée, nous n'avons formellement établi un théorème de la *division euclidienne* que dans le cas où A est un corps (cf. cours III.4.2 ;) sans compter que nous n'avons même défini les anneaux de polynôme que dans le cas où A est un anneau commutatif (cf. cours III,) et que nous nous sommes bornés à ne donner la plupart des résultat que dans le cas où A est intègre. Or si l'on veut considérer l'anneau $\mathcal{M}_n(\mathbb{K})$ on sait de longue date qu'il n'est ni intègre ni commutatif. Qui plus est, on risque d'être amené, comme on l'a déjà fait (cf. DOC n° III, n° III.1.exercice D,) à identifier les deux anneaux

$$\big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ et } \mathcal{M}_n(\mathbb{K}[X]) \textbf{ (cf. question 3) .)}$$

On rappelle que, pour un anneau commutatif A, on note $\mathcal{M}_n(A)$ l'anneau des matrices carrées de taille $n \times n$ à coefficients dans A. On rapelle que cet anneau est isomorphe à l'anneau $\mathrm{End}_{A-\mathbf{mod}}(A^n)$ des endomorphismes du A-module libre A^n ; cet isomorphisme n'étant pas canonique mais donné par le choix d'une base de A^n.

2) (6.5points) (**L'anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$**)
Notons $\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathcal{M}_n(\mathbb{K})$. On va définir l'anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ des polynômes à une indéterminée à coefficients dans l'anneau $\mathcal{M}_n(\mathbb{K})$ des matrices $n \times n$ comme le sous anneaux des éléments presques nuls de l'anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ des séries formelles à coefficients dans $\mathcal{M}_n(\mathbb{K})$ dont on rappelle brièvement la construction ci-après. On suit en cela le même schéma que celui exposé dans le chapitre III du cours pour les annaux commutatifs.

i) (Addition : groupe abélien)
Puisque $(\mathcal{M}_n(\mathbb{K}),+)$ est un groupe abélien, $\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}$ a une structure naturelle de groupe abélien donnée par l'addition terme à terme (cf. cours I.6.1.i) ;) pour laquelle l'élément neutre est la suite nulle de valeur constante égale à $0_{\mathcal{M}_n(\mathbb{K})}$ et pour laquelle l'opposé d'une suite $\big(M_k\big)_{,k\in\mathbb{N}}$ est la suite $\big(-M_k\big)_{,k\in\mathbb{N}}$.

ii) (Multiplication : anneau)
Comme dans le cas où A est un anneau commutatif, on définira le *produit de* CAUCHY sur $\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}$ (cf. cours III.1.2.2,)

$$\forall (M,P) \in \mathcal{M}_n(\mathbb{K})^{\mathbb{N}} \times \mathcal{M}_n(\mathbb{K})^{\mathbb{N}},\ (M *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} P)_k\ :=\ \sum_{i=0}^{k} M_i *_{\mathcal{M}_n(\mathbb{K})} P_{k-i}\ .$$

Il faut d'ores et déjà remarquer que $*_{\mathcal{M}_n(\mathbb{K})}$ n'étant pas commutative, $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ ne le sera pas davantage. Il est cependant toute à fait élémentaire de vérifier que $\big(U_k\big)_{,k\in\mathbb{N}}$ définie par

$$U_0\ :=\ I\ =\ 1_{\mathcal{M}_n(\mathbb{K})} \text{ et } \forall k \in \mathbb{N}^*,\ U_k\ :=\ 0_{\mathcal{M}_n(\mathbb{K})},$$

est un élément neutre pour $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ qu'on notera abusivment I ou même 1 dans la suite, et que

$$\begin{array}{lll} \forall (M,P,Q) \in \mathcal{M}_n(\mathbb{K})^{\mathbb{N}} \times \mathcal{M}_n(\mathbb{K})^{\mathbb{N}} \times \mathcal{M}_n(\mathbb{K})^{\mathbb{N}}, & (M+P) *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} Q & = M *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} Q + P *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} Q \\ \text{et} & M *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} (P+Q) & = M *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} P + M *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} Q\ ; \end{array}$$

c'est-à-dire que $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ est distributive sur $+$.
On notera $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ l'anneau ainsi construit.

iii) (Anneau des polynômes)

On s'intéressera cependant surtout au sous-anneau $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ de $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ constitué des suites presque nulles, *i.e.* des suites $\big(M_k\big)_{,k\in\mathbb{N}}$ pour lesquels il existe $p \in \mathbb{N}$ tel que pour tout $q \geq p, M_q = 0_{\mathcal{M}_n(\mathbb{K})}$.

Il est fastidieux mais sans grande difficulté de vérifier que

$$\big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ est effectivement un sous-anneau de } \big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$$

ce qui signifie (cf. cours I.3.3,) que $\big(\big(\mathcal{M}_n(\mathbb{K})\big)[X],+\big)$ est un sous-groupe de $\big(\big(\mathcal{M}_n(\mathbb{K})\big)[X],+\big)$, que $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ est stable par le produit de CAUCHY $*_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}}$ et que l'élément unité I est dans $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$.

Il ne s'agit rien moins, mais rien de plus non plus que de vérifier que la somme et le produit de deux suites presque nulle est encore une suite presque nulle ; les arguments étant alors exactement de même nature que dans le cas d'un anneau commutatif.

iv) (Degré et valuation)

On peut encore définir la *valuation* $\mathrm{val}(\cdot)$ d'un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ (cf. cours III.1.14,) ou de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ et le *degré* $\deg(\cdot)$ d'un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ (cf. cours III.2.3.) Cependant il convient de s'arrêter un instant sur leurs propriétés (cf. b).)

v) (Morphisme structural)

L'application

$$\iota : \mathcal{M}_n(\mathbb{K}) \to \big(\mathcal{M}_n(\mathbb{K})\big)[[X]], \ M \mapsto (M, 0, 0, \ldots, 0, \ldots)$$

est encore un morphisme injectif d'anneaux qui est en fait à valeurs dans $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$; identifiant $\mathcal{M}_n(\mathbb{K})$ à un sous-anneau de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$; si bien que, pour tout $M \in \mathcal{M}_n(\mathbb{K})$ on notera simplement M pour la série formelle (resp. le polynôme) dont le terme de rang 0 est M et les autres termes sont nuls.

Il est encore clair que l'image $\mathrm{Im}\,\iota$ de ι est l'ensemble des éléments de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ de degré 0.

vi) (Loi externe, structure de $\mathcal{M}_n(\mathbb{K})$-module)

Pour tout

$$(A, M) \in \mathcal{M}_n(\mathbb{K}) \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]$$

on peut définir $A \cdot M := A *_{\left(\mathcal{M}_n(\mathbb{K})\right)[X]} M$, en considérant A comme un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ à travers ι.

vii) (Base)

En X l'élément $(0, 1, 0, \ldots, 0, \ldots) \in \big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$, on constate que c'est en fait un élément de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$, et que

$$\forall k \in \mathbb{N}, \ X^k := X *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} \cdots *_{\mathcal{M}_n(\mathbb{K})^{\mathbb{N}}} X$$

est la suite dont le $i^{\text{ième}}$ terme est $\delta_{k,i}$. Comme dans le cas commutatif il n'est pas dificile de montrer que $\{X^k\}_{,k\in\mathbb{N}}$ est une $\mathcal{M}_n(\mathbb{K})$-base de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$.

a) (6.5points) ($n = 1$)

Que dire de $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ et $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ lorsque $n = 1$?

Solution : *Dans ce cas $\mathcal{M}_n(\mathbb{K})$ est canoniquement isomorphe comme anneau à $\mathbb{K}$ et $\big(\mathcal{M}_n(\mathbb{K})\big)[[X]]$ n'est autre que l'anneau $\mathbb{K}[[X]]$ des séries formelles à coefficients dans $\mathbb{K}$ tandis que $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ n'est autre que l'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$.*

b) (6.5points) (**Valuation et degré**)

Soit $(P, Q) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]$, que peut-on dire de :

$$\begin{aligned} &\mathrm{val}(P+Q),\\ &\mathrm{val}(P*Q),\\ &\deg(P+Q)\\ \text{et}\quad &\deg(P*Q)\,. \end{aligned}$$

Bien qu'on n'ait pas, en général, $P * Q = Q * P$, aurait-on cependant

$$\deg(P*Q) = \deg(Q*P)\ ?$$

Solution :

$*$) ***(Somme)***

Comme dans le cas d'un anneau de polynômes à coefficients dans un anneau commutatif on a encore

$$\mathrm{val}(P+Q) \geq \min(\mathrm{val}(p), \mathrm{val}(Q)) \text{ et } \deg(P+Q) \leq \max(\deg(P), \deg(Q))$$

avec égalité dans le cas de valuations (resp. degrés) différents, puisque ces résultats ne reposent que sur la structure de groupe abélien de $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$.

†) ***(Produit)***

Il découle presque immédiatement de la définition du produit de CAUCHY *que*

$$\mathrm{val}(P*Q) \;\geq\; \mathrm{val}(P)+\mathrm{val}(Q) \text{et } \deg(P*Q) \;\leq\; \deg(P)+\deg(Q)\,.$$

On avait cependant bien remarqué qu'on avait égalité dans le cas des anneaux intègres.

Ici il suffit de s'intéresser à des éléments de degré 0*, pour obtenir des contre-exemples. Dès que* $n \geq 2$ *en effet, on sait bien qu'on peut trouver*

$$(A,B) \in \mathcal{M}_n(\mathbb{K})\times\mathcal{M}_n(\mathbb{K}) \text{ tel que } A\neq 0\,,\; B\neq 0 \text{ et } A*B = 0\,.$$

Il s'ensuit que

$$\mathrm{val}(A*B) = +\infty > 0 = \mathrm{val}(A)+\mathrm{val}(B) \text{ et } \deg(A*B) = -\infty < 0 = \deg(A)+\deg(B)\,.$$

‡) *On peut aussi trouver*

$$(A,B) \in \mathcal{M}_n(\mathbb{K})\times\mathcal{M}_n(\mathbb{K}) \text{ tel que } A*B = 0 \text{ et } B*A\neq 0\,.$$

ce qui entraîne

$$\deg(A*B) = -\infty \text{ et } \deg(B*A) = 0\,.$$

3) (6.5points) Montrer qu'il existe un unique morphisme d'anneau $\mathcal{M}_n(\mathbb{K})$-linéaire :

$$\begin{array}{rccl}\phi: & \big(\mathcal{M}_n(\mathbb{K})\big)[X] & \longrightarrow & \mathcal{M}_n(\mathbb{K}[X]) \\ & X & \longmapsto & M_1 := \begin{pmatrix} X & 0 & \dots & 0 & 0 \\ 0 & X & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & X & 0 \\ 0 & 0 & \dots & 0 & X \end{pmatrix}\end{array}$$

et que de plus ϕ est un isomorphisme.

Indication : *On pourra noter*

$$\forall i\in\mathbb{N},\; M_i := M_1^i$$

et remarquer que M_i *commute avec tous les éléments de* $\mathcal{M}_n(\mathbb{K}[X])$.

Solution :

i) ***(Condition nécessaire (unicité))***

Notons $M_1 \in \mathcal{M}_n(\mathbb{K}[X])$ *la matrice*

$$XI := \begin{pmatrix} X & 0 & \dots & 0 & 0 \\ 0 & X & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & X & 0 \\ 0 & 0 & \dots & 0 & X \end{pmatrix}\,.$$

Si ϕ *est un morphisme d'anneau,*

$$\forall k\in\mathbb{N},\; \phi(X^k) = \phi(X)^k = M_1^k = M_k := \begin{pmatrix} X^k & 0 & \dots & 0 & 0 \\ 0 & X^k & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & X^k & 0 \\ 0 & 0 & \dots & 0 & X^k \end{pmatrix}\,.$$

Puisque $\{X^k\}_{k\in\mathbb{N}} \subset \big(\mathcal{M}_n(\mathbb{K})\big)[X]$ *est une base de* $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$*, si on demande à* ϕ *d'être* $\mathcal{M}_n(\mathbb{K})$*-linéaire il est entièrement déterminé.*

*ii) (**Condition suffisante (existence)**)*

Reste à montrer que le morphisme $\mathcal{M}_n(\mathbb{K})$-linéaire défini ci-dessus est bien un morphisme d'anneaux.

Il est claire que

$$\phi(1_{\left(\mathcal{M}_n(\mathbb{K})\right)[X]}) \;=\; \phi(X^0) \;=\; M_0 \;=\; \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} .$$

De plus :

$$\begin{aligned} &\forall P \;:=\; \sum_{i=0}^{d} A_i X^i \in \left(\mathcal{M}_n(\mathbb{K})\right)[X], \\ &\forall Q \;:=\; \sum_{i=0}^{e} B_i X^i \in \left(\mathcal{M}_n(\mathbb{K})\right)[X], \\ &\phi(P * Q) \;=\; \phi\left(\sum_{i=0}^{d}\sum_{j=0}^{e} A_i * B_j X^{i+j}\right) \\ &\qquad = \sum_{i=0}^{d}\sum_{j=0}^{e} A_i * B_j * \phi(X^{i+j}) \\ &\qquad = \sum_{i=0}^{d}\sum_{j=0}^{e} A_i * B_j * M_{i+j} \\ &\qquad = \sum_{i=0}^{d}\sum_{j=0}^{e} A_i * B_j * M_i * M_j \; . \end{aligned}$$

On rencontre le seul point délicat de la preuve ici, ou du moins le seul qui diffère vraiement d'un calcul analogue dans des anneaux commutatifs. Il faut en effet remarquer ici que

$$\forall i \in \mathbb{N},\; \forall A \in \mathcal{M}_n(\mathbb{K}[X]),\; M_i * A \;=\; A * M_i \; ;$$

c'est-à-dire que les matrices M_i commutent avec toutes les autres ; ce qui est bien connu (ce sont des matrices scalaires, à coefficients dans $\mathbb{K}[X]$ certes.)

Il s'ensuit que :

$$\begin{aligned} \phi(P * Q) \;&=\; \sum_{i=0}^{d}\sum_{j=0}^{e} A_i * M_i * B_j * M_j \\ &=\; \sum_{i=0}^{d} A_i * M_i * \sum_{j=0}^{e} B_j * M_j \\ &=\; \phi(P) * \phi(Q) \; . \end{aligned}$$

*iii) (**Bijectivité**)*

Il suffit de montrer que $\{M_k\}_{k\,\in\,\mathbb{N}}$ est une base de $\mathcal{M}_n(\mathbb{K}[X])$. C'est essentiellement ce qu'on a fait au DOC n° III, n° III.1.exercice D, question 1).

Il est presque immédiat de montrer que $\{M_k\}_{k\,\in\,\mathbb{N}}$ est une famille libre. Si en effet $\displaystyle\sum_{i=1}^{r} A_i * M_i \;=\; 0,$

$$\forall 1 \le j \le n,\; \forall 1 \le k \le n,\; \sum_{i=1}^{r} A_{i,j,k} X^i \;=\; 0 \; ;$$

ce qui entraîne,, puisque $\{X^k\}_{k\,\in\,\mathbb{N}} \;\subset\; \mathbb{K}[X]$ est une base de $\mathbb{K}[X]$,

$$\forall 1 \le i \le r,\; \forall 1 \le j \le n,\; \forall 1 \le k \le n,\; A_{i,j,k} \;=\; 0 \textit{ i.e. } \forall 1 \le i \le r,\; A_i \;=\; 0_{\mathcal{M}_n(\mathbb{K})} \; .$$

Pour tout

$$(M_{i,j})\frac{1 \le i \le n}{1 \le j \le n} \;\in\; \mathcal{M}_n(\mathbb{K}[X]) \; ,\; \forall 1 \le i \le n,\; \forall 1 \le j \le n,\; M_{i,j} \;\in\; \mathbb{K}[X] \; .$$

Donc

$$M_{i,j} \;=\; \sum_{\ell=0}^{d_{i,j}} \alpha_{i,j,\ell} X^{\ell} \; .$$

On prolongera les applications $\alpha_{i,j,.}$ en posant

$$\forall \ell \in \mathbb{N},\ \ell\ >\ d_{i,j}\ \Rightarrow\ \alpha_{i,j,\ell}\ =\ 0\ .$$

Posons alors

$$d\ :=\ \max_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ n}}(d_{i,j})\ \text{et}\ \forall 0 \leq \ell \leq d,\ A_\ell\ \textit{la matrice}\ \alpha_{i,j,\ell}\ . \qquad 1$$

Il est ensuite facile de constater que

$$M\ =\ \sum_{\ell=0}^{d} A_\ell * M_\ell\ . \qquad 2$$

L'isomorphisme ϕ ci-dessus permet donc d'identifier (en tant qu'anneau) les polynômes dont les coefficients sont des matrices $\big(\mathcal{M}_n(\mathbb{K})\big)[X]$ au matrices dont les coefficients sont des polynômes $\mathcal{M}_n(\mathbb{K}[X])$. On se placera donc, dans la suite, sous l'un ou l'autre point de vue, selon ce qui sera le plus commode. En particulier on oubliera la notation M_i pour lui préférer X^i, dont on gardera bien à l'esprit que c'est une matrice qui commute avec n'importe quel élément de $\mathcal{M}_n(\mathbb{K}[X])$. On notera I l'unité de ces anneaux qui est la matrice identité de $\mathcal{M}_n(\mathbb{K})$.

4) (6.5points) (**Valuation et degré**)

Pour $M\ \in\ \big(\mathcal{M}_n(\mathbb{K})\big)[X]$ comparer la valuation et le degré de M définis en question 2), iv) et les valuations et degré respectifs des coefficients de la matrice $\phi(M)$.

Solution : *Si on note*

$$\phi(M)\ =\ (M_{i,j})_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ n}}$$

on rappelle que les $M_{i,j}$ sont des éléments de $\mathbb{K}[X]$. Les formules question 3), iii).1 et question 3), iii).2 montrent alors que

$$\deg(M)\ =\ \max_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ n}}(\deg(M_{i,j}))\ \text{et}\ \text{val}(M)\ =\ \min_{\substack{1\ \leq\ i\ \leq\ n\\ 1\ \leq\ j\ \leq\ n}}(\text{val}(M_{i,j}))\ .$$

5) (6.5points) (**Éléments inversibles**)

Puisque $\mathcal{M}_n(\mathbb{K})$ est un sous-anneau de $\phi\ :\ \big(\mathcal{M}_n(\mathbb{K})\big)[X]\ \cong\ \mathcal{M}_n(\mathbb{K}[X])$, tout inversible de $\mathcal{M}_n(\mathbb{K})$ est encore inversible dans $\mathcal{M}_n(\mathbb{K}[X])$. En revanche il n'est pas tout à fait immédiat de déterminer exactement ce qu'est $(\mathcal{M}_n(\mathbb{K}[X]))^\times$; ce dont d'ailleurs nous n'aurons pas explicitement besoin. On peut cependant remarquer :

a) (6.5points) (**Matrice de carré nul**)

Montrer que si $A\ \in\ \mathcal{M}_n(\mathbb{K})$ vérifie $A^2\ =\ 0$, $I - AX$ est inversible.

Solution : *En effet,*

$$(I - AX) * (I + AX)\ =\ I^2 - (AX)^2\ =\ I - A^2X^2\ =\ I\ .$$

b) (6.5points) (**Matrices nilpotentes**)

Plus généralement montrer que si $A\ \in\ \mathcal{M}_n(\mathbb{K})$ est tel que $A^n\ =\ 0$, (nilpotente d'échelon n (cf. cours IV.8.1,)) $I - AX$ est inversible.

Solution : *Puisque X et A commutent, on a :*

$$(I - AX) * \sum_{i=0}^{n-1} X^i A^i\ =\ I - X^n A^n\ =\ I\ .$$

6) (6.5points) (**Division euclidienne**)

Pour tout $(M, P)\ \in\ \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]$ tel que

$$P\ =\ \sum_{i=0}^{d} P_i X^i\ \text{ avec }\ P_d\ \in\ \mathcal{M}_n(\mathbb{K})^\times\ \text{ inversible,}$$

montrer qu'il existe

$$(Q, R)\ \in\ \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X]\ \text{ tel que }\ M\ =\ P * Q + R\ \text{et}\ \deg(R)\ <\ \deg(P)\ .$$

Indication : *On pourra adapter la méthode utilisée dans le III.7.7.*

Solution : *On procède comme dans le III.7.7. On pourrait d'ailleurs renvoyer à ce texte en justifiant que l'argument clef est que le coefficient de plus haut degré de P est inversible. Cependant, outre le fait qu'on doit ttraiter la question pour un anneau non intègre, une difficulté supplémentaire réside ici dans le fait que les coefficients que nous considérons appartiennent à un anneau qui n'est pas commutatif. L'honnêteté veut donc que l'on réexamine les arguments de cette preuve sous les hypothèses faibles faites ici.*

i) *($\deg(M) < \deg(P)$)*
Il suffit, dans ce cas de prendre

$$Q = 0 \text{ et } R = M .$$

ii) *($\deg(M) \geq \deg(P)$)*

$*$) *Il existe (cf. III.7.7.question 3),)*

$$(S, C) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ tel que } M = P * S + C \text{ et } \deg(C) < \deg(M) .$$

En effet, définissons S par

$$S_{\deg(M)-\deg(P)} = P_d^{-1} * M_{\deg(M)} \text{ et } \forall k \in \mathbb{N},\ k \neq \deg(M) - \deg(P)\ ,\ S_k = 0 .$$

Par construction on a alors

$$C := M - P * S \text{ avec } \deg(C) < \deg(M) .$$

†) (***Raisonement par récurrence***)
On termine l'argument par récurrence sur l'entier $\deg(M) - \deg(P)$ (cf. III.7.7.question 4).) En effet, C étant construit comme ci-dessus, $\deg(C) - \deg(P) < \deg(M) - \deg(P)$, on peut écrire

$$C = P * T + R \text{ avec } \deg(R) < \deg(P)$$

d'où il résulte

$$M = P * S + C = P * S + P * T + R = P(S + T) + R .$$

7) (6.5points) (**Facteurs irréductibles**)
Soit

$$A \in \mathcal{M}_n(\mathbb{K}) \text{ et } M := P_{\textbf{min } A} I \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \cong \mathcal{M}_n(\mathbb{K}[X]) .$$

a) (6.5points) (**Division euclidienne**)
Montrer qu'il existe

$$(Q, R) \in \big(\mathcal{M}_n(\mathbb{K})\big)[X] \times \big(\mathcal{M}_n(\mathbb{K})\big)[X] \text{ tel que } M = (A - IX) * Q + R \text{ et } \deg(R) < 1 .$$

Solution : *Il faut juste constater que $A - IX$ est de degré 1 et de coefficient de plus haut degré I qui est inversible si bien qu'on est dans les conditions d'application de la question 6).*

b) (6.5points) Montrer que $R = 0$.
Solution : *Il suffit d'évaluer l'identité précédente en A.*

c) (6.5points)

$$P_{\text{car } A} | [P_{\text{min } A}]^n .$$

Solution : *Il découle de a) et b) que $M = (A - IX) * Q$. d'où il résulte*

$$[P_{min\ A}]^n = \det(M) = \det(A - IX) * \det(Q) = P_{car\ A} * \det(Q) .$$

d) (6.5points) (**Facteurs irréductible**)
En déduire que tout facteur irréductible de $P_{\text{car } A}$ est un facteur irréductible de $P_{\text{min } A}$.
Solution : *C'est bien entendu maintenant une conséquence immédiate de c) et du lemme de* GAUSS.

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Examen partiel du 3 mars 2020
Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Exercice A : (6points) **On note** (x_1, x_2, x_3) **les coordonnées d'un vecteur** $x \in \mathbb{Z}^3$. **On considère dans** $A := \mathbb{Z}^3$ **le sous-groupe** B **engendré par** $v = (6, -12, 0)$ **et** $w = (0, 8, 4)$.

1) On note $A^* := \mathrm{Hom}_{\mathbf{Gr}}(A, \mathbb{Z})$ **l'ensemble des homomorphismes de groupes de** A **à valeurs dans** $\mathbb{Z}$, **également appelé ensemble des *formes linéaires entières* sur** A.

a) Rappeler rapidement pourquoi A^* est un groupe abélien.

b) Le groupe A^* est-il de type fini ? libre ? (On peut parfaitement résoudre la fin de l'exercice sans répondre à cette question.)

c) Montrer que

$$A^* \to \mathbb{Z}\,,\ f \mapsto f(v) \text{ (resp. } A^* \to \mathbb{Z}\,,\ f \mapsto f(w)\ )$$

est un morphisme de groupes dont l'image est

$$\text{le sous-groupe } 6\mathbb{Z} \text{ de } \mathbb{Z} \text{ (resp. le sous-groupe } 4\mathbb{Z} \text{ de } \mathbb{Z}\ .)$$

d) En déduire que

$$\forall f \in A^*,\ f(B) \subset 2\mathbb{Z}\,.$$

2) Soit $f \in A^*$ **la forme linéaire définie par** $x \mapsto x_1 - x_3$.

a) Trouver $v_1 \in B$ tel que $f(v_1) = 2$.

b) Montrer que $v_1 = 2u_1$ pour un $u_1 \in A$.

3) Montrer que

a)

$$A = \mathbb{Z}u_1 \oplus \mathrm{Ker}\, f\ ;$$

b) puis que

$$B = \mathbb{Z} \cdot 2u_1 \oplus (\mathrm{Ker}\, f \cap B) = \mathbb{Z}v_1 \oplus (\mathrm{Ker}\, f \cap B)\,.$$

4) **a)** Écrire les coordonnées d'un vecteur $\lambda v + \mu w$ $(\lambda, \mu \in \mathbb{Z})$.

b) En déduire que $\mathrm{Ker}\, f \cap B$ est l'ensemble des vecteurs de la forme $(12t, 0, 12t)$ où t décrit $\mathbb{Z}$.

c) En déduire une base de B, et une base

$$\{u_1, u_2, u_3\} \text{ de } A \text{ telle que } B = \mathbb{Z} \cdot 2u_1 \oplus \mathbb{Z} \cdot 12u_2\,.$$

Exercice B : (7pts) **Pour un groupe abélien G, on dira que G *possède une* $\mathbb{Z}$*-base* s'il possède une base en tant que groupe abélien libre (ou encore en tant que $\mathbb{Z}$-module libre.)**

On note A le groupe abélien $\mathbb{Z}^n$ vu comme sous-groupe de l'espace vectoriel $V := \mathbb{Q}^n$. Soit $B \subset A$ un sous-groupe. On note W le sous-$\mathbb{Q}$-espace vectoriel de V engendré par B et par $i : A \hookrightarrow V$ l'injection naturelle de A dans V.

1) **a)** Montrer que des vecteurs $v_1, v_2, \ldots, v_m \in V$ sont linéairement indépendants sur $\mathbb{Q}$ si et seulement si ils le sont sur $\mathbb{Z}$.

b) Montrer que tout sous-groupe de type fini $G \subset V$ est libre de rang $r \leq n$.

c) Est-ce que V est un groupe abélien de type fini ? (On pourra considérer le cas $n = 1$.)

2) Rappeler rapidement (en citant le théorème adéquat) pourquoi il existe $r \in \mathbb{N}, r \leq n$ tel que $B \cong \mathbb{Z}^r$.

3) Supposons qu'il existe une $\mathbb{Z}$-base $(u_1, \cdots, u_r)$ de B qui puisse se compléter en une $\mathbb{Z}$-base $(u_1, \cdots, u_n)$ de A. Montrer alors que $B = A \cap W$.

4) Supposons réciproquement que $B = A \cap W$. On va montrer qu'alors (cf. f),) B possède une base qui se complète en une base de A.

Soit $W' := V/W$ l'espace vectoriel quotient de V par W et soit $p : V \to W'$ la surjection canonique.

a) Montrer que $p \circ i : A \to W'$ est un morphisme de groupes dont B est le noyau.

b) En notant $q : A \to A/B$ la surjection canonique, montrer qu'il existe un unique morphisme de groupes injectif

$$j : A/B \hookrightarrow W' \text{ tel que } j \circ q = p \circ i .$$

c) Montrer que le groupe abélien quotient $C := A/B$ est libre de type fini de rang $\leq n$.

Soit $c_1, \ldots, c_s$ une $\mathbb{Z}$-base de C, $a_1, \ldots, a_s$ des relèvements des c_k (c'est-à-dire que $\forall 1 \leq k \leq s,\ q(a_k) = c_k$,) dans A, et $C' \subset A$ le sous-groupe engendré par les a_k ,$1 \leq k \leq s$.

d) Montrer que l'application quotient $q : A \to A/B = C$ se restreint en un isomorphisme de C' vers C.

e) En déduire que $A \cong B \oplus C'$ et donc que A est isomorphe à $B \times C$.

f) Montrer enfin qu'il existe une $\mathbb{Z}$-base de B qui se complète en une $\mathbb{Z}$-base de A.

5) Soit $b \neq 0$ un élément de A et B le sous-groupe qu'il engendre.

Montrer que les conditions suivantes sont équivalentes :

i) Le sous-groupe B possède une $\mathbb{Z}$-base qui se complète en une $\mathbb{Z}$-base de A.

ii)
$$B = A \cap W .$$

iii)
$$\mathbf{Pgcd}\big(b_k\ ,1 \leq k \leq n\big) = 1\ ,\ b = (b_1, \cdots, b_n) .$$

Exercice C : (2points) **Considérons le diagramme commutatif de groupes abéliens à lignes exactes suivant :**

$$\begin{array}{ccccccccc} 0 & \to & N_1 & \xrightarrow{i_1} & A_1 & \xrightarrow{p_1} & Q_1 & \to & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \to & N_2 & \xrightarrow{i_2} & A_2 & \xrightarrow{p_2} & Q_2 & \to & 0 \end{array}$$

c'est-à-dire que pour $j = 1$ ou 2 :

- **N_j, A_j et Q_j sont des groupes abéliens,**
- **i_j est un morphisme de groupes injectif,**
- **p_j est un morphisme de groupe surjectif,**
- $$\operatorname{Im} i_j = \operatorname{Ker} p_j ,$$
- $$g \circ i_1 = i_2 \circ f \text{ et } h \circ p_1 = p_2 \circ g .$$

1) Montrer que si g est injectif, f l'est aussi ; si g est surjectif, h l'est aussi.

2) Montrer que si f et h sont injectifs il en est de même de g.

3) Montrer que si f et h sont surjectifs il en est de même de g.

Exercice D : (5points) **Soit A un anneau principal. Pour tout $x \in A$, on notera xA l'idéal principal engendré par x, A/xA l'anneau quotient et $\pi_x : A \to A/xA$ la surjection canonique.**

Soient

$$b \in A \setminus \{0\}\,,\ B := A/bA \text{ et } q : B \to C$$

un morphisme d'anneaux surjectif, dont on note $D := \operatorname{Ker} q$ le noyau.

1) Montrer qu'il existe $c \in A \setminus \{0\}$ et un isomorphisme d'anneaux $\phi : A/cA \to C$ tels que

$$\phi \circ \pi_c = q \circ \pi_b \text{ et } c|b\,.$$

2) Montrer que $\pi_b^{-1}(D)$ est un idéal de A, le déterminer et justifier que

$$D = \pi_b[\pi_b^{-1}(D)]\,.$$

3) En notant $\gamma : A \to A\,,\ x \mapsto cx$, montrer que $\pi_b \circ \gamma$ est un morphisme de groupes d'image D.

4) En étudiant le noyau de $\pi_b \circ \gamma$ montrer qu'il existe $d \in A$ tel que $b = cd$ et un isomorphisme de groupes

$$\delta : A/dA \cong D \text{ tel que } \delta \circ \pi_d = \pi_b \circ \gamma\,.$$

5) On suppose désormais que c et d sont premiers entre eux.

a) Rappeler pourquoi il existe

$$(u, v) \in A \times A\,,\ cu + dv = 1\,.$$

b) Pour tout $\alpha \in C$, soit $x \in A$ tel que

$$\alpha = q[\pi_b(x)] = \phi[\pi_c(x)]\,.$$

Posons alors $s(\alpha) := \pi_b(dvx)$.

Montrer que $s(\alpha)$ est bien définie (indépendamment du choix de x,) et qu'ainsi défini

i) $s : C \to B$ est un morphisme de groupes ;

ii)

$$q \circ s = \mathrm{Id}_C\,;$$

iii)

$$\forall \alpha \in C,\ \forall a \in A,\ s\big[q[\pi_b(a)]\alpha\big] = s\big[\phi[\pi_c(a)]\alpha\big] = \pi_b(a)s(\alpha)\,.$$

6) Montrer réciproquement que s'il existe une application $s : C \to B$ vérifiant les points i) à iii) de la question 5), b), c et d sont premiers entre eux.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Corrigé de l'examen partiel du 3 mars 2020

Exercice A : (6points) **On note** (x_1, x_2, x_3) **les coordonnées d'un vecteur** $x \in \mathbb{Z}^3$. **On considère dans** $A := \mathbb{Z}^3$ **le sous-groupe** B **engendré par** $v = (6, -12, 0)$ **et** $w = (0, 8, 4)$.

1) (2pts) **On note** $A^* := \mathrm{Hom}_{\mathbf{Gr}}(A, \mathbb{Z})$ **l'ensemble des homomorphismes de groupes de** A **à valeurs dans** $\mathbb{Z}$, **également appelé ensemble des *formes linéaires entières* sur** A.

a) (0.5pts) Rappeler rapidement pourquoi A^* est un groupe abélien.
Solution : *On sait que pour deux groupes G et H, si H est abélien $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ est un groupe abélien (cf. I.6.2.)*

b) (bonus) Le groupe A^* est-il de type fini ? libre ? (On peut parfaitement résoudre la fin de l'exercice sans répondre à cette question.)
Solution : *Puisque A est libre de rang n, il possède une base $(e_1, \ldots, e_n)$. Alors $\forall 1 \leq i \leq n$, il existe un unique*

$$e_i^* : A \to \mathbb{Z}, \ e_j \mapsto \delta_{i,j}, 1 \leq j \leq n \ \textit{(cf. II.2.10 .)}$$

Il est dès lors facile de montrer (ou à tout le moins les arguments sont-ils exactement ceux utilisés dans le cas des espaces vectoriels) que $e_i^*, 1 \leq i \leq n$ est une base de A^* qu'on pourrait tout à fait appeler base duale de $e_i, 1 \leq i \leq n$. Il s'ensuit que A^* est alors libre de même rang n que A.

c) (1pt) Montrer que

$$A^* \to \mathbb{Z}, \ f \mapsto f(v) \text{ (resp. } A^* \to \mathbb{Z}, \ f \mapsto f(w) \text{)}$$

est un morphisme de groupes dont l'image est

$$\text{le sous-groupe } 6\mathbb{Z} \text{ de } \mathbb{Z} \text{ (resp. le sous-groupe } 4\mathbb{Z} \text{ de } \mathbb{Z} .)$$

Solution : *D'abord*

$$\forall (f, g) \in A^* \times A^*, \ \forall x \in A, \ (f + g)(x) = f(x) + g(x)$$

ce qui prouve que

$$A^* \to \mathbb{Z}, \ f \mapsto f(x)$$

est un morphisme de groupes.
Notons

$$v' := (1, -2, 0) \text{ et } w' := (0, 2, 1),$$

si bien que

$$v = 6v' \text{ et } w = 4w' .$$

Il s'ensuit que :

$$\begin{array}{rrcl} \forall f \in A^*, & f(v) & = & f(6v') \\ & & = & 6f(v') \\ & f(v) & = & f(4w') \\ & & = & 4f(w') . \end{array}$$

Il s'ensuit que

$$\mathrm{Im}\,(A^* \to \mathbb{Z}, \ f \mapsto f(v)) \subset 6\mathbb{Z} \text{ et } \mathrm{Im}\,(A^* \to \mathbb{Z}, \ f \mapsto f(w)) \subset 4\mathbb{Z} .$$

Or pour

$$f = x \mapsto x_1 \ (\textit{resp. } f = x \mapsto x_3 ,)$$

on a

$$f(v) = 6 \ (\textit{resp. } f(w) = 4 .)$$

Puisque $\mathrm{Im}\,(A^* \to \mathbb{Z}, \ f \mapsto f(v))$ et $\mathrm{Im}\,(A^* \to \mathbb{Z}, \ f \mapsto f(w))$ sont des sous-groupes de $\mathbb{Z}$ et du fait des inclusions obtenues plus haut on a finalement

$$\mathrm{Im}\,(A^* \to \mathbb{Z}, \ f \mapsto f(v)) = 6\mathbb{Z} \textit{ et } \mathrm{Im}\,(A^* \to \mathbb{Z}, \ f \mapsto f(w)) = 4\mathbb{Z} .$$

d) (0.5pts) En déduire que

$$\forall f \in A^*,\ f(B) \subset 2\mathbb{Z}\,.$$

Solution : *Pour tout* $x \in B$ *il existe* $(a,b) \in \mathbb{Z}\times\mathbb{Z}$ *tel que* $x = av+bw$; *si bien que pour tout* $f \in A^*$,

$$f(xx) = f(av+bw) = af(v) + bf(w)\,.$$

Il s'ensuit que

$$\forall x \in B,\ f(x) \in 6\mathbb{Z} + 4\mathbb{Z}$$

si bien que

$$f(B) \subset 6\mathbb{Z} + 4\mathbb{Z}\,.$$

Or $2 = (6 \wedge 4)$, *si bien que*

$$6\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}\,.$$

2) (1pt) **Soit** $f \in A^*$ **la forme linéaire définie par** $x \mapsto x_1 - x_3$.

a) (0.5pts) Trouver $v_1 \in B$ tel que $f(v_1) = 2$.
Solution : *On prend* $v_1 = v + w$.

b) (0.5pts) Montrer que $v_1 = 2u_1$ pour un $u_1 \in A$.
Solution : *Il suffit de prendre* $u_1 = (3,-2,2)$.

3) (2pt) Montrer que

a) (1pt)

$$A = \mathbb{Z}u_1 \oplus \operatorname{Ker} f\,;$$

Solution : *Puisque*

$$f(v_1) = 2 \text{ et } v_1 = 2u_1,$$

$f(u_1) = 1$. *Il s'ensuit que* f *est un morphisme surjectif, dont on peut même explicitement donner une section*

$$s : \mathbb{Z} \to A\,,\ a \mapsto au_1\,.$$

Il est en effet immédiat, que s *étant ainsi définie, on a* $f \circ s = \mathrm{Id}_{\mathbb{Z}}$. *La suite exacte*

$$0 \to \operatorname{Ker} f \longrightarrow A \xrightarrow{f} \operatorname{Im} f = \mathbb{Z} \to 0$$

est donc scindée, si bien qu'on a

$$A = \operatorname{Ker} f \oplus \operatorname{Im} s = \operatorname{Ker} f \oplus \mathbb{Z}u_1\,.$$

b) (1pt) puis que

$$B = \mathbb{Z}\cdot 2u_1 \oplus (\operatorname{Ker} f \cap B) = \mathbb{Z}v_1 \oplus (\operatorname{Ker} f \cap B)\,.$$

Solution : **ATTENTION !** *Il ne suffit pas en général que* $A = A' \oplus A''$ $B \subset A$ *pour que* $B = (B \cap A') \oplus (B \cap A'')$; *et ce quelle que soit la structure linéaire considérée. On pourra par exemple penser à la décomposition du plan en somme directe des deux axes de coordonnées et considérer la première bissectrice dont l'intersection avec chacun des axes est le singleton* $\{0\}$, *ce qui ne peut donner une décomposition en somme directe d'une droite.*

Pour tout $x \in B$, $f(x) \in 2\mathbb{Z}$. *Il existe donc* $k_x \in \mathbb{Z}$ *tel que* $f(x) = 2k_x$.

Il s'ensuit que :

$$\begin{aligned} f(x - k_x v_1) &= f(x - 2k_x u_1) \\ &= f(x) - 2k_x f(u_1) \\ &= 0\,; \end{aligned}$$

c'est-à-dire que

$$y := x - 2k_x u_1 = x - k_x v_1 \in \operatorname{Ker} f\,.$$

Or

$$x \in B, k_x v_1 \in B \Rightarrow y \in B\,;$$

si bien qu'on a montré que

$$B = \mathbb{Z}v_1 + (\operatorname{Ker} f \cap B)\,.$$

Puisqu'on a montré à la question précédente que $\operatorname{Ker} f \cap \mathbb{Z}u_1 = \{0\}$, *on a en fait :*

$$B = \mathbb{Z}v_1 \oplus (\operatorname{Ker} f \cap B)\,.$$

4) (3pts) **a)** (0.5pts) Écrire les coordonnées d'un vecteur $\lambda v + \mu w$ $(\lambda, \mu \in \mathbb{Z})$.
Solution :

$$\forall (\lambda, \mu) \in \mathbb{Z} \times \mathbb{Z},\ \lambda v\ +\ \mu w\ =\ (6\lambda, -12\lambda + 8\mu, 4\mu)\ .$$

b) (1pt) En déduire que $\operatorname{Ker} f \cap B$ est l'ensemble des vecteurs de la forme $(12t, 0, 12t)$ où t décrit $\mathbb{Z}$.
Solution :

$$\begin{array}{lrcl}
\forall x \in A, & x & \in & \operatorname{Ker} f \cap B \\
\Leftrightarrow & x\ \in\ B & \text{et} & x\ \in\ \operatorname{Ker} f \\
\Leftrightarrow & \exists (\lambda, \mu)\ \in\ \mathbb{Z} \times \mathbb{Z},\ x = \lambda v + \mu w & \text{et} & f(x) = 0 \\
\Leftrightarrow & x = (6\lambda, -12\lambda + 8\mu, 4\mu) & \text{et} & T\lambda - 4\mu = 0 \\
\Leftrightarrow & x & = & (6\lambda, 0, 6\lambda)\ .
\end{array}$$

Or $6\lambda - 4\mu\ =\ 0$ *i.e.* $3\lambda - 2\mu$ *si bien que,* 2 *et* 3 *étant premiers entre eux,* $2|\lambda$ *i.e.*

$$\exists t\ \in\ \mathbb{Z},\ \lambda\ =\ 2t\ \Leftrightarrow\ \exists t\ \in\ \mathbb{Z},\ x\ =\ (12t, 0, 12t)\ .$$

c) (1.5pts) En déduire une base de B, et une base

$$\{u_1, u_2, u_3\} \text{ de } A \text{ telle que } B\ =\ \mathbb{Z} \cdot 2u_1\ \oplus\ \mathbb{Z} \cdot 12u_2\ .$$

Solution : *On a établi que*

$$B\ =\ \mathbb{Z}v_1\ \oplus\ (B\ \cap\ \operatorname{Ker} f)\ =\ \mathbb{Z}2u_1\ \oplus\ (B\ \cap\ \operatorname{Ker} f)\ .$$

Il découle du fait que

$$B\ \cap\ \operatorname{Ker} f\ =\ \{(12t, 0, 12t)\ ,\ t\ \in\ \mathbb{Z}\}$$

que

$$B\ \cap\ \operatorname{Ker} f\ =\ \mathbb{Z}v_2 \text{ avec } v_2\ =\ (12, 0, 12)\ .$$

Il s'ensuit que (v_1, v_2) *est une base de* B.
De plus en posant $u_2\ :=\ (1, 0, 1)$, *on a*

$$v_2\ =\ 12u_2\ .$$

Il est clair que puisque $v_2\ \in\ \operatorname{Ker} f$ *que*

$$f(v_2)\ =\ 0\ \Rightarrow\ f(12u_2)\ =\ 0\ \Rightarrow\ 12f(u_2)\ =\ 0\ \Rightarrow\ f(u_2)\ =\ 0\ \Rightarrow\ u_2\ \in\ \operatorname{Ker} f\ .$$

Comme on a montré que

$$A\ =\ \mathbb{Z}u_1\ \oplus\ \operatorname{Ker} f,$$

si l'on peut déterminer un vecteur u_3 *tel que* (u_2, u_3) *soit une base de* $\operatorname{Ker} f$, (u_1, u_2, u_3) *sera une base de* A, *répondant, qui plus est, à la condition*

$$v_1\ =\ 2u_1 \text{ et } v_2\ =\ 12u_2\ .$$

$$\begin{array}{lrcl}
\forall x = (x_1, x_2, x_3) \in \operatorname{Ker} f, & f(x) & = & 0 \\
\Leftrightarrow & x_1 - x_3 & = & 0 \\
\Leftrightarrow & x & = & (x_1, x_2, x_1) \\
\Leftrightarrow & x & = & x_1(1, 0, 1) + x_2(0, 1, 0)\ .
\end{array}$$

On constate donc qu'en posant $u_3\ :=\ (0, 1, 0)$, (u_2, u_3) *est une famille génératrice de* $\operatorname{Ker} f$ *dont il est immédiat de constater qu'elle est libre, ce qui permet de conclure.*

Exercice B : (7pts) **Pour un groupe abélien G, on dira que G *possède une* $\mathbb{Z}$*-base* s'il possède une base en tant que groupe abélien libre (ou encore en tant que $\mathbb{Z}$-module libre.)**

On note A le groupe abélien $\mathbb{Z}^n$ vu comme sous-groupe de l'espace vectoriel $V := \mathbb{Q}^n$. Soit $B \subset A$ un sous-groupe. On note W le sous-$\mathbb{Q}$-espace vectoriel de V engendré par B et par $i : A \hookrightarrow V$ l'injection naturelle de A dans V.

1) (3pts) **a)** (1pt) Montrer que des vecteurs $v_1, v_2, \ldots, v_m \in V$ sont linéairement indépendants sur $\mathbb{Q}$ si et seulement si ils le sont sur $\mathbb{Z}$.

Solution : *Puisque $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, une combinaison linéaires des vecteurs $v_{i\ ,1\leq i\leq m}$ à coefficients dans $\mathbb{Z}$ est, en particulier une combinaison linéaire à coefficients dans $\mathbb{Q}$ si bien que si la famille $v_{i\ ,1\leq i\leq m}$ est libre sur $\mathbb{Q}$ elle l'est sur $\mathbb{Z}$.*

Réciproquement, soit $q_{i\ ,1\leq i\leq m} \in \mathbb{Q}$ tel que $\sum_{i=1}^{m} q_i v_i = 0$. On écrit

$$\forall 1 \leq i \leq m,\ q_i = \frac{n_i}{d_i}\ ,\ n_i \in \mathbb{Z}\ ,\ d_i \in \mathbb{N}^* \text{ et } d := \prod_{i=1}^{m} d_i\ .$$

Alors

$$\forall 1 \leq i \leq m,\ dq_i \in \mathbb{Z} \text{ et } \sum_{i=1}^{m} dq_i v_i = 0\ .$$

Si l'on suppose la famille $v_{i\ ,1\leq i\leq m}$ libre sur $\mathbb{Z}$, il s'ensuit que $\forall 1 \leq i \leq m,\ dq_i = 0$, d'où $\forall 1 \leq i \leq m,\ q_i = 0$, si bien que la famille $v_{i\ ,1\leq i\leq m}$ est libre sur $\mathbb{Q}$.

b) (1pt) Montrer que tout sous-groupe de type fini $G \subset V$ est libre de rang $r \leq n$.

Solution : *On peut donner au moins deux preuves de ce résultat :*

i) Soit $S := \{g_1, \ldots, g_s\}$ une famille génératrice de G en tant que groupe abélien de type fini.
Choisissons une $\mathbb{Q}$-base $(v_1, \ldots, v_n)$ de V. Alors

$$\forall 1 \leq i \leq s,\ \exists g_{i,j\ ,1\ \leq\ j\ \leq\ n} \in \mathbb{Q}, \quad \text{tel que } g_i = \sum_{j=1}^{n} g_{i,j} v_j\ .$$

Notons alors

$$\forall 1 \leq i \leq s,\ \forall 1 \leq j \leq n,\ g_{i,j} = \frac{n_{i,j}}{d_{i,j}}\ ,\ n_{i,j} \in \mathbb{Z}\ ,\ d_{i,j} \in \mathbb{N}^*\ .$$

Posons encore

$$\forall 1 \leq j \leq n,\ w_j := \frac{1}{\prod_{i=1}^{s} d_{i,j}} v_j\ .$$

La famille $w_{j\ ,1\leq j\leq n}$ reste évidemment une $\mathbb{Q}$-base de V et par conséquent, en vertu du point précédent, une famille $\mathbb{Z}$-libre. De plus

$$\forall 1 \leq i \leq s,\ \exists h_{i,j\ ,1\ \leq\ j\ \leq\ n} \in \mathbb{Z}, \quad \text{tels que } g_i = \sum_{j=1}^{n} h_{i,j} w_j\ .$$

Le groupe G est donc un sous-groupe du groupe abélien libre engendré par les $w_{j\ ,1\leq j\leq n}$. Ce dernier étant de rang n, G est de rang $r \leq n$, en vertu du théorème II.4.6.

ii) Un élément non nul $x \in G$ reste non nul dans V si bien que $\{x\}$ est une famille $\mathbb{Q}$-libre de V. Elle est donc en particulier $\mathbb{Z}$-libre d'après le point précédent, si bien que

$$\forall a \in \mathbb{Z},\ a \cdot x = 0 \Rightarrow a = 0\ .$$

On en déduit que G est donc un groupe abélien sans torsion (cf. II.5.2.vii).) Puisque G est de type fini par hypothèse, il résulte du théorème II.6.2 que G est un groupe abélien libre. Soit donc une $\mathbb{Z}$-base $v_{i\ ,1\leq i\leq r}$ de G. C'est aussi une famille $\mathbb{Q}$-libre, si bien que le sous-$\mathbb{Q}$-espace vectoriel $\mathrm{Vect}\big\{(v_1, \ldots, v_r)\big\}$ de V est de dimension r ce qui entraîne que $r \leq n$.

c) (1pt) Est-ce que V est un groupe abélien de type fini ? (On pourra considérer le cas $n = 1$.)

Solution : *Dans le cas $n = 1, V = \mathbb{Q}$. On observe d'abor que*

$$\forall (q_1 := \frac{n_1}{d_1}, q_2 := \frac{n_2}{d_2} \in \mathbb{Q} \times \mathbb{Q},\ d_2 q_1 - d_1 q_2 = 0$$

si bien qu'une famille $\mathbb{Z}$-libre de $\mathbb{Q}$ contient au plus un élément.

Puisque $\mathbb{Q}$ est sans $\mathbb{Z}$-torsion s'il était de type fini il serait libre (cf. II.6.2,) et par conséquent, d'après ce qui précède de rang 1.

C'est un résulta bien connu que $\mathbb{Q}$ n'a pas de famille $\mathbb{Z}$-génératrice à 1 élément si bien que $\mathbb{Q}$ n'est ni libre ni de type fini.

2) (0.5pts) Rappeler rapidement (en citant le théorème adéquat) pourquoi il existe $r \in \mathbb{N}, r \leq n$ tel que $B \cong \mathbb{Z}^r$.
Solution : *(cf. II.4.6.)*

3) (1pt) Supposons qu'il existe une $\mathbb{Z}$-base $(u_1, \cdots, u_r)$ de B qui puisse se compléter en une $\mathbb{Z}$-base $(u_1, \cdots, u_n)$ de A. Montrer alors que $B = A \cap W$.
Solution : *Puisque*

$$B \subset A \text{ et } B \subset W$$

on a toujours $B \subset A \cap W$.

Réciproquement pour tout $x \in A \cap W$, *il existe* $x_{k\ ,1\leq k\leq n} \in \mathbb{Z}$ *tel que* $x = \sum_{k=1}^{n} x_k u_k$. *Par ailleurs, puisque* W *est le* $\mathbb{Q}$*-espace vectoriel engendré par* B, *il existe*

$$b_{k\ ,1\leq k\leq s} \in B \text{ et } q_{k\ ,1\leq k\leq s} \in \mathbb{Q} \text{ tels que } x = \sum_{k=1}^{s} q_k b_k \,.$$

Puisque $u_{k\ ,1\leq k\leq r}$ *est une* $\mathbb{Z}$*-base de* B *chacun des* $b_{k\ ,1\leq k\leq s}$ *peut se décomposer sur cette base, si bien qu'en fait il existe*

$$y_{k\ ,1\leq k\leq r} \in \mathbb{Q} \, tq \; x = \sum_{k=1}^{r} y_r u_r \,.$$

Dans le $\mathbb{Q}$*-espace vectoriel* V, *on a donc les égalités*

$$\sum_{k=1}^{n} x_k u_k = x = \sum_{k=1}^{r} y_r u_r \,.$$

Or il résulte de la question 1), a) que $u_{k\ ,1\leq k\leq n}$ *est une famille* $\mathbb{Q}$*-libre, si bien qu'il découle des égalité ci-dessus que*

$$\forall 1 \leq k \leq n, \; x_k = y_k$$

ce qui assure en particulier que

$$\forall r+1 \leq k \leq n, \; x_k = 0 \text{ et } \forall 1 \leq k \leq r, \; y_k \in \mathbb{Z} \,.$$

Ceci assure finalement que $x \in B$.

4) (4.5pts) **Supposons réciproquement que** $B = A \cap W$. **On va montrer qu'alors (cf. f),)** B **possède une base qui se complète en une base de** A.
Soit $W' := V/W$ **l'espace vectoriel quotient de** V **par** W **et soit** $p : V \to W'$ **la surjection canonique.**

a) (0.5pts) Montrer que $p \circ i : A \to W'$ est un morphisme de groupes dont B est le noyau.
Solution : *L'application* p *est un morphisme de* $\mathbb{Q}$*-espaces vectoriels donc en particulier un morphisme de groupes. L'application* i *est par définition un morphisme de groupes il en est donc de même de* $p \circ i$.
Pour tout $x \in A$,

$$\begin{array}{rrcl} & p \circ i(x) & = & 0 \\ \Leftrightarrow & i(x) & \in & \operatorname{Ker} p \\ \Leftrightarrow & i(x) & \in & W \\ \Leftrightarrow & x & \in & A \cap W \\ \Leftrightarrow & x & \in & B \,. \end{array}$$

b) (0.5pts) En notant $q : A \to A/B$ la surjection canonique, montrer qu'il existe un unique morphisme de groupes injectif

$$j : A/B \hookrightarrow W' \text{ tel que } j \circ q = p \circ i \,.$$

Solution : *D'après le point précédent,, puisque* $\operatorname{Ker}(p \circ i) = B$, *il existe, en vertu de la proposition I.8.11, un unique morphisme de groupes injectif*

$$j : A/B \hookrightarrow W' \text{ tel que } j \circ q = p \circ i \,.$$

c) (0.5pts) Montrer que le groupe abélien quotient $C := A/B$ est libre de type fini de rang $\leq n$.
Solution : *Puisque* A *est de type fini,* A/B *l'est aussi. Or, puisque* j *est injectif, d'après la b),* A/B *est isomorphe à* $j(A/B)$ *qui est un sous-groupe de type fini du* $\mathbb{Q}$*-espace vectoriel* W' *lui-même de dimension finie comme quotient de* V.
Il résulte alors de question 1), b) que $C = A/B$ *est libre de type fini de rang* $\leq n$.

Soit $c_1, \ldots, c_s$ **une** $\mathbb{Z}$**-base de** C, $a_1, \ldots, a_s$ **des relèvements des** c_k **(c'est-à-dire que** $\forall 1 \leq k \leq s,\ q(a_k) = c_k$,**) dans** A, **et** $C' \subset A$ **le sous-groupe engendré par les** $a_{k\ ,1\leq k\leq s}$.

d) (1pt) Montrer que l'application quotient $q : A \to A/B = C$ se restreint en un isomorphisme de C' vers C.
Solution : *Il existe un unique morphisme de groupes*

$$\sigma : C \to A\ ,\ c_k \mapsto a_{k\ ,1\ \leq\ k\ \leq\ s}\ \textit{(cf. II.2.10 .)}$$

Puisque $\forall 1 \leq k \leq s,\ a_k \in C'$, σ *est en fait à valeurs dans* C'.
Comme

$$\forall 1 \leq k \leq s,\ q(\sigma(c_k)) = q(a_k) = c_k$$

et que $c_{k\ ,1\leq k\leq s}$ *est une base de* C,

$$q \circ \sigma = \mathrm{Id}_C\ .$$

Par ailleurs, puisque $c_{k\ ,1\leq k\leq s}$ *est une base de* C, $a_{k\ ,1\leq k\leq s}$ *est une famille libre de* A *est partant une base du sous module* C' *qu'elle engendre.*
De plus,

$$\forall 1 \leq k \leq s,\ \sigma(q(a_k)) = \sigma(c_k) = a_k\ ,$$

ce qui assure que

$$\sigma \circ q_{|C'} = \mathrm{Id}_{C'}\ .$$

Finalement $q_{|C'} : C' \cong C$ *est un isomorphisme d'inverse* σ.

e) (1pt) En déduire que $A \cong B \oplus C'$ et donc que A est isomorphe à $B \times C$.
Solution : *On a en fait montré (cf. d),) que la suite exacte*

$$0 \to B \longrightarrow A \xrightarrow{\ q\ } A/B \to 0$$

est scindée (cf. I.9.11.i),) ou encore que σ *est une section de* q. *Il résulte alors du théorème I.9.15, que*

$$A = \mathrm{Ker}\, q \oplus \mathrm{Im}\, \sigma = B \oplus C'\ .$$

Cependant, puisqu'on ne demandait pas explicitement en d) de construire une section pour q, *on peut prouver le résultat en s'en tenant au fait que* $q_{|C'} : C' \to C$ *est un isomorphisme. Cela revient en fait, peu ou prou, à refaire les construction de I.9.*
En effet, pour tout $x \in A$, *il existe* $x_{k\ ,1\leq k\leq s} \in \mathbb{Z}$ *tel que* $q(x) = \sum_{k=1}^{s} x_s c_s$. *Il s'ensuit que* $q\big(x - \sum_{k=1}^{s} x_s a_s\big) = 0$, *i.e.*

$$y = x - \sum_{k=1}^{s} x_s a_s \in \mathrm{Ker}\, q = B\ .$$

Posant $z := \sum_{k=1}^{s} x_s a_s$ *on a*

$$(y, z) \in B \times C' \text{ et } x = y + z \textit{ i.e. } A = B + C'\ .$$

Or :

$$\begin{aligned}
&\forall x \in B \cap C',\quad \exists x_{k\ ,1\leq k\leq s} \in \mathbb{Z},\ x = \sum_{k=1}^{s} x_k a_k \quad \text{et} \quad q(x) = 0 \\
\Rightarrow \quad & q\big(\sum_{k=1}^{s} x_k a_k\big) = 0 \\
\Rightarrow \quad & \sum_{k=1}^{s} x_k q(a_k) = 0 \\
\Rightarrow \quad & \sum_{k=1}^{s} x_k c_k = 0 \\
\Rightarrow \quad & \forall 1 \leq k \leq s,\ x_k = 0
\end{aligned}$$

puisque $c_{k\ ,1\leq k\leq s}$ *est une base de* C. *Il s'ensuit donc que* $x = 0$ *et donc que* $B \cap C' = \{0\}$ *et donc que*

$$A = B \oplus C'$$

qui est isomorphe à $B \times C$ *en vertu de d).*

f) (1pt) Montrer enfin qu'il existe une $\mathbb{Z}$-base de B qui se complète en une $\mathbb{Z}$-base de A.

