

Algèbre 2

Notes de cours
Master 2 Mathématiques 2017-2018

Julien Bichon
UFR de Mathématiques
Université Clermont Auvergne
julien.bichon@uca.fr

Les pages qui suivent constituent les notes de cours “Algèbre 2” du Master 2 Mathématiques. Bien sûr, il est probable que des coquilles ou erreurs se sont glissées dans ce document, merci de me les signaler !

Voici quelques références utiles.

- D. Dummit, R. Foote, *Abstract algebra*. Third edition, John Wiley & Sons, 2004.
- D. Guin, *Algèbre* (tome 1). Belin, 1997.
- G. Rauch, *Les groupes finis et leurs représentations*. Ellipses, 2001.
- J. P. Serre, *Représentations linéaires des groupes fini*. Hermann, Paris, 1978.
- P. Tauvel, *Mathématiques générales pour l’agrégation*. Masson, Paris, 1997.

Table des matières

I Modules	4
A Définitions	4
B Sous-modules	7
C Modules quotients	10
II Modules libres	12
A Définition et exemples	12
B Le théorème de la base incomplète	14
C Rang d'un module libre	14
D Module de torsion	18
III Algèbres	19
A Définitions	19
B L'algèbre d'un monoïde	21
C Algèbres de polynômes	22
IV Matrices à coefficients dans un anneau commutatif	24
A Matrices	24
B Centre et idéaux d'une algèbre de matrices	25
C Déterminant	26
D Application aux endomorphismes d'un module libre	28
E Application : les entiers algébriques	30
F Opération sur les lignes et colonnes d'une matrice	31
G Applications aux groupes linéaires	34
V Modules de type fini sur un anneau principal	36
A Les théorèmes de structures : énoncé	36
B Le théorème de la base adaptée	37
C Structure des modules de type fini	39
D Application à la réduction des endomorphismes d'un espace vectoriel	43
D.1 Forme canonique de Jordan	45
D.2 Facteurs invariants et forme canonique rationnelle	48
VI Représentations linéaires des groupes finis	52
A Introduction	52
B Définitions	52
C Constructions et exemples de représentations	55
C.1 Représentations de dimension un	55
C.2 Représentations de permutation	56
C.3 Somme directe de représentations	56
C.4 Représentation duale	58
D Énoncé des théorèmes principaux	58
E Représentations unitaires et complète réductibilité des représentations	60
E.1 Groupe unitaire	60
E.2 Représentations unitaires	61

F	Le lemme de Schur	62
G	Invariants et moyenne	63
H	Relations d'orthogonalité et applications	64
I	Structure de l'algèbre du groupe	67
J	Caractères	68
K	Application : le théorème "pq" de Burnside	72
L	Exemples de représentations et de tables de caractères.	74
	L.1 Groupes abéliens	74
	L.2 Groupes diédraux	74
	L.3 Le groupe quaternionique d'ordre 8	75
	L.4 Groupes symétriques et alternés	75
	L.5 Le groupe dicyclique d'ordre 12	77
A	Appendices	78
A	Une autre preuve du théorème de la base adaptée	78
B	Le lemme des noyaux	80

I Modules

Rappel : un anneau est un triplet $(A, +, \cdot)$ où A est un ensemble non vide et

$$+ : A \times A \longrightarrow A, \quad \cdot : A \times A \longrightarrow A$$

sont des lois (internes) sur A satisfaisant aux axiomes qui suivent.

1. $(A, +)$ est un groupe abélien. Le neutre est alors noté 0_A ou 0 , et le symétrique d'un élément $a \in A$ est noté $-a$.
2. (A, \cdot) est un monoïde, c'est-à-dire que la loi \cdot est associative et possède un élément neutre, noté 1_A ou 1 .
3. On a, $\forall a, b, c \in A : a \cdot (b + c) = a \cdot b + a \cdot c$, et $(b + c) \cdot a = b \cdot a + c \cdot a$.

Dans ce chapitre on va étudier les **modules** sur un anneau. Cela permet
→ de généraliser et raffiner des résultats d'algèbre linéaire (les modules sur les corps étant les espaces vectoriels),
→ d'obtenir des résultats structurels sur les anneaux (de la même manière, on obtient des résultats sur les groupes en les faisant opérer sur des ensembles).

Dans la suite A est un anneau.

A Définitions

Définition A.1. Un A -module (à gauche) est un triplet $(M, +, \cdot)$ où $(M, +)$ est un groupe abélien et $\cdot : A \times M \longrightarrow M$ est une loi externe

$$A \times M \longrightarrow M \\ (a, x) \longmapsto a \cdot x$$

vérifiant les axiomes suivants ($\forall a, b \in A, \forall x, y \in M$) :

1. $a \cdot (x + y) = a \cdot x + a \cdot y$,
2. $(a + b) \cdot x = a \cdot x + b \cdot x$,
3. $(ab) \cdot x = a \cdot (b \cdot x)$,
4. $1 \cdot x = x$.

Exemples A.2. 1. A est un A -module, la loi externe étant la multiplication de A .
2. Pour $n \in \mathbb{N}^*$, A^n est un A -module, dont le groupe abélien sous-jacent est le groupe abélien produit A^n et la loi externe est donnée par

$$a \cdot (x_1, \dots, x_n) = (ax_1, \dots, ax_n)$$

3. Si A est un corps, un A -module est exactement un A -espace vectoriel.

4. $A = \mathbb{Z}$. Les \mathbb{Z} -modules sont exactement les groupes abéliens.

En effet : Un \mathbb{Z} -module est en particulier un groupe abélien. Réciproquement si M est groupe abélien, on définit une loi externe

$$\begin{aligned}\mathbb{Z} \times M &\longrightarrow M \\ (n, x) &\longmapsto n.x\end{aligned}$$

de la manière suivante. Si $n \geq 0$, on pose $n.x = \underbrace{x + \dots + x}_{n \text{ fois}}$ et si $n \leq 0$, on pose $n.x = -((-n).x)$. On vérifie que cela munit bien M d'une structure de \mathbb{Z} -module (exercice).

5. Si I est un ensemble et M est un A -module, notons M^I l'ensemble des applications $I \longrightarrow M$. Alors on vérifie que M^I est un A -module, pour les lois suivantes ($f, g \in M^I$, $a \in A$).

- $(f + g)(x) := f(x) + g(x)$,
- $(a.f)(x) := a.f(x)$.

La notion de module est donc une (vaste) généralisation des notions de groupe abélien et d'espace vectoriel. Un certain nombre de constructions et résultats sur les espaces vectoriels se généralisent sans problème aux modules, alors que d'autres résultats ne se généraliseront pas (comme par exemple l'existence d'une base).

Définition A.3. Soient M et N des A -modules. Une **application A -linéaire de M vers N** , ou encore un **morphisme de A -modules de M vers N** , est une application $f : M \longrightarrow N$ telle que $\forall x, y \in M, \forall a \in A$, on a

1. $f(x + y) = f(x) + f(y)$,
2. $f(a.x) = a.f(x)$.

L'ensemble des applications A -linéaire de M vers N est noté $\text{Hom}_A(M, N)$, avec de plus quand $M = N$, $\text{Hom}_A(M, M) = \text{End}_A(M)$. Un **isomorphisme de A -modules**, ou encore un **isomorphisme A -linéaire**, est une application A -linéaire bijective.

On vérifiera que la composée de deux applications A -linéaires est encore une application A -linéaire, et que la bijection inverse d'un isomorphisme A -linéaire est encore A -linéaire.

Exemples A.4. 1. Soit $a \in A$. L'application $f_a : A \longrightarrow A, b \longmapsto ba$, est une application A -linéaire.

2. Soit $n \in \mathbb{N}^*$ et $i \in \{1, \dots, n\}$. La i -ème projection $p_i : A^n \longrightarrow A$ est une application A -linéaire.

3. Si M et N sont des \mathbb{Z} -modules, un morphisme de \mathbb{Z} -modules $M \longrightarrow N$ est exactement un morphisme de groupes (vérifier).

Proposition A.5. Soient M et N des A -modules.

1. L'ensemble $\text{Hom}_A(M, N)$ est naturellement un groupe abélien avec pour $f, g \in \text{Hom}_A(M, N)$,

$$(f + g)(x) := f(x) + g(x), \forall x \in M$$

2. Si de plus A est commutatif, alors $\text{Hom}_A(M, N)$ est un A -module avec pour $a \in A$, $f \in \text{Hom}_A(M, N)$,

$$(a.f)(x) := a.f(x), \forall x \in M$$

3. $\text{End}_A(M)$ est un anneau, avec pour multiplication la composition des applications A -linéaires.

Preuve. Exercice. \square

Le résultat suivant est une reformulation très utile de la définition de A -module. On pourra le comparer à la situation analogue de la formulation d'une opération d'un groupe G sur un ensemble X en termes d'un morphisme de groupes $G \rightarrow S_X$.

Proposition A.6. Soit $M = (M, +)$ un groupe abélien. Il est équivalent de se donner

1. une structure de A -module sur M ,
2. un morphisme d'anneaux $\varphi : A \rightarrow \text{End}_{\mathbb{Z}}(M)$.

Preuve. Supposons d'abord que M est un A -module, avec loi externe $A \times M \rightarrow M$ $(a, x) \mapsto a.x$. Soit alors l'application $l_a : M \rightarrow M$, $l_a(x) = a.x$, qui est un morphisme de groupes. Ceci définit donc une application

$$\begin{aligned} \varphi : A &\rightarrow \text{End}_{\mathbb{Z}}(M) \\ a &\mapsto l_a \end{aligned}$$

On vérifie que φ est un morphisme d'anneaux.

Réciproquement, si $\varphi : A \rightarrow \text{End}_{\mathbb{Z}}(M)$ est un morphisme d'anneaux, on définit une loi externe sur M

$$\begin{aligned} A \times M &\rightarrow M \\ (a, x) &\mapsto a.x := \varphi(a)(x) \end{aligned}$$

et on vérifie que $(M, +, \cdot)$ est bien un A -module. \square

Le résultat suivant est très utile pour transporter une structure de module sur un anneau donné vers un autre anneau.

Proposition A.7. Soient A et B des anneaux et soit $f : A \rightarrow B$ un morphisme d'anneaux ($f(1_A) = 1_B$ et $\forall a, b \in A$, $f(ab) = f(a)f(b)$, $f(a + b) = f(a) + f(b)$). Soit M un B -module. Alors f induit une structure de A -module sur M , définie par : $\forall a \in A, \forall x \in M$, $a.x := f(a).x$.

Preuve. Exercice. \square

Exemple A.8. Si $A \subset B$ est un sous-anneau, alors la multiplication de B induit par restriction une structure de A -module sur B .

B Sous-modules

Les concepts introduits dans ce paragraphe sont des adaptations directes du cas des espaces vectoriels.

Définition B.1. Soit M un A -module. On dit qu'un sous-ensemble N de M est un **sous- A -module** de M (ou plus simplement un **sous-module** de M) si

1. $0 \in N$,
2. $\forall x, y \in N, x + y \in N$,
3. $\forall a \in A, \forall x \in N, a.x \in N$.

Un sous-module est donc en particulier un sous-groupe.

- Exemple B.2.**
1. Soit M un A -module : $\{0\}$ et M sont des sous-modules de M .
 2. Les sous-modules du A -module A sont exactement les idéaux à gauche de A .
 3. Soit M un A -module et $x \in M$. Alors $Ax = \{a.x, a \in A\}$ est un sous-module de M (à vérifier).
 4. Soit M un \mathbb{Z} -module. Les sous-modules de M sont exactement ses sous-groupes.
 5. Si I est un ensemble et M est un A -module, notons $M^{(I)}$ l'ensemble des applications $I \rightarrow M$ à support fini, c'est-à-dire les applications nulles en dehors d'un ensemble fini. Alors $M^{(I)}$ est un sous-module de M^I .

Un sous- A -module est un A -module, pour les lois induites.

Proposition B.3. Soient M et N des A -modules et $f : M \rightarrow N$ une application A -linéaire.

1. Si $M' \subset M$ est un sous-module, alors $f(M')$ est un sous-module de N . En particulier $\text{Im}(f) = f(M)$ est un sous-module de N .
2. Si $N' \subset N$ est un sous-module, alors $f^{-1}(N')$ est un sous-module de M . En particulier $\text{Ker}(f) = f^{-1}(\{0\})$ est un sous module de M .

Preuve. Exercice. \square

Exemple B.4. Soit $(a_1, \dots, a_n) \in A^n$. Alors

$$M = \{(x_1, \dots, x_n) \in A^n \mid x_1 a_1 + \dots + x_n a_n = 0\}$$

est un sous-module de A^n . En effet l'application

$$\begin{aligned} f : A^n &\longrightarrow A \\ (x_1, \dots, x_n) &\longmapsto x_1 a_1 + \dots + x_n a_n \end{aligned}$$

est A -linéaire (vérifier), et $M = \text{Ker}(f)$.

Définition-Proposition B.5. Soient I un ensemble et $(M_i)_{i \in I}$ une famille de A -modules. Alors les lois produit munissent $\prod_{i \in I} M_i$ d'une structure de A -module :

$$(x_i) + (y_i) = (x_i + y_i), a \cdot (x_i) = (a \cdot x_i)$$

Le A -module obtenu, noté encore $\prod_{i \in I} M_i$, est appelé le **A -module produit** des $(M_i)_{i \in I}$.

Preuve. Exercice. \square

Exemple B.6. Si $M_i = M$ pour tout i , le A -module $\prod_i M_i$ est l'ensemble des suites d'éléments de M indexées par I . Il s'identifie au A -module M^I déjà défini des applications $I \rightarrow M$.

Définition-Proposition B.7. Soit $(M_i)_{i \in I}$ une famille de A -modules. On note

$$\bigoplus_{i \in I} M_i = \{(x_i) \in \prod_{i \in I} M_i \mid \exists J \subset I \text{ fini tq } x_i = 0 \text{ pour } i \notin J\}$$

Alors $\bigoplus_{i \in I} M_i$ est un sous-module de $\prod_{i \in I} M_i$, appelé **somme directe** des $(M_i)_{i \in I}$.

Preuve. Exercice. \square

Exemple B.8. Si $M_i = M$ pour tout i , le A -module $\bigoplus_{i \in I} M_i$ est l'ensemble des suites d'éléments de M indexées par I et à support fini. Il s'identifie au A -module $M^{(I)}$ des applications à support fini $I \rightarrow M$.

Définition B.9. Soient M un A -module et $(M_i)_{i \in I}$ une famille de sous-modules de M . On dira (abusivement) que M est **somme directe** des $(M_i)_{i \in I}$, et on notera $M = \bigoplus_{i \in I} M_i$, si l'application A -linéaire

$$\begin{aligned} \bigoplus_{i \in I} M_i &\longrightarrow M \\ (x_i) &\longmapsto \sum_{i \in I} x_i \end{aligned}$$

est un isomorphisme.

On a la reformulation immédiate suivante, qui est souvent la plus utile.

Proposition B.10. Soient M un A -module et $(M_i)_{i \in I}$ une famille de sous-modules de M . Alors $M = \bigoplus_{i \in I} M_i$ si et seulement si tout élément $x \in M$ s'écrit $x = \sum_{i \in I} x_i$, pour un unique $(x_i) \in \bigoplus_{i \in I} M_i$.

Un résultat important pour les espaces vectoriels est l'existence de supplémentaires pour les sous-espaces vectoriels (conséquence du théorème de la base incomplète). Au niveau des modules, on a la caractérisation suivante pour les sous-modules qui admettent un supplémentaire.

Proposition B.11. Soient M un A -module et $M' \subset M$ est un sous-module. Il existe un sous A -module $M'' \subset M$ tel que $M = M' \oplus M''$ (un supplémentaire) si et seulement si il existe une projection $p \in \text{End}_A(M)$ (c'est-à-dire $p \circ p = p$) telle que $M' = p(M)$. Dans ce cas on a alors $M'' = \text{Ker}(p)$.

Preuve. Si $M = M' \oplus M''$, il existe pour tout $x \in M$, des éléments uniques $x' \in M'$ et $x'' \in M''$ tels que $x = x' + x''$. Soit $p : M \rightarrow M$ l'application définie par $p(x) = x'$. On voit facilement que p est A -linéaire, que p est une projection et que $\text{Ker}(p) = M''$.

Réciproquement s'il existe une projection $p \in \text{End}_A(M)$ telle que $M' = p(M)$, on prend $M'' = \text{Ker}(p)$, et on vérifie que l'application A -linéaire $M' \oplus M'' \rightarrow M$, $(x', x'') \mapsto x' + x''$, est un isomorphisme (car $\forall x \in M$, on a $x = p(x) + (x - p(x))$).

L'exemple suivant montre alors que le résultat d'existence d'un supplémentaire pour un sous-espace vectoriel n'est plus vraie en général pour les modules.

Exemple B.12. Soit $n > 1$. Il n'existe pas de sous-module M du \mathbb{Z} -module \mathbb{Z} tel que $\mathbb{Z} = n\mathbb{Z} \oplus M$.

En effet : si un tel M existe, il existe une projection $p \in \text{End}_{\mathbb{Z}}(\mathbb{Z})$ telle que $p(\mathbb{Z}) = n\mathbb{Z}$. Mais on a alors $n\mathbb{Z} = p(\mathbb{Z}) = p \circ p(\mathbb{Z}) = p(n\mathbb{Z}) = np(\mathbb{Z}) = n^2\mathbb{Z}$, ce qui implique $n = 0$ ou $n = \pm 1$. \square

Le résultat suivant est lui aussi souvent utile.

Proposition B.13. Soient M un A -module et M_1, \dots, M_n une famille A -modules. Les assertions suivantes sont équivalentes.

1. $M \cong M_1 \oplus \dots \oplus M_n$.
2. Il existe, pour tout $i \in \{1, \dots, n\}$, des applications A -linéaires $u_i : M_i \rightarrow M$ et $p_i : M \rightarrow M_i$ telles que

$$p_i \circ u_j = \delta_{ij} \text{id}_{M_i}, \quad \text{id}_M = \sum_{i=1}^n u_i \circ p_i$$

Preuve. Notons pour tout i , $p_i : M_1 \oplus \dots \oplus M_n \rightarrow M_i$ la i -ème projection, et $u_i : M_i \rightarrow M_1 \oplus \dots \oplus M_n$ la i -ème injection. Ces applications A -linéaires vérifient

$$p_i \circ u_j = \delta_{ij} \text{id}_{M_i}, \quad \text{id}_{M_1 \oplus \dots \oplus M_n} = \sum_{i=1}^n u_i \circ p_i$$

(1) \Rightarrow (2). Soit $f : M \rightarrow M_1 \oplus \dots \oplus M_n$ un isomorphisme A -linéaire. Alors les applications A -linéaires $v_i = f^{-1} \circ u_i$ et $q_i = p_i \circ f$ vérifient les conditions demandées et on a le résultat.

(2) \Rightarrow (1) Supposons qu'il existe des applications A -linéaires $v_i : M_i \rightarrow M$ et $q_i : M \rightarrow M_i$ telles que $q_i \circ v_j = \delta_{ij} \text{id}_{M_i}$, $\text{id}_M = \sum_{i=1}^n v_i \circ q_i$. On vérifie alors que l'application A -linéaire

$$\begin{aligned} \bigoplus_{i=1}^n M_i &\longrightarrow M \\ (x_i) &\longmapsto \sum_{i=1}^n v_i(x_i) \end{aligned}$$

est un isomorphisme. \square

Définition-Proposition B.14. Soient M un A -module et $(M_i)_{i \in I}$ une famille de sous-modules de M . Alors

$$\sum_{i \in I} M_i = \left\{ \sum_{i \in I} x_i, (x_i) \in \bigoplus_{i \in I} M_i \right\}$$

est un sous-module de M , appelé la somme des sous-modules $(M_i)_{i \in I}$.

Preuve. Exercice. \square

Exemple B.15. Soient M un A -module et N et P des sous-modules de M . On a $M = N \oplus P \iff [M = N + P \text{ et } N \cap P = \{0\}]$.

Définition-Proposition B.16. Soient M un A -module et $(M_i)_{i \in I}$ une famille de sous-modules de M . Alors $\bigcap_{i \in I} M_i$ est un sous-module de M .

Si $S \subset M$, notons $A.S$ (ou AS) l'intersection de tous les sous-modules de M contenant S : c'est le plus petit sous-module de M contenant S , et on dit que AS est le **sous-module engendré par S** . On a

$$A.S = \sum_{x \in S} Ax$$

L'ensemble $A.S$ est l'**ensemble des combinaisons linéaires (à coefficients dans A) des éléments de S** . Si $M = A.S$, on dit S est une **partie génératrice de M** , ou encore **engendre M** . Un **A -module de type fini** est un A -module engendré par une partie finie.

Preuve. Exercice. \square

Remarque. La définition s'applique aussi dans le cas où la partie S est vide, avec alors $A.S = \{0\}$.

Exemple B.17. Le A -module A^n est de type fini, engendré par la partie $\{e_1, \dots, e_n\}$, où $e_i = (0, \dots, 0, \underbrace{1}_{i\text{-eme place}}, 0, \dots, 0)$.

Exemple B.18. Soient M un A -module et $(M_i)_{i \in I}$ une famille de sous-modules de M . Alors le sous-module de M engendré par $\bigcup_{i \in I} M_i$ est $\sum_{i \in I} M_i$ (vérifier).

C Modules quotients

Rappel. Soient $M = (M, +)$ un groupe abélien et $N \subset M$ un sous-groupe. Considérons la relation \mathcal{R}_N définie sur M par

$$x \mathcal{R}_N y \iff x - y \in N$$

La relation \mathcal{R}_N est une relation d'équivalence, on note M/N l'ensemble des classes d'équivalences et $p : M \rightarrow M/N$ la surjection canonique (on note aussi $p(x) = \bar{x}$, etc). Alors il

existe une unique structure de groupe (abélien) sur M/N telle que la surjection canonique soit un morphisme de groupes (de telle sorte que $\overline{x+y} = \overline{x} + \overline{y}$, le neutre est $\overline{0} = p(0)$).

Proposition C.1. Soient $M = (M, +)$ un A -module et $N \subset M$ un sous-module. Il existe sur M/N une unique structure de A -module telle que la surjection canonique $p : M \rightarrow M/N$ soit A -linéaire.

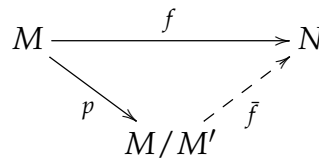
Preuve. Il reste à construire la loi externe $A \times M/N \rightarrow M/N$. Soit $x, y \in M$ tels que $x - y \in N$. Alors $a.(x - y) \in N$ car N est un sous-module. Ainsi $a.x - a.y = a.x + a.(-y) = a.(x - y) \in N$. Ce calcul montre que l'on peut définir une application

$$\begin{aligned} A \times M/N &\rightarrow M/N \\ (a, p(x)) &\mapsto a.p(x) = p(a.x) \end{aligned}$$

On vérifie que muni de cette loi, le groupe abélien M/N est bien un A -module. La surjection canonique est A -linéaire par construction de la structure de A -module, et il est clair que cette propriété assure l'unicité de cette structure. \square

Théorème C.2 (de factorisation et d'isomorphisme pour les A -modules). Soient M et N des A -modules et $f : M \rightarrow N$ une application A -linéaire.

1. Soit $M' \subset M$ un sous-module. Si $f(M') = 0$, alors il existe une unique application A -linéaire $\overline{f} : M/M' \rightarrow N$ telle que $\overline{f} \circ p = f$ ($p : M \rightarrow M/M'$ est la surjection canonique).



2. f induit un isomorphisme de A -modules $M/\text{Ker}(f) \cong \text{Im}(f)$

Preuve. 1. Soient $x, y \in M$ tels que $x - y \in M'$. Alors $f(x - y) = 0$, d'où $f(x) = f(y)$. Ce calcul montre que l'on peut définir une application $\overline{f} : M/M' \rightarrow N$, $\overline{f}(p(x)) = f(x)$. On vérifie que \overline{f} est A -linéaire, et par construction $\overline{f} \circ p = f$. L'unicité provient de la surjectivité de p .

2. On applique la construction précédente à $M' = \text{Ker}(f)$ pour obtenir une application A -linéaire $\overline{f} : M/\text{Ker}(f) \rightarrow \text{Im}(f)$. Le théorème d'isomorphisme pour les groupes assure que f est un isomorphisme de groupes, et est donc un isomorphisme A -linéaire. \square

Exemple C.3. Soit $(a_1, \dots, a_n) \in A^n$ et soit $M = \{(x_1, \dots, x_n) \in A^n \mid x_1 a_1 + \dots + x_n a_n = 0\}$: c'est un sous-module de A^n . Alors les A -modules A^n/M et $Aa_1 + \dots + Aa_n$ sont isomorphes.

En effet : L'application

$$\begin{aligned} f : A^n &\rightarrow Aa_1 + \dots + Aa_n \\ (x_1, \dots, x_n) &\mapsto x_1 a_1 + \dots + x_n a_n \end{aligned}$$

est A -linéaire, avec $\text{Ker}(f) = M$ et $\text{Im}(f) = Aa_1 + \dots + Aa_n$: le théorème d'isomorphisme donne le résultat.

II Modules libres

Dans ce chapitre on étudie une classe importante de modules : les modules libres, qui sont les modules admettant une base. On verra que si l'anneau de base n'est pas corps, il n'existe pas nécessairement une base.

Dans la suite A est un anneau non nul.

A Définition et exemples

Définition A.1. Soit M un A -module et $(x_i)_{i \in I} \in M^I$ une famille d'éléments de M .

1. On dit que la partie $\{x_i\}_{i \in I}$ **engendre** M , ou est **une partie génératrice** de M , lorsque M est engendré par la partie $\{x_i\}_{i \in I}$, c'est-à-dire lorsque $M = \sum_{i \in I} Ax_i$.
2. On dit que la partie $\{x_i\}_{i \in I}$ est **libre**, ou encore **linéairement indépendante**, lorsque

$$\forall (a_i)_{i \in I} \in A^{(I)}, \sum_{i \in I} a_i x_i = 0 \implies a_i = 0, \forall i \in I$$

3. On dit que la partie $\{x_i\}_{i \in I}$ est une **base** de M si elle est libre et génératrice.

Ainsi, la partie $\{x_i\}_{i \in I}$ est une base de M si tout élément de M s'écrit de manière *unique* sous la forme $\sum_{i \in I} a_i x_i$ pour $(a_i) \in A^{(I)}$.

Remarque : on peut formuler les définitions précédentes pour la famille $(x_i)_{i \in I}$ de M , on parle alors de famille libre, famille génératrice.

Définition A.2. On dit qu'un A -module est **libre** s'il possède une base.

Par convention on dira que le module nul est libre (avec \emptyset pour base).

Exemple A.3. 1. Pour $n \in \mathbb{N}^*$, le A -module A^n est libre, et la partie $\{e_1, \dots, e_n\}$, où $e_i = (0, \dots, \underbrace{0, 1, 0, \dots, 0}_{\text{place } i})$, est une base de A^n (la base canonique). On fait de plus

la convention $A^0 = \{0\}$, c'est bien un module libre.

2. Soit I un ensemble. Le A -module $A^{(I)}$ des fonctions à support fini $I \rightarrow A$ est libre. Pour $i \in I$, notons e_i la fonction caractéristique du singleton $\{i\}$. Alors $\{e_i\}_{i \in I}$ est une base de $A^{(I)}$.

Preuve. Si $f \in A^{(I)}$, Soit $J \subset I$ le support de $f : J = \{i \in I \mid f(i) \neq 0\}$. On vérifie alors que $f = \sum_{i \in J} f(i)e_i$, ce qui montre que la partie $\{e_i\}_{i \in I}$ engendre $A^{(I)}$. Soit $(a_i)_{i \in I} \in A^{(I)}$ tel que $\sum_{i \in I} a_i e_i = 0$. Alors pour tout $i_0 \in I$, on a $0 = \sum_{i \in I} a_i e_i(i_0) = a_{i_0}$. Ceci montre que la partie $\{e_i\}_{i \in I}$ est libre. \square

Le théorème qui suit est une propriété cruciale des modules libres.

Théorème A.4. Soit M un A -module libre de base $\{e_i\}_{i \in I}$. Soit N un A -module et $x_i, i \in I$, des éléments de N . Alors il existe une unique application A -linéaire $f : M \rightarrow N$ telle que $\forall i \in I$, on a $f(e_i) = x_i$.

Preuve. Pour montrer l'unicité, supposons qu'il existe une telle application f . Soit $x \in M$: on a $x = \sum_{i \in I} a_i \cdot e_i$ pour $(a_i) \in A^{(I)}$. Alors par linéarité de f on a $f(x) = \sum_{i \in I} a_i \cdot f(e_i) = \sum_{i \in I} a_i \cdot x_i$, et cela montre l'unicité.

On construit alors f de la manière suivante. Soit $x \in M$: x s'écrit de manière *unique* sous la forme $x = \sum_{i \in I} a_i \cdot e_i$ pour $(a_i) \in A^{(I)}$. On pose alors $f(x) = \sum_{i \in I} a_i \cdot x_i$. Ceci définit une application $f : M \rightarrow N$ telle que $\forall i \in I, f(e_i) = x_i$, et on vérifie sans problème que f est linéaire. \square

Corollaire A.5. Si M est un A -module libre, il existe un ensemble I tel que les A -modules $A^{(I)}$ et M soient isomorphes.

Preuve. Soit $\{x_i\}_{i \in I}$ une base de M . On considère le A -module libre $A^{(I)}$, de base $\{e_i\}_{i \in I}$. Il existe, par le théorème précédent, des applications A -linéaires $f : A^{(I)} \rightarrow M$ et $g : M \rightarrow A^{(I)}$ telles que $\forall i \in I, f(e_i) = x_i$ et $g(x_i) = e_i$. Alors $\forall i \in I, g \circ f(e_i) = e_i$ et puisque $\{e_i\}_{i \in I}$ est une base de $A^{(I)}$, la linéarité de $g \circ f$ assure que $g \circ f = \text{id}_{A^{(I)}}$. De même on voit que $f \circ g = \text{id}_M$, et on a bien l'isomorphisme annoncé. \square

Corollaire A.6. Tout A -module est quotient d'un module libre.

Preuve. Soit $\{x_i\}_{i \in I}$ une partie génératrice de M et soit $f : A^{(I)} \rightarrow M$ l'unique application A -linéaire telle que $\forall i \in I, f(e_i) = x_i$. On a donc $x_i \in \text{Im}(f), \forall i \in I$, et $\sum_{i \in I} Ax_i = M \subset \text{Im}(f)$, et ainsi f est surjective. Le théorème d'isomorphisme permet de conclure. \square

Corollaire A.7. Soient M et N des A -modules et $f : M \rightarrow N$ une application A -linéaire surjective. Si N est libre, il existe une application A -linéaire $s : N \rightarrow M$ telle que $f \circ s = \text{id}_N$.

Preuve. Soit $\{e_i\}_{i \in I}$ une base de N . Comme f est surjective, il existe, pour tout $i \in I, x_i \in M$ tel que $f(x_i) = e_i$. Soit $s : N \rightarrow M$ l'unique application A -linéaire telle $\forall i \in I, s(e_i) = x_i$. On a alors $f \circ s(e_i) = e_i, \forall i \in I$, et donc $f \circ s = \text{id}_N$ par linéarité (et le fait que $\{e_i\}_{i \in I}$ est une base de N). \square

Corollaire A.8. Si A est un anneau intègre qui n'est pas un corps (par exemple $A = \mathbb{Z}$), alors il existe des A -modules non libres.

Preuve. L'anneau A est intègre et n'est pas un corps, il existe donc un élément $a \in A$ non nul tel que $I = Aa \subsetneq A$ et A/I est non nul. Supposons que le A -module A/I est libre. Soit $p : A \rightarrow A/I$ la surjection canonique. Il existe, d'après le corollaire précédent, une application A -linéaire $s : A/I \rightarrow A$ telle que $p \circ s = \text{id}_{A/I}$. Comme $a \in I$, on a, en utilisant la linéarité de $s, 0 = s(p(a)) = s(a \cdot p(1)) = as(p(1))$. L'anneau A est intègre et $a \neq 0$, donc $s(p(1)) = 0$. Mais alors $p(1) = p \circ s(p(1)) = 0$, ce qui implique $1 \in I$ et $I = A$: on aboutit à une contradiction. \square

B Le théorème de la base incomplète

On vient donc de voir qu'en toute généralité, il existe des modules non libres si A n'est pas un corps.

Théorème B.1 (de la base incomplète). Supposons que A est un corps. Soient M un A -module, S une partie libre de M et X une partie génératrice de M . Alors il existe une base \mathcal{B} de M telle que $S \subset \mathcal{B} \subset X$.

Preuve. Soit I l'ensemble des parties libres E de M telles que $S \subset E \subset X$: I est non vide car $S \in I$. On munit I de l'ordre induit par l'inclusion des parties de M . On voit facilement que I est ordonné *inductif* (toute partie non vide totalement ordonnée admet un majorant). On peut donc utiliser le lemme de Zorn : I possède un élément maximal, que l'on note \mathcal{B} . Montrons que \mathcal{B} est une base de M : on sait déjà que c'est une partie libre, il reste à voir que c'est une partie génératrice de M . Tout élément de M est combinaison linéaire d'éléments de X , il suffit donc de voir que tout élément de X est combinaison linéaire d'éléments de \mathcal{B} . Soit $x \in X \setminus \mathcal{B}$. Alors la partie $\mathcal{B} \cup \{x\}$ n'est pas libre par maximalité de \mathcal{B} . Il existe donc $e_1, \dots, e_n \in \mathcal{B}$, $a_1, \dots, a_n \in A$ et $b \in \mathcal{B}$ tels que $a_1.e_1 + \dots + a_n.e_n + b.x = 0$, avec $b \neq 0$ (car \mathcal{B} est libre). Alors $b.x = -\sum_{i=1}^n a_i.e_i = \sum_{i=1}^n (-a_i).e_i$. Comme A est un corps, $b \neq 0$ est inversible et on a

$$x = 1.x = (b^{-1}b).x = b^{-1}.(b.x) = b^{-1}.(\sum_{i=1}^n (-a_i).e_i) = \sum_{i=1}^n (-b^{-1}a_i).e_i$$

ce qui montre que x est combinaison linéaire d'éléments de \mathcal{B} . \square

Corollaire B.2. Si A est un corps, tout A -espace vectoriel (A -module) possède une base.

