

Algèbre II
Cours de Maîtrise Grenoble
2me semestre 2002–2003

Chris Peters

MAI 2003

Table des matières

| | | |
|----------|--|----------|
| 1 | Quelques rappels | 5 |
| 1.1 | Modules | 5 |
| 1.2 | Modules de type fini | 6 |
| 1.3 | Anneaux principaux | 6 |
| 2 | Modules sur des anneaux principaux | 9 |
| 2.1 | Modules libres | 9 |
| 2.2 | Théorème de structure | 11 |
| 2.3 | Application : forme normal de Jordan | 14 |

Chapitre 1

Quelques rappels

1.1 Modules

Soit R un anneau commutatif avec 1 et soit $(M, +)$ un groupe abélien.

Définition 1.1.1. On dit que M est un R -module, si

1. R opère sur M , c.à.d. pour tout $r \in R$ et $x \in M$, un produit $rx \in M$ est défini tel que pour tout $r, s \in R$ et $x \in M$ on a $(rs)x = r(sx)$ et $1x = x$;
2. soit $r \in R$ et soit $\varphi(r) : M \rightarrow M$ la multiplication par r . Alors $\varphi(r)$ est un homomorphisme de groupes ;
3. $\forall s, r \in R$ on a $\varphi(r + s) = \varphi(r) + \varphi(s)$.

Exemple 1.1.2. 1. Un idéal I d'un anneau R est un R -module.

2. Pour $R = k$, un corps, la notion de k -module est la même chose que celle de k -espace vectoriel.
3. Un $k[X]$ -module est la donnée d'un k -espace vectoriel avec une transformation linéaire.
4. Un groupe abélien est un \mathbb{Z} -module.

Définition 1.1.3. Une application $f : M \rightarrow N$ entre R -modules est une APPLICATION R -LINÉAIRE ou HOMOMORPHISME DE R -MODULES si

$$\begin{aligned} \forall x, y \in M, & \quad f(x + y) = f(x) + f(y) \\ \forall s \in R, x \in M, & \quad f(s \cdot x) = s \cdot f(x). \end{aligned}$$

Si de plus f est bijectif alors f^{-1} est un R -homomorphisme, et on dit que f est un ISOMORPHISME de R -modules.

Exemple 1.1.4. 1. Dans le cas de $R = k$, un corps, la définition ci-dessus est la même que celle donnée dans l'algèbre linéaire.

2. La composition de deux applications linéaires est une application linéaire.

3. Si $f : M \rightarrow N$ est injective, on dit que M est un SOUS-MODULE de N . Le groupe quotient N/M hérite de l'action de R sur M la structure d'un R -module, le MODULE QUOTIENT. Comme pour les anneaux et leurs idéaux on a :

L'image $\text{Im}(f)$ d'une application R -linéaire $f : M \rightarrow N$ est un sous-module de N , son noyau $\text{Ker}(f)$ est un sous-module de M . Le module $\text{Im}(f)$ est isomorphe à $M/\text{Ker}(f)$:

$$M/\text{Ker}(f) \xrightarrow{\sim} \text{Im}(f)$$

$$x + \text{Ker}(f) \mapsto f(x).$$

1.2 Modules de type fini

Comme pour les k -espace vectoriels on a la notion de SOMME DIRECTE de R -modules :

Définition 1.2.1. Soit M un R -module et $M_1, M_2 \subset M$ deux sous-modules. Si $M = M_1 + M_2$ et si de plus $M_1 \cap M_2 = 0$ on dit que M est la SOMME DIRECTE de M_1 et M_2 :

$$M = M_1 \oplus M_2.$$

Dans la suite on se concentre sur des modules de type fini :

Définition 1.2.2. Un R -module M est DE TYPE FINI s'il y a $x_1, \dots, x_r \in M$ tels que $M = Rx_1 + \dots + Rx_r$. Si cette somme est directe on dit que M est LIBRE de type fini.

Donc M est libre de type fini si M est isomorphe à

$$R^n := \bigoplus^n R$$

et de type fini si M est un quotient de R^n .

1.3 Anneaux principaux

Un anneau commutatif R est PRINCIPAL si tout idéal est engendré par un seul élément.