Solution : *Le sous-groupe B étant libre de rang $r \leq n$ (cf. question 2),) il existe une $\mathbb{Z}$-base $b_{k\ ,1\leq k\leq r}$, de B.*

On rappelle que, puisque $\forall 1 \leq k \leq s,\ q(a_k) = c_k$ et $c_{k\ ,1\leq k\leq s}$ est une base de C, $a_{k\ ,1\leq k\leq s}$ est une famille libre de A, et partant une base du sous-groupe C' qu'elle engendre.

Puisque (cf. e),) $A = B \oplus C'$, la famille $(b_1, \ldots, b_r, a_1, \ldots, a_s)$ est une base de A.

5) (bonus) **Soit $b \neq 0$ un élément de A et B le sous-groupe qu'il engendre.**

Montrer que les conditions suivantes sont équivalentes :

i) Le sous-groupe B possède une $\mathbb{Z}$-base qui se complète en une $\mathbb{Z}$-base de A.

ii)
$$B = A \cap W\ .$$

iii)
$$\mathbf{Pgcd}\big(b_{k\ ,1\leq k\leq n}\big) = 1\ ,\ b = (b_1, \cdots, b_n)\ .$$

Solution : *i) $\Rightarrow$ ii) a été montré en question 3) tandis que ii) $\Rightarrow$ i) a été montré en question 4).*

Montrons donc :

*§) **(ii) $\Rightarrow$ iii))***

*Notons d le **Pgcd** des $b_{i\ ,1\leq i\leq n}$ et*
$$\forall 1 \leq i \leq n,\ bc_i = dc_i\ ,\ c_i \in \mathbb{Z}\ .$$

Il s'ensuit que
$$c := (c_1, \ldots, c_n) \in A\ .$$

Or
$$c = \frac{1}{d}b \in W$$

si bien que
$$c \in A \cap W = B\ .$$

Il existe donc $k \in \mathbb{Z}$ tel que $c = kb$; c'est-à-dire
$$\forall 1 \leq i \leq n,\ c_i = kb_i\ .$$

Or b étant non nul, il existe au moins $1 \leq i \leq n$ tel que $b_i \neq 0$. Il vient alors
$$b_i = dc_i = dkb_i \Rightarrow b_i(1 - dk) = 0$$

si bien que" d est inversible ce qui signifie exactement que les $b_{i\ ,1\leq i\leq n}$ sont premiers entre eux.

*¶) **(iii) $\Rightarrow$ ii))***

On a toujours $B \subset A \cap W$. Soit donc $x \in A \cap W$, il existe $q \in \mathbb{Q}$ tel que $x = qb$. On peut écrire $q = \frac{\delta}{\nu}$ avec ν et δ premiers entre eux. Or $x \in A$ entraîne que
$$\forall 1 \leq i \leq n,\ qb_i \in \mathbb{Z} \Rightarrow \frac{\nu}{\delta}b_i \in \mathbb{Z} \Rightarrow \delta | b_i\ .$$

Or le fait que $b_{i\ ,1\leq i\leq n}$ sont premiers entre eux, entraîne que δ est inversible i.e. $q \in \mathbb{Z}$ i.e. $x \in B$.

On peut remarquer que la notion de vecteur primitif (cf. cours C.1.3,) et ses conséquences permettrait de montrer immédiatement que iii) $\Rightarrow$ i).

Exercice C : (2points) **Considérons le diagramme commutatif de groupes abéliens à lignes exactes suivant :**

$$\begin{array}{ccccccccc} 0 & \to & N_1 & \xrightarrow{i_1} & A_1 & \xrightarrow{p_1} & Q_1 & \to & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \to & N_2 & \xrightarrow{i_2} & A_2 & \xrightarrow{p_2} & Q_2 & \to & 0 \end{array}$$

c'est-à-dire que pour $j = 1$ ou 2 :

- **— N_j, A_j et Q_j sont des groupes abéliens,**
- **— i_j est un morphisme de groupes injectif,**
- **— p_j est un morphisme de groupe surjectif,**
- **—**
$$\mathrm{Im}\, i_j = \mathrm{Ker}\, p_j\ ,$$
- **—**
$$g \circ i_1 = i_2 \circ f \text{ et } h \circ p_1 = p_2 \circ g\ .$$

1) (1pt) Montrer que si g est injectif, f l'est aussi ; si g est surjectif, h l'est aussi.

Solution :

i) Si g est injectif, $g \circ i_1$ l'est encore ; ce qui entraîne que $i_2 \circ f$ est injectif. C'est alors un résultat bien connu et qui vaut pour des applications, sans hypothèse qu'elles soient des morphismes, qu'alors f est injectif.

ii) Si g est surjectif, il en va de même de $p_2 \circ g$ et par conséquent de $h \circ p_1$. Comme ci-dessus, c'est un résultat ensembliste que cela entraîne que h est surjectif.

2) (1pt) Montrer que si f et h sont injectifs il en est de même de g.

Solution :

$$\begin{array}{lrcl}
\forall x \in A_1, & g(x) & = & 0 \\
\Rightarrow & p_2(g(x)) & = & 0 \\
\Rightarrow & h(p_1(x)) & = & 0 \\
\Rightarrow & p_1(x) & = & 0 \\
\Rightarrow & x & \in & \operatorname{Ker} p_1 \\
\Rightarrow & x & \in & \operatorname{Im} i_1 \\
\Rightarrow & \exists y \in N_1,\ x & = & i_1(y) \\
\Rightarrow & i_2(g(y)) = f(i_1(y)) & = & f(x) = 0 \\
\Rightarrow & g(y) & = & 0 \\
\Rightarrow & y & = & 0 \\
\Rightarrow & x & = & i_1(y) = 0\ .
\end{array}$$

3) (1pt) Montrer que si f et h sont surjectifs il en est de même de g.

Solution : *Pour tout $y \in A_2$, il existe $x \in Q_1$ tel que $h(x) = p_2(y)$ puisque h est surjectif. Il existe alors $z \in A_1$ tel que $p_1(z) = x$, puisque p_1 est surjectif. On a alors :*

$$\begin{array}{rcl}
p_2(y - g(z) & = & p_2(y) - p_2(g(z)) \\
& = & h(x) - h(p_1(z)) \\
& = & 0\ .
\end{array}$$

Puisque la ligne du bas est exacte, il existe $w \in N_2$ tel que

$$y - g(z) = i_2(w)\ .$$

Puisque f est surjectif, il existe $t \in N_1$ tel que $w = f(t)$. Il s'ensuit que :

$$\begin{array}{rcl}
y & = & g(z) + i_2(w) \\
& = & g(z) + i_2(f(t)) \\
& = & g(z) + g(i_1(t)) \\
& = & g(z + i_1(t))\ .
\end{array}$$

Exercice D : (5points) **Soit A un anneau principal. Pour tout $x \in A$, on notera xA l'idéal principal engendré par x, A/xA l'anneau quotient et $\pi_x : A \to A/xA$ la surjection canonique.**

Soient

$$b \in A \setminus \{0\}\ ,\ B := A/bA \text{ et } q : B \to C$$

un morphisme d'anneaux surjectif, dont on note $D := \operatorname{Ker} q$ le noyau.

1) (1pt) Montrer qu'il existe $c \in A \setminus \{0\}$ et un isomorphisme d'anneaux $\phi : A/cA \to C$ tels que

$$\phi \circ \pi_c = q \circ \pi_b \text{ et } c|b\ .$$

Solution : *La composée $q \circ \pi_b : A \to C$ est un morphisme d'aneaux surjectif. Son noyau est un idéal de A. Puisque A est principal, il existe $c \in A$ tel que $\operatorname{Ker}(q \circ \pi_b) = cA$.*

Or

$$bA = \operatorname{Ker} \pi_b \subset \operatorname{Ker}(q \circ \pi_b)$$

si bien que $bA \subset cA$ ce qui équivaut à

$$c|b\ .$$

Il résulte enfin de la proposition I.8.11 que $q \circ \pi_b$ se factorise à travers A/cA i.e. il existe un isomorphisme $\phi : A/cA \cong C$ tel que le diagramme suivant est commutatif :

$$\begin{array}{ccc}
A & \xrightarrow{\pi_b} & B \\
{\scriptstyle \pi_c}\downarrow & & \downarrow{\scriptstyle q} \\
A/cA & \xrightarrow{\phi} & C\ .
\end{array}$$

1

2) (1pt) Montrer que $\pi_b^{-1}(D)$ est un idéal de A, le déterminer et justifier que

$$D \;=\; \pi_b[\pi_b^{-1}(D)]\;.$$

Solution : *L'image inverse d'un idéal par un morphisme d'anneaux est un idéal.*
Par ailleurs

$$\pi_b^{-1}(D) \;=\; \pi_b^{-1}(\operatorname{Ker} q) \;=\; \operatorname{Ker}(q\circ\pi_b) \;=\; \operatorname{Ker}(\phi\circ\pi_c) \;=\; \operatorname{Ker}\pi_c \;=\; cA\;.$$ *(cf. question 1), 1 .)*

Enfin puisque π_b est un morphisme surjectif,

$$D \;=\; \pi_b[\pi_b^{-1}(D)]\;.$$

3) (1pt) En notant $\gamma \;:\; A \;\to\; A\;,\; x \;\mapsto\; cx$, montrer que $\pi_b \;\circ\; \gamma$ est un morphisme de groupes d'image D.
Solution : *Découle presqu'immédiatement de question 2).*

4) (1pt) En étudiant le noyau de $\pi_b \;\circ\; \gamma$ montrer qu'il existe $d \;\in\; A$ tel que $b \;=\; cd$ et un isomorphisme de groupes

$$\delta \;:\; A/dA \;\cong\; D \text{ tel que } \delta\circ\pi_d \;=\; \pi_b\circ\gamma\;.$$

Solution :

$$\begin{array}{lrcl}
\forall x\in A, & \pi_b[\gamma(x)] & = & 0\\
\Leftrightarrow & \gamma(x) & \in & \operatorname{Ker}\pi_b\\
\Leftrightarrow & cx & \in & bA\\
\Leftrightarrow & \exists y\;\in\;A,\; cx & = & by\;.
\end{array}$$

Comme (cf. question 1), $c|b$, *posons* $b \;=\; dc$. *Il s'ensuit que :*

$$\begin{array}{lrcl}
\forall x\in A, & x & \in & \operatorname{Ker}(\pi_b\circ\gamma)\\
\Leftrightarrow & \exists y\;\in\;A,\; cx & = & by\\
\Leftrightarrow & cx & = & cdy\\
\Leftrightarrow & x & = & dy\;,
\end{array}$$

la dernière équivalence résultant du fait que A est un anneau intègre.
On a donc montré que $\operatorname{Ker}(\pi_b\circ\gamma) \;=\; dA$ *ce qui permet de factoriser (puisque $\pi_b \;\circ\; \gamma$ est surjectif (cf. question 3),)) $\pi_b \;\circ\; \gamma$ en un isomorphisme $\delta \;:\; A/dA \;\cong\; D$ i.e. le diagramme suivant est commutatif :*

$$\begin{array}{ccc}
A & \xrightarrow{\;\gamma\;} & A\\
{\scriptstyle\pi_d}\downarrow & & \downarrow{\scriptstyle\pi_b}\\
A/dA & \xrightarrow{\;\delta\;} & D\;.
\end{array}$$ *1*

5) (1pt) **On suppose désormais que c et d sont premiers entre eux.**

a) (0.5pts) Rappeler pourquoi il existe

$$(u,v) \;\in\; A\times A\;,\; cu+dv \;=\; 1\;.$$

Solution : *Théorème de* BÉZOUT *(cf. I.13.2.1.)*

b) (2pts) **Pour tout $\alpha \;\in\; C$, soit $x \;\in\; A$ tel que**

$$\alpha \;=\; q[\pi_b(x)] \;=\; \phi[\pi_c(x)]\;.$$

Posons alors $s(\alpha) \;:=\; \pi_b(dvx)$.
Montrer que $s(\alpha)$ est bien définie (indépendamment du choix de x,)
Solution : *Pour tout $\alpha \;\in\; C$, soit $(x,y) \;\in\; (q\circ\pi_b^{-1}(\{\alpha\})\times(q\circ\pi_b^{-1}(\{\alpha\})$. Alors :*

$$\begin{array}{lrcl}
 & q[\pi_b(x-y)] & = & 0\\
\Leftrightarrow & \phi[\pi_c(x-y)] & = & 0\\
\Leftrightarrow & \pi_c(x-y) & = & 0\\
\Leftrightarrow \exists z\;\in\;A,\; x-y & = & cz & \\
\Rightarrow & \pi_b[dv(x-y)] & = & \pi_b(cdvz)\\
\Rightarrow \pi_b(dvx)-\pi_b(dvy) & = & \pi_b(bvz) & \\
\Rightarrow & \pi_b(dvx)-\pi_b(dvy) & = & 0\\
\Rightarrow & \pi_b(dvx) & = & \pi_b(dvy)
\end{array}$$

ce qui assure que l'application $s \;:\; B \;\to\; C$ est bien définie.
et qu'ainsi défini

i) $s : C \to B$ est un morphisme de groupes ;

Solution : *Pour tout* $(\alpha, \beta) \in C \times C$, *soit* $(x, y) \in (q \circ \pi_b)^{-1}(\{\alpha\}) \times (q \circ \pi_b)^{-1}(\{\beta\})$. *Alors, puisque* $q \circ \pi_b$ *est un morphisme (au moins de groupes,)* $(x, y) \in (q \circ \pi_b)^{-1}(\{\alpha + \beta\})$. *Il s'ensuit que :*

$$\begin{aligned} s(\alpha+\beta) &= \pi_b[dv(x+y)] \\ &= \pi_b(dvx + dvy) \\ &= \pi_b(dvx) + \pi_b(dvy) \\ &= s(\alpha) + s(\beta) \end{aligned}$$

ce qui assure que s *est un morphisme de groupes.*

ii)

$$q \circ s = \mathrm{Id}_C ;$$

Solution : *POur tout* $\alpha \in C$, *soit* $x \in (q \circ \pi_b)^{-1}(\{\alpha\})$. *Puisque* $cu + dv = 1$, $x = cux + dvx$. *il s'ensuit que :*

$$\begin{aligned} q[s(\alpha)] &= q[\pi_b(dvx)] \\ &= q[\pi_b(x - cux)] \\ &= q[\pi_b(x)] - q[\pi_b(cux)] \\ &= \alpha q[\pi_b[\gamma(ux)]] \\ &= \alpha - q[\delta[\pi_d(ux)]] \\ &= \alpha \end{aligned}$$

puisque δ *(cf. question 4), 1,) est à valeurs dans* $D = \mathrm{Ker}\, q$.

iii)

$$\forall \alpha \in C,\ \forall a \in A,\ s\big[q[\pi_b(a)]\alpha\big] = s\big[\phi[\pi_c(a)]\alpha\big] = \pi_b(a)s(\alpha) .$$

Solution :

$$\begin{aligned} \forall \alpha \in C,\ \forall a \in A,\ \forall x \in (q \circ \pi_b)^{-1}(\{\alpha\}), \quad s\big[q[\pi_b(a)]\alpha\big] &= s\big[\phi[\pi_c(a)]\alpha\big] \\ &= s\big[q[\pi_b(a)]q[\pi_b(x)]\big] \\ &= s\big[q[\pi_b(ax)]\big] \\ &= \pi_b(dvax) \\ &= \pi_b(a)\pi_b(dvx) \\ &= \pi_b(a)s(\alpha) . \end{aligned}$$

On a en fait montré ici que s *est non seulement un morphisme de groupes mais encore un morphisme de* A*-modules pour les structures naturelles sur* B *et* C *i.e. celles déduites de leur structure de* A*-algèbre. (cf. cours A.2.1,)*

6) (bonus) Montrer réciproquement que s'il existe une application $s : C \to B$ vérifiant les points i) à iii) de la question 5), b), c et d sont premiers entre eux.

Solution : *Puisque* q *est un morphisme d'anneaux,* $q(1_B) = 1_C$. *Par ailleurs, puisque* $q \circ s = \mathrm{Id}_C$,

$$\begin{aligned} & q[s(1_C)] = 1_C \\ \Rightarrow \quad & q[s(1_C)] = q(1_B) \\ \Rightarrow \quad & q[1_B - s(1_C)] = 0 . \end{aligned}$$

Il existe donc $\alpha \in D$ *tel que* $1_B - s(1_C) = \alpha$. *Soit*

$$(x, y) \in A \times A \text{ tel que } s(1_C) = \pi_b(x) \text{ et } \pi_b[\gamma(y)] = \delta[\pi_d(y)] = \alpha .$$

On a alors

$$\begin{aligned} \pi_b[1_A - x - \gamma(y)] &= 1_B - \pi_b(x) - \pi_b[\gamma(y)] \\ &= 1_B - (1_B - s(1_C)) - \alpha \\ &= 0 . \end{aligned}$$

Il existe donc $z \in A$ *tel que*

$$1_A - x - cy - bz = 0 . \qquad 1$$

Enfin on a :

$$\begin{aligned}\delta[\pi_d(x)] &= \pi_b[\gamma(x)]\\ &= \pi_b(cx)\\ &= \pi_b(c)\pi_b(x)\\ &= \pi_b(c)s(1_C)\\ &= s\big[\phi[\pi_c(c)]1_C\big]\\ &= 0\ .\end{aligned}$$

Or δ est un isomorphisme (cf. question 4),) si bien que $\pi_d(x) = 0$, c'est-à-dire qu'il existe $w \in A$ tel que $x = dw$. L'égalité 1 devient alors

$$1_A = dw + cy + bz = c(y + dz) + dw = cy + d(cz + w)$$

ce qui prouve, grâce au théorème de BÉZOUT *(cf. I.13.2.1,) que c et d sont premiers entre eux.*

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Examen du du 12 juin 2020
Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Exercice A : **1)** Parmi les groupes suivants, lesquels sont isomorphes (vous devez justifier votre réponse) :

$$\begin{aligned} G_1 =& \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z} \\ G_2 =& \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ G_3 =& \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \end{aligned}$$

Lesquels sont cycliques ?

2) Déterminer les classes d'isomorphisme de groupes abéliens de cardinal 441.

3) On rappelle que deux matrices A et $B \in \mathcal{M}_n(\mathbb{Q})$ **sont *semblables* ou *conjuguées* s'il existe une matrice**

$$P \in \mathrm{GL}_n(\mathbb{Q}) \text{ telle que } B = P^{-1}AP\,.$$

La classe de *similitude* ou de *conjugaison* de A **est alors l'ensemble des matrices semblables ou conjuguées à** A.

Déterminer les classes de conjugaison de matrices $A \in \mathcal{M}_4(\mathbb{Q})$ dont le polynôme caractéristique $P_{\mathrm{car}\,A}$ est

$$P_{\mathrm{car}\,A} = (X^2 - 5X + 6)^2 \in \mathbb{Q}[X]\,.$$

4) Soient p **et** q **deux nombres premiers distincts, (resp. deux polynômes irréductibles distincts dans** $\mathbb{Q}[X]$.**)**

a) Déterminer le nombre de classes d'isomorphismes de groupes abéliens de cardinal p^2q^2 (resp. de classes de similitude de matrices $A \in \mathcal{M}_{\deg(p)+\deg(q)}(\mathbb{Q})$ de polynôme caractéristique $P_{\mathrm{car}\,A} = p^2q^2$.)

b) Même question pour les groupes abéliens de cardinal p^4q^3 (resp. les matrices de polynôme caractéristique p^4q^3.)

Exercice B : **On considère dans** $\mathbb{Z}^4$ **le sous-ensemble** G **suivant :**

$$G := \{(x,y,z,t) \in \mathbb{Z}^4 \,;\, x + 2y + 3z = 0 \text{ et } 2y + 5t = 0\}\,.$$

Montrer que G est un groupe libre de rang 2. Déterminer $\mathbb{Z}^4/G$.

Exercice C : Soit $p \in \mathbb{N}$ un nombre premier, $k := \mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, *)$ le corps à p éléments et $A := k[X]$ l'anneau des polynômes à une indéterminée à coefficients dans k.

Pour tout $n \in \mathbb{N}$, on note $U(n)$ (resp. $I(n)$) l'ensemble des éléments unitaires (resp. unitaires irréductibles) de degré n de A et $u(n)$ (resp. $i(n)$) le cardinal de $U(n)$ (resp. $I(n)$.)

1) **a)** Calculer $u(0)$, $i(0)$, $u(1)$ et $i(1)$.

b) Calculer $u(2)$ et montrer que $i(2) = \dfrac{p(p-1)}{2}$.

Indication : *On pourra remarquer que $I(2)$ est le complémentaire dans $U(2)$ des polynômes qui se factorisent.*

c) Calculer $u(3)$ et $i(3)$.

2) **a)** Déterminer le nombre de classes de similitude dans $\mathcal{M}_2(k)$. Caractériser celle qui correspondent à des endomorphismes cycliques.

b) Même question dans $\mathcal{M}_3(k)$.

Exercice D : (Puissances d'une matrice nilpotente)

Soit A une matrice à coefficients dans un corps $\mathbb{K}$ dont les invariants de similitude sont

$$(X^5, X^4, X^4, X^3, X^3, X^3, X^2, X, X, X)\ .$$

1) Quels sont les invariants de similitude de A^2 .

2) Quels sont les invariants de similitude de A^3 ?

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Corrigé de l'examen du 12 juin 2020

Exercice A : **1)** Parmi les groupes suivants, lesquels sont isomorphes (vous devez justifier votre réponse) :

$$G_1 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z}$$
$$G_2 = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$
$$G_3 = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

Lesquels sont cycliques ?

Solution : *Même si dans certains cas simples d'autres arguments peuvent être utilisés, (nombre d'éléments, ordre des éléments . . . ,) le corollaire II.10.7 du cours apporte toujours une réponse systématique à la question des classes d'isomorphismes de groupes abéliens. Cependant, pour pouvoir lutiliser, il faut connaître les facteurs invariants du groupe et pour cela déterminer sa décomposition canonique (cf. cours II.10.5.i).)*

G_1 *Ainsi le groupe* $G_1 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z}$ *n'est pas décomposé sous sa forme canonique, puisque*

$$9 \not| 49 \text{ et } 49 \not| 9 .$$

Cependant le théorème chinois des restes assure que

$$G_1 \cong \mathbb{Z}/441\mathbb{Z}$$

qui est une décomposition canonique de paramètres $r = 1$ *et* $d_1 = 441$. *Ce groupe est cyclique.*

G_2 *De même* $G_2 = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ *n'est pas donné non plus sous sa forme canonique, laquelle est, en vertu du théorème chinois des restes*

$$G_2 \cong \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z} \text{ de paramètres } r = 2 , \ d_1 = 21 \text{ et } d_2 = 21 .$$

Ce groupe n'est pas cyclique.

G_3 *Par les mêmes arguments que ci-dessus,*

$$G_3 \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/63\mathbb{Z} \text{ de paramètres } r = 2 , \ d_1 = 63 \text{ et } d_2 = 7$$

qui n'est pas non plus cycliques.

Aucun des groupes G_1, G_2, G_3 *ne sont isomorphes entre eux puisque leurs séquences de paramètres sont toutes deux à deux distinctes.*

2) Déterminer les classes d'isomorphisme de groupes abéliens de cardinal 441.

Solution : *Puisque* $441 = 3^2 * 7^2$, *on a déjà (cf. question 1),) identifié les classes d'isomorphismes des groupes*

$$G_1 = \mathbb{Z}/441\mathbb{Z} , \ G_2 = \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z} \text{ et } G_3 = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/63\mathbb{Z} .$$

La seule autre classe qu'on n'a pas déterminée est celle de

$$G_4 := \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/147\mathbb{Z} .$$

3) On rappelle que deux matrices $A \text{ et } B \in \mathcal{M}_n(\mathbb{Q})$ **sont *semblables* ou *conjuguées* s'il existe une matrice**

$$P \in \mathrm{GL}_n(\mathbb{Q}) \text{ telle que } B = P^{-1}AP .$$

La classe de *similitude* ou de *conjugaison* de A **est alors l'ensemble des matrices semblables ou conjuguées à** A.

Déterminer les classes de conjugaison de matrices $A \in \mathcal{M}_4(\mathbb{Q})$ dont le polynôme caractéristique $P_{\text{car } A}$ est

$$P_{\text{car } A} = (X^2 - 5X + 6)^2 \in \mathbb{Q}[X] .$$

Solution : *On sait (cf. cours IV.11.8,) que deux matrices* $A \text{ et } B \in \mathcal{M}_4(\mathbb{Q})$ *sont semblables si et seulement si elles ont les mêmes invariants de similitude. Déterminer les classes de similitude équivaut donc à déterminer les invariants de similitude*

μ_i ,$1\leq i\leq r$ $\in$ $\mathbb{Q}[X]$ *correspondant à des matrices dont le polynôme caractéristique est* (X^2-5X+6). *Or on sait qu'alors (cf. cours IV.11.11,) que*

$$P_{\text{min } A} \;=\; \mu_1 \;,\; P_{\text{car } A} \;=\; \prod_{i=1}^{r} \mu_i \text{ et } \forall 1\leq i\leq r-1,\; \mu_{i+1}|\mu_i \;.$$

Pour déterminer les suites μ_i ,$1\leq i\leq r$ *répondant aux conditions ci(-dessus, il est, bien entendu, beaucoup plus facile de raisonner sur des polynômes factorisés en produit d'irréductibles. Ainsi*

$$P_{\text{car}\,.} \;=\; (X^2-5X+6)^2 \;=\; [(X-2)(X-3)]^2 \;=\; (X-2)^2(X-3)^2 \;.$$

Les suites d'invatirant d'invariants de similitude qu'on peut alors obtenir sonts :

$$\begin{array}{c|c} \mu_1 & \mu_2 \\ (X-2)^2(X-3)^2 & 1 \\ (X-2)(X-3) & (X-2)(X-3) \\ (X-2)^2(X-3) & (X-3) \\ (X-2)(X-3)^2 & (X-2)\;. \end{array}$$

4) Soient p et q deux nombres premiers distincts, (resp. deux polynômes irréductibles distincts dans $\mathbb{Q}[X]$.)

a) Déterminer le nombre de classes d'isomorphismes de groupes abéliens de cardinal p^2q^2 (resp. de classes de similitude de matrices $A \in \mathcal{M}_{\deg(p)+\deg(q)}(\mathbb{Q})$ de polynôme caractéristique $P_{\text{car } A} = p^2q^2$.)

Solution : *On a en fait répondu à cette question (cf. question 1) , question 3).) En effet les seuls arguments qu'on a utilisés, en dehors des théorèmes de structure (cf. cours II.10.5 , IV.11.5,) sont le fait que* 3 *et* 7 *(resp.* $X-2$ *et* $X-3$*) sont premiers entre eux. Ainsi ici on trouvera* 4 *classes d'isomorphismes de groupes abéliens (resp. de similitude de matrices) correspondant aux suites de facteurs invariants*

$$(P^2q^2)\;,\; (p^2q,q)\;,\; (pq^2,p)\;,\; (pq,pq)\;.$$

b) Même question pour les groupes abéliens de cardinal p^4q^3 (resp. les matrices de polynôme caractéristique p^4q^3.)

Solution : *Il s'agit de déterminer des suites* μ_i ,$1\leq i\leq r$ $\in$ $\mathbb{Z}$(*resp.* $\mathbb{Q}[X]$) *telles que :*

—
$$\forall 1\leq i\leq r,\; \mu_i \;=\; p^{\alpha_i}q^{\beta_i}\;;$$

—
$$\forall 1\leq i\leq r-1,\; \alpha_{i+1} \;\leq\; \alpha_i \text{ et } \beta_{i+1} \;\leq\; \beta_i\;;$$

—
$$\sum_{i=1}^{r}\alpha_i \;=\; 4 \text{ et } \sum_{i=1}^{r}\beta_i \;=\; 3\;.$$

Il s'ensuit qu'une telle suite est entièrement déterminée par un couple formé d'une partition de 4 *et une partition de* 3. *Les premières*

$$(4)\;,\; (3,1)\;,\; (2,2)\;,\; (2,1,1)\;,\; (1,1,1,1)$$

sont au nombre de 5 *tandis que les seconde*

$$(3)\;,\; (2,1)\;,\; (1,1,1)$$

sont au nombre de 3.

Il y a donc 15 *classes d'isomorphismes de groupes abéliens de cardinal (resp. classes de similitude de polynome caractéristique)* p^4q^3.

Exercice B : On considère dans $\mathbb{Z}^4$ le sous-ensemble G suivant :

$$G \;:=\; \{(x,y,z,t) \;\in\; \mathbb{Z}^4\;;\; x+2y+3z \;=\; 0 \text{ et } 2y+5t \;=\; 0\}\;.$$

Montrer que G est un groupe libre de rang 2. Déterminer $\mathbb{Z}^4/G$.

Solution : *Voici une solution théorique. Considèrons l'application*

$$\begin{array}{rccc} f: & \mathbb{Z}^4 & \longrightarrow & \mathbb{Z}^2 \\ & (x,y,z,t) & \longmapsto & (x+2y+3z, 2y+5t) \end{array}$$

On a

$$\text{Ker } f \;\subset\; \mathbb{Z}^4 \text{ et } \text{Im } f \;\subset\; \mathbb{Z}^2 \;:$$

ce sont des sous-groupes de groupes libres de type fini, donc ils sont libres de type fini. Notons $f_{\mathbb{Q}} : \mathbb{Q}^4 \to \mathbb{Q}^2$ *l'application linéaire telle que* $f_{\mathbb{Q}_{|\mathbb{Z}^4}} = f$ *: on a*

$$\mathrm{rg}(\mathrm{Ker}\, f) = \dim_{\mathbb{Q}} \mathrm{Ker}\, f_{\mathbb{Q}}\ \mathrm{rg}(\mathrm{Im}\, f) = \dim_{\mathbb{Q}} \mathrm{Im}\, f_{\mathbb{Q}} = 2,$$

Donc

$$G \cong \mathrm{Ker}\, f \cong \mathbb{Z}^2 \text{ et } \mathbb{Z}^4/G \cong \mathrm{Im}\, f \cong \mathbb{Z}^2\ .$$

Et voici une solution moins théorique.

On résoud en faisant attention de ne pas diviser par des entiers non inversibles : La deuxième équation implique que 5 *divise* y *:* $y = 5u$, $t = -2u$ *avec* $u \in \mathbb{Z}$. *On pose pour faire joli* $z = v$. *Le système dans* $\mathbb{Z}$ *est donc équivalent à*

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = u \begin{pmatrix} -5 \\ 5 \\ 0 \\ -2 \end{pmatrix} + v \begin{pmatrix} -3 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Autrement dit, G *est un groupe libre de rang 2 et de base* $(-5, 5, 0, -2)$ *et* $(-3, 0, 1, 0)$.

Peut-on compléter en une base de $\mathbb{Z}^4$ *? On va d'abord le faire en essayant ! Il s'agit de trouver une matrice de déterminant* ± 1 *de la forme* $\begin{pmatrix} -5 & 5 & 0 & -2 \\ -3 & 0 & 1 & 0 \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$. *On se ramène à trouver une matrice de la forme* $\begin{pmatrix} -5 & 5 & -2 \\ * & * & * \\ * & * & * \end{pmatrix}$. *Cela est possible car les entiers* $(-5, 5, 2)$ *sont premiers entre eux : par exemple,* $\begin{pmatrix} -5 & 5 & -2 \\ * & -2 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ *(*$5 - 2 \times 2 = 1$ *par* BÉZOUT *!). Ainsi, les matrices* $\begin{pmatrix} -5 & 5 & 0 & -2 \\ -3 & 0 & 1 & 0 \\ * & -2 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ *conviennent. Les éléments* $f_1 = (-5, 5, 0, -2)$, $f_2 = (-3, 0, 1, 0)$, $f_3 = (0, -2, 0, 1)$ *et* $f_4 = (1, 0, 0, 0)$ *forment une base de* $\mathbb{Z}^4$. *Le quotient* $\mathbb{Z}^4/G$ *est donc libre de rang 2 : soit* φ *le morphisme de groupes de* $\mathbb{Z}^4$ *dans* $\mathbb{Z}^2$ *tel que* $\varphi(f_1) = 0$, $\varphi(f_2) = 0$, $\varphi(f_3) = (1, 0)$, $\varphi(f_4) = (0, 1)$ *est surjectif de noyau* G. *Il se factorise donc en un isomorphisme de* $\mathbb{Z}^4/G$ *sur* $\mathbb{Z}^2$.

Exercice C : Soit $p \in \mathbb{N}$ **un nombre premier,** $k := \mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, *)$ **le corps à** p **éléments et** $A := k[X]$ **l'anneau des polynômes à une indéterminée à coefficients dans** k.

Pour tout $n \in \mathbb{N}$, **on note** $U(n)$ **(resp.** $I(n)$**) l'ensemble des éléments unitaires (resp. unitaires irréductibles) de degré** n **de** A **et** $u(n)$ **(resp.** $i(n)$**) le cardinal de** $U(n)$ **(resp.** $I(n)$**.)**

1) a) Calculer $u(0)$, $i(0)$, $u(1)$ et $i(1)$.

Solution : *On a* $U(0) = \{1\}$ *d'où* $u(0) = 1$, $I(0) = \{1\}$ *d'où* $i(0) = 1$.

Les polynômes unitaire de degré 1 *sont de la forme* $X + a$,$a \in \mathbb{F}_p$ *et ils sont tous irréductibles d'où*

$$u(1) = i(1) = p\ .$$

b) Calculer $u(2)$ et montrer que $i(2) = \dfrac{p(p-1)}{2}$.

Indication : *On pourra remarquer que* $I(2)$ *est le complémentaire dans* $U(2)$ *des polynômes qui se factorisent.*

Solution : *Un polynôme unitaire de degré* 2 *s'écrit*

$$X^2 + aX + b \text{ avec } (a, b) \in \mathbb{F}_p \times \mathbb{F}_p\ .$$

Il s'ensuit que

$$u(2) = \#(U(2)) = p^2\ .$$

Pour tout $P \in U(2)$, $P \notin I(2)$,

$$P = (X + a)(X + b)\ ,_{(a,b) \in \mathbb{F}_p \times \mathbb{F}_p}\ .$$

L'ensemble des polynômes de la forme

$$(X + a)(X + b) \text{ avec } a \neq b$$

est en bijection avec les parties à 2 *éléments de* $I(1)$ *et il y a donc* $\binom{p}{2}$ *tels éléments. Il y a en outre* p *polynômes de la forme* $(X + a)^2$. *Il s'ensuit que*

$$i(2) = u(2) - \binom{p}{2} - p = p^2 - \frac{p(p-1)}{2} - p = \frac{1}{2}(2p^2 - p^2 + p - 2p) = \frac{p(p-1)}{2}\ .$$

c) Calculer $u(3)$ et $i(3)$.

Solution : *Un polynomes unitaire de degré* 3 *s'écrit* $X^3 + aX^2 + bX + c$ *d'où il vient, pour les même raisons que ci-dessus que*

$$u(3) \;=\; \#(U(3)) \;=\; p^3 \;.$$

Introduisons les sous-ensembles suivants de $U(3) \setminus I(3)$ *qui en forment en fait une partition :*

$$\begin{array}{rcl} U_{(2,1)}(3) & := & \{P \in U(3)\,;\, \exists (Q,R) \in I(2)\times I(1),\; P = QR\} \\ U_{(1,1,1)}(3) & := & \{P \in U(3)\,;\, \exists (Q,R,T) \in I(1)\times I(1)\times I(1),\; Q\neq R\,,\; Q\neq T\,,\; R\neq T\,,\; P = QRT\} \\ U_{(2)}(3) & := & \{P \in U(3)\,;\, \exists (Q,R) \in I(1)\times I(1),\; Q\neq R\,,\; P = QR\} \\ U_{(3)}(3) & := & \{P \in U(3)\,;\, \exists Q \in I(1),\; P = Q^3\}\,. \end{array} \qquad (1)$$

On a alors :

$$\begin{array}{rcccl} u_{(2,1)}(3) & := & \#\big(U_{(2,1)}(3)\big) & = & i(1)i(2) \\ u_{(1,1,1)}(3) & := & \#\big(U_{(1,1,1)}(3)\big) & = & \binom{i(1)}{3} \\ u_{(2)}(3) & := & \#\big(U_{(2)}(3)\big) & = & \binom{i(1)}{2} \\ u_{(3)}(3) & := & \#\big(U_{(3)}(3)\big) & = & i(1)\,. \end{array} \qquad (2)$$

Comme :

$$U(3) \;=\; I(3) \cup U_{(2,1)}(3) \cup U_{(1,1,1)}(3) \cup U_{(2)}(3) \cup U_{(3)}(3) \;\; \textit{les unions étant disjointes,} \qquad (3)$$

Il vient (cf. b) :)

$$\begin{array}{rcl} i(3) & = & u(3) - u_{(2,1)}(3) - u_{(1,1,1)}(3) - u_{(2)}(3) - u_{(3)}(3) \\ & = & u(3) - i(1)i(2) - \binom{i(1)}{3} - \binom{i(1)}{2} - i(1) \\ & = & p^3 - p\frac{p(p-1)}{2} - \frac{p(p-1)(p-2)}{6} - \frac{p(p-1)}{2} - p \\ & = & p^3 - \frac{1}{6}\left(3p^2(p-1) + p(p-1)(p-2) + 3p(p-1) + 6p\right) \\ & = & p^3 - \frac{1}{6}\left(3p^3 - 3p^2 + p^3 - 3p^2 + 2p + 3p^2 - 3p + 6p\right) \\ & = & p^3 - \frac{1}{6}\left(4p^3 - 3p^2 + 5p\right) \\ & = & \frac{1}{6}\left(2p^3 + 3p^2 - 5p\right)\;. \end{array} \qquad (4)$$

2) Remarque 2).1 Notons S l'ensemble des suites finies

$$\mu_{i\,,1\leq i\leq r} \in A \;\text{ telles que }\; \forall 1\leq i\leq r-1,\; \mu_{i+1}|\mu_i\;,\; \forall 1\leq i\leq r,\; \mu_i \notin A^\times\;. \qquad (1)$$

Notons :

$$\begin{array}{rcccl} \pi_n : & \mathcal{M}_n(k) & \longrightarrow & U(n)\subset A \\ & M & \longmapsto & P_{\text{car}\,M} \\ \chi : & S & \longrightarrow & A \\ & \mu_{i\,,1\leq i\leq r} & \longmapsto & \prod_{i=1}^{r}{}' \mu_i \\ \sigma_n : & \mathcal{M}_n(k) & \longrightarrow & S \\ & M & \longmapsto & \text{la suite des invariants de similitude (cf. cours IV.11.9.)} \end{array}$$

On a (cf. cours IV.11.11,)

$$\pi_n \;=\; \chi \circ \sigma_n\;. \qquad (2)$$

De plus (cf. cours IV.11.8,) les applications π_n et σ_n sont constantes sur les classes de similitude de matrices. si donc on note $\Gamma(n)$ l'ensemble des classes de similitude de matrices dans $\mathcal{M}_n(k)$, on a encore, à un abus de notation près, des application π_n et σ_n :

$$\begin{array}{lrcl} \pi_n : & \Gamma(n) & \longrightarrow & U(n) \\ & C & \longmapsto & \pi_n(M)\;,\; \forall M\in C, \\ \sigma_n : & \Gamma(n) & \longrightarrow & S \\ & C & \longmapsto & \sigma_n(M)\;,\; \forall M\in C, \\ \text{vérifiant encore} & \pi_n & \underset{\Sigma_n}{=} & \chi\circ\sigma_n \\ \textit{i.e.}\text{le diagramme suivant est commutatif :} & \Gamma(n) & \xrightarrow[\Sigma_n]{} & S \\ & & \searrow \pi_n & \big\downarrow \chi \\ & & & U(n)\,. \end{array} \qquad (3)$$

On peut donner les propriétés suivantes des applications π_n et σ_n qui traduisent les résultats de la théorie (cf. cours IV.11,) de réduction de FROBENIUS :

Lemme 2).1.4 *L'application σ_n est injective ou de manière équivalente induit une bijection (cf. IV.11.8,)*

$$\sigma_n \,:\, \Gamma(n) \,\cong\, \sigma_n(\Gamma(n)) \,=\, \sigma_n(\mathcal{M}_n(k))\,.$$

Lemme 2).1.5 *L'application π_n est surjective puisqu'à tout polynôme unitaire de degré n, $P \in U(n)$ on peut associer une matrice compagnon (cf. IV.4.4,) dont P est le polynôme caractéristique.*

On a ainsi :

$$\Gamma(n) \,\cong\, \sigma_n(\Gamma(n)) \,=\, \coprod_{p \,\in\, U(n)} \chi^{-1}(\{P\})\,; \tag{6}$$

d'où il résulte, tous les ensembles considérés étant finis dès que k l'est :

$$\#\big(\Gamma(n)\big) \,=\, \sum_{P \,\in\, U(n)} \#\big(\chi^{-1}(\{P\})\big)\,. \tag{7}$$

Il découle de la définition de χ et de celle de S (cf. 1,) que pour tout polynôme unitaire irréductible $P \in I(n)$ $\chi^{-1}(\{P\})$ est un singleton. Il en résulte alors que d'une part :

Lemme 2).1.8 *Pour tout $P \in I(n)$ $\pi_n^{-1}(\{P\}) = \sigma_n^{-1}(\{\chi^{-1}(\{P\})\})$ est cyclique.*

$$\begin{aligned}
\#\big(\Gamma(n)\big) &= \sum_{P \,\in\, U(n)} \#\big(\chi^{-1}(\{P\})\big) \\
&= \sum_{P \,\in\, I(n)} \#\big(\chi^{-1}(\{P\})\big) + \sum_{P \,\in\, U(n) \,\setminus\, I(n)} \#\big(\chi^{-1}(\{P\})\big) \\
&= \#(I(n)) + \sum_{P \,\in\, U(n) \,\setminus\, I(n)} \#\big(\chi^{-1}(\{P\})\big) \\
&= i(n) + \sum_{P \,\in\, U(n) \,\setminus\, I(n)} \#\big(\chi^{-1}(\{P\})\big)
\end{aligned} \tag{9}$$

On constate encore que :

Lemme 2).1.10 *Pour tout $C \in \Gamma(n)$ C est cyclique si et seulement si*

$$\sigma_n(C) \,=\, (\pi_n(C)) \text{ (cf. IV.11.11 ;)}$$

ce qui établit une bijection entre les classes cycliques et $U(n)$.

a) Déterminer le nombre de classes de similitude dans $\mathcal{M}_2(k)$. Caractériser celle qui correspondent à des endomorphismes cycliques.

Solution : *On a établit*

$$\#\big(\Gamma(2)\big) \,=\, \#\big(I(2)\big) \,+\, \sum_{P \,\in\, U(2) \,\setminus\, I(2)} \#\big(\chi^{-1}(\{P\})\big)\,.\ \textit{(cf. 2).1.9 .)}$$

Or $U(2) \setminus I(2) = V(2) \cup W(2)$ *avec*

$$\begin{aligned}
V(2) &:= \{P \in U(2)\,;\, \exists (Q,R) \in I(1)\times I(1),\, q \neq R\,,\, P = QR\} \\
\text{et}\quad W(2) &:= \{P \in U(2)\,;\, \exists q \in I(1),\, P = Q^2\}\,.
\end{aligned}$$

Il en résulte que

$$\begin{aligned}
v(2) &:= \#\big(V(2)\big) = \binom{i(1)}{2} = \frac{p(p-1)}{2} \\
w(2) &:= \#\big(W(2)\big) = \#\big(I(1)\big) = p\,.
\end{aligned}$$

De plus :
$\forall P = QR \in V(2)$,

$$\chi^{-1}(\{P\}) \,=\, \{(P)\}\,;$$

$\forall P = Q^2 \in W(2)$,

$$\chi^{-1}(\{P\}) \,=\, \{(Q^2),(Q,Q)\}\,.$$

Il s'ensuit que :

$$\begin{aligned}\#\big(\Gamma(2)\big) &= \#\big(I(2)\big) + \sum_{P\,\in\,V(2)} \#\big(\chi^{-1}(\{P\})\big) + \sum_{P\,\in\,W(2)} \#\big(\chi^{-1}(\{P\})\big) \\ &= i(2) + v(2) + 2w(2)\,.\end{aligned}$$

Il vient alors (cf. question 1), b) :)

$$\begin{aligned}\#\big(\Gamma(2)\big) &= i(2) + v(2) + 2w(2) \\ &= \frac{p(p-1)}{2} + \frac{p(p-1)}{2} + 2p \\ &= p(p+1)\,.\end{aligned}$$

b) Même question dans $\mathcal{M}_3(k)$.
Solution : *Le raisonement est le même qu'en a) en particulier on peut encore écrire :*

$$\#\big(\Gamma(3)\big) \;=\; \sum_{P\,\in\,I(3)} \#\big(\chi^{-1}(\{P\})\big) + \sum_{P\,\in\,U(3)\,\setminus\,I(3)} \#\big(\chi^{-1}(\{P\})\big) \;=\; i(3) + \sum_{P\,\in\,U(3)\,\setminus I(3)} \#\big(\chi^{-1}(\{P\})\big)\,. \qquad 1$$

La seule complication vient du fait que la combinatoire des polynômes unitaire non irréductibles de degré 3 *est un peut plus complexe. On a, en effet*

$$U(3)\;\setminus\;I(3) \;=\; U_{(2,1)}(3)\;\cup\;U_{(1,1,1)}(3)\;\cup\;U_{(2)}(3)\;\cup\;U_{(3)}(3)$$ *l'union étant disjointe. (cf. question 1), c).1 .)*

Or :
$\forall P \;=\; QR \in U_{(2,1)}(3)$, *$Q$ étant irréductible R $\not|Q$ et*

$$\chi^{-1}(\{P\}) \;=\; \{(P)\}\,;$$

$\forall P \;=\; QRT \in U_{(1,1,1)}(3)$, *les polynômes Q, R et T étant deux à deux premiers entre eux,*

$$\chi^{-1}(\{P\}) \;=\; \{(P)\}\,;$$

$\forall P \;=\; Q^2R \in U_{(2)}(3)$, *$Q$ et R étant premiers entre eux,*

$$\chi^{-1}(\{P\}) \;=\; \{(Q^2R)(QR, Q)\}\,;$$

$\forall P \;=\; Q^3 \in U_{(3)}(3)$,

$$\chi^{-1}(\{P\}) \;=\; \{(Q^3), (Q^2, Q), (Q, Q, Q)\}\,.$$

Il en résulte que :

$$\#\big(\Gamma(3)\big) \;=\; \#\big(I(3)\big) \;+\; \#\big(U_{(2,1)}(3)\big) \;+\; \#\big(U_{(1,1,1)}(3)\big) \;+\; 2\#\big(U_{(2)}(3)\big) \;+\; 3\#\big(U_{(3)}(3)\big)\,.$$

Ceci se réécrit (cf. question 1), c).2 question 1), c).4 :)

$$\begin{aligned}\#\big(\Gamma(3)\big) &= i(3) + u_{(2,1)}(3) + u_{(1,,1,1)}(3) + 2u_{(2)}(3) + 3u_{(3)}(3) \\ &= i(3) + u_{(2,1)}(3) + u_{(1,,1,1)}(3) + u_{(2)}(3) + u_{(3)}(3) + u_{(2)}(3) + 2u_{(3)}(3) \\ &= u(3) + u_{(2)}(3) + 2u_{(3)}(3) \\ &= u(3) + i(1)i(2) + 2i(1) \\ &= p^3 + p\frac{p(p-1)}{2} + 2p \\ &= \frac{1}{2}\left(2p^3 - p^2 + 2p\right)\,.\end{aligned}$$

Exercice D : (**Puissances d'une matrice nilpotente**)

Soit A une matrice à coefficients dans un corps $\mathbb{K}$ dont les invariants de similitude sont

$$(X^5, X^4, X^4, X^3, X^3, X^3, X^2, X, X, X)\,.$$

1) Quels sont les invariants de similitude de A^2 .

Solution : *Le tableau de* YOUNG *de A est :*

$$\begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & * & * & * & \\ * & * & * & & \\ * & * & * & & \\ * & * & * & & \\ * & * & & & \\ * & & & & \\ * & & & & \\ * & & & & \end{pmatrix}.$$

Ceci entraîne que le tableau de YOUNG *de A^2 est :*

$$\begin{pmatrix} * & * & * \\ * & * & \\ * & * & \\ * & * & \\ * & * & \\ * & * & \\ * & * & \\ * & * & \\ * & * & \\ * & & \\ * & & \\ * & & \\ * & & \\ * & & \\ * & & \\ * & & \\ * & & \\ * & & \end{pmatrix}$$

si bien que les invariants de similitude de A^2 sont :

$$(X^3, X^2, X^2, X^2, X^2, X^2, X^2, X^2, X^2, X, X, X, X, X, X, X, X)\,.$$

2) Quels sont les invariants de similitude de A^3 ?

Solution : *En utilisant le tableau de* YOUNG *de A (cf. question 1),) on détermine celui de A^3 qui et alors :*

$$\begin{pmatrix} * & * \\ * & * \\ * & * \\ * & * \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \\ * & \end{pmatrix}$$

si bien que les invariants de similitude de A^3 sont

$$(X^2, X^2, X^2, X^2, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X) .$$

Université Paris Sud — Année 2018–2019

L3/S6 M305 — Algèbre II

Examen partiel du 15 mars 2019
Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Le barème est indicatif, mais en cas de modification le poids relatif des exercice ne sera pas significativement modifié.

Exercice A : Les groupes abéliens

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \ \times \ \mathbb{Z}/25\mathbb{Z} \text{ et } \mathbb{Z}/25\mathbb{Z} \ \times \ \mathbb{Z}/25\mathbb{Z}$$

sont-ils isomorphes ?

Exercice B : Soient

$$0 \ \to \ N \xrightarrow{\ i\ } M \xrightarrow{\ p\ } Q \ \to \ 0$$

une suite exacte courte de groupes abéliens, R un groupe abélien et $f \ : \ R \ \to \ Q$ un morphisme de groupes.

On note

$$r \ : \ R \times M \ \to \ R \, , \ (x,y) \ \mapsto \ x \text{ et } q \ : \ R \times M \ \to \ M \, , \ (x,y) \ \mapsto \ y \, .$$

Enfin on note

$$P \ := \ \{(x,y) \ \in \ R \times M \, ; \ f[r(x,y)] \ = \ p[q(x,y)]\} \, .$$

1) $R \times M$ étant muni de sa structure produit, montrer que P en est un sous-groupe.

2) Montrer que, si f est injectif,

$$q_{|P} \ : \ P \ \to \ M$$

induit un isomorphisme

$$P \ \cong \ p^{-1}[f(R)] \, .$$

3) Montrer que $r_{|P}$ est un morphisme surjectif de noyau isomorphe à N et qu'on a donc une suite exacte

$$0 \ \to \ N \ \longrightarrow \ P \xrightarrow{\ r_{|P}\ } R \ \to \ 0 \, .$$

Exercice C : 1) (L'anneau $\mathbb{Z}[j]$ des entiers d'EISENSTEIN)

On note

$$\sigma \ : \ \mathbb{C} \ \to \ \mathbb{C} \, , \ a + ib \ \mapsto \ a - ib$$

la conjugaison complexe. On note

$$j \ := \ e^{\dfrac{2i\pi}{3}} \ \in \ \mathbb{C}$$

qui vérifie

$$j^3 \ = \ 1 \, , \ 1 + j + j^2 \ = \ 0 \text{ et } \sigma(j) \ = \ j^2 \, .$$

a) Montrer que si le polynôme $1 + X + X^2 \ \in \ \mathbb{Q}[X]$ a une racine dans $\mathbb{Q}$ celle-ci est entière et en déduire que j n'est pas rationnel.

b) On note $\mathbb{Z}[j]$ le sous-anneau de $\mathbb{C}$ défini par

$$\mathbb{Z}[j] \ := \ \{a + bj \ , \ (a, b) \ \in \ \mathbb{Z} \times \mathbb{Z}\}$$

muni des lois d'addition et de multiplication induites par celles de $\mathbb{C}$.

Montrer que $\mathbb{Z}[j]$ est un $\mathbb{Z}$-module (groupe abélien) libre de rang 2 et en donner une base.

c) Soit

$$N \ : \ \mathbb{C} \ \to \ \mathbb{R} \ , \ z \ \mapsto \ z \cdot \sigma(z) \ .$$

Montrer que N se restreint en une application encore notée $N \ : \ \mathbb{Z}[j] \ \to \ \mathbb{N}$ vérifiant

$$\forall \alpha \in \mathbb{Z}[j] \setminus \{0\}, \ N(\alpha) \ \geq \ 1 \text{ et } \forall (\alpha, \beta) \in \mathbb{Z}[j] \times \mathbb{Z}[j], \ N(\alpha\beta) \ = \ N(\alpha)N(\beta) \ .$$

d) Déterminer le groupe $U \ := \ \mathbb{Z}[j]^{\times}$ des éléments inversibles de $\mathbb{Z}[j]$.

On admettra dans la suite que, pour tout $z \ \in \ \mathbb{C}$ il existe $\alpha \ \in \ \mathbb{Z}[j]$ tel que $N(z - \alpha) \ < \ 1$.

e) Montrer que l'anneau $\mathbb{Z}[j]$ est principal.

f) Soit $\rho \ := \ 1 - j \ \in \ \mathbb{Z}[j]$.

Montrer que ρ est irréductible dans $\mathbb{Z}[j]$ et divise 3.

Indication : *on pourra calculer $N(\rho)$.*

g) On note $\kappa \ := \ \mathbb{Z}[j]/(\mathbb{Z}[j]\rho)$.

Que peut-on dire de l'anneau κ ? Montrer que la composée du morphisme

$$\mathbb{Z} \ \to \ \mathbb{Z}[j] \ , \ a \ \mapsto \ a + 0j \text{ et de la surjection canonique } \mathbb{Z}[j] \ \to \ \mathbb{Z}[j]/(\mathbb{Z}[j]\rho)$$

se factorise en un isomorphisme

$$\mathbb{F}_3 \ := \ \mathbb{Z}/3\mathbb{Z} \ \cong \ \kappa \ .$$

h) Pour tout $\alpha \ \in \ \mathbb{Z}[j]$, on notera désormais $v(\alpha)$ sa valuation ρ-adique *i.e.* le plus grand entier naturel k tel que $\rho^k | \alpha$.

Rappeler rapidement pourquoi

$$\forall (\alpha, \beta) \in \mathbb{Z}[j] \times \mathbb{Z}[j], \ v(\alpha\beta) \ = \ v(\alpha) \ + \ v(\beta) \text{ et } v(\alpha + \beta) \ \geq \ \min(v(\alpha), v(\beta)) \ .$$

2) (L'équation $\alpha^3 + \beta^3 + \gamma^3 \ = \ 0$))

Dans la suite on considère

$$(\alpha, \beta, \gamma) \ \in \ \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que } \alpha^3 \ + \ \beta^3 \ + \ \gamma^3 \ = \ 0 \ .$$

Dans cette question, l'élément $\rho \ \in \ \mathbb{Z}[j]$ est défini comme à la question 1), f).

a) Montrer que ρ divise l'un des trois facteurs

$$(\alpha + \beta) \ , \ (\beta + \gamma) \text{ ou } (\gamma + \alpha)$$

Indication : *on pourra vérifier que*

$$(\alpha + \beta + \gamma)^3 \ = \ 3(\alpha + \beta)(\beta + \gamma)(\gamma + \alpha) \ .$$

On suppose dans la suite que $\rho | (\alpha + \beta)$. On suppose de plus que $\alpha, \beta,$ et γ sont deux à deux premiers entre eux.

b) i) Montrer que l'on peut supposer que

$$\alpha \ \equiv \ 1 \ [\rho] \text{ et } \beta \ \equiv \ -1 \ [\rho]$$

Indication : *on pourra utiliser la question 1), g).*

ii) En écrivant $\alpha \ = \ 1 + \lambda\rho$ et en étudiant les congruences possibles de λ modulo ρ, montrer que,

$$\alpha \ \equiv \ 1 \ [\rho^2] \text{ ou } j\alpha \ \equiv \ 1 \ [\rho^2] \text{ ou } j^2\alpha \ \equiv \ 1 \ [\rho^2] \ ;$$

on admettra sans refaire les calculs, qu'un résultat analogue vaut pour β, *i.e.*

$$\beta \ \equiv \ -1 \ [\rho^2] \text{ ou } j\beta \ \equiv \ -1 \ [\rho^2] \text{ ou } j^2\beta \ \equiv \ -1 \ [\rho^2] \ .$$

iii) Montrer que

$$v(\alpha\beta\gamma) \;=\; v(\gamma) \;>\; 0\,.$$

c) Montrer qu'il existe

$$(\alpha_1, \beta_1, \gamma_1) \;\in\; \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que}$$

i)

$$\alpha_1 \;\equiv\; 1\;[\rho^2]\;,\; \beta_1 \;\equiv\; -1\;[\rho^2]\;;$$

ii)

$$\alpha_1^3 \;+\; \beta_1^3 \;+\; \gamma_1^3 \;=\; 0\,;$$

iii)

$$v(\alpha_1\beta_1\gamma_1) \;=\; v(\alpha\beta\gamma) \;>\; 0$$

iv) α_1, β_1 et γ_1 sont deux à deux premiers entre eux.

d) Montrer qu'il existe

$$(A, B, C) \;\in\; \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que} \qquad \begin{aligned} \alpha_1 + j\beta_1 &= A\rho, \\ j\alpha_1 + \beta_1 &= B\rho \\ \text{et} \qquad j^2(\alpha_1 + \beta_1) &= C\rho\,. \end{aligned}$$

e) Montrer que :

i) A et B sont premiers entre eux

Indication : *on pourra calculer*

$$\rho(Bj^2 - Aj) \text{ et } \rho(Aj^2 - Bj)\,;$$

Un calcul tout à fait similaire et qu'on ne demande pas de faire montre que A et C (resp. B et C,) sont également premiers entre eux.

ii) $A + B + C \;=\; 0\,;$

iii)

$$A \;\equiv\; 1\;[\rho]\;,\; B \;\equiv\; -1\;[\rho] \text{ et } C \;\equiv\; 0\;[\rho]\,;$$

iv)

$$\rho^3 ABC \;=\; -\gamma_1^3\,.$$

f) Montrer qu'il existe

$$(u, \alpha_2, \beta_2, \gamma_2) \;\in\; \mathbb{Z}[j]^\times \times \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que } u\alpha_2^3 \;=\; A\,,\; u\beta_2^3 \;=\; B \text{ et } u\gamma_2^3 \;=\; C\,.$$

g) Montrer que

$$v(\gamma_2) \;=\; v(\gamma) - 1$$

et en déduire que

$$v(\alpha_2\beta_2\gamma_2) \;=\; v(\alpha\beta\gamma) - 1\,.$$

h) (Bonus)
Montrer qu'il n'existe pas d'entiers $(a, b, c) \;\in\; \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ non nuls tels que

$$a^3 + b^3 \;=\; c^3\,.$$

Université Paris Sud — Année 2018–2019

L3/S6 M305 — Algèbre II

Corrigé de l'examen partiel du ? ?

