Quatre exposés sur la théorie de l'élimination

Patrice PHILIPPON

Cours de DEA intensif

CIRM-Luminy

18-22 Avril 1993.

Exposé n°1 : Rappels d'algèbre commutative

Patrice PHILIPPON

UMR 9994 du CNRS-Problèmes Diophantiens,
Université P. & M. Curie, T.46-56, 5ème ét., F-75252 PARIS cedex 05.

Cet exposé est consacré à des rappels sur la notion de longueur d'un module et les décompositions primaires des idéaux (§1), les notions de rang d'un idéal, de dimension d'un module et les anneaux semi-réguliers (§2) et la notion de diviseur dans les anneaux intègres et les anneaux de Krull (§3). Nous donnons quelques démonstrations et renvoyons aux ouvrages de références pour les résultats plus difficiles et les développements des théories.

§ 1. **Longueurs des modules et décompositions primaires des idéaux**

Une bonne référence pour ce paragraphe est [2], chap.4 & 2 et [3], chap.4.

Soit R un anneau commutatif, unitaire et M un R-module non nul. On dit que M est *simple* s'il n'a pas de sous-module propre, non nul.

Une *suite de composition* d'un R-module M quelconque est une chaîne $M = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_\ell = 0$ de R-modules telle que chaque quotient M_{i-1}/M_i $(i = 1, \ldots \ell)$ soit un R-module simple.

On montre (et nous l'admettrons), *voir* [2], §1.7, thm.5, que les suites de composition d'un module M ont toutes le même nombre de quotients et que toute suite $M = M_0 \supset N_1 \supset \ldots \supset M_t$ peut-être raffinée en une suite de composition.

On appelle *longueur* du R-module M, notée $\ell(M)$, le nombre de quotients ℓ d'une suite de composition de M. S'il n'en existe pas, on pose $\ell(M) = \infty$, et on note aussi $\ell(0) = 0$. En particulier, si M est simple on a $\ell(M) = 1$.

Comme le montre la proposition suivante, si M est un R-module libre de rang r (*i.e.* $M \simeq R^r$) alors $\ell(M) = r.\ell(R)$. Si I est un idéal de R contenu dans $\mathrm{Ann}_R M$, alors M est un R/I-module et $\ell_{R/I}(M) = \ell_R(M)$.

Si R est un corps, la notion de longueur de R-module coïncide avec celle de dimension d'espace vectoriel.

Proposition 1 – *Si N est un sous-module d'un module M on a*

$$\ell(M) = \ell(N) + \ell(M/N) \ .$$

Démonstration – Notons $\varphi : M \to M/N$ la surjection cannonique et considérons des suites $N = N_0 \supset N_1 \supset \ldots \supset N_{\ell'}$ et $M/N = L_0 \supset L_1 \supset \ldots \supset L_{\ell''}$ de modules emboîtés, alors

$$M = \varphi^{-1}(L_0) \supset \ldots \supset \varphi^{-1}(L_{\ell''}) = N = N_0 \supset N_1 \supset \ldots \supset N_{\ell'}$$

est une suite de sous-modules de M emboîtés. Si $\ell(N) = \infty$ ou $\ell(M/N) = \infty$, on en déduit en prenant ℓ' ou ℓ'' arbitraire que $\ell(M) = \infty$ et le résultat est vrai. Sinon on prend $\ell' = \ell(N)$ et $\ell'' = \ell(M/N)$, les quotients N_{i-1}/N_i et $\varphi^{-1}(L_{i-1})/\varphi^{-1}(L_i) \simeq L_{i-1}/L_i$ sont simples, ce qui montre qu'on a obtenu une suite de composition de M et donc $\ell(M) = \ell' + \ell'' = \ell(N) + \ell(M/N)$. □

En liaison avec la notion de longueur, voici une propriété générale très utile des modules de type fini sur un anneau nœthérien. Nous la donnons ici dans une version graduée pour un anneau de polynômes.