Exemple 1.3.1. Une norme euclidienne est une fonction

$$g : R \setminus \{0\} \rightarrow \mathbb{N}$$

telle que $\forall s, t \in R \setminus \{0\}$ avec $rs \neq 0$

1. $g(st) \geq \max(g(s), g(t))$,

2. on a “division avec reste” : il y a $q, r \in R$ telle que

$$s = qt + r, \quad r = 0 \text{ où bien } g(r) < g(t).$$

C'est facile à voir que R est principal : un idéal $I \subset R$, $I \neq (0)$ est engendré par $r \in R$ telle que $g(r)$ est minimal.

Des exemples concrets : $R = \mathbb{Z}$, $R = k[X]$, $R = \mathbb{Z}[i]$.

On rappelle (sans démonstration) qu'un anneau euclidien R est FACTORIEL, c.à.d. que chaque $r \in R$ s'écrit de façon essentiellement unique comme

$$r = \varepsilon p_1^{k_1} \cdots p_r^{k_r}, \quad k_j \in \mathbb{N},$$

où les p_j sont des premiers et ε est une unité.

Un élément premier p n'engendre pas forcément un idéal premier (p) : par exemple 2 est premier dans $\mathbb{Z}[\sqrt{-5}]$, mais (2) n'est pas un idéal premier, car $-6 = (\sqrt{-5} - 1)(\sqrt{-5} + 1)$. Mais on a :

Proposition 1.3.2. *soit R anneau principal. Soit $I = (p) \subset R$ un idéal.*

Alors, les énoncés suivantes sont équivalentes :

- I est premier,
- p est premier,
- I est maximal,
- $R/I = R/pR$ est un corps.

La démonstration est laissée comme exercice. Par exemple, si p est premier et $J = (q) \subset (p)$, alors q divise p . Donc si $J \neq (p)$, q est un unité et engendre R . Donc (p) est un idéal maximal.

Chapitre 2

Modules sur des anneaux principaux

2.1 Modules libres

Dans ce paragraphe, R est un anneau principal sans diviseurs de zéro.

Proposition 2.1.1. *Soit M un R -module libre de type fini et $M \cong R^n$. Alors n ne dépend pas de l'isomorphisme et s'appelle RANG de M .*

Démonstration : Soit $p \in R$ premier. Alors $k = R/pR$ est un corps et M/pM est un k -espace vectoriel. Si $M \cong R^n$, alors $M/pM \cong k^n$. Le nombre n est alors la dimension de M/pM comme k -espace vectoriel.

Une BASE d'un R module M de rang n est un ensemble $\{x_1, \dots, x_n\}$ d'éléments de M tel que $M = Rx_1 \oplus \dots \oplus Rx_n$.

Définition 2.1.2. – Le sous-module de torsion $T(M)$ de M est le sous-module des $x \in M$ annulé par un élément non-nul de R .
– Si $M = T(M)$ on appelle M un MODULE DE TORSION.

On verra (Thm. 2.1.5) que le quotient $M/T(M)$ est libre.

Proposition 2.1.3. *Soit M un R -module libre de rang fini et $M' \subset M$ un sous-module. Alors M' est libre.*

Démonstration : On suppose que $M \cong R^n$. La preuve est par récurrence par rapport à n . Pour $n = 1$, M' est un idéal de R et donc engendré par un seul élément. On peut supposer que $M = R^n$. Pour $r \leq n$ on regarde R^r comme sous-module de R^n engendré par les r premières vecteurs de la base standard. Soit $M'_r = M' \cap R^r$. Par récurrence on peut supposer que $M'_r = Rx_1 \oplus \dots \oplus Rx_r$. Les $(r+1)$ -ièmes coordonnées des éléments de M'_{r+1} forment un idéal engendré par s . Soit $x \in M'_{r+1}$ un élément correspondant. Alors tout $y \in M'_{r+1}$ s'écrit de façon unique comme $y = tx + y'$, $t \in \mathbb{R}$, $y' \in M'_r$. On a donc

$$M'_{r+1} = Rx \oplus Rx_1 \oplus \dots \oplus Rx_r.$$

Proposition 2.1.4. *On suppose que R est un anneau euclidien. Soit M un R -module libre de rang fini n et $M' \subset M$ un sous-module de rang m . Alors M admet une base $\{x_1, \dots, x_n\}$ telle que $M' = R(q_{n-m+1}x_{n-m+1}) \oplus R(q_{n-m+2}x_{n-m+2}) \cdots \oplus R(q_n x_n)$ et $q_{n-m+1} | q_{n-m+2} | \cdots | q_n$.*