Exercice A : 1) (L'anneau $\mathbb{Z}[j]$ des entiers d'EISENSTEIN)

On note

$$\sigma \, : \, \mathbb{C} \, \to \, \mathbb{C} \, , \, a + ib \, \mapsto \, a - ib$$

la conjugaison complexe. On note

$$j \, := \, e^{\frac{2i\pi}{3}} \, \in \, \mathbb{C}$$

qui vérifie

$$j^3 \, = \, 1 \, , \, 1 + j + j^2 \, = \, 0 \, \text{et} \, \sigma(j) \, = \, j^2 \, .$$

a) Montrer que si le polynôme $1 + X + X^2 \, \in \, \mathbb{Q}[X]$ a une racine dans $\mathbb{Q}$ celle-ci est entière et en déduire que j n'est pas rationnel.

Solution : *Soit*

$$\frac{r}{s} \, , \, r \, \in \, \mathbb{Z} \, , \, s \, \in \, \mathbb{Z} \, \setminus \{0\}$$

une racine rationnelle de $1 + X + X^2$. *Alors* $1 + \frac{r}{s} + \frac{r^2}{s^2} \, = \, 0$, *ce qui entraîne* $s^2 + rs + r^2 \, = \, 0$. *On peut, bien entendu, choisir* r *et* s *premiers entre eux. Il vient alors* $s(s + r) \, = \, r^2$ *ce qui entraîne* $s|r^2$ *et donc* $s|1$ *i.e.* $\frac{r}{s}$ *est entier.*

Or pour tout $n \, \in \, \mathbb{Z}$,

$$1 + n + n^2 \, \geq \, 1,$$

si bien que $1 + X + X^2$ *n'a pas de racine entière, donc pas de racine rationnelle.*

Le nombre complexe j *étant racine de* $1 + X + X^2$, *il n'est donc pas rationnel.*

b) On note $\mathbb{Z}[j]$ le sous-anneau de $\mathbb{C}$ défini par

$$\mathbb{Z}[j] \, := \, \{a + bj \, , \, (a, b) \, \in \, \mathbb{Z} \times \mathbb{Z}\}$$

muni des lois d'addition et de multiplication induites par celles de $\mathbb{C}$.

Montrer que $\mathbb{Z}[j]$ est un $\mathbb{Z}$-module (groupe abélien) libre de rang 2 et en donner une base.

Solution : *Par définition* $\{1, j\}$ *est une partie génératrice de* $\mathbb{Z}[j]$ *comme* $\mathbb{Z}$*-module.*

Par ailleurs

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}, \;\; a + bj \, = \, 0,$$

entraîne, si $b \, \neq \, 0$, $j \, = \, -\frac{a}{b}$ *ce qui n'est pas possible d'après la a). Si* $b \, = \, 0$ *alors* $a \, = \, 0$. *La partie* $\{1, j\}$ *est donc libre dans* $\mathbb{Z}[j]$ *si bien que c'est une base.*

c) Soit

$$N \, : \, \mathbb{C} \, \to \, \mathbb{R} \, , \, z \, \mapsto \, z \cdot \sigma(z) \, .$$

Montrer que N se restreint en une application encore notée $N \, : \, \mathbb{Z}[j] \, \to \, \mathbb{N}$ vérifiant

$$\forall \alpha \in \mathbb{Z}[j] \setminus \{0\}, \; N(\alpha) \, \geq \, 1 \, \text{et} \, \forall (\alpha, \beta) \in \mathbb{Z}[j] \times \mathbb{Z}[j], \; N(\alpha\beta) \, = \, N(\alpha)N(\beta) \, .$$

Solution : *On remarque que*

$$\forall a + bj \in \mathbb{Z}[j], \; \sigma(a + bj) \, = \, a + b\sigma(j) \, = \, a + bj^2 \, = \, a - b - bj \, \in \, \mathbb{Z}[j] \, .$$

L'automorphisme
σ *de* $\mathbb{C}$ *se restreint donc en un automorphisme (encore noté* $\sigma \, : \, \mathbb{Z}[j] \, \to \, \mathbb{Z}[j]$*) de* $\mathbb{Z}[j]$.

On a alors :

$$\begin{array}{rcl} \forall a + bj \in \mathbb{Z}[j], \quad N(a + bj) & = & (a + bj)\sigma(a + bj) \\ & = & (a + bj)(a - b - bj) \\ & = & a^2 - ab - abj + abj - b^2 j - b^2 j^2 \\ & = & a^2 - ab + b^2 \\ & \in & \mathbb{Z} \, . \end{array}$$

Or

$$a^2 - ab + b^2 \;=\; (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 \;\geq 0,$$

si bien que N *est à valeurs dans* $\mathbb{N}$. *Par ailleurs la réduction de Gauß de* N *donnée ci-dessus assure que* N *est définie positive et en tout cas que*

$$N(\alpha) \;=\; 0 \;\Rightarrow\; \alpha \;=\; 0,$$

si bien que

$$\forall \alpha \in \mathbb{Z}[j] \setminus \{0\},\; N(\alpha) \;\geq\; 1\,.$$

Enfin :

$$\begin{array}{rcl} \forall (\alpha,\beta) \in \mathbb{Z}[j] \times \mathbb{Z}[j], \quad N(\alpha\beta) & = & \alpha\beta\sigma(\alpha\beta) \\ & = & \alpha\sigma(\alpha)\beta\sigma(\beta) \\ & = & N(\alpha)N(\beta)\,. \end{array}$$

d) Déterminer le groupe $U \;:=\; \mathbb{Z}[j]^\times$ des éléments inversibles de $\mathbb{Z}[j]$.
Solution : *Pour tout* $u \;\in\; \mathbb{Z}[j]$, $\{u\}U$, *s'il existe* $v \;\in\; \mathbb{Z}[j]$, *tel que* $uv \;=\; 1$. *Ceci entraîne*

$$N(uv) \;=\; N(u)N(v) \;=\; 1\,.$$

Puisque $N(0) \;=\; 0$, *on a nécessairement* u *et* v *non nuls. Il s'ensuit que*

$$N(u) \;\geq\; 1 \text{ et } N(v) \;\geq\; 1$$

d'où

$$N(u) \;=\; N(v) \;=\; 1\,.$$

On constate alors que

$$U \;=\; \{1, -j, j^2, -1, j, -j^2\}$$

dans lequel $-j$ *est d'ordre* 6 *ce qui permet de donner un isomorphisme*

$$\mathbb{Z}/6\mathbb{Z} \;\to\; U\;,\; k \;\mapsto\; (-j)^k\,.$$

On admettra dans la suite que, pour tout $z \;\in\; \mathbb{C}$ **il existe** $\alpha \;\in\; \mathbb{Z}[j]$ **tel que** $N(z - \alpha) \;<\; 1$.

e) Montrer que l'anneau $\mathbb{Z}[j]$ est principal.
Solution : *Il suffit de remarquer que* N *est un stathme euclidien. Or pour tout*

$$(\alpha,\beta) \;\in\; \mathbb{Z}[j] \times (\mathbb{Z}[j] \setminus \{0\}),$$

il existe $\chi \;\in\; \mathbb{Z}[j]$ *tel que* $N(\frac{\alpha}{\beta} - \chi) \;<\; 1$. *d'où il vient, en posant* $\rho \;:=\; \alpha - \beta\chi$,

$$\alpha \;=\; \beta\chi \;+\; \rho \text{ et } N(\rho) \;<\; N(\beta)\,.$$

f) Soit $\rho \;:=\; 1 - j \;\in\; \mathbb{Z}[j]$.
Montrer que ρ est irréductible dans $\mathbb{Z}[j]$ et divise 3.
Indication : *on pourra calculer* $N(\rho)$.
Solution :

$$N(1-j) \;=\; (1-j)(1-j^2) \;=\; 1 - j - j^2 + j^3 \;=\; 3\,.$$

S'il existe

$$(\alpha,\beta) \;\in\; \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tels que } \rho \;=\; \alpha\beta,$$

alors

$$3 \;=\; N(\rho) \;=\; N(\alpha)N(\beta) \text{ (cf. c) .)}$$

Comme trois est irréductible dans $\mathbb{Z}$, $N(\alpha) \;\in\; \mathbb{N}$, $N(\beta) \;\in\; \mathbb{N}$, *on a*

$$N(\alpha) \;=\; 1 \text{ ou } N(\beta) \;=\; 1,$$

c'est-à-dire, d'après la d), que α *ou* β *est inversible et donc que* ρ *est irréductible.*
On a montré ci-dessus que $\rho\sigma(\rho) \;=\; 3$ *si bien que*

$$\rho | 3\,.$$

g) On note $\kappa := \mathbb{Z}[j]/(\mathbb{Z}[j]\rho)$.

Que peut-on dire de l'anneau κ ? Montrer que la composée du morphisme

$$\mathbb{Z} \to \mathbb{Z}[j] \ , \ a \mapsto a + 0j \text{ et de la surjection canonique } \mathbb{Z}[j] \to \mathbb{Z}[j]/(\mathbb{Z}[j]\rho)$$

se factorise en un isomorphisme

$$\mathbb{F}_3 := \mathbb{Z}/3\mathbb{Z} \cong \kappa \ .$$

Solution : *Puisque ρ est irréductible (cf. f),) dans l'anneau principal $\mathbb{Z}[j]$ l'idéal $\mathbb{Z}[j]\rho$ est maximal si bien que κ est un corps. Considérons le morphisme*

$$\psi : \mathbb{Z} \to \kappa \text{ composé de l'injection } \mathbb{Z} \hookrightarrow \mathbb{Z}[j] \text{ et de la surjection canonique } \mathbb{Z}[j] \to \kappa \ .$$

D'après la f), $3 \in \mathbb{Z}[j]\rho$ si bien que le morphisme ψ se factorise en un morphisme $\phi : \mathbb{F}_3 \to \kappa$ tel que le diagramme

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}[j] \\ \downarrow & \searrow^{\psi} & \downarrow \\ \mathbb{F}_3 & \xrightarrow{\phi} & \kappa \end{array}$$

(où les morphismes verticaux sont les surjections canoniques,) est commutatif.

Puisque $\mathbb{F}_3$ et κ sont des corps le morphisme ϕ est injectif.

Pour tout $\xi \in \kappa$, soit $\alpha := a + bj \in \mathbb{Z}[j]$ un antécédent de ξ par la surjection canonique. Alors $\alpha + b\rho = a + b$ est encore un antécédent de ξ. Il existe alors $k \in \mathbb{Z}$ tel que

$$a + b = \pm 1 + 3k = \pm 1 - j^2\rho^2 \ .$$

Il s'ensuit que ± 1 est un antécédent de ξ, si bien que

$$\xi = \pm\phi(1_{\mathbb{F}_3}) \ .$$

h) Pour tout $\alpha \in \mathbb{Z}[j]$, on notera désormais $v(\alpha)$ sa valuation ρ-adique *i.e.* le plus grand entier naturel k tel que $\rho^k | \alpha$.

Rappeler rapidement pourquoi

$$\forall (\alpha, \beta) \in \mathbb{Z}[j] \times \mathbb{Z}[j], \ v(\alpha\beta) = v(\alpha) + v(\beta) \text{ et } v(\alpha + \beta) \geq \min(v(\alpha), v(\beta)) \ .$$

2) (L'équation $\alpha^3 + \beta^3 + \gamma^3 = 0$))

Dans la suite on considère

$$(\alpha, \beta, \gamma) \in \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que } \alpha^3 + \beta^3 + \gamma^3 = 0 \ .$$

Dans cette question, l'élément $\rho \in \mathbb{Z}[j]$ est défini comme à la question 1), f).

a) Montrer que ρ divise l'un des trois facteurs

$$(\alpha + \beta) \ , \ (\beta + \gamma) \text{ ou } (\gamma + \alpha)$$

Indication : *on pourra vérifier que*

$$(\alpha + \beta + \gamma)^3 = 3(\alpha + \beta)(\beta + \gamma)(\gamma + \alpha) \ .$$

Solution :

$$\begin{array}{rcl} (\alpha + \beta + \gamma)^3 & = & \big(\alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \beta\gamma + \gamma\alpha)\big)(\alpha + \beta + \gamma) \\ & = & \alpha^3 + \beta^2\alpha + \gamma^2\alpha + 2(\alpha^2\beta + \alpha\beta\gamma + \gamma\alpha^2) + \\ & & \alpha^2\beta + \beta^3 + \beta\gamma^2 2 + 2(\alpha\beta^2 + \gamma\beta^2 + \alpha\beta\gamma) + \\ & & \alpha^2\gamma + \beta^2\gamma + \gamma^3 + 2(\alpha\beta\gamma + \beta\gamma^2 + \alpha\gamma^2) \\ & = & \alpha^3 + \beta^3 + \gamma^3 + \\ & & 3(\alpha^2\beta + \alpha^2\gamma + \beta^2\alpha + \beta^2\gamma + \gamma^2\alpha + \gamma^2\beta + 2\alpha\beta\gamma) \\ & = & 3\big((\alpha + \beta)(\beta + \gamma)(\gamma + \alpha)\big) \ . \end{array}$$

On a alors :

i) ($\rho | (\alpha + \beta + \gamma)$)

En effet, d'après la question 1), f), $\rho | 3$ donc

$$\rho | 3(\alpha + \beta)(\beta + \gamma)(\gamma + \alpha)$$

c'est-à-dire, d'après ce qui précède,

$$\rho | (\alpha + \beta + \gamma)^3 \ .$$

Or toujours d'après la question 1), f), ρ est irréductible, si bien que d'après le lemme de Gauß,

$$\rho | (\alpha + \beta + \gamma) \ .$$

ii) $(\rho|\big((\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\big))$

Il s'ensuit immédiatement que

$$\rho^3|(\alpha+\beta+\gamma)^3\ .$$

Or

$$(\alpha+\beta+\gamma)^3\ =\ 3(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\ .$$

On a donc

$$\begin{array}{rrcl} & \rho^3 & | & \big(3(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\big) \\ \Leftrightarrow & (\rho^2\rho) & | & \big(3(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\big) \\ \Leftrightarrow & (-3j\rho) & | & \big(3(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\big) \\ \Leftrightarrow & \rho & | & \big(-j^2(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\big)\ . \end{array}$$

Or $-j^2$ *est inversible, (voir question 1), d),) si bien que*

$$\rho|\big((\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)\big)\ .$$

iii) L'élément ρ *étant irréductible dans* $\mathbb{Z}[j]$ *c'est encore une fois le lemme de Gauß qui permet de conclure.*

On suppose dans la suite que $\rho|(\alpha+\beta)$. **On suppose de plus que** $\alpha,\beta,$ **et** γ **sont deux à deux premiers entre eux.**

b) i) Montrer que l'on peut supposer que

$$\alpha\ \equiv\ 1\ [\rho]\ \text{et}\ \beta\ \equiv\ -1\ [\rho]$$

Indication : *on pourra utiliser la question 1), g).*

Solution : *Notons* $f\ :\ \mathbb{Z}[j]\ \to\ \kappa$ *la surjection canonique. L'hypothèse que* $\rho|\alpha+\beta$ *signifie que* $f(\alpha+\beta)\ =\ 0$. *Or on n'a pas* $f(\alpha)\ =\ 0$, *sans quoi on aurait aussi* $f(\beta)\ =\ 0$, *i.e.*

$$\rho|\alpha\ \text{et}\ \rho|\beta$$

ce qui contredit l'hypothèse que α *et* β *sont premiers entre eux. On a donc, puisque* κ *est isomorphe à* $\mathbb{F}_3$ *(cf. question 1), g),)*

$$f(\alpha)\ =\ \pm 1_{\mathbb{F}_3}\ \text{et}\ \beta\ =\ -\alpha\ .$$

ii) En écrivant $\alpha\ =\ 1+\lambda\rho$ et en étudiant les congruences possibles de λ modulo ρ, montrer que,

$$\alpha\ \equiv\ 1\ [\rho^2]\ \text{ou}\ j\alpha\ \equiv\ 1\ [\rho^2]\ \text{ou}\ j^2\alpha\ \equiv\ 1\ [\rho^2]\ ;$$

on admettra sans refaire les calculs, qu'un résultat analogue vaut pour β, *i.e.*

$$\beta\ \equiv\ -1\ [\rho^2]\ \text{ou}\ j\beta\ \equiv\ -1\ [\rho^2]\ \text{ou}\ j^2\beta\ \equiv\ -1\ [\rho^2]\ .$$

Solution : *Il en résulte qu'il existe* $\lambda\ \in\ \mathbb{Z}[j]$ *tel que* $\alpha\ =\ 1+\lambda\rho$. *Puisque* $\lambda\ \in\ \mathbb{Z}[j]$, *il existe* $\mu\ \in\ \mathbb{Z}[j]$ *tel que* $\lambda\ =\ \mu\rho$ *Dans ce cas,* $\alpha\ =\ 1+\mu\rho^2$ *ce qui prouve le résultat.*

$\lambda\ =\ 1+\mu\rho$

$$\begin{array}{rcl} j\alpha & = & (1-\rho)\alpha \\ & = & (1-\rho)(1+\lambda\rho) \\ & = & (1-\rho)(1+(1+\mu\rho)\rho) \\ & = & (1-\rho)(1+\rho+\mu\rho^2) \\ & = & 1-\rho+\rho-\rho^2+\mu\rho^2-\mu\rho^3 \\ & = & 1-\rho^2(1-\mu+\mu\rho) \end{array}$$

ce qui prouve le résultat.

$\lambda\ =\ -1+\mu\rho$

$$\begin{array}{rcl} j^2\alpha & = & j^2(1+(-1+\mu\rho)\rho) \\ & = & j^2(1-\rho+\mu\rho^2) \\ & = & j^2-j^2+j^3+j^2\mu\rho^2 \\ & = & 1+j^2\mu\rho^2 \end{array}$$

ce qui prouve le résultat.

iii) Montrer que

$$v(\alpha\beta\gamma) \;=\; v(\gamma) \;>\; 0\,.$$

Solution : *Il résulte du point i) que*

$$v(\alpha) \;=\; v(\beta) \;=\; 0\,.$$

Il s'ensuit que

$$v(\alpha\beta\gamma) \;=\; v(\alpha)+v(\beta)+v(\gamma) \;=\; v(\gamma)\ \textit{(cf. question 1), h) .)}$$

Or

$$v(\gamma) \;=\; v\big(\alpha+\beta+\gamma-(\alpha+\beta)\big) \;\geq\; \min\big(v(\alpha+\beta+\gamma), v(\alpha+\beta)\big)\,.$$

Or il découle de l'hypothèse $\rho|\alpha+\beta\ v(\alpha+\beta) \;>\; 0$, *et de la a) que* $v(\alpha+\beta+\gamma) \;>\; 0$ *ce qui prouve le résultat.*

c) Montrer qu'il existe

$$(\alpha_1,\beta_1,\gamma_1) \;\in\; \mathbb{Z}[j]\times\mathbb{Z}[j]\times\mathbb{Z}[j] \text{ tel que}$$

i)

$$\alpha_1 \;\equiv\; 1\;[\rho^2]\,,\ \beta_1 \;\equiv\; -1\;[\rho^2]\,;$$

ii)

$$\alpha_1^3 \;+\; \beta_1^3 \;+\; \gamma_1^3 \;=\; 0\,;$$

iii)

$$v(\alpha_1\beta_1\gamma_1) \;=\; v(\alpha\beta\gamma) \;>\; 0$$

iv) α_1, β_1 et γ_1 sont deux à deux premiers entre eux.

Solution : *Si on modifie* α *et* β *comme en b).ii), i.e. en posant*

$$\alpha_1 \;=\; \alpha \text{ ou } j\alpha \textit{ ou } j^2\alpha \text{ et } \beta_1 \;=\; \beta \text{ ou } j\beta \text{ ou } j^2\beta,$$

on peut satisfaire la condition i).

Puisque $j^3 \;=\; 1$ *et que* $\alpha^3+\beta^3+\gamma^3 \;=\; 0$, *la condition ii) reste satisfaite.*

Puisque j *et* j^2 *sont inversibles* α_1 *et* α *(resp.* β_1 *et* β*) sont associés si bien que* α_1,β_1 *et* γ_1 *restent deux à deux premiers entre eux et que la condition iv) reste vérifiée.*

Enfin, toujours du fait que j *et* j^2 *sont inversibles,* $v(j) \;=\; v(j^2) \;=\; 0$ *si bien que*

$$v(\alpha_1) \;=\; v(\alpha) \text{ et } v(\beta_1) \;=\; v(\beta)\,.$$

Il s'ensuit que b).iii) entraîne immédiatement iii).

d) Montrer qu'il existe

$$(A,B,C) \;\in\; \mathbb{Z}[j]\times\mathbb{Z}[j]\times\mathbb{Z}[j] \text{ tel que} \qquad \begin{aligned} \alpha_1+j\beta_1 &= A\rho,\\ j\alpha_1+\beta_1 &= B\rho\\ \text{et}\qquad\qquad j^2(\alpha_1+\beta_1) &= C\rho\,. \end{aligned}$$

Solution : *On remarque que*

$$\alpha_1+j\beta_1 \;=\; \alpha_1+\beta_1-\rho\beta_1\,.$$

Or d'après c).i), $\rho|\alpha_1+\beta_1$ *si bien que*

$$\rho|\alpha_1+j\beta_1$$

et qu'il existe donc

$$A \;\in\; \mathbb{Z}[j] \textit{ tel que } \alpha_1+j\beta_1 \;=\; A\rho\,.$$

De même, on remarque que

$$j\alpha_1+\beta_1 \;=\; \alpha_1+\beta_1-\rho\alpha_1,$$

ce qui pour les même raisons, assure de l'existence de

$$B \;\in\; \mathbb{Z}[j] \textit{ tel que } j\alpha_1+\beta_1 \;=\; B\rho\,.$$

Enfin il suffit de remarquer une fois encore que $\rho|\alpha_1+\beta_1$ *pour assurer l'existence de*

$$C \;\in\; \mathbb{Z}[j] \textit{ tel que } j^2(\alpha_1+\beta_1) \;=\; C\rho\,.$$

e) Montrer que :

i) A et B sont premiers entre eux

Indication : *on pourra calculer*

$$\rho(Bj^2 - Aj) \text{ et } \rho(Aj^2 - Bj) \; ;$$

Un calcul tout à fait similaire et qu'on ne demande pas de faire montre que A et C (resp. B et C,) sont également premiers entre eux.

Solution :

$$\rho(Bj^2 - Aj) \; = \; j^3\alpha_1 + j^2\beta_1 - j\alpha_1 - j^2\beta_1 \; = \; (1-j)\alpha_1 \; = \; \rho\alpha_1$$

d'où

$$Aj^2 - Bj \; = \; \alpha_1 \; .$$

$$\rho(Aj^2 - Bj) \; = \; j^2\alpha_1 + j^3\beta_1 - j^2\alpha_1 - j\beta_1 \; = \; (1-j)\beta_1 \; = \; \rho\beta_1$$

d'où

$$Aj^2 - Bj \; = \; \beta_1 \; .$$

Ainsi tout diviseur commun à A et B est un diviseur commun à α_1 et β_1 qui sont premiers entre eux d'après c).iv). Il en est donc de même de A et B.

De même

$$\rho(jC - A) \; = \; \rho\beta_1 \text{ et } \rho(C - jA) \; = \; -j\rho\alpha_1 \; .$$

Ce qui prouve, comme j est inversible, que A et C sont premiers entre eux.

Le calcul pour μB et C est vraiement le même.

ii) $A + B + C \; = \; 0$;

Solution :

$$\rho(A + B + C) \; = \; \alpha_1 + j\beta_1 + j\alpha_1 + \beta_1 + j^2(\alpha_1 + \beta_1) \; = \; (\alpha_1 + \beta_1)(1 + j + j^2) \; = \; 0 \; .$$

iii)

$$A \; \equiv \; 1 \; [\rho] \; , \; B \; \equiv \; -1 \; [\rho] \text{ et } C \; \equiv \; 0 \; [\rho] \; ;$$

Solution : *D'après c).i), écrivons*

$$\alpha_1 \; = \; 1 + \lambda\rho^2 \text{ et } \beta_1 \; = \; -1 + \mu\rho^2 \; .$$

Il vient alors

$$A\rho \; = \; 1 + \lambda\rho^2 + j(-1 + \mu\rho^2) \; = \; (1-j) + (\lambda + j\mu)\rho^2 \; = \; \rho(1 + (\lambda + j\mu)\rho)$$

d'où

$$A \; = \; 1 + (\lambda + j\mu)\rho \; .$$

De même

$$B\rho \; = \; j(1 + \lambda\rho^2) - 1 + \mu\rho^2 \; = \; \rho(-1 + (j\lambda + \mu)\rho)$$

d'où

$$B \; = \; -1 + (j\lambda + \mu)\rho \; .$$

Enfin

$$C\rho \; = \; j^2(1 + \lambda\rho^2 - 1 + \mu\rho^2) \; = \; \rho(j^2(\lambda + \mu)\rho)$$

d'où

$$C \; = \; j^2(\lambda + \mu)\rho \; .$$

iv)

$$\rho^3 ABC \; = \; -\gamma_1^3 \; .$$

Solution :

$$\begin{aligned} \rho^3 ABC &= (\alpha_1 + \beta_1 j)(\alpha_1 + \beta_1 j^2)(\alpha_1 + \beta_1) \\ &= \alpha_1^3 + \beta_1^3 \\ &= -\gamma_1^3 \; . \end{aligned}$$

f) Montrer qu'il existe

$$(u, \alpha_2, \beta_2, \gamma_2) \in \mathbb{Z}[j]^\times \times \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que } u\alpha_2^3 = A\,,\ u\beta_2^3 = B \text{ et } u\gamma_2^3 = C\,.$$

Solution : *On a montré en e).iv) que*

$$\rho^3 ABC = -\gamma_1^3\,.$$

Or il découle de c).i) et c).iii) que $v(\gamma_1) > 0$ *ou encore que* $\rho|\gamma_1$. *Il existe donc* $\theta \in \mathbb{Z}[j]$ *tel que* $\gamma_1 = \rho\theta$ *ce qui entraîne* $\rho^3 ABC = -\rho^3\theta^3$ *et donc*

$$ABC = (-\theta)^3\,.$$

Or A, B *et* C *sont deux à deux premiers entr eux d'après e).i),si bien qu'il existe*

$$(\alpha_2, \beta_2, \gamma_2) \in \mathbb{Z}[j] \times \mathbb{Z}[j] \times \mathbb{Z}[j] \text{ tel que } \alpha_2^3 = A\,,\ \beta_2^3 = B \text{ et } \gamma_2^3 = C\,.$$

g) Montrer que

$$v(\gamma_2) = v(\gamma) - 1$$

et en déduire que

$$v(\alpha_2\beta_2\gamma_2) = v(\alpha\beta\gamma) - 1\,.$$

Solution : *On a* $\gamma_2^3 = C$ *d'où* $3v(\gamma_2) = v(C)$. *Or d'après e).iii)* $v(A) = v(B) = 0$, *d'où* $v(C) = v(ABC)$ *ce qui, en utilisant e).iv), donne*

$$3 + 3v(\gamma_2) = v(\rho^3\gamma_2) = v(\rho^3 C) = v(\rho^3 ABC) = v(\gamma_1^3) = 3v(\gamma_1)\,.$$

Il s'ensuit que $v(\gamma_2) = v(\gamma_1) - 1$. *Or d'après c),*

$$v(\gamma_1) = v(\alpha_1\beta_1\gamma_1) = v(\alpha\beta\gamma)\,.$$

Il s'ensuit que $v(\gamma_2) = v(\alpha\beta\gamma) - 1$. *Or d'après e).iii),*

$$3v(\alpha_2) = v(A) = 0 \text{ et } 3v(\beta_2) = v(B) = 0$$

d'où $v(\alpha_2) = v(\beta_2) = 0$ *et finalement*

$$v(\alpha_2\beta_2\gamma_2) = v(\gamma_2) = v(\alpha\beta\gamma) - 1\,.$$

h) (Bonus)
Montrer qu'il n'existe pas d'entiers $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ non nuls tels que

$$a^3 + b^3 = c^3\,.$$

Université Paris Sud — Année 2018–2019

L3/S6 M305 — Algèbre II

Examen du 6 mai 2019
Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Exercice A : Soit $A := \mathbb{Z}^2$ muni de sa structure de groupe abélien dont on note $\begin{pmatrix} x \\ y \end{pmatrix}$ les éléments.

1) (**Base**)
Soit $\mathcal{B} := \left(\begin{pmatrix} r \\ s \end{pmatrix}, \begin{pmatrix} t \\ u \end{pmatrix} \right)$ un couple d'éléments de A.

a) À quelle condition nécessaire et suffisante $\mathcal{B}$ est-elle une famille libre de A ?

b) Montrer que $\mathcal{B}$ est une base de A si et seulement si $ru - st = \pm 1$.

c) Montrer que si $\mathcal{B}$ est une base de A,

$$\left(\begin{pmatrix} r \\ s \end{pmatrix}, \begin{pmatrix} t' \\ u' \end{pmatrix} \right) \text{ est une base de } A \text{ si et seulement si}$$

$$\exists k \in \mathbb{Z}, \text{ tel que } \begin{pmatrix} t \\ u \end{pmatrix} - \begin{pmatrix} t' \\ u' \end{pmatrix} = k \begin{pmatrix} r \\ s \end{pmatrix} \text{ ou } \begin{pmatrix} t \\ u \end{pmatrix} + \begin{pmatrix} t' \\ u' \end{pmatrix} = k \begin{pmatrix} r \\ s \end{pmatrix}.$$

Soient $\left(b_1 := \begin{pmatrix} 6 \\ 9 \end{pmatrix}, b_2 := \begin{pmatrix} 15 \\ 25 \end{pmatrix} \right) \in A \times A$ et

$$B := \text{Vect}\{b_1, b_2\} = \{xb_1 + yb_2 \,,\, (x, y) \in \mathbb{Z}^2\} \subset A\,.$$

2) **a)** Montrer qu'il existe

$$(a, b) \in \mathbb{N}^2 \,,\, (a_1, a_2) \in A \times A \text{ tels que :}$$

i) $b_1 = aa_1$;

ii) (a_1, a_2) est une base de A ;

iii) (aa_1, ba_2) est une base de B

et que sous les hypothèses i) à iii) le triplet (a, b, a_1) est unique. Qu'en est-il de a_2 ?

b) La base (aa_1, ba_2) déterminée en a) est-elle adaptée à $B \subset A$?

c) Soient

$$d := a \wedge b \,,\, da' := a \,,\, db' = b \,,\, m \text{ le } \textbf{Ppcm} \text{ de } a \text{ et } b \text{ et } c_1 := a'a_1 + b'a_2 \,.$$

Montrer qu'il existe $c_2 \in A$ tel que (c_1, c_2) est une base de A et qu'alors (dc_1, mc_2) est une base de B.

d) Donner une base adaptée à $B \subset A$ et les facteurs invariants de A/B.

Exercice B : (Commutant)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie n et $u \in \mathrm{End}_{\mathbb{K}}(E)$. On appelle *commutant de* u et on note

$$\mathrm{Com}(u) := \{v \in \mathrm{End}_{\mathbb{K}}(E) \,;\, u \circ v = v \circ u\} \subset \mathrm{End}_{\mathbb{K}}(E)$$

l'ensemble des endomorphismes de E qui commutent avec u. On rappelle que $\mathbb{K}[u] \subset \mathrm{End}_{\mathbb{K}}(E)$ est l'ensemble des polynômes en u *i.e.* l'image de $\mathbb{K}[X]$ par le morphisme $X \mapsto u$.

1) Montrer que $\mathrm{Com}(u)$ est un sous espace vectoriel de $\mathrm{End}_{\mathbb{K}}(E)$.

2) On suppose dans cette question que u est cyclique et que $x_0 \in E$ est un vecteur cyclique pour u.

a) En considérant l'application

$$\varphi : \mathrm{Com}(u) \to E \,,\, v \mapsto v(x_0),$$

montrer que l'on a $\dim_{\mathbb{K}} \mathrm{Com}(u) \leqslant n$.

b) Montrer que $\dim \mathbb{K}[u] \geq n$ et que

$$\mathrm{Com}(u) = \mathbb{K}[u] \,.$$

On pourra remarquer, en particulier que si u est nilpotent d'échelon n (cf. cours IV.8.1,)

$$\mathrm{Com}(u) \cong \mathbb{K}[u] \,.$$

3) Supposons que $E = \bigoplus_{i=1}^{r} E_i$ avec E_i stable par u. Comparer

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \text{ et } \sum_{i=1}^{r} \dim_{\mathbb{K}} \mathrm{Com}(u_{|E_i}) \,.$$

4) On suppose que $E = E_1 \oplus E_2$, où E_i est stable par u, cyclique de polynôme minimal μ_i avec $\mu_2 | \mu_1$.

a) Montrer qu'il existe une base $\mathcal{B}$ de E telle que :

$$M_{\mathcal{B}}(u) = \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix}$$

où pour tout polynôme $R \in \mathbb{K}[X]$, C_R désigne la matrice compagnon de R.

b) En déduire qu'il existe un endomorphisme $v \in \mathrm{Com}(u) \setminus \{0\}$ dont la matrice dans la base $\mathcal{B}$ est de la forme

$$M_{\mathcal{B}}(v) = \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix} .$$

c) Montrer que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) > n \,.$$

5) Déduire de ce qui précède que, si u n'est pas cyclique $\dim_{\mathbb{K}} \mathrm{Com}(u) > n$; puis que $\dim_{\mathbb{K}} \mathrm{Com}(u) = n$ si et seulement si u est cyclique.

Exercice C : (Réduction de JORDAN et tableaux de YOUNG)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \text{ on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

1) Quand $\varepsilon = n$, décrire complètement la suite $\dim_{\mathbb{K}} N_i \,, i \in \mathbb{N}$.

2) (Injection de FROBENIUS)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \text{ on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

On note

$$\forall i \in \mathbb{N}^*, \ \sigma(i) := \dim_{\mathbb{K}} N_i - \dim_{\mathbb{K}} N_{i-1} \,.$$

Il est vraisemblable que nombre des énoncés de cet exercice peuvent être obtenus comme corollaires du théorème IV.10.10 de réduction de JORDAN, mais on va chercher à les établir ici par des méthodes plus élémentaires.

a) Étant donnés un $\mathbb{K}$-espace vectoriel V de dimension finie et $W \subset V$ un sous-espace de V, , rappeler ce que vaut $\dim_{\mathbb{K}} V/W$ en fonction de $\dim_{\mathbb{K}} V$ et $\dim_{\mathbb{K}} W$.

b) Montrer que

$$\forall i \in \mathbb{N}, \ \sigma(i) \geq 0 \,.$$

c) Vérifier que, pour tout $i \in \mathbb{N}$, la restriction $f_{|N_{i+1}}$ de f à N_{i+1} est à valeurs dans N_i.

Pour tout $i \in \mathbb{N}$, on note

$$p_i : N_{i+1} \to N_{i+1}/N_i \text{ la surjection canonique } .$$

d) Montrer que, pour tout $i \in \mathbb{N}$, il existe un unique morphisme

$$f_i : N_{i+2}/N_{i+1} \to N_{i+1}/N_i tq \ f_i \circ p_{i+1} = p_i \circ f_{|N_{i+2}} \,.$$

e) Montrer que

$$\forall i \in \mathbb{N}, \ f_i \text{ est injective } .$$

On l'appellera l'*injection de* FROBENIUS.

f) Déduire de ce qui précède que $\sigma(\cdot)$ est décroissante.

3) (Tableaux de YOUNG)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \ \textbf{on note} \ N_k := \mathrm{Ker}\, f^k \,\mathrm{et}\, n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

a) Justifier, en citant précisément le théorème que vous utilisez, mais sans le redémontrer bien entendu, qu'il existe un entier $m \in \mathbb{N}^*$, des entiers strictement positifs r_j ,$1 \leq j \leq m$ et des sous espaces E_j ,$1 \leq j \leq m$ tels que :

J$_1$)
$$E = \bigoplus_{j=1}^{m} E_j \ ;$$

J$_2$) $\forall 1 \leq j \leq m$, E_j est stable par f ;

J$_3$)
$$\forall 1 \leq j \leq m-1, \ r_j \geq r_{j+1} \ ;$$

J$_4$) le sous-espace $(E_j, f_{|E_j})$ est cyclique de polynômes minimal X^{r_j}.

b) Que vaut $\displaystyle\sum_{j=1}^{m} r_j$?

On définit le *tableau de* YOUNG de (E, f) comme le tableau constitué de m lignes, alignées sur la gauche et tel que la $j^{\text{ième}}$ ligne comporte r_j cases. Par exemple si $m = 3, (r_1, r_2, r_3) = (5, 4, 1)$, le tableau de YOUNG est

$$Y(E,f) = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix} .$$

c) Montrer que pour tout $j \in \mathbb{N}^*$, $\sigma(j) := \dim_{\mathbb{K}} N_j - \dim_{\mathbb{K}} N_{j-1}$ est la hauteur (le nombre de cases) de la $j^{\text{ième}}$ colonne du tableau de YOUNG $Y(E, f)$.

d) **a)** Donner les invariants de similitudes de f nilpotent dont le tableau de YOUNG est

$$Y(E,f) = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix} .$$

b) Quelle est la dimension de E ?

c) Quels sont le tableau de YOUNG de f^2 et ses invariants de similitude.

Université Paris Sud — Année 2018–2019

L3/S6 M305 — Algèbre II

Corrigé de l'examen du 6 mai 2019

Exercice A : Soit $A := \mathbb{Z}^2$ muni de sa structure de groupe abélien dont on note $\begin{pmatrix} x \\ y \end{pmatrix}$ les éléments.

1) (Base)
Soit $\mathcal{B} := \left(\begin{pmatrix} r \\ s \end{pmatrix}, \begin{pmatrix} t \\ u \end{pmatrix} \right)$ un couple d'éléments de A.

a) À quelle condition nécessaire et suffisante $\mathcal{B}$ est-elle une famille libre de A ?
Solution : *Pour $(x, y) \in \mathbb{Z}^2$, l'équation $x\begin{pmatrix} r \\ s \end{pmatrix} + y\begin{pmatrix} t \\ u \end{pmatrix} = 0$ équivaut à :*

$$\{rx + ty = 0\}$$

b) Montrer que $\mathcal{B}$ est une base de A si et seulement si $ru - st = \pm 1$.
Solution :

c) Montrer que si $\mathcal{B}$ est une base de A,

$\left(\begin{pmatrix} r \\ s \end{pmatrix}, \begin{pmatrix} t' \\ u' \end{pmatrix} \right)$ est une base de A si et seulement si

$$\exists k \in \mathbb{Z}, \text{ tel que } \begin{pmatrix} t \\ u \end{pmatrix} - \begin{pmatrix} t' \\ u' \end{pmatrix} = k\begin{pmatrix} r \\ s \end{pmatrix} \text{ ou } \begin{pmatrix} t \\ u \end{pmatrix} + \begin{pmatrix} t' \\ u' \end{pmatrix} = k\begin{pmatrix} r \\ s \end{pmatrix}.$$

Solution :

Soient $\left(b_1 := \begin{pmatrix} 6 \\ 9 \end{pmatrix}, b_2 := \begin{pmatrix} 15 \\ 25 \end{pmatrix} \right) \in A \times A$ et

$$B := \text{Vect}\{b_1, b_2\} = \{xb_1 + yb_2 \,,\, (x, y) \in \mathbb{Z}^2\} \subset A\,.$$

2) a) Montrer qu'il existe

$$(a, b) \in \mathbb{N}^2 \,,\, (a_1, a_2) \in A \times A \text{ tels que :}$$

i) $b_1 = aa_1$;

ii) (a_1, a_2) est une base de A ;

iii) (aa_1, ba_2) est une base de B

et que sous les hypothèses i) à iii) le triplet (a, b, a_1) est unique. Qu'en est-il de a_2 ?

Solution : *Si (a_1, a_2) est une base de A, en posant $a_1 := \begin{pmatrix} r \\ s \end{pmatrix}$, nécessairement r et s sont premiers entre eux d'après la question 1), b). Si de plus,*

$$\exists a \in \mathbb{N}, \text{ tel que } b_1 = aa_1,$$

on a

$$a := 6 \wedge 9 = 3 \text{ et } a_1 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

Alors, d'après la question 1), b) $\left(a_1, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right)$ est une base de A et, d'après question 1), c), (a_1, a_2) est une base de A si et seulement si

$$\text{il existe } \epsilon = \pm 1 \text{ et } \exists k \in \mathbb{Z}, \text{ tels que } a_2 = \begin{pmatrix} \epsilon + 2k \\ 2\epsilon + 3k \end{pmatrix}.$$

S'il existe $b \in \mathbb{N}^*$ satisfaisant iii), on a un isomorphisme $A/B \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ce qui prouve l'unicité de b.

En prenant $a_2 := \begin{pmatrix} 3 \\ 5 \end{pmatrix}$ (a_1, a_2) satisfait ii) en vertu de la question 1), b). En prenant $b := 5$, $(aa_1, ba_2) = (b_1, b_2)$ est bien une famille génératrice de B qui est libre puisque (a_1, a_2) l'est si bien que iii) est satisfait.

Reste à prouver l'unicité de a_2. On sait, d'après question 1), c) que si a_2' vérifie ii),

$$\exists \epsilon = \pm 1 \ , \ \exists k \in \mathbb{Z}, \text{ tels que } a_2' = \epsilon a_2 + k a_1 \ .$$

Si de plus (a_1, a_2') vérifie iii), en particulier :

$$\begin{array}{lrcl}
\exists (x, y) \in \mathbb{Z}^2, & b_2 & = & axa_1 + bya_2' \\
\Leftrightarrow & ba_2 & = & axa_1 + by(\epsilon a_2 + k a_1) \\
\Leftrightarrow & \left\{\begin{array}{rcl} ax + byk & = & 0 \\ 1 - y\epsilon & = & 0 \end{array}\right\} & & \\
\Leftrightarrow & \left\{\begin{array}{rcl} ax + byk & = & 0 \\ y & = & \epsilon \end{array}\right\} & & \\
\Rightarrow & ax + bk\epsilon & = & 0
\end{array}$$

a_2 n'est pas unique on peut ajuster k et x sous certaines contraintes de divisibilité.

b) La base (aa_1, ba_2) déterminée en a) est-elle adaptée à $B \subset A$?

Solution : *On n'a*

$$\text{ni } a|b \ \text{ ni } b|a$$

si bien que la base (aa_1, ba_2) n'est pas adaptée.

c) Soient

$$d := a \wedge b \ , \ da' := a \ , \ db' = b \ , \ m \text{ le } \textbf{Ppcm} \text{ de } a \text{ et } b \text{ et } c_1 := a'a_1 + b'a_2 \ .$$

Montrer qu'il existe $c_2 \in A$ tel que (c_1, c_2) est une base de A et qu'alors (dc_1, mc_2) est une base de B.

Solution : *Dans la base (a_1, a_2), c_1 a pour couple de coordonnées (a', b'). Or par définition a' et b' sont premiers entre eux, si bien qu'il existe*

$$(u, v) \in \mathbb{Z}^2 \text{ tel que } a'v - b'u = 1 \ .$$

D'après la question 1), b), $\left(\begin{pmatrix} a' \\ b' \end{pmatrix}, \begin{pmatrix} u \\ v \end{pmatrix}\right)$ est une base de A.

De plus

$$dc_1 = da'a_1 + db'a_2 = aa_1 + ba_2 = b_1 + b_2 \in B$$

et

$$mc_2 = mua_1 + mva_2 = ub'aa_1 + va'ba_2 = ub'b_1 + va'b_2 \in B \ .$$

Il en découle que :

$$\begin{array}{lrcl}
\left\{\begin{array}{rcl} dc_1 & = & b_1 + b_2 \\ mc_2 & = & ub'b_1 + va'b_2 \end{array}\right\} & & & \\
\Leftrightarrow & \left\{\begin{array}{rcl} (va' - ub')b_1 & = & va'dc_1 - mc_2 \\ (va' - ub')b_2 & = & mc_2 - b'udc_1 \end{array}\right\} & & \\
\Leftrightarrow & \left\{\begin{array}{rcl} b_1 & = & vac_1 - mc_2 \\ b_2 & = & mc_2 - ubc_1 \end{array}\right\} & &
\end{array}$$

Il en résulte que (dc_1, mc_2) est génératrice de B et que c'est donc une base.

d) Donner une base adaptée à $B \subset A$ et les facteurs invariants de A/B.

Exercice B : (Commutant)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie n et $u \in \mathrm{End}_{\mathbb{K}}(E)$. On appelle *commutant de* u et on note

$$\mathrm{Com}(u) := \{v \in \mathrm{End}_{\mathbb{K}}(E)\,;\, u \circ v = v \circ u\} \subset \mathrm{End}_{\mathbb{K}}(E)$$

l'ensemble des endomorphismes de E qui commutent avec u. On rappelle que $\mathbb{K}[u] \subset \mathrm{End}_{\mathbb{K}}(E)$ est l'ensemble des polynômes en u *i.e.* l'image de $\mathbb{K}[X]$ par le morphisme $X \mapsto u$.

1) Montrer que $\mathrm{Com}(u)$ est un sous espace vectoriel de $\mathrm{End}_{\mathbb{K}}(E)$.

Solution : *Il est clair que l'application nulle et l'identité de E appartiennent à $\mathrm{Com}(u)$ qui est donc non vide. Par ailleurs pour v et w dans $\mathrm{Com}(u)$, a et b dans $\mathbb{K}$,*

$$\begin{aligned} u \circ (av + bw) &= u \circ av + u \circ bw \\ &= av \circ u + bw \circ u \\ &= (av + bw) \circ u \end{aligned}$$

c'est-à-dire que $av + bw \in \mathrm{Com}(u)$ ce qui prouve que $\mathrm{Com}(u)$ est un sous espace vectoriel de $\mathrm{End}_{\mathbb{K}}(E)$.

On peut également constater que l'application

$$\mathrm{End}_{\mathbb{K}}(E) \to \mathrm{End}_{\mathbb{K}}(E)\,,\ v \mapsto u \circ v - v \circ u$$

est linéaire et que $\mathrm{Com}(u)$ est son noyau.

2) On suppose dans cette question que u est cyclique et que $x_0 \in E$ est un vecteur cyclique pour u.

a) En considérant l'application

$$\varphi : \mathrm{Com}(u) \to E\,,\ v \mapsto v(x_0),$$

montrer que l'on a $\dim_{\mathbb{K}} \mathrm{Com}(u) \leqslant n$.

Solution : *Soit $v \in \mathrm{Com}(u)$ tel que $\phi(v) = 0$ c'est-à-dire que $v(x_0) = 0$. On en déduit alors que*

$$\forall 1 \leq k \leq n-1,\ v[u^k(x_0)] = u^k[v(x_0)] = u^k(0) = 0$$

c'est-à-dire que v s'annule sur une base de E et donc que $v = 0$.

Il s'ensuit que ϕ est injective ce qui entraîne

$$\dim \mathrm{Com}(u) \leq \mathrm{rg}(\phi) \leq \dim E \leq n\,.$$

b) Montrer que $\dim \mathbb{K}[u] \geq n$ et que

$$\mathrm{Com}(u) = \mathbb{K}[u]\,.$$

On pourra remarquer, en particulier que si u est nilpotent d'échelon n (cf. cours IV.8.1,)

$$\mathrm{Com}(u) \cong \mathbb{K}[u]\,.$$

Solution :

i) Considérons la famille $F_U := \{u^i\}_{,0 \leq i \leq n-1} \subset \mathbb{K}[u]$. Pour tout n-uplet $(a_0, \ldots, a_{n-1})$ d'éléments de $\mathbb{K}$,

$$\begin{aligned} & \sum_{i=0}^{n-1} a_i u^i = 0 \\ \Rightarrow & \sum_{i=0}^{n-1} a_i u^i(x_0) = 0 \\ \Rightarrow & \qquad a_i = 0\ \forall 0 \leq i \leq n-1, \end{aligned}$$

puisque $\mathcal{B}$ est une base de E. Il en résulte que F_u est une famille libre de cardinal n de $\mathbb{K}[u]$ qui est donc de dimension au moins n.

On pourrait aussi voir que

$$\mathbb{K}[u] \cong \mathbb{K}[X]/P_{\min u}$$

qui est (cf. TD n° V, exercice C,) un espace vectoriel de dimension $\deg(P_{\min u})$. Or u étant cyclique

$$\deg(P_{\min u}) = n \text{ (cf. IV.4.1 .)}$$

ii) Pour tout $v \in \mathbb{K}[u]$, *il existe*

$$a_{i\ ,0\leq i\leq k} \in \mathbb{K} \text{ tel que } v = \sum_{i=0}^{k} a_i u^i .$$

Il s'ensuit que

$$\begin{aligned} u\circ v &= u\circ\big(\sum_{i=0}^{k} a_i u^i\big) \\ &= \sum_{i=0}^{k} a_i u^{i+1} \\ &= \big(\sum_{i=0}^{k} a_i u^i\big)\circ u \\ &= v\circ u . \end{aligned}$$

Il en résulte donc que $\mathbb{K}[u] \subset \mathrm{Com}(u)$ *ce qui combiné aux inégalités précédemment obtenues sur les dimensions donne finalement*

$$\mathbb{K}[u] = \mathrm{Com}(u) .$$

3) Supposons que $E = \bigoplus_{i=1}^{r} E_i$ avec E_i stable par u. Comparer

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \text{ et } \sum_{i=1}^{r} \dim_{\mathbb{K}} \mathrm{Com}(u_{|E_i}) .$$

Solution : *Notons* $\forall 1\leq i\leq r,\ u_i := u_{|E_i}$. *Pour tout* $v_{i\ ,1\leq i\leq r} \in \mathrm{Com}(u_i)$ *notons* $v \in \mathrm{End}_{\mathbb{K}}(E)$ *l'unique endomorphisme de* E *défini par*

$$\forall x := \sum_{i=1}^{r} x_{i\ ,x_i\in E_i} \in E,\ v(x) := \sum_{i=1}^{r} v_i(x_i) .$$

Notons que si l'on s'est donné des bases des sous-espaces E_i *dont la réunion forme une base de* E, *ce qui précède revient à écrire la matrice de* v *par blocs. De manière plus abstraite, c'est une conséquence de la proposition A.4.7.*

Alors :

$$\begin{aligned} \forall x\in E,\quad u[v(x)] &= u\big(\sum_{i=1}^{r} v(x_i)\big) \\ &= u\big(\sum_{i=1}^{r} v_i(x_i)\big) \\ &= \sum_{i=1}^{r} u[v_i(x_i)] \\ &= \sum_{i=1}^{r} u_i[v_i(x)] \\ &= \sum_{i=1}^{r} v_i[u_i(x_i)] \\ &= v\big(\sum_{i=1}^{r} u_i(x_i)\big) \\ &= v[u(x)] . \end{aligned}$$

On construit ainsi une application

$$\gamma : \prod_{i=1}^{r} \mathrm{Com}(u_i) \to \mathrm{Com}(u) .$$

C'est une vérification assez pénible mais sans grande difficulté que de montrer que γ *est linéaire. De plus :*

$$\begin{aligned} &\forall v_{i\ ,1\leq i\leq r} \in \prod_{i=1}^{r} \mathrm{Com}(u_i), && \gamma(v) = 0 \\ &\Leftrightarrow && \forall 1\leq i\leq r,\ \forall x\in E_i,\ \gamma(v)(x) = 0 \\ &\Leftrightarrow && v_i(x) = 0 \\ &\Leftrightarrow && \forall 1\leq i\leq r,\ v_i = 0 ; \end{aligned}$$

c'est-à-dire que γ est injective ; d'où l'on déduit que

$$\sum_{i=1}^{r} \dim_{\mathbb{K}} \mathrm{Com}(u_i) \;=\; \dim_{\mathbb{K}}\big(\prod_{i=1}^{r} \mathrm{Com}(u_i)\big) \;\leq\; \dim_{\mathbb{K}} \mathrm{Com}(u)\,.$$

4) On suppose que $E \;=\; E_1 \,\oplus\, E_2$, où E_i est stable par u, cyclique de polynôme minimal μ_i avec $\mu_2|\mu_1$.

a) Montrer qu'il existe une base $\mathcal{B}$ de E telle que :

$$M_{\mathcal{B}}(u) \;=\; \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix}$$

où pour tout polynôme $R \,\in\, \mathbb{K}[X]$, C_R désigne la matrice compagnon de R.

Solution : *Par définition des espaces Cycliques (cf. cours IV.4.1.)*

b) En déduire qu'il existe un endomorphisme $v \,\in\, \mathrm{Com}(u) \,\setminus\, \{0\}$ dont la matrice dans la base $\mathcal{B}$ est de la forme

$$M_{\mathcal{B}}(v) \;=\; \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}.$$

Solution : *Si un tel v existe :*

$$\begin{array}{rcl} & M_{\mathcal{B}}(u)M_{\mathcal{B}}(v) - M_{\mathcal{B}}(v)M_{\mathcal{B}}(u) \;=\; 0 \\ \Leftrightarrow \quad \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix} \cdot \begin{pmatrix} C_{\mu_1} & 0 \\ 0 & C_{\mu_2} \end{pmatrix} & = & 0 \\ \Leftrightarrow \quad \begin{pmatrix} 0 & 0 \\ C_{\mu_2}A & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ AC_{\mu_1} & 0 \end{pmatrix} & = & 0 \\ \Leftrightarrow \quad C_{\mu_2}A - AC_{\mu_1} & = & 0\,. \end{array}$$

Une matrice non nulle $\begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}$ par blocs correspond à un morphisme $v \,:\, E_1 \,\to\, E_2$. La condition de commutation correspond à $v \,\circ\, u_1 \;=\; u_2 \,\circ\, v$ ce qui signifie exactement que v est un morphisme de $\mathbb{K}[X]$-modules (cf. cours IV.1.) Or $E_i \;=\; \mathbb{K}[X]/\mu_i$ avec $\mu_2|\mu_1$. On sait bien que dans ce cas, on a un morphisme naturel factorisant les projections canoniques :

$$\begin{array}{ccc} & \mathbb{K}[X] & \\ & \downarrow \;\; \searrow & \\ \mathbb{K}[X]/\mu_1 & \to & \mathbb{K}[X]/\mu_2\,. \end{array}$$

Si l'isomorphisme $E_i \;\cong\; \mathbb{K}[X]/\mu_i$ est donné par un vecteur cyclique x_i, dans les identifications ci-dessus, v est l'unique morphisme

$$v \,:\, E_1 \,\to\, E_2\,,\; x_1 \,\mapsto\, x_2 \,\text{et}\, v \,\circ\, u_1 \;=\; u_2 \,\circ\, v\,.$$

c) Montrer que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \;>\; n\,.$$

Solution : *Pour $i \;=\; 1$ ou 2, notons*

$$V_i \;:=\; \big\{v \,\in\, \mathrm{End}_{\mathbb{K}}(E)\,;\; E_{j\,,j\,=\,1\,\text{ou}\,2} \text{ est stable par } v\,,\; v_{|E_i} \,\in\, \mathrm{Com}(u_{|E_i})\,,\; v_{|E_{3-i}} \;=\; 0\big\}\,.$$

On a alors $V_i \;\cong\; \mathrm{Com}(u_{|E_i})$, $V_i \;\subset\; \mathrm{Com}(u)$ et la somme $V_1 + V_2$ est directe. On en déduit que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \;\geq\; \dim_{\mathbb{K}} V_1 + \dim_{\mathbb{K}} V_2 \;\geq\; \dim_{\mathbb{K}} E_1 + \dim_{\mathbb{K}} E_2$$

en utilisant les résultats de la question 2). Or l'endomorphisme v construit en b) n'appartient pas à $V_1 \;\oplus\; V_2$ ce qui rend strict l'inégalité précédente.

5) Déduire de ce qui précède que, si u n'est pas cyclique $\dim_{\mathbb{K}} \mathrm{Com}(u) \;>\; n$; puis que $\dim_{\mathbb{K}} \mathrm{Com}(u) \;=\; n$ si et seulement si u est cyclique.

Solution : *On a vu (cf. question 2), b),) que lorsque u est cyclique* $\dim_{\mathbb{K}} \mathrm{Com}(u) \;=\; n$.

Si u n'est pas cyclique, il existe en vertu du théorème IV.11.5 de réduction de FROBENIUS *une décomposition de*

$$E \;=\; \bigoplus_{i=1}^{r} E_i$$

en sous-espaces cycliques. L'énoncé d'unicité IV.11.5.2) dans le théorème loc. cit., assure alors que nécessairement $r \;\geq\; 2$. En appliquant alors un argument de récurrence sur r, on montre (cf. question 4),) que

$$\dim_{\mathbb{K}} \mathrm{Com}(u) \;>\; n\,.$$

Exercice C : (Réduction de JORDAN et tableaux de YOUNG)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \text{ on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

1) Quand $\varepsilon = n$, décrire complètement la suite $\dim_{\mathbb{K}} N_i \,,_{i \in \mathbb{N}}$.

Solution : *Choisissons une base $e_i \,,_{0 \leq i \leq n-1}$ donnée par un vecteur*

$$x \in E \text{ tel que } \{e_i := f^i(x)\} \,,_{0 \,\leq\, i \,\leq\, \varepsilon-1} \text{ soit une base de } E \text{ (cf. Problème n° II, exercice A, question 1) .)}$$

Alors :

$$\begin{array}{rcl} \forall 1 \leq i \leq n, \quad \forall 0 \leq j \leq n-1-i, \; f^i(e_j) & = & e_{i+j} \\ \forall n-i \leq j \leq n-1, \; f^i(e_j) & = & 0 \,. \end{array}$$

Il s'ensuit que

$$\begin{array}{ll} f_{|\mathrm{Vect}\left\{e_j \,,_{0 \leq j \leq n-1-i}\right\}} & \text{est injective} \\ f_{|\mathrm{Vect}\left\{e_j \,,_{n-i \leq j \leq n-1}\right\}} & \text{est nulle .} \end{array}$$

Comme par ailleurs

$$E = \mathrm{Vect}\left\{e_j \,,_{0 \leq j \leq n-1-i}\right\} \oplus \mathrm{Vect}\left\{e_j \,,_{n-i \leq j \leq n-1}\right\},$$

on en déduit que

$$\forall 0 \leq i \leq n-1, \; N_i = \mathrm{Vect}\left\{e_j \,,_{n-i \leq j \leq n-1}\right\} \Rightarrow \dim_{\mathbb{K}} N_i = i \,.$$

Enfin $f^n = 0$, si bien que

$$\forall i \in \mathbb{N}, \; i \geq n = \dim_{\mathbb{K}} N_i = n \,.$$

2) (Injection de FROBENIUS)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \text{ on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

On note

$$\forall i \in \mathbb{N}^*, \; \sigma(i) := \dim_{\mathbb{K}} N_i - \dim_{\mathbb{K}} N_{i-1} \,.$$

Il est vraisemblable que nombre des énoncés de cet exercice peuvent être obtenus comme corollaires du théorème IV.10.10 de réduction de JORDAN, mais on va chercher à les établir ici par des méthodes plus élémentaires.

a) Étant donnés un $\mathbb{K}$-espace vectoriel V de dimension finie et $W \subset V$ un sous-espace de V, , rappeler ce que vaut $\dim_{\mathbb{K}} V/W$ en fonction de $\dim_{\mathbb{K}} V$ et $\dim_{\mathbb{K}} W$.