Preuve. Soit M un A -espace vectoriel. Si M est nul il n'y a rien à montrer, sinon on prend $x \in M$, $x \neq 0$. La partie $\{x\}$ est libre car A est un corps, et on peut appliquer le théorème de la base incomplète (en prenant par exemple $X = M$ comme partie génératrice). \square

C Rang d'un module libre

On se propose de démontrer le résultat suivant.

Théorème C.1. Soient A un anneau commutatif non nul et M un A -module libre. Toutes les bases de M ont le même cardinal.

On verra plus loin que le théorème n'est pas vrai si A n'est pas supposé commutatif. On va commencer par établir le résultat dans le cas où le module libre admet une base ayant un nombre fini d'éléments. On aura besoin de la notion suivante.

Définition C.2. Soient M_1, \dots, M_n, V des A -modules. Une application $f : M_1 \times \dots \times M_n \longrightarrow V$ est dite *n -linéaire* si pour chaque i et des éléments fixés $x_j \in M_j$, $j \neq i$, l'application

$$M_i \longrightarrow V, x \longmapsto f(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)$$

est A -linéaire. Quand $M_i = M, \forall i$ et $V = A$, on dit que $f : M^n \longrightarrow A$ est une **forme n -linéaire sur M** .

On dit qu'une forme n -linéaire $f : M^n \longrightarrow A$ est **alternée** si pour tout $(x_1, \dots, x_n) \in M^n$, alors $x_i = x_j$ avec $i \neq j$ entraîne $f(x_1, \dots, x_n) = 0$.

Proposition C.3. Soit A un anneau commutatif (non nul) et soit M un A -module.

1. Si $f : M^n \longrightarrow A$ est une forme n -linéaire alternée, on a pour tout $\sigma \in S_n$ et tout $(x_1, \dots, x_n) \in M^n$,

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma)f(x_1, \dots, x_n)$$

2. Si M admet une partie génératrice ayant $p < n$ éléments, alors toute forme n -linéaire alternée sur M est nulle.
3. Si M est un A -module libre ayant une base $\{e_1, \dots, e_n\}$ à n éléments, il existe une unique forme n -linéaire alternée $\Delta : M^n \longrightarrow A$ telle que $\Delta(e_1, \dots, e_n) = 1$

Preuve. 1. Supposons dans un premier temps que σ est une transposition : $\sigma = (i, j)$ avec $i < j$. Alors

$$f(x_1, \dots, x_i + x_j, \dots, x_j + x_i, \dots, x_n) = 0$$

$$\Rightarrow f(x_1, \dots, x_i, \dots, x_i, \dots, x_n) + f(x_1, \dots, x_i, \dots, x_j, \dots, x_n) +$$

$$f(x_1, \dots, x_j, \dots, x_j, \dots, x_n) + f(x_1, \dots, x_j, \dots, x_i, \dots, x_n) = 0$$

$$\Rightarrow f(x_1, \dots, x_j, \dots, x_i, \dots, x_n) = -f(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = \varepsilon(\sigma)f(x_1, \dots, x_i, \dots, x_j, \dots, x_n)$$

Pour traiter le cas général, on remarque que l'on a une application

$$M^n \times S_n \longrightarrow M^n$$

$$((x_1, \dots, x_n), \sigma) \longmapsto (x_1, \dots, x_n) \cdot \sigma = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

qui vérifie $(x_1, \dots, x_n) \cdot (\sigma\tau) = ((x_1, \dots, x_n) \cdot \sigma) \cdot \tau, \forall \sigma, \tau \in S_n$ et $(x_1, \dots, x_n) \cdot 1 = (x_1, \dots, x_n)$. Le groupe S_n est engendré par les transpositions et la signature est un morphisme de groupes, le résultat se montre donc sans difficulté par récurrence sur le nombre de transpositions dont la permutation σ est un produit, à partir de la première étape.

2. Supposons que $\{e_1, \dots, e_p\}$ est une partie génératrice de M . Pour $(x_1, \dots, x_n) \in M^n$, on écrit pour chaque $i, x_i = \sum_{j=1}^p a_{ij}e_j$. On a donc,

$$f(x_1, \dots, x_n) = \sum_{j_1, \dots, j_n} a_{j_1 1} \cdots a_{j_n n} f(e_{j_1}, \dots, e_{j_n}) = 0$$

car f est n -linéaire et alternée et $p < n$.

3. Supposons que $\{e_1, \dots, e_n\}$ est une partie génératrice de M . Pour $(x_1, \dots, x_n) \in M^n$, on a, en reprenant les notations précédentes

$$f(x_1, \dots, x_n) = \sum_{j_1, \dots, j_n} a_{j_1 1} \cdots a_{j_n n} f(e_{j_1}, \dots, e_{j_n})$$

$$= \sum_{\sigma \in S_n} a_{\sigma(1)1} \cdots a_{\sigma(n)n} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \left(\sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} \right) f(e_1, \dots, e_n)$$

Il existe donc au plus une forme n -linéaire alternée $f : M^n \longrightarrow A$ telle que $f(e_1, \dots, e_n) = 1$. Si maintenant $\{e_1, \dots, e_n\}$ est une base de M , on définit une application

$$\Delta : M^n \longrightarrow A$$

en posant

$$\Delta(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

où comme précédemment, on a, pour chaque i , $x_i = \sum_{j=1}^p a_{ji} e_j$. Il est clair que $\Delta(e_1, \dots, e_n) = 1$ et on vérifie sans difficulté que Δ est n -linéaire. Soit $(x_1, \dots, x_n) \in M^n$ avec $x_i = x_j$ pour $i < j$. On a

$$\begin{aligned} \Delta(x_1, \dots, x_n) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} \\ &= \sum_{\sigma \in A_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} + \sum_{\sigma \in A_n(i,j)} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} \\ &= \sum_{\sigma \in A_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} + \sum_{\sigma \in A_n} \varepsilon(\sigma(i,j)) a_{\sigma(1)1} \cdots a_{\sigma(j)i} \cdots a_{\sigma(i)j} \cdots a_{\sigma(n)n} \\ &= \sum_{\sigma \in A_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} + \sum_{\sigma \in A_n} -\varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(j)j} \cdots a_{\sigma(i)i} \cdots a_{\sigma(n)n} \\ &= 0 \end{aligned}$$

Ceci montre que Δ est alternée. \square

Preuve du théorème C.1. Etape 1. Supposons que M admet une base finie, et soit $(e_i)_{i \in I}$ une telle base. Soit $(f_j)_{j \in J}$ une autre base de M . Montrons que J est fini.

Pour tout $i \in I$, il existe un élément $(a_{ij})_{j \in J} \in A^{(J)}$ tel que

$$e_i = \sum_{j \in J} a_{ij} f_j$$

Notons $S_i \subset J$ le support (fini) de $(a_{ij})_{j \in J}$: $S_i = \{j \in J \mid a_{ij} \neq 0\}$. Soit $J' = \cup_{i \in I} S_i \subset J$. Soit M' le sous-module de M engendré par les $f_j, j \in J'$. Comme $\forall i \in I$, on a $e_i \in M'$, on a donc $M' = M$ et $J = J'$ (par l'indépendance linéaire des f_j) et donc J est fini.

Si $n = \text{Card}(I)$ et $p = \text{Card}(J)$ avec \cdot , il existe par la proposition précédente une forme n -linéaire alternée non nulle et on a nécessairement $p \geq n$, et l'argument symétrique montre que $p = n$.

Etape 2. Soient $(e_i)_{i \in I}$ et $(f_j)_{j \in J}$ deux bases de M . On peut supposer que I et J sont infinis. Montrons d'abord que $\text{Card}(I) \leq \text{Card}(J \times \mathbb{N})$. Pour tout $j \in J$, soit $(a_{ij})_{i \in I} \in A^{(I)}$ tels que $f_j = \sum_{i \in I} a_{ij} e_i$, et notons $S_j \subset I$ le support (fini) de $(a_{ij})_{i \in I}$: $S_j = \{i \in I \mid a_{ij} \neq 0\}$. Soit $I' = \cup_{j \in J} S_j$. Tous les f_j appartiennent à M' , le sous module de M engendré par les $e_i, i \in I'$, donc $M' = M$. On a donc $I' = I$ (car pour $i \in I$, e_i est combinaison linéaire d'éléments $e_{i'}, i' \in I$, et par l'indépendance linéaire on a $i \in I'$) et ainsi

$$\text{Card}(I) = \text{Card}(I') = \text{Card}(\cup_{j \in J} S_j) \leq \text{Card}(J \times \mathbb{N})$$

L'inégalité de droite s'obtient en utilisant le lemme suivant.

Lemme C.4. Soit E un ensemble et $(E_j)_{j \in J}$ des parties de E . Alors $\text{Card}(\cup_{j \in J} E_j) \leq \text{Card}(J \times E)$. En particulier si les E_j sont finis, on a $\text{Card}(\cup_{j \in J} E_j) \leq \text{Card}(J \times \mathbb{N})$.

Preuve du lemme. Pour chaque $x \in \cup_{j \in J} E_j$, on choisit un élément $\tau(x) \in J$ tel que $x \in E_{\tau(x)}$. On construit ainsi une injection $(\cup_{j \in J} E_j) \hookrightarrow (J \times E)$ en associant à $x \in \cup_{j \in J} E_j$ le couple $(\tau(x), x)$. Si les E_j sont finis, on fixe pour tout j une injection $\nu_j : E_j \hookrightarrow \mathbb{N}$, et on obtient une application injective $\cup_{j \in J} E_j \hookrightarrow J \times \mathbb{N}, x \mapsto (\tau(x), \nu_{\tau(x)}(x))$. \square

Comme J est infini, on a $\text{Card}(J \times \mathbb{N}) = \text{Card}(J)$ (propriété vraie pour tout ensemble infini, admise si elle n'est pas déjà connue), et donc $\text{Card}(I) \leq \text{Card}(J)$. En échangeant les rôles de I et J , on obtient $\text{Card}(J) \leq \text{Card}(I)$ et le théorème de Cantor-Bernstein permet de conclure que $\text{Card}(I) = \text{Card}(J)$. \square

Définition C.5. Soit A un anneau commutatif non nul. Le cardinal d'une base d'un A -module libre est appelé le **rang** (ou **dimension** si A est un corps) du module.

Exemple C.6. 1. Le A -module libre A^n est libre de rang n .

2. Si M et N sont des A -modules libres de rang respectifs m et n , alors $M \oplus N$ est libre de rang $m + n$.

Remarque. Si A est un corps non commutatif, il est également vrai que toutes les bases d'un A -module (A -espace vectoriel) ont même cardinal. Par contre le résultat n'est plus vrai si A n'est pas un corps, comme le montre l'exemple suivant.

Exemple C.7. Soit K un corps commutatif. Soit V un K -espace vectoriel ayant une base $(e_n)_{n \in \mathbb{N}}$ (par exemple $V = K^{(\mathbb{N})}$). Considérons l'anneau $A = \text{End}_K(V)$ des endomorphismes K -linéaires de V . Alors A possède une base ayant un élément, ainsi qu'une base ayant deux éléments.

En effet : A est bien sûr un A -module libre avec une base à un élément ($1_A = \text{id}_V$). Considérons maintenant les éléments u, v de $A = \text{End}_K(V)$ définis par

$$u(e_i) = e_{2i}, v(e_i) = e_{2i+1}, \forall i \in \mathbb{N}$$

ainsi que les les éléments u', v' de A définis par

$$u'(e_i) = \begin{cases} e_{\frac{i}{2}} & \text{si } i \text{ est pair} \\ 0 & \text{si } i \text{ impair} \end{cases} \quad v'(e_i) = \begin{cases} e_{\frac{i-1}{2}} & \text{si } i \text{ est impair} \\ 0 & \text{si } i \text{ est pair} \end{cases}$$

On vérifie alors que $u' \circ u = \text{id}_V = v' \circ v = u \circ u' + v \circ v'$, et $u' \circ v = 0 = v' \circ u$. Montrons que (u', v') est une base du A -module A . Si $f \in A$, on a $f = f \circ \text{id}_V = (f \circ u) \circ u' + (f \circ v) \circ v'$, ce qui montre que (u', v') engendrent A . Si $f, g \in A$ vérifient $f \circ u' + g \circ v' = 0$, alors $f \circ u' \circ u = 0 = f$ et $g \circ v' \circ v = 0 = g$ (par les identités précédentes), donc (u', v') est une famille libre, et est donc une base du A -module A . \square

On termine la section en mentionnant la non-généralisation d'autres résultats classiques sur les espaces vectoriels aux modules arbitraires.

Remarques C.8. 1. Un sous-module d'un module libre n'est pas nécessairement libre.

2. Un sous-module d'un module de type fini n'est pas nécessairement de type fini.

En effet : 1. Considérons $A = \mathbb{Z}/n^2\mathbb{Z}$, $n \geq 2$. Pour $k \in \mathbb{Z}$, notons \bar{k} sa classe dans A . Soit $M = \{\overline{kn}, k \in \mathbb{Z}\} = \{\overline{0}, \overline{n}, \dots, \overline{(n-1)n}\}$. C'est un idéal de A , c'est-à-dire un sous-module de A . Montrons qu'aucun élément de M n'est libre, ce qui montrera que M ne possède pas de base et donc n'est pas libre. Soit $x \in M$: $x = \overline{kn}$. Alors on a $\overline{n} \cdot \overline{x} = \overline{n} \overline{kn} = \overline{n^2 k} = \overline{0}$, avec $\overline{n} \neq 0$, ce qui montre que x n'est pas libre.

2. Soit K un corps et $A = K^{\mathbb{N}}$. Alors $M = A$ est un A -module de type fini, mais $K^{(\mathbb{N})}$ n'est pas un sous-module de type fini de A . Sinon, il existerait $f_1, \dots, f_m \in K^{(\mathbb{N})}$ tels que $K^{(\mathbb{N})} = Af_1 + \dots + Af_m$. Soit $J = \{k \in \mathbb{N}, \exists i \in \{1, \dots, m\} \text{ tq } f_i(k) \neq 0\}$. Alors J est fini car $f_1, \dots, f_m \in A^{(I)}$, et pour tout élément $f \in Af_1 + \dots + Af_m$, on a $f(k) = 0$ pour $k \notin J$. Puisque J est fini, il existe donc f qui n'appartient pas à $Af_1 + \dots + Af_m$, ce qui donne une contradiction. \square

D Module de torsion

Pour un module M , on introduit un sous-ensemble (un sous-module si A est intègre et commutatif) qui permet à l'occasion de montrer qu'un module n'est pas libre.

Définition-Proposition D.1. Soit M un A -module. Le sous-ensemble de **torsion** de M est défini par

$$T(M) := \{x \in M \mid \exists a \in A \setminus \{0\} \text{ tq } a.x = 0\}$$

Si A est intègre et commutatif, alors $T(M)$ est un sous-module de M .

Preuve. Il est clair que $0 \in M$. Soient $x, y \in T(M)$: il existe $a, b \in A \setminus \{0\}$ tels que $a.x = 0 = b.y$. Alors $ab.(x + y) = 0$ car A commutatif, avec $ab \neq 0$ car A intègre. De plus $\forall c \in A$, on a $a.(c.x) = c.(a.x) = 0$, d'où $c.x \in T(M)$. \square

Proposition D.2. Si A est un anneau intègre et M est un A -module libre, alors $T(M) = (0)$.

Preuve. Soit $\{e_i\}_{i \in I}$ une base de M et $x \in M : x = \sum_{i \in I} a_i.e_i$ pour $(a_i)_{i \in I} \in A^{(I)}$. Si $x \in T(M)$, soit $a \in A \setminus \{0\}$ tel que $a.x = 0$. Alors $\sum_{i \in I} (aa_i).e_i = 0$, donc $aa_i = 0$, pour tout i . L'anneau A est intègre, donc $a_i = 0, \forall i$, et $x = 0$. \square

- Exemple D.3.**
1. Si M est un groupe abélien (\mathbb{Z} -module) fini, alors $T(M) = M$.
 2. Si $M = A/I$ ($I \neq (0)$ idéal de A), alors $T(A/I) = A/I$ (ce qui redémontre que A/I n'est pas un module libre si A est intègre et commutatif).
 3. Si $M = N \oplus P$, alors $T(M) = T(N) \oplus T(P)$.
 4. On a $T(\mathbb{Q}) = (0)$, mais \mathbb{Q} n'est pas un \mathbb{Z} -module libre.

On verra plus loin que si A est un anneau principal et si M est un A -module de type fini, alors M est libre si et seulement si $T(M) = (0)$.

III Algèbres

Dans ce chapitre A est un anneau commutatif.

A Définitions

Définition A.1. Soient M, N, P des A -modules et $f : M \times N \rightarrow P$ une application. On dit que f est une application A -bilinéaire si c'est une application 2-linéaire, c'est-à-dire si f est A -linéaire en chaque variable :

1. $f(a.x+y, z) = a.f(x, z) + f(y, z), \forall a \in A, \forall x, y \in M, \forall z \in N$;
2. $f(x, a.y+z) = a.f(x, y) + f(x, z), \forall a \in A, \forall x \in M, \forall y, z \in N$.

Définition A.2. Une A -algèbre est un A -module R muni d'une application A -bilinéaire

$$\begin{aligned} R \times R &\longrightarrow R \\ (x, y) &\longmapsto x * y \end{aligned}$$

telle que $\forall x, y, z \in R$, on a $(x * y) * z = x * (y * z)$, et il existe $1 \in R$ tel que $x * 1 = 1 * x = x$, $\forall x \in R$.

Les axiomes ci-dessus impliquent que $(R, +, *)$ est un anneau.

Exemples A.3. 1. Les \mathbb{Z} -algèbres sont exactement les anneaux.

2. Soit R un anneau et soit

$$Z(R) = \{x \in R \mid yx = xy, \forall y \in R\}$$

le centre de R (c'est un sous-anneau de R). Alors R est une $Z(R)$ -algèbre, la structure de $Z(R)$ -module étant induite par la multiplication de R . Plus généralement si A est un sous-anneau de $Z(R)$, alors R est une A -algèbre (vérifier). Encore plus généralement, tout morphisme d'anneaux $A \rightarrow Z(R)$ induit une structure de A -algèbre sur A .

3. $\mathcal{M}_n(A)$, l'ensemble des matrices $n \times n$ à coefficients dans A , est un A -module et un anneau, et est une A -algèbre (cet exemple sera étudié dans le chapitre suivant).
4. Si I est un ensemble, le A -module A^I est une A -algèbre, le produit étant donné par le produit ponctuel des fonctions (vérifier).
5. Si M est un A -module, alors $\text{End}_A(M)$ est une A -algèbre.

Les lemmes suivants sont très utiles pour construire des algèbres.

Lemme A.4. Soient M, N, P des A -modules. Supposons que M et N sont libres de bases respectives $\{e_i\}_{i \in I}$ et $\{e'_j\}_{j \in J}$. Soit $\{x_{ij}\}_{i \in I, j \in J}$ une famille d'éléments de P . Alors il existe une unique application A -bilinéaire $f : M \times N \rightarrow P$ telle que $f(e_i, e'_j) = x_{ij}, \forall i \in I, \forall j \in J$.

Preuve. Exercice. \square

Lemme A.5. Soit R un A -module engendré par une famille $\{e_i\}_{i \in I}$. Soit $m : R \times R \rightarrow R$, $(x, y) \mapsto x \cdot y$ une application A -bilinéaire telle que

1. $e_i \cdot (e_j \cdot e_k) = (e_i \cdot e_j) \cdot e_k, \forall i, j, k \in I$
2. il existe $e \in R$ tel que $e_i \cdot e = e_i = e \cdot e_i, \forall i \in I$.

Alors m munit R d'une structure de A -algèbre (l'unité de l'anneau R est e).

Preuve. Il suffit de vérifier que $\forall x, y, z \in R$, on a $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ et $x \cdot e = e \cdot x = x$. Cela se fait sans difficulté à partir de la bilinéarité de m et des hypothèses. \square

Exemple A.6. Soit I est un ensemble fini, et considérons l'unique application bilinéaire $A^I \times A^I \rightarrow A^I$, $(e_i, e_j) \mapsto \delta_{ij}e_i$. Elle munit le A -module libre $A^I (= A^{(I)}$ car I est fini) d'une structure de A -algèbre. Le produit correspond en fait au produit ponctuel des fonctions.

Définition A.7. Si R et S sont des R -algèbres, un **morphisme de A -algèbres** $f : R \rightarrow S$ est une application A -linéaire qui est aussi un morphisme d'anneaux.

On vérifiera que la composée de deux morphismes de A -algèbres est encore un morphisme de A -algèbres. Bien sûr un isomorphisme de A -algèbres est un morphisme de A -algèbres bijectif, et on vérifiera que la bijection inverse d'un isomorphisme de A -algèbres est encore un isomorphisme de A -algèbres.

Plus généralement, les définitions, constructions et résultats sur les modules et anneaux ont des analogues évidents. Nous ne les énoncerons pas, mais citons tout de même les faits suivants.

\rightsquigarrow **Sous-algèbres.** Une sous-algèbre est un sous-anneau qui est un sous-module.

\rightsquigarrow **Idéaux dans une algèbre.** Si R est une A -algèbre et I est un idéal de R , alors I est automatiquement un sous A -module (vérifier), et on peut former la A -algèbre quotient R/I .

\rightsquigarrow **Noyau d'un morphisme d'algèbres.** Le noyau d'un morphisme d'algèbres est un idéal, et on a un théorème d'isomorphisme pour les algèbres.

\rightsquigarrow **Modules sur une algèbre.** Si R est une A -algèbre et M est un R -module, alors M est automatiquement un A -module, avec $a.m = (a.1_R).m$. Plus généralement on a

Proposition A.8. Soit R une A -algèbre et soit M un A -module. Il est équivalent de se donner

1. une structure de R -module sur M telle que $a.m = (a.1_R).m, \forall a \in A, \forall m \in M$;
2. un morphisme de A -algèbres $\varphi : R \rightarrow \text{End}_A(M)$.

La démonstration est laissée en exercice.

La structure de A -module d'un module sur une A -algèbre R peut s'avérer très utile pour l'étude des R -modules. Par exemple, si $A = k$ est un corps et si R est une k -algèbre de dimension finie (i.e. est de dimension finie comme k -espace vectoriel), alors si M est un R -module avec $0 < \dim_k(M) < \dim_k(R)$, on voit que M n'est pas un R -module libre.

B L'algèbre d'un monoïde

On présente dans cette section une construction très importante d'algèbre : l'algèbre d'un monoïde. Cette construction englobe non seulement les algèbres de polynômes, mais aussi bien d'autres exemples intéressants.

Soit $G = (G, \cdot)$ est un monoïde (la loi $\cdot : G \times G \longrightarrow G$ est associative et possède un élément neutre, noté 1). On considère le A -module libre $A^{(G)}$, avec sa base canonique $\{e_g\}_{g \in G}$.

Définition-Proposition B.1. Soit $G = (G, \cdot)$ un monoïde. Il existe sur $A^{(G)}$ une unique structure de A -algèbre dont la structure sous-jacente de A -module est celle de $A^{(G)}$, et dont le produit $*$: $A^{(G)} \times A^{(G)} \longrightarrow A^{(G)}$ vérifie, $\forall g, h \in G$, $e_g * e_h = e_{gh}$. L'élément neutre multiplicatif est e_1 . Le produit $*$ est appelé **produit de convolution**. La A -algèbre obtenue, notée $A[G]$, est appelée **la A -algèbre du monoïde G** .

Preuve. L'existence de l'application A -bilinéaire $*$: $A^{(G)} \times A^{(G)} \longrightarrow A^{(G)}$ est assurée par un lemme précédent ($A^{(G)}$ est un A -module libre de base $\{e_g\}_{g \in G}$). Les identités

$$(e_g * e_h) * e_s = e_g * (e_h * e_s), \quad e_g * e_1 = e_g = e_1 * e_g, \quad \forall g, h, s \in G$$

sont assurées par les propriétés du monoïde G , et on obtient bien la A -algèbre annoncée. \square

L'application $i : A \longrightarrow A[G], a \longmapsto a.e_1$, est un morphisme d'anneaux injectif, qui permet d'identifier A à un sous-anneau de $A[G]$.

Théorème B.2 (Propriété universelle de l'algèbre d'un monoïde). Soient R une A -algèbre, G un monoïde et $f : G \longrightarrow R$ une application multiplicative, c'est-à-dire que $f(xy) = f(x)f(y), \forall x, y \in G$, et $f(1) = 1$. Alors il existe un unique morphisme de A -algèbres

$$\bar{f} : A[G] \longrightarrow R \text{ tel que } \bar{f}(e_g) = f(g), \quad \forall g \in G$$

Preuve. Comme $A[G]$ est un A -module libre de base $\{e_g\}_{g \in G}$, il existe une unique application A -linéaire $\bar{f} : A[G] \longrightarrow R$ tel que $\bar{f}(e_g) = f(g), \forall g \in G$. On a $\bar{f}(e_1) = f(1) = 1$. Pour $x = \sum_{g \in G} x_g.e_g$ et $y = \sum_{g \in G} y_g.e_g$, on a $xy = \sum_{s \in G} (\sum_{gh=s} x_g y_h).e_s$, et donc

$$\bar{f}(xy) = \sum_{s \in G} (\sum_{gh=s} x_g y_h).f(s)$$

alors que

$$\bar{f}(x)\bar{f}(y) = \sum_{g, h \in G} (x_g y_h).(f(g)f(h)) = \sum_{g, h \in G} (x_g y_h).f(gh) = \sum_{s \in G} (\sum_{gh=s} x_g y_h).f(s)$$

et ainsi \bar{f} est un morphisme d'algèbres. \square

Remarque. La A -algèbre $A[G]$ est commutative si et seulement si le monoïde G est commutatif.

On décrira au chapitre VI la structure de l'algèbre $\mathbb{C}[G]$ lorsque G est un groupe fini. On utilisera le résultat suivant.

Proposition B.3. Soit G un groupe fini. Alors $Z(A[G])$, le centre de $A[G]$, est un A -module libre de rang égal au nombre de classes de conjugaison de G .

Preuve. Soit $\phi \in A[G]$. Alors puisque les $(e_g)_{g \in G}$ forment une base de $A[G]$, il est clair que $\phi \in Z(A[G]) \iff [\forall g \in G, e_g * \phi = e_g * \phi]$, d'où en multipliant à gauche par $e_{g^{-1}}$, $\phi \in Z(A[G]) \iff [\forall g \in G, e_g * \phi * e_{g^{-1}} = \phi]$ donc

$$\phi \in Z(A[G]) \iff \forall g \in G, \phi = \sum_{h \in G} \phi(h)e_h = e_g * \phi * e_{g^{-1}} = \sum_{y \in G} \phi(y)e_{gyg^{-1}} = \sum_{h \in G} \phi(g^{-1}hg)e_h$$

Ceci montre que $\phi \in Z(A[G]) \iff \forall g, h \in G, \phi(ghg^{-1}) = \phi(h)$ (ϕ est une fonction centrale sur G).

Soit C une classe de conjugaison de G . On pose $x_C = \sum_{g \in C} e_g$. Alors la fonction x_C est la fonction indicatrice de la classe de conjugaison C : $x_C(g) = 1$ si $g \in C$ et $x_C(g) = 0$ si $g \notin C$. Ainsi x_C est constante sur les classes de conjugaison, et est une fonction centrale, d'où $x_C \in Z(A[G])$. Soient C_1, \dots, C_t les classes de conjugaison de G : $G = C_1 \amalg \dots \amalg C_t$. On sait donc que $Ax_{C_1} + \dots + Ax_{C_t} \subset Z(A[G])$. Montrons que x_{C_1}, \dots, x_{C_t} est une base de $Z(A[G])$. Déjà ces éléments sont linéairement indépendants car les $(e_g)_{g \in G}$ le sont et les classes de conjugaison sont disjointes. Soit maintenant $\phi \in Z(A[G])$. Alors ϕ est une fonction centrale, et donc est constante sur les classes de conjugaison de G . Si C est une classe de conjugaison de G , notons $\phi(C)$ la valeur de ϕ sur n'importe quel élément de C . On obtient alors

$$\phi = \sum_{g \in G} \phi(g)e_g = \sum_{i=1}^t \sum_{g \in C_i} \phi(g)e_g = \sum_{i=1}^t \sum_{g \in C_i} \phi(C_i)e_g = \sum_{i=1}^t \phi(C_i) \sum_{g \in C_i} e_g = \sum_{i=1}^t \phi(C_i)x_{C_i},$$

ce qui assure bien que x_{C_1}, \dots, x_{C_t} est une partie génératrice de $Z(A[G])$, et donc une base de $Z(A[G])$ qui est donc un A -module libre de rang le nombre de classes de conjugaison de G . \square

C Algèbres de polynômes

On va utiliser la construction du paragraphe précédent pour (re)définir une classe d'algèbres très importante : les algèbres de polynômes.

Soit $n \in \mathbb{N}^*$. Considérons le monoïde additif \mathbb{N}^n . Pour $i \in \{1, \dots, n\}$, notons $X_i = e_{(0, \dots, 1, \dots, 0)}$, où le 1 est situé à la i -ème place. Par définition du produit dans $A[\mathbb{N}^n]$, on a, pour $(i_1, \dots, i_n) \in \mathbb{N}^n$,

$$e_{(i_1, \dots, i_n)} = X_1^{i_1} \cdots X_n^{i_n}$$

avec bien sûr la convention $X_i^0 = 1 = e_{(0, \dots, 0)}$. Les $X_1^{i_1} \cdots X_n^{i_n}, (i_1, \dots, i_n) \in \mathbb{N}^n$ forment donc une base du A -module libre $A[\mathbb{N}^n]$, et on écrit alors

$$A[\mathbb{N}^n] = A[X_1, \dots, X_n]$$

Définition C.1. L'algèbre $A[X_1, \dots, X_n] = A[\mathbb{N}^n]$ est l'algèbre des polynôme à n variables à coefficients dans A . Les éléments de $A[X_1, \dots, X_n]$ sont appelés les polynômes à coefficients dans A .

A s'identifie à un sous-anneau de $A[X_1, \dots, X_n]$ (avec $a = a1$), et donc si B est un sous-anneau de A , il s'identifie à un sous-anneau de $A[X_1, \dots, X_n]$, que l'on peut donc voir comme une B -algèbre.

La propriété universelle de $A[X_1, \dots, X_n]$ est la suivante.

Théorème C.2. Soient B une A -algèbre et $b_1, \dots, b_n \in B$ tels que $b_i b_j = b_j b_i$ pour tous i, j . Alors il existe une unique morphisme de A -algèbres

$$\varphi : A[X_1, \dots, X_n] \longrightarrow B$$

tel que $\varphi(X_i) = b_i, \forall i \in \{1, \dots, n\}$. Pour $P \in A[X_1, \dots, X_n]$, on note $P(b_1, \dots, b_n) = \varphi(P)$.

Preuve. On considère d'abord l'application $\mathbb{N}^n \longrightarrow B, (i_1, \dots, i_n) \longmapsto b_1^{i_1} \cdots b_n^{i_n}$, qui est multiplicative car les b_i commutent deux à deux. On applique ensuite la propriété universelle de l'algèbre du monoïde \mathbb{N}^n . \square

Corollaire C.3. Soient A et B des anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A[X_1, \dots, X_n] \longrightarrow B[X_1, \dots, X_n]$ tel que $\tilde{f}|_A = f$ et $\tilde{f}(X_i) = X_i$, pour tout i .

Preuve. On peut construire \tilde{f} directement, ou bien utiliser le résultat précédent en munissant $B[X_1, \dots, X_n]$ de la structure de A -algèbre induite par la composition $A \rightarrow B \hookrightarrow B[X_1, \dots, X_n]$. \square

Le résultat qui suit est très utile pour montrer des résultats par récurrence sur le nombre de variables.

Proposition C.4. Les A -algèbres $A[X_1, \dots, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes.

Preuve. Il existe un unique morphisme de A -algèbres $f : A[X_1, \dots, X_n] \longrightarrow A[X_1, \dots, X_{n-1}][X_n]$ tel que $f(X_i) = X_i$, pour tout i . On vérifie que f est un isomorphisme (par exemple en remarquant que f envoie une base de $A[X_1, \dots, X_n]$ sur une base de $A[X_1, \dots, X_{n-1}][X_n]$, ou encore en construisant un isomorphisme inverse). \square

IV Matrices à coefficients dans un anneau commutatif

Dans ce chapitre A est un anneau commutatif.

A Matrices

Soient $n, p \in \mathbb{N}^*$. On note $\mathcal{M}_{n,p}(A)$ l'ensemble des matrices $n \times p$ à coefficients dans A . C' est un A -module, pour les lois usuelles ($\forall (a_{ij}), (b_{ij}) \in \mathcal{M}_{n,p}(A)$)

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

$$a.(b_{ij}) = (ab_{ij})$$

Pour $(i, j) \in \{1, \dots, n\} \times \{1, \dots, p\}$, on note $E_{ij} \in \mathcal{M}_{n,p}(A)$ la matrice dont tous les coefficients sont nuls à l'exception de celui situé sur la i -ème ligne et la j -ème colonne, qui vaut 1. Toute matrice $M = (a_{ij}) \in \mathcal{M}_{n,p}(A)$ s'écrit de manière unique sous la forme $M = \sum_{i,j} a_{ij}E_{ij}$. Ainsi $\mathcal{M}_{n,p}(A)$ est un A -module libre de rang np .