Proposition 2 – *Soit R un anneau commutatif, nœthérien, $A = R[z_0, \ldots, z_n]$, M un A-module gradué, de type fini et N un sous-module homogène de M.*
(i) *Il existe un entier $s \geq 0$ et des éléments homogènes $m_0, \ldots, m_{s-1} \in M$ tels que les sous-modules $N_i = N + Am_0 + \ldots + Am_{i-1}$ $(i = 0, \ldots, s)$ satisfont $N_0 = N$, $N_s = M$ et $N_{i+1}/N_i \simeq A/\mathfrak{p}_i$ où $\mathfrak{p}_i$ est un idéal premier homogène de A $(i = 0, \ldots, s-1)$. De plus, l'isomorphisme ci-dessus applique les éléments homogènes de $A/\mathfrak{p}_i$ sur ceux de N_{i+1}/N_i en augmentant les degrés du degré de m_i.*
(ii) *Si $N = 0$, les premiers isolés associés à $\operatorname{Ann}_A M$ sont exactement les premiers de la collection $\mathfrak{p}_0, \ldots, \mathfrak{p}_{s-1}$ qui ne contiennent strictement aucun de ces premiers. Soit $\mathfrak{p}$ un premier isolé associé à $\operatorname{Ann}_A M$, le nombre de $\mathfrak{p}_i$ $(0 \leq i < s)$ égaux à $\mathfrak{p}$ est égal à la longueur $\ell(M_\mathfrak{p})$ du $A_\mathfrak{p}$-module $M_\mathfrak{p}$.*

Démonstration – (i) On procède par récurrence, supposons construits $N_0, \ldots, N_i$ et $N_i \subsetneq M$. Considérons la famille d'idéaux homogènes, $(N_i :_A m)$ lorsque m parcourt les éléments homogènes de $M \setminus N_i$, l'anneau A étant nœthérien cette famille admet un élément maximal, disons $\mathfrak{p}_i = N_i :_A m_i$ avec $m_i \in M \setminus N_i$, m_i homogène. Montrons que $\mathfrak{p}_i$ est premier, si $a, b \in A$, satisfont $ab \in \mathfrak{p}_i$ et $b \notin \mathfrak{p}_i$ alors $bm_i \notin N_i$ et $N_i :_A bm_i \supset N_i :_A m_i = \mathfrak{p}_i$, d'où $N_i :_A bm_i = \mathfrak{p}_i$ par la maximalité de $\mathfrak{p}_i$. Mais $abm_i \in N_i$ et donc $a \in N_i :_A bm_i = \mathfrak{p}_i$ ce qui prouve que cet idéal est bien premier.

On pose $N_{i+1} = N_i + Am_i$, c'est un sous-module homogène de M, $N_i \subsetneq N_{i+1}$ et l'application $A \to N_{i+1}/N_i$ qui à $a \in A$ associe l'image de am_i dans N_{i+1}/N_i est un homomorphisme surjectif de noyau $\mathfrak{p}_i$ et degré égal au degré de m_i. Ceci montre $N_{i+1}/N_i \simeq A/\mathfrak{p}_i$.

Enfin, le module M étant de type fini, la suite $N_0 \subset \ldots \subset N_i \subset \ldots$ doit être ultimement stationnaire par la propriété de nœthérianité, ce qui entraîne l'existence d'un entier $s \geq 0$ tel que $N_s = M$.
(ii) Comme $\mathfrak{p}_i$ annule N_{i+1}/N_i on a $\mathfrak{p}_i N_{i+1} \subseteq N_i$ et par suite $\mathfrak{p}_0 \ldots \mathfrak{p}_{s-1} M \subseteq N_0 = 0$. Soit $\mathfrak{p}$ un premier contenant $\operatorname{Ann}_A M$, alors $\mathfrak{p}_0 \ldots \mathfrak{p}_{s-1} \subseteq \operatorname{Ann}_A M \subseteq \mathfrak{p}$ et $\mathfrak{p} \supseteq \mathfrak{p}_j$ pour un certain $0 \leq j < s$. D'un autre côté, $\operatorname{Ann}_A M \subseteq \cap_{i=0}^{s-1} \mathfrak{p}_i$, et $\operatorname{Rad}(\operatorname{Ann}_A M) = \operatorname{Rad}(\cap_{i=0}^{s-1} \mathfrak{p}_i)$ est l'intersection des $\mathfrak{p}_i$ $(0 \leq i < s)$ ne contenant strictement aucun des premiers $\mathfrak{p}_0, \ldots, \mathfrak{p}_{s-1}$.