Solution : *On a*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W$$

en application par exemple du théorème I.9.19 qui se déduit en fait du fait que V/W est isomorphe à n'importe qu'elle supplémentaire de W dans V.

b) Montrer que

$$\forall i \in \mathbb{N},\ \sigma(i)\ \geq 0\ .$$

Solution : *(cf. Problème n° II, exercice A, question 3),) d'où l'on peut même déduire plus précisément que*

$$\forall 1 \leq i \leq \varepsilon,\ \sigma(i)\ >\ 0 \text{ et } \forall k \in \mathbb{N},\ k\ >\ \varepsilon\ \Rightarrow\ \sigma(k)\ =\ 0\ .$$

c) Vérifier que, pour tout $i\ \in\ \mathbb{N}$, la restriction $f_{|N_{i+1}}$ de f à N_{i+1} est à valeurs dans N_i.
Solution :

$$\forall x \in N_{i+1},\ u^i[u(x)]\ =\ u^{i+1}(x)\ =\ 0\ \Leftrightarrow\ u(x)\ \in\ N_i\ .$$

Pour tout $i\ \in\ \mathbb{N}$, **on note**

$$p_i\ :\ N_{i+1}\ \to\ N_{i+1}/N_i \textbf{ la surjection canonique}\ .$$

d) Montrer que, pour tout $i\ \in\ \mathbb{N}$, il existe un unique morphisme

$$f_i\ :\ N_{i+2}/N_{i+1}\ \to\ N_{i+1}/N_i tq\ f_i\ \circ\ p_{i+1}\ =\ p_i\ \circ\ f_{|N_{i+2}}\ .$$

Solution : *Considérons le diagramme commutatif :*

$$\begin{array}{ccc} N_{i+1} & \hookrightarrow & N_{i+2} \\ {\scriptstyle f_{|N_{i+1}}}\downarrow & & \downarrow{\scriptstyle f_{|N_{i+2}}} \\ N_i & \hookrightarrow & N_{i+1} \end{array}$$

dont les flèches horizontales sont injectives. On obtient, par factorisation un morphisme

$$f_i\ :\ N_{i+2}/N_{i+1}\ \to\ N_{i+1}/N_i$$

si bien qu'on a un morphisme de suites exactes (c'est-à-dire un diagramme commutatif à lignes exactes) :

$$\begin{array}{ccccccccc} 0 & \to & N_{i+1} & \longrightarrow & N_{i+2} & \xrightarrow{p_{i+1}} & N_{i+2}/N_{i+1} & \to & 0 \\ & & {\scriptstyle f_{|N_{i+1}}}\downarrow & & {\scriptstyle f_{|N_{i+2}}}\downarrow & & \downarrow{\scriptstyle f_i} & & \\ 0 & \to & N_i & \longrightarrow & N_{i+1} & \xrightarrow{p_i} & N_{i+1}/N_i & \to & 0 \end{array}\ .$$

e) Montrer que

$$\forall i \in \mathbb{N},\ f_i \text{ est injective}\ .$$

On l'appellera l'*injection de* FROBENIUS.
Solution :

$$\forall y \in N_{i+2}/N_{i+1},\ \exists x\ \in\ N_{i+2},\ \textit{tel que}\ p_{i+1}(x)\ =\ y\ .$$

Alors :

$$\begin{array}{rrcl} & f_i(y) & = & 0 \\ \Leftrightarrow & f_i[p_{i+1}(x)] & = & 0 \\ \Leftrightarrow & p_i[u(x)] & = & 0 \\ \Leftrightarrow & u(x) & \in & N_i \\ \Rightarrow & x & \in & N_{i+1} \\ \Rightarrow & p_{i+1}(x) & = & 0 \\ \Rightarrow & y & = & 0\ . \end{array}$$

Ainsi f_i est injective.

f) Déduire de ce qui précède que $\sigma(\cdot)$ est décroissante.
Solution :

$$\begin{array}{rcll} \forall i \in \mathbb{N},\quad \sigma(i+1)-\sigma(i) & = & \big(\dim_{\mathbb{K}} N_{i+1} - \dim_{\mathbb{K}} N_i\big) & \\ & & -\big(\dim_{\mathbb{K}} N_i - \dim_{\mathbb{K}} N_{i-1}\big) & \textit{(cf. a) .)} \\ & = & \dim_{\mathbb{K}} N_{i+1}/N_i - \dim_{\mathbb{K}} N_i/N_{i-1} & \end{array}$$

Or f_{i-1} étant injectif (cf. e),)

$$\dim_{\mathbb{K}} N_{i+1}/N_i\ \leq\ \dim_{\mathbb{K}} N_i/N_{i-1}$$

ce qui conclut.

3) (Tableaux de YOUNG)

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

On suppose qu'il existe un entier $\varepsilon \in \mathbb{N}^*$ tel que

$$f^{\varepsilon} = 0 \,\mathrm{et} f^{\varepsilon-1} \neq 0$$

autrement dit tel que f soit nilpotent d'échelon (d'indice) ε (cf. cours IV.8.1.)

Étant donné un endomorphisme $f \in \mathrm{End}(E)$ de E,

$$\forall k \in \mathbb{N}, \ \textbf{on note } N_k := \mathrm{Ker}\, f^k \text{ et } n_k := \dim N_k$$

(avec la convention que $f^0 = \mathrm{Id}_E$.)

a) Justifier, en citant précisément le théorème que vous utilisez, mais sans le redémontrer bien entendu, qu'il existe un entier $m \in \mathbb{N}^*$, des entiers strictement positifs r_j ,$1 \leq j \leq m$ et des sous espaces E_j ,$1 \leq j \leq m$ tels que :

J$_1$)
$$E = \bigoplus_{j=1}^{m} E_j \ ;$$

J$_2$) $\forall 1 \leq j \leq m$, E_j est stable par f ;

J$_3$)
$$\forall 1 \leq j \leq m-1, \ r_j \geq r_{j+1} \ ;$$

J$_4$) le sous-espace $(E_j, f_{|E_j})$ est cyclique de polynômes minimal X^{r_j}.

Solution : *Le polynôme minimal de f est X^{ε}. Il est sindé et n'a qu'un facteur irréductible, si bien que dans ce cas, aussibien le théorème IV.11.5 de réduction de* FROBENIUS *que le théorème IV.10.10 donne le résultat demandé.*

b) Que vaut $\displaystyle\sum_{j=1}^{m} r_j$?

Solution : *Puisque les sous-espaces E_j ,$1 \leq j \leq m$ sont cycliques, on a :*

$$\forall 1 \leq j \leq m, \ \dim_{\mathbb{K}} E_j = \deg(P_{\mathit{min}\, f_{|E_j}}) = r_j \ \textit{(cf. IV.4.1 .)}$$

Or il résulte de a).J$_1$) que

$$n = \dim_{\mathbb{K}} E = \sum_{j=1}^{m} \dim_{\mathbb{K}} E_j = \sum_{j=1}^{m} r_j \ .$$

On définit le *tableau de* YOUNG de (E, f) comme le tableau constitué de m lignes, alignées sur la gauche et tel que la $j^{\text{ième}}$ ligne comporte r_j cases. Par exemple si $m = 3, (r_1, r_2, r_3) = (5, 4, 1)$, le tableau de YOUNG est

$$Y(E,f) = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix} .$$

c) Montrer que pour tout $j \in \mathbb{N}^*, \sigma(j) := \dim_{\mathbb{K}} N_j - \dim_{\mathbb{K}} N_{j-1}$ est la hauteur (le nombre de cases) de la $j^{\text{ième}}$ colonne du tableau de YOUNG $Y(E, f)$.

Solution : *Si l'on note h_j la hauteur de la $j^{\text{ième}}$ colonne du tableau de* YOUNG*, par construction*

$$h_j = \#\big(\{i \in \mathbb{N} \,;\, r_i \geq j\}\big) \, .$$

Puisque le tableau de YOUNG *est construit en rangeant les r_i par ordre décroissant, on a*

$$\forall 1 \leq i \leq h_j, \ r_i \geq j \text{ et } \forall h_j + 1 \leq i \leq m, \ r_i < j \, .$$

Alors

$$\begin{array}{rrcccccl} \forall 1 \leq i \leq h_j, & n_{i,j} & = & j & \text{et} & n_{i,j-1} & = & j-1 \\ \forall h_j + 1 \leq i \leq m, & n_{i,j} & = & r_j & \text{et} & n_{i,j-1} & = & r_j \end{array} \quad \textit{(cf. Problème n° II, exercice C, question 4) .)}$$

Il s'ensuit que :

$$\begin{aligned}\sigma(j) &= n_j - n_{j-1}\\ &= \sum_{i=1}^{m} n_{i,j} - n_{i,j-1}\\ &= \sum_{i=1}^{h_j} n_{i,j} - n_{i,j-1} + \sum_{i=h_j+1}^{m} n_{i,j} - n_{i,j-1}\\ &= \sum_{i=1}^{h_j} j - (j-1) + \sum_{i=h_j+1}^{m} r_j - r_j\\ &= h_j\ .\end{aligned}$$

d) **a)** Donner les invariants de similitudes de f nilpotent dont le tableau de YOUNG est

$$Y(E,f) \;=\; \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & \\ * & & & & \end{pmatrix}\ .$$

Solution : *On a immédiatement*

$$m \;=\; 3\ ,\ r_1 \;=\; 5\ ,\ r_2 \;=\; 4 \text{ et } r_3 \;=\; 1\ .$$

b) Quelle est la dimension de E ?
Solution :

$$\dim_{\mathbb{K}} E \;=\; \sum_{i=1}^{m} r_i \;=\; 5 \;+\; 4 \;+\; 1 \;=\; 10\ .\ \textit{(cf. b) .)}$$

c) Quels sont le tableau de YOUNG de f^2 et ses invariants de similitude.
Solution : *Cette question est l'une de celles qui met le mieux en évidence l'intérêt des tableaux de* YOUNG *dans l'études des endomorphismes nilpotents. En effet ces tableaux mettent en relation (leur lignes) les invariants de similitude $r_{i\ ,1\leq i\leq m}$ d'un endomorphisme nilpotent et les sauts (les colonnes) dans la suite des noyaux itérés $\sigma(j)\ ,_{1\ \leq\ j\ \leq\ r_1}$. Comme chaque fois qu'on établit de telles correspondances il se peut que, suivant les situations, certains invariants soient plus facile à calculer ; ce qui permet de déterminer les autres.*

Typpiquement si l'on note $g \;:=\; f^2$, on va constater que les sauts dans la suites des noyaux sont assez faciles à déterminer alors qu'il semble beaucoup moins immédiat de calculer les invariants de similitude. En effet,

$$\begin{aligned}\forall j \in \mathbb{N}^*,\quad \dim_{\mathbb{K}} \operatorname{Ker} g^j - \dim_{\mathbb{K}} \operatorname{Ker} g^{j-1} &= \dim_{\mathbb{K}} \operatorname{Ker} f^{2j} - \dim_{\mathbb{K}} \operatorname{Ker} f^{2j-2}\\ &= n_{2j} - n_{2j-2}\\ &= (n_{2j} - n_{2j-1}) + (n_{2j-1} - n_{2j-2})\ .\end{aligned}$$

Il faut donc « empiler l'une sur l'autre » (cf. c),) deux colonnes successives du tableau de f pour obtenir celui de g. Il en résulte, dans le cas particulier considéré ici que

$$Y(E,f^2) \;=\; Y(E,g) \;=\; \begin{pmatrix} * & * & * \\ * & * & \\ * & * & \\ * & * & \\ * & & . \end{pmatrix}\ .$$

Il an résulte que

$$m \;=\; 5\ ,\ r_1 \;=\; 3\ ,\ r_2 \;=\; r_3 \;=\; r_4 \;=\; 2 \;=\; r_5 \;=\; 1\ .$$

Université Paris Sud **Année 2018–2019**

L3/S6 M305 **Algèbre II**

Examen du 14 juin 2019
Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Exercice A : (**Groupes abéliens à** 144 **éléments**)
Donner les classes d'isomorphismes de groupes abéliens de cardinal 144.

Exercice B : (**Facteurs invariants**)
Soit A **le groupe abélien libre** $\mathbb{Z}^3 = \{(x,y,z)\,,\ x \in \mathbb{Z}, y \in \mathbb{Z}, z \in \mathbb{Z}\}$. **Soient**

$$\big(b_1 := (4,5,9), b_2 := (7,6,13), b_3 := (2,8,10)\big) \in A \times A \times A$$

et B **le sous-groupe de** A **engendré par** b_1**,**b_2 **et** b_3.

1) Justifier (en citant le théorème adéquat) que B est un groupe abélien libre.

2) **On note** B' **le sous-groupe de** A **engendré par** b_1 **et** b_2.

a) La famille (b_1, b_2, b_3) est-elle libre ?

b) Comparer B et B'.

c) Quel est le rang de B ? de B' ?

3) Donner les facteurs invariants du groupe quotient A/B.

4) **Soit** $a \in \mathbb{N}^*$, **et** B_a **le sous-groupe de** A **engendré par** ab_1, ab_2 **et** ab_3.
Déterminer les facteurs invariants du quotient A/B_a.

Exercice C : (**Commutation d'endomorphismes**)

1) **Soient** A **un anneau** $\mathfrak{I}$ **et** $\mathfrak{J}$ **des idéaux de** A **tels que** $\mathfrak{J} \subset \mathfrak{I}$.

$$\textbf{On note } p_{\mathfrak{I}} : A \to A/\mathfrak{I} \text{ et } p_{\mathfrak{J}} : A \to A/\mathfrak{J} \textbf{ les surjections canoniques } .$$

Montrer qu'il existe un unique morphisme d'anneaux

$$\phi : A/\mathfrak{J} \to A/\mathfrak{I} \text{ tel que } \phi \circ p_{\mathfrak{J}} = p_{\mathfrak{I}}$$

et que ϕ est surjectif.

Dans la suite, $\mathbb{K}$ **est un corps,** $\mathbb{K}[X]$ **l'anneau des polynômes à une indéterminée à coefficients dans** $\mathbb{K}$, P **et** Q **des éléments de** $\mathbb{K}[X]$ **tels que** $P|Q$.

2) Montrer qu'il existe un unique morphisme d'anneaux

$$\phi : \mathbb{K}[X]/Q\mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X] \text{ tel que } \forall R \in \mathbb{K}[X],\ \phi(R \bmod Q) = R \bmod P\,.$$

3) Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. On suppose que $E = F \oplus G$, où F et G sont des sous-espaces cycliques pour u de polynômes minimaux respectifs P et Q.

a) Donner deux caractérisations du fait que F et G sont cycliques.

b) Donner un isomorphisme $\mathbb{K}$-linéaire

$$\alpha : \mathbb{K}[X]/P\mathbb{K}[X] \cong F (\text{resp. } \beta : \mathbb{K}[X]/Q\mathbb{K}[X] \cong G .)$$

c) À l'aide de ce qui précède construire un morphisme $\mathbb{K}$-linéaire non nul

$$\psi : G \to F \text{ tel que } u_{|F} \circ \psi = \psi \circ u_{|G} .$$

d) En déduire finalement qu'il existe un endomorphisme $\mathbb{K}$-linéaire $\eta \in \mathrm{End}_{\mathbb{K}}(E)$ de E, tel que G ne soit pas stable par η et

$$\eta \circ u = u \circ \eta .$$

Exercice D : (L'anneau $\mathbb{Z}_{(3)}$)

Soit

$$V := \left\{ \frac{r}{s} \in \mathbb{Q} , \ r \text{ et } s \textbf{ premiers entre eux } , \ 3 \not| s \right\} .$$

Dans la suite, lorsqu'on écrira $\frac{r}{s} \in \mathbb{Q}$, on supposera toujours r et s premiers entre eux.

1) Montrer que V est un sous-anneau de $\mathbb{Q}$.

2) Montrer que V est un anneau intègre.

3) Montrer que $\mathbb{Z} \subset \mathbb{Q}$ est un sous-anneau de V.

4) Soit $\mathfrak{I} \subset V$ un idéal de V. Montrer que :

a) $\mathbb{Z} \cap \mathfrak{I}$ est un idéal de $\mathbb{Z}$;

b) si $\mathfrak{I} \neq \{0\}$, il existe $n \in \mathbb{N}$ tel que $\mathfrak{I} \cap \mathbb{Z} = 3^n\mathbb{Z}$;

c) $\mathfrak{I} \neq \{0\} \Rightarrow \mathfrak{I} = 3^n V$;

d) V est un anneau principal.

Pour tout

$$n \in \mathbb{N}^*, \textbf{ on note } \pi_n : \mathbb{Z} \to \mathbb{Z}/3^n\mathbb{Z} \textbf{ la surjection canonique} .$$

5) Montrer que pour tout $\frac{r}{s} \in V$, et tout $n \in \mathbb{N}^*$, $\pi_n(s)$ est inversible dans l'anneau $\mathbb{Z}/3^n\mathbb{Z}$.

6) Pour tout

$$\frac{r}{s} \in V \text{ et } \textbf{tout } n \in \mathbb{N}^* , \textbf{ on note } \pi'_n(\frac{r}{s}) := \pi_n(r)\pi_n(s)^{-1} .$$

a) Montrer que π'_n est un morphisme d'anneaux et que π'_n est surjectif.

b) Quel est le noyau de π'_n ?

7) a) Quels sont les idéaux premiers de V ?

b) Quels sont les idéaux maximaux de V ?

c) Montrer que si $u \in V$ est inversible, u n'appartient à aucun des idéaux $\mathfrak{I} \neq V$ de V et en particulier n'appartient pas à $3V$.

d) Quel est le groupe $V^\times$ des éléments inversibles de V ?

Université Paris Sud — Année 2018–2019

L3/S6 M305 — Algèbre II

Corrigé de l'examen du 14 juin 2019

Exercice A : (**Groupes abéliens à** 144 **éléments**)

Donner les classes d'isomorphismes de groupes abéliens de cardinal 144.

Solution : *On sait que les classes d'isomorphismes de groupes abéliens finis sont caractérisées par leurs facteurs invariants. Si G est un groupe abéliens de cardinal 96, il existe un unique entier $r \in \mathbb{N}$, et un unique r-uplet d_i ,$_{1\leq i\leq r}$ d'entiers naturels tels que*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \text{ et } \forall 1 \leq i \leq r-1,\ d_i | d_{i+1} .$$

Il s'ensuit que

$$\#(G) = \prod_{i=1}^{r} d_i .$$

Il s'ensuit que

$$\forall 1 \leq i \leq r,\ d_i | \#(G) .$$

Il s'ensuit que si p est un nombre premier

$$\exists i\ ,\ p|d_i \Leftrightarrow p|\#(G) .$$

Il s'ensuit encore que

$$p|\#(G) \Leftrightarrow p|d_r .$$

Ici

$$\#(G) = 96 = 2^4 3^2$$

si bien que

$$6 = 2 * 3 | d_r .$$

On a donc

$$d_r = 2^a 3^b\ ,\ 1 \leq a \leq 4\ ,\ 1 \leq b \leq 2 .$$

On a alors :

$a=4$	$b=2$	$\Rightarrow$	$r=1,$	$d_1=144$;
$a=4$	$b=1$	$\Rightarrow$	$r=2,$	$d_2=48, d_1=3$;
$a=3$	$b=2$	$\Rightarrow$	$r=2,$	$d_2=72, d_1=2$;
$a=3$	$b=1$	$\Rightarrow$	$r=2,$	$d_2=24, d_1=6$;
$a=2$	$b=2$	$\Rightarrow$	$r=2,$	$d_2=36, d_1=4$;
		ou	$r=3,\ d_3=36, d_2=2, d_1=2$;	
$a=2$	$b=1$	$\Rightarrow$	$r=2,$	$d_2=12, d_1=12$;
		ou	$r=3,\ d_3=12, d_2=6, d_1=2$;	
$a=1$	$b=2$	$\Rightarrow$	$r=4,$	$d_4=18, d_3=2, d_2=2, d_1=2$;
$a=1$	$b=1$	$\Rightarrow$	$r=4,$	$d_4=6, d_3=6, d_2=2, d_1=2$.

Exercice B : (**Facteurs invariants**)

Soit A le groupe abélien libre $\mathbb{Z}^3 = \{(x,y,z)\ ,\ x \in \mathbb{Z}, y \in \mathbb{Z}, z \in \mathbb{Z}\}$. Soient

$$\big(b_1 := (4,5,9), b_2 := (7,6,13), b_3 := (2,8,10)\big) \in A \times A \times A$$

et B le sous-groupe de A engendré par b_1,b_2 et b_3.

1) Justifier (en citant le théorème adéquat) que B est un groupe abélien libre.

2) On note B' le sous-groupe de A engendré par b_1 et b_2.

a) La famille (b_1, b_2, b_3) est-elle libre ?
Solution :

$$\begin{aligned} & xb_1 + yb_2 + zb_3 = 0 \\ \Leftrightarrow & \left\{\begin{array}{rcl} 4x + 7y + 2z & = & 0 \\ 5x + 6y + 8z & = & 0 \\ 9x + 13y + 10z & = & 0 \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} 4x + 7y + 2z & = & 0 \\ 5x + 6y + 8z & = & 0 \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} 4x + 7y + 2z & = & 0 \\ -11x - 22y & = & 0 \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} 4x + 7y + 2z & = & 0 \\ x + 2y & = & 0 \end{array}\right\} \end{aligned}$$

b) Comparer B et B'.

c) Quel est le rang de B ? de B' ?

3) Donner les facteurs invariants du groupe quotient A/B.

4) Soit $a \in \mathbb{N}^*$, et B_a le sous-groupe de A engendré par ab_1, ab_2 et ab_3.
Déterminer les facteurs invariants du quotient A/B_a.

Exercice C : (Commutation d'endomorphismes)

1) Soient A un anneau $\mathfrak{I}$ et $\mathfrak{J}$ des idéaux de A tels que $\mathfrak{J} \subset \mathfrak{I}$.

On note $p_{\mathfrak{I}} : A \to A/\mathfrak{I}$ et $p_{\mathfrak{J}} : A \to A/\mathfrak{J}$ les surjections canoniques .

Montrer qu'il existe un unique morphisme d'anneaux

$$\phi : A/\mathfrak{J} \to A/\mathfrak{I} \text{ tel que } \phi \circ p_{\mathfrak{J}} = p_{\mathfrak{I}}$$

et que ϕ est surjectif.
Solution : *Comme* $\operatorname{Ker} p_{\mathfrak{I}} = \mathfrak{I}$, *et* $\mathfrak{J} \subset \mathfrak{I}$, *le morphisme d'anneaux* $p_{\mathfrak{I}}$ *se factorise de manière unique à travers* $A/\mathfrak{J}$. *Comme* $p_{\mathfrak{I}}$ *est surjectif,* ϕ *l'est aussi.*

Dans la suite, $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$, P et Q des éléments de $\mathbb{K}[X]$ tels que $P|Q$.

2) Montrer qu'il existe un unique morphisme d'anneaux

$$\phi : \mathbb{K}[X]/Q\mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X] \text{ tel que } \forall R \in \mathbb{K}[X],\ \phi(R \bmod Q) = R \bmod P\,.$$

Solution : *C'est une application directe de la question 1), en prenant*

$$A := \mathbb{K}[X]\,,\ \mathfrak{I} := P\mathbb{K}[X] \text{ et } \mathfrak{J} := Q\mathbb{K}[X]\,.$$

3) Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \operatorname{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. On suppose que $E = F \oplus G$, où F et G sont des sous-espaces cycliques pour u de polynômes minimaux respectifs P et Q.

a) Donner deux caractérisations du fait que F et G sont cycliques.

b) Donner un isomorphisme $\mathbb{K}$-linéaire

$$\alpha \,:\, \mathbb{K}[X]/P\mathbb{K}[X] \,\cong\, F(\text{resp. } \beta \,:\, \mathbb{K}[X]/Q\mathbb{K}[X] \,\cong\, G\,.)$$

Solution : *Puisque F (resp. G,) est cyclique, il existe un vecteur $v \in F$ (resp. $w \in G$,) cyclique pour u. Il existe alors un unique isomorphisme $\mathbb{K}$-linéaire*

$$\mathbb{K}[X]/P\mathbb{K}[X] \,\to\, F\,,\; X^k \bmod P \,\mapsto\, u^k(v)\; (\textit{resp.}\; \mathbb{K}[X]/Q\mathbb{K}[X] \,\to\, G\,,\; X^k \bmod Q \,\mapsto\, u^k(w)\,)_{k\,\in\,\mathbb{N}}\,.$$

c) À l'aide de ce qui précède construire un morphisme $\mathbb{K}$-linéaire non nul

$$\psi \,:\, G \,\to\, F \text{ tel que } u_{|F} \circ \psi \,=\, \psi \circ u_{|G}\,.$$

Solution : *Le morphisme ϕ étant comme à la question 2) et les isomorphisme α et β comme en b), l'application*

$$\psi \,:=\, \alpha \circ \beta^{-1}$$

répond à la question.

d) En déduire finalement qu'il existe un endomorphisme $\mathbb{K}$-linéaire $\eta \in \mathrm{End}_{\mathbb{K}}(E)$ de E, tel que G ne soit pas stable par η et

$$\eta \circ u \,=\, u \circ \eta\,.$$

Solution : *Le morphisme ψ étant celui de c), il suffit de définir η par*

$$\eta_{|G} \,:=\, \psi \text{ et } \eta_{|F} \,:=\, 0\,.$$

Exercice D : (**L'anneau $\mathbb{Z}_{(3)}$**)
Soit

$$V \,:=\, \Big\{\frac{r}{s} \,\in\, \mathbb{Q}\,,\; r \text{ et } s \textbf{ premiers entre eux }\,,\; 3 \not| s\Big\}\,.$$

Dans la suite, lorsqu'on écrira $\frac{r}{s} \in \mathbb{Q}$, on supposera toujours r et s premiers entre eux.

1) Montrer que V est un sous-anneau de $\mathbb{Q}$.
Solution :

*i) (**Addition**)*

$$\textit{Pour } \Big(\frac{r}{s}, \frac{t}{u}\Big) \,\in\, V \times V\,,\; \frac{r}{s} +_{\mathbb{Q}} \frac{t}{u} \,=\, \frac{ru+ts}{su}\,.$$

Or

$$3 \not| s \text{ et } 3 \not| u \,\Rightarrow\, 3 \not| su$$

*puisque 3 est premier. Si même $ru+ts$ et su ne sont pas premiers entre eux, quitte à diviser par leur **Pgcd** d, on aura toujours $3 \not| \frac{su}{d}$. L'addition $+_{\mathbb{Q}}$ de $\mathbb{Q}$ se restreint donc en une loi interne associative sur V pour laquelle 0 est manifestement un élément neutre et telle que pour tout $\frac{r}{s} \in V$, $-\frac{r}{s}$ est un opposé. Cette loi restant également comutative, $(V,+)$ est un groupe abélien.*

*ii) (**Multiplication**)*

$$\textit{Pour } \Big(\frac{r}{s}, \frac{t}{u}\Big) \,\in\, V \times V\,,\; \frac{r}{s} *_{\mathbb{Q}} \frac{t}{u} \,=\, \frac{rt}{su}\,.$$

Or, pour les mêmes raisons que ci-dessus, $3 \not| su$, si bien que $*_{\mathbb{Q}}$ se restreint en une loi interne associative sur V pour laquelle 1 est manifestement un élément neutre. Cette loi reste distributive sur $+$ ce qui fait de $(V,+,*)$ un anneau (qui est même commutatif.)

2) Montrer que V est un anneau intègre.
Solution : *C'est un sous-anneau de $\mathbb{Q}$ qui est intègre.*

3) Montrer que $\mathbb{Z} \subset \mathbb{Q}$ est un sous-anneau de V.
Solution : *Puisque V est un anneau il existe un unique morphisme*

$$\mathbb{Z} \to V\ ,\ 1 \mapsto 1\ .$$

Il suffit alors de constater que le morphisme $\mathbb{Z} \to \mathbb{Q}$ qui est injectif est en fait à valeurs dans V. Or ce dernier est donné par

$$a \mapsto \frac{a}{1}\ ,\ \forall a \in \mathbb{Z},$$

ce qui prouve l'assertion.

4) Soit $\mathfrak{I} \subset V$ un idéal de V. Montrer que :

a) $\mathbb{Z} \cap \mathfrak{I}$ est un idéal de $\mathbb{Z}$;

b) si $\mathfrak{I} \neq \{0\}$, il existe $n \in \mathbb{N}$ tel que $\mathfrak{I} \cap \mathbb{Z} = 3^n\mathbb{Z}$;
Solution : *Puisque $\mathfrak{J} := \mathfrak{I} \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, il existe $d \in \mathbb{Z}$ tel que $\mathfrak{J} = d\mathbb{Z}$. Il existe alors un unique $n \in \mathbb{N}$ et un unique $u \in \mathbb{Z}$ tels que $d = 3^n u$ et $3 \not| u$. ainsi $\frac{1}{u} \in V$. Or comme $d \in \mathfrak{I}, 3^n = \frac{1}{u}d \in \mathfrak{I}$. Comme $d^n \in \mathbb{Z}, 3^n \in \mathfrak{J}$ si bien que $d|3^n$ c'est-à-dire que $3^u|3jjj^n$ ou encore que $u|1$. Il s'ensuit que*

$$\mathfrak{I} \cap \mathbb{Z} = \mathfrak{J} = d\mathbb{Z} = 3^n\mathbb{Z}\ .$$

c) $\mathfrak{I} \neq \{0\} \Rightarrow \mathfrak{I} = 3^n V$;
Solution : *Notons encore $\mathfrak{J} := \mathfrak{I} \cap \mathbb{Z}$. D'après le point précédent, $\mathfrak{J} = 3^n\mathbb{Z}$. Comme*

$$\mathfrak{J} \subset \mathfrak{I} \subset V,$$

$3^n \in \mathfrak{I}$ *si bien que*

$$3^n V \subset \mathfrak{I}.\ .$$

Réciproquement, pour tout $\frac{r}{s} \in \mathfrak{I}$, on a encore $r = s\frac{r}{s} \in \mathfrak{I}$. Or $r \in \mathbb{Z}$ si bien que $r \in \mathfrak{J}$. Il s'ensuit qu'il existe $t \in \mathbb{Z}$ tel que $r = 3^n t$, ce qui entraîne que $\frac{r}{s} = 3^n\frac{t}{s}$. Or $\frac{t}{s} \in V$ si bien que $\frac{r}{s} \in 3^n V$ ce qui entraîne finalement que

$$\mathfrak{I} \subset 3^n V\ .$$

d) V est un anneau principal.
Solution : *Résulte immédiatement du point précédent. L'idéal $\{0\}$, pourrait être traité dans le même formalisme en posant $\{0\} = 3^\infty\mathbb{Z}$.*

Pour tout

$$n \in \mathbb{N}^*,\ \textbf{on note}\ \pi_n : \mathbb{Z} \to \mathbb{Z}/3^n\mathbb{Z}\ \textbf{la surjection canonique}\ .$$

5) Montrer que pour tout $\frac{r}{s} \in V$, et tout $n \in \mathbb{N}^*$, $\pi_n(s)$ est inversible dans l'anneau $\mathbb{Z}/3^n\mathbb{Z}$.

6) Pour tout

$$\frac{r}{s} \in V \text{ et } \textbf{tout } n \in \mathbb{N}^*\ ,\ \textbf{on note } \pi'_n(\frac{r}{s}) := \pi_n(r)\pi_n(s)^{-1}\ .$$

a) Montrer que π'_n est un morphisme d'anneaux et que π'_n est surjectif.

b) Quel est le noyau de π'_n ?
Solution : *On sait déjà que $\mathrm{Ker}\,\pi'_n$ est un idéal de V et donc, d'après la question 4), c) qu'il existe $k \in \mathbb{N}$, tel que $\mathrm{Ker}\,\pi'_n = 3^k V$. Or $\pi'_n(3^n) = \pi_n(3^n) = 0$, donc $3^n \in \mathrm{Ker}\,\pi'_n$ d'où $k \leq n$.*
En outre $\frac{r}{s} \in \mathrm{Ker}\,\pi'_n$ entraîne

$$\pi_n(r)\pi_n(s)^{-1} = 0 \Rightarrow \pi_n(r)\pi_n(s)^{-1}\pi_n(s) = 0 \Rightarrow \pi_n(r) = 0 \Rightarrow 3^n|r\ .$$

Il en résulte que

$$\mathrm{Ker}\,\pi'_n 3^n V\ .$$

7) **a)** Quels sont les idéaux premiers de V ?

Solution : *On sait depuis la question 2) que V est intègre si bien que $\{0\}$ est un idéal premier dans V.*

On sait depuis la question 4), c) que les idéaux non nuls de V sont de la forme 3^nV et depuis la question 6), b) que ce sont le
noyaux respectifs des morphismes surjectifs π'_n. On a donc pour tout $n \in \mathbb{N}^*$, un isomorphisme d'anneaux $V/3^nV \cong \mathbb{Z}/3^n\mathbb{Z}$
Or l'idéal 3^nV est premier si et seulement si le quotient $V/3^nV$ est intègre i.e. si et seulement si $\mathbb{Z}/3^n\mathbb{Z}$ est intègre ce qui n'arriv
que pour $n = 1$.

Les idéaux premiers de V sont donc $\{0\}$ et $3V$.

b) Quels sont les idéaux maximaux de V ?

Solution : *On sait que les idéaux maximaux sont à chercher parmi les idéaux premiers. Or on a montré en a), que les idéau*
premiers de V sont $\{0\}$ et $3V$. On sait en outre que $\mathfrak{m}$ est un idéal maximal de V si et seulement si $V/\mathfrak{m}$ est un corps. C
$V/3V \cong \mathbb{Z}/3\mathbb{Z}$ qui est bien un corps. L'idéal $3V$ est donc maximal.

Comme $\{0\}$ est strictement inclus dans $3V$ il ne peut être maximal.

Le seul idéal maximal de V est donc $3V$.

c) Montrer que si $u \in V$ est inversible, u n'appartient à aucun des idéaux $\mathfrak{I} \neq V$ de V et en particulier n'appartient pa
à $3V$.

Solution :

$$\forall u \in V,\ u \in \mathfrak{I} \cap V^\times \Rightarrow \mathfrak{I} = V\ .$$

d) Quel est le groupe $V^\times$ des éléments inversibles de V ?

Solution : *Il résulte du point c) que $V^\times \subset V \setminus 3V$.*

Réciproquement si $\frac{r}{s}3V \notin$, $3 \not| r$, si bien que $\frac{s}{r} \in V$ et que par conséquent
$setin\frac{r}{s}V^\times$. On a finalement

$$V^\times = V \setminus 3V\ .$$

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Document n° I

17 mars 2020

n° I.1 . −Exercices à chercher

Dans aucun des trois groupes de TD les exercices d'applications du théorème de la base adaptée (théorème II.11.12) n'ont été traités lors des dernières séances. Nous vous proposons donc de chercher ces exercices (TD n° IV, exercice D et suivants,) dont un corrigé sera mis en ligne à la fin de la semaine.

n° I.2 . −Pour avancer dans le cours

Vous pouvez approfondir le cours consacré aux anneaux de polynômes. Néanmoins pour ceux pour qui son contenu serait déjà bien connu nous suggérons de commencer à étudier le chapitre IV du cours. Les paragraphes IV.2 et IV.3 comportent un certain nombre de notions sans doute déjà connues. Il est conseillé de se rapporter au paragraphe IV.1 au fil de la lecture lorsqu'on estimera que la notion de module peut éclairer la compréhension. Nous n'interdisons pas absolument l'étude systématique de ce paragraphe mais elle pourrait s'avérer ardue et formelle.

Enfin il est absolument nécessaire pour pouvoir aborder la suite du cours d'étudier attentivement le paragraphe IV.4 à propos duquel des exercices seront proposés en fin de semaine.

n° I.2.1 . −Approfondir le chapitre III

Dans le chapitre III, nombre de démonstrations ont été laissées en exercices. Ces exercices ont été regroupés au paragraphe III.7 du polycopié. Les exercices III.7.1 à III.7.8 donnent en particulier des preuves des résultats du cours. Il est conseillé de chercher ces exercices et de se reporter ensuite au corrigé ci-après pour vérifier ses résultats.

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 $n \in \mathbb{N}$. On reprends les notations données en III.1.2.

Exercice III.7.1 [Addition]

Pour tout $(a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, on définit l'élément $a +_{A^{\mathbb{N}}} b \in A^{\mathbb{N}}$ par $(a +_{A^{\mathbb{N}}} b)_n := a_n + b_n$.

Montrer que $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}})$ ainsi construit est un groupe abélien dont on précisera l'élément neutre z.

Solution :

*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.*

Dorénavant on notera simplement $+$ **pour** $+_{A^{\mathbb{N}}}$ **si aucune confusion n'est à craindre.**

Exercice III.7.2 [Multiplication]
Pour tout $(a,b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, **on définit** $a *_{A^{\mathbb{N}}} b$ **par**

$$(a *_{A^{\mathbb{N}}} b)_n \;:=\; \sum_{k=0}^{n} a_k * b_{n-k}\,.$$

Montrer que :

1) l'élément $\upsilon \in A^{\mathbb{N}}$ défini par

$$\upsilon_0 \;:=\; 1 \text{ et } \forall n \in \mathbb{N},\; n \geq 1 \;\Rightarrow\; \upsilon_n \;:=\; 0,$$

est un élément neutre pour $*_{A^{\mathbb{N}}}$;
Solution : *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

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

2)

$$\forall (a,b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\; a *_{A^{\mathbb{N}}} b \;=\; b *_{A^{\mathbb{N}}} a\,;$$

Solution :

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

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

3)

$$\forall (a,b,c) \in A^{\mathbb{N}} \times A^{\mathbb{N}} \times A^{\mathbb{N}},\; a *_{A^{\mathbb{N}}} (b +_{A^{\mathbb{N}}} c) \;=\; a *_{A^{\mathbb{N}}} b \;+_{A^{\mathbb{N}}}\; a *_{A^{\mathbb{N}}} c\,.$$

Solution :

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

De même on notera $*$ au lieu de $*_{A^{\mathbb{N}}}$ si aucune confusion n'est à craindre.

Exercice III.7.3 [Anneau] Énoncer et démontrer les propriétés de $+_{A^{\mathbb{N}}}$ et $*_{A^{\mathbb{N}}}$ qui font de

$$(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}) \text{ un anneau commutatif .}$$

Solution : *On a montré en III.7.1 que $(A, +_{A^{\mathbb{N}}})$ est un groupe abélien. Par ailleurs on a vue (cf. III.7.2.question 1),) que $*_{A^{\mathbb{N}}}$ possède un élément neutre v, (cf. III.7.2.question 2),) que $*_{A^{\mathbb{N}}}$ est commutative et (cf. III.7.2.question 3),) que $*_{A^{\mathbb{N}}}$ est distributive à gauche sur $+_{A^{\mathbb{N}}}$. Puisque $*_{A^{\mathbb{N}}}$ est commutative elle est en fait distributive.*

Il resterait à montrer que :

*i) (**Associativité**)*

$*_{A^{\mathbb{N}}}$ est associative pour assurer que $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ est un anneau commutatif. C'est une vérification fastidieuse mais sans réelle difficulté. En effet :

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

Exercice III.7.4 [Valuation]

1) Rappeler ce que signifie que l'anneau A est intègre.
Solution :

$$\forall (a, b) \in A \times A, \ a * b \ = \ 0 \ \Rightarrow \ a \ = \ 0 \ \vee \ b \ = \ 0$$

ou de manière équivalente que $\{0\}$ est un idéal premier.

On suppose, dans toute la suite de la III.7.4 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 $a_v \neq 0$.
Solution : *Puisque $a \neq \zeta, V := \{n \in \mathbb{N} \, ; \, a_n \neq 0\}$ est non vide et possède donc un plus petit élément v.*

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

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}, \ \mathrm{val}(a *_{A^{\mathbb{N}}} b) \ = \ \mathrm{val}(a) \ + \ \mathrm{val}(b) \ ;$$

Solution : *Si $b \ = \ \zeta, a * b \ = \ \zeta$ d'où*

$$\mathrm{val}(a * b) \ = \ (+\infty) \ = \ \mathrm{val}(a) + (+\infty) \ = \ \mathrm{val}(a) + \mathrm{val}(b) \ .$$

Si $a \neq \zeta$ et $b \neq \zeta$ pour tout $0 \leq n < \mathrm{val}(a) + \mathrm{val}(b)$,

$$(a *_{A^{\mathbb{N}}} b)_n \ = \ \sum_{k=0}^{n} a_k * b_{n-k} \ .$$

Or si $k < \mathrm{val}(a)$, $a_k = 0$, et donc $a_k * b_{n-k} = 0$. Si $k \geq \mathrm{val}(a)$, $n - k \leq n - \mathrm{val}(a) < \mathrm{val}(b)$ si bien que $b_{n-k} \ = \ 0$. Il s'ensuit que

$$\forall 0 \leq n < \mathrm{val}(a) + \mathrm{val}(b) \ , \ (a * b)_n \ = \ 0$$

ce qui entraîne, par définition même de $\mathrm{val}(\cdot)$,

$$\mathrm{val}(a*b) \;\geq\; \mathrm{val}(a)+\mathrm{val}(b)\;.$$

Enfin :

$$\begin{array}{rcl}
(a*b)_{\mathrm{val}(a)+\mathrm{val}(b)} & = & \displaystyle\sum_{k=0}^{\mathrm{val}(a)+\mathrm{val}(b)} a_k * b_{\mathrm{val}(a)+\mathrm{val}(b)-k} \\
& = & \displaystyle\sum_{k=0}^{\mathrm{val}(a)-1} a_k * b_{\mathrm{val}(a)+\mathrm{val}(b)-k} + a_{\mathrm{val}(a)} * b_{\mathrm{val}(b)} + \sum_{k=\mathrm{val}(a)+1}^{\mathrm{val}(a)+\mathrm{val}(b)} a_k * b_{\mathrm{val}(a)+\mathrm{val}(b)-k} \\
& = & a_{\mathrm{val}(a)} * b_{\mathrm{val}(b)} + \displaystyle\sum_{k=0}^{\mathrm{val}(b)-1} a_{\mathrm{val}(a)+\mathrm{val}(b)-k} * b_k \\
& = & a_{\mathrm{val}(a)} * b_{\mathrm{val}(b)} \\
& \neq & 0
\end{array}$$

si bien que

$$\mathrm{val}(a *_{A^{\mathbb{N}}} b) \;=\; \mathrm{val}(a) \;+\; \mathrm{val}(b)\;.$$

4) En déduire que $(A^{\mathbb{N}},\, +_{A^{\mathbb{N}}}\,,\, *_{A^{\mathbb{N}}}\,)$ est un anneau intègre.

Solution :

$$\begin{array}{lrcl}
\forall (a,b)\in A^{\mathbb{N}}\times A^{\mathbb{N}}, & a *_{A^{\mathbb{N}}} b & = & \zeta \\
\Rightarrow & \mathrm{val}(a *_{A^{\mathbb{N}}} b) & = & (+\infty) \\
\Rightarrow & \mathrm{val}(a) = (+\infty) & \vee & \mathrm{val}(b) = (+\infty) \\
\Rightarrow & a = \zeta & \vee & b = \zeta\;.
\end{array}$$

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 $\mathrm{val}(a)\neq\mathrm{val}(b)$.

Solution : *Si* $a=\zeta$, $a+b \;=\; b$ *si bien que*

$$\mathrm{val}(a+b) \;=\; \mathrm{val}(b) \;=\; \min(\mathrm{val}(b),(+\infty))\;.$$

Si $a\neq\zeta$ *et* $b\neq\zeta$, *pour tout* $0\leq n<\min(\mathrm{val}(a),\mathrm{val}(b))$, $n<\mathrm{val}(a) \;\Rightarrow\; a_n=0$, $n<\mathrm{val}(b) \;\Rightarrow\; b_n=0$ *si bien que* $(a+_{A^{\mathbb{N}}} b)_n \;=\; a_n+b_n \;=\; 0$. *Il s'ensuit donc que*

$$\mathrm{val}(a +_{A^{\mathbb{N}}} b) \;\geq\; \min(\mathrm{val}(a),\mathrm{val}(b))\;.$$

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.

Solution : *Tout d'abord* $\zeta\in\mathfrak{m}$ *puisque* $\mathrm{val}(\zeta) \;=\; (+\infty)>0$. *On a donc* $\mathfrak{m} \;\neq\; \emptyset$. *Par ailleurs,*

$$\begin{array}{ll}
\forall (x,y)\in\mathfrak{m}\times\mathfrak{m}, & \\
\forall (a,b)\in A^{\mathbb{N}}\times A^{\mathbb{N}}, \quad \mathrm{val}(a *_{A^{\mathbb{N}}} x +_{A^{\mathbb{N}}} b *_{A^{\mathbb{N}}} y) & \geq \min(\mathrm{val}(a *_{A^{\mathbb{N}}} x),\mathrm{val}(b *_{A^{\mathbb{N}}} y)) \\
& \geq \min(\mathrm{val}(a)+\mathrm{val}(x),\mathrm{val}(b)+\mathrm{val}(y)) \\
& > 0
\end{array}$$

c'est-à-dire que

$$a *_{A^{\mathbb{N}}} x \;+_{A^{\mathbb{N}}}\; b *_{A^{\mathbb{N}}} y \;\in\; \mathfrak{m}\;.$$

On peut aussi caractériser $\mathfrak{m}$ *comme l'ensemble des éléments* $a \;\in\; A^{\mathbb{N}}$ *tels que* $a_0 \;=\; 0$.

Exercice III.7.5 [Morphisme structural]

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

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

Montrer que l'application $i : A \to A^{\mathbb{N}}$ ainsi définie est un morphisme injectif d'anneaux.

Solution :

*i) (**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

$$i(a+b) = i(a) +_{A^{\mathbb{N}}} i(b) \text{ (cf. III.7.1 ;)}$$

c'est-à-dire que

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

est un morphisme de groupes.

ii) $(*_{A^{\mathbb{N}}})$

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

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

iii) $(1 \mapsto u)$

Par définition même de υ *(cf. III.7.2.question 1),) 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.

*iv) (**Injectivité**)*

Pour tout $a \in A$, $i(a) = z$, *entraîne que* $a = i(a)_0 = 0$ *ce qui assure l'injectivité de* i.

On note désormais

$$\mathcal{P} := \{a \in A^{\mathbb{N}}\,;\, \exists n \in \mathbb{N},\ \forall p \in \mathbb{N},\ p \geq n \Rightarrow a_p = 0\}$$

le sous-ensemble de $A^{\mathbb{N}}$ des suites « presque nulles » autrement dit dont le terme est nul à partir d'un certain rang.

Exercice III.7.6 [degré]

On suppose encore 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

$$a_d \neq 0 \text{ et } \forall n \in \mathbb{N},\ n > d \Rightarrow a_n = 0\,.$$

Solution : *Si* $a \neq \zeta$,

$$V := \{n \in \mathbb{N}\,;\, a_n \neq 0\} \neq \emptyset\,.$$

Si $a \in P$, *par hypotèse, il existe* $n \in \mathbb{N}$, *tel que* $V \subset [0;n]$. *Il en résulte que* V *admet un plus grand élément* d *qui répond à la question.*

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

$$\forall (a,b) \in \mathcal{P} \times \mathcal{P},\ \deg(a *_{A^{\mathbb{N}}} b) = \deg(a) + \deg(b)\ .$$

Solution : *Si* $b = \zeta$, $a * b = \zeta$ *d'où*

$$\deg(a * b) = (-\infty) = \deg(a) + (-\infty) = \deg(a) + \deg(b)\ .$$

Si $a \neq \zeta$ *et* $b \neq \zeta$ *pour tout* $n > \deg(a) + \deg(b)$,

$$(a *_{A^{\mathbb{N}}} b)_n = \sum_{k=0}^{n} a_k * b_{n-k}\ .$$

Or si $k > \deg(a)$, $a_k = 0$, *et donc* $a_k * b_{n-k} = 0$. *Si* $k \leq \deg(a)$, $n - k \geq n - \deg(a) > \deg(b)$ *si bien que* $b_{n-k} = 0$. *Il s'ensuit que*

$$\forall n > \deg(a) + \deg(b)\ ,\ (a * b)_n = 0$$

ce qui entraîne, par définition même de $\deg(\cdot)$,

$$\deg(a * b) \leq \deg(a) + \deg(b)\ .$$

Enfin :

$$\begin{aligned}
(a * b)_{\deg(a)+\deg(b)} &= \sum_{k=0}^{\deg(a)+\deg(b)} a_k * b_{\deg(a)+\deg(b)-k} \\
&= \sum_{k=0}^{\deg(a)-1} a_k * b_{\deg(a)+\deg(b)-k} + a_{\deg(a)} * b_{\deg(b)} + \sum_{k=\deg(a)+1}^{\deg(a)+\deg(b)} a_k * b_{\deg(a)+\deg(b)-k} \\
&= a_{\deg(a)} * b_{\deg(b)} \\
&\neq 0
\end{aligned}$$

si bien que

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

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 $\deg(a) \neq \deg(b)$.

Solution : *Si* $a = \zeta$, $a + b = b$ *si bien que*

$$\deg(a + b) = \deg(b) = \max(\deg(b), (-\infty))\ .$$

Si $a \neq \zeta$ *et* $b \neq \zeta$, *pour tout* $n > \max(\deg(a), \deg(b))$, $n > \deg(a) \Rightarrow a_n = 0$, $n > \deg(b) \Rightarrow b_n = 0$ *si bien que* $(a +_{A^{\mathbb{N}}} b)_n = a_n + b_n = 0$. *Il s'ensuit donc que*

$$\deg(a +_{A^{\mathbb{N}}} b) \leq \max(\deg(a), \deg(b))\ .$$

4) En déduire que $(\mathcal{P},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$ est un anneau commutatif intègre.

Solution :

*i) (**Groupe abélien**)*

Le point III.7.6.question 3) assure que $+_{A^{\mathbb{N}}}$ *se restreint à* $\mathcal{P}$ *et est donc une loi interne sur* $\mathcal{P}$. *Elle reste bien entendu associative. L'élément neutre* ζ *appartient à* $\mathcal{P}$ *et reste donc un élément neutre. Il est immédiat de constater que si* $a \in \mathcal{P}$, $-a \in \mathcal{P}$ *si bien que tout élément de* $\mathcal{P}$ *ppossède un opposé. Enfin la loi* $+_{A^{\mathbb{N}}}$ *étant commutative sur* $A^{\mathbb{N}}$ *le reste sur* $\mathcal{P}$. *Ceci fait de* $(\mathcal{P},\ +_{A^{\mathbb{N}}}\ )$ *un groupe abélien.*

*ii) (**Anneau commutatif**)*

Le point III.7.6.question 2) assure que la loi $*_{A^{\mathbb{N}}}$ *se restreint à* $\mathcal{P}$. *Elle reste associative, commutative, distributive sur* $+_{A^{\mathbb{N}}}$ *et l'élément neutre* u *appartient à* $\mathcal{P}$ *ce qui fait de* $(\mathcal{P},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$ *un anneau commuttatif.*

iii) ***(Intégrité)***

Pour tout $(a,b) \in \mathcal{P}\times\mathcal{P}$, a et b sont en particulier des éléments de $A^{\mathbb{N}}$ et si $a *_{A^{\mathbb{N}}} b = z$ on a vu en III.7.4.question 4) que $a = z$ ou $b = z$ ce qui assure que $\mathcal{P}$ est 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 III.7.4.question 6).)

Solution : *Tout d'abord $z \in \mathcal{P}$ et $z \in \mathfrak{m}$ donc*

$$z \in \mathfrak{m}_0 \Rightarrow \mathfrak{m}_0 \neq \emptyset\,.$$

Par ailleurs

$$\forall (x,y)\in\mathfrak{m}_0\times\mathfrak{m}_0,\ \forall (a,b)\in\mathcal{P}\times\mathcal{P},\ a*x+b*y \in \mathcal{P}$$

d'après les points III.7.6.question 3) et III.7.6.question 2). De plus $ax+by \in \mathfrak{m}$ puisque $\mathfrak{m}$ est un idéal de $A^{\mathbb{N}}$. Il s'ensuit que

$$a*x+b*y \in \mathcal{P}\cap\mathfrak{m} = \mathfrak{m}_0\,.$$

6) Montrer que pour tout $(a,b) \in \mathcal{P}\times\mathcal{P}$, si b divise a et $a \neq \zeta$, $\deg(b) \leq \deg(a)$

Solution : *Si $b|a$, il existe $c \in \mathcal{P}$ tel que $a = b*c$. Il résulte alors du point III.7.6.question 2) que $\deg(a) = \deg(b) + \deg(c)$. Or si $a \neq z, c \neq z$ si bien que $\deg(a), \deg(b)$ et $\deg(c)$ sont des entiers naturels ce qui assure le résultat.*

7) Montrer que l'image du morphisme i défini à la III.7.5, 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.

Solution : *Pour tout $a \in A$, il est clair que $i(a) \in \mathcal{P}$ et même que $\deg(i(a)) = 0$. Réciproquement si $a \in \mathcal{P}$ avec $\deg(a) = 0$, on a $i(a_0) = a$. Il s'ensuit que*

$$\operatorname{Im} i = \{a \in \mathcal{P}\,;\, \deg(a) = 0\}\,.$$

Les lois $+_{A^{\mathbb{N}}}$ et $*_{A^{\mathbb{N}}}$ sur $\mathcal{P}$ étant données par celles de $A^{\mathbb{N}}$ ainsi que les éléments neutre z et u, i reste un morphisme injectif d'anneaux à valeurs dans $\mathcal{P}$.

8) Montrer que la restriction $i^\times := i_{|A^\times}$ de i à l'ensemble $A^\times$ des éléments inversibles de A est un morphisme bijectif de groupes 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.*

Solution :

i) ***(Groupes des inversibles)***

Rappelons d'abord que, pour tout anneau $(R,+,*)$ l'ensemble $R^\times$ est un groupe pour la loi $*$. En effet si $(r,s)\in R^\times\times R^\times$, il existe $(t,u)\in R\times R$ tels que $r*t = t*r = 1$ et $s*u = u*s = 1$.Il s'ensuit que $r*s*u*t = 1$ et $u*t*r*s = 1$ si bien que $r*s \in R^\times$. Ainsi la loi $*$ se restreint à $R^\times$ en une loi interne.

L'élément neutre 1 pour $*$ étant son propre inverse, appartient bien entendu à $R^\times$ et est un élément neutre pour $*$ restreinte à $R^\times$.

Enfin si $r \in R^\times$, r possède, par définition un inverse s dans R. Puisque r est aussi l'inverse de s $s \in R^\times$, si bien que r possède un inverse dans $R^\times$.

ii) *($\operatorname{Im} i^\times \subset \mathcal{P}^\times$)*

POur tout $a \in A^\times$, il existe $b \in A^\times$ tel que $a*b = b*a = 1$. Il s'ensuit que

$$i(a*b) = i(b*a) = i(1) \Rightarrow i(a)*_{A^{\mathbb{N}}} i(b) = i(b)*_{A^{\mathbb{N}}} i(a) = u$$

c'est-à-dire que $i^\times(a) = i(a) \in \mathcal{P}^\times$.

iii) *($i^\times$* ***est un morphisme)***

$$\forall (a,b)\in A^\times\times A^\times,\ i^\times(a*b) = i(a*b) = i(a)*_{A^{\mathbb{N}}} i(b) = i^\times(a)\ *_{A^{\mathbb{N}}}\ i^\times(b)$$

du fait que i est un morphisme d'anneaux. Il s'ensuit que

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

est un morphisme de groupes.

*iv) (**Bijectivité de** $i^\times$)*
L'application $i^\times$ étant la restriction d'une application injective est encore injective.
Pour tout $a \in \mathcal{P}^\times$, il existe $b \in \mathcal{P}^\times$ tel que $a *_{A^{\mathbb{N}}} b = u$. Il en résulte que

$$\deg(a) + degb = \deg(u) = 0$$

ce qui entrraîne

$$\deg(a) = degb = 0 .$$

On a vu en III.7.6.question 7) que cela signifie que $a \in \operatorname{Im} i$ et $b \in \operatorname{Im} i$. Dans ce cas on a nécessairement

$$a = i(a_0) \text{ et } b = i(b_0) .$$

Il s'ensuit que

$$a * b = u \Rightarrow i(a_0) *_{A^{\mathbb{N}}} i(b_0) = i(1) \Rightarrow i(a_0 * b_0) = i(1) \Rightarrow a_0 * b_0 = 1$$

la dernière implication provenant du fait que i est un morphisme injectif. Il en résulte que $a_0 \in A^\times$ ce qui assure la surjectivité de $i^\times$.

Exercice III.7.7 [Division euclidienne]

1) Rappeler ce que signifie l'assertion : A est un corps.
Solution : *L'anneau A est un corps si tout élément non nul de A est inversible i.e.*

$$A^\times = A \setminus \{0\} .$$

On suppose, jusqu'à la fin de III.7.7 que A est un corps.
Soit $b \in \mathcal{P}, b \neq \zeta$.

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

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

Solution : *Il suffit de prendre*

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

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

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

Solution : *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 $c := a - b *_{A^{\mathbb{N}}} s$.

4) Montrer finalement que, pour tout $a \in \mathcal{P}$ il existe un unique $(q, r) \in \mathcal{P} \times \mathcal{P}$ tel que :

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

Solution :

*i) (**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 il découle de III.7.6.question 3) que

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

Or d'après III.7.6.question 6), 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.7.6.question 4),) $q_1 = q_2$.

ii) ***(existence)***

Pour $\deg(a) < \deg(b)$, *le résultat a été établi (cf. III.7.7.question 2).)*

Si $\deg(a) \geq \deg(b)$, *il existe (cf. III.7.7.question 3),)* (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 $q := s + t$.

Exercice III.7.8 [Théorème chinois des restes dans $\mathbb{K}[X]$]

Cet exercice particularise, au cas des anneaux de polynômes sur un corps, les résultats obtenus pour des anneaux généraux au TD n° II, exercice B, question 3), ou encore pour les anneaux principaux, dont $\mathbb{K}[X]$ est un cas particulier, en I.13.4.

Dans tout cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur 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.

Solution : *Il suffit de remarquer que*

$$\forall Q' \in \mathbb{K}[X], \ Q' \in Q \, mod \, P \Leftrightarrow Q' - Q \in P\mathbb{K}[X] .$$

2) Montrer que si P_1 et P_2 sont deux éléments premiers entre eux de $\mathbb{K}[X]$, leur PPCM est leur produit.

Solution : *Lemme de* GAUSS *(cf. III.5.2.3.)*

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 :

$$\begin{aligned} (\alpha_1, \alpha_2) + (\beta_1, \beta_2) &:= (\alpha_1 + \beta_1, \alpha_2 + \beta_2) \\ (\alpha_1, \alpha_2) * (\beta_1, \beta_2) &:= (\alpha_1 * \beta_1, \alpha_2 * \beta_2) . \end{aligned}$$

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 $+$.

Solution : *(cf. I.7.)*

b) Montrer que l'application

$$\begin{array}{rccc} \phi : & \mathbb{K}[X] & \to & \mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2 \\ & Q & \mapsto & (Q \bmod P_1, Q \bmod P_2) \end{array}$$

est un morphisme d'anneaux.