Le produit usuel des matrices définit pour $n, p, q \in \mathbb{N}^*$, une application A -bilinéaire

$$\begin{aligned} \mathcal{M}_{n,p}(A) \times \mathcal{M}_{p,q}(A) &\longrightarrow \mathcal{M}_{n,q}(A) \\ (M = (a_{ik}), N = (b_{kj})) &\longmapsto MN = \left(\sum_{k=1}^p a_{ik}b_{kj} \right) \end{aligned}$$

Pour $i \in \{1, \dots, n\}, j, k \in \{1, \dots, p\}, l \in \{1, \dots, q\}$, on a

$$E_{ij}E_{kl} = \delta_{jk}E_{il},$$

et cette formule définit totalement, par bilinéarité, le produit des matrices.

Lorsque $n = p$, $\mathcal{M}_n(A) = \mathcal{M}_{n,n}(A)$ est une A -algèbre, dont la multiplication est le produit des matrices. La matrice identité (unité pour le produit des matrices) est notée I_n . C' est une algèbre non commutative si $n \geq 2$.

On pose

$$GL_n(A) = U(\mathcal{M}_n(A)) = \{M \in \mathcal{M}_n(A) \mid \exists M' \in \mathcal{M}_n(A) \text{ tq } MM' = I_n = M'M\}.$$

C' est un groupe pour la multiplication des matrices. Les matrices suivantes seront très utiles dans la suite.

Définition-Proposition A.1. Soit $a \in A$ et $i, j \in \{1, \dots, n\}$, avec $i \neq j$. La matrice

$$F_{ij}(a) := I_n + aE_{ij}$$

est inversible, d'inverse $F_{ij}(-a)$.

La vérification est immédiate.

B Centre et idéaux d'une algèbre de matrices

Dans ce paragraphe on se propose d'étudier quelques propriétés des algèbres de matrices : calcul de leur centre et description des idéaux (quand A est un corps).

Proposition B.1. On a $Z(\mathcal{M}_n(A)) = \{aI_n, a \in A\}$, d'où un isomorphisme d'anneaux $Z(\mathcal{M}_n(A)) \cong A$.

Le résultat est une conséquence immédiate du résultat plus précis suivant.

Proposition B.2. Soit $M \in \mathcal{M}_n(A)$. Les assertions suivantes sont équivalentes.

1. Il existe $a \in A$ tel que $M = aI_n$.
2. M commute avec les matrices $E_{ij}, \forall i \neq j$.
3. M commute avec les matrices $F_{ij}(1), \forall i \neq j$.

Preuve. Comme la matrice identité I_n commute avec toutes les matrices et $F_{ij}(1) = I_n + E_{ij}$, il est clair que (1) \Rightarrow (2) et que (2) \Leftrightarrow (3). Il reste à voir que (2) \Rightarrow (1). Soit $M = \sum_{k,l} a_{kl}E_{kl}$ vérifiant (2). Fixons $i \neq j$. On a $ME_{ij} = \sum_k a_{ki}E_{kj}$ et $E_{ij}M = \sum_l a_{jl}E_{il}$, d'où $a_{ii} = a_{jj}$, et si $k \neq i$ et $l \neq j$, $a_{ki} = 0 = a_{jl}$. Ceci est vrai pour tout $i \neq j$, d'où le résultat. \square

Proposition B.3. Supposons que $A = k$ est un corps. Alors les seuls idéaux bilatères de $\mathcal{M}_n(k)$ sont (0) et $\mathcal{M}_n(k)$.

Preuve. Soit $I \neq (0)$ un idéal de $\mathcal{M}_n(k)$. Supposons dans un premier temps qu'il existe i, j tels que $E_{ij} \in I$. Alors pour tous k, l , on a $E_{kl} = E_{ki}E_{ij}E_{jl} \in I$. Comme I est automatiquement un sous k -espace vectoriel, on en déduit que $I = \mathcal{M}_n(k)$.

Soit maintenant $M = \sum_{kl} a_{kl}E_{kl} \in I$ non nulle : il existe i, j tels que $a_{ij} \neq 0$. On a $E_{ii}ME_{jj} = a_{ij}E_{ij} \in I$, d'où $E_{ij} = a_{ij}^{-1}a_{ij}E_{ij} \in I$. On est ramené au cas précédent. \square

Exercice. Si $I \subset A$ est un idéal, on note $\mathcal{M}_n(I)$ les matrices à coefficients dans I . Vérifier que $\mathcal{M}_n(I)$ est un idéal de $\mathcal{M}_n(A)$, et que tout idéal de $\mathcal{M}_n(A)$ est de cette forme.

Par contre $\mathcal{M}_n(A)$ admet toujours des idéaux à gauche.

Proposition B.4. Pour $i \in \{1, \dots, n\}$, notons $J_i \subset \mathcal{M}_n(A)$ l'ensemble des matrices dont les termes sont nuls en dehors de la i -ème colonne. Alors J_i est un idéal à gauche de $\mathcal{M}_n(A)$. De plus, en tant que $\mathcal{M}_n(A)$ -module, on a $\mathcal{M}_n(A) = J_1 \oplus \dots \oplus J_n$.

Preuve. On a $J_i = \sum_{l=1}^n AE_{li}$, et la vérification est un calcul facile. \square

C Déterminant

Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$, on pose

$$\det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

C'est le **déterminant** de M . Ceci définit une application $\det : \mathcal{M}_n(A) \longrightarrow A$.

On se propose de montrer le résultat suivant.

Théorème C.1 (Cramer). Soit $M \in \mathcal{M}_n(A)$. Alors

$$M \in \mathrm{GL}_n(A) \iff \det(M) \in U(A).$$

Exercice. Montrer le résultat si $n = 2$.

Schéma de la preuve. On verra plus loin que pour $M, N \in \mathcal{M}_n(A)$, on a $\det(MN) = \det(M) \det(N)$. Puisque $\det(I_n) = 1$, on en déduit aisément que $M \in \mathrm{GL}_n(A) \Rightarrow \det(M) \in U(A)$. La réciproque sera démontrée plus loin, avec en plus une formule pour le calcul de l'inverse de M si $\det(M) \in U(A)$. \square

Notation-convention.

1. Soit E est un A -module libre de rang n et soit $\mathbf{e} = (e_1, \dots, e_n)$ une base de E . On a vu (Proposition C.3 du chapitre II) qu'il existe une unique forme n -linéaire alternée $\Delta : E^n \longrightarrow A$ telle que $\Delta(e_1, \dots, e_n) = 1$. Pour $(x_1, \dots, x_n) \in E^n$, avec $\forall i, x_i = \sum_j a_{ji} e_j$, on a

$$\Delta(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} = \det(M), \text{ avec } M = (a_{ij})$$

On notera $\det_{\mathbf{e}}(x_1, \dots, x_n)$ cet élément de A .

2. Une matrice $M \in \mathcal{M}_n(A)$ est notée (C_1, \dots, C_n) où C_1, \dots, C_n sont les colonnes de M . Ainsi le A -module libre $\mathcal{M}_n(A)$ de rang n^2 est vu comme le produit de n copies du A -module libre $\mathcal{M}_{n,1}(A)$ (de rang n et de base $\mathcal{E} = (E_{11}, \dots, E_{n1})$). Avec cette convention, $\det : \mathcal{M}_n(A) \longrightarrow A$ est une forme n -linéaire alternée, et $\det(M) = \det_{\mathcal{E}}(C_1, \dots, C_n)$.

Proposition C.2. Pour $M, N \in \mathcal{M}_n(A)$, on a

$$\det({}^t M) = \det(M) \quad \text{et} \quad \det(MN) = \det(M) \det(N)$$

Preuve. Ecrivons $M = (a_{ij})$. Pour $\sigma \in S_n$, on a

$$a_{\sigma(1)1} \cdots a_{\sigma(n)n} = a_{1\sigma^{-1}(1)} \cdots a_{n\sigma^{-1}(n)}$$

d'où

$$\det({}^t M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n} = \det(M)$$

car $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ pour tout $\sigma \in S_n$. Soient M_1, \dots, M_n les colonnes de M . Si $N = (b_{ij})$, alors MN est la matrice dont les colonnes sont C_1, \dots, C_n où $C_j = \sum_{l=1}^n b_{lj} M_l$. Alors on a

$$\det(MN) = \det_{\mathcal{E}}(C_1, \dots, C_n) = \left(\sum_{\sigma \in S_n} \varepsilon(\sigma) b_{\sigma(1)1} \cdots b_{\sigma(n)n} \right) \det_{\mathcal{E}}(M_1, \dots, M_n) = \det(N) \det(M)$$

ce qui donne le résultat. \square

Définition C.3. Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$. Pour $i, j \in \{1, \dots, n\}$, soit $M_{ij} \in \mathcal{M}_{n-1}(A)$ la matrice obtenue à partir de A en effaçant la ligne i et la colonne j . L'élément $(-1)^{i+j} \det(M_{ij})$ est appelé le **cofacteur** (i, j) de M . On note $\tilde{M} \in \mathcal{M}_n(A)$ la matrice dont les coefficients sont les cofacteurs de A .

Théorème C.4 (Développement d'un déterminant suivant les lignes ou les colonnes). Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$. Pour chaque $i \in \{1, \dots, n\}$, on a

$$\det(M) = \sum_{k=1}^n (-1)^{i+k} a_{ik} \det(M_{ik}) = \sum_{k=1}^n (-1)^{i+k} a_{ki} \det(M_{ki})$$

La première formule est le développement de $\det(M)$ suivant la ligne i , la deuxième formule est le développement de $\det(M)$ suivant la colonne i .

Preuve. Soit $\mathbf{e} = (e_1, \dots, e_n)$ la base canonique de A^n . Notons, pour $1 \leq i \leq n$, $v_i = \sum_{k=1}^n a_{ki} e_k$. On a $\det(M) = \det_{\mathbf{e}}(v_1, \dots, v_n)$. Pour $1 \leq k \leq n$, notons $\mathbf{f}_k = (e_k, e_1, \dots, e_{k-1}, e_{k+1}, \dots, e_n)$. Posons également, pour $1 \leq k, j \leq n$,

$$N_{kj} = \begin{pmatrix} 1 & a_{k1} & \dots & a_{k,j-1} & a_{k,j+1} & \dots & a_{k,n} \\ 0 & & & & & & \\ \vdots & & & M_{kj} & & & \\ 0 & & & & & & \end{pmatrix}$$

On a $\det(M_{kj}) = \det(N_{kj})$. D'autre part on a $\det(N_{kj}) = \det_{\mathbf{f}_k}(e_k, v_1, \dots, \widehat{v}_j, \dots, v_n)$. Posons

$$\begin{aligned} \alpha_{kj} &= \det_{\mathbf{e}}(v_1, \dots, v_{j-1}, e_k, v_{j+1}, \dots, v_n) \\ &= (-1)^{j-1} \det_{\mathbf{e}}(e_k, v_1, \dots, \widehat{v}_j, \dots, v_n) = (-1)^{j-1} (-1)^{k-1} \det_{\mathbf{f}_k}(e_k, v_1, \dots, \widehat{v}_j, \dots, v_n) \end{aligned}$$

La dernière identité est obtenue en utilisant le fait que pour $\sigma \in S_n$, si on note $\sigma \cdot \mathbf{e}$ la base $(e_{\sigma(1)}, \dots, e_{\sigma(n)})$, on a $\det_{\sigma \cdot \mathbf{e}}(v_1, \dots, v_n) = \varepsilon(\sigma) \det_{\mathbf{e}}(v_1, \dots, v_n)$. La multilinéarité du déterminant assure que

$$\det(M) = \det_{\mathbf{e}}(v_1, \dots, v_n) = \sum_{k=1}^n a_{kj} \alpha_{kj} = \sum_{k=1}^n a_{kj} (-1)^{k+j} \det(M_{kj})$$

Ceci donne la deuxième formule, et la première est obtenue par transposition (${}^t(M_{ik}) = ({}^tM)_{ki}$). \square

Théorème C.5 (Formule pour l'inverse d'une matrice). Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$. On a

$$M {}^t\tilde{M} = \det(M) I_n = {}^t\tilde{M} M$$

et M est inversible si et seulement si $\det(M) \in U(A)$.

Preuve. Soient $1 \leq l \neq j \leq n$. Soit $N = (a'_{ki})$ la matrice obtenue à partir de M en remplaçant la colonne j par la colonne l : $a'_{ki} = a_{ki}$ si $i \neq j$ et $a'_{kj} = a_{kl}$. Comme N a deux colonnes identiques on a $\det(N) = 0$. D'autre part pour tout k on a $\det(M_{kj}) = \det(N_{kj})$. Alors la formule précédente donne

$$0 = \det(N) = \sum_{k=1}^n a'_{kj} (-1)^{k+j} \det(N_{kj}) = \sum_{k=1}^n a_{kl} (-1)^{k+j} \det(M_{kj})$$

Ceci, combiné avec la formule précédente pour $\det(M)$, donne $\det(M) I_n = {}^t\tilde{M} M$. L'autre partie de la formule s'obtient par transposition. La dernière assertion est immédiate. \square

D Application aux endomorphismes d'un module libre

De même que pour les application linéaires entre espaces vectoriels, les applications linéaires entre modules libres sont déterminées par les matrices associées.

Définition D.1. Soient E et E' des A -modules libres de rangs respectifs n et p et de base respectives $\mathcal{B} = \{e_1, \dots, e_n\}$ et $\mathcal{B}' = \{e'_1, \dots, e'_p\}$. Soit $u \in \text{Hom}_A(E, E')$. **La matrice de u relativement aux bases \mathcal{B} et \mathcal{B}' est la matrice $M_{\mathcal{B}, \mathcal{B}'}(u) = (\alpha_{ji}) \in \mathcal{M}_{p,n}(A)$ définie par**

$$u(e_i) = \sum_{j=1}^p \alpha_{ji} e'_j, \forall i \in \{1, \dots, n\}$$

Lorsque $E = E'$ et $\mathcal{B} = \mathcal{B}'$, on note $M_{\mathcal{B}, \mathcal{B}}(u) = M_{\mathcal{B}}(u)$, c'est la matrice de u relativement à la base \mathcal{B} (ou dans la base \mathcal{B}).

Réciproquement, la donnée d'une matrice $M \in \mathcal{M}_{p,n}(A)$ détermine une unique application linéaire $E \rightarrow E'$.

Proposition D.2. Soient E et E' des A -modules libres de rangs respectifs n et p et de bases respectives \mathcal{B} et \mathcal{B}' . L'application

$$\begin{aligned} \text{Hom}_A(E, E') &\longrightarrow \mathcal{M}_{p,n}(A) \\ u &\longmapsto M_{\mathcal{B}, \mathcal{B}'}(u) \end{aligned}$$

est un isomorphisme A -linéaire.

Preuve. Exercice \square

Proposition D.3. Soient E, E' et E'' des A -modules libres de rangs respectifs n, p et r et de base respectives $\mathcal{B}, \mathcal{B}'$ et \mathcal{B}'' . Pour $u \in \text{Hom}_A(E, E')$ et $v \in \text{Hom}_A(E', E'')$, on a

$$M_{\mathcal{B}, \mathcal{B}''}(v \circ u) = M_{\mathcal{B}', \mathcal{B}''}(v) M_{\mathcal{B}, \mathcal{B}'}(u)$$

Preuve. Exercice \square

Corollaire D.4. Soient E et E' des A -modules libres de rangs respectifs n et p et de base respectives \mathcal{B} et \mathcal{B}' . Soit $u \in \text{Hom}_A(E, E')$. Alors u est un isomorphisme si et seulement si la matrice $M_{\mathcal{B}, \mathcal{B}'}(u)$ est inversible (et dans ce cas nécessairement $n = p$).

Corollaire D.5. Soit E un A -module libre de rang n et de base \mathcal{B} . L'application

$$\begin{aligned} \text{End}_A(E) &\longrightarrow \mathcal{M}_n(A) \\ u &\longmapsto M_{\mathcal{B}}(u) \end{aligned}$$

est un isomorphisme de A -algèbres. En particulier u est un isomorphisme si et seulement si $M_{\mathcal{B}}(u) \in \text{GL}_n(A)$. Cette application induit en particulier un isomorphisme de groupes $\text{Aut}_A(E) \cong \text{GL}_n(A)$.

Soit E un A -module libre de rang n et de bases \mathcal{B} et \mathcal{B}' . Soit $u \in \text{End}_A(M)$. On a

$$M_{\mathcal{B}}(u) = M_{\mathcal{B}',\mathcal{B}}(\text{id}_M)M_{\mathcal{B}'}(u)M_{\mathcal{B},\mathcal{B}'}(\text{id}_M) = M_{\mathcal{B},\mathcal{B}'}(\text{id}_M)^{-1}M_{\mathcal{B}'}(u)M_{\mathcal{B},\mathcal{B}'}(\text{id}_M)$$

Ainsi on a $\det(M_{\mathcal{B}}(u)) = \det(M_{\mathcal{B}'}(u))$. Ce calcul légitime la définition suivante.

Définition D.6. Soit E un A -module libre de rang fini et $u \in \text{End}_A(E)$. Le déterminant de u est le déterminant de la matrice de u (relativement à n'importe quelle base de E).

Théorème D.7. Soit E un A -module libre de rang fini et $u \in \text{End}_A(E)$. Les assertions suivantes sont équivalentes.

1. u est un isomorphisme.
2. u est surjectif.
3. $\det(u) \in U(A)$.

Preuve. Le théorème C.5 et les considérations précédentes assurent que (1) \iff (3) et on a bien sûr (1) \implies (2). Si u est surjectif, comme E est libre, il existe par le chapitre II une application linéaire $v : E \rightarrow E$ telle que $u \circ v = \text{id}_E$, d'où $\det(u) \in U(A)$. \square

Corollaire D.8. Si $A = K$ est un corps et E est un K -espace vectoriel de dimension finie, alors pour $u \in \text{End}_K(E)$, les assertions suivantes sont équivalentes.

1. u est un isomorphisme.
2. u est surjectif.
3. u est injectif.
4. $\det(u) \neq 0$.

Preuve. Il reste à voir que si u est injectif alors il est surjectif. Si u est injectif, alors $u(E) \subset E$ est un sous-espace de dimension égale à celle de E , et ainsi $E = u(E)$ (compléter une base de $u(E)$ en une base de E ...) \square

Théorème D.9. Supposons que A est un anneau intègre. Soit E un A -module libre de rang fini et $u \in \text{End}_A(E)$. Les assertions suivantes sont équivalentes.

1. u est injectif.
2. $\det(u) \neq 0$.

Preuve. Soit $(\mathcal{E}_1, \dots, \mathcal{E}_n)$ une base de E et soit $M = (a_{ij}) \in \mathcal{M}_n(A)$ la matrice de u dans cette base. Soit $K = \text{Fr}(A)$ le corps des fractions de A et soit $\tilde{u} : K^n \rightarrow K^n$ l'application K -linéaire dont la matrice dans la base canonique (e_1, \dots, e_n) est $M : \tilde{u}(e_i) = \sum_{j=1}^n a_{ji} \cdot e_j$ pour tout i . On a $\det(u) = \det(\tilde{u})$. Alors $\det(u) \neq 0$ si et seulement si \tilde{u} est un isomorphisme. Un élément $\sum_{i=1}^n a_i \cdot \mathcal{E}_i$ du noyau de u ($a_1, \dots, a_n \in A$) fournit un élément $\sum_{i=1}^n a_i \cdot e_i$ du noyau de \tilde{u} . Donc si $\det(u) \neq 0$, alors u est injectif.

Réciproquement si $\det(u) = 0 = \det(\tilde{u})$, soit $\sum_{i=1}^n \lambda_i \cdot e_i \in \text{Ker}(\tilde{u})$ ($\lambda_1, \dots, \lambda_n \in K$ non tous nuls). Soit $d \in A$ tel que $\forall i, d\lambda_i \in A$. Alors $\sum_{i=1}^n (d\lambda_i) \cdot \mathcal{E}_i \neq 0$ appartient au noyau de u , et u est non injectif. \square

Exemple D.10. Soit $u : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ l'application \mathbb{Z} -linéaire dont la matrice dans la base canonique est $\begin{pmatrix} 2 & 4 \\ 3 & 1 \end{pmatrix}$. Alors u est injective mais non surjective.

E Application : les entiers algébriques

Définition E.1. Soit $A \subset B$ une extension d'anneaux (commutatifs), c'est-à-dire que B est un anneau et A un sous-anneau $B : A \subset B$. On dit qu'un élément $x \in B$ est **entier sur** A s'il existe un polynôme unitaire $P \in A[X]$ tel que $P(x) = 0$. On note

$$\mathcal{O}_{B/A} = \{x \in B \mid x \text{ est entier sur } A\}$$

On se propose de montrer que $\mathcal{O}_{B/A}$ est un sous-anneau de B .

Lorsque A et B sont des corps, un élément entier sur A est exactement un élément algébrique sur A . Mais si A n'est pas un corps, la notion d'entier est plus restrictive : par exemple un élément de \mathbb{Q} est entier sur \mathbb{Z} si et seulement si il appartient à \mathbb{Z} . Plus généralement, on a le résultat suivant.

Proposition E.2. Soit A un anneau factoriel et soit $K = \text{Fr}(A)$ le corps des fractions de A . Alors $\mathcal{O}_{K/A} = A$.

Preuve. Soit $x \in K$ entier sur A . On peut écrire $x = \frac{p}{q}$ avec $(p, q) \in A \times A^*$ premiers entre eux. Il existe $n \in \mathbb{N}^*$ et $a_0, \dots, a_{n-1} \in A$ tels que

$$\frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0 = 0$$

ce qui donne en multipliant par q^n

$$p^n = -(a_{n-1}p^{n-1}q + \dots + a_1pq^{n-1} + a_0q^n)$$

et donc $q|p^n$, donc $q|p$ (lemme de Gauss), et donc $q \in U(A)$. Ainsi $x \in A$. \square

Théorème E.3. Soit $A \subset B$ une extension d'anneaux et soit $x \in B$. Les assertions suivantes sont équivalentes.

1. x est entier sur A .
2. $A[x]$ est un A -module de type fini.
3. Il existe un sous-anneau R de B contenant x , tel que $A \subset R \subset B$ et qui est de type fini comme A -module.

Preuve. (1) \Rightarrow (2) est laissé en exercice et (2) \Rightarrow (3) est évident. Montrons (3) \Rightarrow (1). Soient w_1, \dots, w_n une famille de générateurs de R comme A -module. Il existe des éléments $a_{ij}, 1 \leq i, j \leq n$, tels que $\forall i, R \ni xw_i = \sum_{j=1}^n a_{ij}w_j$, c'est-à-dire que

$$\forall i, \sum_{j=1}^n (\delta_{ij}x - a_{ij})w_j = 0$$

Posons $\lambda_{ij} = \delta_{ij}x - a_{ij}$ et considérons la matrices $M = (\lambda_{ij}) \in \mathcal{M}_n(R)$. Les relations précédentes donnent

$$M \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

La relation ${}^t\tilde{M}M = \det(M)I_n$ assure alors que $\det(M)w_i = 0, \forall i$. Mais w_1, \dots, w_n engendrent R comme A -module, donc il existe $b_1, \dots, b_n \in A$ tels que $1 = \sum_{i=1}^n b_i w_i$, et on en déduit que $\det(M) = 0$. Ainsi si $P = \det(\delta_{ij}X - a_{ij}) \in A[X]$, on a $P(x) = 0$ avec P unitaire : x est entier sur A . \square

Corollaire E.4. Soit $A \subset B$ une extension d'anneaux. Alors $\mathcal{O}_{B/A}$ est un sous-anneau de B .

Preuve. Pour $x, y \in \mathcal{O}_{B/A}$, il est clair que $A[x, y]$ est un A -module de type fini, et ainsi par le théorème précédent on a $A[x, y] \subset \mathcal{O}_{B/A}$ et donc $x - y, xy \in \mathcal{O}_{B/A}$. Enfin on a $A \subset \mathcal{O}_{B/A}$, donc $1 \in \mathcal{O}_{B/A}$, ce qui assure que $\mathcal{O}_{B/A}$ est un sous-anneau de B . \square

Définition E.5. Soit R un anneau. On dit qu'un élément $x \in R$ est un **entier algébrique** s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$. On note \mathcal{O}_R l'ensemble des entiers algébriques de R .

Soit R un anneau et soit ϕ l'unique morphisme d'anneaux de \mathbb{Z} dans R . Un élément $x \in R$ est entier algébrique et seulement s'il est entier sur $\phi(\mathbb{Z})$. Les résultats précédents donnent donc en particulier le résultat suivant.

Théorème E.6. Soit R un anneau (commutatif) et soit $x \in R$. Les assertions suivantes sont équivalentes.

1. x est entier algébrique.
2. $\mathbb{Z}[x]$ (le sous-anneau de R engendré par x) est un \mathbb{Z} -module de type fini.
3. Il existe un sous-anneau T de R contenant x , qui est de type fini comme \mathbb{Z} -module.

En particulier \mathcal{O}_R est un sous anneau de R .

Exemple E.7. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. On peut montrer que

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega] = \mathbb{Z} \oplus \omega\mathbb{Z}$$

où

$$\omega = \begin{cases} \sqrt{d} & \text{si } d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod{4} \end{cases}$$

F Opération sur les lignes et colonnes d'une matrice

Définition F.1. Etant donnée une matrice $M \in \mathcal{M}_{s,n}(A)$, on considère les opérations suivantes (dites **opérations élémentaires sur les lignes** de M) :

(L1) On ajoute à une ligne donnée un multiple (quelconque) d'une autre ligne de M .

(L2) On multiplie une ligne de M par un élément inversible de A .

(L3) On permute deux lignes de M .

Remarque F.2. Considérons les matrices inversibles suivantes :

1. Pour $i \neq j$ et $\lambda \in A$, on note $F_{ij}(\lambda) \in \mathcal{M}_{s,s}(A)$ est la matrice dont les coefficients diagonaux sont égaux à 1 et dont les autres coefficients sont nuls sauf celui de la ligne i et de la colonne j qui est égal à λ (voir le paragraphe A).
2. Pour $1 \leq i \leq s$ et $\alpha \in A$ avec α inversible, on note $E_i(\alpha) \in \mathcal{M}_{s,s}(A)$ la matrice diagonale dont les coefficients sont égaux à 1 sauf le i -ème qui est égal à α .

Alors (L1) revient à multiplier M à gauche par une matrice $F_{ij}(\lambda)$ et (L2) revient à multiplier M à gauche par une matrice $E_i(\alpha)$. Par ailleurs l'échange de deux lignes (L3) peut être obtenu à partir de 4 opérations (L1) ou (L2).

Définition F.3. On considère également les opérations suivantes (dites *opérations élémentaires sur les colonnes* de M) :

(C1) On ajoute à une colonne donnée un multiple (quelconque) d'une autre colonne de M .

(C2) On multiplie une colonne de M par un élément inversible de A .

(C3) On permute deux colonnes de M .

Remarque F.4. Ces opérations reviennent à multiplier M à droite par les matrices $F_{ij}(\lambda)$ et $E_i(\alpha)$ de taille $n \times n$ définies comme ci-dessus.

Définition-Proposition F.5. Soient M et N dans $\mathcal{M}_{s,n}(A)$. On dit que N est **équivalente** à M si N peut être obtenue à partir de M en lui appliquant une succession d'opérations élémentaires sur les lignes et les colonnes. On note $M \sim N$. Ceci définit une relation d'équivalence sur $\mathcal{M}_{s,n}(A)$.

Rappelons qu'un anneau euclidien est un anneau intègre A muni d'une application (stathme) $v : A \setminus \{0\} \rightarrow \mathbb{N}$ telle que pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que

$$a = bq + r, \text{ avec } r = 0 \text{ ou } v(r) < v(b)$$

Théorème F.6. Supposons que A est un anneau euclidien. Soit $R \in \mathcal{M}_{s,n}(A)$. Alors R est équivalente à une matrice de la forme $\text{diag}(d_1, \dots, d_t)$ avec $d_1 \mid d_2 \mid \dots \mid d_t$ dans A où $t = \min(s, n)$.

On peut démontrer que la suite (d_1, \dots, d_t) du théorème est unique à multiplication près par un élément inversible de A , ce qui justifie le terme de *facteurs invariants* pour la matrice.

Bien sûr, la notation $\text{diag}(d_1, \dots, d_t)$ désigne la matrice $s \times n$ dont le coefficient (i, j) vaut zéro pour $i \neq j$ et le coefficient (i, i) vaut d_i , pour $1 \leq i \leq t = \min(s, n)$

Preuve. Notons v le stathme de A . Cette démonstration permettra alors d'obtenir un algorithme pour passer de R à la matrice des facteurs invariants.

Notons $R = (a_{ij})_{1 \leq i \leq s, 1 \leq j \leq n}$.

1. Fixons i et j tels que $a_{ij} \neq 0$. Montrons que l'on peut remplacer tous les coefficients de la ligne i et de la colonne j (autres que a_{ij} lui-même) par les restes de leurs divisions euclidiennes par a_{ij} . Soit $k \neq j$. On a $a_{ik} = q_{ik}a_{ij} + r_{ik}$ avec $r_{ik} = 0$ ou $v(r_{ik}) < v(a_{ij})$. Si on soustrait q_{ik} fois la colonne j à la colonne k , et le coefficient de la ligne i et de la colonne k devient r_{ik} .
On raisonne de même pour transformer la colonne j .
2. Notons \mathcal{C} l'ensemble de tous les coefficients non nuls de toutes les matrices équivalentes à R . Soit $d_1 \in \mathcal{C}$ avec $v(d_1)$ minimal dans $\{v(x); x \in \mathcal{C}\}$, et supposons que d_1 soit l'un des coefficients de R (quitte à remplacer R par une matrice qui lui est équivalente). Quitte à permuter des lignes et/ou les colonnes de R , on peut supposer que d_1 est le coefficient de la première ligne et de la première colonne.
On sait que l'on peut remplacer tous les coefficients de la première ligne et de la première colonne autres que d_1 par les restes de leurs divisions euclidiennes par d_1 . Par minimalité de $v(d_1)$, tous ces restes sont nuls.
On s'est donc ramené à une matrice équivalente à R qui est de la forme $\begin{pmatrix} d_1 & 0 \\ 0 & R_1 \end{pmatrix}$ avec $R_1 \in \mathcal{M}_{s-1, n-1}(A)$.
De plus, d_1 divise tous les coefficients de R_1 . En effet, soit $2 \leq i \leq s$. Si on ajoute la première ligne de R à la i -ème, on a une matrice dont la i -ème ligne est $(d_1 \ a_{i2} \ \dots \ a_{in})$, et on sait d'après l'étape précédente que l'on peut remplacer tous les a_{ij} pour $j = 2, \dots, n$ par le reste de la division euclidienne de a_{ij} par d_1 . Par minimalité de $v(d_1)$ on en déduit que ces restes sont nuls, c'est-à-dire que $d_1 \mid a_{ij}$ pour tout $2 \leq j \leq n$.
3. On applique les deux étapes précédentes à R_1 . Cela ne changera pas la première ligne et la première colonne de R , et on en déduit que R est équivalente à une matrice de la forme $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & R_2 \end{pmatrix}$ avec $d_1 \mid d_2$ et d_2 divise tous les coefficients de R_2 .
4. Par récurrence, on obtient une matrice $\text{diag}(d_1, \dots, d_t)$ équivalente à R avec $d_1 \mid d_2 \mid \dots \mid d_t$ et $t = \min(s, n)$. \square

Remarque F.7. On obtient l'algorithme suivant :

Etape 1 Soit d_1 le coefficient non nul de R avec $v(d_1)$ minimal. Par permutation des lignes et des colonnes on place le coefficient non nul de R dont l'image par v est minimale en position $(1, 1)$.

Etape 2 On ajoute des multiples de la première colonne (*resp.* ligne) aux autres colonnes (*resp.* lignes) afin d'obtenir des coefficients nuls ou dont l'image par v est strictement inférieure à a_{11} sur la première ligne (*resp.* colonne).

Etape 3 On répète les étapes 1 et 2 jusqu'à obtenir une matrice de la forme $\begin{pmatrix} a_{11} & 0 \\ 0 & R_1 \end{pmatrix}$.

Etape 4 Si a_{11} divise tous les coefficients de R_1 on répète les étapes précédentes sur R_1 .

Etape 5 Si a_{11} ne divise pas a_{ij} avec $i \geq 2$ et $j \geq 2$, on ajoute la i ème ligne à la première et on reprend à l'étape 1.

Exemple F.8. $A = \mathbb{Q}[X]$ et $R = \begin{pmatrix} X & 0 & 0 \\ 0 & 1-X & 0 \\ 0 & 0 & (1-X)(1+X) \end{pmatrix}$. L'anneau A est bien euclidien avec $v = \text{deg}$.

Les opérations successives suivantes : $L_1 \rightarrow L_1 + L_2$; $C_2 \rightarrow C_2 + C_1$; $C_1 \leftrightarrow C_2$; $L_2 \rightarrow L_2 + (X-1)L_1$; $C_2 \rightarrow C_2 - XC_1$; $L_2 \rightarrow L_2 + L_3$; $C_3 \rightarrow C_3 + C_2$; $C_2 \leftrightarrow C_3$; $L_3 - (1+X)L_2$; $C_3 \rightarrow C_3 + XC_2$; $C_2 \rightarrow -C_2$ et $C_3 \rightarrow -C_3$ donnent la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & X(X-1)(X+1) \end{pmatrix}$

donc les facteurs invariants sont 1, $X-1$ et $X(X-1)(X+1)$.