On a $(N_{i+1})_\mathfrak{p} \neq (N_i)_\mathfrak{p}$ si et seulement si $(N_{i+1}/N_i)_\mathfrak{p} \simeq (A/\mathfrak{p}_i)_\mathfrak{p} \neq 0$ et, comme $\mathfrak{p}$ ne contient strictement aucun des $\mathfrak{p}_0, \ldots, \mathfrak{p}_{s-1}$, ceci n'est possible que lorsque $\mathfrak{p}_i = \mathfrak{p}$. Soit $i_1, \ldots, i_t$ la suite des indices $i \in \{0, \ldots, s-1\}$ tels que $\mathfrak{p}_i = \mathfrak{p}$, notons $N'_0 = 0$, $N'_{j+1} = (N_{i_j+1})_\mathfrak{p}$ $(j = 0, \ldots, t-1)$. On a une chaîne de $A_\mathfrak{p}$-modules $M_\mathfrak{p} = N'_t \supset \ldots \supset N'_0 = 0$ telle que $N'_{i+1}/N'_i \simeq A_\mathfrak{p}/\mathfrak{p}.A_\mathfrak{p}$ $(i = 0, \ldots, t-1)$. Mais ce dernier module est simple, on a donc une suite de composition de $M_\mathfrak{p}$ et $t = \ell(M_\mathfrak{p})$. □

Dans le cas d'un module M de type fini sur un anneau nœthérien R on peut montrer (*cf.*[2], §4.3, prop.7) que $\ell(M) < \infty$ si et seulement s'il existe un nombre fini d'idéaux maximaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ de R dont le produit annule M (*i.e* $\mathfrak{m}_1 \ldots \mathfrak{m}_s.M = 0$). Ceci indique que les notions de longueur et module simple sont le plus utile pour les modules sur un *anneau local* (anneau commutatif, unitaire, nœthérien n'ayant qu'un seul idéal maximal).

Proposition 3 – *Soient R un anneau local, d'idéal maximal $\mathfrak{p}$ et M un R-module de type fini. On a $\ell(M) < \infty$ si et seulement s'il existe $\nu \geq 0$ tel que $\mathfrak{p}^\nu \subset \operatorname{Ann}_R M$. En particulier, si M est simple alors $\operatorname{Ann}_R M = \mathfrak{p}$.*

Démonstration – On a $M = 0$ si et seulement si $\operatorname{Ann}_R M = R$ et sinon $\operatorname{Ann}_R M \subset \mathfrak{p}$. Supposons $\ell(M) < \infty$ alors la suite de modules emboîtés $M \supset \mathfrak{p}M \supset \ldots \supset \mathfrak{p}^i M \supset \ldots$ doit être ultimement stationnaire, il existe donc $\nu \geq 0$ tel que $\mathfrak{p}^\nu M = \mathfrak{p}^{\nu+1} M$ et le R-module $\mathfrak{p}^\nu M$ est de type fini. Soient $m_1, \ldots, m_r$ des générateurs de $\mathfrak{p}^\nu M$, la relation $\mathfrak{p}^\nu M = \mathfrak{p}^{\nu+1} M$ s'écrit

$$m_i = \sum_{j=1}^{r} \alpha_{ij} m_j \quad (\alpha_{ij} \in \mathfrak{p},\ i = 1, \ldots, r) \ .$$

Soient $A = (\alpha_{ij})_{1 \leq i,j \leq r}$ et $\Delta = \operatorname{Det}(\operatorname{Id} - A)$, on a $\Delta m_i = 0$ $(i = 1, \ldots, r)$ et $\Delta \in 1 + \mathfrak{p}$. Ainsi $\Delta \notin \mathfrak{p}$ est inversible dans R et $\Delta.\mathfrak{p}^\nu M = 0$ entraîne

$\mathfrak{p}^\nu M = 0$, c'est-à-dire $\mathfrak{p}^\nu \subset \operatorname{Ann}_R M$. En particulier, si $\mathfrak{p}M = M$ alors $M = 0$ et $\operatorname{Ann}_R M = R$