Démonstration : Soit

$$(A_{ij}(\underline{B}, \underline{C})) = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \cdots & \vdots \\ A_{n1} & \cdots & A_{nm} \end{pmatrix}$$

la matrice de l'inclusion $M' \hookrightarrow M$ par rapport à des bases \underline{B} de M' et \underline{C} de M . On suppose les bases choisies de telle façon qu'un de ses coefficients réalise $a := \min\{A_{ij}(\underline{B}, \underline{C}) \mid 1 \leq i \leq m, 1 \leq j \leq n, \underline{B}, \underline{C}\}$. On peut supposer que $a = A_{11}$. La minimalité implique que a divise toutes les coefficients A_{ij} de A . La méthode de Gauss s'applique alors et produit des bases $\{\underline{B}', \underline{C}'\}$ telle que par rapport à elles la matrice de l'inclusion $M' \hookrightarrow M$ devient

$$A' = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & A'_{22} & \cdots & A'_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & A'_{n2} & \cdots & A'_{nm} \end{pmatrix}$$

Soit $\underline{C}' = \{x_2, \dots, x_n\}$. Par récurrence on peut supposer que $q_k x_k, k = n - m + 2, \dots, n$ est une base de M'_1 et donc la matrice A' est diagonale. Puisque $a = A_{11} = A'_{11}$ divise toutes les coefficients de A' on a bien $A'_{11} | A'_{22} | \cdots | A'_{nn}$.

Théorème 2.1.5. (PREMIER THÉORÈME DE STRUCTURE : EXISTENCE, LE CAS DES MODULES SUR UN ANNEAU EUCLIDIEN) *On suppose que R est un anneau euclidien. Soit M une R -module de type fini, alors*

$$M \cong R^s \oplus R/q_1 R \oplus \cdots \oplus R/q_r R, \quad q_1 | q_2 | \cdots | q_r.$$

Alors $T(M) \cong R/q_1 R \oplus \cdots \oplus R/q_r R$ et $M/T(M)$ est libre de rang s , c'est le RANG de M .

Démonstration : On a une surjection $\varphi : F \rightarrow M$, avec F libre. Le noyau $M' \subset M$ de φ est un sous-module. Une application du théorème donne le résultat.

Remarque. – On verra plus loin (2.2.3) que les idéaux (q_j) sont aussi uniquement déterminés par M . On les appelle les DIVISEURS ÉLÉMENTAIRES DE M .

– La Prop. 2.1.4 et donc son Corollaire est aussi vrai pour R un anneau principal. On donnera une démonstration indépendante du Corollaire (2.2.9).

2.2 Théorème de structure

Dans ce paragraphe, R est un anneau principal sans diviseurs de zéro et M est un R -module de type fini.

Définition 2.2.1. – Soit $p \in R$ premier, alors on pose

$$M(p) = \{x \in M \mid \exists n \geq 1 \text{ telle que } p^n x = 0\}$$

- Si $x \in T(M)$ l'idéal $(\pi(x)) = \text{Ker}\{r \mapsto rx\}$ ou bien l'élément $\pi(x)$ est appelé la PÉRIODE de x .
- Pour $s \in R$ on pose

$$M^{(s)} = \{x \in M \mid sx = 0\}.$$

Exemple 2.2.2. Soit $p \in R$ premier et $M = R/(p^k)R$, alors $M = M(p)$ et $M^{(p^\ell)} = p^{k-\ell}R/p^kR$. En particulier $M^{(p^k)} = M(p)$. Si q est un premier différent de p , on a $M(q) = 0$ et $M^{(q)} = M$.

Ensuite, on peut montrer l'unicité :

Théorème 2.2.3. (PREMIER THÉORÈME DE STRUCTURE : UNICITÉ) *Soit M un R -module de torsion et supposons que*

$$M \cong \bigoplus_{i=1}^r R/q_i R, \quad q_1 | q_2 | \cdots | q_r.$$

Alors les idéaux (q_j) , $j = 1, \dots, r$ sont uniquement déterminés par M .