Solution : *(cf. I.7.)*

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 $\mathbb{K}[X] \to \mathbb{K}[X]/K$.

Solution :

$$\begin{array}{lrcl} \forall q \in \mathbb{K}[X], & Q & \in & \operatorname{Ker} \phi \\ \Leftrightarrow & Q \, mod \, P_1 = 0 & \text{et} & Q \, mod \, P_2 = 0 \\ \Leftrightarrow & Q & \in & P_1\mathbb{K}[X] \cap P_2\mathbb{K}[X] \\ \Leftrightarrow & \operatorname{Ker} \phi & = & P_1\mathbb{K}[X] \cap P_2\mathbb{K}[X] . \end{array}$$

Le morphisme ϕ *se factorise donc en*

$$\begin{array}{ccc} \mathbb{K}[X] & & \\ {\scriptstyle \pi}\downarrow & \searrow {\scriptstyle \phi} & \\ \mathbb{K}[X]/K & \xrightarrow{\gamma} & \mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2 \end{array}$$

(cf. I.8.)

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.

Solution : *Pour tout* $(\alpha_1, \alpha_2) \in \mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2$, *soit*

$$(Q_1, Q_2) \in \mathbb{K}[X] \times \mathbb{K}[X] \text{ tel que } \alpha_1 = Q_1 \bmod P_1 \text{ et } \alpha_2 = Q_2 \bmod P_2 .$$

Puisque P_1 *et* P_2 *sont premiers entre eux, il existe (cf. III.5.2.1,)*

$$(U_1, U_2) \in \mathbb{K}[X] \times \mathbb{K}[X] \text{ tel que } U_1P_1 + U_2P_2 = 1 .$$

Ceci se réécrit

$$U_{3-i}P_{3-i} \bmod P_i = 1 \bmod P_i \text{ et } U_{3-i}P_{3-i} \bmod P_{-i} = 0 \bmod P_{3-i} .$$

Il s'ensuit que

$$\begin{array}{rcccl} Q_2U_1P_1 + Q_1U_2P_2 \bmod P_1 & = & Q_1 \bmod P_1 & = & \alpha_1 \\ Q_2U_1P_1 + Q_1U_2P_2 \bmod P_2 & = & Q_2 \bmod P_2 & = & \alpha_2 ; \end{array}$$

si bien que $Q_2U_1P_1 + Q_1U_2P82$ *est un antécédent de* (α_1, α_2) *par* ϕ.

Le morphisme ϕ *est alors surjectif, ce qui entraîne que* γ *l'est, si bien que* γ *est un isomorphisme.*

Le noyau K *de* γ *est alors égale à*

$$\mathrm{PPCM}(P_1, P_2) = P_1P_2 .$$

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.

Solution : *Les hypothèses équivalent en fait au système de congruence :*

$$\left\{\begin{array}{rcl} P & \equiv & 1\,[(X-a)] \\ P & \equiv & 1\,[(X-b)] \end{array}\right\} .$$

Puisque $(X-a)$ *et* $(X-b)$ *sont premiers entre eux*

$$\big(\frac{1}{b-a}[(X-a)-(X-b)] = 1\big)$$

le théorème chinois des restes assure que l'ensemble des solutions de ce système est une classe de congruence modulo

$$\mathrm{PPCM}((X-a),(X-b)) = (X-a)(X-b) .$$

En utilisant les notations de l'exercice, les hypothèses se réécrivent également

$$\phi(P) = (1,1) = 1_{\mathbb{K}[X]/(X-a)\times\mathbb{K}[X]/(Xb)} .$$

Or γ *étant un morphisme d'anneaux,*

$$\gamma^{-1}(\phi(P)) = \gamma^{-1}(1) = 1_{\mathbb{K}[X]/(X-a)(X-b)}$$

ce qui équivaut encore à $\pi(P) = 1$, *ou encore*

$$P \equiv 1\,[(X-a)(X-b)]$$

i.e. le reste de la division euclidienne de P *par* $(X-a)(X-b)$ *est* 1.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Document n° II

20 mars 2020

Corrigé de certains exercices du TD n° IV

Exercice D : Soient

$$v_1 := (1,4,2,5)\,,\ v_2 := (3,7,11,6)\,,\ v_3 := (4,13,10,2)\,,\ v_4 := (5,11,9,7)$$

des éléments de $\mathbb{Z}^4$.

Déterminer le sous-groupe A de $\mathbb{Z}^4$ engendré par les éléments v_i ,$_{1\leq i\leq 4}$ c'est-à-dire donner une base adaptée pour A.

Solution : *Puisque l'anneau* $\mathbb{Z}$ *est euclidien, on peut mettre en œuvre l'algorithme d'*EUCLIDE–GAUSS *exposé en II.11.9 et II.11.10 :*

Considérons la matrice

$$V := \begin{pmatrix} 1 & 3 & 4 & 5 \\ 4 & 7 & 13 & 11 \\ 2 & 11 & 10 & 9 \\ 5 & 6 & 2 & 7 \end{pmatrix}$$

Nul besoin d'effectuer l'étape II.11.10.i).a) puisque $V_{1,1} = 1$ *est déjà l'élément de* V *de plus petite valeurs absolue. On passe donc à l'étape II.11.10.i).b) qui donne la matrice*

$$V_1 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & -5 & -3 & -9 \\ 2 & 5 & 2 & -1 \\ 5 & -9 & -18 & -18 \end{pmatrix} \text{ et } V_2 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -5 & -3 & -9 \\ 0 & 5 & 2 & -1 \\ 0 & -9 & -18 & -18 \end{pmatrix}.$$

On a ici déjà une matrice de la forme II.11.10.i).c).1 sans besoin d'opération supplémentaire.
La deuxième étape II.11.10.ii) n'est pas nécessaire non plus puisque $(V_2)_{1,1}$ *divise tous les coefficients de la matrice* 3×3

$$W_1 := \begin{pmatrix} -5 & -3 & -9 \\ 5 & 2 & -1 \\ -9 & -18 & -18 \end{pmatrix}.$$

On doit alors effectuer l'étape II.11.10.i).a) pour amener le coefficients $(W_1)_{2,3} = -1$ *en position* $1,1$ *qui donne la matrice*

$$W_2 := \begin{pmatrix} 1 & 5 & 2 \\ 9 & -5 & -3 \\ 18 & -9 & -18 \end{pmatrix}.$$

On a également enlevé les signes moins dans la première colonne de W_2*. En appliquant l'étape II.11.10.i).b) à* W_2*, on obtient*

$$W_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -50 & -21 \\ 0 & -99 & -54 \end{pmatrix}.$$

Une fois encore, le coefficient $(W_3)_{1,1}$ *étant égal à* 1*, l'étape II.11.10.ii) est automatiquement satisfaite et l'on peut désormais considérer la matrice*

$$Z_1 := \begin{pmatrix} 50 & 21 \\ 99 & 54 \end{pmatrix}.$$

L'étape II.11.10.i).a) donne alors

$$Z_2 := \begin{pmatrix} 21 & 50 \\ 54 & 99 \end{pmatrix};$$

puis l'étape II.11.10.i).b) donne

$$\begin{pmatrix} 21 & 8 \\ 54 & -9 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 21 & 8 \\ 12 & -25 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 8 & 21 \\ -25 & 12 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 8 & 5 \\ -25 & 62 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 8 & 5 \\ -1 & 77 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 1 & -77 \\ 8 & 5 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 1 & 0 \\ 8 & 621 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 621 \end{pmatrix}.$$

Exercice E : Déterminer à isomorphisme près les groupes abéliens de cardinal 300.

Solution : *On sait (cf. II.10.7,) que deux groupes abéliens de finis sont isomorphes si et seulement si ils ont les mêmes facteurs invariants. Autrement dit déterminer à isomorphismes près, ou encore déterminer les classes d'isomorphismes des groupes de cardinal* 300 *revient à déterminer les séquence* d_i ,$_{1\leq i\leq r}$ *de facteurs invariants correspondant à des groupes abéliens de cardinal* 300. *Or on a alors pour un tel groupe* A,

$$\#(A) = \prod_{i=1}^{r} d_i .$$

En écrivant $300 = 2^2 * 3 * 5^2$, *on a nécessairement* $r \leq 2$. *On a également*

$$2 * 3 * 5 | d_1 .$$

$r = 2$ *Correspond aux groupes*

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \, , \; \mathbb{Z}/150\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ et } \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} .$$

$r = 1$ *correspond au groupe* $\mathbb{Z}/300\mathbb{Z}$.
On a donc déterminé 4 *classes d'isomorphismes pour les groupes abéliens de cardinal* 300.

Exercice F : Cet exercice reprend les étapes de l'étude des sous-groupes d'un groupe abélien libre de type fini de manière effective.

Soit A **le groupe abélien libre** $\mathbb{Z}^2$ **et** B **le sous-groupe de** A **engendré par les éléments** $b_1 = (-4, 12)$ **et** $b_2 = (-8, 12)$**. On désire calculer les facteurs invariants (diviseurs élémentaires) de** A/B**.**

1) Donner un homomorphisme f de A dans $\mathbb{Z}$ tel que l'image de B soit maximale.
Solution : *Soit* f *un morphisme de* A *dans* $\mathbb{Z}$, *l'image de* B *est de la forme* $n\mathbb{Z}$ *puisque c'est un sous-groupe de* $\mathbb{Z}$.
Puisque l'image de B *est engendrée par* $(f(b_1) = 4f(-1, 3), f(b_2) = 4f(-3, 3)$ *elle est donc contenue dans* $4\mathbb{Z}$.
Soit f *tel que* $f(1, 0) = 1$ *et* $f(0, 1) = 0$. *Alors* $f(b_1) = -4$, $f(b_2) = -12$, *donc* $f(B) = 4\mathbb{Z}$. *Ce* f *répond à la question.*

2) On note d un générateur de $f(B)$. Donner un élément a_2 de A tel que da_2 soit dans B et tel que $f(a_2) = 1$.
Solution : *On a donc* $d = 4$. *On peut prendre* $a_2 = (1, -3)$.

3) Calculer une base a_1 du noyau de f. Calculer l'intersection B' du noyau de f avec B et exprimer un générateur de B' d'une part en fonction de a_1 et d'autre part dans le système générateur de B.
Solution : *On a* $a_1 = (0, 1)$. *L'intersection du noyau de* f *et de* B' *est donné par l'équation* $xb_1 + yb_2 = za_1$ *avec* x, y, z *des entiers, c'est-à-dire* $-4x - 8y = 0$, $12x + 12y = z$. *Donc* $x = -2y$, $z = -12y$. *Une base de* B' *est donc donnée par* $2b_1 - b_2 = 12a_1$.

4) Calculer les facteurs invariants de A/B.

Solution : *On a trouvé une base (a_1, a_2) de A telle que $(12a_1, 4a_2)$ soit une base de B.*
Les facteurs invariants de A/B sont donc $(12, 4)$.
Remarquons que le déterminant de $\begin{pmatrix} -4 & 12 \\ -8 & 12 \end{pmatrix}$ est $48 = 4 \times 12$ et que le groupe A/B est d'ordre 48.

Exercice G : **1)** Soit $A = \mathbb{Z}^2$ et B le sous-groupe de A engendré par $b_1 = (14, 2)$ et $b_2 = (2, 4)$. Calculer une base de A adaptée à B. Donner la structure du quotient A/B.

Solution : *Si $f : A \to \mathbb{Z}$ est un morphisme de groupes, il vérifie nécessairement $f(B) \subset 2\mathbb{Z}$. Réciproquement, si on prend f définie par $f(x, y) = x$, on a $f(B) \supset 2\mathbb{Z}$, donc $f(B) = 2\mathbb{Z}$. On a $f(b_2) = 2$ et si $a_2 = (1, 2)$, $b_2 = 2a_2$ et $f(a_2) = 1$. On en déduit que*

$$A = < a_2 > \oplus \operatorname{Ker} f \, .$$

Pour trouver le second élément de la base, calculons $\operatorname{Ker} f \cap B$.
Il s'agit de trouver les solutions dans $\mathbb{Z}$ de $(0, y) = ub_1 + vb_2$, ce qui est équivalent à

$$\begin{cases} 0 = & 14u + 2v \\ y = & 2u + 4v \end{cases} \Leftrightarrow \begin{cases} 0 = & 7u + v \\ y = & 2u + 4v \end{cases} \Leftrightarrow \begin{cases} v = & -7u \\ y = & -26u \end{cases}$$

Ce qui a une solution en y si et seulement si 26 divise y.
Soit $a_1 = (0, 1)$. On a $26a_1 = -b_1 + 7b_2$.
Donc (a_1, a_2) est une base adaptée de A puisque $26a_1, 2a_2$ est une base de B et que $2|26$.
Le quotient A/B est isomorphe à $\mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2) Soit G un groupe abélien (noté additivement) et possédant deux générateurs a et b tels que

$$14a \, + \, 2b \, = \, 0_G \text{ et } 2a \, + \, 4b \, = \, 0_G \, .$$

Montrer que G est isomorphe à un quotient d'un groupe d'ordre 52 dont on donnera la structure.

Solution : *Soit*

$$\varphi \, : \, A \, := \, \mathbb{Z}^2 \, \to \, G$$

l'homomorphisme surjectif $(x, y) \mapsto xa + yb$. Le noyau de φ contient le sous-groupe de A engendré par b_1 et b_2, noté B dans la question précédente. Par le théorème de factorisation, φ se factorise en un homomorphisme de $G_1 = A/B$ sur G et G est isomorphe au quotient de G_1 par le sous-groupe $\operatorname{Ker} \varphi/B$. On peut alors utiliser les résultats de la question précédente.

Exercice H : Soit $e_1 = (a_1, \ldots, a_n)$ un élément de $\mathbb{Z}^n$ tel que le **Pgcd** des a_i vaille 1 [9]
Montrer qu'il existe une base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$ dont le premier vecteur est e_1.
Que peut-on dire du quotient $\mathbb{Z}^n/\mathbb{Z}e_1$?
Adapter l'exercice en ne supposant plus que le **Pgcd** vaut 1.

Solution : *Notons f_i la base canonique de $\mathbb{Z}^n$. Le pgcd des a_i étant 1, il existe des entiers u_i tel que $\sum_{i=1}^n u_i a_i = 1$. Soit φ l'homomorphisme de groupes $\mathbb{Z}^n \to \mathbb{Z}$ tel que $\varphi(f_i) = u_i$. On a donc explicitement $\varphi(\sum_{i=1}^n x_i f_i) = \sum_{i=1}^n x_i u_i$. L'image de e_1 par φ est 1. Donc φ est surjective. Soit $B := \operatorname{Ker} \varphi$ son noyau. Tout élément v de $\mathbb{Z}^n$ est la somme d'un élément de B et d'un multiple de e_1 (en effet, si $\varphi(v) = m \in \mathbb{Z}$, $v - me_1$ appartient à B) et $B \cap \mathbb{Z}e_1 = \{0\}$. Comme B est un sous-groupe d'un groupe libre de type fini, il est libre et admet une base $(e_2, \cdots, e_n)$. Alors, $(e_1, \cdots, e_n)$ est une base de $\mathbb{Z}^n$.*

Le quotient $\mathbb{Z}/\mathbb{Z}e_1$ est libre de rang $n - 1$. Si le pgcd des a_i vaut d, soit $a_i' = a_i/d$. On peut appliquer ce qui précède aux $e_1' = (a_i')$. Il existe une base de $\mathbb{Z}^n$ dont le premier vecteur est e_1'. Le $\mathbb{Z}$-module $\mathbb{Z}e_1$ a alors comme base de_1'. Donc le quotient $\mathbb{Z}^n/\mathbb{Z}e_1$ est isomorphe à $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}^{n-1}$.

9. Un tel vecteur est dit *primitif* et un certain nombre d'autres propriétés des vecteurs primitifs sont étudiées dans le cours en C.1.3.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Document n° III

23 mars 2020

On se propose, dans cette séance de prouver le théorème de CAYLEY–HAMILTON (cf. cours IV.7.2.)

La preuve, ou plutôt les preuves, du théorème sont présentées sous forme d'exercices au paragraphe n° III.1 afin que vous puissiez les chercher. Les solutions de ces exercices sont données dans le paragraphe n° III.2 afin que vous puissiez vous y reporter ensuite.

N'hésitez surtout pas à poser toutes vos questions à vos enseignants par les moyens mis à votre disposition.

Bon travail ! (P.L.)

n° III.1 . −Le théorème de CAYLEY–HAMILTON

On peut donner une preuve relativement élémentaire du théorème de CAYLEY–HAMILTON dans le cas où (E, u) est un *espace cyclique* (cf. exercice A à exercice C.)
On donne en particulier (cf. exercice A,) d'autres caractérisations équivalentes à celles déjà données des espaces cycliques (cf. cours IV.4.1.)

Cependant, si l'on veut déduire le cas général du théorème de CAYLEY–HAMILTON du cas particulier des espaces cycliques, il faudrait pouvoir décomposer tout espace en somme directe de sous-espaces cycliques. Un tel résultat est fourni par le théorème de réduction de FROBENIUS (cf. cours IV.11.5) vers lequel un premier pas est fait à l' TD n° VI, exercice D.

On peut cependant donner une preuve directe du théorème de CAYLEY–HAMILTON sans y avoir recours (cf. exercice D.)

Exercice A : (Endomorphismes cycliques)
Soient $\mathbb{K}$ un corps, $d \in \mathbb{N}^*$ un entier et E un $\mathbb{K}$-espace vectoriel de dimension d.
Pour $u \in \mathrm{End}_{\mathbb{K}}(E)$ montrer que les assertions suivantes sont équivalentes :

Cyc$_1$) Il existe $x \in E$ tel que la famille $u^i(x)_{\,0 \leq i \leq d-1}$ est libre.

Cyc$_2$) Il existe $x \in E$ tel que la famille $u^i(x)_{\,0 \leq i \leq d-1}$ est une base.

Cyc$_3$) Il existe une base $\mathcal{B} := e_{i\,,1\leq i\leq d}$ de E, un d-uplet $a_{i\,,0\leq i\leq d-1} \in \mathbb{K}$ d'éléments de $\mathbb{K}$, tels que la matrice $C = (C_{i,j})_{\substack{1 \leq i \leq d \\ 1 \leq j \leq d}}$ de u dans la base $\mathcal{B}$ est telle que :

Comp$_1$)
$$\forall 1 \leq j \leq d-2,\ \forall j+2 \leq i \leq d,\ C_{i,j} = 0\,;$$

Comp$_2$)
$$\forall 1 \leq j \leq d-1,\ C_{j+1,j} = 1\,;$$

Comp$_3$)
$$\forall 1 \leq j \leq d-1,\ \forall 1 \leq i \leq j,\ C_{i,j} = 0\,;$$

Comp$_4$)
$$\forall 1 \leq i \leq d,\ C_{i,d} = -a_{i-1}\,.$$

Autrement dit C est une *matrice compagnon i.e.* de la forme :

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix} .$$

Définition A.1 Si u vérifie les propriétés Cyc_1) à Cyc_3), on dira que E est un *espace cyclique* pour u (cf. cours IV.4.2.)

Exercice B : (Polynôme caractéristique d'une matrice compagnon)

Soient $\mathbb{K}$ un corps et $d \in \mathbb{N}^*$ un entier.

Pour $a_{i\ ,0\leq i\leq d-1} \in \mathbb{K}^d$, on note $A_{(a_0,\dots,a_{d-1})}$ la matrice

$$A_{(a_0,\dots,a_{d-1})} := \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

et à tout $\lambda \in \mathbb{K}$, on associe

$$\Delta_{(a_0,\dots,a_{d-1})}(\lambda) := \det(\lambda \text{Id} - A_{(a_0,\dots,a_{n-1})}) .$$

1) **a)** Calculer $\Delta_{(a_0,\dots,a_{d-1})}(\lambda)$ en fonction de $\Delta_{(a_1,\dots,a_{d-1})}(\lambda)$ et a_0.

b) Calculer $\Delta_{(a_0,\dots,a_{d-1})}(\lambda)$ en fonction de $\Delta_{(a_0,\dots,a_{d-2})}(\lambda)$ et a_{d-1}.

2) Déduire de l'une des deux formules précédentes $\Delta_{(a_0,\dots,a_{d-1})}(\lambda)$.

Exercice C : (Théorème de CAYLEY–HAMILTON pour les espaces cycliques)

Soient $\mathbb{K}$ un corps, $d \in \mathbb{N}^*$ un entier et $f \in \text{End}_{\mathbb{K}}(E)$ est tel que E est un espace cyclique pour f. Le d-uplet $a_{i\ ,0\leq i\leq d-1}$ étant donné par le point exercice A, Cyc_3), on note

$$P := X^d + \sum_{i=0}^{d-1} a_i X^i \in \mathbb{K}[X] .$$

1) Montrer que P est un polynôme annulateur de f.

2) Montrer que le degré n du polynôme minimal $P_{\min f}$ de f est supérieur ou égal à d.

3) En déduire finalement que $P_{\min f} = P$.

Exercice D : (Théorème de CAYLEY–HAMILTON et formules de CRAMER)

Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice carrée de taille $n \in \mathbb{N}^*$ à coefficients dans un corps commutatif $\mathbb{K}$. Soit P le polynôme caractéristique de A. On veut prouver le théorème de CAYLEY–HAMILTON pour A à savoir $P(A) = 0$.

On note 1_n la matrice identité de taille n dans $\mathcal{M}_n(\mathbb{K})$. On considère la matrice

$$B := X \cdot 1_n - A \in \mathcal{M}_n(\mathbb{K}[X])$$

à coefficients dans l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$. Le polynôme P est le déterminant de B. On note C la matrice adjointe de B c'est-à-dire la matrices des cofacteurs de B qui est telle, en vertu des formules de CRAMER, que

$$B \cdot C = C \cdot B = \det(B) \cdot 1_n .$$

1) Montrer qu'il existe un unique $n-1$-uplet $C_{i\ ,1\leq i\leq n-1}$ de matrices dans $\mathcal{M}_n(\mathbb{K})$ tel que :

$$C = X^{n-1} \cdot 1_n + \sum_{i=1}^{n-1} X^{n-1-i} \cdot C_i . \qquad 1$$

2) En posant

$$P \ := \ X^n \ + \ \sum_{i=1}^{n} a_i X^{n-i} \, ,$$

prouver les égalités :

$$\begin{array}{rcl} -A + C_1 & = & a_1 \cdot 1_n \\ -A \cdot C_k + C_{k+1} & = & a_{k+1} \cdot 1_n \\ -A \cdot C_{n-1} & = & a_n \cdot 1_n \end{array}$$

pour tout $1 \ \leq \ k \ \leq \ n-2$.

3) En déduire que $P(A) \ = \ 0$.

4) En tirer le théorème de CAYLEY–HAMILTON (cf. cours IV.7.2,) pour un endomorphisme u d'un $\mathbb{K}$-espace vectoriel de dimension n.

n° III.2 . −Solution des exercices

Exercice A : (Endomorphismes cycliques)
Soient $\mathbb{K}$ un corps, $d \ \in \ \mathbb{N}^*$ un entier et E un $\mathbb{K}$-espace vectoriel de dimension d.

Pour $u \ \in \ \mathrm{End}_{\mathbb{K}}(E)$ montrer que les assertions suivantes sont équivalentes :

Cyc$_1$) Il existe $x \ \in \ E$ tel que la famille $u^i(x)_{\,0 \ \leq \ i \ \leq \ d-1}$ est libre.

Cyc$_2$) Il existe $x \ \in \ E$ tel que la famille $u^i(x)_{\,0 \ \leq \ i \ \leq \ d-1}$ est une base.

Cyc$_3$) Il existe une base $\mathcal{B} \ := \ e_{i\,,1 \leq i \leq d}$ de E, un d-uplet $a_{i\,,0 \leq i \leq d-1} \ \in \ \mathbb{K}$ d'éléments de $\mathbb{K}$, tels que la matrice $C \ = \ (C_{i,j})_{\substack{1 \ \leq \ i \ \leq \ d \\ 1 \ \leq \ j \ \leq \ d}}$ de u dans la base $\mathcal{B}$ est telle que :

Comp$_1$)
$$\forall 1 \leq j \leq d-2, \ \forall j+2 \leq i \leq d, \ C_{i,j} \ = \ 0 \, ;$$

Comp$_2$)
$$\forall 1 \leq j \leq d-1, \ C_{j+1,j} \ = \ 1 \, ;$$

Comp$_3$)
$$\forall 1 \leq j \leq d-1, \ \forall 1 \leq i \leq j, \ C_{i,j} \ = \ 0 \, ;$$

Comp$_4$)
$$\forall 1 \leq i \leq d, \ C_{i,d} \ = \ -a_{i-1} \, .$$

Autrement dit C est une *matrice compagnon i.e.* de la forme :

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix} .$$

Définition A.1 Si u vérifie les propriétés Cyc$_1$) à Cyc$_3$), on dira que E est un *espace cyclique* pour u (cf. cours IV.4.2.)

Solution :

*i) (**Cyc$_1$) $\Leftrightarrow$ Cyc$_2$**))*
Le fait que Cyc$_2$) entraîne Cyc$_1$) est tautologique.
Réciproquement s'il existe $x \ \in \ E$ tel que la famille $f^i(x)_{\,0 \ \leq \ i \ \leq \ n-1}$ est libre comme son cardinal est n qui est aussi la dimension de E, cette famille est une base.

*ii) (**Cyc$_2$**) $\Rightarrow$ **Cyc$_3$**))*

Soit $x \in E$, tel que $f^i(x)_{\,0 \le i \le d-1}$ est une base. Posons $\forall 1 \le i \le d,\ e_i := f^{i-1}(x)$. On a alors

$$\forall 1 \le i \le d-1,\ f(e_i) = f[f^{i-1}(x)] = f^i(x) = e_{i+1}\,.$$

Par ailleurs $f(e_d)$ est un élément de E qui se décompose dans la base $e_{i\,,1\le i\le d}$ c'est-à-dire qu'il existe un unique d-uplet $a_{i\,,0\le i\le d-1}$ tel que

$$f(e_d) = \sum_{i=1}^{d} a_{i-1}e_i = \sum_{i=1}^{d} a_{i-1}f^{i-1}(e_1)\,.$$

La matrice M de f dans la base $\mathcal{B} := e_{i\,,1\le i\le d}$ a alors la forme spécifiée par les points Cyc$_3$).Comp$_1$) à Cyc$_3$).Comp$_4$) :

$$M = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

*iii) (**Cyc$_3$**) $\Rightarrow$ **Cyc$_2$**))*

S'il existe une base $e_{i\,,1\le i\le d}$ dans laquelle la matrice de f a la forme spécifiée par les points Cyc$_3$).Comp$_1$) à Cyc$_3$).Comp$_4$),

$$\forall 1 \le i \le d-1,\ f(e_i) = e_{i+1} \Rightarrow e_i = f^{i-1}(e_1)$$

si bien que e_1 satisfait à la condition Cyc$_2$).

Exercice B : (Polynôme caractéristique d'une matrice compagnon)

Soient $\mathbb{K}$ un corps et $d \in \mathbb{N}^*$ un entier.

Pour $a_{i\,,0\le i\le d-1} \in \mathbb{K}^d$, on note $A_{(a_0,\dots,a_{d-1})}$ la matrice

$$A_{(a_0,\dots,a_{d-1})} := \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

et à tout $\lambda \in \mathbb{K}$, on associe

$$\Delta_{(a_0,\dots,a_{d-1})}(\lambda) := \det(\lambda \mathrm{Id} - A_{(a_0,\dots,a_{n-1})})\,.$$

1) a) Calculer $\Delta_{(a_0,\dots,a_{d-1})}(\lambda)$ en fonction de $\Delta_{(a_1,\dots,a_{d-1})}(\lambda)$ et a_0.

b) Calculer $\Delta_{(a_0,\dots,a_{d-1})}(\lambda)$ en fonction de $\Delta_{(a_0,\dots,a_{d-2})}(\lambda)$ et a_{d-1}.

2) Déduire de l'une des deux formules précédentes $\Delta_{(a_0,\dots,a_{d-1})}(\lambda)$.

Exercice C : (Théorème de CAYLEY–HAMILTON pour les espaces cycliques)

Soient $\mathbb{K}$ un corps, $d \in \mathbb{N}^*$ un entier et $f \in \mathrm{End}_{\mathbb{K}}(E)$ est tel que E est un espace cyclique pour f. Le d-uplet $a_{i\,,0\le i\le d-1}$ étant donné par le point exercice A, Cyc$_3$), on note

$$P := X^d + \sum_{i=0}^{d-1} a_i X^i \in \mathbb{K}[X]\,.$$

1) Montrer que P est un polynôme annulateur de f.

Solution : *Ceci revient à montrer que*

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

Puisque $P(f)$ est un endomorphisme de E? il suffit de montrer, $e_{i\,,1\le i\le n}$ étant une base de E, que $\forall 1 \le i \le n,\ P(f)(e_i) = 0$. Prenons précisément pour base la base e_i donnée par le point exercice A, Cyc$_3$) associée au d-uplet $a_{i\,,0\le i\le d-1}$ définissant P. On a alors :

i) ($P(f)(e_1)$)

$$\begin{aligned} P(f)(e_1) &= f^d(e_1) - \sum_{i=0}^{d-1} a_i f^i(e_1) \\ &= f(e_d) - \sum_{i=0}^{d-1} a_i e_i \\ &= 0\,. \end{aligned}$$

ii) $(P(f)(e_i))$
On peut d'abord remarquer que $f \circ P(f) \;=\; P(f) \circ f$ *et que, par conséquent,* $\forall k \in \mathbb{N},\; f^k \circ P(f) \;=\; P(f) \circ f^k$.
Ainsi $\forall 2 \leq i \leq d$,

$$\begin{aligned} P(f)(e_i) &= P(f)[f^{i-1}(e_1)] \\ &= f^{i-1}[P(f)(e_1)] \\ &= f^{i-1}(0) \\ &= 0\,. \end{aligned}$$

2) Montrer que le degré n du polynôme minimal $P_{\min f}$ de f est supérieur ou égal à d.
Solution : *Notons*

$$P_{min\,f} \;=\; X^n + \sum_{i=0}^{n-1} b_i X^i \;\in\; \mathbb{K}[X]$$

le polynôme minimal de f. *Alors*

$$\forall x \in E,\; P_{min\,f}(f)(x) \;=\; 0$$

et en particulier pour un élément x *vérifiant exercice A, Cyc*$_1$*) :*

$$P_{min\,f}(f)(x) \;=0 \;\Leftrightarrow\; f^n(x) + \sum_{i=0}^{n-1} f^i(x) \;=\; 0$$

qui signifie que la famille $f^i(x)\,,0 \leq i \leq n$ *est liée. Or* $f^i(x)\,,0 \leq i \leq d-1$ *étant libre,* $n \geq d$.

3) En déduire finalement que $P_{\min f} \;=\; P$.
Solution : *On a montré à la question 1) que* $P_{min\,f}$ *divise* P. *Or* $\deg(P) \;=\; n$ *et* $\deg(P_{min\,f}) \;\geq n$ *comme* P *et* $P_{min\,f}$ *sont unitaires,*

$$P \;=\; P_{min\,f}\,.$$

Exercice D : (Théorème de CAYLEY–HAMILTON et formules de CRAMER)
Soit $A \;\in\; \mathcal{M}_n(\mathbb{K})$ **une matrice carrée de taille** $n \;\in\; \mathbb{N}^*$ **à coefficients dans un corps commutatif** $\mathbb{K}$. **Soit** P **le polynôme caractéristique de** A. **On veut prouver le théorème de CAYLEY–HAMILTON pour** A **à savoir** $P(A) \;=\; 0\,.$
On note 1_n **la matrice identité de taille** n **dans** $\mathcal{M}_n(\mathbb{K})$. **On considère la matrice**

$$B \;:=\; X \cdot 1_n - A \;\in\; \mathcal{M}_n(\mathbb{K}[X])$$

à coefficients dans l'anneau $\mathbb{K}[X]$ **des polynômes à une indéterminée à coefficients dans** $\mathbb{K}$. **Le polynôme** P **est le déterminant de** B. **On note** C **la matrice adjointe de** B **c'est-à-dire la matrices des cofacteurs de** B **qui est telle, en vertu des formules de CRAMER, que**

$$B \cdot C \;=\; C \cdot B \;=\; \det(B) \cdot 1_n\,.$$

1) Montrer qu'il existe un unique $n-1$-uplet $C_i\,,1 \leq i \leq n-1}$ de matrices dans $\mathcal{M}_n(\mathbb{K})$ tel que :

$$C \;=\; X^{n-1} \cdot 1_n \;+\; \sum_{i=1}^{n-1} X^{n-1-i} \cdot C_i\,. \qquad 1$$

Solution : *Notons* $C \;=\; (\gamma_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$. *Alors* $\forall 1 \leq i \leq n,\; \forall 1 \leq j \leq n,\; \gamma_{i,j}$ *est un déterminant calculé sur* $n-1$ *lignes et* $n-1$ *colonnes de* B *si bien que c'et un polynôme de degré inférieur ou égal à* $n-1$. *Il existe donc* $\gamma_{i,j,k}\,,0 \leq k \leq n-1}$ *tels que*

$$\forall 1 \leq i \leq n,\; \forall 1 \leq j \leq n,\; \gamma_{i,j} \;=\; \sum_{k=0}^{n-1} \gamma_{i,j,k} X^{n-1-k}\,.$$

Posons alors

$$C_k \;:=\; (\gamma_{i,j,k})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \;\in\; \mathcal{M}_n(\mathbb{K})\,.$$

On a alors

$$C \;=\; \sum_{k=0}^{n-1} X^{n--1-k} \cdot C_k$$

qui est presque la formule 1 à ceci près qu'il faut encore établir que $C_0 \;=\; 1_n$.
Pour $i \neq j$, *le cofacteur* $\gamma_{i,j}$ *correspond à la matrice* B *dont on a enlvé la ligne* i *et la colonne* j, *et c'est donc un polynôme de degré au plus* $n-2$, *si bien que* $\gamma_{i,j,0} \;=\; 0$. *On constate ensuite que* $\gamma_{i,i,0} \;=\; 1$.

2) En posant

$$P \;:=\; X^n \;+\; \sum_{i=1}^{n} a_i X^{n-i}\,,$$

prouver les égalités :

$$\begin{array}{rcl} -A + C_1 & = & a_1 \cdot 1_n \\ -A \cdot C_k + C_{k+1} & = & a_{k+1} \cdot 1_n \\ -A \cdot C_{n-1} & = & a_n \cdot 1_n \end{array}$$

pour tout $1 \;\leq\; k \;\leq\; n-2$.

Solution : *La matrice C étant la matrice des cofacteurs de B, on a*

$$B \cdot C \;=\; C \cdot B \;=\; \det(B) \cdot 1_n \;=\; P \cdot 1_n\,.$$

Ce qui s'écrit encore :

$$\begin{array}{rcl} (X \cdot 1_n - A) \cdot C & = & P \cdot 1_n \\ \Leftrightarrow \quad (X \cdot 1_n - A) \cdot \big(X^{n-1} \cdot 1_n + \sum_{i=1}^{n-1} X^{n-1-i} \cdot C_i\big) & = & \big(X^n + \sum_{i=1}^{n} a_i X^{n-i}\big) \cdot 1_n\,. \end{array}$$

En utilisant que $X^i\,,_{\in \mathbb{N}}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]$, on obtient :

$$\begin{array}{rcl} X^{n-1} \cdot (-A + C_1) & = & a_1 X^{n-1} \cdot 1_n \\ \Rightarrow \qquad (-A + C_1) & = & a_1 \cdot 1_n \\ X^{n-i} \cdot (C_i - A \cdot C_{i-1}) & = & a_i X^{n-i} \cdot 1_n \;\forall 2 \leq i \leq n-1, \\ \Rightarrow \qquad C_i - A \cdot C_{i-1} & = & a_i \cdot 1_n \;\forall 2 \leq i \leq n-1, \\ -A \cdot C_{n-1} & = & a_n \cdot 1_n\,. \end{array}$$

3) En déduire que $P(A) \;=\; 0$.

Solution : *On a :*

$$\begin{array}{rcl} P(A) & = & A^n + \sum_{i=1}^{n} a_i \cdot A^{n-i} \\ & = & A^n + \sum_{i=1}^{n} A^{n-i} \cdot a_i \cdot 1_n \\ & = & A^n + A^{n-1} \cdot (-A + C_1) + \sum_{i=2}^{n-1} A^{n-i} \cdot (-A \cdot C_{i-1} + C_i) - A \cdot C_{n-1} \\ & = & A^{n-1} \cdot C_1 - \sum_{i=2}^{n-1} A^{n+1-i} \cdot C_{i-1} + \sum_{i=2}^{n-1} A^{n-i} \cdot C_i - A \cdot C_{n-1} \\ & = & A^{n-1} \cdot C_1 + \sum_{i=2}^{n-1} A^{n-i} \cdot C_i - \big(\sum_{i=1}^{n-2} A^{n-i} \cdot C_i + A \cdot C_{n-1}\big) \\ & = & \sum_{i=1}^{n-1} A^{n-i} \cdot C_i - \sum_{i=1}^{n-1} A^{n-i} \cdot C_i \\ & = & 0\,. \end{array}$$

4) En tirer le théorème de CAYLEY–HAMILTON (cf. cours IV.7.2,) pour un endomorphisme u d'un $\mathbb{K}$-espace vectoriel de dimension n.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Document n° IV

27 mars 2020

n° IV.1 . – TD n° IV

Exercice C : (**Structure des groupes finis(cf. TD n° VII, exercice C.)**)

1) Parmi les groupes suivants, lesquels sont isomorphes (vous devez justifier votre réponse) :

$$\begin{aligned} G_1 =& \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \\ G_2 =& \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ G_3 =& \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ G_4 =& (\mathbb{Z}/25\mathbb{Z})^\times \times \mathbb{Z}/5\mathbb{Z} \end{aligned}$$

Lesquels sont cycliques ?

Solution : *Même si dans certains cas simples d'autres arguments peuvent être utilisés, (nombre d'éléments, ordre des éléments . . . ,) le corollaire II.10.7 du cours apporte toujours une réponse systématique à la question des classes d'isomorphismes de groupes abéliens. Cependant, pour pouvoir lutiliser, il faut connaître les facteurs invariants du groupe et pour cela déterminer sa décomposition canonique (cf. cours II.10.5.i).)*

G_1 *Ainsi le groupe* $G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ *n'est pas décomposé sous sa forme canonique, puisque*

$$4 \not| 25 \text{ et } 25 \not| 4 .$$

Cependant le théorème chinois des restes assure que

$$G_1 \cong \mathbb{Z}/100\mathbb{Z}$$

qui est une décomposition canonique de paramètres $r = 1$ *et* $d_1 = 100$. *Ce groupe est cyclique.*

G_2 *De même* $G_2 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ *n'est pas donné non plus sous sa forme canonique, laquelle est, en vertu du théorème chinois des restes*

$$G_2 \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \text{ de paramètres } r = 2 , \ d_1 = 10 \text{ et } d_2 = 10 .$$

Ce groupe n'est pas cyclique.

G_3 *Par les mêmes arguments que ci-dessus,*

$$G_3 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \text{ de paramètres } r = 2 , \ d_1 = 20 \text{ et } d_2 = 5$$

qui n'est pas non plus cycliques.

G_4 *Il faut déterminer* $(\mathbb{Z}/25\mathbb{Z})^\times$ *qui est un groupe à* 20 *éléments ; ce qui ne donne pas sa structure. Néanmoins, on peut remarquer que*

$$2^{10} = 1024 \equiv -1 \ [25] .$$

Ainsi l'o'rdre de 2 *dans* $(\mathbb{Z}/25\mathbb{Z})^\times$ *divise* 20 *mais ne divise pas* 10. *C'est donc* 4 *ou* 20. *Or*

$$2^4 \equiv 16 \neq 1 \ [25],$$

si bien que 2 *est d'ordre* 20 *et que, par conséquent,*

$$(\mathbb{Z}/25\mathbb{Z})^\times \cong \mathbb{Z}/20\mathbb{Z}$$

et que finalement

$$G_4 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \cong G_3 .$$

Aucun des groupes G_1, G_2, G_3 *ne sont isomorphes entre eux puisque leurs séquences de paramètres sont toutes deux à deux distinctes.*

2) Combien y a-t-il de classes d'isomorphismes de groupes abéliens de cardinal 1400 et possédant au moins un sous-groupe non cyclique d'ordre une puissance de 2 ? Donner leurs invariants (ou diviseurs élémentaires).

Solution : $1400 = 2^3 \times 5^2 \times 7$.

On sait que si G est un groupe abélien avec $\#(G) = 1400$, et si

$$G \cong \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \text{ avec } \forall 1 \leq i \leq r-1,\ d_{i+1}|d_i,$$

$$1400 = \#(G) = \prod_{i=1}^{r} d_i\ .$$

Si donc p est un nombre premier tel que $p|\#(G)$ il existe $1 \leq i \leq r$ tel que $p|d_i$ ce qui entraîne $p|d_1$. Ainsi on a

$$(2 * 5 * 7)|d_1\ .$$

Il en résulte aussi que $i \leq v_p(\#(G))$, ce qui entraîne finalement

$$r \leq \max_{p \in \mathbb{P}}(v_p(\#(G))) \text{ i.e. } r \leq 3\ .$$

$r = 1$

$$G_1 \cong \mathbb{Z}/1400\mathbb{Z}\,;$$

Or G_1 est cyclique est tous ses sous-groupes le sont donc ; il n'a donc pas de sous-groupe non cyclique, a fortiori de cardinal une puissance de 2.

$r = 2$

$$\begin{array}{rcl} & G_2 & \cong \mathbb{Z}/700\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \text{ou} & G_3 & \cong \mathbb{Z}/280\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \text{ou} & G_4 & \cong \mathbb{Z}/140\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}\,. \end{array}$$

Le groupe $\mathbb{Z}/700\mathbb{Z}$, (resp. $\mathbb{Z}/140\mathbb{Z}$,) (resp. $\mathbb{Z}/10\mathbb{Z}$,) est cyclique de cardinal divisible par 2 et possède donc un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Il en résulte que G_2 et G_4, possèdent des sous-groupes isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i.e. non cycliques d'ordre une puissance de 2.
En revanche, si H est un sous-groupe de G_3, de cardinal 2^k, pour tout

$$(x, y) \in H\ ,\ x \in \mathbb{Z}/280\mathbb{Z}\ ,\ y \in \mathbb{Z}/5\mathbb{Z},$$

$$0 = 2^k(x, y) = (2^k x, 2^k y)\ ;$$

si bien que $2^k y = 0$, ce qui entraîne $y = 0$, puisque 2^k est inversible dans l'anneau $\mathbb{Z}/5\mathbb{Z}$. Il s'ensuit que H est alors isomorphe à un sous-groupe de $\mathbb{Z}/280\mathbb{Z}$ et par conséquent cyclique.

$r = 3$

$$\begin{array}{rcl} & G_5 & \cong \mathbb{Z}/70\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \text{ou} & G_6 & \cong \mathbb{Z}/350\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,. \end{array}$$

Pour les raisons déjà données plus haut, G_5 et G_6 ont un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3) Soient r, s et t trois entiers positifs. On désire calculer en fonction de r, s et t les invariants $(d_1, d_2, \ldots, d_k)$ du groupe abélien

$$A := \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z}\,.$$

a) Que vaut d_1 ?

Solution : *Si on écrit A sous sa forme canonique*

$$A = \prod_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z} \text{ avec } \forall 1 \leq i \leq k-1,\ d_{i+1}|d_i,$$

pour tout $x \in A$, $d_1 x = 0$, si bien que d_1 divise l'exposant de A. Par ailleurs, $\mathbb{Z}/d_1\mathbb{Z}$ contient un élément d'ordre d_1 et par conséquent A contient un élément d'ordre d_1, si bien que d_1 est exactement l'exposant de A.
Or si

$$A = \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z},$$

*l'exposant de A est le **Ppcm** de r, s et t.*

b) Calculer de deux manières le nombre d'éléments d'ordre divisant d_k et montrer que $k \leq 3$ et que d_3 est le **Pgcd** de r, s et t.

Solution : *On sait que* $\forall a \in \mathbb{N},\ , \forall d \in \mathbb{N},\ ,$ *le sous-groupe* $\mathbb{Z}/a\mathbb{Z}[d]$ *de* $\mathbb{Z}/a\mathbb{Z}$ *des éléments de* d*-torsion i.e. dont l'ordre divise* d*, est isomorphe à* $\mathbb{Z}/(a \wedge d)\mathbb{Z}$.

Par ailleurs pour G *et* H *des groupes abéliens*

$$(x, y) \ \in \ (G \times H)[d] \ \Leftrightarrow \ x \ \in \ G[d] \text{ et } y \ \in \ H[d] \, ;$$

si bien que

$$(G \times H)[d] \ \cong \ G[d] \times H[d] \, .$$

Il en résulte que, d'une part :

$$\begin{aligned} \#(A[d_k]) &= \#\big((\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z})[d_k]\big) \\ &= \#\big(\mathbb{Z}/(r \wedge d_k)\mathbb{Z} \times \mathbb{Z}/(s \wedge d_k)\mathbb{Z} \times \mathbb{Z}/(t \wedge d_k)\mathbb{Z}\big) \\ &= (r \wedge d_k) * (s \wedge d_k) * (t \wedge d_k) \, . \end{aligned}$$

d'autre part :

$$\begin{aligned} \#(A[d_k]) &= \#\big(\prod_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}[d_k]\big) \\ &= \#\big(\prod_{i=1}^{k} \mathbb{Z}/(d_i \wedge d_k)\mathbb{Z}\big) \\ &= d_k^k \, . \end{aligned}$$

On obtient donc

$$d_k^k \ = \ \#(A[d_k]) \ = \ (r \wedge d_k) * (s \wedge d_k) * (t \wedge d_k) \, .$$

Puisque $(u \wedge d_k) \ \leq \ d_k$ *pour* $u \ = \ r, s, \text{ ou } t$, $d_k^k \ \leq d_k^3$ *donc* $k \ \leq \ 3$.

Si $k < 3$, d_3 *n'est a priori pas défini par le théorème II.10.5.i) ; cependant on peut prolonger la suite* d_i *en posant* $d_i \ = \ 1$ *pour tout* $i > k$. *On a donc toujours alors la relation*

$$\forall i \in \mathbb{N},\ d_{i+1} | d_i \, .$$

On a encore

$$\#\big(A[d_3]\big) \ = \ d_3^3 \ = \ (d_3 \wedge r) * (d_3 \wedge s) * (d_3 \wedge t) \, .$$

Or

$$\forall u \ = \ r \, , \ s \text{ ou } t \, , \ ((d_3 \wedge u)) | d_3$$

si bien que

$$\forall u \ = \ r \, , \ s \text{ ou } t \, , \ d_3 \ = \ (u \wedge d_3) \, ;$$

et finalement

$$\forall u \ = \ r \, , \ s \text{ ou } t \, , \ d_3 | u \, .$$

On en conclut que d_3 *divise le* ***Pgcd*** *de* r, s, *et* t.

Soit d *le* ***Pgcd*** *de* r, s *et* t. *Alors*

$$\forall u \ = \ r \, , \ s \text{ ou } t \, , \ (d \wedge u) \ = \ d \, .$$

Il s'ensuit que

$$\#\big(A[d]\big) \ = \ (d \wedge r) * (d \wedge s) * (d \wedge t) \ = \ d^3 \, .$$

Par ailleurs

$$d^3 \ = \ \#\big(A[d]\big) \ = \ (d \wedge d_1) * (d \wedge d_2) * (d \wedge d_3) \, ;$$

ce qui entraîne $d | d_i$.

c) Montrer que

$$d_2 \ = \ \mathrm{PPCM}\big((r \wedge s), (s \wedge t), (t \wedge r)\big) \, .$$

Solution : *Il suffit de montrer que*

$$\frac{rst}{\textbf{\textit{Pgcd}}(r, s, t)\textbf{\textit{Ppcm}}(r, s, t)} \ = \ \textbf{\textit{Ppcm}}\big((r \wedge s), (s \wedge t), (t \wedge r)\big) \, .$$

4) Montrer que si A et B sont des groupes abéliens finis et

$$A \times A \cong B \times B, \text{ alors } \cong AB .$$

Solution : *Écrivons la décomposition canonique (cf. cours II.10.5.i))*

$$A = \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \text{ avec } \forall 1 \leq i \leq r-1,\ d_{i+1}|d_i .$$

On a alors

$$A \times A \cong \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}/d_i\mathbb{Z} .$$

Posons alors

$$\rho := 2r \text{ et } \forall 1 \leq i \leq r,\ \delta_{2i-1} = \delta_{2i} = d_i .$$

On a alors

$$A \times A \cong \prod_{i=1}^{\rho} \mathbb{Z}/\delta_i\mathbb{Z}$$

qui est bien la décomposition canonique de $A \times A$, puisque

$$\forall 1 \leq i \leq \rho - 1,\ \delta_{i+1}|\delta_i .$$

On en conclut ainsi, grâce à l'énoncé d'unicité II.10.5.ii), que si $A \times A$ et $B \times B$ ont même décomposition canonique, il en est de même pour A et B.

n° IV.2 . −Corrigé des exercices du TD n° V

Exercice A : Soit A un anneau commutatif intègre.

1) Montrer que A est un corps si et seulement si $A[X]$ est principal.

Solution : *Dans le cas où A est un corps on a vu (cf. cours III.4.2,) que $A[X]$ est un anneau euclidien donc principal. Réciproquement supposons que $A[X]$ est principal. Montrons d'abord que :*

*i) (**L'idéal engendré par X est maximal**)*

En effet si $\mathfrak{I}$ est un idéal contenant $XA[X]$, puisque A est principal, il existe $P \in A[X]$ tel que $\mathfrak{I} = PA[X]$. Ainsi $P|X$; ce qui entraîne, A étant un anneau intègre, (cf. cours III.2.2.ii),) que $0 \leq \deg(P) \leq 1$.

$\deg(P) = 0$ Dans ce cas,, posons $P = a, a \in A$. De plus $\exists Q \in A[X]$, tel que $aQ = X$. Il résulte toujours de III.2.2.ii) que $\deg(Q) = 1$, et qu'on peut donc écrire

$$Q = bX + c\ ,\ (b,c) \in A \times A .$$

Il en résulte que

$$X = abX + ac\ ;$$

ce qui entraîne (cf. cours III.2.5.v),) que

$$ab = 1 \text{ et } c = 0 .$$

En particulier

$$a \in A^{\times}\ ,\ P = a \text{ et } \mathfrak{I} = A .$$

$\deg(P) = 1$ Il existe donc

$$(a,b) \in A \times A \text{ tel que } P = aX + b \text{ et } Q \in A[X] \text{ tel que } X = PQ .$$

Or $\deg(Q) = 0$, i.e. $Q = c, c \in A$ et

$$acX + bc = X \Rightarrow b = 0 \text{ et } ac = 1 \Rightarrow \mathfrak{I} = XA[X] .$$

ii) $(A[X]/XA[X] \cong A)$

Il suffit de constater que $XA[X]$ est le noyau du morphisme d'anneaux $A[X] \to A$ qui a un polynôme associe son coefficient de degré 0.

Finalement si $A[X]$ est principal, $XA[X]$ est maximal et $A \cong A[X]/XA[X]$ est donc un corps.

2) En déduire que $A[X,Y]$ et $\mathbb{Z}[X]$ ne sont pas principaux.

Solution : *Puisque $A[X,Y] = A[X][Y]$, pour qu'il soit principal il faudrait, d'après la question précédente, que $A[X]$ soit un corps. Or (cf. cours III.2.5.iii),) $A[X]^\times = A^\times$ au moins dans le cas où A est intègre. X ne sra donc pas inversible dans $A[X]$ si bien que $A[X]$ n'est pas un corps. Dans le cas où A ne serait même pas intègre, la situation n'aura pas tendance à s'améliorer, puisqu'alors $A[X]$ ne sera lui-même pas intègre et a fortiori donc pas un corps.*

On sait bien que $\mathbb{Z}$ n'est pas un corps et que $\mathbb{Z}[X]$ ne peut donc être principal.

Exercice B : (Idéaux maximaux, polynômes irréductibles)

Soit A un anneau commutatif.

1) Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme à une indéterminée à coefficients dans $\mathbb{K}$. Montrer que l'idéal $P\mathbb{K}[X] := \{P * Q\ ,\ Q \in \mathbb{K}[X]\}$ est maximal si et seulement si P est irréductible.

Solution : *On a établi dans le cours, grâce au théorème de Bézout dans l'anneau $\mathbb{K}[X]$ que le quotient $\mathbb{K}[X]/P\mathbb{K}[X]$ est un corps si et seulement si P est irréductible.*

On peut aussi, procéder sans intermédiaire comme suite : Si P est irréductible, P ne divise pas 1 autrement dit

$$1 \notin P\mathbb{K}[X] \Rightarrow P\mathbb{K}[X] \neq \mathbb{K}[X]\,.$$

Par ailleurs, d'après le lemme d'Euclide P est premier si bien que pour tout $Q \notin \mathbb{K}[X]$, P et Q sont premiers entre eux. Il s'ensuit qu'il existe, en vertu du théorème de Bézout un couple $(U,V) \in \mathbb{K}[X] \times \mathbb{K}[X]$, tel que $PU + QV = 1$. Ceci assure alors que $P\mathbb{K}[X]$ est maximal.

2) Montrer que le résultat de la question 1) se généralise à n'importe quel anneau principal, à savoir que si A est un anneau principal, un idéal $\mathfrak{I}$ de A est maximal si et seulement s'il existe un élément irréductible $p \in A$ tel que $\mathfrak{I} = Ap$.

3) Dans cette question $A := \mathbb{Z}[X]$ l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{Z}$.

a) Déterminer l'ensemble $A^\times$ des éléments inversibles de A.

Solution : *Pour tout $P \in A$, P est inversible si et seulement s'il existe $Q \in A$ tel que $P * Q = 1$. Comme $\mathbb{Z}$ est un anneau intègre,*

$$P * Q = 1 \Rightarrow \deg(P) + \deg(Q) = 0 \Rightarrow \deg(P) = \deg(Q) = 0\,.$$

Il existe donc $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ tel que $P = a$ et $Q = b$. D'où $ab = 1$ c'est-à-dire que a et b sont des éléments inversibles de $\mathbb{Z}$. On a donc

$$A^\times = \mathbb{Z}^\times = \{-1, 1\}\,.$$

b) Vérifier que le polynôme $X^2 + 1 \in A$ est irréductible.

Solution : *Soient $(P,Q) \in A \times A$, tel que $P * Q = X^2 + 1$. Puisque $\mathbb{Z}$ est un anneau intègre, $\deg(P) + \deg(Q) = 2$. Étant donnés les rôles symétriques joués par P et Q on est amené à considérer les situations suivantes :*

*i) ($\deg(P) = 0$ **et** $\deg(Q) = 2$)*

Dans ce cas, on peut écrire

$$P = a \text{ et } Q = bX^2 + cX + d\,.$$

Alors

$$P * Q = X^2 + 1 \Rightarrow a * d = 1 \Rightarrow a \in \mathbb{Z}^\times \Rightarrow P \in A^\times\,.$$

ii) ($\deg(P) = \deg(Q) = 1$)

Dans ce cas on peut écrire

$$P = aX + b \text{ et } Q = cX + d\,.$$

On a alors

$$X^2 + 1 = acX^2 + (ad + bc)X + cd \Rightarrow \left\{\begin{array}{rcl} ac & = & 1 \\ ad + bc & = & 0 \\ cd & = & 1\,. \end{array}\right\}$$

On peut donc, sans perte de généralité, écrire

$$P = X - a \text{ et } Q = X - b\,,\ (a,b) \in \mathbb{Z} \times \mathbb{Z}\,.$$

Il s'ensuit alors que a et b sont des racines de $X^2 + 1$, or ce polynôme n'a pas de racine dans $\mathbb{Z}$ puisque

$$\forall a \in \mathbb{Z},\ a^2 + 1 \geq 1\,.$$

Il ressort donc des points i) et ii) que

$$\forall (P,Q) \in A \times A,\ P * Q \ = \ X^2+1 \ \Rightarrow \ P \ \in \ A^\times \text{ ou } Q \ \in \ A^\times$$

c'est-à-dire que X^2+1 est irréductible.

c) Montrer que, pour tout $P \ \in \ A$, il existe un unique couple $(Q,R) \in A \times A$ tel que

$$P \ = \ Q * (X^2+1) \ + \ R \text{ et } \deg(R) \ \leq \ 1 \, .$$

Solution :

*i) (**Unicité**)*
Le raisonnement est ici exactement le même que dans le cas de $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps.

*ii) (**Existence**)*
On peut envisager deux preuves différentes :

$*$) tout d'abord P et X^2+1 étant des éléments de $\mathbb{Q}[X]$, il existe $(Q,R) \in \mathbb{Q}[X] \times \mathbb{Q}[X]$ tel que $P \ = \ Q*(X^2+1) + R$. On peut ensuite montrer que Q et R sont en fait dans A mais cela revient en fait presque à faire la démonstration directement comme suit :

†) On démontre ce résultat par récurrence sur le degré de P.
$\deg(P) \ \leq \ 1$ *Dans ce cas $Q \ = \ 0$ et $R \ = \ P$ répond à la question.*
$\deg(P) > 1$ *On écrit alors $P \ := \ \sum_{i=0}^{d} a_i X^i$. Posons alors*

$$P_1 \ := \ P - a_d X^{d-2}(X^2+1) \ = \ \sum_{i=0}^{d-3} a_i X^i + (a_{d-2} - a_d) X^{d-2} + a_{d-1} X^{d-1} \, .$$

En particulier $\deg(P_1) \leq d-1$. En faisant l'hypothèse de récurrence convenable il existe alors $(Q_1,R) \in A \times A$ tel que

$$P_1 \ = \ (X^2+1)Q_1 + R \text{ et } \deg(R) \ \leq \ 1 \, .$$

Il s'ensuit que

$$P \ = \ P_1 + a_d X^{d-2}(X^2+1) \ = \ (a_d X^{d-2} + Q_1) * (X^2+1) + R \, .$$

Posons donc finalement $Q \ := \ (a_d X^{d-2} + Q_1$ qui répond à la question.