Réciproquement, si $\mathfrak{p}^\nu \subset \operatorname{Ann}_R M$ on considère la suite de modules emboîtés $M \supset \mathfrak{p}M \supset \mathfrak{p}^2 M \supset \ldots \supset \mathfrak{p}^\nu M = 0$. Les modules quotients $N_i = \mathfrak{p}^i M/\mathfrak{p}^{i+1}M$ sont de type fini et annulés par $\mathfrak{p}$, ils peuvent être vus comme $R/\mathfrak{p}$ -modules et on a alors $\ell_R(N_i) \le \ell_{R/\mathfrak{p}}(N_i)$. Mais $R/\mathfrak{p}$ est un corps et N_i est donc un espace vectoriel de dimension finie sur $R/\mathfrak{p}$, d'où $\ell_R(N_i) < \infty$ et $\ell(M) = \sum_{i=0}^{\nu-1} \ell(N_i) < \infty$ avec la proposition 1.

Si M est simple on doit avoir $\mathfrak{p}M = 0$ car $\mathfrak{p}M \neq M$, d'où $\operatorname{Ann}_R M = \mathfrak{p}$. □

La notion de longueur s'applique aux idéaux (vus comme modules). On suppose maintenant l'anneau R commutatif, unitaire et nœthérien. Rappelons qu'un idéal propre $\mathfrak{p}$ de R est *premier* si $ab \in \mathfrak{p}$ entraîne $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Un idéal propre $\mathfrak{q}$ de R est dit *primaire* si $ab \in \mathfrak{q}$ et $b \notin \mathfrak{q}$ entraîne l'existence d'un entier $k > 0$ tel que $a^k \in \mathfrak{q}$.

Si I est un idéal de R on appelle *radical de* I , que nous noterons $\operatorname{Rad} I$, l'idéal des éléments de R dont une puissance appartient à I . Et on vérifie facilement que le radical d'un idéal primaire $\mathfrak{q}$ est premier, si $\mathfrak{p} = \operatorname{Rad}\mathfrak{q}$ on dit que $\mathfrak{q}$ est $\mathfrak{p}$ -primaire.

Un idéal $\mathfrak{p}$ de R est premier si et seulement si l'anneau quotient $R/\mathfrak{p}$ est intègre. Le théorème suivant est un classique (*cf.* [3], chap. 4, §4 par exemple).

Théorème de Lasker-Nœther – *Tout idéal* I *de* R *s'écrit comme intersection d'un nombre fini d'idéaux primaires.*

Soit $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$ une telle écriture, on vérifie aisément que l'intersection de deux idéaux primaires de même radical est encore un idéal primaire, on peut donc supposer que les idéaux premiers $\operatorname{Rad}\mathfrak{q}_1, \ldots, \operatorname{Rad}\mathfrak{q}_m$ sont deux à deux distincts et que $I \not\subset \cap_{i\neq i_0} \mathfrak{q}_i$ pour tout $i_0 = 1, \ldots, m$. Une décomposition ayant ces propriétés est appelée *décomposition normale* (ou *de Lasker*) de I , elle n'est pas unique. En revanche, les idéaux premiers $\operatorname{Rad}\mathfrak{q}_1, \ldots, \operatorname{Rad}\mathfrak{q}_m$ sont indépendants de la décomposition choisie et sont appelés les *premiers associés* à I , leur ensemble est noté $\operatorname{Ass} I$. Les idéaux premiers de $\operatorname{Ass} I$ qui ne contiennent aucun autre idéal de $\operatorname{Ass} I$ sont appelés les *premiers isolés* (ou *minimaux*) de I , les autres éléments de $\operatorname{Ass} I$ sont les *premiers immergés*.

Si $\mathfrak{q}$ est $\mathfrak{p}$ -primaire la longueur du $R_\mathfrak{p}$ -module $R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$ est égale au nombre d'éléments ℓ de la plus longue chaîne d'idéaux $\mathfrak{p}$ -primaires emboîtés

$$\mathfrak{q} = \mathfrak{q}_1 \subsetneq \ \ldots \subsetneq \ \mathfrak{q}_\ell = \mathfrak{p} \ ,$$

et on l'appelle encore longueur de l'idéal primaire $\mathfrak{q}$. En particulier, le $R_\mathfrak{p}$ -module $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ est simple.