Démonstration : On va déterminer $M^{(p)}$

- Le cas $M = R/p^k R$, p premier. Alors $M^{(p)}$ est le sous-module $sR/p^k R$ et puisque le noyau de la composition

$$R \rightarrow sR \rightarrow sR/p^k R$$

est égal à pR on en déduit un isomorphisme :

$$M^{(p)} \cong R/pR = k.$$

- Le cas $M = \bigoplus_{i=1}^r R/q_i R$. On déduit de ce qui précède :

$$M^{(p)} = \{(x_1, \dots, x_r) \in M \mid px_i = 0, \forall i = 1, \dots, r\}.$$

Donc, $\dim_k M^{(p)}$ vaut le nombre des q_i divisible par p . En particulier, si $p|q_1$, p divisant toutes les q_i , on a $\dim_k M^{(p)} = r$.

Cela montre que r est déterminé par M , car pour un autre représentation $M = \bigoplus_{i=1}^s R/q'_i R$ le nombre p divise r facteurs, donc $s \geq r$ et, par symétrie, $s = r$.

On considère maintenant pM où p est un diviseur premier de q_1 . Pour tout $s, t \in R$ avec $(s, t) = 1$ on a $tR/stR \cong R/sR$ et donc :

$$pM \cong \bigoplus_{i=1}^r R/s_j R, \quad q_j = ps_j.$$

On effectue une récurrence sur le nombre de facteurs premiers dans la décomposition de q_r . Si ce nombre est 1, alors $q_1 = \dots = q_r = p$ avec p premier. Puisque $qM \cong M$ si q est un premier différent de p et $pM = 0$ cela montre l'unicité dans ce cas. On suppose maintenant qu'il y a plusieurs facteurs premiers dans la décomposition de q_r . On prend un, disons p et applique la formule ci-dessus. On suppose s_1, \dots, s_k sont des unités, mais que s_{k+1} n'est pas une unité. Par récurrence on sait que les idéaux (s_j) , $j = k+1, \dots, r$ sont uniquement déterminé par M et p . Aussi k est déterminé par M et p . Donc, si $M \cong \bigoplus_{i=1}^r R/q'_i$ est une autre décomposition, $(q'_1) = \dots = (q'_k) = (p)$ et $(q'_j) = (ps_j) = (q_j)$ pour $j = k+1, \dots, r$.

On va aussi donner une démonstration du théorème 2.1.4 dans le cas où R est un anneau principal sans diviseurs de zéro. D'abord un lemme clé :

Lemme 2.2.4. *Soit $M = T(M)$ un R -module de torsion de type fini. Alors*

$$M = \bigoplus_{p \text{ premier}} M(p).$$

Démonstration : Puisque $T(M)$ est de type fini, il y a $r \in R$ telle que $rM = 0$. Supposons que $r = st$ avec $(s, t) = 1$. Alors on a

$$M = M^{(s)} \oplus M^{(t)}.$$

C'est une conséquence immédiat du fait qu'on peut écrire $1 = as + bt$. Ensuite, si $r = p_1^{a_1} \dots p_r^{a_r}$ et $q_i = p_i^{a_i}$, $i = 1, \dots, r$, alors

$$M = \bigoplus_{i=1}^r M^{(q_i)}, \quad M^{(q_i)} = M(p_i).$$

On continue avec quelques préparations.

Lemme 2.2.5. *On suppose $p^n M = 0$ et soit $x \in M$ de période p^n . Alors, si $\bar{y} \in M/xM$, il y a un représentant de \bar{y} ayant la même période que \bar{y} .*

Démonstration : Soit $y' \in M$ un représentant de \bar{y}' et supposons que p^k est une période de \bar{y}' . Alors $p^k y' \in xM$ et donc $p^k y' = (p^\ell s)z$ où $(p, s) = 1$. Si $\ell = n$ alors $p^k y' = 0$ et y' est aussi de période p^k . Sinon, $\ell > n$ et $p^\ell s y'$ est de période $p^{n-\ell}$ et y' est de période $p^{n-\ell+k}$. Puisque $n - \ell + k \leq n$, on a $k \leq \ell$ et $y = y' - p^{\ell-k} s z$ est un représentant de \bar{y} avec $p^k y = 0$.