On sait que $D = PRQ$ où P est donnée par les opérations sur les lignes et Q est donnée par les opérations sur les colonnes. Pour les trouver, on applique les opérations que l'on a faites sur les lignes de R à I_3 (pour P) et les opérations que l'on a faites sur les colonnes de R à I_3 (pour Q). On obtient

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1-X & -X & -1 \\ (X-1)(X+1) & X(X+1) & X \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} 1 & 1-X & (1-X)(1+X) \\ 1 & -X & -X(1+X) \\ 0 & 1 & X \end{pmatrix}.$$

Exemple F.9. $A = \mathbb{Z}$ et $R = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$. L'anneau \mathbb{Z} est bien euclidien avec $v = ||$.

La suite d'opérations sur les lignes et les colonnes $L_1 \leftrightarrow L_3$; $L_2 \rightarrow L_2 - 4L_1$; $L_3 \rightarrow L_3 - 7L_1$; $C_2 \rightarrow C_2 - 2C_1$; $C_3 \rightarrow C_3 - 3C_1$; $L_2 \rightarrow -L_2$; $L_3 \rightarrow L_3 + 2L_2$ et $C_3 \rightarrow C_3 - 2C_2$ donne $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. On sait que $D = PRQ$ avec P et Q obtenues comme dans l'exemple

précédent. En pratique, nous voulons souvent Q^{-1} plutôt que Q , et celle-ci est obtenue en effectuant, sur I_3 , les opérations inverses sur les colonnes et dans l'ordre inverse. On obtient

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 4 \\ 1 & -2 & 1 \end{pmatrix} \quad \text{et} \quad Q^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

G Applications aux groupes linéaires

Une première application directe des opérations élémentaires sur les lignes et colonnes est de fournir des générateurs du groupe linéaire $GL_n(A)$.

Théorème G.1. Si A est un anneau euclidien, le groupe $GL_n(A)$ est engendré par les matrices

$$\{F_{ij}(\lambda), 1 \leq i \neq j \leq n, \lambda \in A\} \cup \{E_i(\alpha), 1 \leq i \leq n, \alpha \in U(A)\}$$

Preuve. Notons $X = \{F_{ij}(\lambda), 1 \leq i \neq j \leq n, \lambda \in k\} \cup \{E_i(\alpha), 1 \leq i \leq n, \alpha \in U(A)\}$. Pour $M \in GL_n(A)$, les opérations élémentaires sur les lignes et les colonnes de M assurent l'existence de $P_1, \dots, P_m, Q_1, \dots, Q_r \in X$ et $d_1, \dots, d_n \in U(A)$ tels que

$$P_1 \cdots P_m M Q_1 \cdots Q_r = \text{diag}(d_1, \dots, d_n)$$

et puisque $\text{diag}(d_1, \dots, d_n) \in \langle X \rangle$, on a bien $M \in \langle X \rangle$. \square

Exemple G.2. Le groupe $GL_2(\mathbb{Z})$ est engendré par les 4 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

En fait, en utilisant les relations

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

on voit que $GL_2(\mathbb{Z})$ est engendré par les 3 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Le groupe $SL_n(A)$ est défini par

$$SL_n(A) = \{M \in \mathcal{M}_n(A) \mid \det(M) = 1\}$$

C'est un sous-groupe normal de $GL_n(A)$ car $\det : GL_n(A) \rightarrow U(A)$ est un morphisme de groupes.

Proposition G.3. On a un isomorphisme de groupes $GL_n(A) \cong SL_n(A) \rtimes U(A)$.

Preuve. Soit H le sous-groupe de $GL_n(A)$ formé par les matrices $E_1(a) = \text{diag}(a, 1, \dots, 1)$, $a \in U(A)$. On voit facilement que $H \cap SL_n(A) = \{1\}$, $GL_n(A) = HSL_n(A)$, et puisque $SL_n(A) \triangleleft GL_n(A)$, la caractérisation des produits semi-directs assure que $GL_n(A) \cong SL_n(A) \rtimes H$, et on a le résultat car $H \cong U(A)$. \square

Théorème G.4. Si A est un anneau euclidien, le groupe $SL_n(A)$ est engendré par les matrices

$$\{E_{ij}(\lambda), 1 \leq i \neq j \leq n, \lambda \in A\}$$

Preuve. Les matrices en question sont bien sûr dans $SL_n(A)$. Deux matrices $M, N \in SL_n(A)$ sont dites fortement équivalentes si elles peuvent être obtenues l'une à partir de l'autre seulement à partir des opérations (L1) et (C1). Il s'agit donc de montrer qu'une matrice quelconque de $SL_n(A)$ est fortement équivalente à la matrice identité. Les opérations d'échange (L3) et (C3) ne sont pas autorisées en général. Néanmoins on peut échanger deux colonnes C_i et C_j au signe près, via la suite d'opérations (C1) suivante :

$$(C_i, C_j) \rightarrow (C_i + C_j, C_j) \rightarrow (C_i + C_j, -C_i) \rightarrow (C_j, -C_i)$$

Bien sûr on peut faire la même chose pour les lignes.

En reprenant point par point la preuve du théorème F.6, on voit alors qu'une matrice de $SL_n(A)$ est fortement équivalente à une matrice du type $\text{diag}(d_1, \dots, d_n)$ avec $d_1 \cdots d_n = 1$. En effet l'étape 1 n'utilise que les opérations (L1)-(C1), alors que dans l'étape 2, on peut utiliser la remarque précédente sur l'échange au signe près des lignes et colonnes (dans un anneau euclidien A on peut toujours remplacer le stathme v par un stathme v' tel que $v'(ua) = v'(a)$, $\forall u \in U(A)$, en posant $v'(a) = \min\{v(ua), u \in U(A)\}$). Finalement on voit sans difficulté qu'une matrice de $SL_n(A)$ est fortement équivalente à I_n . \square

Exemple G.5. Le groupe $SL_2(\mathbb{Z})$ est engendré par les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

V Modules de type fini sur un anneau principal

L'existence d'une base pour un espace vectoriel s'interprète comme un théorème de structure : Si M est un K -espace vectoriel (K un corps), il existe un ensemble I tel que $M \cong K^{(I)}$. On généralise ce résultat aux modules de type fini sur un anneau principal. On appliquera ensuite le théorème de structure à la réduction des endomorphismes, pour montrer en particulier le fait que toute matrice à coefficients dans un corps algébriquement clos est similaire à une matrice en forme canonique de Jordan.

A Les théorèmes de structures : énoncé

Théorème A.1 (de structure, version facteurs invariants). Soient A un anneau principal et M un A -module de type fini.

1. On a un isomorphisme de A -modules

$$M \cong A^n \oplus A/(a_1) \oplus \cdots \oplus A/(a_r)$$

pour des entiers $r, n \geq 0$ et des éléments non inversibles $a_1, \dots, a_r \in A^*$ tels que $a_1 | a_2 | \cdots | a_r$.

2. La donnée précédente (n, a_1, \dots, a_r) détermine uniquement le module M , à multiplication près des a_i par des inversibles. Les éléments a_1, \dots, a_r sont appelés **les facteurs invariants de M** .

Théorème A.2 (de structure, version diviseurs élémentaires). Soient A un anneau principal et M un A -module de type fini.

1. On a un isomorphisme de A -modules

$$M \cong A^n \oplus A/(p_1^{m_1}) \oplus \cdots \oplus A/(p_s^{m_s})$$

pour $n, s \in \mathbb{N}$, et p_1, \dots, p_s des irréductibles de A (non nécessairement deux à deux distincts).

2. La donnée précédente $(n, p_1^{m_1}, \dots, p_s^{m_s})$ détermine uniquement le module M , à multiplication par des inversibles près pour les irréductibles, et à l'ordre près. Les éléments $p_1^{m_1}, \dots, p_s^{m_s}$ sont appelés **les diviseurs élémentaires de M** .

Corollaire A.3. Un groupe abélien fini est isomorphe à un produit de groupes cycliques

Preuve. Si M est groupe abélien fini, c'est en particulier un \mathbb{Z} -module de type fini. Le n du théorème est nul car M est fini, d'où le résultat. \square

B Le théorème de la base adaptée

Les théorèmes de structures seront des conséquences du théorème suivant.

Théorème B.1 (de la base adaptée). Soient A un anneau principal, M un A -module libre de rang fini, et $N \subset M$ un sous-module. Il existe une base $\{e_1, \dots, e_n\}$ de M , un entier $p \leq n$ et des éléments $a_1, \dots, a_p \in A$ tels que $\{a_1.e_1, \dots, a_p.e_p\}$ soit une base de N et $a_1|a_2|\dots|a_p$.

En particulier tout sous-module d'un module d'un module libre de rang fini est libre si A est principal (on avait vu que cela n'est pas vrai en général).

Le but du paragraphe est de démontrer ce résultat. On commence par énoncer un lemme élémentaire, qui sera utilisé librement dans la suite. La preuve est laissée en exercice.

Lemme B.2. Soient A un anneau intègre et M un A -module libre. Soit $x \in M \setminus \{0\}$. Alors $Ax \subset M$ est un A -module libre de rang 1.

Tout d'abord, on a un résultat moins précis que le théorème de la base adaptée.

Théorème B.3. Soient A un anneau principal et M un A -module libre de rang n . Alors tout sous-module de M est libre de rang $\leq n$.

Preuve. Soit E un sous-module de M . On peut supposer E et M non nuls. Soit $\{x_1, \dots, x_n\}$ une base de M . et soit $f : M \rightarrow A$ l'unique application linéaire telle que $f(x_i) = \delta_{i1}$. Il existe $a \in A$ tel que $f(E) = Aa$, car A est principal. On démontre le résultat par récurrence sur n .

\rightsquigarrow Supposons $n = 1$. Alors f est un isomorphisme et f induit un isomorphisme $E \cong Aa$ avec $a \neq 0$, qui est donc libre de rang 1.

\rightsquigarrow Supposons $n \geq 2$ et le résultat montré pour les modules libres de rang $< n$. Si $a = 0$, on a $E \subset \text{Ker}(f) = Ax_2 + \dots + Ax_n$ qui est un module libre de rang $n - 1$, et donc l'hypothèse de récurrence donne le résultat. Supposons donc $a \neq 0$, c'est-à-dire $E \not\subset \text{Ker}(f)$. Soit $Q = E \cap \text{Ker}(f)$, par hypothèse de récurrence c'est un module libre de rang $\leq n - 1$, il admet donc une base e_2, \dots, e_q , avec $2 \leq q \leq n$. Soit $e_1 \in E \setminus \{0\}$ tel que $f(e_1) = a$ ($f(E) = Aa$). Pour $x \in E$, on a $f(x) = ba = f(be_1)$, donc $x - be_1 \in \text{Ker}(f) \cap E = Q$, donc

$$E = Q + Ae_1 = Ae_1 + Ae_2 + \dots + Ae_q$$

Il reste donc à voir que la famille $\{e_1, \dots, e_q\}$ est libre. Soient $c_1, \dots, c_q \in A$ tels que $c_1e_1 + \dots + c_qe_q = 0$. Alors on a

$$-c_1a = f(-c_1.e_1) = f(c_2e_2 + \dots + c_qe_q) = 0$$

d'où $c_1 = 0$, et l'indépendance linéaire de e_2, \dots, e_q permet de conclure. \square

Le résultat suivant ne sera pas utilisé dans la suite. La preuve est laissée en exercice.

Corollaire B.4. Si M est un A -module de type fini sur un anneau principal A , alors tout sous-module de M est de type fini.

Preuve du théorème de la base adaptée. La preuve que nous allons donner utilise les résultats sur les opérations élémentaires sur les matrices, où nous avons utilisé l'hypothèse que A est euclidien. On

consultera l'appendice pour une preuve indépendante des opérations élémentaires, et donc valable pour un anneau principal quelconque, mais un peu plus difficile.

Soit N un sous-module du A -module libre A^n . On sait par le théorème précédent que le sous-module N de A^n est libre de rang fini, et nous voulons en fait montrer que l'on peut choisir une base de N particulière.

Soit $\mathcal{B} = \{e_1, \dots, e_n\}$ une base de A^n et soit $\mathcal{G} = \{x_1, \dots, x_s\}$ un système générateur de N . Pour tout $1 \leq i \leq s$ on peut écrire $x_i = \sum_{j=1}^n a_{ij}e_j$ avec $a_{ij} \in A$ de manière unique.

Alors N est entièrement déterminé par le couple (\mathcal{B}, R) où \mathcal{B} est une base de A^n et R est la matrice $R = (a_{ij})_{1 \leq i \leq s, 1 \leq j \leq n}$.

Les opérations élémentaires sur les lignes et colonnes de R fournissent des matrices $P \in \text{GL}_s(A)$, $Q \in \text{GL}_n(A)$ telles que

$$PRQ = \text{diag}(d_1, \dots, d_t)$$

avec $d_1 \mid \dots \mid d_t$ dans A et $t = \min(s, n)$. Posons

$$e'_j = \sum_{k=1}^n (Q^{-1})_{jk}e_k, \quad \forall j \in \{1, \dots, n\}$$

$$x'_i = \sum_{l=1}^s P_{il}x_l, \quad \forall i \in \{1, \dots, s\}$$

Les matrices P et Q étant inversibles, il est clair que $\{e'_1, \dots, e'_n\}$ est une nouvelle base de A^n et que $\{x'_1, \dots, x'_s\}$ est une nouvelle partie génératrice de N . On a, pour $1 \leq i \leq s$,

$$x'_i = \sum_{l=1}^s P_{il}x_l = \sum_{l=1}^s \sum_{k=1}^n P_{il}a_{lk}e_k = \sum_{l=1}^s \sum_{k=1}^n \sum_{j=1}^n P_{il}a_{lk}Q_{kj}e'_j = d_i e'_i$$

(avec la convention $d_i = 0$ si $i > n$). Soit r le nombre de d_i non nuls : $r \leq t \leq n$. Dans cette nouvelle base de A^n , les générateurs de N sont donnés par $x'_i = d_i e'_i$. Donc $N = \langle d_1 e'_1, \dots, d_r e'_r \rangle$ (puisque les autres générateurs sont nuls). Enfin, on voit facilement que $\{d_1 e'_1, \dots, d_r e'_r\}$ est une famille libre (A est intègre et les d_i sont non nuls pour $1 \leq i \leq r$) et donc une base de N , qui est donc libre de rang $r \leq n$. \square

Remarque B.5. La démonstration précédente fournit non seulement l'existence de la base adaptée, mais aussi un moyen de la construire (quand A est euclidien donc). On reprend les données précédentes :

N est un sous-module du A -module libre A^n , $\mathcal{B} = \{e_1, \dots, e_n\}$ est une base de A^n , $\mathcal{G} = \{x_1, \dots, x_s\}$ est un système générateur de N avec $x_i = \sum_{j=1}^n a_{ij}e_j$, $R = (a_{ij}) \in \mathcal{M}_{s,n}(A)$.

Les opérations sur les colonnes de R fournissent la base adaptée. Plus précisément, si $P \in \text{GL}_s(A)$, $Q \in \text{GL}_n(A)$ sont les matrices telles que

$$PRQ = \text{diag}(d_1, \dots, d_t)$$

avec $d_1 \mid \dots \mid d_t$, la matrice Q est obtenue en appliquant les mêmes opérations sur les colonnes à la matrice identité I_n . La base adaptée $\{e'_1, \dots, e'_n\}$ est donnée par

$$e'_j = \sum_{k=1}^n (Q^{-1})_{jk}e_k, \quad \forall j \in \{1, \dots, n\}$$

et pour trouver Q^{-1} , il suffit d'appliquer en sens inverse les opérations inverses sur les colonnes à la matrice I_n . Les coordonnées de la nouvelle base dans l'ancienne sont données par les lignes de la matrice obtenue.

Exemple B.6. Soit M le groupe abélien libre \mathbb{Z}^3 de base $\{f_1, f_2, f_3\}$ et soit N le sous-module engendré par g_1, g_2 et g_3 avec $g_1 = -4f_1 - 6f_2 + 7f_3, g_2 = 2f_1 + 2f_2 + 4f_3, g_3 = 6f_1 + 6f_2 + 15f_3$. Pour trouver une base adaptée, on étudie la matrice

$$R = \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix}$$

Grâce aux opérations élémentaires sur les lignes et les colonnes suivantes : $L_1 \leftrightarrow L_2; L_2 \rightarrow L_2 + 2L_1; L_3 \rightarrow L_3 - 3L_1; C_2 \rightarrow C_2 - C_1; C_3 \rightarrow C_3 - 2C_1; L_1 \rightarrow L_1 + L_3; C_3 \rightarrow C_3 - C_1; C_3 \leftrightarrow C_1; C_3 \rightarrow C_3 - 2C_1; L_2 \rightarrow L_2 - 15L_1; L_3 \rightarrow L_3 - 3L_1; L_2 \rightarrow -L_2; C_3 \rightarrow C_3 - 15C_2; L_3 \rightarrow -L_3$ (par exemple), on obtient $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$. Il existe donc une base $\tilde{\mathcal{B}} = \{\tilde{e}_1, \tilde{e}_2, \tilde{e}_3\}$

de M telle que $\{\tilde{e}_1, 2\tilde{e}_2, 6\tilde{e}_3\}$ soit une base de N (et donc N est libre de rang 3).

Pour trouver la base $\tilde{\mathcal{B}}$, on applique en sens inverse les opérations inverses sur les colonnes à la matrice I_3 , pour obtenir la matrice $Q^{-1} = \begin{pmatrix} 2 & 2 & 7 \\ 15 & 16 & 45 \\ 1 & 1 & 3 \end{pmatrix}$, et donc $\tilde{e}_1 = 2f_1 + 2f_2 + 7f_3, \tilde{e}_2 = 15f_1 + 16f_2 + 45f_3, \tilde{e}_3 = f_1 + f_2 + 3f_3$.

C Structure des modules de type fini

Le premier résultat est une conséquence directe du théorème de la base adaptée.

Corollaire C.1. Soient A un anneau principal et M un A -module de type fini. Alors M est isomorphe comme A -module à $\bigoplus_{i=1}^n (A/(a_i))$ où les (a_i) sont des idéaux de A tels que $(a_i) \supset (a_{i+1})$.

Preuve. Puisque M est de type fini, on sait que c'est un quotient d'un module libre de type fini A^n . On a donc un morphisme surjectif $\varphi : A^n \twoheadrightarrow M$.

$\text{Ker } \varphi$ est un sous-module de A^n , donc d'après le théorème de la base adaptée, il existe une base $\{e_1, \dots, e_n\}$ de A^n et une base $\{a_1 e_1, \dots, a_q e_q\}$ de $\text{Ker } \varphi$ avec $a_1 \mid a_2 \mid \dots \mid a_q$. On pose $a_i = 0$ pour $q \leq i \leq n$. L'application A -linéaire surjective

$$\begin{aligned} A^n &\longrightarrow A/(a_1) \oplus \dots \oplus A/(a_n) \\ \sum_{i=1}^n b_i \cdot e_i &\longmapsto (\bar{b}_1, \dots, \bar{b}_n) \end{aligned}$$

a alors $\text{Ker}(\varphi)$ pour noyau, et donc $M \cong A^n / \text{Ker}(\varphi) \cong \bigoplus_{i=1}^n (A/(a_i))$. □

Exemple C.2. Soit G est le quotient du groupe abélien libre \mathbb{Z}^3 de base $\{f_1, f_2, f_3\}$ par le sous-module N engendré par g_1, g_2 et g_3 avec $g_1 = -4f_1 - 6f_2 + 7f_3, g_2 = 2f_1 + 2f_2 + 4f_3, g_3 = 6f_1 + 6f_2 + 15f_3$.

On veut écrire G comme une somme directe de groupes monogènes.

On a vu qu'il existe une base $\tilde{\mathcal{B}} = \{\tilde{e}_1, \tilde{e}_2, \tilde{e}_3\}$ de M telle que $\{\tilde{e}_1, 2\tilde{e}_2, 6\tilde{e}_3\}$ soit une base de N . Donc

$$G = \mathbb{Z}^3 / N \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Corollaire C.3. Soit M un A -module de type fini. Alors il existe $r \in \mathbb{N}$, $q \in \mathbb{N}$ et a_1, \dots, a_q dans A non nuls et non inversibles vérifiant $a_1 \mid \dots \mid a_q$ tels que $M \cong A^r \oplus A/(a_1) \oplus \dots \oplus A/(a_q)$.

Preuve. On applique le Corollaire C.1. Soit r le nombre de a_i qui sont nuls, donc $(a_n) = \dots = (a_{n-r+1}) = \{0\}$ et donc pour $n - r < i \leq n$ on a $A/(a_i) = A$. De plus, si a_i est inversible, $(a_i) = A$ donc $A/(a_i) = \{0\}$ et on peut donc l'ignorer dans la décomposition. Quitte à renuméroter les a_i on suppose donc que a_1 (et donc tous les a_i non nuls, soit jusqu'à a_q) n'est pas inversible. Donc $M \cong \bigoplus_{i=1}^q A/(a_i) \oplus A^r$. \square

Corollaire C.4. Avec les notations du corollaire C.3, le sous module de torsion de M est $T(M) \cong A/(a_1) \oplus \dots \oplus A/(a_q)$.

Preuve. D'après le corollaire C.3, on a

$$T(M) \cong T(A^r) \oplus T(A/(a_1)) \oplus \dots \oplus T(A/(a_q)) = A/(a_1) \oplus \dots \oplus A/(a_q)$$

car A intègre. \square

Corollaire C.5. Soit M un A -module de type fini. Si M est sans torsion, alors M est libre.

On va maintenant montrer le théorème de structure en version diviseurs élémentaires, grâce à la version suivante du théorème chinois.

Lemme C.6. Soit $M = Ax$ un A -module monogène et soit $\text{Ann}_A(x) = (d)$ (on rappelle que $\text{Ann}_A(x) = \{a \in A \mid a.x = 0\}$).

(i) M est isomorphe comme A -module à $A/(d)$.

(ii) Si $d = pq$ et p, q premiers entre eux dans A , alors $M = Ay \oplus Az$ avec $y = qx, z = px$, $\text{Ann}_A(y) = (p)$, $\text{Ann}_A(z) = (q)$.

Preuve. (i) On applique le théorème d'isomorphisme au morphisme de A -modules $\varphi : A \rightarrow M$, $a \mapsto a.x$.

(ii) Il est clair que $p \in \text{Ann}_A(y)$ puisque $py = pqx = dx = 0$ donc $(p) \subset \text{Ann}_A(y)$. Soit maintenant $c \in \text{Ann}_A(y)$. On a donc $0 = cy = cqx$ donc $cq \in \text{Ann}_A(x) = (pq)$ donc $cq = pqr$ avec $r \in A$. Donc $c = pr \in (p)$ et donc $\text{Ann}_A(y) = (p)$. De même $\text{Ann}_A(z) = (q)$.

Puisque A est principal on sait qu'il existe $u, v \in A$ tels que $1 = up + vq$. Donc $x = upx + vqx = uz + vy \in Az + Ay$. Donc $Ax = Ay + Az$.

Soit maintenant $t \in Ay \cap Az$. Alors $pt = 0$ puisque $t \in Ay$ et $p \in \text{Ann}_A(y)$, et $qt = 0$ de même. Donc $t = upt + vqt = 0$. Donc $Ay \cap Az = \{0\}$ et donc $M = Ay \oplus Az$. \square

Corollaire C.7. Soit M un A -module de type fini. Alors $M \cong A^s \oplus (\bigoplus A/(p^{n_r}))$ où p parcourt les éléments irréductibles de A et où les n_r sont des entiers positifs presque tous nuls. Les p^{n_r} sont appelés les **diviseurs élémentaires** de M .

Preuve. On sait que $M \cong \bigoplus_{i=1}^n A/(a_i)$. On factorise chaque $a_i = u \prod p^{n_{p,i}}$ avec u inversible et p irréductible. On décompose ensuite à l'aide du lemme C.6. \square

On étudie maintenant l'unicité dans les théorèmes de structure. Le lemme suivant est l'outil technique clé pour la preuve.

Lemme C.8. - Soit M un A -module et soit p un élément irréductible de A . Pour $n \in \mathbb{N}$, on considère le A -module $p^n M / p^{n+1} M$.

1. La structure de A -module sur M induit une structure de $A/(p)$ -module sur $p^n M / p^{n+1} M$, et donc de $A/(p)$ -espace vectoriel sur $p^n M / p^{n+1} M$.
2. Si M et N sont des A -modules isomorphes, alors les $A/(p)$ -espaces vectoriels $p^n M / p^{n+1} M$ et $p^n N / p^{n+1} N$ sont isomorphes.
3. Si $M = M_1 \oplus \dots \oplus M_r$, alors $p^n M / p^{n+1} M \cong p^n M_1 / p^{n+1} M_1 \oplus \dots \oplus p^n M_r / p^{n+1} M_r$.
4. Si $M = A/(d)$ pour $d \in A$, alors $\dim_{A/(p)}(p^n M / p^{n+1} M) = 1$ si p^{n+1} divise d et $\dim_{A/(p)}(p^n M / p^{n+1} M) = 0$ sinon.

Preuve. Soient $a, b \in A, x, y \in M$. Le calcul

$$(ap^n).x - (bp^n).y = a.(p^n.x - p^n.y) + (a - b).(p^n.y)$$

montre que l'on a une application bien définie

$$\begin{aligned} A/(p) \times p^n M / p^{n+1} M &\longrightarrow p^n M / p^{n+1} M \\ (\bar{a}, \widetilde{p^n.x}) &\longmapsto \widetilde{(ap^n).x} \end{aligned}$$

qui munit $p^n M / p^{n+1} M$ d'une structure de $A/(p)$ -module, et $A/(p)$ est un corps car A est principal.

Les points 2 et 3 sont laissés en exercice. Pour le point 4, soit $n \in \mathbb{N}$. Pour tout $x \in M$ la structure de $A/(p)$ -module sur $p^n M / p^{n+1} M$ donne une application $A/(p)$ -linéaire

$$\begin{aligned} \varphi_x : A/(p) &\longrightarrow p^n M / p^{n+1} M \\ \bar{a} &\longmapsto \widetilde{(p^n a).x} \end{aligned}$$

Comme $M = A/(d)$, si on prend x la classe de 1 dans $A/(d)$, on a $M = Ax$ et alors φ_x est surjective. Pour $a \in A$, on a $\bar{a} \in \text{Ker}(\varphi_x)$ si et seulement si il existe $b \in A$ tel que $p^n a - p^{n+1} b \in \text{Ann}_A(x) = (d)$, ce qui est encore équivalent à $p^n a \in (p^{n+1}, d)$.

Si p^{n+1} divise d , alors $(p^{n+1}) = (p^{n+1}, d)$ et on obtient facilement que $\bar{a} \in \text{Ker}(\varphi_x) \iff a \in (p)$, donc φ_x est injectif et est un isomorphisme. Sinon, p étant irréductible, le p.g.c.d. de p^{n+1} et d est de la forme p^r avec $r \in \mathbb{N}, r \leq n$, de sorte que $ap^n \in (p^r) = (p^{n+1}, d)$ pour tout $a \in A$. Ainsi φ_x est nul, et étant surjectif, on a $p^n M / p^{n+1} M = (0)$. \square

Théorème C.9 (Unicité des facteurs invariants). Supposons que

$$A^m \oplus A/(a_1) \oplus \dots \oplus A/(a_r) \cong A^n \oplus A/(b_1) \oplus \dots \oplus A/(b_s)$$

pour des entiers $m, r, n, s \geq 0$ et des éléments non inversibles $a_1, \dots, a_r, b_1, \dots, b_s \in A^*$ tels que $a_1 | a_2 | \dots | a_r$ et $b_1 | b_2 | \dots | b_s$. Alors $m = n, r = s$, et pour $1 \leq i \leq r, (a_i) = (b_i)$.

Preuve. Un isomorphisme de A -modules $M \cong N$ induit des isomorphismes $M/T(M) \cong N/T(N)$ et $T(M) \cong T(N)$. Donc l'isomorphisme du théorème induit des isomorphismes

$$A^m \cong A^n \quad \text{et} \quad A/(a_1) \oplus \dots \oplus A/(a_r) \cong A/(b_1) \oplus \dots \oplus A/(b_s)$$

Donc $m = n$ par l'unicité du cardinal d'une base d'un module libre (A est commutatif).

Si $r = 0$, M est libre, et $s = 0$ aussi. On peut donc supposer que $r, s > 0$, et sans perte de généralité que $r \leq s$.

Pour $1 \leq i \leq r$, on pose $M_i = A/(a_i)$. En outre, posons $M = \bigoplus_{i=1}^r M_i$. Soient $p \in A$ irréductible et $l \in \mathbb{N}$. Le lemme C.8 assure que l'on a un isomorphisme de $A/(p)$ -espaces vectoriels :

$$p^l M / p^{l+1} M \cong \bigoplus_{i=1}^r p^l M_i / p^{l+1} M_i.$$

et que le $A/(p)$ -espace vectoriel $p^l M / p^{l+1} M$ est isomorphe au $A/(p)$ -espace vectoriel $(A/(p))^t$ où t est le cardinal de l'ensemble $\{i \in \{1, \dots, r\}; p^{l+1} | a_i\}$.

Soit $i \in \{1, \dots, r\}$. Puisque $a_1 \mid \dots \mid a_i \mid \dots \mid a_r$, ce qui précède montre donc que, pour tout irréductible p dans A et tout $l \in \mathbb{N}$,

$$p^{l+1} | a_i \iff \dim_{A/(p)} p^l M / p^{l+1} M \geq r + 1 - i.$$

Si $r > s$, posons $b'_i = 1$ pour $1 \leq i \leq r - s$ et $b'_i = b_{i-r+s}$ pour $r - s + 1 \leq i \leq r$. On a

$$M \cong A/(b_1) \oplus \dots \oplus A/(b_s) \cong A/(b'_1) \oplus \dots \oplus A/(b'_r)$$

Bien sûr, ce qui précède s'applique : pour tout irréductible p dans A , tout $l \in \mathbb{N}$ et tout $i \in \{1, \dots, r\}$, on a

$$p^{l+1} | b'_i \iff \dim_{A/(p)} p^l M / p^{l+1} M \geq r + 1 - i.$$

Finalement, on a montré que, pour tout irréductible p dans A et tout $l \in \mathbb{N}$,

$$p^{l+1} | a_i \iff p^{l+1} | b'_i.$$

Pour $i = 1$, on a $b'_1 = 1$ alors que a_1 n'est pas inversible, et est donc divisé par un irréductible : contradiction. Donc $r = s$, et l'argument précédent s'applique, $\forall i, \forall l \in \mathbb{N}, p^{l+1} | a_i \iff p^{l+1} | b_i$. En écrivant les décompositions de a_i et b_i en produit de facteurs irréductibles, on en déduit que $(a_i) = (b_i)$. \square

Théorème C.10 (Unicité des diviseurs élémentaires). Si M est un A -module de type fini avec

$$M \cong A^s \oplus (\bigoplus_{i \in I} A/(p_i^{r_i})) \cong A^{s'} \oplus (\bigoplus_{i \in I'} A/((p'_i)^{r'_i}))$$

où $s, s' \in \mathbb{N}$, I, I' sont des ensembles finis, les p_i et les p'_i sont des irréductibles de A et les $r_i, r'_i \in \mathbb{N}^*$, alors $s = s'$ et il existe une bijection $\tau : I \rightarrow I'$ telle que $\forall i \in I$, on a $p_i \sim p'_{\tau(i)}$ et $r_i = r'_{\tau(i)}$.

Preuve. Comme dans le début de la preuve du théorème précédent, l'isomorphisme du théorème induit des isomorphismes

$$A^s \cong A^{s'} \text{ et } \bigoplus_{i \in I} A/(p_i^{r_i}) \cong \bigoplus_{i \in I'} A/((p'_i)^{r'_i})$$

et $s = s'$ par l'unicité du cardinal d'une base d'un module libre (A est commutatif). Pour $p \in A$ irréductible et $n \in \mathbb{N}^*$, soit $f(p, n)$ le nombre d'indices $i \in I$ tels que $p_i \sim p$ et $r_i = n$ et soit $f'(p, n)$ est le nombre d'indices $i \in I'$ tels que $p'_i \sim p$ et $r'_i = n$. Il s'agit de montrer que $f(p, n) = f'(p, n)$ pour tout p et tout n .

Si on pose $E = \bigoplus_{i \in I} A/(p_i^{r_i})$, le lemme C.8 assure pour tout irréductible p de A et tout $n \in \mathbb{N}^*$, on a $\dim_{A/(p)}(p^{n-1}E/p^nE) = d(p, n)$, où $d(p, n)$ est le nombre d'indices $i \in I$ tels que $p_i \sim p$ et $r_i \geq n$. En définissant de même $d'(p, n)$ comme le nombre d'indices $i' \in I'$ tels que $p'_i \sim p$ et $r'_i \geq n$, on obtient

$d(p, n) = d'(p, n)$. Finalement on a $f(p, n) = d(p, n) - d(p, n + 1) = d'(p, n) - d'(p, n + 1) = f'(p, n)$, ce qui donne le résultat. \square

Notons, pour finir ce paragraphe, que les considérations précédentes donnent aussi une méthode effective pour déterminer les facteurs invariants d'un module de type fini :

Méthode pour déterminer les facteurs invariants d'un A -module de type fini M

1. On fixe une application A -linéaire surjective $\varphi : A^n \rightarrow M$, et on choisit une base $\{e_1, \dots, e_n\}$ de A^n .
2. On détermine une famille de générateurs x_1, \dots, x_s de $\text{Ker}(\varphi)$, que l'on écrit

$$x_i = \sum_{j=1}^n a_{ij}e_j, \text{ pour une matrice } R = (a_{ij}) \in \mathcal{M}_{s,n}(A)$$

et on appelle R la **matrice des relations de M relativement à la base $\{e_1, \dots, e_n\}$** .