Dans la suite on a toujours $A \ = \ \mathbb{Z}[X]$, p est un nombre premier,

$$I \ := \ (X^2+1) * A \ = \ \{(X^2+1) * P \, , \ P \ \in \ A\} \, , \ J \ := \ \{(X^2+1) * P + p * Q \, , \ (P,Q) \in A \times A\} \, .$$

4) et l'on suppose de plus que $p \ = \ 7$. On note alors $\mathbb{F}_7 \ := \ (\mathbb{Z}/7\mathbb{Z}, +, *)$ le corps à 7 éléments et $\mathbb{F}_7[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{F}_7$.

a) Montrer que le polynôme X^2+1 est irréductible dans $\mathbb{F}_7[X]$.
Solution : *On se trouve ici encore dans l'une des deux situations question 3), b).i) ou question 3), b).ii) c'est-à-dire que si X^2+1 n'est pas irréductible il possède une racine dans $\mathbb{F}_7$. Or les carrés dans $\mathbb{F}_7$ sont*

$$1^2 \ = \ 1 \, , \ 2^2 \ = \ -3 \ = \ 3^2 \ = \ 2$$

si bien que -1 n'est pas un carré dans $\mathbb{F}_7$ ce qu'on peut d'ailleurs aussi déduire du fait que 7 n'est pas congru à 1 modulo 4.

b) On note $k \ := \ \mathbb{F}_7[X]/(X^2+1) * \mathbb{F}_7[X]$. Montrer qu'on a un isomorphisme

$$A/J \ \cong \ k$$

et en déduire que J est maximal dans A.
Solution :

i) ($\phi \ : \ A \ \to \ k$)
La surjection canonique $\pi_7 \ : \ \mathbb{Z} \ \to \ \mathbb{F}_7$ induit un morphisme surjectif d'anneaux

$$\Pi_7[X] \ : \ A \ = \ \mathbb{Z}[X] \ \to \ \mathbb{F}_7[X] \, , \ X \ \mapsto \ X \, .$$

Notons $\pi_k \ : \ \mathbb{F}_7[X] \ \to \ k$ la surjection canonique si bien qu'on obtient un morphisme surjectif d'anneaux :

$$\phi \ := \ \pi_k \ \circ \ \pi_7 \ : \ A \ \to \ k \, .$$

ii) ($\mathrm{Ker}\,\phi$)
On montre que $\mathrm{Ker}\,\phi = J$ *ce qui donnne l'existence d'un isomorphisme*

$$\psi : A/J \cong k$$

tel que $\psi \circ \pi_J = \phi$ *où* $\pi_J : A \to A/J$ *est la surjection canonique.*

iii) Il en résulte que A/J *est un corps et donc que* J *est un idéal maximal.*

Exercice C : (**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**

$$\pi : \mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X] \text{ la surjection canonique.}$$

Montrer que :

1) $\mathbb{K}[X]/P\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel ;
Solution : *L'anneau* $\mathbb{K}[X]$ *est au moins un groupe abélien et l'idéal* $P\mathbb{K}[X]$ *un sous-groupe si bien que le morphisme* $\pi : \mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X]$ *est au moins un morphisme de groupes (cf. cours I.8.) C'est cependant également un morphisme d'anneaux.*
L'inclusion naturelle $\mathbb{K} \hookrightarrow \mathbb{K}[X]$ *(cf. cours III.2.5.ii),) est un morphisme d'anneaux, si bien que la composée*

$$\mathbb{K} \to \mathbb{K}[X]/P\mathbb{K}[X] \text{ est encore un morphisme d'anneaux}$$

faisant de $\mathbb{K}[X]/P\mathbb{K}[X]$ *une* $\mathbb{K}$*-algèbre (cf. cours A.1.6,) et donc un* $\mathbb{K}$*-module (cf. cours A.1.1,) i.e. un* $\mathbb{K}$*-espace vectoriel.*
Plus explicitement la loi externe sur $\mathbb{K}[X]/P\mathbb{K}[X]$ *est donnée par*

$$\forall (a, Q) \in \mathbb{K} \times \mathbb{K}[X],\ a \cdot Q \bmod P = aQ \bmod P\ ;$$

2)

$$\big(\pi(1), \pi(X), \ldots, \pi(X^{\deg(P)-1})\big) \text{ en est une base ;}$$

Solution : *Notons* $E := \mathbb{K}[X]/P\mathbb{K}[X]$. *Pour tout* $\alpha \in E$, *il existe donc* $Q \in \mathbb{K}[X]$ *tel que* $\alpha = \pi(Q)$. *Or en effectuant la division euclidienne de* Q *par* P, *on prouve l'existence de* $R \in \mathbb{K}[X]$ *tel que*

$$\pi(R) = \alpha \text{ et } \deg(R) < \deg(P)\ .$$

Ceci prouve que l'ensemble

$$\{\pi(1), \ldots, \pi(X^{\deg(P)-1})\} = \{1 \bmod P, \ldots, X^{\deg(P)-1} \bmod\}$$

est générateur du $\mathbb{K}$*-espace vectoriel* E.
Pour $a_{i\ ,0\leq i\leq \deg(P)-1} \in \mathbb{K}$, *des éléments de* $\mathbb{K}$,

$$\sum_{i=0}^{\deg(P)-1} a_i X^i \bmod P = 0,$$

si et seulement si

$$\sum_{i=0}^{\deg(P)-1} a_i X^i \in \mathrm{Ker}\,\pi$$

si et seulement si

$$P \Big| \sum_{i=0}^{\deg(P)-1} a_i X^i$$

ce qui entraîne

$$\forall 0 \leq i \leq \deg(P) - 1,\ a_i = 0$$

et assure que $\{1 \bmod P, \ldots, X^{\deg(P)-1} \bmod P\}$ *est une partie libre du* $\mathbb{K}$*-espace vectoriel* E.

3)

$$\text{par conséquent } \dim_{\mathbb{K}} \mathbb{K}[X]/P\mathbb{K}[X] = \deg(P)\ .$$

Exercice D : (Le critère d'Eisenstein)

Soit A un anneau principal et p un élément irréductible de A. On note $\pi : A \to \kappa := A/p$ la surjection canonique et $\pi[X] : A[X] \to \kappa[X]$ le morphisme entre les anneaux de polynômes qui s'en déduit (qui consiste à réduire les coefficients modulo p.) On note $\mathbb{K}$ le corps des fractions de A. On pourra ne considérer que le cas où $A = \mathbb{Z}$ et $\mathbb{K} = \mathbb{Q}$.

Soit $P := X^n + a_{n-1}X^{n-1} + \cdots a_1.X + a_0 \in A[X]$ un polynôme unitaire non constant à coefficients dans A.

On note v_p les valuations p-adiques (cf. I.14.9,'III.7.11.)

On dit que P est *p-Eisenstein* si les deux conditions suivantes sont vérifiées :

i) Pour tout $i \leq n-1$, p divise a_i (*i.e.* $v_p(a_i) > 0$.)

ii) p^2 ne divise pas a_0 (*i.e.* $v_p(a_0) = 1$.)

1) Montrer que pour tout $P \in A[X]$, tout $Q \in A[X]$, P est p-Eisenstein et $Q|P$ entraîne $\pi[X](Q) = \pm X^{\deg(Q)}$.

Solution : *Si $Q|P$ il existe $R \in A[X]$ tel que $P = Q * R$. Or $\overline{P} = \overline{Q} * \overline{R}$ c'est-à-dire que $\overline{Q}|\overline{P}$. Or si P vérifie †, $\overline{P} = X^{\deg(P)}$. On a donc*

$\overline{Q}*\overline{R} = X^{\deg(P)}$. Or $\deg(X) = 1$ entraîne X irréductible (cf. III.5.2.6.) On peut allors utiliser l'unicité dans la proposition III.5.5.1 pour assurer qu'il existe des entiers a et b avec $a + b = \deg(P)$ tels que $\overline{Q} = X^a$ et $\overline{R} = X^b$.

En écrivant enfin $P = Q * R$ dans $A[X]$, (avec $Q = \sum_{i=0}^{\deg(Q)} b_i X^i$ et $R = \sum_{i=0}^{\deg(R)} c_i X^i$,) on a en particulier $a_{\deg(P)} = b_{\deg(Q)} c_{\deg(R)}$ ce qui entraîne, si P vérifie †, que $b_{\deg(Q)}$ est inversible i.e.vaut ± 1 et donc que $\overline{b}_{\deg(Q)} = \pm 1$. Il en résulte finalement que

$$\deg(\overline{Q}) = \deg(Q) \text{ et } \overline{Q} = X^{\deg(Q)} = X^{\deg(\overline{Q})} .$$

2) Pour tout

$$P \in A[X] \, , \; Q := \sum_{i=0}^{\deg(Q)} b_i X^i \in A[X] \, , \; R := \sum_{i=0}^{\deg(R)} c_i X^i \in A[x],$$

montrer que $P = Q * R$, P est p-Eisenstein $\deg(Q) > 0$, $\deg(R) > 0$ entraîne $v_p(b_0) > 0$ et $v_p(c_0) > 0$.

Solution : *D'après question 1) $P = Q * R$ et P satisfait † entraîne $\overline{Q} = X^{\deg(Q)}$ et $\overline{R}^{\deg(R)}$. Ceci entraîne*

$$\forall 0 \leq i \leq \deg(Q) - 1, \; v_p(b_i) > 0 \text{ et } \forall 0 \leq i \leq \deg(R) - 1, \; v_p(c_i) > 0 \, .$$

Ceci entraîne bien entendu si $\deg(Q) > 0$ et $\deg(R) > 0$,

$$v_p(b_0) > 0 \text{ et } v_p(c_0) > 0 \, .$$

3) Déduire de ce qui précède que pour $P \in A[X]$, P est p-Eisenstein entraîne P est irréductible.

Solution : *Il résulte de question 2) que $P = Q * R$, P satisfait †, $\deg(Q) > 0$, $\deg(R) > 0$, entraîne $v_p(b_0) > 0$ et $v_p(c_0) > 0$. On a alors*

$$v_p(a_0) = v_p(b_0 * c_0) = v_p(b_0) + v_p(c_0) > 1$$

(cf. I.14.9.question 2), Val_5).) Le fait que P satisfait † entraîne donc, par contraposée, que

$$\deg(Q) = 0 \text{ ou } \deg(R) = 0 \Rightarrow \big(\deg(Q) = 0 \text{ et } b_0 | a_{\deg(P)} \big) \text{ ou } \big(\deg(R) = 0 \text{ et } c_0 | a_{\deg(P)} \big)$$

c'est-à-dire, comme $a_{\deg(P)} = 1$, que Q ou r est inversible, donc que P est irréductible.

4) Montrer finalement qu'il existe des polynômes irréductibles de tout degré dans $\mathbb{K}[X]$.

Solution : *Il résulte de question 3) que pour tout nombre premier $p \in \mathcal{P}$ et tout entier $n \in \mathbb{N}^*$, le polynôme $X^n - p \in A[X]$ est irréductible. Or il résulte de la III.7.12.question 3) que ce polynôme est alors irréductible dans $\mathbb{K}[X]$.*

Exercice E : ($\mathbb{K}[X]$**-modules**)
Soit $\mathbb{K}$ un corps.

1) Montrer que E est un $\mathbb{K}[X]$-module si et seulement si, E est un $\mathbb{K}$-espace vectoriel muni d'un endomorphisme u tel que pour tout $v \in E$, $X \cdot v = u(v)$.

Solution :

*i) (**Si** e **est un** $\mathbb{K}[X]$**-module**)*

L'ensemble E est alors muni d'une loi interne $+$ qui en fait un groupe abélien (cf. cours A.1.1.Mod$_0$).) De plus E est muni d'une loi externe $\cdot : \mathbb{K}[X] \times E \to E$ vérifiant les axiomes A.1.1.Mod$_1$) à A.1.1.Mod$_4$). En particulier cette loi externe se restreint en une loi externe $\cdot_{\mathbb{K}} : \mathbb{K} \times E \to E$, qui, puisque $\mathbb{K}$ est un sous-anneau de $\mathbb{K}[X]$ (cf. cours III.2.5.ii),) vérifie encore les axiomes A.1.1.Mod$_1$) à A.1.1.Mod$_4$). Ceci signifie exactement que $(E, +, \cdot_{\mathbb{K}})$ est un $\mathbb{K}$-espace vectoriel.

Puisque E est, par hypothèse un $\mathbb{K}[X]$-module, l'axiome A.1.1.Mod$_1$) assure que

$$\forall (v, w) \in E \times E,\ X \cdot (v + w) = X \cdot v + X \cdot w$$

si bien que l'application

$$u : E \to E\ ,\ v \mapsto X \cdot v \text{ est un endomorphisme du groupe abélien } (E, +)\ .$$

Enfin pour tout $a \in \mathbb{K}$, en considérant a comme un polynôme de degré 0, ou de manière équivalente en utilisant le fait que $\cdot_{\mathbb{K}}$ est la restriction de $\cdot$, on a $a \cdot v = a \cdot_{\mathbb{K}} v$ pour tout $v \in E$. En utilisant l'axiome A.1.1.Mod$_3$) il vient alors :

$$\begin{array}{rcl} \forall (a, v) \in \mathbb{K} \times E, \quad u(a \cdot_{\mathbb{K}} v) & = & X \cdot (a \cdot_{\mathbb{K}} v) \\ & = & X \cdot (a \cdot v) \\ & = & (a *_{\mathbb{K}} [X]X) \cdot v \\ & = & a \cdot (X \cdot v \\ & = & a \cdot_{\mathbb{K}} (X \cdot v) \\ & = & a \cdot_{\mathbb{K}} u(v)\ ; \end{array}$$

ce qui prouve que u est $\mathbb{K}$-linéaire.

*ii) (**Réciproquement**)*

Supposons que E soit un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. Il existe alors une unique loi externe

$$\cdot : \mathbb{K}[X] \times E \to E\ ,\ (X, v) \mapsto u(v)$$

et satisfaisant les axiomes A.1.1.Mod$_2$)à A.1.1.Mod$_4$).

En effet, si une telle loi externe existe, il résulte de l'axiome A.1.1.Mod$_3$) que,

$$\forall n \in \mathbb{N},\ \forall v \in E,\ X^n \cdot v = u^n(v)$$

(où u^n désigne le $n^{\text{ième}}$ itéré de u.) Le même axiome assure que, nécessairement

$$\forall a \in \mathbb{K},\ \forall n \in \mathbb{N},\ \forall v \in E,\ aX^n \cdot v = au^n(v)\ .$$

L'axiome A.1.1.Mod$_2$) entraîne alors que, pour tout

$$P := \sum_{i=0}^{d} a_i X^i \in \mathbb{K}[X]\ ,\ \forall v \in E,\ P \cdot v = \sum_{i=0}^{d} a_i u^i(v)\ .$$

L'unicité de $\cdot$ est donc assurée et reste à constater, ce qui est très élémentaire, que la loi externe définie par la formule ci-dessus vérifie bien les axiomes A.1.1.Mod$_2$) à A.1.1.Mod$_4$).

*iii) (**Remarque**)*

On constate que les constructions faites en i) et ii) sont inverse l'une de l'autre au sens où :

- *si l'on dispose d'une structure de $\mathbb{K}[X]$-module sur E et qu'on lui associe un endomorphisme u comme dans le procédé i), la structure de $\mathbb{K}[X]$-module associée à u dans le procédé ii) est exactement celle dont on est parti.*
- *De même si à un endomorphisme u on associe une structure de $\mathbb{K}[X]$-module comme en ii) ; l'endomorphisme qui sera associé à cette dernière graçe au procédé i) est exactement l'endomorphisme u de départ.*

*iv) (**Remarque**)*

On aurait pu répondre à la question, i.e. établir l'équivalence entre $\mathbb{K}[X]$-module et couple (E, u) en utilisant la description des A-modules donnée en A.1.4. En effet :

- *Une structure de $\mathbb{K}[X]$-module sur E est un morphisme d'anneaux $\mathbb{K}[X] \to \mathrm{End}_{\mathbf{Gr}}(E)$. La composée de ce dernier avec l'injection naturelle $\mathbb{K} \hookrightarrow \mathbb{K}[X]$ est un morphisme d'anneaux $\mathbb{K} \to \mathrm{End}_{\mathbf{Gr}}(E)$ qui donne à E une structure de $\mathbb{K}$-module i.e. précisément de $\mathbb{K}$-espace vectoriel (c'est exactement la situation décrite en A.1.8.b).)*
  L'image de X dans $\mathrm{End}_{\mathbf{Gr}}(E)$ est un endomorphisme du groupe abélien $(E, +)$. On laisse le lecteur vérifier que, du fait que $\mathbb{K}[X] \to \mathrm{End}_{\mathbf{Gr}}(E)$ est un morphisme d'anneaux et $\mathbb{K}$ un sous-anneau de $\mathbb{K}[X]$, u est bien $\mathbb{K}$-linéaire.
- *Réciproquement, si E est un $\mathbb{K}$-espace vectoriel muni d'un $\mathbb{K}$-endomorphisme u, il existe, par propriété universelle des anneaux de polynômes (cf. cours III.2.9,) il existe un unique morphisme d'anneau*

$$\mathbb{K}[X] \to \mathrm{End}_{\mathbf{Gr}}(E)\ ,\ X \mapsto u\ .$$

On parlera pour E du $\mathbb{K}$-*espace vectoriel sous-jacent*.

2) Décrire les morphismes de $\mathbb{K}[X]$-modules (en termes d'applications $\mathbb{K}$-linéaires.)
Solution :

i) Soient E et F des $\mathbb{K}[X]$-modules et $f : E \to F$ un morphisme de $\mathbb{K}[X]$-module. Notons

$$u \in \mathrm{End}_{\mathbb{K}}(E) \text{ (resp. } v \in \mathrm{End}_{\mathbb{K}}(F) \text{)}$$

l'endomorphisme donné par la structure de $\mathbb{K}[X]$-module comme en question 1), i).
Si f est un morphisme de $\mathbb{K}[X]$-modules (cf. cours A.2.1 :)

$$\begin{array}{lrcl} \forall x \in E, & f(X \cdot x) & = & X \cdot f(x) \\ \Leftrightarrow & f(u(x)) & = & v(f(x)) \, . \end{array}$$

Si donc $f : E \to F$ est un morphisme de $\mathbb{K}[X]$-modules, $f \circ u = v \circ f$ ou encore le carré suivant est commutatif :

$$\begin{array}{ccc} E & \xrightarrow{u} & E \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ F & \xrightarrow{v} & F \, . \end{array}$$

ii) Réciproquement suppposons donnés E, F, u, v, f tels que l'on ait un diagramme commutatif d'espaces vectoriels comme ci-dessus. L'endomorphisme u (resp. v,) donne à E (resp. F,) une structure de $\mathbb{K}[X]$-module grâce au procédé question 1), ii). Le fait que $f \circ u = v \circ f$ signifie exactement que

$$\forall x \in E, \; f(X \cdot x) = X \cdot f(x) \, ;$$

ce qui entraîne d'abord que

$$\forall n \in \mathbb{N}, \; \forall x \in E, \; f(X^n \cdot x) = X^n \cdot f(x) \, ;$$

puis, du ffait que f est déjà $\mathbb{K}$-linéaire,

$$\forall P \in \mathbb{K}[X], \; \forall x \in E, \; f(P \cdot x) = P \cdot f(x) \, ;$$

c'est-à-dire que f est bien un morphisme de $\mathbb{K}[X]$-modules.

On en déduit donc que $f : E \to F$ est un morphisme de $\mathbb{K}[X]$-modules si et seulement si f est une application linéaire (i.e. un morphisme de $\mathbb{K}$-espaces vectoriels ou encore de $\mathbb{K}$-modules) telle que

$$f \circ u = v \circ f$$

où u (resp. v,) est l'endomorphisme $\mathbb{K}$-linéaire de E (resp. F,) qui lui donne sa structure de $\mathbb{K}[X]$-module.

3) Étant donné un $\mathbb{K}[X]$-module E, décrire :

a) Les sous-$\mathbb{K}[X]$-modules de E,
Solution :

i) — *Si F est un sous-$\mathbb{K}[X]$-module de E, F est en particulier un sous-groupe du groupe abélien $(E, +)$. De plus, en vertu de la proposition A.3.6, F est stable par combinaisons linéaires à coefficients dans $\mathbb{K}[X]$. Il est donc en particulier stable par combinaisons linéaires à coefficient dans $\mathbb{K}$; autrement dit, F est au moins un sous-$\mathbb{K}$-espace vectoriel de E. De plus*

$$\forall x \in F, \; X \cdot x \in F \, ;$$

ce qui signifie, u étant l'endomorphisme définissant la structure de $\mathbb{K}[X]$-module sur E,

$$\forall x \in F, \; u(x) \in F \, ;$$

autrement dit F est un sous-$\mathbb{K}$-espace vectoriel de E stable par u.

— *Réciproquement, si F est un sous-$\mathbb{K}$-espace vectoriel de E stable par u, il est encore stable par u^n pour tout $n \in \mathbb{N}$, ce qui signifie que*

$$\forall x \in F, \; \forall n \in \mathbb{N}, \; X \cdot x \in F \, ;$$

ce qui entraîne, F étant stable par combinaisons linéaires à coefficients dans $\mathbb{K}$, que

$$\forall P \in \mathbb{K}[X], \; \forall x \in F, \; P \cdot x \in F \, ;$$

ce qui entraîne que F est un sous-$\mathbb{K}[X]$-module de E.

Ainsi F est un sous-$\mathbb{K}[X]$-module de E si et seulement si F est un sous-$\mathbb{K}$-espace vectoriel de E stable par l'endomorphisme u de E définissant la structure de $\mathbb{K}[X]$-module sur E.

*ii) (**Remarque**)*

On aurait pu dire que, F est un sous-$\mathbb{K}[X]$-module de E sis et seulement si l'inclusion naturelle $\mathrm{Id}_{E|F} : F \to E$ est un morphisme de $\mathbb{K}[X]$-module ce qui revient, grâce à la caractérisation de tels morphismes qu'on a donnée (cf. question 2),) exactement à dire que F est un sous-$\mathbb{K}$-espace vectoriel stable.

b) Les quotients de E.

Solution : *Soit $q : E \to F$ un morphisme surjectif de $\mathbb{K}[X]$-modules. L'application q est en particulier un morphisme de $\mathbb{K}$-espace vectoriels i.e. une application linéaire (cf. question 2).)*

Remarquons alors que le noyau $\mathrm{Ker}\, q$ est autant son noyau en tant que morphisme de $\mathbb{K}[X]$-modules, qu'en tant que $\mathbb{K}$-espaces vectoriels ; puisqu'il s'agit toujours du noyau du morphisme de groupes sous-jacent. Cependant si l'on considère q comme un morphisme de $\mathbb{K}[X]$-module $\mathrm{Ker}\, q$ est un sous-$\mathbb{K}[X]$-module de E (cf. cours A.5.2 ;) c'est-à-dire un sous-$\mathbb{K}$-espace vectoriel de E stable par l'endomorphisme de structure u (cf. a).)

Réciproquement si $q : E \to F$ est une application linéaire surjective dont le noyau est stable par l'endomorphisme u de structure de E, il existe (cf. cours I.8.11,) un unique endomorphisme $\mathbb{K}$-linéaire $v : F \to F$ tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} E & \xrightarrow{u} & E \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q} \\ F & \xrightarrow{v} & F\,. \end{array}$$

En conclusion, une application $q : E \to F$ est un morphisme de $\mathbb{K}[X]$-modules si et seulement si c'est une application linéaire dont le noyau est stable par l'endomorphisme de structure de E.

c) Les suites exactes courtes

$$0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0\,.$$

Solution : *Si*

$$0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$$

est une suite exacte courte de $\mathbb{K}[X]$-modules N, E et Q sont au moins des $\mathbb{K}$-espaces vectoriels (resp. des groupes abéliens) tandis que i et p sont aumoins des applications linéaire (resp. des morphismes de groupes.)

Puisque les notions de noyaux et d'images sont toujours celles des morphismes de groupes sous-jacents, et que les suites exactes sont caractérisée en termes de noyaux noyaux et d'images (cf. cours I.9.1,) la suite

$$0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$$

est encore exacte comme suite de $\mathbb{K}$-espaces vectoriels (resp. de groupes abéliens.)

Si de plus N, E et Q sont des $\mathbb{K}[X]$-modules, E est en particulier muni d'un endomorphisme de structure u (cf. question 1).) On a vue ci-dessus que N est nécessairement stable par u ce qui revient à dire que, si v l'endomorphisme de structure de N c'est l'unique (du fait de l'injectivité de i,) endomorphisme de N satisfaisant $i \circ v = u \circ i$. L'endomorphisme de structure w de Q est alors l'unique endomorphisme de Q de sorte que le diagramme suivant soit commutatif :

$$\begin{array}{ccccccccc} 0 & \to & N & \xrightarrow{i} & E & \xrightarrow{p} & Q & \to & 0 \\ & & {\scriptstyle v}\downarrow & & {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle w} & & \\ 0 & \to & N & \xrightarrow{i} & E & \xrightarrow{p} & Q & \to & 0 \end{array}$$

.

Une suite exacte courte de $\mathbb{K}[X]$-modules est donc en définitive un diagramme commutatif de $\mathbb{K}$-espaces vectoriels comme ci-dessus.

4) Montrer qu'un $\mathbb{K}[X]$-module E est de type fini et de torsion si et seulement si le $\mathbb{K}$-espace vectoriel E est de dimension finie.

Solution : *Ce résultat est bien évidemment à rapprocher du TD n° III, exercice D ; les arguments de la preuve étant dailleurs ici exactement ceux donnés là.*

*i) (**Dimension finie entraîne de type fini et de torsion**)*

Si E est un $\mathbb{K}$-espace vectoriel de dimension finie, il possède une base ou à tout le moins une famille génératrice finie : $(e_1, \ldots, e_n)$. Tout élément $x \in E$ s'écrit $x = \sum_{i=0}^{n} a_i e_i$ où $a_{i\,,1\leq i\leq n} \in \mathbb{K}$ sont des éléments du corps $\mathbb{K}$. Mais ce dernier étant un sous-anneau de $\mathbb{K}[X]$ on peut considérer les $a_{i\,,1\leq i\leq n}$ comme des éléments de $\mathbb{K}[X]$ et la combinaison linéaire ci-dessus comme une combinaison linéaire à coefficients dans $\mathbb{K}[X]$. Il s'ensuit que $e_{i\,,1\leq i\leq n}$ apparaît comme une partie génératrice de E vu comme $\mathbb{K}[X]$-module.

***Attention** Même si $e_{i\,,1\leq i\leq n}$ est une partie libre de E en tant que $\mathbb{K}$-espace vectoriel, elle n'a aucune raison de le rester dans E vu comme $\mathbb{K}[X]$-module. La suite montre d'ailleurs qu'elle a peu de chance de le rester !*

Si u est l'endomorphisme de structure de E i.e. celui construit en question 1), i), donné par l'action de X sur E, c'est un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie, et il possède donc (cf. cours IV.2.6,) un polynôme annulateur non nul, ce qui signifie exactement que E est de torsion en tant que $\mathbb{K}[X]$-module.

*ii) (**De type fini et de torsion entraîne de dimension finie**)*

Notons u l'endomorphisme de structure de E. Puisque E est de type fini comme $\mathbb{K}[X]$-module, soit $e_{i\ ,1\leq i\leq n}$ une partie génératrice finie de E. Puisque E est de torsion, chacun des e_i est de torsion, ce qui signifie exactement que le polynôme minimal $P^{e_i}_{min\,u}$ (cf. cours IV.2.2.iii),) est non nul.

Notons $\varepsilon_{i\ ,1\leq i\leq n}$ la base canonique de $\mathbb{K}[X]^n$ (cf. cours II.1.4.c),) et

$$\pi\ :\ \mathbb{K}[X]^n\ \rightarrow\ E\ ,\ \varepsilon_i\ \mapsto\ e_i \text{ (cf. II.2.10 .)}$$

Le fait que $e_{i\ ,1\leq i\leq n}$ est une partie $\mathbb{K}[X]$-génératrice de E signifie exactement que le morphisme π ci-dessus est surjectif. Il n'est pas difficile de voir que son noyau est

$$\prod_{i=1}^{n} P^{e_i}_{min\,u}\mathbb{K}[X]\ .$$

On en déduit, par factorisation des morphismes (cf. cours I.8.11,) un morphisme surjectif de $\mathbb{K}[X]$-modules

$$\overline{\pi}\ :\ \prod_{i=1}^{n} \mathbb{K}[X]/P^{e_i}_{min\,u}\mathbb{K}[X]\ \rightarrow\ E\ .$$

Or (cf. exercice C,)

$$\forall 1\leq i\leq n,\ \mathbb{K}[X]/P^{e_i}_{min\,u}\mathbb{K}[X]$$

est un $\mathbb{K}$-espace vectoriel de dimension finie. Il s'ensuit que $\prod_{i=1}^{n} \mathbb{K}[X]/P^{e_i}_{min\,u}\mathbb{K}[X]$ est encore un $\mathbb{K}$-espace vectoriel de dimension finie. Le morphisme $\overline{\pi}$ étant en particulier unne application linéaire surjective, il en résulte finalement que E est de dimension finie.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Document n° V

30 mars 2020

Vers le théorème de décomposition de DUNFORD

Le chapitre IV dont nous avons commencé l'étude doit conduire à un certain nombre d'énoncés de réduction des endomorphismes, c'est-à-dire de théorème permetttant de donner une forme plus « simple », c'est-à-dire concrètement, une écriture plus simple de la matrice, d'un endomorphisme donné. La *diagonalisation* (cf. cours IV.5.4,) est une réduction particulièrement agréable, mais on sait bien qu'on ne peut l'obtenir que dans des cas très particuliers. Les hypothèses nécessaires pour obtenir une décomposition de DUNFORD (cf. cours IV.9.1,) sont déjà moins contraignantes, tout en permettant néanmoins d'obtenir des résultats quant aux itérés d'une matrice par exemple.

On a donné, dans le DOC n° III une preuve du théorème de CAYLEY–HAMILTON (cf. cours IV.7.2,) ce qui correspond à la lecture des paragraphes IV.5 à IV.7. Outre l'énoncé de ce théorème, il serait bon d'être familier avec les notions de *valeur propre*, *vecteur propre*, *espace propre* (cf. cours IV.5.2,) dont nous espérons cependant qu'elles faisaient déjà partie de vos connaissances.

On peut concevoir que la lecture du paragraphe IV.3 ait quelque peu dérouté le lecteur dans la mesure où les résultats qu'il contient n'ont pas encore été vraiment utilisés et en particulier n'entrent pas dans la preuve du théorème IV.7.2 de CAYLEY–HAMILTON.

Les résultats du paragraphe IV.3 mentionné ci-dessus sont, en revanche absolument crutiaux pour énoncer et démontrer le théorème de décomposition de DUNFORD (cf. cours IV.9.3,) que nous allons énoncer et démontrer dans cette séance.

Le théorème IV.3.2 est un ingrédient essentielle de la démonstration du théorème IV.9.3. Le théorème IV.3.2 est l'exact analogue des théorèmes II.8.3 et B.2.3 lesquels sont tous des conséquences du théorème de BÉZOUT dont l'incarnation dans le cadre de la réduction des endomorphismes étudiée au chapitre IV est le *lemme des noyaux* (cf. cours IV.2.4.iii).)

On prêtera cependant une attention particulière au point IV.3.2.iv) dont la conséquence vis-à-vis de la décomposition de DUNFORD est IV.9.1.Dun$_1$). On constatera l'importance d'un tel énoncé, dont une des conséquence est que l'anneau $\mathbb{K}[\delta, \nu]$ est commutatif et qu'on peut donc y applicquer des règles de calcul comme la formule du binôme de NEWTON.

n° V.0 . −Erratum

J'adresse mes remerciements et mes félicitations à la personne qui a détecté une erreur dans la proposition IV.2.3.iv) : Si l'on suppose que f est surjective alors

$$P_{\min v} | P_{\min u}$$

et ce n'est pas vrai en général. On pourra remarquer qu'en II.5.3.iv) et A.7.3.iv), on s'est passé de l'hypothèse de surjectivité sur le morphisme en ne considérant que son image.

n° V.1 . −Réduction de DUNFORD

On a déjà noté l'importance du théorème IV.3.2 dans tout ce qui suit. Il est également indispensable d'être familiarisé avec les définitions données au paragraphe IV.8 et en particulier IV.8.1. On pourra pour l'instant omettre de s'intéresser aux questions liées aux blocs de JORDAN (cf. cours IV.8.4.)

On se propose dans ce qui suit, de démontrer un certain nombre d'énoncés conduisant à la preuve du théorème IV.9.3 de décomposition de DUNFORD. Vous êtes invités à chercher vous-même la preuve des énoncés proposés au paragraphe n° V.1 et à vous reporter ensuite aux preuves données dans le paragraphe n° V.2. **On fixe les notations suivantes utilisées dans tout ce texte : $\mathbb{K}$ est un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $d \in \mathbb{N}^*$ et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E. On note $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{K}$ et $P_{\min u} \in \mathbb{K}[X]$ le polynôme minimal de u.**

Si vous avez quelques doutes quant à vos connaissances concernant le *lemme des noyaux* (cf. cours IV.2.4.iii),) nous vous conseillons en préalable à ce qui suit à en refaire la démonstration que vous trouverez en *loc. cit.*.

1) (**Proposition IV.9.2**)

Pour $\lambda \in \mathbb{K}$, si $X - \lambda | P_{\min u}$ (c'est-à-dire (cf. cours IV.5.1.d),) si λ est valeur propre de u,) on note E_λ le sous-espace caractéristique (cf. cours IV.3.1,) associé à $X - \lambda$.

Montrer qu'alors

$$u_{|E_\lambda} = \lambda \mathrm{Id}_{E_\lambda} + \nu$$

où ν est nilpotent *i.e.* $u_{|E_\lambda}$ a une décomposition de DUNFORD (cf. cours IV.9.1.)

2) rappeler pourquoi il existe des polynômes irréductibles deux à deux distincts $P_{i\ ,1\leq i\leq r}$ et des entiers $\alpha_{i\ ,1\leq i\leq r}$ tels que

$$P_{\min u} \ = \ \prod_{i=1}^{r} P_i^{\alpha_i} \ .$$

3) En déduire une décomposition de E en somme directe de sous-espaces caractéristiques :

$$E \ = \ \bigoplus_{i=1}^{r} E_i \text{ avec } E_i \ = \ \mathrm{Ker}\, P_i^{\alpha_i}(u) \ = \ E[P_i^{\alpha_i}] \text{ (cf. IV.3.2 .)}$$

4) Pour tout $1 \ \leq \ i \ \leq \ r$ considérons la décomposition de E en somme directe

$$E \ = \ E_i \ \oplus \ \bigoplus_{1 \ \leq \ j \ \leq \ r \ j \ \neq \ i} E_j$$

qui donne lieu à une projection

$$p_i \ : \ E \ \rightarrow \ E_i \text{ parallèlement à } \bigoplus_{1 \ \leq \ j \ \leq \ r \ j \ \neq \ i} E_j \ .$$

Montrer qu'alors

$$\forall 1 \leq i \leq r, \ p_i \ \in \ \mathbb{K}[u] \ .$$

On suppose désormais que le polynôme minimal $P_{\min u}$ de u est scindé ; c'est-à-dire qu'il existe $\lambda_{i\ ,1\leq i\leq r} \ \in \ \mathbb{K}$ tel que

$$P_{\min u} \ = \ \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i} \ .$$

5) Rappeler pourquoi les $E_{i\ ,1\leq i\leq r}$ définis en 3) sont stable par u et montrer qu'en notant $u_i \ := \ u_{|E_i}$, il existe

$$\nu_i \ \in \ \mathbb{K}[u_i] \ , \ \delta_i \ \in \ \mathbb{K}[u_i] \ \text{ tels que } \ u_i \ = \ \delta_i + \nu_i \ , \ \delta_i \ \circ \ \nu_i \ = \ \nu_i \ \circ \ \delta_i$$

avec ν_i nilpotent et δ_i diagonal.

6) On pose

$$\begin{array}{rccc} \delta \ := \ \bigoplus_{i=1}^{r} \delta_i \ \circ \ p_i : & E & \longrightarrow & E \\ & x & \longmapsto & \sum_{i=1}^{r} \delta_i[p_i(x)] \\ \text{et } \nu := & u - \delta & & . \end{array}$$

Montrer qu'alors :

i)

$$\delta \ \in \ \mathbb{K}[u] \text{ et } \nu \ \in \ \mathbb{K}[u] \ ;$$

ii)

$$u \ = \ \delta \ + \ \nu \text{ et } \nu \ \circ \ \delta \ = \ \delta \ \circ \ \nu \ ;$$

iii)

$$\delta \text{ est diagonalisable ;}$$

iv)

$$\nu_{|E_i} \ = \ \nu_i \text{ et } \nu \text{ est nilpotent } .$$

Peut-on préciser l'échlon de nilpotence (cf. cours IV.8.1,) de ν ?

7) Soit $u \ = \ \delta + \nu$ une décomposition de DUNFORD (cf. cours IV.9.1.) Puisque δ est diagonalisable, notons $E_{\lambda\ ,\lambda \ \in \ \mathrm{Sp}(\delta)}$ ses espace propres et l'on a alors

$$E \ = \ \bigoplus_{\lambda \ \in \ \mathrm{Sp}(\delta)} E_\lambda \ .$$

Montrer que :

i)

$$\forall \lambda \in \mathrm{Sp}(\delta), \ E_\lambda \text{ est stable par } u \text{ et } \nu \ ;$$

ii)

$$\mathrm{Sp}(u) \subset \mathrm{Sp}(\delta) ;$$

iii)

$$\mathrm{Sp}(\delta) \subset \mathrm{Sp}(u) \text{ et finalement } \mathrm{Sp}(u) = \mathrm{Sp}(\delta) ;$$

iv) les sous-espace propres E_{λ} ,$_{\lambda \in \mathrm{Sp}(\delta)}$ sont les sous-espaces caractéristiques de u.

v) La décomposition $u = \delta + \nu$ satisfaisant IV.9.1.Dun$_1$) à IV.9.1.Dun$_4$) est unique.

8) Conclure qu'on a le théorème IV.9.3 de décomposition de DUNFORD : *P*our tout $u \in \mathrm{End}_{\mathbb{K}}(E)$, si (de manière équivalente) $P_{\min u}$ ou $P_{\mathrm{car}\, u}$ est scindé, (E, u) admet une unique décomposition de DUNFORD.

n° V.2 . −Preuves des énoncés du paragraphe n° V.1

1) (**Proposition IV.9.2**)
Pour $\lambda \in \mathbb{K}$, si $X - \lambda | P_{\min u}$ (c'est-à-dire (cf. cours IV.5.1.d),) si λ est valeur propre de u,) on note E_{λ} le sous-espace caractéristique (cf. cours IV.3.1,) associé à $X - \lambda$.
Montrer qu'alors

$$u_{|E_{\lambda}} = \lambda \mathrm{Id}_{E_{\lambda}} + \nu$$

où ν est nilpotent *i.e.* $u_{|E_{\lambda}}$ a une décomposition de DUNFORD (cf. cours IV.9.1.)
Solution : *(cf. cours IV.9.2.)*

2) rappeler pourquoi il existe des polynômes irréductibles deux à deux distincts P_{i} ,$_{1 \leq i \leq r}$ et des entiers α_{i} ,$_{1 \leq i \leq r}$ tels que

$$P_{\min u} = \prod_{i=1}^{r} P_i^{\alpha_i} .$$

Solution : *Il s'agit du théorème fondamental de l'arithmétique dans les anneaux de polynômes (cf. cours III.5.5.)*

3) En déduire une décomposition de E en somme directe de sous-espaces caractéristiques :

$$E = \bigoplus_{i=1}^{r} E_i \text{ avec } E_i = \mathrm{Ker}\, P_i^{\alpha_i}(u) = E[P_i^{\alpha_i}] \text{ (cf. IV.3.2 .)}$$

Solution : *Ceci n'est autre que le théorème IV.3.2, dont on rappelle que l'ingrédient principal est le lemme des noyaux (cf. cours IV.2.4.iii)) et donc finalement le théorème de* BÉZOUT *dans les anneaux de polynomes (cf. cours III.5.2.1.)*

4) Pour tout $1 \leq i \leq r$ considérons la décomposition de E en somme directe

$$E = E_i \oplus \bigoplus_{1 \leq j \leq r \; j \neq i} E_j$$

qui donne lieu à une projection

$$p_i : E \to E_i \text{ parallèlement à } \bigoplus_{1 \leq j \leq r \; j \neq i} E_j .$$

Montrer qu'alors

$$\forall 1 \leq i \leq r, \; p_i \in \mathbb{K}[u] .$$

Solution : *On pourrait simplement s'en remetre à IV.3.2.iv).*
On peut à nouveau détailler l'argument ici : Pour tout $1 \leq i \leq r$, *notons*

$$Q_i := \prod_{1 \leq i \leq r \; i \neq j} P_j^{\alpha_j} .$$

Les polynôme P_i *et* Q_i *sont bien évidemment premiers entre eux,* $P_{\min u} = P_i Q_i$ *si bien que* $E = \mathrm{Ker}\,(P_i Q_i)(u)$ *et l'on est donc dans le cadre d'application du lemme des noyaux (cf. cours IV.2.4.iii).) On ne redonne pas ici le calcul donné dans la preuve de loc. cit., auquel on se reportra et qui assure que* $_i$ *est un polynôme en* u.

On suppose désormais que le polynôme minimal $P_{\min u}$ de u est scindé ; c'est-à-dire qu'il existe $\lambda_{i\ ,1\leq i\leq r} \in \mathbb{K}$ tel que

$$P_{\min u} \ = \ \prod_{i=1}^{r} (X-\lambda_i)^{\alpha_i} \ .$$

5) Rappeler pourquoi les $E_{i\ ,1\leq i\leq r}$ définis en 3) sont stable par u et montrer qu'en notant $u_i \ := \ u_{|E_i}$, il existe

$$\nu_i \ \in \ \mathbb{K}[u_i] \ , \ \delta_i \ \in \ \mathbb{K}[u_i] \ \text{ tels que } \ u_i \ = \ \delta_i + \nu_i \ , \ \delta_i \ \circ \ \nu_i \ = \ \nu_i \ \circ \ \delta_i$$

avec ν_i nilpotent et δ_i diagonal.

Solution : *Les sous-espaces caractéristiques sont stables par u et c'est encore un corollaire du lemme des noyaux. Posons donc $u_i \ := \ u_{|E_i}$.*

On peut alors appliquer 1) (c'est-à-dire la proposition IV.9.2) à chacun des couple (e_i, u_i). Par construction, $\delta_i \ := \ \lambda_i \mathrm{Id}_{E_i}$ et $\nu_i \ := \ (u - \lambda_i \mathrm{Id}_{E_i})$ sont des éléments de $\mathbb{K}[u_i]$ et qui, par conséquent commutent entre eux. Il est en effet presque immédiat de vérifier que $\mathbb{K}[u_i]$ est un anneau commutatif. Un énoncé caractérisant tous les endomorphismes commutant avec un endomorphisme donné, peut être obtenu mais cela demande un peu de travail.

6) On pose

$$\begin{array}{rccc} \delta \ := \ \bigoplus_{i=1}^{r} \delta_i \ \circ \ p_i : & E & \longrightarrow & E \\ & x & \longmapsto & \sum_{i=1}^{r} \delta_i[p_i(x)] \\ \text{et } \nu := & u - \delta & & . \end{array}$$

Montrer qu'alors :

i)

$$\delta \ \in \ \mathbb{K}[u] \text{ et } \nu \ \in \ \mathbb{K}[u] \ ;$$

Solution : *On a montré en 4) que,*

$$\forall 1 \leq i \leq r, \ \exists \xi_i \ \in \ \mathbb{K}[X], \quad \textit{tel que } \ p_i \ = \ \xi_i(u) \ .$$

$$\textit{De plus } \forall 1 \leq i \leq r, \ \delta_i \ = \ \lambda_i \mathrm{Id}_{E_i} \ \textit{(cf. 5) .)}$$

D'où il résulte que

$$\delta \ \circ \ p_i \ = \ \lambda_i i \xi_i(u) \ .$$

À strictement parler ce morphisme est à valeurs dans E_i et non dans E. Puisque E_i est un sous-ensemble de E, on peut néanmoins le voir comme un morphisme à valeurs dans E. On a finalement

$$\delta \ = \ \big(\sum_{i=1}^{r} \lambda_i \xi_i\big)(u) \ \in \ \mathbb{K}[u] \ .$$

Il est immédiat alors que

$$\nu \ = \ u - \delta \ \in \ \mathbb{K}[u] \ .$$

ii)

$$u \ = \ \delta \ + \ \nu \text{ et } \nu \ \circ \ \delta \ = \ \delta \ \circ \ \nu \ ;$$

Solution : *Par définition $u \ = \ \delta \ + \ \nu$. On a montré (cf. i),) que δ et ν sont des éléments de $\mathbb{K}[u]$ qui est un anneau comutatif.*

iii)

$$\delta \text{ est diagonalisable ;}$$

Solution : *Montrons qu'en fait les espaces caractéristiques E_i de u sont les espaces propres de δ. En effet :*

$$\begin{array}{rcl} \forall x \in E_i, \quad \delta(x) & = & \sum_{j=1}^{r} \delta_j \ \circ \ p_j(x) \\ & = & \delta_i \circ p_i(x) \\ & = & \delta_i(x) \\ & = & \lambda_i x \ . \end{array}$$

L'espace E est somme directe d'espaces propres pour δ ; c'est-à-dire que δ est diagonalisable.

iv)

$$\nu_{|E_i} \;=\; \nu_i \text{ et } \nu \text{ est nilpotent } .$$

Peut-on préciser l'échlon de nilpotence (cf. cours IV.8.1,) de ν ?

Solution : *En utilisant le calcul de $\delta(x)$ fait ci-dessus (cf. iii) :)*

$$\begin{array}{rcl} \forall x \in E_i, \quad \nu(x) & = & u(x) - \delta(x) \\ & = & u_i(x) - \lambda_i x \\ & = & \nu_i(x) \; . \end{array}$$

Pour tout $x \in E$, écrivons

$$x \;=\; \sum_{i=1}^{r} x_i \;,\; x_i \;\in\; E_i \; .$$

On a alors :

$$\begin{array}{rcl} \forall k \in \mathbb{N}, \quad \nu^k(x) & = & \nu^k\big(\sum_{i=1}^{r} x_i\big) \\ & = & \sum_{i=1}^{r} \nu^k(x_i) \\ & = & \sum_{i=1}^{r} {\nu_{|E_i}}^k(x_i) \\ & = & \sum_{i=1}^{r} \nu_i^k(x_i) \; . \end{array}$$

Pour $k \;\geq\; \max_{1 \,\leq\, i \,\leq\, r}(\alpha_i)$ et tout $x \;\in\; E$, on a donc $\nu^k(x) \;=\; 0$, puisqu'il découle de 1) (c'est-à-dire de la proposition IV.9.2) que ν_i est nilpotent α_i. On montre ainsi que ν est déchelon inférieur à $\max_{1 \,\leq\, i \,\leq\, r}(\alpha_i)$. Il suffit cependant de prendre $x \;\in\; E_i$, pour établir que l'échelon de ν est supérieur à $\alpha_i \; \forall 1 \leq i \leq r,$ et l'on a ainsi l'égalité entre l'échelon de nilpotence de ν et $\max_{1 \,\leq\, i \,\leq\, r}(\alpha_i)$.

7) Soit $u \;=\; \delta + \nu$ une décomposition de DUNFORD (cf. cours IV.9.1.) Puisque δ est diagonalisable, notons $E_{\lambda \,,\lambda \,\in\, \mathrm{Sp}(\delta)}$ ses espace propres et l'on a alors

$$E \;=\; \bigoplus_{\lambda \,\in\, \mathrm{Sp}(\delta)} E_\lambda \; .$$

Montrer que :

i)

$$\forall \lambda \in \mathrm{Sp}(\delta), \; E_\lambda \text{ est stable par } u \text{ et } \nu \; ;$$

Solution :

$$\begin{array}{rcl} \forall \lambda \in \mathrm{Sp}(\delta), \; \forall x \in E_\lambda, \quad \delta[u(x)] & = & \delta[(\delta + \nu)(x)] \\ & = & (\nu + \delta)[\delta(x)] \\ & = & u[\delta(x)] \\ & = & u(\lambda x) \\ & = & \lambda u(x) \\ \Rightarrow \qquad\qquad\qquad u(x) & \in & E_\lambda \; . \end{array}$$

Puisque E_λ est stable par u et par δ il est stable par $\nu \;=\; u - \delta$; ce qui pourrait aussi se déduire immédiatement du fait que ν et δ commutent.

ii)

$$\mathrm{Sp}(u) \;\subset\; \mathrm{Sp}(\delta) \; ;$$

Solution : *Pour tout $\mu \;\in\; \mathrm{Sp}(u)$, il existe $x \;\in\; E \setminus \{0\}$ tel que $u(x) \;=\; \mu x$. En écrivant*

$$x \;=\; \sum_{\lambda \,\in\, \mathrm{Sp}(\delta)} x_\lambda \;,\; x_\lambda \;\in\; E_\lambda,$$

on a :

$$\begin{array}{rcl} & & u(x) \;=\; \mu x \\ \Leftrightarrow u\big(\sum_{\lambda \,\in\, \mathrm{Sp}(\delta)} x_\lambda\big) & & = \; \mu \sum_{\lambda \,\in\, \mathrm{Sp}(\delta)} x_\lambda \\ \Leftrightarrow & \sum_{\lambda \,\in\, \mathrm{Sp}(\delta)} u(x_\lambda) & = \quad \sum_{\lambda \,\in\, \mathrm{Sp}(\delta)} \mu x_\lambda \\ & \forall \lambda \in \mathrm{Sp}(\delta), \; u(x_\lambda) & = \quad \mu x_\lambda \; ; \end{array}$$

la dernière équivalence résultant du fait que $E = \bigoplus_{\lambda \in \mathrm{Sp}(\delta)} E_\lambda$ *et que chacun des* E_λ *est stable par* u *(cf. i).)*

Puisque $x \neq 0$,

$$\exists \lambda \in \mathrm{Sp}(\delta),\ x_\lambda \neq 0\ .$$

Puisque ν *est nilpotent il existe alors* $k \in \mathbb{N}$ *tel que* $\nu^k(x_\lambda) \neq 0$, *et* $\nu^{k+1}(x_\lambda) = 0$. *On a alors :*

$$\begin{array}{rrcl}
 & u(x_\lambda) & = & \mu x_\lambda \\
\Leftrightarrow & (\delta+\nu)(x_\lambda) & = & \mu x_\lambda \\
\Leftrightarrow & \lambda x_\lambda + \nu(x_\lambda) & = & \mu x_\lambda \\
\Leftrightarrow & (\mu-\lambda)(x_\lambda) & = & \nu(x_\lambda) \\
\Rightarrow & 0 & = & \nu^{k+1}(x_\lambda) \\
 & & = & \nu^k[\nu(x_\lambda)] \\
 & & = & \nu^k[(\mu-\lambda)(x_\lambda)] \\
 & & = & (\mu-\lambda)\nu^k(x_\lambda) \\
\Rightarrow & \mu-\lambda & = & 0 \\
\Rightarrow & \mu & \in & \mathrm{Sp}(\delta)\ ;
\end{array}$$

si bien que $\mathrm{Sp}(u) \subset \mathrm{Sp}(\delta)$.

iii)

$$\mathrm{Sp}(\delta) \subset \mathrm{Sp}(u) \text{ et finalement } \mathrm{Sp}(u) = \mathrm{Sp}(\delta)\ ;$$

Solution : *Pour tout* $\lambda \in \mathrm{Sp}(\delta)$, *il existe* $x \in E_\lambda \setminus \{0\}$ *tel que* $\delta(x) = \lambda x$. *Par ailleurs*

$$\nu(x) = u(x) - \delta(x) = u(x) - \lambda x\ .$$

Or ν *étant nilpotent et* $x \neq 0$, *il existe* $k \in \mathbb{N}$ *tel que* $\nu^k(x) \neq 0$ *et*

$$\begin{array}{rrcl}
 & \nu^{k+1}(x) & = & 0 \\
\Leftrightarrow & \nu^k[(u-\delta)(x)] & = & 0 \\
\Leftrightarrow & \nu^k[u(x)-\lambda x] & = & 0 \\
\Leftrightarrow & (u-\lambda)[\nu^k(x)] & = & 0\ ;
\end{array}$$

c'est-à-dire que $\nu^k(x)$ *est un vecteur propre pour* u *associé à la valeur propre* λ *et donc que* $\lambda \in \mathrm{Sp}(u)$. *Il s'ensuit que*

$$\mathrm{Sp}(\delta) \subset \mathrm{Sp}(u) \text{ } \textit{et finalement, en vertu de ii), que } \mathrm{Sp}(u) = \mathrm{Sp}(\delta)\ .$$

iv) les sous-espace propres $E_{\lambda\ ,\lambda \in \mathrm{Sp}(\delta)}$ sont les sous-espaces caractéristiques de u.

Solution : *Notons* m_λ *l'échelon de nilpotence de* $\nu_{|E_\lambda}$ *(on rapelle (cf. i),) que* E_λ *est stable par* ν.*) Il est clair que* $\forall \lambda \in \mathrm{Sp}(\delta)$, m_λ *est inférieur ou égal à l'échelon de nilpotence de* ν.

$$\begin{array}{lrcl}
\forall \lambda \in \mathrm{Sp}(\delta),\ \forall x \in E_\lambda, & \nu^{m_\lambda}(x) & = & 0 \\
\Leftrightarrow & (u-\delta)^{m_\lambda}(x) & = & 0 \\
\Leftrightarrow & (u-\lambda \mathrm{Id}_{E_i})^{m_\lambda}(x) & = & 0\ .
\end{array}$$

D'où il résulte que

$$\forall \lambda \in \mathrm{Sp}(\delta),\ E_\lambda \subset \mathrm{Ker}\left((u-\lambda \mathrm{Id})^{m_\lambda}\right)\ .$$

Le lemme des noyaux assure que la somme

$$\sum_{\lambda \in \mathrm{Sp}(\delta)} \mathrm{Ker}\left((u-\lambda)^{m_\lambda}\right)$$

est directe. L'inclusion précédente assure alors que

$$\forall \lambda \in \mathrm{Sp}(\delta),\ E_\lambda = \mathrm{Ker}\left((u-\lambda)^{m_\lambda}\right)\ .$$

v) La décomposition $u = \delta + \nu$ satisfaisant IV.9.1.Dun$_1$) à IV.9.1.Dun$_4$) est unique.

Solution : *Supposons données deux décompositions de* DUNFORD *de* u,

$$u = \delta_1 + \nu_1 = \delta_2 + \nu_2$$

satisfaisant IV.9.1.Dun$_1$*)à IV.9.1.Dun*$_4$*). Alors on a (cf. iii),)*

$$S := \mathrm{Sp}(\delta_1) = \mathrm{Sp}(u) = \mathrm{Sp}(\delta_2)\ ;$$

l'espace E *est somme directe*

$$E = \bigoplus_{\lambda \in S} E_\lambda$$

où les $E_{\lambda\ ,\lambda \in S}$ *sont à la fois les espaces propres de* δ_1 *et* δ_2 *et les espaces caractéristiques de* u *Il en découle immédiatement que* $\delta_1 = \delta_2$, *et donc que* $\nu_1 = \nu_2$.

8) Conclure qu'on a le théorème IV.9.3 de décomposition de DUNFORD : *P*our tout $u \in \mathrm{End}_{\mathbb{K}}(E)$, si (de manière équivalente) $P_{\min\, u}$ ou $P_{\mathrm{car}\, u}$ est scindé, (E, u) admet une unique décomposition de DUNFORD.

Solution : *L'existence de la décomposition résulte de 6) et l'unicité de 7).*

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Document n° VI

3 avril 2020

Corrigé du TD n° VI

Exercice A : (Décomposition de DUNFORD)

1) Soit A la matrice

$$A := \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 2 \end{pmatrix}$$

et f l'endomorphisme de $\mathbb{R}^3$ associé.

a) Factoriser le polynôme caractéristique de A.

Solution : *Soit $P_{car\,f} := \det(X - A)$, le polynôme caractéristique de A (ou encore de f.) Alors :*

$$\begin{aligned}
P_{car\,f} &= \begin{vmatrix} X-1 & 1 & 0 \\ -1 & X & 1 \\ 1 & 0 & X-2 \end{vmatrix} \\
&= \begin{vmatrix} X-1 & 1 & 0 \\ -1 & X & 1 \\ 0 & X & X-1 \end{vmatrix} \\
&= \begin{vmatrix} X-1 & 1 & 0 \\ 0 & X & 1 \\ X-1 & X & X-1 \end{vmatrix} \\
&= (X-1) \cdot \begin{vmatrix} 1 & 1 & 0 \\ 0 & X & 1 \\ 1 & X & X-1 \end{vmatrix} \\
&= (X-1) \cdot \begin{vmatrix} 1 & 1 & 0 \\ 0 & X & 1 \\ 0 & X-1 & X-1 \end{vmatrix} \\
&= (X-1)^2 \cdot \begin{vmatrix} 1 & 1 & 0 \\ 0 & X & 1 \\ 0 & 1 & 1 \end{vmatrix} \\
&= (X-1)^3 .
\end{aligned}$$

b) Déterminer les sous-espaces propres et caractéristiques de A.

Solution : *On a vu (cf. a),) que le polynôme caractéristique $P_{car\,f}$ de f, est $P_{car\,f} = (X-1)^3$. Il découle du théorème de* CAYLEY–HAMILTON *(cf. cours IV.7.2,) que le polynôme minimal $P_{min\,f}$ est $(X-1)^\alpha$ avec $\alpha \leq 3$. Ce dernier n'a qu'un facteur irréductible $X - 1$ si bien que $\mathbb{R}^3$ est le sous-espace caractéristique associé à ce facteur.*

Soit E_1 le sous-espace propre associé à la valeur propre 1 :

$$\begin{aligned}
&\forall v := \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_1, && f(v) = v \\
\Leftrightarrow \quad & && A \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\
\Leftrightarrow \quad & && \left\{ \begin{array}{rcl} y & = & 0 \\ x-y-z & = & 0 \\ x-z & = & 0 \end{array} \right\} \\
\Leftrightarrow \quad & && \left\{ \begin{array}{rcl} x-z & = & 0 \\ y & = & 0 \end{array} \right\} \\
\Leftrightarrow \quad & && v = x \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} .
\end{aligned}$$

Posons $u_1 := \begin{pmatrix}1\\0\\1\end{pmatrix}$. *Alors* $E_1 = \mathrm{Vect}\{u_1\}$.

c) Démontrer qu'il existe une base de $\mathbb{R}^3$ dans laquelle la matrice de f est

$$B = \begin{pmatrix}1 & 1 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}$$

et trouver une matrice P inversible telle que $A = PBP^{-1}$.

Solution : *Bien entendu le théorème de réduction de* JORDAN *(cf. cours IV.10.10,) assure que l'on peut trouver une base dans laquelle la matrice de f a la forme demandée. Cependant, si l'on construit explicitement cette base on aura également justifié cette écriture de f.*

Il est immédiat de constater, sur la forme de la matrice B demandée, que si une telle base existe, son premier vecteur est propre pour la valeur propre 1. Ainsi on pourra prendre le vecteur u_1 construit en b).

On prendra cependant garde qu'il est maladroit de procéder ainsi en général, puisque la forme de la matrice impose que, si u_2 et u_3 sont les deux autres vecteurs de base, on a nécessairement

$$f(u_2) = u_1 + u_2\ ,\ f(u_3) = u2 + u_3\ .$$

Notons $g := f - \mathrm{Id}$. *On a alors*

$$g(u_3) = f(u_3) - u_3 = u_2\ ,\ g(u_2) = f(u_2) - u_2 = u_1\ ,\ g(u_1) = f(u_1) - u_1 = 0\ .$$

Si bien que

$$0 = g(u_1) = g^2(u_2) = g^3(u_3)\ .$$

Cependant ici E_1 étant une droite, on n'aura, de toute façon guère de latitude pour choisir u_1.