On a besoin d'une notion auxiliaire :

Définition 2.2.6. Soit M un R -module. On dit que $x_1, \dots, x_r \in M$ forment un SYSTÈME NON-LIÉ si $s_1 x_1 + \dots + s_r x_r = 0$, $s_1, \dots, s_k \in R$ implique $s_1 x_1 = \dots = s_r x_r = 0$.

Cette notion diffère de la notion "linéairement indépendant". Un système linéairement indépendant est non-lié, mais la réciproque n'est pas toujours vrai, sauf si R est un corps.

Corollaire 2.2.7. Soit $\{\bar{x}_1, \dots, \bar{x}_r\}$ un système non-lié dans M/xM . Alors, avec $x_j \in M$ une représentant ayant la même période de \bar{x}_j , le système $\{x, x_1, \dots, x_r\}$ est non-lié.

Démonstration : On suppose que $sx + s_1 x_1 + \dots + s_r x_r = 0$. Notre hypothèse donne que $s_k \bar{x}_k = 0$ pour $k = 1, \dots, r$. Si \bar{x}_k est de période p^{a_k} , alors $p^{a_k} | s_k$ et donc $s_k x_k = 0$ car x_k est aussi de période p^{a_k} . Finalement on a aussi $sx = 0$.

Le point clé de la démonstration est :

Proposition 2.2.8. On suppose que $M = M(p)$. Alors

$$M \cong \bigoplus_{k=1}^r R/p^{\nu_k} R, \quad 1 \leq \nu_1 \leq \dots \leq \nu_r.$$

Démonstration : Soit $y \in M$ tel que $\pi(y) = p^k$ soit maximale. Soit $k = R/pR$. On considère $M^{(p)} \subset M$ et $\bar{M}^{(p)} \subset \bar{M}$ comme deux k -espaces vectoriels. Soit $\{\bar{y}_1, \dots, \bar{y}_m\}$ une base de $\bar{M}^{(p)}$. Cela implique que $\{\bar{y}_1, \dots, \bar{y}_m\}$ est un système non-lié. Les \bar{y}_k sont tous de période p . On applique le Corr. 2.2.7 avec $x = yp^{k-1}$. Il y a donc des représentants y_k de période p . Puisque x est aussi de période p , le système $\{x, y_1, \dots, y_m\}$ est un système non-lié dans $M^{(p)}$ et k -indépendant si on voit $M^{(p)}$ comme k -espace vectoriel. Donc $\dim_k M^{(p)} > \dim_k \bar{M}^{(p)}$. On peut donc effectuer une récurrence sur $\dim M^{(p)}$ et on peut supposer que l'existence de la décomposition est déjà montré pour \bar{M} . Il existent donc $\bar{y}_2, \dots, \bar{y}_r \in \bar{M}$ telle que \bar{y}_k est de période p^{ν_k} , $k = 2, \dots, r$ et tel que $\nu_2 \leq \dots \leq \nu_r$. On applique de nouveau le Corr. 2.2.7 et on trouve des éléments $y_k \in M$ de période p^{ν_k} et telle que $\{x, y_2, \dots, y_s\}$ est non-lié. La maximalité de $\pi(x)$ achève la démonstration.

De cette Proposition et du Lemme. 2.2.4 on déduit :

Théorème 2.2.9. (PREMIER THÉORÈME DE STRUCTURE : EXISTENCE) Soit $M = T(M)$ un R -module de type fini. Alors

$$M = \bigoplus_{i=1}^r R/q_i R, \quad q_1 | q_2 | \cdots | q_r.$$

Une application de 2.1.5 et de 2.2.3 donne :

Lemme 2.2.10. Soit $M = M(p)$ un R -module de type fini. Alors on a une décomposition

$$M = M(p) \cong \bigoplus_{k=1}^r R/p^{\nu_k} R, \quad 1 \leq \nu_1 \leq \cdots \leq \nu_r.$$

La suite des ν_j est uniquement déterminé par M .