3. On détermine les facteurs invariants de la matrice R , pour obtenir $P \in \text{GL}_s(A)$, $Q \in \text{GL}_n(A)$ telles que

$$PRQ = \text{diag}(d_1, \dots, d_t)$$

avec $d_1 \mid \dots \mid d_t$ et $t = \min(s, n)$. Les facteurs invariants de M sont alors les d_i non nuls et non inversibles.

D Application à la réduction des endomorphismes d'un espace vectoriel

On va appliquer les résultats précédents à la réduction des endomorphismes d'un espace vectoriel. Dans la suite K est un corps. On s'intéresse aux problèmes (reliés) suivants. Soit E un K -espace vectoriel de dimension finie.

1. Soit $u \in \text{End}_K(E)$. Trouver une base de E dans laquelle la matrice de u est la plus simple possible.
2. Soient $u, v \in \text{End}_K(E)$. Trouver une condition nécessaire et suffisante pour que u et v soient conjugués (similaires), c'est-à-dire qu'il existe $w \in \text{GL}(E)$ tel que $u = w \circ v \circ w^{-1}$.

Voici le résultat de base.

Proposition D.1. Soient E un K -espace vectoriel de dimension finie, et $u \in \text{End}_K(E)$. Soit $\varphi : K[X] \longrightarrow \text{End}_K(E)$ l'unique morphisme de K -algèbres tel que $\varphi(X) = u$. Pour $P \in K[X]$, on écrit $P(u) = \varphi(P)$.

1. Le morphisme d'algèbres $\varphi : K[X] \longrightarrow \text{End}_K(E)$ est non injectif. Il existe donc un unique polynôme unitaire $P_u \in K[X]$ tel que $\text{Ker}(\varphi) = (P_u)$. Le polynôme P_u est le polynôme minimal de u .
2. Le morphisme d'algèbres $\varphi : K[X] \longrightarrow \text{End}_K(E)$ munit E d'une structure de $K[X]$ -module, définie par $\forall x \in E, \forall P \in K[X], P.x = P(u)(x)$. Un sous-espace de E est stable par u si et seulement si c'est un sous- $K[X]$ -module.
3. Soient $u, v \in \text{End}_K(E)$. Notons E_u et E_v les structures respectives de $K[X]$ -modules sur E que l'on vient de définir. Alors u et v sont conjugués si et seulement si les $K[X]$ -modules E_u et E_v sont isomorphes.

Preuve. 1. Le morphisme d'algèbres φ est non injectif car $\text{End}_K(E)$ est un K -espace vectoriel de dimension finie. $\text{Ker}(\varphi)$ est un idéal de $K[X]$, donc l'existence du polynôme minimal P_u de u provient du fait que $K[X]$ est principal.

2. La deuxième assertion est immédiate car $X.x = u(x)$ pour tout $x \in E$ (on note également que $\text{Ker}(\varphi) = \text{Ann}_{K[X]}(E_u)$).

3. Soit $f : E \longrightarrow E$ une application K -linéaire. Si f est un morphisme de $K[X]$ -modules $E_u \longrightarrow E_v$, on a $\forall x \in E, f(X.x) = X.f(x)$, c'est-à-dire $f \circ u = v \circ f$. Donc si f est un isomorphisme de $K[X]$ -modules $E_u \longrightarrow E_v$, alors u et v sont conjugués. Réciproquement, s'il existe $f \in \text{GL}(E)$ tel que $v = f \circ u \circ f^{-1}$, on a pour tout $P \in K[X], f \circ P(u) = P(v) \circ f$, ce qui montre que f est un isomorphisme $E_u \cong E_v$. \square

Les théorèmes de structures des $K[X]$ -modules se traduisent ainsi.

Théorème D.2. Soient E un K -espace vectoriel de dimension finie, et $u \in \text{End}_K(E)$.

1. Il existe des polynômes unitaires irréductibles $P_1, \dots, P_s \in K[X]$, et des entiers $m_1, \dots, m_s \geq 1$ tels que l'on a un isomorphisme de $K[X]$ -modules

$$E_u \cong K[X]/(P_1^{m_1}) \oplus \dots \oplus K[X]/(P_s^{m_s})$$

avec $P_u = \text{PPCM}(P_1^{m_1}, \dots, P_s^{m_s})$. Les polynômes $P_1^{m_1}, \dots, P_s^{m_s}$ sont appelés les diviseurs élémentaires associés à u . Deux endomorphismes de E sont conjugués si et seulement si ils ont les mêmes diviseurs élémentaires associés (à l'ordre près).

2. Il existe une unique famille de polynômes unitaires (Q_1, \dots, Q_r) non constants tels que

$$E_u \cong K[X]/(Q_1) \oplus \dots \oplus K[X]/(Q_r)$$

et $Q_1 | Q_2 | \dots | Q_r$, et on a $P_u = Q_r$. Les polynômes Q_1, \dots, Q_r sont appelés les facteurs invariants de u . Deux endomorphismes de E sont conjugués si et seulement si ils ont les mêmes facteurs invariants.

Preuve. 1. On applique le théorème de structure des $K[X]$ -modules de type fini en version diviseurs élémentaires. Comme E_u est de dimension finie, il n'y a pas de partie libre et on obtient donc l'isomorphisme annoncé. On a $\text{Ann}_{K[X]}(E_u) = (P_u)$, et puisqu'en général si A est un anneau principal on a $\text{Ann}(A/(a_1) \oplus \dots \oplus A/(a_m)) = (\text{PPCM}(a_1, \dots, a_m))$, on obtient la deuxième assertion. Soient $u, v \in \text{End}_K(E)$. Alors u et v sont conjugués si et seulement si les $K[X]$ -modules E_u et E_v sont isomorphes, et le résultat d'unicité des diviseurs élémentaires pour les $K[X]$ -modules de type fini donne le résultat.

2. La preuve est similaire en utilisant le théorème de structure des $K[X]$ -modules de type fini en version facteurs invariants. \square

Comme première application, on a le résultat fondamental suivant (qui, bien sûr, de manière plus élémentaire, est également une conséquence du lemme des noyaux, voir l'appendice).

Corollaire D.3. Soit E un K -espace vectoriel de dimension finie et soit $u \in \text{End}_K(E)$. Alors u est diagonalisable si et seulement si P_u est scindé sur K à racines simples.

Preuve. S'il existe une base de E dans laquelle la matrice de u est diagonale, on voit facilement que P_u divise un polynôme scindé à racines simples sur K , et est donc scindé à racines simples. Réciproquement supposons P_u est scindé à racines simples. On a

$$E_u \cong K[X]/(P_1^{m_1}) \oplus \cdots \oplus K[X]/(P_s^{m_s})$$

avec P_1, \dots, P_s unitaires irréductibles et $P_u = \text{PPCM}(P_1^{m_1}, \dots, P_s^{m_s})$. L'hypothèse sur P_u assure que $m_1 = \cdots = m_s = 1$ et que chaque P_i est de degré 1. Donc chaque sous $K[X]$ -module $K[X]/(P_i)$ est un K -espace vectoriel de dimension 1 et on a le résultat. \square

On s'intéresse maintenant au premier problème : trouver une base de E dans laquelle la matrice de $u \in \text{End}_K(E)$ est la plus simple possible. La première version, la forme canonique de Jordan, ne fonctionne bien en général que si le corps de base algébriquement clos. La deuxième version, la forme canonique rationnelle, qui utilise les facteurs invariants du $K[X]$ -module E_u , fonctionne sur n'importe quel corps.

D.1 Forme canonique de Jordan

Définition D.4. Une *matrice de Jordan élémentaire* est une matrice de la forme

$$J_\lambda = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & & \vdots \\ \vdots & & \ddots & 1 & 0 \\ & & & \lambda & 1 \\ 0 & \cdots & & 0 & \lambda \end{pmatrix}, \quad \lambda \in K$$

où les coefficients non indiqués sont nuls. On dit qu'une matrice est en *forme canonique de Jordan* si elle est diagonale par blocs, les blocs étant des matrices de Jordan élémentaires.

Théorème D.5. Soit E un K -espace vectoriel de dimension finie, et soit $u \in \text{End}_K(E)$. Les assertions suivantes sont équivalentes.

1. Il existe une base de E dans laquelle la matrice de u est en forme canonique de Jordan.
2. Le polynôme minimal P_u de u est scindé sur K .

Preuve. S'il existe une base de E dans laquelle la matrice de u est en forme canonique de Jordan, on voit facilement que P_u divise un polynôme scindé sur K , et est donc scindé.

Réciproquement, en gardant les notations précédentes, soit

$$\Psi : E_u \longrightarrow K[X]/(P_1^{m_1}) \oplus \cdots \oplus K[X]/(P_s^{m_s})$$

un isomorphisme de $K[X]$ -modules, avec P_1, \dots, P_s unitaires irréductibles et $P_u = \text{PPCM}(P_1^{m_1}, \dots, P_s^{m_s})$. Si P_u est scindé sur K , il suit que les P_i sont de degré 1 et donc on a un isomorphisme de $K[X]$ -modules

$$\Psi : E_u \longrightarrow K[X]/((X - \lambda_1)^{m_1}) \oplus \dots \oplus K[X]/((X - \lambda_s)^{m_s})$$

Pour $i \in \{1, \dots, n\}$, notons $E_i = \Psi^{-1}(K[X]/((X - \lambda_i)^{m_i}))$. Chaque E_i est un sous- $K[X]$ -module de E , donc est stable par u , et on a $E = E_1 \oplus \dots \oplus E_s$ comme $K[X]$ -module. Il suffit donc de montrer que pour tout i , il existe une base de E_i dans laquelle la matrice de $u|_{E_i}$ soit une matrice de Jordan élémentaire. On utilise le lemme suivant.

Lemme D.6. Soit $\lambda \in K$ et $r \geq 1$. Considérons le $K[X]$ -module $K[X]/((X - \lambda)^r)$ (qui est aussi un anneau et un K -espace vectoriel) et notons x la classe de X dans $K[X]/((X - \lambda)^r)$. Pour $k \in \{1, \dots, r\}$, notons $e_k = (x - \lambda)^{r-k}$. Alors $\{e_1, \dots, e_r\}$ est une base du K -espace vectoriel $K[X]/((X - \lambda)^r)$, avec $X.e_1 = \lambda e_1$ et pour $k \geq 2$, $X.e_k = e_{k-1} + \lambda e_k$

Preuve du lemme. On vérifie facilement, par division euclidienne, que $\dim_K(K[X]/((X - \lambda)^r)) \leq r$, et un argument de degré montre que e_1, \dots, e_r est une famille libre. Ainsi on a $\dim_K(K[X]/((X - \lambda)^r)) = r$, et $\{e_1, \dots, e_r\}$ est une base. On a

$$X.e_1 = X.(x - \lambda)^{r-1} = x(x - \lambda)^{r-1} = (x - \lambda + \lambda)(x - \lambda)^{r-1} = (x - \lambda)^r + \lambda(x - \lambda)^{r-1} = \lambda e_1$$

et pour $k \geq 2$

$$X.e_k = x(x - \lambda)^{r-k} = (x - \lambda + \lambda)(x - \lambda)^{r-k} = (x - \lambda)^{r-k+1} + \lambda(x - \lambda)^{r-k} = e_{k-1} + \lambda e_k \quad \square$$

On termine maintenant aisément la preuve du théorème : pour chaque i on transporte la base précédente du lemme via Ψ pour obtenir une base f_1, \dots, f_{m_i} de E_i telle $u(f_1) = \lambda_i f_1$ et pour $k \geq 2$, $u(f_k) = f_{k-1} + \lambda_i f_k$, et la matrice de $u|_{E_i}$ dans cette base est une matrice de Jordan élémentaire. \square

Théorème D.7. Soit E un K -espace vectoriel de dimension finie, avec K algébriquement clos.

1. Il existe, pour tout $u \in \text{End}_K(E)$, une base de E dans laquelle la matrice de u est en forme canonique de Jordan.
2. Deux endomorphismes de E sont conjugués si et seulement si il ont la même forme canonique de Jordan (à permutation des blocs de Jordan près).

Preuve. Le polynôme minimal de u est scindé sur K , on applique donc le théorème précédent. On a vu dans la preuve du théorème précédent que la forme canonique de Jordan de u est complètement déterminée par l'isomorphisme de $K[X]$ -modules

$$\Psi : E_u \longrightarrow K[X]/((X - \lambda_1)^{m_1}) \oplus \dots \oplus K[X]/((X - \lambda_s)^{m_s})$$

L'unicité de la forme canonique de Jordan est donc une conséquence de l'unicité des diviseurs élémentaires dans le théorème de structure des $K[X]$ -modules de type fini. \square

L'existence d'une base dans laquelle la matrice de $u \in \text{End}_K(E)$ est en forme canonique de Jordan est un résultat théorique. En pratique on utilise le **polynôme caractéristique de u** , défini par $\chi_u(X) = \det(XI_n - M)$ (où M est la matrice de u dans n'importe quelle base et $n = \dim(E)$). Les valeurs propres de u sont exactement les racines de χ_u dans K (ce sont également exactement les racines du polynôme minimal P_u dans K).

Théorème D.8 (Cayley-Hamilton). Pour $u \in \text{End}_K(E)$, on a $\chi_u(u) = 0$, et donc le polynôme minimal de u divise χ_u .

Preuve. Le résultat est facile à vérifier si la matrice de u dans une base est en forme canonique de Jordan, donc on a le résultat si K est algébriquement clos. Sinon, soit \bar{K} une clôture algébrique de K . On fixe une base \mathcal{B} de E , et soit $\bar{u} : \bar{K}^n \rightarrow \bar{K}^n$ ($n = \dim_K(E)$) l'endomorphisme dont la matrice M dans la base canonique est la matrice de u dans la base \mathcal{B} . Alors $\chi_{\bar{u}}(X) = \det(XI_n - M) = \chi_u(X)$. Par le cas K algébriquement clos on a $0 = \chi_{\bar{u}}(\bar{u}) = \chi_u(M) = \chi_u(u)$. \square

Corollaire D.9. Soit E un K -espace vectoriel de dimension finie, et soit $u \in \text{End}_K(E)$. Les assertions suivantes sont équivalentes.

1. Il existe une base de E dans laquelle la matrice de u est en forme canonique de Jordan.
2. Le polynôme minimal P_u de u est scindé sur K .
3. Le polynôme caractéristique χ_u de u est scindé sur K .

Preuve. (2) \Rightarrow (1) provient du théorème D.7, (1) \Rightarrow (3) est une vérification immédiate, alors que (3) \Rightarrow (2) est une conséquence du théorème de Cayley-Hamilton. \square

Enfin, pour mettre un endomorphisme en forme canonique de Jordan, on utilise le résultat suivant.

Proposition D.10 (lemme des noyaux). Soit $P \in K[X]$ avec $P = P_1 \cdots P_r$ où les P_i sont premiers entre eux deux à deux. Pour $u \in \text{End}_K(E)$, on a

$$\text{Ker}(P(u)) = \text{Ker}(P_1(u)) \oplus \cdots \oplus \text{Ker}(P_r(u))$$

où $\text{Ker}(P_1(u)), \dots, \text{Ker}(P_r(u))$ sont des sous-espaces u -stables.

Preuve. Le résultat est une application du théorème de Bezout aux polynômes Q_1, \dots, Q_r définis par $Q_i = \prod_{j \neq i} P_j$, qui sont premiers entre eux. Voir l'appendice. \square

On obtient finalement :

Méthode pour mettre un endomorphisme en forme canonique de Jordan

1. On calcule χ_u , que l'on décompose

$$\chi_u(X) = (X - \lambda_1)^{m_1} \cdots (X - \lambda_r)^{m_r}, \lambda_1, \dots, \lambda_r \in K, \lambda_i \neq \lambda_j \text{ si } i \neq j, m_1, \dots, m_r \in \mathbb{N}^*$$

2. Le lemme des noyaux assure alors que l'on a une décomposition en **sous-espaces caractéristiques**

$$E_u = \text{Ker}((u - \lambda_1)^{m_1}) \oplus \cdots \oplus \text{Ker}((u - \lambda_r)^{m_r})$$

On étudie alors pour chaque $i \in \{1, \dots, r\}$, la suite de sous-espaces

$$\text{Ker}(u - \lambda_i) \subset \text{Ker}((u - \lambda_i)^2) \subset \cdots \subset \text{Ker}((u - \lambda_i)^{m_i})$$

Il existe un plus petit entier $p_i \in \{1, \dots, m_i\}$ tel que

$$\text{Ker}((u - \lambda_i)^{p_i}) = \text{Ker}((u - \lambda_i)^{m_i})$$

(qui est en fait le plus petit entier d tel que $\text{Ker}((u - \lambda_i)^d) = \text{Ker}((u - \lambda_i)^{d+1})$) et on a donc

$$E_u = \text{Ker}((u - \lambda_1)^{p_1}) \oplus \cdots \oplus \text{Ker}((u - \lambda_r)^{p_r})$$

On a alors

$$P_u(X) = (X - \lambda_1)^{p_1} \cdots (X - \lambda_r)^{p_r}$$

On travaille enfin sur chaque espace $\text{Ker}((u - \lambda_i)^{p_i})$ pour trouver une base dans laquelle la matrice de u est en forme canonique de Jordan (le nombre de blocs de Jordan pour $u|_{\text{Ker}((u - \lambda_i)^{p_i})}$ est égal à $\dim(\text{Ker}(u - \lambda_i))$). En petite dimension cela peut se faire "à la main", en étudiant la suite de sous-espaces $\text{Ker}(u - \lambda_1) \subset \text{Ker}(u - \lambda_1)^2 \subset \dots \subset \text{Ker}(u - \lambda_1)^{p_1}$, et sinon la meilleure méthode est celle des facteurs invariants, voir le paragraphe suivant (proposition D.16).

D.2 Facteurs invariants et forme canonique rationnelle

Définition D.11. Soit $Q(X) = X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0 \in K[X]$ un polynôme unitaire. La matrice

$$\mathcal{C}(Q) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ & & & & -a_1 \\ & I_{m-1} & & & \vdots \\ & & & & -a_{m-1} \end{pmatrix} \in \mathcal{M}_m(K)$$

est appelée la *matrice compagnon* de Q .

Proposition D.12. Pour $Q(X) \in K[X]$ un polynôme unitaire, le polynôme caractéristique de la matrice $\mathcal{C}(Q)$ est égal à Q : $\chi_{\mathcal{C}(Q)} = Q$.

Preuve. On remplace la ligne 1, L_1 , de $XI_m - \mathcal{C}(Q)$ par

$$L_1 + XL_2 + X^2L_3 + \dots + X^{m-1}L_m$$

ce qui ne change pas le déterminant, et donne le résultat. \square

Définition D.13. On dit qu'une matrice est en *forme canonique rationnelle* si elle est de la forme

$$\mathcal{C}(Q_1, \dots, Q_r) := \begin{pmatrix} \mathcal{C}(Q_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathcal{C}(Q_r) \end{pmatrix}.$$

pour des polynômes unitaires Q_1, \dots, Q_r tels que $Q_1 | Q_2 | \dots | Q_r$

Théorème D.14 (Forme canonique rationnelle d'un endomorphisme). Soit $u \in \text{End}_K(E)$. Alors il existe une base de E dans laquelle la matrice de u est en forme canonique rationnelle. Plus précisément si Q_1, \dots, Q_r sont les facteurs invariants de u , il existe une base de E dans laquelle la matrice de u est

$$\mathcal{C}(Q_1, \dots, Q_r) := \begin{pmatrix} \mathcal{C}(Q_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathcal{C}(Q_r) \end{pmatrix}.$$

Réciproquement les facteurs invariants d'une telle matrice sont Q_1, \dots, Q_r .

Preuve. Supposons d'abord que $r = 1$. Dans ce cas $E_u \cong K[X]/(Q_1)$, et il existe $e \in E$ tel que $E_u = K[X]e$. Soit $m = \deg(Q_1)$. Le polynôme minimal de u est Q_1 .

Vérifions $\{e, u(e), \dots, u^{m-1}(e)\}$ est une base de E . Tout élément $x \in E$ est de la forme $x = P.e = P(u)(e)$ pour un polynôme $P \in K[X]$ car $E_u = K[X]u$. Soient $R, S \in K[X]$ tels que $P = Q_1R + S$ avec $\deg(S) < m$. Alors $x = P.e = (RQ_1).e + S.e = R(u)Q_1(u)(e) + S(u)(e) = S(u)(e)$, ce qui montre que x est combinaison linéaire de $e, u(e), \dots, u^{m-1}(e)$. Si maintenant $\lambda_0, \dots, \lambda_{m-1} \in K$ vérifient $\sum_{i=0}^{m-1} \lambda_i u^i(e) = 0$, posons $R(X) = \sum_{i=0}^{m-1} \lambda_i X^i$. On a alors $R.e = 0$, d'où puisque $E_u = K[X]e$, $R \in \text{Ann}_{K[X]}(E_u) = (Q_1)$ et donc Q_1 divise R et ainsi si $R \neq 0$ on a $\deg(Q_1) \leq \deg(R)$. Or on a $\deg(R) \leq m-1 < \deg(Q_1)$, donc $R = 0$ et $\lambda_0 = \dots = \lambda_{m-1} = 0$.

On vérifie alors sans difficulté que la matrice de u dans la base $\{e, u(e), \dots, u^{m-1}(e)\}$ est $\mathcal{C}(Q_1)$. Le cas général se déduit du cas $r = 1$: si $E_u \cong K[X]/(Q_1) \oplus \dots \oplus K[X]/(Q_r)$, on obtient la base voulue en faisant la réunion des bases des sous-espaces $K[X]/(Q_i)$.

Réciproquement, si la matrice dans une base de u est $\mathcal{C}(Q)$, alors cette base est de la forme $\{e, u(e), \dots, u^{m-1}(e)\}$ ($m = \deg(Q)$) pour un certain $e \in E$ et alors l'application $K[X]$ -linéaire $K[X] \rightarrow E_u, P \mapsto P(u)(e)$ induit un isomorphisme $K[X]/(Q) \cong E_u$, ce qui montre que Q est l'unique facteur invariant de u . Dans le cas général, si $\mathcal{C}(Q_1, \dots, Q_r)$ est la matrice de u dans une base, alors l'argument précédent va assurer que $E_u \cong K[X]/(Q_1) \oplus \dots \oplus K[X]/(Q_r)$ et donc Q_1, \dots, Q_r sont bien les facteurs invariants de u . \square

Corollaire D.15. Deux endomorphismes de E sont conjugués si et seulement si ils ont la même forme canonique rationnelle.

Proposition D.16 (Recherche pratique des facteurs invariants). Soit $u \in \text{End}_K(E)$. Soit $\mathcal{B} = \{e_1, \dots, e_n\}$ une base de E comme K -espace vectoriel et soit M la matrice de u dans la base \mathcal{B} . Alors les facteurs invariants de u (ou de M) sont les facteurs invariants non inversibles de la matrice

$${}^tM - XI_n \in \mathcal{M}_n(K[X])$$

Plus précisément, soit $\{\varepsilon_1, \dots, \varepsilon_n\}$ une base du $K[X]$ -module libre $K[X]^n$ et soit $\theta : K[X]^n \rightarrow E_u$ l'unique application $K[X]$ -linéaire qui envoie ε_i sur e_i , pour tout i .

1. La matrice des relations du $K[X]$ -module E_u relative à $\{\varepsilon_1, \dots, \varepsilon_n\}$ est ${}^tM - XI_n$.
2. Soient $Q_1, \dots, Q_r \in K[X]$ les facteurs invariants de u . Soit $\{\tilde{\varepsilon}_1, \dots, \tilde{\varepsilon}_n\}$ la base adaptée au sous- $K[X]$ -module $\text{Ker}(\theta) : \{\tilde{\varepsilon}_1, \dots, \tilde{\varepsilon}_{n-r}, Q_1\tilde{\varepsilon}_{n-r+1}, \dots, Q_r\tilde{\varepsilon}_n\}$ est une base de $\text{Ker}(\theta)$. On a $\theta(\tilde{\varepsilon}_i) = 0$ pour $1 \leq i \leq n-r$ et $\theta(\tilde{\varepsilon}_{n-r+i}) =: f_i \in E_u \setminus \{0\}$ pour $1 \leq i \leq r$. Alors la famille

$$f_1, u(f_1), \dots, u^{k_1-1}(f_1), \quad k_1 = \deg(Q_1)$$

$$f_2, u(f_2), \dots, u^{k_2-1}(f_2), \quad k_2 = \deg(Q_2)$$

...

$$f_r, u(f_r), \dots, u^{k_r-1}(f_r), \quad k_r = \deg(Q_r)$$

est une base de E dans laquelle la matrice de u est

$$\mathcal{C}(Q_1, \dots, Q_r) := \begin{pmatrix} \mathcal{C}(Q_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathcal{C}(Q_r) \end{pmatrix}$$

Preuve. Ecrivons $A = K[X]$. Le A -module E_u est de type fini. On l'écrit comme le quotient d'un A -module libre : \mathcal{B} engendre E_u comme A -module, donc E_u est un quotient de A^n . Notons $\{\varepsilon_1, \dots, \varepsilon_n\}$

une base du A -module libre A^n . Soit $\theta : A^n \rightarrow E$ le morphisme de A -modules défini par $\theta(\varepsilon_i) = e_i$ pour tout i . Alors $E \cong A^n / \text{Ker } \theta$.

Posons $M = (a_{ij})_{1 \leq i, j \leq n}$. Alors $u(e_i) = \sum_j a_{ji} e_j$ pour tout i , c'est-à-dire que $\sum_j a_{ji} e_j - X e_i = 0$, donc pour tout i l'élément $x_i = \sum_j a_{ji} e_j - X e_i$ est dans le noyau de θ . Les coordonnées de x_i dans la base $\{\varepsilon_1, \dots, \varepsilon_n\}$ forment la ligne i de ${}^t M - X I_n$. Donc pour conclure, il nous faut montrer que les x_i engendrent $\text{Ker } \theta$. On a déjà l'inclusion $\sum_{i=1}^n A x_i \subset \text{Ker } \theta$.

On vient de voir que pour tout i , $X e_i$ est dans $(\bigoplus_{j=1}^n K e_j) + \sum_{i=1}^n A x_i$, donc par récurrence, on peut dire de même pour tout $X^m e_i$ et donc pour tout $P(X) e_i$ avec $P(X) \in A$. Soit maintenant $z \in \text{Ker } \theta$. Puisque $\{\varepsilon_1, \dots, \varepsilon_n\}$ est une base du A -module A^n , on peut écrire $z = \sum_i P_i(X) \varepsilon_i$ avec $P_i \in A$. D'après ce qui précède, on peut donc écrire $z = \sum_{i=1}^n \lambda_i \varepsilon_i + y$ avec $y \in A x_1 + \dots + A x_n$ et $\lambda_i \in k$. On sait déjà que $y \in \text{Ker } \theta$ par l'inclusion que l'on a déjà montrée, donc on a aussi $\sum_{i=1}^n \lambda_i \varepsilon_i = z - y \in \text{Ker } \theta$. Donc en appliquant θ on a $\sum_{i=1}^n \lambda_i e_i = 0$. Or $\{e_1, \dots, e_n\}$ est une K -base de E , donc tous les λ_i sont nuls et donc $z = y \in A x_1 + \dots + A x_n$.

Finalement on a bien $\text{Ker } \theta = A x_1 + \dots + A x_n$. Ainsi La matrice des relations du $K[X]$ -module E_u relative à $\{\varepsilon_1, \dots, \varepsilon_n\}$ est ${}^t M - X I_n$. Les facteurs invariants de cette matrice sont du type

$$(1, 1, 1, \dots, 1, Q_1, \dots, Q_r)$$

avec Q_1, \dots, Q_r unitaires non constants, et ce sont les facteurs invariants du $K[X]$ -module E_u (voir fin du paragraphe C), et donc de u . Pour la deuxième assertion, le fait que l'on a bien une base se montre directement en utilisant que $\{\tilde{\varepsilon}_1, \dots, \tilde{\varepsilon}_{n-r}, Q_1 \tilde{\varepsilon}_{n-r+1}, \dots, Q_r \tilde{\varepsilon}_n\}$ est une base de $\text{Ker}(\theta)$, et la dernière est alors immédiate. \square

Exemple D.17. Soit $u \in \text{End}(K^3)$ dont la matrice dans la base canonique $\{e_1, e_2, e_3\}$ est

$$T = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}. \text{ On veut trouver les facteurs invariants de } u.$$

On considère donc la matrice ${}^t T - X I_3 = \begin{pmatrix} 1-X & 1 & 1 \\ -1 & -1-X & -1 \\ 1 & 0 & -X \end{pmatrix}$. Les opérations suivantes : $C_2 \leftrightarrow C_1$; $L_2 \rightarrow L_2 + (X+1)L_1$; $C_2 \rightarrow C_2 - (1-X)C_1$; $C_3 \rightarrow C_3 - C_1$; $L_2 \leftrightarrow L_3$; $C_3 \rightarrow C_3 + X C_2$; $L_3 \rightarrow L_3 + X^2 L_2$; $C_3 \rightarrow -C_3$ donnent la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3 - X \end{pmatrix}$.

On en déduit que le seul facteur invariant de u sont $X^3 - X$ et que $K_u^3 \cong K[X]/(X^3 - X)$.

La matrice compagnon de $X^3 - X$ est $C_{X^3-X} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, qui est donc la forme cano-

nique rationnelle de u .

Soit $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ la base canonique de $K[X]^3$, et considérons l'application $K[X]$ -linéaire $\theta : K[X]^3 \rightarrow K_u^3$, $\varepsilon_i \mapsto e_i$. La base $\{\tilde{\varepsilon}_1, \tilde{\varepsilon}_2, \tilde{\varepsilon}_3\}$ de $K[X]^3$ adaptée à $\text{Ker}(\theta)$ est obtenue grâce à la

matrice Q^{-1} (notations de la remarque B.5). Ici $Q^{-1} = \begin{pmatrix} 1-X & 1 & 1 \\ 1 & 0 & -X \\ 0 & 0 & -1 \end{pmatrix}$, donc la nouvelle

base est donnée par $\tilde{\varepsilon}_1 = (1-X)\varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\tilde{\varepsilon}_2 = \varepsilon_1 - X\varepsilon_3$ et $\tilde{\varepsilon}_3 = -\varepsilon_3$. Alors on a $\theta(\tilde{\varepsilon}_1) = \theta(\tilde{\varepsilon}_2) = 0$ et $\theta(\tilde{\varepsilon}_3) = -e_3$ et θ induit un isomorphisme de $K[X]$ -modules $K[X]/(X^3 - X) \cong E_u$, et $\{e_3, u(e_3) = e_1, u^2(e_3) = e_1 + e_2 + e_3\}$ est une base de K^3 dans laquelle la matrice de u est C_{X^3-X}

Remarque. Dans l'exemple précédent, le calcul des facteurs invariants assure que $X^3 - X$

est le polynôme minimal de u , donc u est en fait diagonalisable.

Remarque D.18. La Proposition D.16 peut être utilisée également pour mettre en forme canonique de Jordan les matrices nilpotentes (et donc bien sûr les matrices M telles que $M - \lambda I_n$ soit nilpotente pour un $\lambda \in K$).

Remarque D.19. A partir de la forme de Jordan, on peut retrouver les facteurs invariants.

On construit un tableau de la façon suivante :

1. A chaque valeur propre λ_{ij} on associe une ligne : on remplit les lignes avec les $(X - \lambda_{ij})^{n_{ij}}$ avec les n_{ij} en ordre décroissant (n_{ij} est la taille du bloc de Jordan), et on complète avec des 1 pour avoir des lignes de même longueur.
2. Pour obtenir les facteurs invariants, on fait le produit colonne par colonne.

Exemple D.20. Les diviseurs élémentaires (polynômes unitaires égaux au signe près aux polynômes caractéristiques des blocs de Jordan) de

$$\begin{pmatrix} \boxed{2} & 0 & 0 & 0 & 0 \\ 0 & \boxed{\begin{matrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{matrix}} & 0 & 0 & 0 \\ 0 & 0 & \boxed{2} & 0 & 0 \\ 0 & 0 & 0 & \boxed{\begin{matrix} 3 & 1 \\ 0 & 3 \end{matrix}} & 0 \\ 0 & 0 & 0 & 0 & \boxed{\begin{matrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{matrix}} \end{pmatrix}$$

sont $X - 2$, $(X - 3)^3$, $X - 2$, $(X - 3)^2$ et $(X - 3)^3$.

$\lambda = 2$	$X - 2$	$X - 2$	1
$\lambda = 3$	$(X - 3)^3$	$(X - 3)^3$	$(X - 3)^2$
Résultat	$(X - 2)(X - 3)^3$ (Q_3)	$(X - 2)(X - 3)^3$ (Q_2)	$(X - 3)^2$ (Q_1)

Les facteurs invariants sont Q_1, Q_2, Q_3 .

VI Représentations linéaires des groupes finis

A Introduction

Dans ce chapitre on étudie les représentations linéaires des groupes finis, qui sont les modules sur l'algèbre du groupe $\mathbb{C}[G]$. On n'utilisera pas (ou peu) la langage des modules, ce qui rend ce chapitre essentiellement indépendant des précédents (à la construction de l'algèbre du groupe près).

On a en vue deux applications. La première concerne la structure de l'algèbre d'un groupe fini. Rappelons que si G est un groupe, l'algèbre du groupe G , notée $\mathbb{C}[G]$, est l'espace vectoriel des fonctions à support fini $G \rightarrow \mathbb{C}$ (de base $\{e_g, g \in G\}$), muni du produit défini par $e_g * e_h = e_{gh}, \forall g, h \in G$.

Théorème A.1. Soit G un groupe fini. On a un isomorphisme d'algèbres

$$\mathbb{C}[G] \cong \prod_{i=1}^r \mathcal{M}_{n_i}(\mathbb{C})$$

où r est le nombre de classes de conjugaison de G et $n_1, \dots, n_r \in \mathbb{N}^*$.