On a :

$$\begin{aligned}(A - \mathrm{Id})^2 &= \begin{pmatrix}0 & -1 & 0\\1 & -1 & -1\\-1 & 0 & 1\end{pmatrix}^2\\ &= \begin{pmatrix}-1 & 1 & 1\\0 & 0 & 0\\-1 & 1 & 1\end{pmatrix}\end{aligned}$$

On cherche u_3 tel que $g^2(u_3) \neq 0$, et en prenant $u_3 := \begin{pmatrix}0\\0\\1\end{pmatrix}$, *on constate que l'on a effectivement $g^2(u_3) = u_1$. On a alors*

$$u_2 = g(u_3) = \begin{pmatrix}0\\-1\\1\end{pmatrix}\ .$$

La matrice inversible P vérifiant $A = PBP^{-1}$, est alors

$$P = \begin{pmatrix}1 & 0 & 0\\0 & -1 & 0\\1 & 1 & 1\end{pmatrix}\ .$$

d) Écrire la décomposition de DUNFORD de B (justifier).

Solution : *soit*

$$D := \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} \text{ et } N := \begin{pmatrix}0 & 1 & 0\\0 & 0 & 1\\0 & 0 & 0\end{pmatrix}\ .$$

Come $D = \mathrm{Id}$ D est un polynôme en B, et ainsi en va-t-il aussi de $N = B - D$. Il en résulte que D et N commutent ($DN = ND$.) Les matrices D (resp. N) étant diagonale (resp. nilpotente,) comme $B = D + N$, on a bien la décomposition de DUNFORD *de B (cf. cours IV.9.1.) À noter que la forme sous laquelle nous avons écrit B est même une réduite de* JORDAN *(cf. cours IV.10.)*

e) Pour $t \in \mathbb{R}$, calculer $\exp tB$.

Solution : *Notons, que la matrice N (cf. d),) est nilpotente d'échelon 3 (cf. cours IV.8.1,) i.e.*

$$N^2 \neq 0 \text{ et } N^3 = 0 .$$

Or :

$$\begin{aligned}
\exp tB &= \sum_{n=0}^{+\infty} \frac{1}{n!} t^n B^n \\
&= \sum_{n=0}^{+\infty} \frac{t^n}{n!} (D+N)^n \\
&= \sum_{n=0}^{+\infty} \frac{t^n}{n!} \left(D^n + nND^{n-1} n(n-1)N^2 D^{n-2}\right) \\
&= \sum_{n=0}^{+\infty} \frac{n^n}{n!} \left(D + nNn(n-1)N^2\right) \\
&= e^t D + te^t N + t^2 e^t N^2 \\
&= \begin{pmatrix} e^t & te^t & t^2 e^t \\ 0 & e^t & te^t \\ 0 & 0 & e^t . \end{pmatrix} .
\end{aligned}$$

f) Donner les solutions des systèmes différentiels

$$Y' = BY \text{ et } X' = AX .$$

Solution :

i) $(Y' = BY)$
Les solutions de $Y' = BY$, sont de la forme $\exp(tB)Y_0$ pour $Y_0 \in \mathbb{R}^3$.

ii) $(X' = AX)$
Pour tout $X \in \mathbb{R}^3$, posons $Y = PX$ où P est définie comme en c). Alors $X' = PY'$ et

$$X' = AX \Leftrightarrow PY' = APY \Leftrightarrow Y' = P^{-1}APY \Leftrightarrow Y' = BY .$$

Il en résulte que

$$Y = \exp(tB)Y_0 \Leftrightarrow X = PY = P\exp(tB)Y_0 .$$

2) Trouver la décomposition de DUNFORD de la matrice/endomorphisme

$$u = \begin{pmatrix} \alpha & x & z \\ 0 & \alpha & y \\ 0 & 0 & \beta \end{pmatrix} .$$

Solution : *On doit donc écrire $u = s + n$ où s est diagonalisable, où n est nilpotente et où s et n commutent. On sait que s et n peuvent être obtenues comme un polynôme d'endomorphismes en u.*
Soient

$$P_1 := (X-\alpha)^2 , \ P_2 := X - \beta .$$

Le polynôme caractéristique de u est $P_{\text{car } u} = P_1 P_2$. Notons $E := \mathbb{K}^3$ sur lequel opère u. On doit distinguer suivant que

$$\alpha = \beta \text{ ou } \alpha \neq \beta .$$

i) $(\alpha = \beta)$
Si $\alpha = \beta$,

$$s = \alpha \mathrm{Id} \text{ et } n = u - s \text{ conviennent.}$$

ii) $(\alpha \neq \beta)$

Dans ce cas P_1 *et* P_2 *sont premier entre eux et le lemme des noyaux (cf. cours IV.2.4.iii),) et le théorème de* CAYLEY–HAMILTON *(cf. cours IV.7.2,) assurent que*

$$E \;=\; \mathrm{Ker}\,(P_1(u)) \;\oplus\; \mathrm{Ker}\,(P_2(u))\;.$$

Les projecteurs sur $\mathrm{Ker}\,(P_1(u))$ *et* $\mathrm{Ker}\,(P_2(u))$ *sont donnés de la manière suivante : écrivons* $1 \;=\; UP_1 + VP_2$, *alors tout vecteur* $v \in E$ *s'écrit sous la forme*

$$v \;=\; (VP_2)(u)(v) \;+\; (UP_1)(u)(v)\;;$$

le projecteur sur $\mathrm{Ker}\,(P_1(u))$ *est donné par* $p_1 = (VP_2)(u)$ *; le projecteur sur* $\mathrm{Ker}\,(P_2(u))$ *est donné par* $p_2 \;=\; (UP_1)(u)$.

Alors,

$$s \;=\; S(u) \;\; \textit{avec} \;\; S \;=\; \alpha VP_2 \;+\; \beta UP_1\;.$$

Le polynôme $S \in \mathbb{K}[X]$ *est alors -solution du système :*

$$\begin{array}{rl} & \left\{\begin{array}{rcl} S & \equiv & \alpha\,[P_1] \\ S & \equiv & \beta\,[P_2] \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} S & \equiv & \alpha\,[(X-\alpha)^2] \\ S & \equiv & \beta\,[(X-\beta)] \end{array}\right\} \end{array}$$

dont on peut au moins discuter l'existence et l'unicité des solutions grâce au théorème chinois des restes.

$$\begin{array}{lrcl} \textit{On a} & (X-\alpha)^2 & = & (X-\beta)(X+\beta-2\alpha)+(\beta-\alpha)^2 \\ \textit{Donc} & (\beta-\alpha)^2 & = & (X-\alpha)^2-(X-\beta)(X+\beta-2\alpha) \\ \textit{d'où} & (\beta-\alpha)^2 S & = & \beta(X-\alpha)^2-\alpha(X-\beta)(X+\beta-2\alpha) \\ & & = & (\beta-\alpha)(X^2-2\alpha X+\beta\alpha) \\ & & = & (\beta-\alpha)((X-\alpha)^2-\alpha^2+\beta\alpha) \\ \text{et} & S & = & \frac{1}{\beta-\alpha}(X-\alpha)^2+\alpha\;. \end{array}$$

On trouve donc que

$$\begin{array}{rcl} s & = & \dfrac{1}{\beta-\alpha}(u-\alpha)^2+\alpha\mathrm{Id} \\ & = & \begin{pmatrix} \alpha & 0 & \frac{xz}{\beta-\alpha}+z \\ 0 & \alpha & y \\ 0 & 0 & \beta \end{pmatrix} \end{array}$$

La matrice n *se calcule par :*

$$\begin{array}{rcl} n & = & u-s \\ & = & \begin{pmatrix} 0 & x & -\frac{xz}{\beta-\alpha} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

Remarquons que si $x = 0$, *la matrice* u *est diagonalisable et on a bien* $n = 0$ *dans ce cas.*

Exercice B : Soit E un espace vectoriel de dimension finie et u un endomorphisme de E. Soit F (resp. G) un sous-espace cyclique de E pour u de polynôme minimal P (resp. Q). On suppose que P et Q sont premiers entre eux.

Montrer que F et G sont en somme directe et que la somme $F \oplus G$ est cyclique. Quel est son polynôme minimal ?

Solution : *Pour tout* $x \in F \cap G$,

$$P(u)(x) \;=\; Q(u)(x) \;=\; 0\;;$$

c'est-à-dire que

$$P^x_{\textit{min}\,u} | P \text{ et } P^x_{\textit{min}\,u} | Q\;.$$

Or $P \wedge Q \;=\; 1$, *si bien que* $P^x_{\textit{min}\,u} \;=\; 1$, *ce qui entraîne* $x \;=\; 0$ *et donc que la somme* $F + G$ *est directe.*

Soit $x \in F$ *(resp.* $y \in G$,*) un vecteur cyclique (cf. cours IV.4.2.iii),) pour* F *(resp.* G.*) Puisque* F *et* G *sont cycliques, ils sont stables par* u *; comme de plus ils sont en somme directe, pour tout* $R \in \mathbb{K}[X]$,

$$\begin{array}{rcrcl} & R(u)(x+y) & = & 0 & \\ \Leftrightarrow & R(u)(x)+R(u)(y) & = & 0 & \\ \Leftrightarrow & R(u)(x)=0 & \text{et} & R(u)(y)=0 & \\ \Leftrightarrow & P|R & \text{et} & Q|R & \\ \Leftrightarrow & PQ & | & R\;. & \end{array}$$

Il s'ensuit que $PQ|P^{(x+y)}_{\min u}$. *Si on note* $H := \mathrm{Vect}\big\{\{u^n((x+y))\}\,,n\in\mathbb{N}\big\}$ *l'espace cyclique engendré par* $x+y$, *il résulte de la relation de divisibilité ci-dessus que*

$$\dim H \;\geq\; \deg(P)+\deg(Q) \;=\; \dim F\oplus G\,.$$

Or $H \subset F \oplus G$ *donc*

$$H \;=\; F \oplus G\,.$$

Exercice C : $(P(u) = \sum P(\lambda_i)u_i)$

Soient E **un** $\mathbb{K}$**-espace vectoriel de dimension finie et** $u \in \mathrm{End}_{\mathbb{K}}(E)$.

1) On suppose u **diagonalisable et on note** $\lambda_1,\ldots,\lambda_p$ **ses valeurs propres supposées deux à deux distinctes.**

a) Montrer qu'il existe des endomorphismes $u_1,\ldots,u_p$ tels que pour tout polynôme $P \in \mathbb{K}[X]$, on ait :

$$P(u) \;=\; \sum_{i=1}^{p} P(\lambda_i)u_i\,. \qquad 1$$

Solution :

ii) ***(Condition nécessaire (analyse))***

Si une telle famille $u_{i\,,1\leq i\leq p} \in \mathrm{End}_{\mathbb{K}}(E)$ *existe, en particulier, pour* $P = X$, *on doit avoir*

$$u \;=\; \sum_{i=1}^{p} \lambda_i u_i\,.$$

Or u *étant diagonalisable, si on note* $E_{i\,,1\leq i\leq p}$ *les espaces propres respectivement associés aux* $\lambda_{i\,,1\leq i\leq p}$,

$$E \;=\; \bigoplus_{i=1}^{p} E_i\,.$$

Pour tout $x \in E$, *il existe donc un unique*

$$x_{i\,,1\leq i\leq p}\, x_i \;\in\; E_i \;\; \textit{tel que} \;\; x \;=\; \sum_{i=1}^{p} x_i\,.$$

On a alors :

$$\begin{aligned} u(x) &= u\big(\sum_{i=1}^{p} x_i\big) \\ &= \sum_{i=1}^{p} u(x_i) \\ &= \sum_{i=1}^{p} \lambda_i x_i\,; \end{aligned}$$

si bien qu'en posant $u_i(x) := x_i$, *on a*

$$\forall x\in E,\; u(x) \;=\; \sum_{i=1}^{p} \lambda_i u_i(x)\,.$$

L'endomorphisme u_i *est en fait la composée de l'inclusion naturelle* $E_i \hookrightarrow E$ *avec la projection de* E *sur* E_i *parallèlement à la somme directe*

$$\bigoplus_{1\,\leq\, j\,\leq\, p\;j\,\neq\, i} E_j\,.$$

*iii) (**Condition suffisante (synthèse)**)*

Pour tous

$$P \;:=\; \sum_{j=1}^{d} a_j X^j \;\in\; \mathbb{K}[X] \text{ et } x \;:=\; \sum_{i=1}^{p} x_{i\,,x_i \,\in\, E_i} \;\in\; E,$$

$$\begin{aligned} P(u)(x) &= \sum_{j=1}^{d} a_j u^j(x) \\ &= \sum_{j=1}^{p} a_j \big(\sum_{i=1}^{p} u^j(x_i)\big) \\ &= \sum_{j=1}^{d} a_j \big(\sum_{i=1}^{p} \lambda_i^j x_i\big) \\ &= \sum_{j=1}^{d} a_j \big(\sum_{i=1}^{p} \lambda_i^j u_i(x)\big) \\ &= \sum_{i=1}^{p} \big(\sum_{j=1}^{d} a_j \lambda_i^j\big) u_i(x) \\ &= \sum_{i=1}^{p} P(\lambda_i) u_i(x)\,. \end{aligned}$$

b) Montrer que pour tout $1 \;\leq\; i \;\leq\; p$, il existe un polynôme P_i tel que $u_i \;=\; P_i(u)$.

Solution :

*i) (**Remarque**)*

Les $u_{i\,,1\leq i\leq p} \in \mathrm{End}_{\mathbb{K}}(E)$, on été construits en a).ii) comme les projections sur les E_i. On peut alors utiliser le lemme des noyaux (cf. cours IV.2.4.iii),) qui assure que les projections sont des polynômes en u.

On n'a cependant pas établi en a) d'énoncé d'unicité assurant qu'on ne puisse pas choisir les $u_{i\,,1\leq i\leq p}$ autrement. Auquel cas il faut, sauf à établir un tel énoncé d'unicité, montrer que le fait que les u_i sont des polynômes en u, ne dépend que de a).1.

*ii) (**Condition nécessaire**)*

Si pour tout $1 \;\leq\; i \;\leq\; p$ un tel polynôme existe et que, simultanément a).1 est satisfaite,

$$u_i \;=\; P_i(u) \;=\; \sum_{j=1}^{p} P_i(\lambda_j) u_i\,.$$

*iii) (**Conditions suffisante**)*

L'identité ci-dessus sera clairement satisfaite dès que

$$P_i(\lambda_i) \;=\; 1 \text{ et } \forall 1 \leq j \leq p,\; j \;\neq\; i \;\Rightarrow\; P_i(\lambda_j) \;=\; 0\,.$$

Puisque les $\lambda_{i\,,1\leq i\leq p}$ sont deux à deux distincts le pollynôme

$$P_i \;:=\; \frac{\prod\limits_{1\,\leq\, j\,\leq\, p\;j\,\neq\, i} (X-\lambda_j)}{\prod\limits_{1\,\leq\, j\,\leq\, p\;j\,\neq\, i} (\lambda_i-\lambda_j)}$$

est bien défini et répond à la question.

2) Réciproquement, soit $u, u_1, \ldots, u_p \;\in\; \mathrm{End}_{\mathbb{K}}(E)$ et $\lambda_1, \ldots, \lambda_p \;\in\; \mathbb{K}$ tels que

$$\forall P \in \mathbb{K}[X],\; P(u) \;=\; \sum_{i=1}^{p} P(\lambda_i) u_i\,.$$

Montrer que u est diagonalisable et

$$\mathrm{Sp}(u) \;\subset\; \{\lambda_1, \ldots, \lambda_p\}\,.$$

Solution : *Considérons le polynôme*

$$P \;:=\; \prod_{i=1}^{p} (X - \lambda_i) \;\in\; \mathbb{K}[X]\,.$$

Pour tout $1 \;\leq\; i \;\leq\; p\; P(\lambda_i) \;=\; 0$, *ce qui entraîne que :*

$$\begin{aligned} P(u) &= \sum_{i=1}^{p} P(\lambda_i) u_i \\ &= 0\,. \end{aligned}$$

Le polynôme P *est donc un polynôme annulateur de* u *et* P *est scindé à racine simples donc* u *est diagonalisable. De plus* $P_{min\,u} | P$ *et* $\mathrm{Sp}(u)$ *s'identifie à l'ensemble des racines de* $P_{min\,u}$ *(cf. cours IV.5.1.)*

Exercice D : (**Sous-espace cyclique**)

Soient $\mathbb{K}$ **un corps,** E **un** $\mathbb{K}$**-espace vectoriel de dimension finie et** $f \;\in\; \mathrm{End}_{\mathbb{K}}(E)$ **un endomorphisme de** E**. Si** x **est un élément de** E**, on appelle *polynôme minimal de* f *en* x (cf. cours IV.2.2.iii),) le polynôme unitaire** $P^{x}_{\mathbf{min}\,f} \;\in\; \mathbb{K}[X]$ **de plus petit degré tel que** $P^{x}_{\mathbf{min}\,f}(f)(x) \;=\; 0$.

1) Montrer que pour tout $x \;\in\; E$, il existe un unique polynôme minimal en x et que $P^{x}_{\min f}$ divise le polynôme minimal $P_{\min f}$ de f.

Solution : *Pour tout* $x \;\in\; E$ *l'ensemble*

$$\mathrm{Ann}_{\mathbb{K}[X]}(x) \;:=\; \{P \;\in\; \mathbb{K}[X]\,;\; P(f)(x) \;=\; 0\}$$

est un idéal de $\mathbb{K}[X]$, *donc un idéal principal. Tous ses générateurs forment donc une unique classe d'association dont un seul représentant est unitaire, qu'on notera* $P^{x}_{min\,f}$ *et qu'on appelera le polynôme minimal de* f *en* x*. Il joue l'exact analogue du rôle de l'ordre d'un élément dans un groupe abélien (cf. cours II.5.2.iii).)*

Bien entendu

$$\forall x \in E,\; P_{min\,f}(x) \;=\; 0,$$

i.e. $P_{min\,f} \;\in\; \mathrm{Ann}_{\mathbb{K}[X]}(x)$ *i.e.*

$$P^{x}_{min\,f} | P_{min\,f}\,.$$

2) On suppose dans cette question que $\mathbb{K}$ **est infini.**

a) Montrer que si $F_1, \cdots, F_n$ sont des sous-espaces vectoriels de E tels que $E \;=\; \bigcup_i F_i$ alors il existe $1 \;\leq\; i \;\leq\; n$ tel que $F_i \;=\; E$.

Solution : *Raisonnons par récurrence sur le nombre* n *de sous-espaces :*

i) $(n \;=\; 1)$
Si $n \;=\; 1, E \;=\; F_1$ *et le résultat est immédiat.*

ii) (***Remarque***)
Rappelons pour mémoire, qu'on a certainement déjà montré un jour que

$$E \;=\; F_1 \;\cup\; F_2 \;\Rightarrow\; F_1 \;\subset\; F_2 \;\vee\; F_2 \;\subset\; F_1\,.$$

Ce résultat confirme que l'assertion que nous cherchons à démontrer est encore vraie pour $n \;=\; 2$*, mais ne nous sera pas utile dans la suite du raisonnement par récurrence. On peut cependant remarquer que l'on n'a pas utilisé, pour démontrer le cas ci-dessus, le fait que* $\mathbb{K}$ *est infini. On s'apercevra, cependant, en lisant attentivement la suite de la preuve, qu'on n'a besoin que de supposer que* $\#(\mathbb{K}) \;\geq\; n$*, et un corps a toujours au moins* 2 *éléments.*

iii) (n **quelconque**)
Considérons $F_{i\ ,1\leq i\leq n}\ \subset\ E$ *et* $G\ \subset\ E$ *des sous-espace vectoriels de* E *tels que*

$$E\ =\ G\ \cup\ \bigcup_{i=1}^{n} F_i\ .$$

$G\ =\ E$ *Si* $G\ =\ E$, *l'assertion est démontrrée.*
$G\ \neq\ E$ *On va alors montrer*

$$G\ \subset\ \bigcup_{i=1}^{n} F_i\ ;$$

ce qui entraînera

$$E\ =\ \bigcup_{i=1}^{n} F_i\ .$$

Si l'on suppose l'assertion vraie pour n *sous-espaces* E *sera alors l'un des* F_i *et l'on aura établi l'assertion pour* $n+1$ *sous-espaces.*
Montrons donc

$$G\ \subset\ \bigcup_{i=1}^{n} F_i\ .$$

Puisque $G\ \neq\ E$, *il existe*

$$x\ \in\ E\ ,\ x\ \notin\ G\ .$$

Pour tout $y\ \in\ G$ *et tout* $a\ \in\ \mathbb{K}\ x-ay\ \notin\ G$. *En effet*

$$x-ay\ \in\ G\ \Rightarrow\ x\ \in\ G\ .$$

Puisque

$$x-ay\ \in\ E\ ,\ x-ay\ \notin\ G\,\text{et}\,E\ =\ G\ \cup\ \bigcup_{i=1}^{n} F_i\ \exists 1\ \leq\ i\ \leq\ n\ ,\ x-ay\ \in\ F_i\ .$$

Puisque $\mathbb{K}$ *est infini, et contient donc au moins* $n+1$ *éléments*

$$\forall y\in G,\ \exists(a,b)\ \in\ \mathbb{K}\times\mathbb{K},\ a\ \neq\ b\ ,\ \exists 1\ \leq\ i\ \leq\ nx-ay\ \in\ F_i\,\text{et}\,x-by\ \in\ F_i\ ;$$

ce qui entraîne puisque $b-a\ \neq\ 0$,

$$y\ =\ \frac{1}{b-a}[(x-ay)-(x-by)]\ \in\ F_i$$

et achève la preuve.

b) En déduire qu'il existe $x\ \in\ E$ tel que $P^x_{\min f}$ soit le polynôme minimal $P_{\min f}$ de f.
Solution : *Notons* D *l'ensemble des diviseur unitaire de* $P_{min\,f}$ *dans* $\mathbb{K}[X]$. *Il découle, par exemple du théorème fondamental de l'arithmétique dans* $\mathbb{K}[X]$ *(cf. cours III.5.5.1,) que* D *est un ensemble fini. Soit*

$$L\ :=\ \{\ell\ \in\ \mathbb{K}[X]\,;\,\exists x\ \in\ E,\ \ell\ =\ P^x_{min\,f}\}\ \subset\ \mathbb{K}[X]\ .$$

On a alors (cf. question 1),) $L\ \subset\ D$ *ce qui implique en particulier que* L *est fini. Pour tout* $\ell\ \in\ L$, *notons*

$$F_\ell\ :=\ \{x\ \in\ E\,;\,P^x_{min\,f}|\ell\}\ =\ \{x\ \in\ E\,;\,\ell(f)(x)\ =\ 0\}\ =\ \operatorname{Ker}\ell(f)\ =\ \{x\ \in\ E\,;\,\ell\cdot x\ =\ 0\}\ =\ E[\ell]\ \subset\ E\ .$$

Les $F_{\ell\ ,\ell\ \in\ L}$ *sont donc des sous-espaces vectoriels de* E, *et (cf. question 1),)*

$$E\ =\ \bigcup_{\ell\ \in\ L} F_\ell\ .$$

Comme L *est fini il existe (cf. a) ,)*

$$\ell\ \in\ LE\ =\ F_\ell\ .$$

Or par définition de L, *il existe*

$$x\ \in\ EP^x_{min\,f}\ =\ \ell\ .$$

En outre, par définition de F_ℓ

$$\forall y\in F_\ell,\ \ell(f)(y)\ =\ 0\ \textit{i.e.}\ \forall y\in E,\ \ell(f)(y)\ =\ 0\ ;$$

c'est-à-dire que $P_{min\,f}|\ell$. *Or par hypothèse,* $\ell|P_{min\,f}$ *si bien que*

$$\ell\ =\ P_{min\,f}\ .$$

Or $\ell\ =\ P^x_{min\,f}$ *donc*

$$P_{min\,f}\ =\ P^x_{min\,f}\ .$$

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Document n° VII

20 avril 2020

Vers le théorème de réduction de FROBENIUS

n° VII.0 . –Introduction

Le principe des théorèmes de réduction étudiés au chapitre IV est de justifier l'existence, (voire d'expliciter la construction) de bases dans lesquelles un endomorphisme donné sécrit de « manière plus simple » : correspondant le plus souvent à une écriture de la matrice diagonale par bloc ; lesquels blocs peuvent, dans les meilleurs cas être caractérisés.

On a vu (cf. Problème n° II, exercice E,) que de tels énoncés (en particulier le théorème IV.10.10 de réduction de JORDAN,) permettent de montrer, qu'une classe de similitude d'endomorphismes nilpotents est caractérisée (entièrement déterminée) par au moins deux suites numériques n_i ,$1\leq i\leq \varepsilon$ (la suite des dimension des noyaux itérés) et r_i ,$1\leq i\leq m$ la suite des dimension des blocs de JORDAN. On a également constaté que le théorème IV.9.3 de décomposition de DUNFORD permet de considérer, d'une part le cas des endomorphismes diagonalisables, et d'autrepart celui des endomorphisme nilpotents. Ce dernier résultat permettant également de répondre à des questions pratiques (cf. TD n° VI, exercice A, question 1), f).)

Néanmoins les deux résultats cités ci-dessus, à savoir le théorème IV.9.3 de décomposition de DUNFORD et le théorème IV.10.10 de réduction de JORDAN requièrent que le polynôme minimal (ou le polynôme caractéristique) de l'endomorphisme considéré soit scindé, *i.e.* que ses facteurs irréductibles soient de degré 1. Ce n'est pas du tout une restriction dès qu'on s'intéresse à des espaces vectoriels sur le corps $\mathbb{C}$ des nombres complexes, ou n'importe quel corps algébriquement clos. Cependant ils interdisent absolument de classifier des matrices

$$\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$$

et ne renseignent absoluement pas sur le fait de savoir que de telles matrices seraient, en quelques sorte les « plus élémentaires » qu'on puisse trouver ; ou de manière équivalente, qu'il existerait, pour tout endomorphisme d'un $\mathbb{R}$-espace vectoriel une base dans laquelle sa matrice serait diagonale par blocs, la dimension de chaque bloc étant majorée par 2. On peut avoir l'intuition que la dimension maximale des blocs dans une écriture diagonale est le degré maximal d'un polynôme irréductible dans $\mathbb{K}[X]$ sans avoir jusqu'ici les moyens de justifier un tel énoncé.

Le théorème IV.11.5 de réduction de FROBENIUS établit, entre autre, la véracité d'un tel énoncé. Il s'ensuit que les polynôme irréductibles dans $\mathbb{R}[X]$ étant au plus de degré 2, on sera en mesure d'écrire une matrice réelle sous une forme diagonale par blocs, dans laquelle la taille des blocs ne dépassra pas 2. L'existence, en revanche, de nombreux polynômes irréductibles dans $\mathbb{Q}[X]$, et notamment le fait qu'il en existe de tous degrés, augmente considérablement la complexité des formes réduites possibles des matrices de $\mathcal{M}_n(\mathbb{Q})$.

De surcroît contrairement aux deux résultats de décomposition de DUNFORD et de réduction de JORDAN le théorème IV.11.5 de réduction de FROBENIUS s'applique sans aucune hypothèse concernant le polynôme minimal ou caractéristique de l'endomorphisme.

Enfin l'importance d'un énoncé comme le théorème IV.11.5 de réduction de FROBENIUS se justifie, dans la présentation que nous avons donnée dans ce cours, par le fait qu'il entre comme ingrédient principal dans la preuve du théorème IV.10.10 dont nous avons déjà vu un certain nombre d'applications (cf. Problème n° II.)

Si même on pouvait éviter d'avoir recours au théorème de réduction de FROBENIUS pour établir le théorème de réduction de JORDAN, il est vraisemblable qu'on échappe difficilement à la construction d'un suplémentaire stable à un sous-espace donné que nous allons présenter an n° VII.2 et qui constitue l'un des deux arguments de l'existence (cf. IV.11.5.1),) d'une réduction de FROBENIUS. Le théorème IV.11.5 de réduction de FROBENIUS est en effet l'exact analogue, dans la correspondance entre endomorphismes et $\mathbb{K}[X]$-modules (cf. IV.1,) du théorème II.10.5 de structure des groupes abéliens finis ; et par conséquent un cas particulier du théorème B.6.13 de structure des modules de torsion sur un anneau principal. Or, à chaque fois, dès qu'on a mis en évidence un premier sous-module cyclique (maximal) C il s'agit de justifier que la suite

$$0 \to C \longrightarrow M \longrightarrow Q \to 0 \text{ (cf. II.10.2.1 , B.6.4.1)}$$

est scindée, c'est-à-dire que $M \cong C \oplus Q$. On sait qu'on a pu donner un argument ad hoc dans le cas des groupes abéliens (cf. II.10.4 ;) et que dans le cas général (cf. B.6.7,) l'argument est assez délicat. Nous allons voir, (cf. n° VII.2,) que dans le cas de la réduction des endomorphismes, des arguments d'algèbre linéaire, pour l'essentiel, permettent de construire un sous-espace vectoriel stable.

n° VII.1 . −Notations

Dans la suite $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$, E un κ-espace vectoriel de dimension finie $n \in \mathbb{N}^*$, $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E de polynôme minimal (cf. cours IV.2.2.iv)) $P_{\min u} \in \mathbb{K}[X]$ et de polynome caractéristique (cf. cours IV.6.1) $P_{\mathrm{car}\, u} \in \mathbb{K}[X]$.

On sait alors, au moins dans le cas où $\mathbb{K}$ est infini, qu'il existe (cf. TD n° VI, exercice D, question 2), b),) un sous-espace cyclique (cf. cours IV.4.2,) $C \subset E$ de polynôme minimal $P_{\min u}$. Pour peu donc qu'on puisse construire un sous-$\mathbb{K}$-espace vectoriel S supplémentaire de C et stable par u un argument de récurrence sur la dimension de E donne presque immédiatement l'énoncé IV.11.5.1) d'existence dans le théorème de réduction de FROBENIUS.

Remarque n° VII.1.1 Remarquons une fois encore, même si nous l'avons déjà signalé à plusieurs reprises, que dans le cas général des modules de torsion sur un anneau principal (cf. cours B.6,) c'est précisément le défaut d'existence d'un invariant numérique comme la dimension (le cardinal dans le cas des groupes abéliens (cf. cours II.10,)) qui interdit le genre de raisonement par récurrence q'uon fait ici.

Remarque n° VII.1.2 L'essentiel de la difficulté dans la construction n° VII.2 réside dans le fait qu'on exige du supplémentaire S de C qu'il soit stable par u ; sans quoi on ne disposerait pas d'un nouveau couple $(S, u_{|S})$ auquel appliquer l'hypothèse de récurrence. Ceci revient en fait à demander que la décomposition $C = C \oplus S$ soit non seulement une décomposition de E vu comme $\mathbb{K}$-espace vectoriel mais encore comme $\mathbb{K}[X]$-module.

n° VII.2 . −Sous-espaces stables

Notation n° VII.2.0 On reprend les notation de n° VII.1 et on suppose donné un sous-$\mathbb{K}$-espace cyclique stable maximal $C \subset E$, *i.e.*tel que

$$u(C) \subset C \text{ et } d := \dim_{\mathbb{K}} C = \deg(P_{\min u}) \text{ (cf. IV.4.1 .)}$$

On propose de répondre aux questions (question 1) à question 8)) suivantes qui conduirons à l'énoncé n° VII.2.9. Les réponses aux questions se trouvent au paragraphe n° VII.3. Il s'agit en fait de reprendre les étapes de la démonstration de la proposition IV.11.3 dont la rédaction dans le cours comporte d'ailleurs un certain nombre de typos et de problèmes de notations.

On conseille enfin d'étudier la dernière étape conduisant de l'énoncé n° VII.2.9 à l'énoncé IV.11.5.1). Bien entendu la question IV.11.5.2) requiert d'autres arguments que nous nous proposons de présenter lors de la prochaine séance.

1) Montrer qu'il existe $e_1 \in C$ tel que $u^i(e_1)\,,0 \leq i \leq d-1$ est une base de C dans laquelle la matrice de la restriction $u_{|C}$ de u à C est $\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}$.

Dans la suite, on note

$$f^{i-1}(e_1) = e_i\,,1\leq i\leq d$$

qu'on complète en une base $e_i\,,d+1\leq i\leq n$ de E. Notons alors $e_i^*\,,1\leq i\leq n \in E^*$ sa base duale.

2) Montrer que

$$\forall \alpha_i\,,0\leq i\leq d-1 \in \mathbb{K},\ e_d^*\big(\sum_{i=0}^{d-1} \alpha_i u^i(e_1)\big) = \alpha_{d-1}\,.$$

On note désormais

$$\begin{aligned} S &:= \{x \in E\,;\, \mathbb{K}[X]\cdot x \subset \mathrm{Ker}\, e_d^*\} \\ &= \{x \in E\,;\, \forall P \in \mathbb{K}[X],\ P\cdot x \in \mathrm{Ker}\, e_d^*\} \\ &= \{x \in E\,;\, \forall P \in \mathbb{K}[X],\ P(u)(x) \in \mathrm{Ker}\, e_d^*\}\,. \end{aligned}$$

3) Montrer que l'ensemble S est un sous-$\mathbb{K}$-espace vectoriel de E stable par u (*i.e.* un sous-$\mathbb{K}[X]$-module de (E, u).

4) Montrer que

$$C \cap S = 0\,.$$

5) Montrer que l'application

$$\phi \,:\, \mathbb{K}[X] \,\to\, E^* \,,\; P \,\mapsto\, e_d^* \circ P(u)$$

est un morphisme $\mathbb{K}$-linéaire dont le noyau est $\mathbb{K}[X]P_{\min u}$.

6) En déduire qu'il existe un unique morphisme $\mathbb{K}$-linéaire injectif $\overline{\phi}$ tel que le diagramme suivant, où la flèche vertical est la surjection canonique, soit commutatif :

$$\begin{array}{rcl} \mathbb{K}[X] & \xrightarrow{\;\phi\;} & E^* \\ \downarrow & \nearrow \overline{\phi} & \\ \mathbb{K}[X]/(\mathbb{K}[X]P_{\min u}) & & \end{array}$$

7) Notons

$$F \,:=\, \mathrm{Im}\,\overline{\phi} \,\subset\, E^* \,.$$

Montrer que :

$$\begin{array}{rcl} S & = & F^\perp \\ & = & \{x \,\in\, E \,;\, \forall f \in F,\; f(x) \,=\, 0\} \,. \end{array}$$

8) Montrer que

$$\dim_{\mathbb{K}} S \,+\, \dim_{\mathbb{K}} C \,=\, \dim_{\mathbb{K}} E \,.$$

Proposition n° VII.2.9 *Le sous-espace cyclique C de E possède un supplémentaire S stable par u.*

n° VII.3 . −Solutions

1) Montrer qu'il existe $e_1 \,\in\, C$ tel que $u^i(e_1)\,,0 \,\leq\, i \,\leq\, d-1$ est une base de C dans laquelle la matrice de la restriction $u_{|C}$ de u à C est $\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}$.

Solution : *(cf. cours IV.4.1.)*

Dans la suite, on note

$$f^{i-1}(e_1) \,=\, e_i\,,1\leq i\leq d$$

qu'on complète en une base $e_i\,,d+1\leq i\leq n$ de E. Notons alors $e_i^*\,,1\leq i\leq n \,\in\, E^*$ sa base duale.

2) Montrer que

$$\forall \alpha_i\,,0\leq i\leq d-1 \in \mathbb{K},\; e_d^*\big(\sum_{i=0}^{d-1} \alpha_i u^i(e_1)\big) \,=\, \alpha_{d-1} \,.$$

Solution : *En effet :*

$$\begin{array}{rcl} e_d^*\big(\sum_{i=0}^{d-1} \alpha_i u^i(e_1)\big) & & \\ & = & e_d^*\big(\sum_{i=0}^{d-1} \alpha_i e_{i+1}\big) \\ & = & \sum_{i=1}^{d} \alpha_{i-1} e_d^*(e_i) \\ & = & \alpha_{d-1} \,. \end{array}$$

On note désormais

$$\begin{aligned} S &:= \{x \in E\,;\, \mathbb{K}[X]\cdot x \subset \operatorname{Ker} e_d^*\} \\ &= \{x \in E\,;\, \forall P \in \mathbb{K}[X],\ P\cdot x \in \operatorname{Ker} e_d^*\} \\ &= \{x \in E\,;\, \forall P \in \mathbb{K}[X],\ P(u)(x) \in \operatorname{Ker} e_d^*\}\,. \end{aligned}$$

3) Montrer que l'ensemble S est un sous-$\mathbb{K}$-espace vectoriel de E stable par u (*i.e.* un sous-$\mathbb{K}[X]$-module de (E,u)).
Solution : *Bien entendu* $0 \in S$ *si bien que* $S \neq \emptyset$.

i) (S ***est un sous-***$\mathbb{K}[X]$***-module de*** (E,u)*.)*
Pour tout

$$(x_1,x_2) \in S\times S\,,\ \textit{tout}\,(A_1,A_2) \in \mathbb{K}[X]\times\mathbb{K}[X]\,,\ \textit{tout}\,P \in \mathbb{K}[X],$$

$$\begin{aligned} e_d^*\big(P\cdot(A_1\cdot x_1 + A_2\cdot x_2)\big) &= e_d^*\big((PA_1)\cdot x_1 + (PA_2)\cdot x_2\big) \\ &= e_d^*[(PA_1)\cdot x_1] + e_d^*[(PA_2)\cdot x_2] \\ &= 0\,; \end{aligned}$$

si bien que

$$A_1\cdot x_1 + A_2\cdot x_2 \in S$$

assurant que S *est un sous-*$\mathbb{K}[X]$*-module de* E.

*ii) (**Autre argument**)*
On pourrait montrer « à la main » sans utiliser explicitement la structure de $\mathbb{K}[X]$*-modules que* S *est un sous-espace vectoriel stable par* u*. La stabilité de* S *par combinaison linéaire à coefficients dans* $\mathbb{K}$ *est très élémentaires à vérifier. Ensuite pour tout* $x \in S$ *et tout* $P \in \mathbb{K}[X]$,

$$P\cdot x = P(u)(x) \in \operatorname{Ker} e_d^*\,.$$

Or $P(u)[u(x)] = (XP)(u)(x)$ *si bien que*

$$e_d^*\big[P(u)[u(x)]\big] = e_d^*\big[(XP)(u)(x)\big] = 0$$

si bien que $u(x) \in S$.

4) Montrer que

$$C \cap S = 0\,.$$

Solution : *Soit* $x \in S\cap C$*. En particulier* $x \in C$ *si bien qu'il existe*

$$\alpha_{i\,,1\le i\le d} \in \mathbb{K} \ \textit{tel que}\ x = \sum_{i=1}^{d}\alpha_i e_i = \sum_{i=1}^{d}\alpha_i u^{i-1}(e_1)\,.$$

Par ailleurs, puisque $x \in S$*, pour tout* $n \in \mathbb{N}$,

$$e_d^*(X^n\cdot x) = e_d^*[u^n(x)] = 0\,.$$

Alors :

$$\begin{aligned} \forall 0\le j\le d-1,\quad 0 &= e_d^*(X^j\cdot x) \\ &= e_d^*\big(u^j[\sum_{i=1}^{d}\alpha_i u^{i-1}(e_1)]\big) \\ &= e_d^*\big(\sum_{i=1}^{d}\alpha_i u^{i+j-1}(e_1)\big) \\ &= \alpha_{d-j}\,. \end{aligned}$$

Il s'ensuit que $x = 0$.

5) Montrer que l'application

$$\phi \,:\, \mathbb{K}[X] \,\to\, E^* \,,\; P \,\mapsto\, e_d^* \circ P(u)$$

est un morphisme $\mathbb{K}$-linéaire dont le noyau est $\mathbb{K}[X]P_{\min u}$.

Solution :

$*$) (ϕ **est** $\mathbb{K}$**-linéaire**)

Puisque u *est un endomorphisme* $\mathbb{K}$*-linéaire de* E*, pour tout* $P \in \mathbb{K}[X]$, $P(u)$ *est encore un endomorphisme* $\mathbb{K}$*-linéaire de* E *et*

$$\phi(P) \,:=\, e_d^* \circ P(u)$$

est donc bien une forme $\mathbb{K}$*-linéaire sur* E *i.e. un élément de* E^*.

$$\begin{array}{l} \forall (P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X], \\ \forall (a,b) \in \mathbb{K} \times \mathbb{K}, \\ \forall x \in E, \end{array} \qquad \begin{array}{rcl} \phi(aP+bQ)(x) & = & e_d^*\big((aP+bQ)(u)(x)\big) \\ & = & e_d^*\big((aP(u)+bQ(u))(x)\big) \\ & = & e_d^*\big(aP(u)(x)+bP(u)(x)\big) \\ & = & a(e_d^* \circ P(u))(x) + b(e_d^* \circ Q(u))(x) \\ & = & a\phi(P)(x) + b\phi(Q)(x) \end{array}$$

d'où il résulte que

$$\phi(aP+bQ) \,=\, a\phi(P) \,+\, b\phi(Q)\,.$$

†) ($\mathbb{K}[X]P_{\min u} \,\subset\, \operatorname{Ker}\phi$)

En outre, pour tout $P \in \mathbb{K}[X]P_{\min u}$, $P_{\min u}|P$ *si bien que* $P(u) \,=\, 0$, *ce qui entraîne*

$$\phi(P) \,=\, e_d^* \circ P(u) \,=\, 0$$

et donc

$$\mathbb{K}[X]P_{\min u} \,\subset\, \operatorname{Ker}\phi\,.$$

Soit $P \in \operatorname{Ker}\phi$.

‡) ($(P(u)(e_i) \,=\, P\cdot E_i \,\in\, \operatorname{Ker} e_d^*$)

$e_d^* \circ P(u) \,=\, 0$. *En particulier, pour tout* $1 \,\le\, i \,\le\, d$,

$$e_d^*\big(P(u)[e_i]\big) \,=\, 0\,.$$

Or $e_i \,\in\, C$, *et* C *est stable par* u *donc* $P(u)(e_i) \,\in\, C$, *si bien que*

$$\forall 1 \le i \le d,\; P\cdot e_i \,=\, P(u)(e_i) \,\in\, C \cap \operatorname{Ker} e_d^*\,. \qquad 1$$

§) ($P\cdot e_i \,\in\, S$)

Or pour tout $j \,\in\, \mathbb{N}$

$$X.j\cdot e_i \,=\, u^j(e_i) \,\in\, C$$

puisque C *est stable sous* u, *si bien qu'il existe*

$$\alpha_{i,j\,,1\,\le\,j\,\le\,d} \,\in\, \mathbb{K} \;\; \textit{tel que} \;\; X^j\cdot e_i \,=\, \sum_{1=j}^{d} \alpha_{i,j} e_j\,.$$

Par conséquent :

$$\begin{array}{rcll} e_d^*\big(X^j\cdot P(u)(e_i)\big) & = & e_d^*\big((X^jP)\cdot e_i\big) & \\ & = & e_d^*\big(P\cdot[X^j\cdot e_i]\big) & \\ & = & e_d^*\big(P\cdot[\sum_{j=1}^{d}\alpha_{i,j}e_j]\big) & 1 \\ & = & \sum_{j=1}^{d}\alpha_{i,j}e_d^*[P\cdot e_j] & \\ & = & 0 \text{ d'après ‡).1.} & \end{array}$$

Puisque $\operatorname{Ker} e_d^*$ *est un* $\mathbb{K}$*-espace vectoriel, il découle de 1 que, pour tout* $Q \,\in\, \mathbb{K}[X]$,

$$Q\cdot(P\cdot e_i) \,\in\, \operatorname{Ker} e_d^*$$

c'est-à-dire que

$$\mathbb{K}[X]\cdot(P\cdot e_i) \,\subset\, \operatorname{Ker} e_d^*\,.$$

Il s'ensuit que $P\cdot e_i \,\in\, S$.

¶) *$(P(u)_{|C} = 0)$*
Or $P \cdot e_i \in C$, et d'après question 4), $C \cap S = \{0\}$. Donc

$$P(u)(e_i) = P \cdot e_i = 0 \,. \qquad 1$$

Comme e_i ,$1 \leq i \leq d$ est une base de C, il s'ensuit que $P(u)_{|C} = 0$.

‖) *($P_{\min u}|P$)*
Il s'ensuit que

$$P_{\min u_{|C}}|P \,.$$

Or C est précisément construit de sorte que

$$P_{\min u} = P_{\min u_{|C}}$$

ce qui termine la preuve.

6) En déduire qu'il existe un unique morphisme $\mathbb{K}$-linéaire injectif $\overline{\phi}$ tel que le diagramme suivant, où la flèche vertical est la surjection canonique, soit commutatif :

$$\begin{array}{rcl} \mathbb{K}[X] & \xrightarrow{\phi} & E^* \\ \downarrow & \nearrow \overline{\phi} & \\ \mathbb{K}[X]/(\mathbb{K}[X]P_{\min u}) & & \end{array}$$

Solution : *Remarquons que $\mathbb{K}[X]P_{\min u}$ est un idéal de $\mathbb{K}[X]$ donc un sous-$\mathbb{K}[X]$-module de KkX lui-même. C'est donc aussi (cf. cours IV.1.2.iii),) un sous-$\mathbb{K}$-espace vectoriel de $\mathbb{K}[X]$* [10]*. Ceci peut également se déduire du fait, que dans question 5), on a identifié*
$\mathbb{K}[X]P_{\min u}$ au noyau d'une application $\mathbb{K}$-linéaire.
Il suffit désormais d'appliquer la factorisation des morphismes de κ-espaces vectoriels à ϕ.

7) Notons

$$F := \operatorname{Im}\overline{\phi} \subset E^* \,.$$

Montrer que :

$$\begin{array}{rcl} S & = & F^{\perp} \\ & = & \{x \in E \,;\, \forall f \in F,\ f(x) = 0\} \,. \end{array}$$

Solution :

∗) *($S \subset F^{\perp}$)*
Pour tout $x \in S$, par définition $\mathbb{K}[X] \cdot x \subset \operatorname{Ker} e_d^*$ c'est-à-dire que :

$$\begin{array}{lrcl} \forall P \in \mathbb{K}[X], & P \cdot x & \in & \operatorname{Ker} e_d^* \\ \Leftrightarrow & e_d^*(P \cdot x) & = & 0 \\ \Leftrightarrow & e_d^*[P(u)(x)] & = & 0 \\ \Leftrightarrow & \phi(P)(x) & = & 0 \\ \Leftrightarrow & S & \subset & ({}^{\perp}\operatorname{Im}\phi) \\ & & = & ({}^{\perp}\operatorname{Im}\overline{\phi}) \\ & & = & F^{\perp} \,. \end{array}$$

†) *($F^{\perp} \subset S$)*

$$\begin{array}{lrcl} \forall x \in F^{\perp},\ \forall P \in \mathbb{K}[X], & \phi(P)(x) & = & 0 \\ \Leftrightarrow & e_d^*[P(u)(x)] & = & 0 \\ \Leftrightarrow & P \cdot x & \in & \operatorname{Ker} e_d^* \\ \Leftrightarrow & x & \in & S \,. \end{array}$$

ce qui achève la preuve.

10. Ni l'un ni l'autre d'ailleurs n'étant de $\mathbb{K}$-dimension finie alors qu'ils sont de type fini come $\mathbb{K}[X]$-modules.

8) Montrer que

$$\dim_{\mathbb{K}} S \ + \ \dim_{\mathbb{K}} C \ = \ \dim_{\mathbb{K}} E \ .$$

Solution : *On déduit de question 6) que*

$$\dim_{\mathbb{K}} \operatorname{Im} \overline{\phi} \ = \ \dim_{\mathbb{K}} \mathbb{K}[X]/\mathbb{K}[X]P_{\mathit{min}\,u} \ .$$

Or $\mathbb{K}[X]/\mathbb{K}[X]P_{\mathit{min}\,u}$ *est un* $\mathbb{K}[X]$*-module cyclique au sens de la définition IV.4.2, si bien qu'en vertu de la proposition IV.4.1,*

$$\dim_{\mathbb{K}} \mathbb{K}[X]/\mathbb{K}[X]P_{\mathit{min}\,u} \ = \ \deg(P_{\mathit{min}\,u}) \ = \ d \ = \ \dim_{\mathbb{K}} C \ .$$

C'est un résultat connu de dualité dans les espaces vectoriels que

$$\dim_{\mathbb{K}} F \ + \ \dim_{\mathbb{K}} F^{\perp} \ = \ \dim_{\mathbb{K}} E$$

et qui permet de conclure.

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Document n° VIII

24 avril 2020

Corrigé du TD n° VII

Exercice A : (**Endomorphismes nilpotents**)
Soit $u \in \mathrm{End}_{\mathbb{K}}(E)$.
Montrrer que :

1) u est nilpotent d'échlon d si et seulement si $P_{\min u} = X^d$.
Solution : *Si u est nilpotent d'échelon d (cf. cours IV.8.1,)*

$$u^d = 0 \text{ et } u^{d-1} \neq 0 .$$

Ainsi X^d est un polynôme annulateur de u i.e.$P_{min\,u} | X^d$; et puisque $u^{d-1} \neq 0$,

$$P_{min\,u} = X^d .$$

Le sens réciproque est immédiat.

2) u est nilpotent d'échelon d et cyclique si et seulement si

$$u \text{ est cyclique et } \dim_{\mathbb{K}} E = d .$$

Solution : *Supposons donc que u est cyclique (cf. cours IV.4.2.)*
Si u est nilpotent d'échelon d,

$$P_{min\,u} = X^d \text{ (cf. question 1) .)}$$

Puisque u est cyclique

$$\dim_{\mathbb{K}} E = \deg(P_{min\,u}) = d \text{ (cf. cours IV.4.1.)}$$

La réciproque n'a en fait pas vraiment de sens.

3) u est nilpotent d'échelon d si et seulement si u est nilpotent de rang $d-1$.
Solution : *C'est évidemment faux si on ne suppose pas u cyclique.*

i) Si maintenant u est cyclique et d'échelon d, on sait qu'il existe un vecteur $e_1 \in E$ cyclique pour u et qu'alors

$$u^{i-1}(e_1)\,, 1 \leq i \leq d \text{ est une base de } E .$$

Il en résulte immédiatement que

$$u^{i-1}(e_1)\,, 2 \leq i \leq d \text{ est une famille libre dans } \mathrm{Im}\, u ;$$

ce qui entraîne que

$$\dim_{\mathbb{K}} \mathrm{Im}\, u \geq d-1 .$$

Or $u[u^{-1}(e_1)] = u^d(e_1) = 0$; ce qui entraîne que $\dim_{\mathbb{K}} \mathrm{Ker}\, u \geq 1$. Il s'ensuit finalement que $\mathrm{rg}(u) = d-1$.

ii) réciproquement, supposons que $\mathrm{rg}(u) = d-1$. Puisque u et cyclique et nilpotent il existe

$$k = \dim_{\mathbb{K}} E \in \mathbb{N}, e_1 \in E \text{ tels que } u^{k-1} \neq 0\,,\ u^k = 0 \text{ et } u^{i-1}(e_1)\,, 1 \leq i \leq k \text{ est une base de } E .$$

Par le même argument qu'en i) on a alors

$$d-1 = k-1 .$$

Exercice B : Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que $V = \oplus_{i=1}^{4} V_i$ où les sous-espaces vectoriels V_i sont des sous-espaces stables par u, cycliques pour u de polynôme minimal respectif x, x, $x(x-1)$, $(x-1)^2$.

1) Quelle est la dimension de V ?

Solution : *La dimension d'un espace cyclique est égale au degré de son polynôme minimal (cf. cours IV.4.1 ;) si bien que V est de dimension 6.*

2) Donner les invariants de similitude de V et écrire une décomposition de FROBENIUS de u.

Solution : *Soit $W_1 = V_2 \oplus V_4$. Comme les polynômes minimaux de V_2 et V_4 sont premiers entre eux, W_1 est un espace cyclique de polynôme minimal $(x-1)^2 x$. On a donc $V = W_1 \oplus V_3 \oplus V_1$ avec $\mu_{V_3} | \mu_{V_3} | \mu_{W_1}$.*

Par unicité des invariants de similitude (cf. cours IV.11.5.2),) ces invariants sont donc $(x(x-1)^2, x(x-1), x)$.

Exercice C : 1) Soient P_1, P_2, P_3, P_4 des polynômes unitaires de $\mathbb{Q}[x]$ irréductibles et distincts deux à deux.

Donner le nombre de classes de similitude des matrices à coefficients dans $\mathbb{Q}$

$$\text{de polynôme caractéristique } P_{\text{car}} \ = \ \pm P_1^7 P_2^6 P_3^7 P_4^4$$

(décomposition de P en facteurs irréductibles) et

$$\text{de polynôme minimal } P_{\text{min}} \ = \ P_1^6 P_2^2 P_3^3 P_4^3 \ .$$

On justifiera en énonçant en particulier le théorème utilisé sur les invariants des classes de similitude.

Solution : *Si M est une matrice de polynôme caractéristique $P_{car} \ = \ \pm P_1^7 P_2^6 P_3^7 P_4^4$*

$$M \ \in \ \mathcal{M}_d(\mathbb{Q}) \ \text{avec} \ d \ = \ 7\deg(P_1) \ + \ 6\deg(P_2) \ + \ 7\deg(P_3) \ + \ 4\deg(P_4) \ .$$

Deux matrices de $\mathcal{M}_d(\mathbb{Q})$ sont semblables si et seulement si elles ont les mêmes invariants de similitude (cf. cours IV.11.8) $\mu_{i\ ,1\leq i\leq r}$. On sait alors que

$$P_{min} \ = \ \mu_1 \ , \ P_{car} \ = \ \prod_{I=1}^{r} \mu_i \ , \ \forall 1 \leq i \leq r-1, \ \mu_{i+1} | \mu_i \ . \qquad 1$$

Dénombrer les classes de similitude, ou les caractériser équivaut donc, à dénombrer, ou caractériser, les suites

$$\mu_{i\ ,1\leq i\leq r} \ \in \ \mathbb{Q}[X] \ \text{satisfaisant 1} \ .$$

Il en résulte que, si une telle suite $\mu_{i\ ,1\leq i\leq r}$ existe,

$$\prod_{i=2}^{r} \mu_i \ = \ P_1 P_2^4 P_3^4 P_4 \ .$$

Il s'ensuit que

$$r \ \leq \ 5 \ , \ P_1 P_4 | \mu_2 \ , \ \forall 3 \leq i \leq r, \ P_1 \ \not| \mu_i \ \text{et} \ P_4 \ \not| \mu_i \ .$$

Si $\alpha_{i\ ,2\leq i\leq r}$ est la valuation P_2-adique de μ_i, i.e.la plus grande puissance de P_2 qui divise μ_i, on a $\alpha_2 + \ldots + \alpha_r \ = \ 4$ avec $\alpha_2 \geq \alpha_3 \ldots \geq \alpha_r$. Autrement dit, on cherche le nombre de partitions de 4. Il y en a 5 :

$$4 \ = \ 4 \ , \ 4 \ = \ 3+1 \ , \ 4 \ = \ 2+2 \ , \ 4 \ = \ 2+1+1 \ , \ 4 \ = \ 1+1+1+1 \ .$$

De même pour P_3. On trouve donc 25 classes de similitude.

On pourra chercher à déterminer, pour quatres nombres premiers deux à deux distincts p_1, p_2, p_3, p_4 le nombre de classes d'isomorphismes de groupes abéliens de cardinal $p_1^7 p_2^6 p_3^7 p_4^4$ et d'exposant $p_1^6 p_2^2 p_3^3 p_4^3$.

2) Soient P_1, P_2, P_3 trois polynômes irréductibles distincts sur un corps K.

a) Combien y a-t-il de classes de similitude de matrices à coefficients dans K ayant comme polynôme minimal $P_1 P_2^2 P_3^2$ et comme polynôme caractéristique $P_1^3 P_2^3 P_3^4$? Pour chacune d'elles, donner les invariants de similitude.

Les classes de similitude sont en bijection avec les suites de polynômes $(\mu_1, \mu_2, \ldots)$ avec $\mu_i | \mu_{i-1}$, $\mu_1 = P_1 P_2^2 P_3^2$ et $\prod \mu_i = (P_1 P_2 P_3)^3$. Elles sont nécessairement de la forme

$$(P_1 P_2^2 P_3, P_1 P_2 P_3^{r_1}, P_1 P_3^{r_2})$$

avec $r_2 \leq r_1 \leq 2$ et $r_1 + r_2 + 1 = 3$. D'où deux solutions :

$$(P_1 P_2^2 P_3, P_1 P_2 P_3, P_1 P_3)$$

$$(P_1 P_2^2 P_3, P_1 P_2 P_3^2, P_1)$$

b) On prend $K = \mathbb{Q}$ et $P_1 = x^2 + 1$, $P_2 = x + 1$ et $P_3 = x - 1$. Parmi les classes de similitudes précédentes, quelles sont celles pour lesquelles la dimension de l'espace propre associé à la valeur propre 1 est supérieure ou égale à 3 ?

Donner la matrice de Frobenius associée à une telle décomposition de Frobenius

Indication : *il ne doit donc apparaître que des matrices compagnons.*

La condition impose que l'on est dans le premier cas. En effet, l'espace propre de u pour la valeur propre 1 restreint à chacun des sous-espaces cycliques est de dimension 1 si P_3 divise le polynôme minimal de ce sous-espace cyclique et de dimension 0 sinon.

$P_1P_2^2P_3 = (x^2+1)(x+1)^2(x-1) = (x^2+1)(x+1)^2(x-1) = (x^4-1)(x+1) = x^5 + x^4 - x - 1$, $P_1P_2P_3 = x^4 - 1$ $P_1P_3 = x^3 - x^2 + x + 1$. *La matrice dans une base adaptée est alors*

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 1 & & & & & & & \\
1 & 0 & 0 & 0 & 1 & & & & & & & \\
0 & 1 & 0 & 0 & 0 & & & & & & & \\
0 & 0 & 1 & 0 & 0 & & & & & & & \\
0 & 0 & 0 & 1 & -1 & & & & & & & \\
 & & & & & 0 & 0 & 0 & 1 & & & \\
 & & & & & 1 & 0 & 0 & 0 & & & \\
 & & & & & 0 & 1 & 0 & 0 & & & \\
 & & & & & 0 & 0 & 1 & 0 & & & \\
 & & & & & & & & & 0 & 0 & -1 \\
 & & & & & & & & & 1 & 0 & -1 \\
 & & & & & & & & & 0 & 1 & 1
\end{pmatrix}$$

Exercice D : (**Endomorphismes anti-involutif**)

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et $f \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme de E anti-involutif ; c'est-à-dire vérifiant $f^2 = -\mathrm{Id}$.

1) Donner un exemple d'un tel endomorphisme sur $\mathbb{R}^2$.

Solution : *L'endomorphisme ρ de $\mathbb{R}^2$, donné dans la base canonique par la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, vérifie $\rho^2 = -\mathrm{Id}$. Dans le cas où $\mathbb{R}^2$ est muni de sa structure euclidienne canonique, ρ est la rotation d'angle $\dfrac{\pi}{2}$.*

2) Montrer que f n'admet pas de valeurs propres réelles. En déduire que la dimension de E est paire.