On déduit de ces deux lemmes :

Théorème 2.2.11. (DEUXIÈME THÉORÈME DE STRUCTURE) Soit $M = T(M)$ un R -module de torsion de type fini. Alors

$$M = \bigoplus_{p \text{ premier}} M(p), \quad M(p) = \bigoplus_{k=1}^r R/p^{\nu_k} R, \quad 1 \leq \nu_1 \leq \cdots \leq \nu_r.$$

La suite des ν_k est uniquement déterminé par M et le nombre premier p .

2.3 Application : forme normal de Jordan

Soit k un corps et $R = k[X]$. Un R -module de type fini est la même chose qu'un k -espace V de dimension finie et un endomorphisme $A \neq 0$. L'application canonique

$$\begin{aligned} \Phi : k[X] &\rightarrow \text{End}(V) \\ F(X) &\mapsto F(A) \end{aligned}$$

donne l'isomorphisme

$$k(X)/(Q(A)(X)) \xrightarrow{\sim} k[A],$$

et $Q(A)(X)$ est appelé le POLYNÔME MINIMAL de A . Dans ce cas $Q(A)$ annule V , V est un R -module de torsion donc, par théorème 2.2.9 une somme directe de modules de la forme $V_Q := k[X]/Q(X)$.

Étudions d'abord de tels modules. Soit $\deg Q = d$. Alors $k[X]/Q(X)$ est un k -espace vectoriel de dimension d et la multiplication par X définit un endomorphisme A_Q de V_Q . Soit $v \in V_Q$ la classe de 1. Alors $V_Q = k[X]v$. Un tel module est appelé CYCLIQUE. Le polynôme Q est le polynôme minimal de

A_Q car pour tout polynôme R on a $R(A_Q(v)) = R(X)v$. Donc R annule V_Q si et seulement si Q divise R . Si $k[X]/Q(X) \cong V$ en tant que $k[X]$ -modules et si v est l'image de la classe de 1, on a bien $V = k[X]v$. Réciproquement, si $V = k[X]v$, et Q est le polynôme minimal de A , l'endomorphisme de multiplication avec X , on a un isomorphisme explicite :

$$\begin{array}{ccc} k[X]/Q(X) & \xrightarrow{\sim} & V \\ F(X) & \mapsto & F(A)v \end{array}$$

Si

$$Q(X) = X^d + a_1X^{d-1} + \cdots + a_d$$

la matrice de A dans la base $\{v, Av, \dots, A^{d-1}v\}$ est égal à :

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & -a_d \\ 1 & 0 & \cdots & 0 & -a_{d-1} \\ 0 & 1 & \ddots & \ddots & \vdots \\ 0 & \vdots & \ddots & 0 & -a_2 \\ 0 & \cdots & \cdots & 1 & -a_1 \end{pmatrix}.$$

On en déduit que le polynôme caractéristique de A est égal à $(-1)^d Q(A)$. Appliquant cela ainsi que les théorèmes 2.2.9 et 2.2.3 on trouve :

Théorème 2.3.1. *Soit $A \in \text{End}(V)$ un endomorphisme d'un k -espace V de dimension fini n . Alors V est somme directe*

$$V = V_1 \oplus \cdots \oplus V_r, \quad V_k \cong k[X]/Q_k(X), \quad k = 1, \dots, r$$

des $k[X]$ -modules cycliques V_k et $Q_1 | \cdots | Q_r$. La suite (Q_1, \dots, Q_r) est uniquement déterminé par A . Le polynôme Q_r est le polynôme minimal $Q(A)$ et $(-1)^n Q_1 \cdots Q_r$ est le polynôme caractéristique de A .

La seule chose à montrer est que $Q_r = Q(A)$. Or, Q_r annule V_r et puisque $Q_k | Q_r$, le polynôme Q_r annule aussi les V_k . Donc Q_r annule tout V et donc $Q(A) | Q_r$. Un polynôme de degré $< \deg Q_r$ ne peut pas annuler V_r et donc ne peut pas annuler V . Donc $Q_r = Q(A)$.