Ce résultat, assez surprenant au premier abord, est une conséquence de la théorie des représentations linéaires de G . La deuxième application est une application interne à la théorie des groupes.

Théorème A.2 (Théorème "pq" de Burnside). Soient p et q des nombres premiers. Soit G un groupe d'ordre $p^\alpha q^\beta$ où $\alpha, \beta \in \mathbb{N}$ vérifient $\alpha + \beta \geq 2$. Alors le groupe G n'est pas simple.

B Définitions

Le corps de base est $K = \mathbb{C}$. On considère un groupe G .

Définition B.1. Une *représentation linéaire* de G est un couple (V, π_V) où V est un espace vectoriel de dimension finie et où $\pi_V : G \rightarrow \text{GL}(V)$ est un morphisme de groupes.

Remarques. 1. On peut aussi définir des représentations linéaires avec un corps de base K quelconque, ainsi que sur des espaces vectoriels de dimension infinie. Nous limiterons au cadre de la définition.

2. Si G est un sous-groupe de $\text{GL}(V)$, alors (V, i) , où i est l'injection $G \hookrightarrow \text{GL}(V)$ est une représentation linéaire de G .

3. Soit $\pi : G \rightarrow \text{GL}_n(\mathbb{C})$ un morphisme de groupes. En identifiant $\text{GL}_n(\mathbb{C})$ et $\text{GL}(\mathbb{C}^n)$, on a une représentation linéaire (π, \mathbb{C}^n) de G .
4. Si (V, π_V) est une représentation de G , alors le morphisme de groupes $\pi_V : G \rightarrow \text{GL}(V)$ induit un morphisme d'algèbres $\widetilde{\pi}_V : \mathbb{C}[G] \rightarrow \text{End}_{\mathbb{C}}(V)$ et donc une structure de $\mathbb{C}[G]$ -module sur V . Réciproquement un tel morphisme d'algèbres induit, par restriction à G , une représentation linéaire de G . La théorie des représentations linéaires d'un groupe G est donc la même que celle des $\mathbb{C}[G]$ -modules. Dans la suite on n'utilisera pas le langage des modules.
5. Si (V, π_V) est une représentation de G et G est fini, alors pour tout $g \in G$, $\pi_V(g)$ est diagonalisable. En effet, on a $\pi_V(g)^{|G|} = \text{id}_V$, donc le polynôme minimal de $\pi_V(g)$, qui divise $X^{|G|} - 1$, est (scindé) à racines simples.

Définition B.2. Un G -espace est un espace vectoriel de dimension finie V muni d'une opération de G sur V

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, v) &\longmapsto g.v \end{aligned}$$

telle que $\forall g \in G, \forall v_1, v_2 \in V, \forall \lambda \in \mathbb{C}$,

$$g.(v_1 + v_2) = g.v_1 + g.v_2, \quad g.(\lambda v) = \lambda(g.v).$$

Proposition B.3. Les notions de G -espace et de représentation linéaire de G sont équivalentes.

Si V est un G -espace, on obtient un morphisme de groupe

$$\begin{aligned} \pi_V : G &\longrightarrow \text{GL}(V) \\ g &\longmapsto \pi_V(g), \quad \pi_V(g)(v) = g.v, \forall v \in V \end{aligned}$$

Réciproquement si (V, π_V) est une représentation linéaire de G , alors on définit sur V une structure de G -espace en posant

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, v) &\longmapsto g.v := \pi_V(g)(v) \end{aligned}$$

Preuve. Si V est un G -espace, on a en particulier une opération de G sur V , et donc le morphisme de groupes annoncé $\pi_V : G \rightarrow S_V$ dans le groupe symétrique de G . Alors pour tout $g \in G$, l'application π_V est linéaire par les axiomes de G -espace, donc est un élément de $\text{GL}(V)$.

Réciproquement si (V, π_V) est une représentation linéaire de G , on vérifie sans difficulté que la formule donnée muni V d'une structure de G -espace. \square

On a donc deux notions équivalentes, que l'on utilisera de façon interchangeable suivant les situations. Plus simplement on dira que V est **une représentation de G** , ce qui signifie que V est un G -espace avec l'opération associée, et que l'on s'est donné le morphisme de groupes correspondant $\pi_V : G \rightarrow \text{GL}(V)$.

Définition B.4. Soient V et W des représentations de G . Un **morphisme de représentations de V dans W** , ou un **G -morphisme**, est une application linéaire $f : V \rightarrow W$ telle que

$$\forall g \in G, \forall v \in V, f(g.v) = g.f(v).$$

L'ensemble des morphismes de représentations de V dans W est noté $\text{Hom}_G(V, W)$. C'est un sous-espace vectoriel de $\text{Hom}(V, W)$ (exercice).

Remarque. Au niveau des morphismes de groupes $\pi_V : G \rightarrow \text{GL}(V)$ et $\pi_W : G \rightarrow \text{GL}(W)$, dire que f est un morphisme entre V et W signifie que $\forall g \in G$, on $f \circ \pi_V(g) = \pi_W(g) \circ f$, c'est-à-dire que les diagrammes suivants sont commutatifs :

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \pi_V(g) \downarrow & & \downarrow \pi_W(g) \\ V & \xrightarrow{f} & W \end{array}$$

On vérifie sans difficulté que la composée de deux G -morphisms est encore un G -morphisme. Un **isomorphisme de représentations**, ou **G -isomorphisme** est un morphisme de représentations qui est bijectif. L'inverse est alors aussi un morphisme de représentations (vérifier).

Définition B.5. La *dimension* d'une représentation est la dimension de l'espace vectoriel sous-jacent.

Il est clair que deux représentations isomorphes ont même dimension.

Définition B.6. Soit (V, π_V) une représentation de G . Le *caractère* de V est la fonction $\chi_V : G \rightarrow \mathbb{C}$ définie par

$$\chi_V(g) = \text{Tr}(\pi_V(g)), \quad \forall g \in G.$$

On dit qu'une fonction $\chi : G \rightarrow \mathbb{C}$ est un *caractère* si χ est le caractère d'une représentation de G .

On verra que, de manière un peu surprenante, une représentation linéaire est entièrement déterminée par son caractère.

Définition B.7. Soit V une représentation de G et soit $W \subset V$ un sous-espace. On dit que W est une *sous-représentation* de V si $\forall g \in G, \forall w \in W, on a g.w \in W$.

Il est clair qu'une sous-représentation est elle-même une représentation de G .

Définition B.8. Soit V une représentation de G . On dit que V est *irréductible* si $V \neq \{0\}$ et si les seules sous-représentations de V sont $\{0\}$ et V .

On définit une relation d'équivalence sur l'ensemble des représentations de G en posant $V \sim W$ si V et W sont isomorphes. On notera $\text{Irr}(G)$ l'ensemble des classes d'isomorphismes de représentations irréductibles. Pour une représentation V de G , on notera $[V]$ sa classe d'isomorphisme.

L'objectif des paragraphes qui suivent est de décrire la structure des représentations d'un groupe fini.

C Constructions et exemples de représentations

On considère toujours un groupe G .

C.1 Représentations de dimension un

Les représentations de dimension 1 de G correspondent exactement aux morphismes de groupes $\pi : G \rightarrow \mathbb{C}^*$. En effet, si V est un espace vectoriel de dimension un, le groupe $GL(V)$ s'identifie à \mathbb{C}^* , ainsi un morphisme de groupes $G \rightarrow GL(V)$ est exactement un morphisme de groupes $G \rightarrow \mathbb{C}^*$.

Une représentation de dimension 1 est nécessairement irréductible, puisque les seuls sous-espaces d'un espace de dimension 1 sont $\{0\}$ et lui-même.

Deux représentations de dimension 1 $\pi, \chi : G \rightarrow \mathbb{C}^*$ sont isomorphes si et seulement si $\pi = \chi$.

On notera \widehat{G} l'ensemble des morphismes de groupes $G \rightarrow \mathbb{C}^*$, qui s'identifie donc à l'ensemble des représentations de dimension 1 de G . On verra qu'en fait si G est un groupe abélien fini, alors $\widehat{G} = \text{Irr}(G)$.

On notera \mathbb{I} la représentation donnée par le morphisme trivial $G \rightarrow \mathbb{C}^*, g \mapsto 1$. On dit que \mathbb{I} est la **représentation triviale** de G .

On vérifie sans difficulté que la loi

$$\begin{aligned} \widehat{G} \times \widehat{G} &\longrightarrow \widehat{G} \\ (\phi, \psi) &\longmapsto \phi \cdot \psi, \phi \cdot \psi(x) = \phi(x)\psi(x), \forall x \in G, \end{aligned}$$

munit \widehat{G} d'une structure de groupe abélien.

Théorème C.1. Si G est un groupe fini abélien, alors les groupes G et \widehat{G} sont isomorphes.

Preuve. Etape 1. Supposons d'abord que $G = C_n = \langle x \rangle$ est cyclique d'ordre n . Pour toute racine n -ième de l'unité $\omega \in \mu_n$, on a un unique morphisme de groupes $\phi_\omega : G \rightarrow \mu_n$ tel que $\phi_\omega(x) = \omega$. Cela donne une application $\mu_n \rightarrow \widehat{G}, \omega \mapsto \phi_\omega$ qui est un morphisme de groupes, injectif car x engendre G . Réciproquement, si $\phi \in \widehat{G}$, on a $\phi(x)^n = \phi(x^n) = \phi(1) = 1$, donc $\phi(x) \in \mu_n$. Puisque x engendre G , on en déduit que $\phi = \phi_\omega$ pour $\omega = \phi(x)$. Ainsi on a un isomorphisme $\mu_n \cong \widehat{G}$, et μ_n étant lui-même un groupe cyclique (engendré par exemple par $e^{\frac{2i\pi}{n}}$), on a bien l'isomorphisme annoncé.

Etape 2. Soient G et H des groupes. Alors on a $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$. En effet on vérifie que l'application

$$\begin{aligned} \theta : \widehat{G \times H} &\longrightarrow \widehat{G} \times \widehat{H} \\ \phi &\longmapsto (\phi \circ i_1, \phi \circ i_2), \end{aligned}$$

où $i_1 : G \rightarrow G \times H, g \mapsto (g, 1)$ et $i_2 : H \rightarrow G \times H, h \mapsto (1, h)$, désignent les injections respectives, est un isomorphisme de groupes.

Etape 3. On peut conclure en utilisant le théorème de structure des groupes finis abéliens : tout groupe abélien fini est isomorphe à un produit de groupes cycliques, donc les étapes 1 et 2 donnent le résultat. \square .

Corollaire C.2. Si G est un groupe fini, alors $|\widehat{G}|$ divise $|G|$.

Preuve. On vérifie que les groupes \widehat{G} et $\widehat{G/D(G)}$ sont isomorphes, où $D(G)$ est le groupe dérivé de G . Le groupe $G/D(G)$ est abélien, donc le théorème assure que $|\widehat{G/D(G)}| = |G/D(G)|$, d'où le résultat en utilisant le théorème de Lagrange. \square

Exercice. Soit $n \geq 2$. Montrer que $\widehat{S}_n = \{\mathbb{I}, \varepsilon\}$, et si $n \geq 5$, alors $\widehat{A}_n = \{\mathbb{I}\}$.

C.2 Représentations de permutation

Soit X un ensemble fini. On note \mathbb{C}^X le \mathbb{C} -espace vectoriel de applications $X \rightarrow \mathbb{C}$. Pour $x \in X$, on note e_x la fonction indicatrice de l'ensemble $\{x\}$: $e_x(x) = 1$ et $e_x(y) = 0$ si $y \neq x$. L'ensemble $(e_x)_{x \in X}$ est une base de \mathbb{C}^X (si $\varphi \in \mathbb{C}^X$, on a $\varphi = \sum_{x \in X} \varphi(x)e_x$).

Proposition C.3. Supposons que G opère sur un ensemble fini X . Alors l'application suivante munit \mathbb{C}^X d'une structure de G -espace

$$G \times \mathbb{C}^X \longrightarrow \mathbb{C}^X$$

$$(g, \varphi) \longmapsto g.\varphi, \quad g.\varphi(x) = \varphi(g^{-1}.x), \quad \forall x \in X.$$

Pour $g \in G$ et $x \in X$, on a $g.e_x = e_{g.x}$.

Preuve. On doit tout d'abord vérifier que l'on a bien une opération. Soit $\varphi \in \mathbb{C}^X$ et $x \in X$. On a $1.\varphi(x) = \varphi(1.x) = \varphi(x)$, d'où $1.\varphi = \varphi$. Soient $g, h \in G$. Alors

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

donc $(gh).\varphi = g.(h.\varphi)$ et on a bien une opération. Il reste à voir que cette opération est linéaire. Soient $\varphi, \psi \in \mathbb{C}^X$ et $\lambda \in \mathbb{C}$. On a

$$g.(\varphi + \lambda\psi)(x) = (\varphi + \lambda\psi)(g^{-1}.x) = \varphi(g^{-1}.x) + \lambda\psi(g^{-1}.x) = g.\varphi(x) + \lambda(g.\psi)(x),$$

donc $g.(\varphi + \lambda\psi) = g.\varphi + \lambda g.\psi$ est \mathbb{C}^X est bien un G -espace.

Pour $x, y \in X$ et $g \in G$, on a $g.e_x(y) = e_x(g^{-1}.y) = 1$ si $x = g^{-1}.y$, c'est-à-dire si $y = g.x$, et 0 sinon. Donc $g.e_x = e_{g.x}$. \square

On obtient ainsi un procédé général pour construire des représentations linéaires. Par exemple pour l'opération de G sur lui-même par translations, on obtient une représentation linéaire de G sur \mathbb{C}^G , appelée **représentation régulière de G** .

C.3 Somme directe de représentations

Les constructions de ce paragraphe sont des cas particuliers de constructions pour les modules (chapitre 1)

Commençons par quelques rappels sur les sommes directes. Soit V un espace vectoriel et soient V_1, \dots, V_n des sous-espaces de V . On dit que V est somme directe des V_i , et on écrit $V = \bigoplus_{i=1}^n V_i$, si tout élément $v \in V$ s'écrit de manière *unique* sous la forme $v = \sum_{i=1}^n v_i$ où $\forall i, v_i \in V_i$.

Si on part maintenant d'une famille V_1, \dots, V_n d'espaces vectoriels, on peut former le produit $\prod_{i=1}^n V_i$, qui est un espace vectoriel pour les lois produit. On peut alors identifier chaque V_i à un sous-espace de $\prod_{i=1}^n V_i$ via l'application linéaire injective

$$V_i \longrightarrow V_1 \times \dots \times V_i \times \dots \times V_n$$

$$v_i \longmapsto (0, \dots, 0, v_i, 0, \dots, 0)$$

et sous cette identification, on a $\prod_{i=1}^n V_i = \bigoplus_{i=1}^n V_i$.

Soient V_1, \dots, V_n des représentations de G . On munit alors $\bigoplus_{i=1}^n V_i$ d'une structure de G -espace grâce à l'application

$$\begin{aligned} G \times \bigoplus_{i=1}^n V_i &\longrightarrow \bigoplus_{i=1}^n V_i \\ (g, (v_i)_{1 \leq i \leq n}) &\longmapsto (g \cdot v_i)_{1 \leq i \leq n} \end{aligned}$$

ce qui au niveau des morphisme de groupes, donne le morphisme

$$\begin{aligned} \pi = \bigoplus_{i=1}^n \pi_{V_i} : G &\longrightarrow \text{GL}\left(\bigoplus_{i=1}^n V_i\right) \\ g &\longmapsto \bigoplus_{i=1}^n \pi_{V_i}(g), (v_i)_{1 \leq i \leq n} \longmapsto (\pi_{V_i}(g)(v_i))_{1 \leq i \leq n} \end{aligned}$$

La représentation de G obtenue est **la somme directe des représentations** V_1, \dots, V_n .

Si maintenant V est une représentation de G et si V_1, \dots, V_n sont des sous-représentations de V telles $V = \bigoplus_{i=1}^n V_i$ en tant qu'espace vectoriel, alors V s'identifie, en tant que représentation de G , à la somme directe des représentations que l'on vient de construire.

Le résultat d'algèbre linéaire élémentaire suivant sera utile.

Lemme C.4. Soient $V_1, \dots, V_n, W_1, \dots, W_p$ des représentations de G . Alors on a un isomorphisme d'espaces vectoriels

$$\text{Hom}_G\left(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^p W_j\right) \cong \bigoplus_{i=1}^n \bigoplus_{j=1}^p \text{Hom}_G(V_i, W_j).$$

Preuve. Posons $V = \bigoplus_{i=1}^n V_i$ et $W = \bigoplus_{j=1}^p W_j$. Pour $1 \leq i \leq n$, notons v_i l'injection $V_i \rightarrow V$ et $p_i : V \rightarrow V_i$ la projection sur la i -ème composante. Pour $1 \leq j \leq p$, notons η_j l'injection $W_j \rightarrow W$ et $q_j : W \rightarrow W_j$ la projection sur la j -ième composante. Ce sont des morphismes de représentations. On obtient donc des application linéaires

$$\begin{aligned} \text{Hom}_G\left(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^p W_j\right) &\longrightarrow \bigoplus_{i=1}^n \bigoplus_{j=1}^p \text{Hom}_G(V_i, W_j) \\ f &\longmapsto (q_j \circ f \circ v_i)_{1 \leq i \leq n, 1 \leq j \leq p} \end{aligned}$$

$$\begin{aligned} \bigoplus_{i=1}^n \bigoplus_{j=1}^p \text{Hom}_G(V_i, W_j) &\longrightarrow \text{Hom}_G\left(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^p W_j\right) \\ (f_{ij})_{1 \leq i \leq n, 1 \leq j \leq p} &\longmapsto \sum_{i,j} \eta_j \circ f_{ij} \circ p_i \end{aligned}$$

On vérifie que ce sont des isomorphismes réciproques, ce qui provient des identités

$$\sum_{i=1}^n v_i \circ p_i = \text{Id}_V, \sum_{j=1}^p \eta_j \circ q_j = \text{Id}_W, p_i \circ v_{i'} = \delta_{ii'} \text{Id}_{V_i}, q_j \circ \eta_{j'} = \delta_{jj'} \text{Id}_{W_j}. \quad \square$$

C.4 Représentation duale

On commence par une construction un peu plus générale.

Proposition C.5. Soient V et W des représentations de G . Alors l'application

$$\begin{aligned} G \times \text{Hom}(V, W) &\longrightarrow \text{Hom}(V, W) \\ (g, f) &\longmapsto g.f := \pi_W(g) \circ f \circ \pi_V(g^{-1}) \end{aligned}$$

munit $\text{Hom}(V, W)$ d'une structure de G -espace.

Preuve. Vérifions d'abord que l'on a bien une opération. Il est clair que $1.f = f$. Soient $g, h \in G$ et $f \in \text{Hom}(V, W)$. Alors

$$(gh).f = \pi_W(gh) \circ f \circ \pi_V((gh)^{-1}) = \pi_W(g) \circ \pi_W(h) \circ f \circ \pi_V(h^{-1}) \circ \pi_V(g^{-1}) = g.(h.f)$$

Enfin il est immédiat, puisque la composition des applications est bilinéaire, que l'opération est bien linéaire. \square

En prenant $W = \mathbb{I}$ la représentation triviale dans la proposition précédente, on obtient donc une structure de G -espace sur $V^* = \text{Hom}(V, \mathbb{C})$. La représentation obtenue, notée V^* est appelée **représentation duale de V** . Le morphisme de groupe correspondant est

$$\begin{aligned} \pi_{V^*} : G &\longrightarrow \text{GL}(V^*) \\ g &\longmapsto {}^t\pi_V(g^{-1}) \end{aligned}$$

(Rappelons que la transposée d'une application linéaire $f : V \longrightarrow W$ est l'application linéaire ${}^t f : W^* \longrightarrow V^*$ définie par ${}^t f(\phi) = \phi \circ f$)

D Énoncé des théorèmes principaux

On peut déjà énoncer le théorème principal sur les représentations d'un groupe fini.

Théorème D.1 (Le théorème de structure des représentations d'un groupe fini). Soit G un groupe fini.

1. L'ensemble $\text{Irr}(G)$ des classes d'isomorphismes de représentations irréductibles de G est fini et son cardinal s est égal au nombre de classes de conjugaison de G .

Soit W_1, \dots, W_s un ensemble complet de représentations irréductibles de G (c'est-à-dire que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$). Notons $d_i = \dim(W_i)$ pour $1 \leq i \leq s$.

2. Soit V une représentation de G . Alors on a un isomorphisme de représentations

$$V \cong \bigoplus_{i=1}^s W_i^{n_i}$$

où les entiers n_1, \dots, n_s sont donnés par $n_i = \dim(\text{Hom}_G(W_i, V))$.

3. On a $|G| = \sum_{i=1}^s d_i^2$.

4. Pour tout $i \in \{1, \dots, s\}$, on a $d_i \mid |G|$, donc la dimension d'une représentation irréductible de G divise l'ordre de G .

5. Le nombre de représentations irréductibles de dimension 1, égal à $|\widehat{G}| = |\text{Hom}(G, \mathbb{C}^*)|$, divise $|G|$.

Rappelons que les classes de conjugaison de G sont les classes d'équivalence pour la relation d'équivalence sur G définie par $x \sim y \iff \exists g \in G$ tel que $y = gxg^{-1}$. La classe de conjugaison d'un élément $g \in G$ est donc l'ensemble $C = \{gxg^{-1}, g \in G\}$, c'est aussi l'orbite de g pour l'opération de G sur lui-même par conjugaison.

Voici quelques illustrations simples de l'utilisation du théorème de structure.

- Si G est un groupe abélien fini, il y a exactement $|G|$ -classes de conjugaison, donc $|G|$ classes d'isomorphisme de représentations irréductibles de G . La formule $|G| = \sum_i d_i^2$ assure que ces représentations sont toutes de dimension 1 (ce qui peut se démontrer aussi plus directement en utilisant le lemme de Schur à venir).

Réciproquement si G est un groupe fini dont toutes les représentations irréductibles sont de dimension 1, alors la formule $\sum_{i=1}^s d_i^2 = s = |G|$ assure que G possède $|G|$ classes de conjugaison, donc que G est abélien.

On a donc le résultat suivant.

Théorème D.2. Soit G un groupe fini. Alors G est abélien si et seulement si toutes ses représentations irréductibles sont de dimension 1.

- Le groupe symétrique S_3 . Si d est la dimension d'une représentation irréductible de S_3 , on a $d^2 \leq |S_3| = 6$, d'où $d \leq 2$. Comme S_3 est non abélien, il existe donc nécessairement une représentation irréductible de dimension 2. En fait on peut construire cette représentation en remarquant que S_3 est le groupe des isométries d'un triangle. Un coup d'oeil à la formule $\sum_i d_i^2 = 6$ assure alors qu'il y a exactement deux autres représentations irréductibles de S_3 non isomorphes, qui sont de dimension 1. Il y a bien sûr la représentation triviale, ainsi que la signature.

En résumé, il y a 3 classes de représentations irréductibles pour S_3 : deux de dimension 1, et une de dimension 2.

On a aussi un critère utile pour montrer qu'une représentation est irréductible.

Théorème D.3. Soit V une représentation d'un groupe fini G . Alors

$$V \text{ est irréductible} \iff \text{End}_G(V) = \text{CIId}_V$$

Le théorème qui suit fournit un critère commode pour savoir si des représentations sont isomorphes.

Théorème D.4. Soient V et W des représentations d'un groupe fini G . Alors

$$V \text{ et } W \text{ sont isomorphes} \iff \chi_V = \chi_W$$

où χ_V et χ_W sont les caractères respectifs de V et W .

la preuve du sens \Rightarrow est facile : soit $f : V \rightarrow W$ un isomorphisme de représentations. On a $\pi_W(g) \circ f = f \circ \pi_V(g)$ pour tout $g \in G$, donc $\pi_W(g) = f \circ \pi_V(g) \circ f^{-1}$, et $\chi_W(g) = \text{Tr}(f \circ \pi_V(g) \circ f^{-1}) = \text{Tr}(\pi_V(g)) = \chi_V(g)$, ce qui donne le résultat. Le sens \Leftarrow sera démontré dans le paragraphe sur les caractères.

Le but des paragraphes qui suivent est de démontrer les trois théorèmes énoncés ici, avec aussi des résultats intermédiaires intéressants. Le point 5 du théorème de structure a déjà été démontré.

On travaille désormais avec un groupe fini fixé G .

E Représentations unitaires et complète réductibilité des représentations

E.1 Groupe unitaire

Soit H un espace de Hilbert complexe de dimension finie (on dit aussi que H est un espace hermitien), c'est-à-dire que H est muni d'un produit scalaire : $\langle , \rangle : H \times H \rightarrow \mathbb{C}$, (\langle , \rangle est semi-linéaire en la deuxième variable).

Rappelons qu'à tout opérateur $u \in \text{End}_{\mathbb{C}}(H)$ correspond un unique opérateur $u^* \in \text{End}_{\mathbb{C}}(H)$, appelé l'adjoint de u , satisfaisant à

$$\langle u(x), y \rangle = \langle x, u^*(y) \rangle, \quad \forall x, y \in H.$$

On a, pour tous $u, v \in \text{End}_{\mathbb{C}}(H)$ et tout $\lambda \in \mathbb{C}$

$$u^{**} = u, (\lambda u)^* = \bar{\lambda} u^*, (u \circ v)^* = v^* \circ u^*, (u + v)^* = u^* + v^*.$$

Définition E.1. Un opérateur $u \in \text{End}_{\mathbb{C}}(H)$ est dit **unitaire** si $u^* \circ u = \text{id}_H = u \circ u^*$. On note $U(H)$ l'ensemble des opérateurs unitaires sur H . C'est un sous-groupe de $GL(H)$, appelé le **groupe unitaire de H** . Le **groupe spécial unitaire de H** , noté $SU(H)$, est défini par $SU(H) = SL(H) \cap U(H)$.

Pour $u \in \text{End}_{\mathbb{C}}(H)$, comme H est de dimension finie, on a $u \in U(H) \iff u^* \circ u = \text{Id}_H \iff u \circ u^* = \text{Id}_H$. On a diverses caractérisations des opérateurs unitaires.

Proposition E.2. Soit $u \in \text{End}_{\mathbb{C}}(H)$. Les assertions suivantes sont équivalentes.

1. $u \in U(H)$.
2. $\forall x, y \in H$, on a $\langle u(x), u(y) \rangle = \langle x, y \rangle$.
3. Pour toute base orthonormée (e_1, \dots, e_n) de H , alors $(u(e_1), \dots, u(e_n))$ est une base orthonormée de H .
4. Il existe une base orthonormée (e_1, \dots, e_n) de H telle que $(u(e_1), \dots, u(e_n))$ est une base orthonormée de H .

Preuve. (1) \Rightarrow (2). Soit $u \in U(H)$ et soient $x, y \in H$. Alors $\langle u(x), u(y) \rangle = \langle x, u^*(u(y)) \rangle = \langle x, y \rangle$.

(2) \Rightarrow (3). On a $\langle u(e_i), u(e_j) \rangle = \langle e_i, e_j \rangle = \delta_{ij}$, et ainsi $(u(e_1), \dots, u(e_n))$ est une base orthonormée de H .

(3) \Rightarrow (4) : immédiat.

(4) \Rightarrow (2). Soient $x = \sum_i \lambda_i e_i$ et $y = \sum_i \mu_i e_i \in H$. On a $\langle u(x), u(y) \rangle = \sum_{i,j} \lambda_i \bar{\mu}_j \langle u(e_i), u(e_j) \rangle = \sum_i \lambda_i \bar{\mu}_i = \langle x, y \rangle$.

(2) \Rightarrow (1). Soient $x, y \in H$. On a

$$\langle x, u^* \circ u(y) - y \rangle = \langle x, u^*(u(y)) \rangle - \langle x, y \rangle = \langle u(x), u(y) \rangle - \langle x, y \rangle = 0.$$

Donc puisque \langle , \rangle est un produit scalaire sur H , on a $u^* \circ u = \text{Id}_H$. \square .

On peut montrer qu'un opérateur unitaire est diagonalisable dans une base orthonormée, ce que nous n'utiliserons pas. Un ingrédient de la preuve est le lemme suivant, qui sera quant à lui utile très bientôt.

Lemme E.3. Soit $u \in \mathbf{U}(H)$ et soit $W \subset H$ un sous-espace vectoriel tel que $u(W) \subset W$. Alors $u(W^\perp) \subset W^\perp$.

Preuve. On a $u(W) = W$ car on est en dimension finie et u est un isomorphisme. Ainsi $u^*(W) = u^{-1}(W) = W$. Pour $x \in W$ et $y \in W^\perp$, on a donc $\langle u(y), x \rangle = \langle y, u^*(x) \rangle = 0$, ce qui montre que $u(W^\perp) \subset W^\perp$. \square

Fixons une base orthonormée de H . Si A est la matrice d'un opérateur u dans cette base on vérifie sans difficulté que la matrice de u^* est la matrice adjointe $A^* = {}^t\bar{A} = (\bar{a}_{ji})$.

L'opérateur u est unitaire si et seulement $A^*A = I_n = AA^*$. Ce langage se transmet donc aux matrices. On définit ainsi les groupes unitaires et spéciaux unitaires

$$\mathbf{U}(n) = \{A \in \mathcal{M}_n(\mathbb{C}) \mid A^*A = I_n = AA^*\}, \quad \mathbf{SU}(n) = \mathbf{SL}_n(\mathbb{C}) \cap \mathbf{U}(n),$$

qui s'identifient aux groupes unitaires de l'espace de Hilbert \mathbb{C}^n avec son produit scalaire canonique (l'unique produit scalaire tel que la base canonique soit orthonormée).

E.2 Représentations unitaires

Définition E.4. Une *représentation unitaire* d'un groupe fini G est la donnée d'un morphisme de groupes $\pi : G \rightarrow \mathbf{U}(H)$ pour un espace de Hilbert H .

Une représentation unitaire est donc en particulier une représentation linéaire. En fait le résultat suivant montre que toute représentation linéaire peut être considérée comme unitaire.

Théorème E.5. Soit V une représentation de G . Alors il existe un produit scalaire $\langle \cdot, \cdot \rangle$ sur V qui est G -invariant :

$$\langle g.v, g.w \rangle = \langle v, w \rangle, \quad \forall g \in G, \forall v, w \in V.$$

Si on note $H = (V, \langle \cdot, \cdot \rangle)$ l'espace de Hilbert correspondant, le morphisme de groupes $\pi_V : G \rightarrow \mathbf{GL}(V)$ est alors à valeurs dans $\mathbf{U}(H)$.

Preuve. Soit (\cdot, \cdot) un produit scalaire quelconque sur V . On pose alors, pour $v, w \in V$,

$$\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} (g.v, g.w).$$

On vérifie sans problème que $\langle \cdot, \cdot \rangle$ est un produit scalaire sur G . Pour $h \in G$, on a

$$\begin{aligned} \langle h.v, h.w \rangle &= \frac{1}{|G|} \sum_{g \in G} (g.(h.v), g.(h.w)) = \\ &= \frac{1}{|G|} \sum_{g \in G} ((gh).v, (gh).w) = \frac{1}{|G|} \sum_{g' \in G} (g'.v, g'.w) = \langle v, w \rangle \end{aligned}$$

où on a effectué le changement de variables (bijectif) $g' = gh$. La dernière assertion est alors immédiate. \square

Le résultat précédent est important, voici les premières applications.

Théorème E.6. Soit V une représentation de G et soit $W \subset V$ une sous-représentation de G . Alors il existe une sous-représentation $Z \subset V$ de G telle que $V = W \oplus Z$.

Preuve. On considère un produit scalaire invariant \langle, \rangle sur V , et soit $Z = W^\perp$. On a $V = W \oplus W^\perp$. Soit $g \in G$, on a $\pi_V(g)(W) \subset W$, donc par le lemme E.3, puisque $\pi_V(g)$ est unitaire, on a $\pi_V(g)(W^\perp) \subset W^\perp$, ce qui montre que W^\perp est une sous-représentation de V . \square

On en déduit que toute représentation est somme directe de représentations irréductibles.

Théorème E.7. Soit V une représentation de G . Alors il existe $t \in \mathbb{N}$ et des représentations irréductibles V_1, \dots, V_t de G telles que $V \cong V_1 \oplus \dots \oplus V_t$.

Preuve. On procède par récurrence sur la dimension de V . Si $\dim V = 0$ on prend $t = 0$ et si $\dim V = 1$ la représentation est irréductible. Supposons donc le résultat montré pour les représentations de dimension $\leq n$ (avec $n \geq 1$) et soit V une représentation de dimension $n + 1$. Si V est irréductible, on a le résultat. Sinon, soit $W \subset V$ une sous-représentation telle que $\{0\} \subsetneq W \subsetneq V$, avec donc $1 \leq \dim W \leq n$. On considère alors une sous-représentation Z de V telle que $V = W \oplus Z$, avec $1 \leq \dim Z \leq n$. On applique l'hypothèse de récurrence à W et Z et on a le résultat. \square

F Le lemme de Schur

Proposition F.1. Soient V et W des représentations de G et soit $f \in \text{Hom}_G(V, W)$. Alors $\text{Ker } f$ est une sous-représentation de V et $\text{Im } f$ est une sous-représentation de W .

La preuve est laissée en exercice.

Théorème F.2 (Lemme de Schur). Soient V_1 et V_2 des représentations irréductibles de G .
 (i) Si V_1 et V_2 ne sont pas isomorphes, alors $\text{Hom}_G(V_1, V_2) = \{0\}$.
 (ii) Si $V_1 = V_2$, alors $\text{Hom}_G(V_1, V_1) = \mathbb{C}\text{Id}_{V_1}$.