Solution : *Soit λ une valeur propre de f, associée à un vecteur propre x. On a alors*

$$-x = f^2(x) = f(\lambda x) = \lambda f(x) = \lambda^2 x\,;$$

si bien que $\lambda^2 = -1$, et que le polynôme caractéristique $P_{\mathrm{car}\,f}$ n'a donc pas de racine réelle. Or un polynôme à coefficients réels de degré impair (théorème des valeurs intermédiaires) à toujours au moins une racine dans $\mathbb{R}$. Il en résulte que $P_{\mathrm{car}\,f}$ est de degré pair. Comme $\dim_{\mathbb{K}} E = \deg(P_{\mathrm{car}\,f})$, E est de dimension paire.

3) Montrer que pour tout $x \in E$, le sous-espace vectoriel $\mathrm{Vect}\big\{x, f(x)\big\}$ est stable par f.

Solution :

$$\begin{array}{lrcl}
\forall y \in \mathrm{Vect}\big\{x, f(x)\big\},\ \exists (a,b) \in \mathbb{R}^2, & y & = & ax + bf(x) \\
\Rightarrow & f(y) & = & f(ax + bf(x)) \\
 & & = & af(x) + bf^2(x) \\
 & & = & af(x) - bx \\
\Rightarrow & y & \in & \mathrm{Vect}\big\{x, f(x)\big\}\,.
\end{array}$$

4) Montrer que si $F \subset E$ est un sous-espace vectoriel de E stable par f et si x est un élément de E tel que $\mathrm{Vect}\big\{x, f(x)\big\} \cap F \neq \{0\}$, alors $x \in F$.

Solution : *Soit $F \subset E$ stable par f et $x \in E$. Si $\mathrm{Vect}\big\{x, f(x)\big\} \cap F \neq \{0\}$, il existe $(a,b) \in \mathbb{R}^2$ tel que :*

$$\begin{array}{rrcl}
 & ax + bf(x) & \in & F \\
\Rightarrow & f[ax + bf(x)] & \in & F \\
\Rightarrow & af(x) - bx & \in & F \\
\Rightarrow & (a^2 + b^2)x & \in & F\,.
\end{array}$$

Or

$$a^2 + b^2 = 0 \Leftrightarrow x = 0$$

et dans ce cas $x \in F$; sinon

$$(a^2 + b^2)x \in F \Rightarrow x \in F\,.$$

5) En déduire que si $\dim E = 2n$, il existe des vecteurs $e_1, \cdots, e_n$ de E tels que $(e_1, f(e_1), \cdots, e_n, f(e_n))$ soit une base de E. Quelle est la matrice de f dans cette base ?

Solution : *Soit $\mathcal{F}$ l'ensemble des sous-espaces de E de dimension $2d \leq 2n$ possédant une base $(e_1, f(e_1), \ldots, e_d, f(e_d))$. Il suffit de montrer que $E \in \mathcal{F}$ pour répondre à la question.*

i)

$$\forall F \in \mathcal{F},\ f(F) \subset F \text{ (cf. question 3) .)}$$

ii) ($\mathcal{F} \neq \emptyset$)

Pour tout vecteur, $e_1 \in E \setminus \{0\}$, $(e_1, f(e_1))$ est une famille libre de E. En effet :

$$\begin{array}{lrcl} \forall (a,b) \in \mathbb{R}^2, & ae_1 + bf(e_1) & = & 0 \\ \Rightarrow & af(e_1) - be_1 & = & 0 \\ \Rightarrow & (a^2+b^2)e_1 & = & 0 \\ \Rightarrow & a^2 + b^2 & = & 0 \\ \Rightarrow & a = b & = & 0\,. \end{array}$$

On a alors bien entendu

$$\mathrm{Vect}\big\{e_1, f(e_1)\big\} \in \mathcal{F}\,.$$

iii) ($E \in \mathcal{F}$)

Puisque $\mathcal{F}$ est non vide et

$$\forall F \in \mathcal{F},\ \dim F \leq \dim E = 2n,$$

$$\{\dim F\}_{,F \in \mathcal{F}}$$

est une partie non vide et majorée de $\mathbb{N}$ qui contient donc un plus grand élément ; i.e.il existe $F \in \mathcal{F}$ de dimension maximale $2d$.

Si $d < n$, il existe

$$e_{d+1} \in E\,,\ e_{d+1} \notin F\,.$$

Puisque F est stable par f (cf. i),) et $e_{d+1} \notin F$,

$$F \cap \mathrm{Vect}\big\{e_{d+1}, f(e_{d+1})\big\} = \emptyset \text{ (cf. question 4) .)}$$

Il est clair qu'alors

$$F' := F \oplus \mathrm{Vect}\big\{e_{d+1}, f(e_{d+1})\big\} \in \mathcal{F} \text{ avec } \dim F' > \dim F\,;$$

ce qui contredit la maximalité de la dimension de F.

Il s'ensuit donc que

$$\dim F = \dim E \Rightarrow F = E \Rightarrow E \in \mathcal{F}\,.$$

*iv) (**Matrice de** f)*

Bien entendu dans une base $(e_1, f(e_1), \ldots, e_n, f(e_n))$ la matrice de f est diagonale par blocs avec des blocs de la forme $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Solution :

Remarque D.6 On constate (cf. question 5), iv),) qu'on a donné une réduction de FROBENIUS de f, puisque les blocs diagonaux $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ sont des matrices compagnons correspondant au polynôme X^2+1. Néanmoins on n'a jamais utilisé dans la démarche suivie, le théorème de réduction de FROBENIUS dont on sait que la preuve présente certaines difficultés.

En fait on a de la chance parce que le polynôme minimal en jeu ici est particulièrement simple. On met immédiatement en évidence un sous-espace cyclique (cf. question 3),) dont on peut constater a posteriori qu'il et maximal.

Une autre des grandes difficultés de la preuve du théorème de FROBENIUS, à savoir la construction d'un sous-espace supplémentaire stable au premier sous-espace cyclique (cf. DOC n° VII,) (cf. cours IV.11.3,) est traitée assez facilement ici (cf. question 4) question 5), iii).)

On pourrait cependant, tout à fait utiliser le théorème de réduction de FROBENIUS pour réduire f. En effet, l'hypothèse faite sur f, $f^2 = -\mathrm{Id}$, signifie que X^2+1 et un polynôme annulateur de f ou encore, ce qui revient au même, que $P_{\min f} | X^2+1$. Or X^2+1 étant irréductible dans $\mathbb{R}[X]$, et $\deg(P_{\min f}) > 0$, $P_{\min f} = X^2+1$. Il résulte alors, du corollaire IV.11.11 du cours (ou du Problème n° II, exercice I) , que $P_{\mathrm{car}\, f} = (X^2+1)^n$. Ceci donne alors immédiatement la réponse à la question 2).

Le téhorème IV.11.5 de réduction de FROBENIUS assure alors que les invariants de similitude de f sont tous égaux à X^2+1, ce qui donne immédiatement la forme question 5), iv).

Exercice E : Soit $\mathbb{K}$ un corps commutatif.

1) Combien y a-t-il de classes de similitude de matrices de $\mathcal{M}_8(\mathbb{K})$ telles que $\operatorname{Im} A = \operatorname{Ker} A$?
Solution : *Une telle matrice est nilpotente et vérifie même* $A^2 = 0$. *De plus*

$$\dim \operatorname{Im} A = \dim \operatorname{Ker} A \Rightarrow \dim \operatorname{Im} A = 4 \Rightarrow A \neq 0 \Rightarrow P_{min\,A} = X^2 .$$

Les invariants de similitude de A *(cf. cours IV.11.9,) sont donc*

$$X^{k_1}, \ldots, X^{k_d} \text{ avec } \forall 1 \leq i \leq d-1,\ k_{i+1} \leq k_i \leq 2 .$$

Les sous espaces E_i ,$_{1 \leq i \leq d}$ *correspondants dans la réduction IV.11.5 de* FROBENIUS *sont alors de dimension* 1 *(resp.* 2*) et la restriction de* A *à* E_i *est semblable à* 0 *(resp.* $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$*.) C'est, à la fois une réduction de* FROBENIUS *et une réduction (cf. cours IV.10.1,) de* JORDAN *puisque les deux formes de matrices donnée ci-dessus, sont à la fois des blocs de* JORDAN *et des matrices compagnons.*

On note qu'alors

$$\dim \operatorname{Ker} A_{|E_i} = 1$$

ce qui antraîne immédiatement

$$d = \dim \operatorname{Ker} A = 4 \text{ et } \forall 1 \leq i \leq 4,\ k_i = 2 .$$

Le diagramme de YOUNG *de* A *(cf. Problème n° II, exercice C,) est*

$$\begin{matrix} * & * \\ * & * \\ * & * \\ * & * \end{matrix}$$

2) Combien y a-t-il de classes de similitude de matrices nilpotentes de $A \in \mathcal{M}_5(\mathbb{K})$ telles que le rang de A^2 soit 2 ?
Solution : *Une telle matrice vérifie* $A^5 = 0$. *Ses invariants de similitude (cf. cours IV.11.9,) sont donc*

$$X^{k_1}, \ldots, X^{k_d} \text{ avec } \forall 1 \leq i \leq d-1,\ k_{i+1} \leq k_i \leq 5 .$$

Puisque $\dim \operatorname{Ker} A^2 = 3$, *le diagramme de* YOUNG *de* A^2 *a trois lignes (cf. Problème n° II, exercice C;) si bien qu'on peut avoir :*

$$\text{Tableau de YOUNG de } A^2 \ : \ \begin{pmatrix} * & * & * \\ * & & \\ * & & \end{pmatrix} \text{ ou } \begin{pmatrix} * & * \\ * & * \\ * & \end{pmatrix} .$$

On a également vu (cf. Problème n° II, exercice C, question 7),) comment se construit le tableau de YOUNG *de* A^2 *à partir de celui de* A ; *ce qui empêche que la première forme soit le tableau de* YOUNG *de* A^2 ; *si bien que celui-ci est nécessairement* $\begin{pmatrix} * & * \\ * & * \\ * & \end{pmatrix}$.

Le seul tableau de YOUNG *possible pour* A *est alors :*

$$\begin{matrix} * & * & * & * \\ * & & & \end{matrix}$$

Il y a donc une seule classe de similitude.

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Document n° IX

27 avril 2020

Unicité dans le théorème IV.11.5 de réduction de FROBENIUS

On a établi (cf. DOC n° VII,) (cf. cours IV.11.5.1),) l'existence, pour tout endomorphisme u d'un $\mathbb{K}$-espace vectoriel E, l'existence d'une décomposition de E en somme directe de sous espaces E_i ,$1\leq i\leq r$ stables et cycliques pour u ; chacun des E_i ayant pour polynôme minimal $\mu_i \ = \ P_{\min u_{|E_i}}$ satisfaisant la condition

$$\forall 1 \leq i \leq r-1,\ \mu_{i+1}|\mu_i \text{ (cf. IV.10.4 .)}$$

Nous allons montrer, dans ce qui suit, que l'entiers $r \in \mathbb{N}$ est la suite μ_i ,$1\leq i\leq r \in \mathbb{K}[X]$ sont uniques ; ce qui correspond au résultat IV.11.5.2) du cours.

Bien entendu cet énoncé d'unicité, est un corollaires du théorème B.6.13.2) et est à rapprocher du théorème II.10.5.ii). Comme dans ce dernier cas, on n'est pas obligé d'avoir recours aux arguments généraux exposés au paragraphe B.6 ; mais on peut utiliser des arguments spécifiques aux $\mathbb{K}$-espaces vectoriels et leur dimension en particulier, tout comme pour les groupes abéliens il était possiblle de raisonner sur leur nombre d'élément.

On trouvera, au paragraphe n° IX.1, un certain nombre de questions qu'on vous invite à résoudre , pour arriver à l'énoncé d'unicité. La solutions sera donnée au paragraphe n° IX.2.

Une fois établi le théorème IV.11.5 de réduction de FROBENIUS, vous pourrez étudier le paragraphe IV.10 du cours et notamment comment le théorème de réduction de FROBENIUS, combiné au théorème IV.3.2 donne le théorème IV.10.10 de JORDAN.

n° IX.0 . −Introduction

Notation n° IX.0.1 Dans tout ce qui suit $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$, E un $\mathbb{K}$espace vectoriel de dimension finie $d \in \mathbb{N}^*$ et $u \in \mathrm{End}_{\mathbb{K}}(E)$ un endomorphisme $\mathbb{K}$-linéaire de E.

Définition n° IX.0.2 (Réduction de FROBENIUS) On rappelle (cf. cours IV.10.4 ,) que le couple (E,u) *possède une réduction de* FROBENIUS si Il existe un entier $r \in \mathbb{N}$, E_j ,$1\leq j\leq r$ des sous-$\mathbb{K}$-espaces vectoriels de E, et des polynômes μ_j ,$1\leq j\leq r \in \mathbb{K}[X]$ tels que :

Frob$_1$)
$$\forall 1 \leq j \leq r,\ E_j \text{ est stable par } u\ .$$

Frob$_2$)
$$\forall 1 \leq j \leq r,\ (E_j, u_{|E_j}) \text{ est cyclique de polynôme minimal } \mu_j\ .$$

Frob$_3$)
$$E \ = \ \bigoplus_{j=1}^{r} E_j\ .$$

Frob$_4$)
$$\forall 1 \leq j \leq r-1,\ \mu_{j+1}|\mu_j\ .$$

n° IX.0.3. – On supposera données dans la suites deux réductions de FROBENIUS de (E, u) :

$$(r \in \mathbb{N}\,,\ E_{i\,,1\leq i\leq r} \subset E\ \mu_{i\,,1\leq i\leq r} \in \mathbb{K}[X]) \text{ et } (s \in \mathbb{N}\,,\ F_{i\,,1\leq i\leq s} \subset E\ \nu_{i\,,1\leq i\leq s} \in \mathbb{K}[X])\ .$$

L'objectif sera de montrer (cf. n° IX.1.question 6),) que

$$r\ =\ s \text{ et } \forall 1 \leq i \leq r,\ \mu_i\ =\ \nu_i\ .$$

Une fois un tel énoncé établi il devient légitime de désigner sous le terme d'*invariants de similitude*

$$(r\ \in\ \mathbb{N}, \mu_{i\,,1\leq i\leq r}\ \in\ \mathbb{K}[X]) \quad \text{(cf. cours IV.11.9.)}$$

n° IX.1 . –Invariants de similitude

On rappelle qu'on se place sous les hypothèses n° IX.0.n° IX.0.3.

1) **a)** Caractériser μ_1 et ν_1.

b) Caractériser

$$\sum_{i=1}^{r} \deg(\mu_i) \text{ (resp. } \sum_{i=1}^{s} \deg(\nu_i)\ .)$$

On pourra supposer dans la suite que

$$\forall n > r\ ,\ \mu_n\ =\ 1 \text{ et } E_n\ =\ \{0\} \text{ (**resp.** } \forall n > s\ ,\ \nu_n\ =\ 1 \text{ et } F_n\ =\ \{0\})\ .$$

2) Montrer que si les deux réductions de FROBENIUS données sont différentes, il existe $t \in \mathbb{N}\ t\ >\ 1$ tel que

$$\forall 1 \leq i \leq t-1,\ \mu_i\ =\ \nu_i \text{ et } \mu_t\ \neq\ \nu_t\ .$$

3) **Soit** $k \in \mathbb{N}^*, k < t$. **Par hypothèse sur** $t\ \mu_k\ =\ \nu_k$ **et on note :**

$$\mu_k\ =\ \nu_k\ =\ X^{d_k} - \sum_{\ell=0}^{d-1} a_\ell X^\ell\ .$$

On note encore

$$u_k\ :=\ u_{|E_k} \text{ et } v_k\ :=\ u_{|F_k}\ .$$

Montrer que :

a) E_k et F_k sont stable par $\mu_t(u)$;

b)

$$\dim_{\mathbb{K}} E_k\ =\ \dim_{\mathbb{K}} F_k\ =\ d_k\ ;$$

c) il existe $x\ \in\ E_k$ (resp. $y\ \in\ F_k$) tel que

$$\{u_k^\ell(x)\}_{,0\ \leq\ \ell\ \leq\ d_k-1} \text{ (resp. } \{v_k^\ell(y)\}_{,0\ \leq\ \ell\ \leq\ d_k-1}\ )$$

est une base de E_k (resp. F_k)

$$u_k^{d_k}(x)\ =\ -\sum_{\ell=0}^{d_k-1} a_\ell u_k^\ell(x) \text{ et } v_k^{d_k}(y)\ =\ -\sum_{\ell=0}^{d_k-1} a_\ell v_k^\ell(y)\ .$$

d)

$$\phi_k\ :\ E_k\ \to\ F_k\ ,\ u_k^\ell(x)\ \mapsto\ v_k^\ell(y),$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels tel que

$$\forall z \in E_k,\ \phi_k[u_k(z)]\ =\ v_k[\phi_k(z)]\ ;$$

1

e)

$$\mathrm{rg}\big(\mu_t(u)_{|F_k}\big)\ =\ \mathrm{rg}\big(\mu_t(u)_{|E_k}\big)\ .$$

4) **a)** Montrer que :

$$\forall k \in \mathbb{N},\ k \geq t \ \Rightarrow\ \mu_t(u_k) \ =\ 0\ ;$$

b) En écrivant $\mu_t(E)$ de deux manières différentes montrer que

$$\mathrm{rg}(\mu_t(u)) \ =\ \sum_{i=1}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big) \ =\ \sum_{j=1}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\ .$$

c) En déduire que

$$\sum_{i=t}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big) \ =\ \sum_{j=t}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\ .$$

d) En déduire finalement que

$$\forall k \ \geq t\ ,\ \mu_t(u)_{|E_k} \ =\ \mu_t(u)_{|F_k} \ =\ 0\ .$$

5) En déduire que

$$\nu_t | \mu_t\ .$$

6) Conclure finalement que

$$r \ =\ s \text{ et } \forall 1 \leq i \leq r,\ \mu_i \ =\ \nu_i\ .$$

n° IX.2 . −Solutions

On rappelle qu'on se place sous les hypothèses n° IX.0.n° IX.0.3.

1) **a)** Caractériser μ_1 et ν_1.

Solution : *Dès l'instant où $\mu_{i\ ,1\leq i\leq r}$ et $\nu_{i\ ,1\leq i\leq s}$ satisfont IV.10.4.Frob$_1$) à IV.10.4.Frob$_4$), on a*

$$\mu_1 \ =\ P_{\min u} \ =\ \nu_1\ .$$

b) Caractériser

$$\sum_{i=1}^{r} \deg(\mu_i) \text{ (resp. } \sum_{i=1}^{s} \deg(\nu_i) \text{ .)}$$

Solution : *En vertu de IV.10.4.Frob$_2$) (cf. cours IV.4.1,)*

$$\forall 1 \leq i \leq r,\ \deg(\mu_i) \ =\ \dim_{\mathbb{K}} E_i \text{ (resp. } \forall 1 \leq i \leq s,\ \deg(\nu_i) \ =\ \dim_{\mathbb{K}} F_i\ .$$

En outre, en vertu de IV.10.4.Frob$_3$),

$$\sum_{i=1}^{r} \dim_{\mathbb{K}} E_i \ =\ \dim_{\mathbb{K}} E \ =\ \sum_{i=1}^{s} \dim_{\mathbb{K}} F_i\ ;$$

si bien que

$$\sum_{i=1}^{r} \deg(\mu_i) \ =\ \dim_{\mathbb{K}} E \ =\ \sum_{i=1}^{s} \deg(\nu_i)\ .$$

On pourra supposer dans la suite que

$$\forall n > r\ ,\ \mu_n \ =\ 1 \text{ et } E_n \ =\ \{0\} \text{ (resp. } \forall n > s\ ,\ \nu_n \ =\ 1 \text{ et } F_n \ =\ \{0\})\ .$$

2) Montrer que si les deux réductions de FROBENIUS données sont différentes, il existe $t \in \mathbb{N}\ t > 1$ tel que

$$\forall 1 \leq i \leq t-1,\ \mu_i \ =\ \nu_i \text{ et } \mu_t \ \neq\ \nu_t\ .$$

Solution : *Si les deux réductions de* FROBENIUS *sont différentes l'ensemble $\{n \in \mathbb{N}\ ;\ \mu_n \neq \nu_n\}$ et non vide et possède donc un plus petit élément t. Or (cf. question 1), a),)*

$$\mu_1 \ =\ P_{\min u} \ =\ \nu_1\ ;$$

si bien que $t > 1$.

3) Soit $k \in \mathbb{N}^*, k < t$. **Par hypothèse sur** t $\mu_k = \nu_k$ **et on note :**

$$\mu_k = \nu_k = X^{d_k} - \sum_{\ell=0}^{d-1} a_\ell X^\ell .$$

On note encore

$$u_k := u_{|E_k} \text{ et } v_k := u_{|F_k} .$$

Montrer que :

a) E_k et F_k sont stable par $\mu_t(u)$;
Solution : *Par hypothèse (cf. IV.10.4.Frob$_1$),) E_k et F_k sont stables par u et donc par nimporte quel polynôme en u.*

b)

$$\dim_{\mathbb{K}} E_k = \dim_{\mathbb{K}} F_k = d_k ;$$

Solution : *Puisque E_k et F_k sont cycliques (cf. IV.10.4.Frob$_2$),) c'est une conséquence de la proposition IV.4.1 du cours.*

c) il existe $x \in E_k$ (resp. $y \in F_k$) tel que

$$\{u_k^\ell(x)\}\,,0 \leq \ell \leq d_k-1 \text{ (resp. } \{v_k^\ell(y)\}\,,0 \leq \ell \leq d_k-1 \text{)}$$

est une base de E_k (resp. F_k)

$$u_k^{d_k}(x) = -\sum_{\ell=0}^{d_k-1} a_\ell u_k^\ell(x) \text{ et } v_k^{d_k}(y) = -\sum_{\ell=0}^{d_k-1} a_\ell v_k^\ell(y) .$$

Solution : *En remarquant que E_k et F_k sont cycliques de même polynôme minimal $\mu_k = \nu_k$. Ceci revient encore à direu que, dans des bases biens choisies, u_k et v_k sont représentés par la même matrice compagnon* $\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d_k-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d_k-1} \end{pmatrix}$.

d)

$$\phi_k : E_k \to F_k , u_k^\ell(x) \mapsto v_k^\ell(y),$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels tel que

$$\forall z \in E_k, \ \phi_k[u_k(z)] = v_k[\phi_k(z)] ; \qquad 1$$

Solution : *L'image d'une base de E_k étant par constructions une base de F_k, ϕ_k est un isomorphisme.*
L'identité 1 étant vérifier pour tous les éléments d'une base, elle est vérifiée (c'est une condition linéaire,) pour tout $z \in E_k$.
On a alors

$$\phi_k \circ u_k = v_k \circ \phi_k$$

ce qui signifie (cf. IV.1.2.ii)q)ue ϕ_k est en fait un isomorphisme du $\mathbb{K}[X]$-module (E_k, u_k) sur le $\mathbb{K}[X]$-module (F_k, v_k).

e)

$$\mathrm{rg}\big(\mu_t(u)_{|F_k}\big) = \mathrm{rg}\big(\mu_t(u)_{|E_k}\big) .$$

Solution : *D'après d).1,*

$$\begin{array}{rrcl}
 & \phi_k \circ u_k & = & v_k \circ \phi_k \\
\Rightarrow & \phi_k \circ u_{|E_k} & = & u_{|F_k} \circ \phi_k \\
\Rightarrow & \phi_k \circ \mu_t(u_{|E_k}) & = & \mu_t(u_{|F_k}) \circ \ \phi_k \\
\Rightarrow & \phi_k \circ \mu_t(u)_{|E_k} & & \\
 & = & \mu_t(u)_{|F_k} \circ \phi_k & \\
\Rightarrow & \mathrm{rg}\big(\phi_k \circ \mu_t(u)_{|E_k}\big) & = & \mathrm{rg}\big(\mu_t(u)_{|F_k} \circ \phi_k\big) \\
\Rightarrow & \mathrm{rg}\big(\mu_t(u)_{|E_k}\big) & = & \mathrm{rg}\big(\mu_t(u)_{|F_k}\big) .
\end{array}$$

4) **a)** Montrer que :

$$\forall k \in \mathbb{N},\ k\ \geq t\ \Rightarrow\ \mu_t(u_k)\ =\ 0\ ;$$

Solution :

$$\forall k \in \mathbb{N},\ k\ \geq\ T\, c \Rightarrow\ \mu_k | \mu_t$$

et μ_k *est le polynôme minimale de* $u_k\ =\ u_{|E_k}$ *si bien que*

$$\mu_t(u)_{|E_k}\ =\ \mu_t(u_{|E_k})\ =\ \mu_t(u_k)\ =\ 0\ .$$

b) En écrivant $\mu_t(E)$ de deux manières différentes montrer que

$$\mathrm{rg}(\mu_t(u))\ =\ \sum_{i=1}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big)\ =\ \sum_{j=1}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\ .$$

Solution : *Puisque les* E_i ,$1 \leq i \leq r$ *et* F_j ,$1 \leq j \leq s$ *sont stables par* u *donc par* $\mu_t(u)$,

$$\mu_t(E)\ =\ \bigoplus_{i=1}^{r} \mu_t(E_i)\ =\ \bigoplus_{j=1}^{s} \mu_t(F_j)$$

d'où il résulte que

$$\mathrm{rg}(\mu_t(u))\ =\ \sum_{i=1}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big)\ =\ \sum_{j=1}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\ .$$

c) En déduire que

$$\sum_{i=t}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big)\ =\ \sum_{j=t}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big)\ .$$

Solution : *C'est une conséquence immédiate de l'égalité ci-dessus (cf. b),) et de la question 3), e).*

d) En déduire finalement que

$$\forall k\ \geq t\ ,\ \mu_t(u)_{|E_k}\ =\ \mu_t(u)_{|F_k}\ =\ 0\ .$$

Solution : *Pour* $k\ \geq\ t$, *on a déjà démontré (cf. a),) que* $\mu_t(u)_{|E_k}\ =\ 0$. *Ceci entraîne (cf. c),)*

$$\sum_{j=t}^{s} \mathrm{rg}\big(\mu_t(u)_{|F_j}\big) \sum_{i=t}^{r} \mathrm{rg}\big(\mu_t(u)_{|E_i}\big)\ =\ 0\ ;$$

ce qui entraîne que

$$\forall k \in \mathbb{N},\ k\ \geq\ t\ \Rightarrow\ \mu_t(u)_{|F_k}\ =\ 0.$$

5) En déduire que

$$\nu_t | \mu_t\ .$$

Solution : *On vient d'établir ci-dessus (cf. question 4), d),) que* $\mu_t(u)_{|F_t}\ =\ 0$, *or le polynôme minimal de* $u_{|F_t}$ *est, par hypothèse,* ν_t, *d'où il suit immédiatement que*

$$\nu_t | \mu_t\ .$$

6) Conclure finalement que

$$r\ =\ s \,\mathrm{et}\, \forall 1 \leq i \leq r,\ \mu_i\ =\ \nu_i\ .$$

Solution : *On vient d'établir (cf. question 5),) que si les suite* $\big(\mu_k\big)$,$k \in \mathbb{N}$, *et* $\big(\nu_k\big)$,$k \in \mathbb{N}$ *sont différentes, il existe un entier* t *pour lequel* $\nu_t | \mu_t$ *. Mais les rôles jouées par ces deux suites étant les mêmes, on a également* $\mu_t | \nu_t$ *si bien que* $\mu_t\ =\ \nu_t$ *et qu'il y a donc une contradiction à supposer que les suites sont différentes ; si bien qu'elles sont égales.*

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Document n° X

28 AVRIL 2020

Corrigé du TD n° VIII

Exercice A : Déterminer les invariants de similitude des matrices sous forme réduite de JORDAN suivantes :

$$A := \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; B := \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \text{ et } C := \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Solution :

i) (A)

On a immédiatement

$$P_{\text{min } A} = (X-2)^2(X-1) \text{ et } P_{\text{car } A} = (WX-2)^2(X-1)^2$$

d'où il vient immédiatement (cf. cours IV.11.11,)

$$r = 2\,,\; \mu_1 = (X-2)^2(X-1)\,,\; \mu_2 = X-1\,.$$

ii) (B)

$$\begin{array}{rrcl} & P_{\text{min } B} = (X-2)^3 & , & P_{\text{car } B} = (X-2)^4 \\ \Rightarrow & r = 2 & , & \mu_1 = (X-2)^4\,,\; \mu_2 = X-2\,. \end{array}$$

iii) (C)

On a

$$P_{\text{min } C} = (X-2)^2 \text{ et } P_{\text{car } C} = (X-2)^4\,.$$

Dans ce cas la donnée du polynôme minimal et du polynôme caractéristique n'est pas suffisante pour déterminer les invariants de similitude. On pourrait en effet avoir

$$\big((X-2)^2,(X-2),(X-2)\big) \text{ou } \big((X-2)^2,(X-2)^2\big)\,.$$

On peut cependant remarquer que la matrice C est diagonale par blocs ; ce qui correspond à une décomposition de $\mathbb{C}^4$ en somme directe. Chacun des sous-espaces a pour polynome minimale $(X-2)^2$ et pour polynôme caractéristique $(X-2)^2$. Pour chacun d'entre eux l'unique invariant de similitude est $(X-2)^2$; ce qui donne une suite $\big((X-2)^2,(X-2)^2\big)$ de décomposition en espaces cycliques de $\mathbb{C}^4$. Puisque le critère de divisibilité successive est satisfait, c'est l'unique réduction de FROBENIUS *(cf. cours IV.11.5.2) ;) ce qui assure qu'on a bien déterminé ainsi les invariants de similitude de C.*

Exercice B : Soit V un espace vectoriel de dimension finie et u un endomorphisme dont la matrice est la suivante dans une base $\mathcal{B} = (e_1, \cdots, e_{14})$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Répondre aux questions suivantes dans l'ordre désiré (en justifiant et en limitant les calculs) :

1) Calculer le polynôme minimal de u.

2) Écrire la décomposition de FROBENIUS de $(V,u) : V \; =$
$dspoplusi1'V_i$ en précisant la valeur de r et la valeur des polynômes minimaux de la restriction de u à V_i.

3) Calculer la dimension des noyaux de u^s pour s entier.

Solution : *On réécrit la matrice en faisant apparaître les blocs de* JORDAN *:*

$$\begin{pmatrix}
0 & 0 & 0 & 0 & & & & & & & & \\
1 & 0 & 0 & 0 & & & & & & & & \\
0 & 1 & 0 & 0 & & & & & & & & \\
0 & 0 & 1 & 0 & & & & & & & & \\
 & & & & 0 & 0 & 0 & & & & & \\
 & & & & 1 & 0 & 0 & & & & & \\
 & & & & 0 & 1 & 0 & & & & & \\
 & & & & & & & 0 & 0 & 0 & & \\
 & & & & & & & 1 & 0 & 0 & & \\
 & & & & & & & 0 & 1 & 0 & & \\
 & & & & & & & & & & 0 & \\
 & & & & & & & & & & & 0 \\
 & & & & & & & & & & 0 & 0 \\
 & & & & & & & & & & 1 & 0
\end{pmatrix}$$

Les polynômes minimaux des blocs de JORDAN *sont respectivement dans l'ordre* X^4, X^3, X^3, X, X, X^2. *Si on note* V_i *les sous-espaces vectoriels correspondant (*V_1 *est engendré par* e_1, ..., e_4, V_2 *est engendré par* e_5, ..., e_8, *etc). Une décomposition de Frobenius de* V *pour* u *est donc*

$$V \; = \; V_1 \oplus V_2 \oplus V_3 \oplus V_6 \oplus V_4 \oplus V_5 \; .$$

Le polynôme minimal de u *est* X^4. *Ses invariants de similitude sont* $(X^4, X^3, X^3, X^2, X, X)$. *Le nombre de blocs de* JORDAN *de taille supérieure ou égale à* i *est égale à* $\dim \mathrm{Ker}\, u^i - \dim \mathrm{Ker}\, u^{i-1}$. *On en déduit que*

$$\begin{aligned}
\dim \mathrm{Ker}\, u &= 6, \\
\dim \mathrm{Ker}\, u^2 = 6+4 &= 10, \\
\dim \mathrm{Ker}\, u^3 = 10+3 &= 13, \\
\dim \mathrm{Ker}\, u^4 = 13+1 &= 14 = \dim V \; .
\end{aligned}$$

Exercice C : (Réduite de JORDAN lorsque P_{car} est connu)

1) Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que le polynôme caractéristique de u est $\pm(X-2)^4(X+3)$ et que le noyau de $u - 2\mathrm{Id}$ est un plan.

Quelles sont les formes possibles de la réduite de JORDAN ?

Solution : *Le nombre de blocs de* JORDAN *correspondant à la valeur propre 2 est* 2 *car le sous-espace propre est de dimension* 2. *Les formes possibles de* JORDAN *sont donc (à permutation près des blocs sur la diagonale)*

$$\begin{pmatrix}
2 & 0 & & & \\
1 & 2 & & & \\
 & & 2 & 0 & \\
 & & 1 & 2 & \\
 & & & & -3
\end{pmatrix}, \begin{pmatrix}
2 & 0 & 0 & & \\
1 & 2 & 0 & & \\
0 & 1 & 2 & & \\
 & & & 2 & \\
 & & & & -3
\end{pmatrix}.$$

2) Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que le polynôme caractéristique de u est $\pm(X-1)^3(X+1)^2$ et que le noyau de $u - \mathrm{Id}$ est un plan.

Quelles sont les formes possibles de la réduite de JORDAN ?

Solution : *Le nombre de blocs de* JORDAN *correspondant à la valeur propre* 1 *est* 2 *car le sous-espace propre est de dimension* 2. *Les formes possibles de* JORDAN *sont donc (à permutation près des blocs sur la diagonale)*

$$\begin{pmatrix}
2 & 0 & & & \\
1 & 2 & & & \\
 & & 2 & 0 & \\
 & & 1 & 2 & \\
 & & & & -3
\end{pmatrix}, \begin{pmatrix}
2 & 0 & 0 & & \\
1 & 2 & 0 & & \\
0 & 1 & 2 & & \\
 & & & 2 & \\
 & & & & -3
\end{pmatrix}.$$

3) Soit V un espace vectoriel de dimension finie et u un endomorphisme de V. On suppose que le polynôme caractéristique de u est $\pm(X+1)^4(X^2-1)^2$ et que le noyau de $u+\mathrm{Id}$ est de dimension 3.

Quelles sont les formes possibles de la réduite de JORDAN ? Donner les invariants de similitude pour chacune.

Solution : *La dimension de V est 8. On a*

$$V \;=\; \mathrm{Ker}\,(u+\mathrm{Id})^6 \;\oplus\; \mathrm{Ker}\,(u-\mathrm{Id})^2\,.$$

La dimension de $\mathrm{Ker}\,(u+\mathrm{Id})^6$ est 6 et la dimension de $\mathrm{Ker}\,(u-\mathrm{Id})^2$ est 2 (polynômes caractéristiques).

Le nombre de blocs de JORDAN correspondant à la valeur propre -1 est 3 car le sous-espace propre est de dimension 3. Donc la réduite de JORDAN de u restreint au noyau de $\mathrm{Ker}\,(u+\mathrm{Id})^6$ est (à permutation près des blocs sur la diagonale)

$$J_1 \;=\; \begin{pmatrix} -1 & & & & & & \\ 1 & -1 & & & & & \\ 0 & 1 & -1 & & & & \\ & & & -1 & & & \\ & & & 1 & -1 & & \\ & & & & & -1 & \\ & & & & & & -1 \end{pmatrix},\; J_2 \;=\; \begin{pmatrix} -1 & & & & & & \\ 1 & -1 & & & & & \\ & & -1 & & & & \\ & & 1 & -1 & & & \\ & & & & -1 & & \\ & & & & 1 & -1 & \\ & & & & & & -1 \end{pmatrix}$$

ou

$$J_3 \;=\; \begin{pmatrix} -1 & & & & & & \\ 1 & -1 & & & & & \\ & 1 & -1 & & & & \\ & & 1 & -1 & & & \\ & & & & -1 & & \\ & & & & & -1 & \\ & & & & & & -1 \end{pmatrix}$$

Le nombre de blocs de JORDAN correspondant à la valeur propre 1 est 1 ou 2.

Donc la réduite de JORDAN de u restreint au noyau de $\ker\,(u-\mathrm{Id})^2$ est (à l'ordre près)

$$J_4 \;=\; \begin{pmatrix} 1 & \\ & 1 \end{pmatrix},\quad J_5 \;=\; \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}$$

Les invariants de similitude sont

— $J_1 \oplus J_4$: $[(x+1)^3(x-1), (x+1)^2(x-1), (x+1)]$
— $J_1 \oplus J_5$: $[(x+1)^3(x-1)^2, (x+1)^2, (x+1)]$
— $J_2 \oplus J_4$: $[(x+1)^2(x-1), (x+1)^2(x-1), (x+1)^2]$
— $J_2 \oplus J_5$: $[(x+1)^2(x-1)^2, (x+1)^2, (x+1)^2]$
— $J_3 \oplus J_4$: $[(x+1)^4(x-1), (x+1)(x-1), (x+1)]$
— $J_3 \oplus J_5$: $[(x+1)^4(x-1)^2, (x+1), (x+1)]$

Exercice D : (**Matrice semblable à son double**)

Soit $A \in \mathcal{M}_n(\mathbb{C})$.

1) Montrer que si A est semblable à $2A$ alors A est une matrice nilpotente.

Solution : *Si A est semblable à $2A$, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ tel que $2A = P^{-1}AP$. Il s'ensuit que :*

$$\begin{array}{rcl} \forall k \in \mathbb{N},\quad 2^k A^k & = & (2A)^k \\ & = & (P^{-1}AP)^k \\ & = & P^{-1}A^kP\,. \end{array}$$

L'application

$$\phi \;:\; \mathcal{M}_n(\mathbb{K}) \;\to\; \mathcal{M}_n(\mathbb{K})\,,\; A \;\mapsto\; P^{-1}AP$$

est linéaire. Il s'ensuit que si $A^k \neq 0$, 2^k est valeur propre de ϕ. Or $\dim_{\mathbb{K}} \mathcal{M}_n(\mathbb{K}) = n^2$; et par conséquent ϕ a au plus n^2 valeurs propres si bien que

$$\forall k \in \mathbb{N},\; k \;>\; n^2 \;\Rightarrow A^k \;=\; 0\,;$$

ainsi A est nilpotente.

2) Montrer que pour tout $k \in \mathbb{N}$, le bloc de JORDAN J_k est semblable à $2J_k$.

Solution : *On peut se donner une base $(e_1, \ldots, e_k)$ telle que*

$$\forall 1 \leq i \leq k-1,\; J_k e_i \;=\; e_{i+1} \text{ et } J_k e_k \;=\; 0\,.$$

S'il existe $P \in \mathrm{GL}_k(\mathbb{K})$ telle que $2J_k = P^{-1}J_kP$,

$$\begin{array}{rcl} \forall 1 \leq i \leq k-1,\quad 2PJ_ke_i & = & J_kPe_i \\ \Rightarrow \qquad\qquad\quad 2Pe_{i+1} & = & J_kPe_i\,. \end{array}$$

Alors $Pe_i = 2e_i$ convient et d'ailleurs également pour $Pe_k = 2e_k$.

3) En déduire qu'une matrice est nilpotente si et seulement si elle est semblable à son double.

Solution : *On a montré (cf. question 1),) que si une matrice est semblable à son double elle est nilpotente.*

Réciproquement, si une matrice A est nilpotente son polynôme minimal est X^d qui est scindé ; si bien qu'elle admet (cf. cours IV.10.10,) une réduite de JORDAN. *Chacun des blocs est (cf. question 2),) semblable à son double, ; ce qui permet de construire par bloc une matrice inversible P telle que $2A = P^{-1}AP$.*

Exercice E : (Matrice semblable à sa transposée)

On va montrer que toute matrice $A \in \mathcal{M}_n(\mathbb{C})$ est semblable à sa transposée.

1) Montrer qu'il suffit de vérifier le résultat pour les matrices avec une unique valeur propre.

Solution : *Dans $\mathbb{C}[X]$ tous les polynômes sont scindés ; si bien que le polynôme caractéristique $P_{car\,A}$ (resp. minimal $P_{min\,a}$) de toute matrice $A \in \mathcal{M}_n(\mathbb{C})$ est scindé. Il s'ensuit (cf. cours IV.10.10,) que toute matrice $A \in \mathcal{M}_n(\mathbb{C})$ admet une réduite de* JORDAN

$$J = \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 & 0 & & & & & & \\ 1 & \lambda_1 & 0 & \dots & 0 & 0 & & & & & & \\ 0 & 1 & \lambda_1 & \dots & 0 & 0 & \dots & & \dots & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \\ 0 & 0 & 0 & \dots & 1 & \lambda_1 & & & & & & \\ & & \vdots & & & & \vdots & & \vdots & & & \\ & & & & & & & \lambda_m & 0 & 0 & \dots & 0 & 0 \\ & & & & & & & 1 & \lambda_m & 0 & \dots & 0 & 0 \\ & & \dots & & & & \dots & 0 & 1 & \lambda_m & \dots & 0 & 0 \\ & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ & & & & & & & 0 & 0 & 0 & \dots & 1 & \lambda_m \end{pmatrix}.$$

Si on sait montrer que $\begin{pmatrix} \lambda_k & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda_k & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda_k & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \lambda_k \end{pmatrix}$ *est semblable à sa transposée, on pourra construire par bloc une matrice inversible P telle que*

$$A = P^{-1}AP\,.$$

On pourrait en fait se contenter de décomposer $\mathbb{C}^n$ en sous-espaces caracgtér'istique (cf. cours IV.3.2.)
La restriction de A à chacun des sous-espaces caractéristiques a une uniuqe valeur propre.

2) Montrer qu'il suffit de vérifier le résultat pour les matrices nilpotentes.

Solution : *Si A ne possède qu'une valeur propre λ, la décomposition de* DUNFORD *(cf. cours IV.9.1,) de A s'écrit*

$$A = \lambda I + N \text{ avec } N \text{ nilpotente}\,.$$

Or pour tout P inversible

$$P^{-1}\lambda I P = \lambda I = {}^t\lambda I\,.$$

Il suffit donc de trouver P inversible telle que $P^{-1}NP = {}^tN$.

3) Démontrer le résultat pour les matrices nilpotentes.

Solution : *Si A est nilpotente elle est semblable à une réduite de* JORDAN. *On peut se ramener au cas d'un seul bloc de* JORDAN $J_k = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$. *On a alors une base $(e_1, \dots, e_k)$ telle que*

$$\forall 1 \le i \le k-1,\ J_k e_i = e_{i+1} \text{ et } J_k e_k = 0\,.$$

La matrice P correspondant à l'endomorphisme $e_i \mapsto e_{k+1-i}$ (matrice anti-diagonale) est alors telle que

$$P^{-1}J_kP = {}^tJ_k\,.$$

Exercice F : On considère les endomorphismes u et v de $\mathbb{C}^3$ dont les matrices dans la base canonique sont respectivement

$$A := \begin{pmatrix} 8 & -16 & -9 \\ 7 & -15 & -9 \\ -7 & 16 & 10 \end{pmatrix} \text{ et } B := \begin{pmatrix} 2 & 2 & -3 \\ 5 & 1 & -5 \\ -3 & 4 & 0 \end{pmatrix} .$$

1) Montrer que $P_{\text{car}\,A} = P_{\text{car}\,B} = (X-1)^3$.

2) Montrer que l'ensemble des matrices M de $\mathcal{M}_3(\mathbb{C})$ vérifiant $(M - \mathrm{Id})^3 = 0$ est constitué de 3 classes de similitudes dont on déterminera les réduites de JORDAN associées.

Solution : *On raisonne sur le polynôme minimal $P_{\text{min}\,M}$. Puisque $(X-1)^3$ est, par hypothèse, un polynôme annulateur de M,*

$$P_{\text{min}\,M} | (X-1)^3 .$$

Puisque les facteurs irréductibles du polynôme caractéristique $P_{\text{car}\,M}$ de M sont ceux de $P_{\text{min}\,M}$ (cf. cours IV.11.11,) (cf. Problème n° II, exercice I,)

$$P_{\text{car}\,M} = (X-3)^3 .$$

i) ($P_{\text{min}\,M} = X-1$)
alors $M = \mathrm{Id}$ et sa classe est d'ailleur constituée du seul élément Id.

ii) ($P_{\text{min}\,M} = (X-1)^2$)
Alors M est semblable à

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

iii) ($P_{\text{min}\,M} = (X-1)^3$)
M est alors semblable à

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} .$$

3) Déterminer la réduite de JORDAN de u ainsi qu'une base de $\mathbb{C}^3$ dans laquelle la matrice de u est sa réduite de JORDAN.

4) Déterminer la réduite de JORDAN de v ainsi qu'une base de $\mathbb{C}^3$ dans laquelle la matrice de v est sa réduite de JORDAN.

Exercice G : (Racine carrée)
Soit $A \in \mathcal{M}_n(\mathbb{C})$. On appelle *racine carrée de* A, toute matrice M de $\mathcal{M}_n(\mathbb{C})$ vérifiant $M^2 = A$.

1) On suppose que A est diagonalisable. Montrer que A admet une racine carrée.

Solution : *La matrice A est diagonalisable signifie que $E = \mathbb{C}^n$ et somme directe $E = \bigoplus_{i=1}^{r} E_i$ de telle sorte que E_i est stable sous A et qu'il existe λ_i ,$_{1 \le i \le r}$ tel que*

$$A_{|E_i} = \lambda_i \mathrm{Id}_{E_i} .$$

Or

$$\forall 1 \le i \le r,\ \exists \mu_i \in \mathbb{C},\ \lambda_i = \mu_i^2 .$$

Définissons R par

$$\forall 1 \le i \le r,\ R_{|E_i} = \mu_i \mathrm{Id}_{E_i} ;$$

qui définit bien $R : E \to E$ puisque $E = \bigoplus_{i=1}^{r} E_i$. De plus on a bien évidemment $R^2 = A$.

2) Dans cette question, on traite le cas où A est nilpotente.

a) Soit $B \in \mathcal{M}_n(\mathbb{C})$ une matrice nilpotente.

Déterminer le tableau de YOUNG associé à B^2 en fonction du tableau de YOUNG associé à B.

Solution : *On renvoi au Problème n° II, exercice C, question 7), pour les détails de la construction du tableau de* YOUNG *en fonction de celui de B. On rappelle simplement que la $j^{\text{ième}}$ colonne du tableau de B^2 est obtenue en « concaténant » la $2j-1^{\text{ième}}$ et la $2j^{\text{ième}}$ colonne du tableau de B.*

b) Étant donnée une matrice nilpotente A dont le tableau de YOUNG est

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix}\ ,\ (\text{resp. } \begin{pmatrix} * & * \\ * & * \\ * & \end{pmatrix})\ ,\ (\text{resp. } \begin{pmatrix} * & * & * \\ * & * & \end{pmatrix})$$

trouver une matrice B telle que $B^2 = A$.

Solution :

i) Si le tableau de YOUNG $Y(A)$ *de* A *est* $\begin{pmatrix} * & * \\ * & * \end{pmatrix}$, *il existe une base* (e_1, e_2, e_3, e_4) *telle que*

$$Ae_1 = e_2\ ,\ Ae_2 = 0\ Ae_3 = e_4 \text{ et } Ae_4 = 0\ .$$

Si on pose $Be_1 = e_3$, *nécessairement* $Be_3\ B^2e_1 = Ae_1 = e_2$. *Il s'ensuit alors que* $Be_2 = B^2e_3 = Ae_3 = e_4$. *Finalement* $Be_4 = B^2e_2 = Ae_2 = 0$.

ii) Si

$$Y(A) = \begin{pmatrix} * & * \\ * & * \\ * & \end{pmatrix},$$

la situation est celle de i) à ceci près que la base se complète en une base $(e_1, e_2, d_3, d_4, d_5)$ *avec* $Ae_5 = 0$. *Il suffit alors de poser* $Be_5 = 0$.

iii) Si

$$Y(A) = \begin{pmatrix} * & * & * \\ * & * & \end{pmatrix},$$

il existe une base $(e_1, e_2, e_3, e_4, e_5)$ *telle que*

$$Ae_1 = e_2\ ,\ Ae_2 = e_3\ ,\ Ae_3 = 0\ ,\ Ae_4 = e_5 \text{ et } Ae_5 = 0\ .$$

si on pose :

$$\begin{array}{rrcl} & Be_1 & := & e_4 \\ \Rightarrow & Be_4 = B^2e_1 = Ae_1 & = & e_2 \\ \Rightarrow & Be_2 = B^2e_4 = Ae_4 & = & e_5 \\ \Rightarrow & Be_5 = B^2e_2 = Ae_2 & = & e_3 \\ \Rightarrow & Be_3 = B^2e_5 = Ae_5 & = & 0 \end{array}$$

ce qui définit bien B *et satisfait à la condition que* $Ae_3 = B^2e_3 = 0$.

c) En déduire que si A est une matrice nilpotente alors A admet une racine carrée si et seulement si le tableau de YOUNG associé à A ne contient pas deux colonnes consécutives de même longueur impaire. En particulier le bloc de JORDAN

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

n'a pas de racine carrée.

Solution : *Pour une matrice nilpotante* A, *on notera* $d_{A,j}$ *la hauteur de la* $j^{\text{ième}}$ *colonne dans son tableau de* YOUNG *qui vaudra* 0 *pour* j *assez grand si on veut que cette suite soit définie sur* $\mathbb{N}$.

On rappelle (cf. Problème n° II, exercice B , Problème n° II, exercice E,) que

$$(d_{A,j})_{,j\,\in\,\mathbb{N}} \text{ est décroissante et } d_{A,j} = \dim \operatorname{Ker} A^j - \dim \operatorname{Ker} A^{j-1}\ .$$

i) (A ***possède une racine carrée****)*

tout d'abord si A *est nilpotante et possède une racine carrée* B, *il existe* $\varepsilon \in \mathbb{N}^*$ *tel que* $A^\varepsilon = 0$, *ce qui entraîne que* $B^{2\varepsilon} = 0$ *et que, par conséquent,* B *est aussi nilpotente et qu'on peut donc lui appliquer le formalisme des tableaux de* YOUNG *(cf. Problème n° II, exercice C.)*

On a vu (cf. a),) que

$$\forall j \in \mathbb{N},\ d_{A,j} = d_{B,2j-1} + d_{B,2j}\ .$$

Par conséquent

$$d_{A,j} \;=\; d_{A,j+1} \;\Leftrightarrow\; d_{B,2j-1} \;+\; d_{B,2j} \;=\; d_{B,2j+1} \;+\; d_{B,2j+2}\;.$$

Or

$$d_{B,2j+1} \;+\; d_{B,2j+2} \;\leq\; 2d_{B,2j},$$

si bien que

$$d_{B,2j-1} \;+\; d_{B,2j} \;\leq\; 2d_{B,2j} \;\Rightarrow\; d_{B,2j-1} \;\leq\; d_{B,2j}\;.$$

Comme par ailleurs $d_{B,2j} \;\leq\; d_{B,2j-1}$

$$d_{B,2j-1} \;=\; d_{B,2j} \;\Rightarrow\; d_{A,j} \;=\; 2d_{B,2j}\;;$$

si bien que $d_{A,j}$ *est pair.*

Si donc A *admet une racine carrée, son tableau de* YOUNG *ne peut avoir de collones consécutives de hauteur impaire.*

ii) ***(Réciproque)***

$*$*)* ***(Réduction au cas d'un tableau de* YOUNG *de hauteur pair)***

Si le tableau de YOUNG *de* A *est de hauteur impaire,* $d_{A,1}$ *est impair. La condition que* $Y(A)$ *n'a pas deux colonnes successives de même hauteur impaire entraîne qe* $d_{A,2} \;<\; d_{A,1}$*. Ceci entraîne que la* $d_{A,1}^{\text{ième}}$ *ligne de* $Y(A)$ *est de longueur* 1 *et donc que* A *possède un bloc de* JORDAN J_1*. L'espace* $\mathbb{C}$ *se décompose donc en somme directe* $\mathbb{C}^n \;=\; D \;\oplus\; H$*, où* D *est une droite,* D *et* H *sont stables par* A $A_{|D} \;=\; 0$ *et* $A_{|H}$ *a pour tableau de* YOUNG $Y(A)$ *privé de sa dernière ligne.*

La restriction $A_{|D}$ *de* A *de à* D *admet bien entendu une racine carrée* 0*, et si* $A_{|H}$ *en admet également une il en sra de même de* A*.*

Reste à voir que le tableau privé de sa dernière ligne continue de satisfaire à la condition sur les colonnes. Or s'il a deux colonnes de même hauteur, il en était déjà ainsi dans $Y(A)$ *; sauf si le fait d'avoir « raccourci » la première colonne fait qu'elle est désormais de même hauteur que la deuxième. Mais alors cette hauteur qui vaut* $d_{A,1} - 1$ *est paire.*

†*)* ***(Réduction à un tableau à*** 2 ***lignes)***

On peut donc désormais supposer que la hauteur $2h$ *du tableau de* YOUNG $Y(A)$ *de* A *est paire. On peut alors écrire*

$$\mathbb{C}^n \;=\; \sum_{i=1}^{2h} E_i$$

où E_i *est stable par* A *et tel que* $A_{|E_i}$ *est cyclique nilpotent de rang* r_i *qui est la longueur de la* $i^{\text{ième}}$ *ligne dans* $Y(A)$*. Notons*

$$H_i\,,_{1\leq i\leq h} \;:=\; E_{2i-1} \;\oplus\; E_{2i}\;.$$

Alors $\forall 1 \leq i \leq h,\; H_i$ *est stable par* A *et le tableau de* YOUNG *de* $A_{|H_i}$ *est un tableau à* 2 *lignes de longueurs respectives* r_{2i-1} *et* r_{2i}*. La condition sur les colonnes de* $Y(A)$ *entraîne qu'alors*

$$r_{2i-1} \;=\; r_{2i} \text{ ou } r_{2i-1} \;=\; r_{2i} \;+\; 1\;.$$

Bien entendu si chacune des restrictions $A_{|H_i}$ *admet une racine carrée, il en sera de même pour* A*.*

‡*)* ***(Tableau à deux lignes)***

On peut donc désormais supposer que $Y(A)$ *a deux lignes de longueurs* r *et* s *avec* $r \;=\; s$ ou $r \;=\; s+1$ *. Il convient alors de généraliser l'argument donné en b).i) (resp. b).iii).)*

On dispose en effet d'une base $(e_1, \ldots, e_r, e_{r+1}, \ldots, e_{r+s})$ *telle que*

$$\forall 1 \leq i \leq r-1,\; \forall r+1 \leq i \leq r+s-1,\; Ae_i \;=\; e_{i+1}\;,\; Ae_r \;=\; 0 \text{ et } Ae_{r+s} \;=\; 0\;.$$

Reste à constater que B *définie par* $Be_1 \;=\; e_{r=1}$ *est uniquement déterminée dès l'instant où l'on exige que* $B^2 \;=\; A$*.*

3) Dans cette question, on traite le cas où A est inversible.

a) Montrer que si B est une matrice nilpotente alors $I + B$ admet une racine carrée (où I est la matrice identité.)

Indication : *On pourra utiliser le développement en série entière de* $x \mapsto \sqrt{1+x}$ *au voisinage de* 0*.*

Solution : *Puisque* I *et* B *commutent, on peut par exemple constater que*

$$(I + \frac{1}{2}B)^2 \;=\; I + B + \frac{1}{4}B^2$$

qui vaut $I + B$ *dès l'instant où* $B^2 \;=\; 0$*.*

Reste à voir si on peut généraliser ce résultat de la manière suivante : Pour tout $d \;\in\; \mathbb{N}\; d \;\geq\; 2$*, existe-t-il un polynôme* $R_d \;\in\; \mathbb{C}_d[X]$ *tel que*

$$R_n^2 - (1+X) \;=\; X^d P\;,\; P \;\in\; \mathbb{C}[X]\;.$$

Si on écrit $R_n = \sum_{k=0}^{d} r_k X^k$ *on a nécessairement*

$$\begin{array}{rrcl} & r_0 & = & 1 \\ & 2r_0r_1 & = & 1 \\ \Rightarrow & r_1 & = & \frac{1}{2} \\ & 2r_0r_2 + r_1^2 & = & 0 \\ \Rightarrow & r_2 & = & -\frac{1}{8} \\ \dots & \dots & & \dots \end{array}$$

ce qui définit bien R_n *par récurrence.*

Il s'ensuit que si B *est nilpotent d'échelon* d, $R_d(B)^2 = I + B$.

b) En déduire que toute matrice inversible admet une racine carrée.

Solution : *Une matrice* A *admet une racine carrée si et seulement si il en est de même de tous ses conjugués* $P^{-1}AP$, $P \in \mathrm{GL}_n(\mathbb{C})$. *On peut donc supposer que* A *est une réduite de* JORDAN

$$A = \bigoplus_{i=1}^{m} A_i := \begin{pmatrix} \lambda_i & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda_i & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda_i & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \lambda_i \end{pmatrix}.$$

Puisque A *est inversible, aucun des* λ_i *n'est nul.*

Il suffit désormais de montrer que chacun des A_i *admet une racine carrée. Or* $A_i - \lambda_i I$ *est nilpotante ainsi que* $B = \frac{1}{\lambda_i}A_i - I$. *D'après le point précédent,*

$$R_d(B)^2 = I + B = \frac{1}{\lambda_i}A_i \text{ (cf. a) .)}$$

En choisissant un nombre complexe μ_i *tel que* $\mu_i^2 = \lambda_i$,

$$(\mu_i R_d(B))^2 = \mu_i^2 \frac{1}{\lambda_i} A_i = A_i \,.$$

4) Donner une condition nécessaire et suffisante pour que A admette une racine carrée.

Université Paris Sud **Année 2019–2020**

L3/S6 M305 **Algèbre II**

Index

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Programme pour le partiel du 3 mars 2020

N.B. Les références renvoient au poly.

- Il est indispensable de connaître les constructions *produit* (cf. I.7,) et *quotient* (cf. I.8,) même si on s'interdira absolument de considéré comme connues leurs généralisations au A-modules.
- Dans une moindre mesure la notion de *suite exacte* (cf. I.9.)
- Il est indispensable de connaître la définition d'anneau principal ainsi que les propriétés de ces anneaux :
  - Théorème de BÉZOUT (cf. I.13.2.1,)
  - lemme de GAUSS (cf. I.13.2.3,)
  - lemme d'EUCLIDE (cf. I.13.2.6,)
  - Théorème fondamental de l'arithmétique (cf. I.13.5)
  - théorème chinois des restes (cf. I.13.4.)

  On peut cependant si l'on veut s'en tenir à l'anneau $\mathbb{Z}$.
- Concernant les groupes abéliens de type fini :
  - La définition (cf. II.3.2,) doit être parfaitement connue ainsi que les énoncés :
  - II.4.6,
  - II.6.4,
  - II.10.5.

De manière général le partiel porte sur le contenu du chapitre II du cours en sachant qu'on ne peut se passer des outils exposés au chapitre I. On exclura cependant du programme du partiel le paragraphe II.11 qui n'aura sans doute pas été complètement traité en cours.

Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

Table des matières