Corollaire 2.3.2. (CAYLEY-HAMILTON) *A satisfait à son polynôme caractéristique.*

On peut aussi appliquer la deuxième théorème de structure :

Proposition 2.3.3. *Soit $A \in \text{End}(V)$ un endomorphisme d'un k -espace V de dimension fini. Soit*

$$Q(A) = P_1^{k_1} \cdots P_s^{k_s}$$

une décomposition du polynôme minimal en facteurs irréductibles. Alors

$$V = \bigoplus_{i=1}^s V(P_i), \quad V(P_i) \cong \bigoplus_{k=1}^r k[X]/(P_i^{\nu_k^{(i)}}), \quad 1 \leq \nu_1^{(i)} \leq \dots \leq \nu_r^{(i)}.$$

La collection des $\nu_k^{(i)}$ est uniquement déterminé par A .

Si en particulier $V = k[X]/(X-a)^d$, v la classe de 1, alors la multiplication par X définit l'endomorphisme A dont la matrice par rapport à la base $\{(A-a)^{d-1}v, (A-a)^{d-2}v, \dots, v\}$ est UN BLOC DE JORDAN :

$$\begin{pmatrix} a & 1 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & a \end{pmatrix}.$$

On en déduit la FORME NORMAL DE JORDAN :

Proposition 2.3.4. *Soit k algébriquement clos, V un k -espace de dimension finie, $A \in \text{End}(V)$. Alors, il existe une base de V telle que la matrice de A par rapport à cette base se décompose en blocs de Jordan. En particulier, $A = S + N$, où S est diagonalisable et N est nilpotent, et $SN = NS$. Il y a des polynômes $P_S(X)$ et $P_N(X)$ telle que $S = P_S(A)$ et $N = P_N(A)$. Une telle décomposition est unique.*

Démonstration : Soit $P_A(X) = \prod_{i=1}^k (X - \lambda_i)^{n_i}$. On a une décomposition A -stable $V = \bigoplus_{i=1}^k V_i$, $V_i = \text{Ker}(A - \lambda_i I)^{n_i}$ et $S|_{V_i} = \lambda_i I$, $N = A - S$. Clairement S et N respectent la décomposition et $SN|_{V_i} = \lambda_i N|_{V_i} = NS|_{V_i}$. Ensuite, on construit $P_S(X)$ comme suit. Puisque les polynômes $P_j = \prod_{i \neq j} (X - \lambda_i)^{n_i}$, $j = 1, \dots, k$ n'ont pas un facteur en commun, on peut trouver Q_1, \dots, Q_k telle que $P_1 Q_1 + \dots + P_k Q_k = 1$. On pose

$$P_S(X) = \sum_j P_j Q_j \lambda_j.$$

On a $P_S(X) \equiv \lambda_i \pmod{(X - \lambda_i)^{n_i}}$ et donc $P_S(A)|_{V_i} = \lambda_i I = S|_{V_i}$. Donc $P_S(X)$ convient. On pose ensuite $P_N(X) = X - P_S(X)$. Si $A = S' + N'$ est un autre décomposition telle que S' et N' commutent, alors S' et A commutent et donc aussi $S = P_S(A)$ commute avec S' . Si de plus S' est diagonalisable, S et S' peuvent être diagonalisés simultanément et donc $S - S' = N' - N$ est diagonalisable. Si de plus N' est nilpotent, $N' - N$ est nilpotent et donc $S - S' = N' - N = 0$.

Si k n'est pas algébriquement clos, on dit que $A \in \text{End}(V)$ est SEMI-SIMPLE si A devient diagonalisable après extension des scalaires de k à une clôture algébrique K . Un argument utilisant l'action du groupe de Galois de $K|k$ et l'unicité de la décomposition additive de Jordan montre :

Corollaire 2.3.5. *Soit V un k -espace de dimension finie, $A \in \text{End}(V)$. Alors $A = S + N$, où S est semi-simple et N est nilpotent, et $SN = NS$. Une telle décomposition est unique. C'est la DÉCOMPOSITION ADDITIVE DE JORDAN.*

Un automorphisme U de V est appelé UNIPOTENT si $U - I$ est nilpotent. Si A est un automorphisme et $A = S + N$ sa décomposition de Jordan, alors S est inversible et en écrivant $A = S(I + S^{-1}N)$ on trouve la DÉCOMPOSITION DE JORDAN MULTIPLICATIVE.

Corollaire 2.3.6. *Soit V un k -espace de dimension finie, $A \in \text{Gl}(V)$. Alors $A = SU$, où S est semi-simple et U est unipotent, et $SU = US$. Une telle décomposition est unique.*