Preuve. Soit $f \in \text{Hom}_G(V_1, V_2)$. D'après la proposition précédente $\text{Ker } f$ est une sous-représentation de V_1 et $\text{Im } f$ est une sous-représentation de V_2 . Comme V_1 et V_2 sont irréductibles, on a $\text{Ker } f = \{0\}$ ou $\text{Ker } f = V_1$, et $\text{Im } f = \{0\}$ ou $\text{Im } f = V_2$. Si $f \neq 0$, alors donc $\text{Ker } f = \{0\}$ et $\text{Im } f = V_2$, donc f est un isomorphisme. Ainsi si V_1 et V_2 ne sont pas isomorphes, on a bien $f = 0$ et $\text{Hom}_G(V_1, V_2) = \{0\}$.

Supposons maintenant que $V_1 = V_2 = V$ et soit $f \in \text{Hom}_G(V, V)$. Soit $\lambda \in \mathbb{C}$ une valeur propre de f . Alors $f - \lambda\text{Id}_V \in \text{Hom}_G(V, V)$ avec $\text{Ker}(f - \lambda\text{Id}_V) \neq \{0\}$. Comme V est irréductible, on a $\text{Ker}(f - \lambda\text{Id}_V) = V$, d'où $f = \lambda\text{Id}_V$, et on a le résultat. \square

On démontre maintenant sans difficulté le critère d'irréductibilité déjà annoncé.

Théorème F.3. Soit V une représentation de G . Alors

$$V \text{ est irréductible } \iff \text{End}_G(V) = \mathbb{C}\text{Id}_V$$

Preuve. Le sens \Rightarrow est donné par la partie ii du lemme de Schur. Réciproquement, si V n'est pas irréductible, on a $V = U \oplus W$ pour des sous-représentations non nulles U et W . On a alors

$$\begin{aligned} \text{End}_G(V, V) &= \text{Hom}_G(U \oplus W, U \oplus W) \\ &\cong \text{Hom}_G(U, U) \oplus \text{Hom}_G(U, W) \oplus \text{Hom}_G(W, U) \oplus \text{Hom}_G(W, W) \end{aligned}$$

et donc $\dim(\text{End}_G(V)) \geq 2$, ce qui donne le résultat. \square

G Invariants et moyenne

Définition-Proposition G.1. Soit V une représentation de G . On considère

$$V^G = \{v \in V \mid g.v = v, \forall g \in G\}.$$

Alors V^G est un sous-espace de V , appelé espace des G -invariants de V .

On vérifie sans difficulté que V^G est bien un sous-espace de V (c'est même une sous-représentation). La proposition qui suit permet de construire tous les G -invariants.

Définition-Proposition G.2. Soit V une représentation de G . On considère l'application

$$\begin{aligned} M : V &\longrightarrow V \\ v &\longmapsto \frac{1}{|G|} \sum_{g \in G} g.v \end{aligned}$$

Alors M est application linéaire, appelée **l'opérateur de moyenne de V** . L'opérateur M est un projecteur ($M \circ M = M$) d'image égale à V^G .

Preuve. On a $M = \frac{1}{|G|} \sum_{g \in G} \pi_V(g)$, donc M est linéaire. On a

$$\begin{aligned} M \circ M &= \frac{1}{|G|^2} \sum_{g,h \in G} \pi_V(g) \circ \pi_V(h) = \frac{1}{|G|^2} \sum_{g,h \in G} \pi_V(gh) \\ &= \frac{1}{|G|^2} \sum_{g,g' \in G} \pi_V(g') = \frac{1}{|G|} \sum_{g \in G} \frac{1}{|G|} \sum_{g' \in G} \pi_V(g') = M, \end{aligned}$$

donc M est bien un projecteur. Pour $v \in V$ et $h \in G$, on a

$$h.M(v) = \frac{1}{|G|} \sum_{g \in G} h.(g.v) = \frac{1}{|G|} \sum_{g \in G} (hg).v = \frac{1}{|G|} \sum_{g \in G} g.v = M(v)$$

donc $M(v) \in V^G$, et $\text{Im } M \subset V^G$. Réciproquement si $v \in V^G$, on a $M(v) = \frac{1}{|G|} \sum_{g \in G} g.v = \frac{1}{|G|} \sum_{g \in G} v = v$, donc $v \in \text{Im } M$ et $V^G \subset \text{Im } M$. \square

On applique alors cela aux applications linéaires entre représentations.

Corollaire G.3. Soient V et W des représentations de G et soit $f : V \longrightarrow W$ une application linéaire. Alors l'application linéaire $M(f) : V \longrightarrow W$ définie par

$$M(f) = \frac{1}{|G|} \sum_{g \in G} \pi_W(g) \circ f \circ \pi_V(g^{-1})$$

appartient à $\text{Hom}_G(V, W)$. De plus si $V = W$, on a $\text{Tr}(M(f)) = \text{Tr}(f)$.

Preuve. On considère la représentation de G sur $\text{Hom}(V, W)$, donnée par $g.f = \pi_W(g) \circ f \circ \pi_V(g^{-1})$ pour $g \in G$. Alors il est immédiat que $f \in \text{Hom}(V, W)^G \iff f \in \text{Hom}_G(V, W)$, donc puisque le

$M(f)$ décrit plus haut est l'opérateur de moyenne de la représentation $\text{Hom}(V, W)$ appliqué à f , on a bien $M(f) \in \text{Hom}_G(V, W) = \text{Hom}(V, W)^G$.

Si $V = W$, alors

$$\text{Tr}(M(f)) = \frac{1}{|G|} \left(\sum_{g \in G} \text{Tr}(\pi_W(g) \circ f \circ \pi_V(g^{-1})) \right) = \frac{1}{|G|} \sum_{g \in G} \text{Tr}(f) = \text{Tr}(f). \quad \square$$

H Relations d'orthogonalité et applications

On note $L^2(G)$ l'espace vectoriel \mathbb{C}^G des fonctions de G dans \mathbb{C} muni du produit scalaire

$$\langle \phi, \psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

Les relations d'orthogonalité expriment l'orthogonalité, dans $L^2(G)$, de certaines fonctions associées à des représentations irréductibles. Elles auront en particulier comme conséquence le fait que l'ensemble $\text{Irr}(G)$ des classes d'isomorphismes de représentations irréductibles de G est fini.

Introduisons quelques notations.

1. Soient V et W des espaces vectoriels et $f \in V^*$, $x \in W$. On note $x \otimes f$ l'application linéaire $V \rightarrow W$ définie par $(x \otimes f)(v) = f(v)x$.

2. Soit V une représentation de G et notons $\pi : G \rightarrow \text{GL}(V)$ le morphisme de groupes correspondant. Soit v_1, \dots, v_n une base de V , et notons π_{ij} , $1 \leq i, j \leq n = \dim V$, les fonctions coordonnées sur G associées à l'identification $\text{GL}(V) \cong \text{GL}_n(\mathbb{C})$ donnée par la base, de telle sorte que

$$\forall g \in G, \quad \pi(g) = \sum_{i,j=1}^n \pi_{ij}(g) v_i \otimes v_j^*.$$

Théorème H.1 (Relations d'orthogonalité, première version). Soient V et W des représentations irréductibles de G avec $n = \dim V$ et $m = \dim W$. Notons $\pi : G \rightarrow \text{GL}(V)$ et $\rho : G \rightarrow \text{GL}(W)$ les morphismes de groupes correspondant, et $(\pi_{ij})_{1 \leq i, j \leq n}$ et $(\rho_{kl})_{1 \leq k, l \leq m}$, les fonctions coordonnées sur G associées au choix de bases de V et W .

(i) Si V et W ne sont pas isomorphes, alors on a

$$\frac{1}{|G|} \sum_{g \in G} \rho_{kl}(g) \pi_{ij}(g^{-1}) = 0, \quad 1 \leq i, j \leq n, 1 \leq k, l \leq m$$

(ii) Si $V = W$ ($\pi = \rho$), alors on a

$$\frac{1}{|G|} \sum_{g \in G} \pi_{kl}(g) \pi_{ij}(g^{-1}) = \frac{\delta_{kj} \delta_{il}}{n}, \quad 1 \leq i, j, k, l \leq n.$$

Preuve. On va obtenir le résultat en faisant la moyenne de certains opérateurs de rang 1 et en appliquant le lemme de Schur. Soient donc v_1, \dots, v_n et w_1, \dots, w_m des bases respectives de V et W , et soient

(π_{ij}) et (ρ_{ij}) les fonctions coordonnées sur G associées. Soient $i_0 \in \{1, \dots, n\}$ et $k_0 \in \{1, \dots, m\}$. Alors

$$\begin{aligned}
M(w_{k_0} \otimes v_{i_0}^*) &= \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ (w_{k_0} \otimes v_{i_0}^*) \circ \pi(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j=1}^n \sum_{k,l=1}^m \rho_{kl}(g) \pi_{ij}(g^{-1}) (w_k \otimes w_l^*) \circ (w_{k_0} \otimes v_{i_0}^*) \circ (v_i \otimes v_j^*) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{j=1}^n \sum_{k=1}^m \rho_{kk_0}(g) \pi_{i_0j}(g^{-1}) (w_k \otimes v_j^*) \\
&= \sum_{j=1}^n \sum_{k=1}^m \left(\frac{1}{|G|} \sum_{g \in G} \rho_{kk_0}(g) \pi_{i_0j}(g^{-1}) \right) (w_k \otimes v_j^*) \in \text{Hom}_G(V, W).
\end{aligned}$$

(i) Supposons V et W non isomorphes. Alors d'après le lemme de Schur $\text{Hom}_G(V, W) = \{0\}$, donc l'opérateur précédent est nul, et puisque $(w_k \otimes v_j^*)$ est une base de $\text{Hom}(V, W)$, chaque coefficient est nul, et on a les relations recherchées.

(ii) Supposons maintenant que $V = W$. Toujours par le lemme de Schur, on obtient $M(v_{k_0} \otimes v_{i_0}^*) = \lambda \text{Id}_V$, pour

$$\lambda = \frac{\text{Tr}(M(v_{k_0} \otimes v_{i_0}^*))}{n} = \frac{\text{Tr}(v_{k_0} \otimes v_{i_0}^*)}{n} = \frac{\delta_{i_0 k_0}}{n}.$$

On a $\text{Id}_V = \sum_j v_j \otimes v_j^*$, donc en identifiant on trouve bien

$$\frac{1}{|G|} \sum_{g \in G} \pi_{kk_0}(g) \pi_{i_0j}(g^{-1}) = \delta_{kj} \lambda = \frac{\delta_{kj} \delta_{i_0 k_0}}{n}. \quad \square$$

On obtient maintenant les relations d'orthogonalité dans $L^2(G)$.

Théorème H.2 (Relations d'orthogonalité dans $L^2(G)$). Pour chaque $\alpha \in \text{Irr}(G)$, fixons V_α une représentation de G telle que $\alpha = [V_\alpha]$, avec $\pi^\alpha : G \rightarrow \text{GL}(V_\alpha)$ le morphisme de groupe correspondant. Notons $d_\alpha = \dim V_\alpha$. Fixons sur V_α un produit scalaire G -invariant et une base orthonormée pour ce produit scalaire, et notons (π_{ij}^α) les fonctions coordonnées sur G associées. Alors on a

$$\langle \pi_{ij}^\alpha, \pi_{kl}^\beta \rangle_G = \frac{\delta_{\alpha\beta} \delta_{ik} \delta_{jl}}{d_\alpha}, \quad \forall \alpha, \beta \in \text{Irr}(G), 1 \leq i, j \leq d_\alpha, 1 \leq k, l \leq d_\beta.$$

Preuve. Pour $\alpha \in \text{Irr}(G)$, on a choisi un produit scalaire invariant sur V_α , donc si on note H_α l'espace de Hilbert associé, on a $\pi^\alpha(G) \subset U(H_\alpha)$, et donc $\overline{\pi^\alpha(g^{-1})} = \pi^\alpha(g)^{-1} = \pi^\alpha(g)^*$, $\forall g \in G$. Au niveau des fonctions coordonnées, cela donne $\overline{\pi_{ij}^\alpha(g^{-1})} = \pi_{ji}^\alpha(g)$, pour $1 \leq i, j \leq d_\alpha$. On a alors

$$\langle \pi_{ij}^\alpha, \pi_{kl}^\beta \rangle_G = \frac{1}{|G|} \sum_{g \in G} \pi_{ij}^\alpha(g) \overline{\pi_{kl}^\beta(g)} = \frac{1}{|G|} \sum_{g \in G} \pi_{ij}^\alpha(g) \pi_{lk}^\beta(g^{-1}) = \frac{\delta_{\alpha\beta} \delta_{ik} \delta_{jl}}{d_\alpha}$$

où l'on a utilisé la première version des relations d'orthogonalité. \square

Corollaire H.3. L'ensemble $\text{Irr}(G)$ des classes de représentations irréductibles de G est fini. On notera $s = |\text{Irr}(G)|$. Si W_1, \dots, W_s sont des représentations de G telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$, alors on a $\sum_{i=1}^s d_i^2 \leq |G|$, où $d_i = \dim W_i$, $\forall i$.

Preuve. En reprenant les notations des relations d'orthogonalité, on voit que $\{\pi_{ij}^\alpha, \alpha \in \text{Irr}(G), 1 \leq i, j \leq d_\alpha\}$ est une famille d'éléments non nuls de $L^2(G)$ qui sont deux à deux orthogonaux. C'est donc une famille libre de $L^2(G)$, qui est de dimension finie égale à $|G|$. On obtient donc à la fois que $\text{Irr}(G)$ est fini et l'inégalité du corollaire. \square

On veut en fait démontrer que l'inégalité précédente est une égalité. Pour cela il faut démontrer que $\{\pi_{ij}^\alpha, \alpha \in \text{Irr}(G), 1 \leq i, j \leq d_\alpha\}$ est une base de $L^2(G)$ (on utilise toujours les notations des relations d'orthogonalité). Pour cela on introduit une transformation \mathcal{F} sur les fonctions de $L^2(G)$, qui est un peu un analogue de la transformée de Fourier sur $L^2(\mathbb{S}^1)$.

Lemme H.4. Soit $\phi \in \mathbb{C}^G$, et soit V une représentation de G . On considère l'application linéaire $\mathcal{F}_V : \mathbb{C}[G] \rightarrow \text{End}(V)$ définie par

$$\mathcal{F}_V(\phi) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_V(g) \in \text{End}(V).$$

1. Si v_1, \dots, v_n est une base de V et si (π_{ij}) sont les fonctions coordonnées sur G correspondantes, on a

$$\mathcal{F}_V(\phi) = \sum_{i,j=1}^n \langle \pi_{ij}, \phi \rangle_G v_i \otimes v_j^*.$$

2. Si V et W sont des représentations de G , on a $\mathcal{F}_{V \oplus W}(\phi) = \mathcal{F}_V(\phi) \oplus \mathcal{F}_W(\phi)$

3. Soient V et W des représentations de G et soit $f : V \rightarrow W$ un G -isomorphisme. Alors on a $\mathcal{F}_W(\phi) = f \circ \mathcal{F}_V(\phi) \circ f^{-1}$.

Preuve. 1. On a

$$\begin{aligned} \mathcal{F}_V(\phi) &= \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_V(g) = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j=1}^n \overline{\phi(g)} \pi_{ij}(g) v_i \otimes v_j^* \\ &= \sum_{i,j=1}^n \left(\frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_{ij}(g) \right) v_i \otimes v_j^* = \sum_{i,j=1}^n \langle \pi_{ij}, \phi \rangle_G v_i \otimes v_j^* \end{aligned}$$

2. On a

$$\begin{aligned} \mathcal{F}_{V \oplus W}(\phi) &= \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_{V \oplus W}(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} (\pi_V(g), \pi_W(g)) \\ &= \left(\frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_V(g), \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_W(g) \right) = \mathcal{F}_V(\phi) \oplus \mathcal{F}_W(\phi). \end{aligned}$$

3. Pour tout $g \in G$, on a $\pi_W(g) \circ f = f \circ \pi_V(g)$, c'est-à-dire $\pi_W(g) = f \circ \pi_V(g) \circ f^{-1}$, d'où le résultat. \square

Théorème H.5 (Théorème de Peter-Weyl pour les groupes finis). On reprend les notations utilisées pour l'énoncé des relations d'orthogonalité. Alors

$$\left\{ \sqrt{d_\alpha} \pi_{ij}^\alpha, \alpha \in \text{Irr}(G), 1 \leq i, j \leq d_\alpha \right\}$$

est une base orthonormée de $L^2(G)$. En particulier

$$\sum_{\alpha \in \text{Irr}(G)} d_\alpha^2 = |G|.$$

Preuve. On sait déjà des relations d'orthogonalité que le système donné est orthonormé, et il faut donc voir que l'on a une base de $L^2(G)$. Soit W le sous-espace de $L^2(G)$ engendré par notre système. Pour voir que $W = L^2(G)$, il suffit de voir que $W^\perp = \{0\}$. Soit donc $\phi \in W^\perp$. En utilisant le 1 du lemme précédent on voit que $\forall \alpha \in \text{Irr}(G)$, on a

$$\mathcal{F}_{V_\alpha}(\phi) = \sum_{i,j=1}^{d_\alpha} \langle \pi_{ij}, \phi \rangle_G v_i \otimes v_j^* = 0.$$

Donc si V est une représentation irréductible quelconque de G , on a $\mathcal{F}_V(\phi) = 0$ d'après la partie 3 du lemme. Si maintenant V est une représentation quelconque de G , elle est somme directe de représentations irréductibles, et on a $\mathcal{F}_V(\phi) = 0$ d'après la partie 2 du lemme.

On applique maintenant ceci à la représentation régulière $R = \mathbb{C}^G$ obtenue en utilisant l'opération de G sur lui-même par translations. Pour $g, x \in G$, on a $\pi_R(g)(e_x) = e_{gx}$. Donc

$$\mathcal{F}_R(\phi)(e_1) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_R(g)(e_1) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} e_g = 0$$

et puisque $(e_g)_{g \in G}$ est une base de \mathbb{C}^G , on conclut que $\phi = 0$. Donc $W^\perp = \{0\}$ et $L^2(G) = W$. La dimension de $L^2(G)$ est $|G|$, et doit être égale au cardinal d'une base quelconque. \square

Corollaire H.6. Soient W_1, \dots, W_s sont des représentations irréductibles de G telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$, où $s = |\text{Irr}(G)|$. Alors on a

$$\sum_{i=1}^s d_i^2 = |G|, \text{ avec } d_i = \dim W_i, \forall i.$$

Preuve. Chaque W_i est isomorphe à exactement un V_α , donc on applique simplement le résultat précédent. \square

I Structure de l'algèbre du groupe

L'objectif est maintenant de montrer que $s = |\text{Irr}(G)|$ est égal au nombre de classes de conjugaison de G . On démontrera au passage le premier théorème de l'introduction.

Soit (V, π_V) une représentation de G . On sait qu'il existe un unique morphisme d'algèbres

$$\widetilde{\pi}_V : \mathbb{C}[G] \longrightarrow \text{End}(V)$$

tel que $\widetilde{\pi}_V(e_g) = \pi_V(g), \forall g \in G$.

En fait pour $\phi \in \mathbb{C}[G]$, on a $\widetilde{\pi}_V(\phi) = |G| \mathcal{F}_V(\overline{\phi})$, où \mathcal{F}_V a été introduit dans le paragraphe précédent. Cela nous permet de montrer facilement le résultat suivant.

Théorème I.1. Soient W_1, \dots, W_s sont des représentations irréductibles de G telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$, où $s = |\text{Irr}(G)|$. Alors on a un isomorphisme d'algèbres

$$\begin{aligned} \Omega : \mathbb{C}[G] &\longrightarrow \prod_{i=1}^s \text{End}(W_i) \\ \phi &\longmapsto (\widetilde{\pi}_{W_i}(\phi))_{1 \leq i \leq s} \end{aligned}$$

Preuve. Chaque $\widetilde{\pi_{W_i}}$ est un morphisme d'algèbres, donc il est facile de voir que Ω est bien un morphisme d'algèbres. On a $\dim(\mathbb{C}[G]) = |G| = \sum_{i=1}^s (\dim W_i)^2 = \dim(\prod_{i=1}^s \text{End}(W_i))$, donc il suffit donc de voir que Ω est injectif. Soit alors $\phi \in \text{Ker } \Omega$: on a $\widetilde{\pi_{W_i}}(\phi) = 0 = \mathcal{F}_{W_i}(\bar{\phi}), \forall i$. On peut raisonner de la même façon que dans la preuve du théorème de Peter-Weyl : on a $\mathcal{F}_V(\bar{\phi}) = 0$ pour toute représentation V et on applique cela à la représentation régulière pour trouver que $\bar{\phi} = 0 = \phi$. \square

On va maintenant utiliser ce théorème pour déterminer s . Si A est une algèbre, on considère son centre $Z(A) = \{a \in A \mid ab = ba, \forall b \in A\}$. C'est une sous-algèbre de A , et donc aussi une algèbre. Si A et B sont des algèbres, alors une vérification immédiate donne $Z(A \times B) = Z(A) \times Z(B)$. Donc en reprenant les notations précédentes, on a

$$Z\left(\prod_{i=1}^s \text{End}(W_i)\right) = \prod_{i=1}^s Z(\text{End}(W_i)) \cong \mathbb{C}^s$$

puisque le centre d'une algèbre de matrices est réduit à \mathbb{C} , et donc

$$\dim(Z(\prod_{i=1}^s \text{End}(W_i))) = s.$$

Théorème I.2. Le nombre $s = |\text{Irr}(G)|$ de classes d'isomorphisme de représentations irréductibles de G est égal au nombre de classes de conjugaison de G .

Preuve. L'isomorphisme d'algèbres $\mathbb{C}[G] \cong \prod_{i=1}^s \text{End}(W_i)$ induit un isomorphisme entre les centres, qui ont donc même dimension, égale à s . On a vu au chapitre 3 que $\dim(Z(\mathbb{C}[G]))$ est égal au nombre de classe de conjugaison de G , d'où le résultat. \square

Fin de la démonstration des points 1, 2 et 3 du théorème de structure des représentations d'un groupe fini.

On vient de finir la preuve de la partie 1, et la partie 3 a été démontrée au paragraphe précédent. Passons au point 2. Soit V une représentation de G et soient W_1, \dots, W_s des représentations irréductibles telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$. Alors V est somme directe de représentations irréductibles, chacune isomorphe à l'un des W_i , donc on a un isomorphisme de représentations

$$V \cong \bigoplus_{i=1}^s W_i^{n_i}$$

pour des entiers $n_1, \dots, n_s \in \mathbb{N}$. Pour $j \in \{1, \dots, s\}$, on a, en utilisant le lemme de Schur,

$$\begin{aligned} \text{Hom}_G(W_j, V) &\cong \text{Hom}_G(W_j, \bigoplus_{i=1}^s W_i^{n_i}) \cong \bigoplus_{i=1}^s \text{Hom}_G(W_j, W_i)^{n_i} \\ &= \text{Hom}_G(W_j, W_j)^{n_j} \cong \mathbb{C}^{n_j} \end{aligned}$$

donc $n_j = \dim(\text{Hom}_G(W_j, V))$. Cela termine la démonstration du point 2.

J Caractères

Rappelons la définition du caractère d'une représentation.

Définition J.1. Soit (V, π_V) une représentation de G . Le **caractère de V** est la fonction $\chi_V : G \rightarrow \mathbb{C}$ définie par

$$\chi_V(g) = \text{Tr}(\pi_V(g)), \quad \forall g \in G.$$

On dit qu'une fonction $\chi : G \rightarrow \mathbb{C}$ est un **caractère** si χ est le caractère d'une représentation de G .

Voici les premières propriétés des caractères.

Proposition J.2. Soient V et W des représentations de G .

1. $\chi_V(1) = \dim V$.
2. Si les représentations V et W sont isomorphes, alors $\chi_V = \chi_W$.
3. On a $\forall g, h \in G, \chi_V(gh) = \chi_V(hg)$, et ainsi χ_V est une fonction centrale sur G .
4. On a $\chi_{V \oplus W} = \chi_V + \chi_W$.

Preuve. On a $\chi_V(1) = \text{Tr}(\pi_V(1)) = \text{Tr}(\text{id}_V) = \dim V$. La deuxième assertion a déjà été montrée. Pour $g, h \in G$ on a $\chi_V(gh) = \text{Tr}(\pi_V(gh)) = \text{Tr}(\pi_V(g) \circ \pi_V(h)) = \text{Tr}(\pi_V(h) \circ \pi_V(g)) = \text{Tr}(\pi_V(hg)) = \chi_V(hg)$. La dernière assertion se montre sans difficulté à partir de l'écriture matricielle de $\pi_{V \oplus W}$. \square

Théorème J.3 (Relations d'orthogonalité des caractères). Soient V et W des représentations irréductibles de G . Alors dans $L^2(G)$ on a

$$\langle \chi_V, \chi_W \rangle_G = \begin{cases} 0 & \text{si } V \text{ et } W \text{ ne sont pas isomorphes,} \\ 1 & \text{si } V \text{ et } W \text{ sont isomorphes.} \end{cases}$$

Preuve. Notons $\pi : G \rightarrow \text{GL}(V)$ et $\rho : G \rightarrow \text{GL}(W)$ les morphismes de groupes correspondant. On fixe sur V et W des produits scalaires G -invariants et soient v_1, \dots, v_n et w_1, \dots, w_m des bases orthonormées respectives de V et W pour ces produits scalaires. On note (π_{ij}) et (ρ_{kl}) les fonctions coordonnées associées sur G . On a

$$\chi_V = \sum_{i=1}^n \pi_{ii} \quad \text{et} \quad \chi_W = \sum_{k=1}^m \rho_{kk}$$

et donc

$$\langle \chi_V, \chi_W \rangle_G = \sum_{i,k} \langle \pi_{ii}, \rho_{kk} \rangle_G.$$

Les relations d'orthogonalité dans $L^2(G)$ assurent alors que $\langle \chi_V, \chi_W \rangle_G = 0$ si $V \not\cong W$. Si $V \cong W$ on a $\chi_V = \chi_W$ par le 2 de la proposition précédente, on peut donc supposer que $V = W$, et alors, toujours grâce aux relations d'orthogonalité dans $L^2(G)$, on a

$$\langle \chi_V, \chi_V \rangle_G = \sum_{i=1}^n \langle \pi_{ii}, \pi_{ii} \rangle_G = \frac{\dim V}{\dim V} = 1. \quad \square$$

Corollaire J.4. Soient V et W des représentations de G avec V irréductible. Alors

$$\langle \chi_V, \chi_W \rangle_G = \dim(\text{Hom}_G(V, W)).$$

Preuve. Soient W_1, \dots, W_s des représentations irréductibles de G telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$, où $s = |\text{Irr}(G)|$. Alors

$$W \cong \bigoplus_{i=1}^s W_i^{m_i}$$

pour $n_i = \dim(\text{Hom}_G(W_i, W))$. On a alors, en utilisant la première proposition, $\chi_W = \sum_{i=1}^s n_i \chi_{W_i}$. Soit i_0 tel que $V \cong W_{i_0} : \chi_V = \chi_{W_{i_0}}$. On a donc, en utilisant les relations d'orthogonalité des caractères,

$$\langle \chi_V, \chi_W \rangle_G = \sum_{i=1}^n n_i \langle \chi_{W_{i_0}}, \chi_{W_i} \rangle = n_{i_0} = \dim(\text{Hom}_G(W_{i_0}, W)) = \dim(\text{Hom}_G(V, W)). \quad \square$$

On arrive alors au résultat important suivant.

Théorème J.5. Soient V et W des représentations d'un groupe fini G . Alors

$$V \text{ et } W \text{ sont isomorphes} \iff \chi_V = \chi_W.$$

Preuve. Soit W_1, \dots, W_s un système complet de représentations irréductibles de G . Alors

$$V \cong \bigoplus_{i=1}^s W_i^{n_i} \quad \text{et} \quad V \cong \bigoplus_{i=1}^s W_i^{m_i}$$

pour $n_i = \dim(\text{Hom}_G(W_i, V))$ et $m_i = \dim(\text{Hom}_G(W_i, W))$. Donc si $\chi_V = \chi_W$, on a pour tout i

$$n_i = \dim(\text{Hom}_G(W_i, V)) = \langle \chi_{W_i}, \chi_V \rangle = \langle \chi_{W_i}, \chi_W \rangle = \dim(\text{Hom}_G(W_i, W)) = m_i.$$

Il est clair alors que V et W sont isomorphes. \square

Proposition J.6. Soit χ un caractère sur G . Alors $\forall g \in G, \chi(g) \in \mathbb{C}$ est un entier algébrique.

Preuve. Soit V une représentation de G telle que $\chi = \chi_V$. Pour $g \in G$, on a $g^{|G|} = 1$ donc $\pi_V(g)^{|G|} = \text{id}_V$, donc les valeurs propres de $\pi_V(g)$ sont des racines de l'unités, donc des entiers algébriques. Alors $\chi(g)$ qui est la trace de $\pi_V(g)$, est la somme des valeurs propres de $\pi_V(g)$, est un entier algébrique (voir chapitre IV). \square

Proposition J.7. Soit χ le caractère d'une représentation irréductible de dimension d de G . Soit C une classe de conjugaison de G . Alors pour tout $g \in C, \frac{|C|\chi(g)}{d}$ est un entier algébrique.

Preuve. $\mathbb{Z}[G]$ est un sous-anneau de $\mathbb{C}[G]$. Considérons $Z(\mathbb{Z}[G])$, le centre de $\mathbb{Z}[G]$. Les éléments de $Z(\mathbb{Z}[G])$ sont exactement les combinaisons linéaires à coefficients entiers des (x_C) , où C parcourt l'ensemble des classes de conjugaison de G (chapitre III). On en déduit que $Z(\mathbb{Z}[G])$ est un groupe abélien de type fini, donc ses éléments, et en particulier x_C pour chaque classe de conjugaison C , sont des entiers algébriques.

Soit (V, π_V) une représentation irréductible telle que $\chi = \chi_V$ et soit $\widetilde{\pi}_V : \mathbb{C}[G] \rightarrow \text{End}(V)$ le morphisme d'algèbre qui prolonge π_V . Soit C une classe de conjugaison de G . L'élément x_C appartient au centre de $\mathbb{C}[G]$, donc $\widetilde{\pi}_V(x_C)$ commute avec tous les $\pi_V(g)$, ce qui signifie que $\widetilde{\pi}_V(x_C) \in \text{End}_G(V)$. Par le lemme de Schur $\widetilde{\pi}_V(x_C) = \lambda \text{id}_V$ pour un $\lambda \in \mathbb{C}$. Puisqu'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x_C) = 0$, on a $\widetilde{\pi}_V(P(x_C)) = 0 = P(\widetilde{\pi}_V(x_C)) = P(\lambda) \text{Id}_V$, donc λ est entier algébrique. On obtient

$$\text{Tr}(\widetilde{\pi}_V(x_C)) = \text{Tr}\left(\sum_{g \in C} \pi_V(g)\right) = \sum_{g \in C} \chi_V(g) = |C|\chi(g) = d\lambda$$

et donc $\frac{|C|\chi(g)}{d} = \lambda$ est entier algébrique. \square

On arrive au résultat suivant, qui termine la démonstration du théorème de structure des représentations.

Théorème J.8. La dimension d'une représentation irréductible de G divise $|G|$.

Preuve. Soit V une représentation irréductible de dimension d de G , de caractère χ . Notons C_1, \dots, C_s les classes de conjugaison distinctes de G . Pour $g \in C_i$, on notera $\chi(C_i)$ la valeur de $\chi(g)$. On sait que $\langle \chi, \chi \rangle_G = 1$, ce qui, explicité, donne

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi(g)} = \frac{1}{|G|} \sum_{i=1}^r \sum_{g \in C_i} \chi(g) \overline{\chi(g)} = \frac{1}{|G|} \sum_{i=1}^r |C_i| \chi(C_i) \overline{\chi(C_i)}$$

ou encore

$$\frac{|G|}{\dim V} = \sum_{i=1}^r \frac{|C_i| \chi(C_i) \overline{\chi(C_i)}}{\dim V}$$

avec pour tout i , par les deux propositions précédentes, $\frac{|C_i| \chi(C_i)}{\dim V}$ et $\overline{\chi(C_i)}$ des entiers algébriques. Une somme d'entiers algébrique est encore un entier algébrique, donc $\frac{|G|}{\dim V}$ est entier algébrique et puisque $\frac{|G|}{\dim V} \in \mathbb{Q}$, on a bien $\frac{|G|}{\dim V} \in \mathbb{Z}$. \square

On termine ce paragraphe par en introduisant la table des caractères du groupe G . Soient C_1, \dots, C_s les classes de conjugaison de G avec la convention $C_1 = \{1\}$. Soient W_1, \dots, W_s des représentations irréductibles de G telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$, avec la convention que W_1 est la représentation triviale. Notons pour tout i , $\chi_i = \chi_{W_i}$. **La table des caractères de G** est alors le tableau suivant :

	$C_1 = \{1\}$	C_2	\dots	C_i	\dots	C_s
χ_1	1	1	\dots	1	\dots	1
χ_2	$d_2 = \chi_2(1)$	$\chi_2(C_2)$	\dots	$\chi_2(C_i)$	\dots	$\chi_2(C_s)$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
χ_j	$d_j = \chi_j(1)$	$\chi_j(C_2)$	\dots	$\chi_j(C_i)$	\dots	$\chi_j(C_s)$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
χ_s	$d_s = \chi_s(1)$	$\chi_s(C_2)$	\dots	$\chi_s(C_i)$	\dots	$\chi_s(C_s)$

L'usage quand on écrit la table des caractères est de remplacer les classes C_i par un représentant.

On considère que l'on a décrit de façon satisfaisante les représentations de G lorsque l'on a calculé sa table des caractères (qui bien sûr dépend de l'ordre choisi sur l'ensembles des classes de conjugaison et sur l'ensemble des classes d'isomorphismes de représentations irréductibles).

Exemple. La table des caractères du groupe symétrique S_3 est

	1	(1, 2)	(1, 2, 3)
χ_1	1	1	1
ε	1	-1	1
χ_2	2	0	-1

où χ_1 est la représentation triviale, ε est la signature, et χ_2 est le caractère de la représentation irréductible de degré 2.

Pour trouver les valeurs de χ_2 dans l'exemple précédent, on peut utiliser la description suivante de la représentation régulière (qui sera aussi utilisée dans le prochain paragraphe).

Proposition J.9. Notons χ_{reg} le caractère de la représentation régulière de G . On a

$$\chi_{\text{reg}}(g) = 0 \text{ si } g \neq 1 \quad \text{et} \quad \chi_{\text{reg}}(1) = |G|.$$

Soient W_1, \dots, W_s un système complet de représentations irréductibles de G . Notons $d_i = \dim W_i$ et $\chi_i = \chi_{W_i}$ pour tout i . Alors

$$\chi_{\text{reg}} = \sum_{i=1}^s d_i \chi_i.$$

Preuve. Notons $R = \mathbb{C}^G$ la représentation régulière de G . On utilise la base $(e_g)_{g \in G}$ de R . On a $\forall g, h \in G, \pi_R(g)(e_h) = e_{gh}$. Si $g \neq 1$, les termes diagonaux de la matrice de $\pi_R(g)$ dans cette base sont nuls ($gh \neq h$), donc $\chi_{\text{reg}}(g) = \text{Tr}(\pi_R(g)) = 0$. Le cas $g = 1$ est clair.

Pour $i \in \{1, \dots, s\}$, on a

$$\dim(\text{Hom}_G(W_i, R)) = \langle \chi_{W_i}, \chi_{\text{reg}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{W_i}(g) \overline{\chi_{\text{reg}}(g)} = \chi_{W_i}(1) = d_i.$$

Le théorème de structure des représentations assure alors que

$$R \cong \bigoplus_{i=1}^s W_i^{d_i}$$

et on a le résultat recherché en passant aux caractères. \square

Le résultat suivant est souvent utile pour construire une table de caractère, il exprime des relations d'“orthogonalité pondérée” pour les lignes et colonnes de la table des caractères.

Proposition J.10. Soient C_1, \dots, C_s les classes de conjugaison de G et soient χ_1, \dots, χ_r les caractères irréductibles de G . Alors la matrice

$$M = \left(\sqrt{\frac{|C_j|}{|G|}} \chi_i(C_j) \right) \in \mathcal{M}_s(\mathbb{C})$$

est unitaire, c'est-à-dire que

$$\sum_{k=1}^s \overline{\chi_k(C_i)} \chi_k(C_j) = \delta_{ij} \frac{|G|}{|C_i|} \quad \text{et} \quad \sum_{k=1}^s \chi_i(C_k) \overline{\chi_j(C_k)} |C_k| = \delta_{ij} |G|$$

En particulier les colonnes de la table des caractères sont deux à deux orthogonales.

Preuve. On applique les relations d'orthogonalité des caractères : $\langle \chi_i, \chi_j \rangle_G = \delta_{ij}$. \square

K Application : le théorème “pq” de Burnside

On démontre dans ce paragraphe le théorème de Burnside annoncé au début.

On aura besoin du lemme suivant, qui concerne les entiers algébriques, et que l'on ne montre pas.

Lemme K.1. Soient $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ des racines de l'unité. Supposons que $\frac{\lambda_1 + \dots + \lambda_n}{n}$ est un entier algébrique. Alors on a l'alternative suivante :

- soit $\lambda_1 + \dots + \lambda_n = 0$,
- soit $\lambda_1 = \dots = \lambda_n$.

Proposition K.2. Soit V une représentation irréductible de G . Soit C une classe de conjugaison de G et soit $g \in C$. Supposons que $\dim V$ et $|C|$ sont premiers entre eux. Alors $\frac{\chi_V(g)}{\dim V}$ est un entier algébrique. Si de plus $\chi_V(g) \neq 0$, alors $\pi_V(g)$ est une homothétie.

Preuve. Puisque $|C|$ et $\dim V$ sont premiers entre eux, le théorème de Bezout fournit $a, b \in \mathbb{Z}$ tels que $a|C| + b \dim V = 1$, ce qui donne

$$\frac{\chi_V(g)}{\dim V} = \frac{a|C|\chi_V(g)}{\dim V} + b\chi_V(g).$$

Or on sait que $\frac{|C|\chi_V(g)}{\dim V}$ et $\chi_V(g)$ sont des entiers algébriques, donc puisque les entiers algébriques sont un sous-anneau de \mathbb{C} , on a démontré la première assertion.

Soient $\lambda_1, \dots, \lambda_n$ ($n = \dim V$) les valeurs propres de $\pi_V(g)$, qui sont des racines de l'unité. On a $\frac{\chi_V(g)}{n} = \frac{\lambda_1 + \dots + \lambda_n}{n}$ qui est un entier algébrique, donc par le lemme si $\chi_V(g) \neq 0$ on a $\lambda_1 = \dots = \lambda_n$, et donc $\pi_V(g)$ est une homothétie ($\pi_V(g)$ est diagonalisable). \square

Proposition K.3. Soit G un groupe tel qu'il existe une classe de conjugaison C de G satisfaisant à $|C| = p^m$ pour p premier et $m \geq 1$. Alors G n'est pas simple.

Preuve. On va utiliser la description du caractère de la représentation régulière. Rappelons que si W_1, \dots, W_s sont des représentations irréductibles telles que $\text{Irr}(G) = \{[W_1], \dots, [W_s]\}$, alors en notant $d_i = \dim W_i$ et $\chi_i = \chi_{W_i}$ pour tout i , on a

$$\chi_{\text{reg}} = \sum_{i=1}^s d_i \chi_i$$

où χ_1 est le caractère de la représentation triviale. Soit $g \in C$ ($g \neq 1$ car $|C| > 1$). On a

$$\chi_{\text{reg}}(g) = 0 = \sum_{i=1}^s d_i \chi_i(g) \Rightarrow \frac{-1}{p} = \sum_{i=2}^s \frac{d_i \chi_i(g)}{p}$$

On $\frac{-1}{p} \in \mathbb{Q} \setminus \mathbb{Z}$, donc $\frac{-1}{p}$ n'est pas entier algébrique, et il existe donc $i \in \{2, \dots, s\}$ tel que $\frac{d_i \chi_i(g)}{p}$ n'est pas entier algébrique. En particulier $\chi_i(g) \neq 0$ et p ne divise pas $d_i = \dim(W_i)$, ce qui assure que $|C|$ et $\dim W_i$ sont premiers entre eux. La dernière proposition assure que $\pi_{W_i}(g)$ est une homothétie.

Supposons maintenant G simple. Comme π_{W_i} est irréductible non triviale, on a $\text{Ker}(\pi_{W_i}) \neq \{1\}$ et donc $\text{Ker}(\pi_{W_i}) = \{1\}$ et π_{W_i} injectif. Comme $\pi_{W_i}(g)$ est une homothétie, il commute avec tous les éléments $\pi_{W_i}(h)$, $h \in G$. Alors puisque π_{W_i} est injectif, on a $g \in Z(G)$ et donc puisque G est simple $Z(G) = G$ ($Z(G) \triangleleft G$). Alors G est abélien, donc toutes les classes de conjugaison sont réduites à un élément, ce qui contredit notre hypothèse. On conclut donc que G n'est pas simple. \square

Théorème K.4 (Théorème "pq" de Burnside). Soient p et q des nombres premiers. Soit G un groupe d'ordre $p^\alpha q^\beta$ où $\alpha, \beta \in \mathbb{N}$ vérifient $\alpha + \beta \geq 2$. Alors le groupe G n'est pas simple.

Preuve. On peut supposer que α et β sont non nuls sinon on connaît le résultat. Montrons qu'il existe une classe de conjugaison $C \neq \{1\}$ telle que q ne divise pas $|C|$. Soient C_1, \dots, C_s les classes de conjugaison distinctes de G avec $C_1 = \{1\}$. Alors comme $G = C_1 \amalg \dots \amalg C_s$, on a

$$|G| = 1 + \sum_{i=2}^s |C_i|.$$

Comme q divise $|G|$, il existe $i \geq 2$ tel que q ne divise pas C_i . Puisque $|C_i|$ divise $|G|$ (c'est une orbite pour l'opération de G sur lui-même par conjugaison), on a donc $|C_i| = p^m$ pour $m \geq 1$ ou $|C_i| = 1$. Dans le premier cas la proposition précédente assure que G n'est pas simple. Dans le deuxième soit $g \neq 1 \in C_i$. Puisque $|C_i| = 1$, on a $g \in Z(G)$, d'où $\{1\} \subsetneq Z(G)$. Si G était simple on aurait $Z(G) = G$ et G serait abélien. Mais un groupe abélien simple est nécessairement cyclique d'ordre premier, ce qui est contraire à notre hypothèse. \square

L Exemples de représentations et de tables de caractères.

L.1 Groupes abéliens

On a vu que les représentations irréductibles d'un groupe fini abélien sont toutes de dimension 1. Si ω est une racine primitive n -ième de l'unité, la table des caractères du groupe cyclique C_n est donc la matrice $(\omega^{ij})_{0 \leq i, j \leq n-1}$. Par exemple, les tables des caractères des groupes cycliques C_2 , C_3 et C_4 sont (on note g un générateur de chacun de ces groupes) :

C_2	1	g
χ_1	1	1
χ_2	1	-1

C_3	1	g	g^2
χ_1	1	1	1
χ_2	1	j	j^2
χ_3	1	j^2	j

C_4	1	g	g^2	g^3
χ_1	1	1	1	1
χ_2	1	i	-1	- i
χ_3	1	-1	1	-1
χ_4	1	- i	-1	i

On a vu également, que si G et H sont des groupes, L'application

$$\begin{aligned} \theta : \widehat{G} \times \widehat{H} &\longrightarrow \widehat{G \times H} \\ (\phi, \psi) &\longmapsto ((g, h) \mapsto \phi(g)\psi(h)), \end{aligned}$$

est un isomorphisme de groupes. Par exemple, la table des caractères du groupe $C_2 \times C_2$ est donc

$C_2 \times C_2$	1	$(g, 1)$	$(1, g)$	(g, g)
χ_1	1	1	1	1
χ_2	1	-1	-1	1
χ_3	1	-1	1	-1
χ_4	1	1	-1	-1

L.2 Groupes diédraux

Soit $n \geq 3$. Le groupe diédral D_n est le groupe des isométries d'un polygone régulier à n sommets. C'est un groupe d'ordre $2n$, non abélien, et engendré par des éléments r, s satisfaisant $r^n = 1 = s^2, sr = r^{n-1}s$, avec de plus

$$D_n = \{r^i s^j, 0 \leq i \leq n-1, 0 \leq j \leq 1\}$$

Le groupe D_n est naturellement muni d'une représentation de dimension 2, qui est irréductible. Plus généralement, on a :

Proposition L.1. 1. On a $\widehat{D}_n \simeq C_2$ si n est impair et $\widehat{D}_n \simeq C_2 \times C_2$ si n est pair.
 2. Notons $\omega = e^{\frac{2i\pi}{n}}$ et posons $l = \frac{n}{2}$ si n est pair et $l = \frac{n-1}{2}$ si n est impair. Alors pour tout $1 \leq h \leq l$, il existe une représentation irréductible de dimension 2 de D_n , notée (V_h, π_h) , définie par

$$\pi_h : D_n \longrightarrow \text{GL}_2(\mathbb{C})$$

$$r, s \longmapsto \begin{pmatrix} \omega^h & 0 \\ 0 & \omega^{-h} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Les représentations V_h , $1 \leq h \leq l$, sont deux à deux non isomorphes. Toute représentation irréductible de D_n est isomorphe à une des représentations précédentes.

En particulier, les tables des caractères des groupes diédraux D_3 , D_4 et D_5 sont :

D_3	1	r	s
χ_1	1	1	1
ε	1	1	-1
χ_2	2	-1	0

D_4	1	r	r^2	s	rs
χ_1	1	1	1	1	1
χ	1	-1	1	-1	1
ϕ	1	-1	1	1	-1
ψ	1	1	1	-1	-1
χ_2	2	0	-2	0	0

D_5	1	r	r^2	s
χ_1	1	1	1	1
χ'_1	1	1	1	-1
χ_2	2	$2 \cos(\frac{\pi}{5})$	$2 \cos(\frac{2\pi}{5})$	0
χ'_2	2	$2 \cos(\frac{2\pi}{5})$	$2 \cos(\frac{\pi}{5})$	0

L.3 Le groupe quaternionique d'ordre 8

Considérons les matrices

$$X = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

et $Q = \{\pm I_2, \pm X, \pm Y, \pm Z\} \subset \text{GL}_2(\mathbb{C})$. C'est un sous-groupe d'ordre 8 non abélien de $\text{GL}_2(\mathbb{C})$, que l'on appelle le groupe quaternionique d'ordre 8. Il est non isomorphe à D_4 , et un groupe non abélien d'ordre 8 est soit isomorphe à D_4 , soit à Q .

Q est naturellement muni d'une représentation de dimension 2, qui est irréductible, et sa table des caractères est la suivante :

Q	1	X	$-I_2$	Y	Z
χ_1	1	1	1	1	1
χ	1	-1	1	-1	1
ϕ	1	-1	1	1	-1
ψ	1	1	1	-1	-1
χ_2	2	0	-2	0	0

On constate que la table des caractères de Q est la même que celle de D_4 . Donc la table des caractères ne détermine pas un groupe fini à isomorphisme près.

L.4 Groupes symétriques et alternés

On va maintenant calculer la table des caractères des groupes A_4 , S_4 et A_5 (nous avons déjà considéré les cas $S_3 \simeq D_3$ et $A_3 \simeq C_3$).

Commençons par quelques considérations générales. Soit $n \geq 3$. Il existe une bijection naturelle entre les classes de conjugaison du groupe symétrique S_n et les partitions de l'entier n (les suites d'entiers $k_1 \geq k_2 \geq \dots \geq k_r \geq 1$ tels que $k_1 + \dots + k_r = n$), donnée par la décomposition d'une permutation en produits de cycles à supports disjoints. Le nombre de classes d'isomorphisme de représentations irréductibles de S_n est donc égal au nombre de partitions de l'entier n .

De plus on a $\widehat{S}_n = \{1, \varepsilon\}$, où ε est la signature.

Rappelons que si G est un groupe fini opérant sur un ensemble fini X , on lui associe la représentation de permutation \mathbb{C}^X , où \mathbb{C}^X est le \mathbb{C} -espace vectoriel (des fonctions $X \rightarrow \mathbb{C}$) de base $(e_x)_{x \in X}$, et où, pour $g \in G$ et $x \in X$, on a $g \cdot e_x = e_{g \cdot x}$.

Proposition L.2. Notons t l'élément $t = \sum_{x \in X} e_x$. L'espace $\mathbb{C}t$ est une sous-représentation de \mathbb{C}^X , et il existe une sous-représentation $V_X \subset \mathbb{C}^X$ telle que $\mathbb{C}^X = \mathbb{C}t \oplus V_X$. La représentation V_X est irréductible si et seulement si G opère 2-transitivement sur X .

On dit que G opère 2-transitivement sur X si et seulement si $\forall x, x', y, y' \in X$ avec $x \neq x'$ et $y \neq y'$, il existe $g \in G$ tel que $y = g \cdot x$ et $y' = g \cdot x'$.

Les groupes S_n et A_n opèrent naturellement sur l'ensemble $\{1, \dots, n\}$, et cette opération est 2-transitive si $n \geq 4$. On obtient donc, pour $n \geq 4$, une représentation irréductible de S_n et une représentation irréductible de A_n . Par ailleurs, en utilisant la signature, on peut construire une autre représentation irréductible de dimension $n - 1$ de S_n , non isomorphe à la précédente. Les caractères de ces deux représentations de S_n sont donnés par les formules

$$\forall \sigma \in S_n, \chi(\sigma) = |\text{Fix}(\sigma)| - 1, \chi'(\sigma) = \varepsilon(\sigma)(|\text{Fix}(\sigma)| - 1)$$

où $\text{Fix}(\sigma)$ est l'ensemble des points fixes de la permutation σ .

On a alors, en utilisant les relations d'orthogonalité, assez d'informations pour écrire les tables de caractères de A_4 et S_4 .

S_4	1	(1, 2, 3, 4)	(1, 2, 3)	(1, 2)(3, 4)	(1, 2)
χ_1	1	1	1	1	1
ε	1	-1	1	1	-1
χ_2	2	0	-1	2	0
χ_3	3	-1	0	-1	1
χ'_3	3	1	0	-1	-1

A_4	1	(1, 2, 3)	(1, 3, 2)	(1, 2)(3, 4)
χ_1	1	1	1	1
χ'_1	1	j	j^2	1
χ''_1	1	j^2	j	1
χ_3	3	0	0	-1

Pour A_5 , on utilise le lemme suivant.

Lemme L.3. Soit G un groupe fini simple non abélien et soit $\pi_V : G \rightarrow \text{GL}(V)$ une représentation irréductible non triviale. Alors $\dim(V) \geq 3$. Supposons $\dim(V) = 3$, et soit $g \in G$. Si g est d'ordre 3, alors $\chi_V(g) = 0$, et si g est d'ordre 2, alors $\chi_V(g) = -1$.

On obtient finalement, avec un peu plus de travail, la table de caractères de A_5 .

A_5	1	(1, 2, 3, 4, 5)	(1, 2, 3, 5, 4)	(1, 2, 3)	(1, 2)(3, 4)
χ_1	1	1	1	1	1
χ_3	3	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	0	-1
χ'_3	3	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$	0	-1
χ_4	4	-1	-1	1	0
χ'_5	5	0	0	-1	1

L.5 Le groupe dicyclique d'ordre 12

Le groupe dicyclique d'ordre 12, que l'on note G_{12} , est un groupe d'ordre 12 engendré par des éléments a, b satisfaisant $a^4 = 1 = b^3, ab = b^2a$. On peut le construire explicitement comme un produit semi-direct $C_3 \rtimes C_4$. On a $\widehat{G_{12}} \simeq C_4$, et sa table de caractères est

G_{12}	1	a	a^2	a^3	b	a^2b
χ_1	1	1	1	1	1	1
ϕ	1	i	-1	$-i$	1	-1
ϕ^2	1	-1	1	-1	1	1
ϕ^3	1	$-i$	-1	i	1	-1
χ_2	2	0	-2	0	-1	1
χ_2'	2	0	2	0	-1	-1

Un groupe non abélien d'ordre 12 est isomorphe à l'un des groupes suivants : A_4, D_6, G_{12} . L'ensemble des résultats précédents nous donne donc la table des caractères de tous les groupes d'ordre inférieur ou égal à 15.

A Appendices

A Une autre preuve du théorème de la base adaptée

Dans cet appendice on donne une preuve du théorème de la base adaptée indépendante des opérations matricielles sur les lignes et colonnes, et donc valable dans un anneau principal général. Elle est plus aride que celle que nous avons présenté dans le chapitre V.

Définition-Proposition A.1. Soient A un anneau principal, M un A -module libre de rang fini et $x \in M$. Soit $\{e_1, \dots, e_n\}$ une base de M , avec $x = \sum_{i=1}^n a_i \cdot e_i$. Soit

$$c(x) = \text{PGCD}(a_1, \dots, a_n) \in A$$

(défini à un inversible près). On a alors

$$\forall a \in A, a|c(x) \iff [\exists y \in M \text{ tq } x = a \cdot y]$$

et $c(x)$ ne dépend pas du choix de la base de M . On dit que $c(x)$ est le **contenu** de x .

Preuve. On peut écrire $x = c(x) \cdot (\sum_{i=1}^n b_i \cdot e_i)$, donc si $a|c(x)$ on a $x = a \cdot y$ pour un $y \in M$. Réciproquement, si $x = a \cdot y$ pour $y \in M$, si on écrit $y = \sum_{i=1}^n b_i e_i$, on obtient $a|a_i, \forall i$, et donc $a|c(x)$.

Un élément $d \in A$ satisfaisant la propriété

$$\forall a \in A, a|d \iff [\exists y \in M \text{ tq } x = a \cdot y]$$

est clairement unique (à multiplication par un inversible près), ce qui assure que la construction de $c(x)$ ne dépend pas du choix d'une base. \square .

Proposition A.2. Soient A un anneau principal, M un A -module libre de rang fini et $x \in M$.

1. Il existe une application A -linéaire $u : M \rightarrow A$ telle que $u(x) = c(x)$.
2. Pour toute application A -linéaire $v : M \rightarrow A$, on a $c(x)|v(x)$.

Preuve. 1. Soit $\{e_1, \dots, e_n\}$ une base de M , avec $x = \sum_{i=1}^n a_i \cdot e_i$. Par le théorème de Bezout il existe $b_1, \dots, b_n \in A$ tels que $c(x) = \sum_{i=1}^n b_i a_i$. Si $u : M \rightarrow A$ est l'unique application A -linéaire telle que $u(e_i) = b_i, \forall i$, on a bien $u(x) = c(x)$.

2. En reprenant les notations précédentes, on a, pour $v \in \text{Hom}_A(M, A)$,

$$v(x) = \sum_{i=1}^n a_i v(e_i) \in \sum_{i=1}^n A a_i = A c(x)$$

ce qui donne le résultat. \square

Proposition A.3. Soient A un anneau principal, M un A -module libre de rang fini et $x \in M$. Les assertions suivantes sont équivalentes.

1. $c(x) = 1$
2. Il existe $u \in \text{Hom}_A(M, A)$ tel que $u(x) = 1$.
3. $x \neq 0$ et il existe $N \subset M$ un sous-module tel que $M = Ax \oplus N$.
4. Il existe une base $\{e_1, \dots, e_n\}$ de M telle que $x \in \{e_1, \dots, e_n\}$.

Preuve. On a (1) \Rightarrow (2) par la proposition précédente, et (4) \Rightarrow (1) est immédiat. Supposons (2) vérifiée et soit $u \in \text{Hom}_A(M, A)$ tel que $u(x) = 1$. Alors on voit facilement que $M = \text{Ker}(u) \oplus Ax$, et ainsi (3) est vérifiée. Supposons finalement que (3) est vérifiée. Soit e_2, \dots, e_n une base de N (N est libre par le théorème B.3 du chapitre V). La partie $\{x, e_2, \dots, e_n\}$ engendre M et on voit facilement qu'elle est libre (en utilisant le lemme B.2, chap. V). \square

Proposition A.4. Soient A un anneau principal, M un A -module libre de rang fini non nul. Alors M contient un élément non nul de contenu minimal, c'est-à-dire un élément $x \in M \setminus \{0\}$ tel que $\forall y \in M \setminus \{0\}, c(y)|c(x) \Rightarrow c(y) \sim c(x)$.

Preuve. On considère la famille $\{Ac(y)\}_{y \in M \setminus \{0\}}$ d'idéaux de A . Elle admet un élément maximal $Ac(x), x \in M \setminus \{0\}$, car A est principal, et on a alors, $\forall y \in M \setminus \{0\}, c(y)|c(x) \Rightarrow (c(x)) \subset (c(y)) \Rightarrow (c(x)) = (c(y)) \Rightarrow c(y) \sim c(x)$. \square

Proposition A.5. Soient A un anneau principal, M un A -module libre de rang fini, N un sous-module non nul de M , $x \in N \setminus \{0\}$ un élément non nul de contenu minimal (calculé dans N) et $e \in M$ tel que $x = c(x).e$. Alors

1. Il existe $M_1 \subset M$ un sous-module tel que $M = Ae \oplus M_1$;
2. Posons $N_1 = M \cap M_1$. On a $N = Ax \oplus N_1$;
3. $c(x)$ est le plus petit élément de $\{c(y)\}_{y \in N \setminus \{0\}}$.

Preuve. 1. On a $c(x) \sim c(x)c(e)$, d'où $c(e) = 1$ et donc la première assertion résulte d'une proposition précédente.

2. Soit $p : M \rightarrow Ae$ la surjection A -linéaire de noyau M_1 avec $p(e) = e$. Le sous-module $p(N)$ de Ae est de la forme $Abe, b \in A$, car A est principal. On a $x = c(x)e$ donc $p(x) = x$ et $x \in p(N) = Abe$, d'où $b|c(x)$. Il existe $y \in N$ tel que $p(y) = be$, donc $b = \varphi(y)$, pour une certaine forme linéaire φ sur M , et $c(y)|b$.

On a $c(y)|b|c(x)$, et comme $c(x)$ est minimal, on a $c(y) \sim c(x) \sim b$. Ainsi $p(N) = Abe = Ac(x)e = Ax \subset N$. Ainsi p induit un projecteur A -linéaire de N dans N , d'image Ax et de noyau $N \cap M_1 = N_1$, d'où $N = Ax \oplus N_1$.

3. Par hypothèse, $c(x)$ est minimal. Montrons que $\forall y \in N \setminus \{0\}$, on a $c(x)|c(y)$. Soit $y \in N \setminus \{0\} : y = \lambda x + y_1$, avec $\lambda \in A$ et $y_1 \in N_1$. En prenant une base de M formée de e et d'éléments de M_1 , on voit que $c(y) = \text{PGCD}(\lambda c(x), c(y_1))$. Pour montrer que $c(x)|c(y)$, il suffit donc de voir que $c(x)|c(y_1)$. Soit $y' = x + y_1 \in N$. On a $c(y') = \text{PGCD}(c(x), c(y_1))|c(x)$ et $c(y') \sim c(x)$ par minimalité de $c(x)$, et ainsi $c(x)|c(y_1)$. \square

Preuve du théorème de la base adaptée. Soit M un A -module libre de rang fini et $N \subset M$ un sous-module libre de rang p (théorème B.3, chap. V). On raisonne par récurrence sur p , le rang de N . Si $p = 0$, il n'y a rien à démontrer. Supposons $p \neq 0$ et le résultat montré pour tous les sous-modules de rang $< p$. Soit $x_1 \in N \setminus \{0\}$ de contenu minimal. Soit $e_1 \in M$ tel que $x_1 = c(x_1)e_1$. D'après la proposition précédente on a $M = Ae_1 \oplus M_1$ et $N = Ax_1 \oplus N_1$, où M_1 est un sous-module de M et $N_1 = N \cap M_1$. Les modules M_1 et N_1 sont libres par le théorème B.3 du chapitre V. D'autre part $\text{rg}(N) = \text{rg}(N_1) + 1$ et $\text{rg}(M) = \text{rg}(M) = \text{rg}(M_1) + 1$, d'où $\text{rg}(N_1) = p - 1$ et on peut appliquer l'hypothèse de récurrence au sous-module $N_1 \subset M_1$. Il existe une base $\{e_2, \dots, e_n\}$ de M_1 et des éléments a_2, \dots, a_p de A^* tels que $\{a_2e_2, \dots, a_pe_p\}$ soit une base de N_1 et $a_2 | \dots | a_p$. Alors $\{e_1, \dots, e_n\}$ est une base de M ($M = Ae_1 \oplus M_1$), et si on pose $a_1 = c(x)$, $\{a_1e_1, a_2e_2, \dots, a_pe_p\}$ est une base de N ($N = Ax_1 \oplus N_1 = Aa_1e_1 \oplus N_1$). Finalement $c(x) = a_1|a_2 = c(a_2e_2)$ par le 3 de la dernière proposition, car a_2 est un contenu de $a_2e_2 \in N$. \square

B Le lemme des noyaux

Dans la suite K est un corps (commutatif).

Théorème B.1. Soient A un K -algèbre, E un K -espace vectoriel et

$$\rho : A \longrightarrow \text{End}_K(E)$$

un morphisme de K -algèbres, munissant E d'une structure de A -module. Supposons que A est un anneau principal, et soit $a \in A$ tel que $\text{Ker}(\rho) = (a)$, que l'on écrit $a = a_1 \cdots a_r$, avec a_1, \dots, a_r premiers entre eux deux à deux. Alors on a

$$E = \text{Ker}(\rho(a_1)) \oplus \cdots \oplus \text{Ker}(\rho(a_r))$$

où chaque $\text{Ker}(\rho(a_1)), \dots, \text{Ker}(\rho(a_r))$ est un sous- A -module de E .

Preuve. Le théorème de Bezout, appliqué aux éléments b_1, \dots, b_r définis par $b_i = \prod_{j \neq i} a_j$, qui sont premiers entre eux dans leur ensemble, fournit des éléments $c_1, \dots, c_r \in A$ tels que

$$c_1 b_1 + \cdots + c_r b_r = 1, \quad \text{et donc} \quad \rho(c_1) \circ \rho(b_1) + \cdots + \rho(c_r) \circ \rho(b_r) = \text{id}_E$$

Ainsi

$$E = \text{Im}(\rho(c_1) \circ \rho(b_1)) + \cdots + \text{Im}(\rho(c_r) \circ \rho(b_r))$$

Pour $x \in E$, on a, pour tout i , $\rho(a_i) \circ \rho(c_i) \circ \rho(b_i)(x) = \rho(c_i) \circ \rho(a)(x) = 0$, d'où $\text{Im}(\rho(c_i) \circ \rho(b_i)) \subset \text{Ker}(\rho(a_i))$, et

$$E = \text{Ker}(\rho(a_1)) + \cdots + \text{Ker}(\rho(a_r))$$

Il reste à voir que cette somme est directe. Supposons donc que $\sum_{i=1}^r x_i = 0$, avec pour tout i , $x_i \in \text{Ker}(\rho(a_i))$. On voit facilement, que pour $j \neq i$, on a $\rho(b_j)(x_i) = 0$. On a donc, pour tout i ,

$$x_i = \sum_{j=1}^r \rho(c_j) \circ \rho(b_j)(x_i) = \rho(c_i) \circ \rho(b_i)(x_i)$$

On a donc, pour tout j ,

$$0 = \rho(b_j) \left(\sum_{i=1}^r x_i \right) = \sum_{i=1}^r \rho(b_j)(x_i) = \rho(b_j)(x_j)$$

et l'identité précédente assure donc que $x_j = 0$ pour tout j , ce qui termine la démonstration, chaque sous-espace $\text{Ker}(\rho(a_i))$ étant un sous- A -module, puisque l'anneau A est commutatif. \square

On en déduit de manière immédiate le lemme des noyaux, tel qu'énoncé dans le chapitre V.

Remarque B.2. Pour tout i , la projection sur $\text{Ker}(\rho(a_i))$ parallèlement à $\bigoplus_{j \neq i} \text{Ker}(\rho(a_j))$ est un élément de $\rho(A)$ (cette remarque est importante quand on établit l'existence de la décomposition de Dunford d'un endomorphisme ayant un polynôme caractéristique scindé).

En effet : En reprenant les notations de la démonstration précédente, on a montré

$$\rho(c_1) \circ \rho(b_1) + \cdots + \rho(c_r) \circ \rho(b_r) = \text{id}_E, \quad \text{donc} \quad E = \text{Im}(\rho(c_1) \circ \rho(b_1)) + \cdots + \text{Im}(\rho(c_r) \circ \rho(b_r));$$

$$\forall i, \text{Im}(\rho(c_i) \circ \rho(b_i)) \subset \text{Ker}(\rho(a_i));$$

$$E = \text{Ker}(\rho(a_1)) \oplus \cdots \oplus \text{Ker}(\rho(a_r))$$

On a en déduit que $\forall i, \text{Im}(\rho(c_i) \circ \rho(b_i)) = \text{Ker}(\rho(a_i))$. Par ailleurs pour $i \neq j$, $\rho(b_i c_i) \circ \rho(b_j c_j) = 0$ car $a_i b_j b_j$. La première identité $\rho(c_1) \circ \rho(b_1) + \cdots + \rho(c_r) \circ \rho(b_r) = \text{id}_E$ donne alors $\rho(b_i c_i) \circ \rho(b_i c_i) = \rho(b_i c_i)$, et finalement $\rho(b_i c_i)$ est bien la projection sur $\text{Ker}(\rho(a_i))$ parallèlement à $\bigoplus_{j \neq i} \text{Ker}(\rho(a_j))$. \square

On peut déduire très simplement du lemme des noyaux le critère fondamental de diagonalisabilité (chapitre V, corollaire D.3) :

Corollaire B.3. Soit E un K -espace vectoriel de dimension finie et soit $u \in \text{End}_K(E)$. Les assertions suivantes sont équivalentes.

1. u est diagonalisable.
2. P_u , le polynôme minimal de u , est scindé sur K à racines simples.
3. Il existe un polynôme $P \in K[X]$ scindé sur K et à racines simples tel que $P(u) = 0$.

Preuve. Il est clair que les assertions (2) et (3) sont équivalentes, car le polynôme minimal de u divise tout polynôme annulateur de u . Si u est diagonalisable, il existe une base de E dans laquelle la matrice de u est

$$M = \begin{pmatrix} \lambda_1 I_{m_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_r I_{m_r} \end{pmatrix}$$

avec $\lambda_1, \dots, \lambda_r \in K$ deux à deux distincts. Le polynôme $P(X) = (X - \lambda_1) \cdots (X - \lambda_r)$ est scindé sur K à racines simples, et annule la matrice M , donc u .

Réciproquement, soit $P(X) = (X - \lambda_1) \cdots (X - \lambda_r) \in K[X]$ un polynôme scindé sur K à racines simples qui annule u . Le lemme des noyaux assure que

$$E = \text{Ker}(u - \lambda_1 \text{id}_E) \oplus \cdots \oplus \text{Ker}(u - \lambda_r \text{id}_E)$$

ce qui permet très facilement de voir que u est diagonalisable. \square