L'*exposant* $e(\mathfrak{q})$ d'un idéal $\mathfrak{p}$ -primaire est le plus petit entier e tel que $\mathfrak{p}^e \subset \mathfrak{q}$.

Lemme 4 – *Soit* $R' = R[z_1, \ldots, z_n]$ *un anneau de polynômes à cœfficients dans* R *,* I *un idéal de* R *et* $I' = I.R'$ *l'idéal de* R' *engendré par les éléments de* I *. Alors, si* I *est premier (resp. primaire) il en est de même de* I' *,* $\operatorname{Rad} I' = (\operatorname{Rad} I).R'$ *et si* $I = I_1 \cap \ldots \cap I_m$ *alors* $I' = (I_1.R') \cap \ldots \cap (I_m.R')$.

Démonstration – Exercice ou *voir* [2], §5.4, prop.9. □

§ 2. **Rang, dimension et anneaux semi-réguliers**

Une bonne référence pour ce paragraphe est [2], chap.4, 5 & 3.

Soit R un anneau commutatif, unitaire et $\mathfrak{p}$ un idéal premier de R , on appelle *rang* (ou *hauteur*), noté $\operatorname{rg}\mathfrak{p}$, de $\mathfrak{p}$ la longueur r de la plus longue chaîne d'idéaux premiers de R emboîtés de la forme

$$\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_r \ .$$

S'il n'existe pas de plus longue chaîne de ce type on note $\operatorname{rg}\mathfrak{p} = \infty$. Si I est un idéal propre de R on note $\operatorname{rg} I = \inf_{\mathfrak{p}\supseteq I} \operatorname{rg}\mathfrak{p}$ où la borne inférieure est prise sur les idéaux premiers de R contenant I (ou sur les premiers isolés associés à I ce qui revient au même). On dit qu'un idéal I est *pur* si tous ses premiers associés ont même rang.

On prendra soin de distinguer la notion de rang d'un idéal de celle de rang d'un module libre fini. En fait, un idéal non nul est un module libre fini si et seulement s'il est principal et alors il est de rang 1 dans les deux sens.

On déduit du lemme 4 , et dans les mêmes notations, que I est premier si et seulement si I' est premier et ces idéaux ont alors même rang.

On appelle *dimension de Krull* de R , notée $\dim R$, la borne supérieure des rangs des idéaux maximaux de R .

Si M est un R-module on appelle *dimension* de M , notée $\dim_R M$, la dimension de l'anneau quotient $R/\operatorname{Ann}_R M$. Lorsque R est un corps, on fera attention à ne pas confondre cette notion avec celle de dimension d'espace vectoriel, en fait dans ce cas, tout R-module est de dimension nulle. En revanche, la dimension de R en tant que R-module est bien la même qu'en tant qu'anneau.

Un résultat fondamental est le théorème de Krull suivant.

Théorème de l'idéal principal – *Si R est nœthérien et $a_1, \ldots, a_s$ sont des éléments de R, alors tout premier isolé associé à $(a_1, \ldots, a_s)$ est de rang $\leq s$. De plus, si I est un idéal propre de R, de rang r, il existe des éléments $a_1, \ldots, a_r \in I$ tels que $\operatorname{rg}(a_1, \ldots, a_i) = i$ $(i = 1, \ldots, r)$. Et les premiers de rang r associés à I sont aussi associés à $(a_1, \ldots, a_r)$.*

Démonstration – *voir* [2], §4.8, thm.22 et prop.15. □

Lemme 5 – *Soit $\mathbf{k}$ un corps et $\mathbf{k}'$ une extension algébrique séparable de $\mathbf{k}$. Si $\mathfrak{p}$ est un idéal premier de $\mathbf{k}[z_1, \ldots, z_n]$ alors l'idéal $\mathfrak{P} = \mathfrak{p}.\mathbf{k}'[z_1, \ldots, z_n]$ admet pour décomposition primaire*

$$\mathfrak{P} = \mathfrak{P}_1 \cap \ldots \cap \mathfrak{P}_s$$

où les idéaux $\mathfrak{P}_i$ sont les premiers de $\mathbf{k}'[z_1, \ldots, z_n]$ tels que $\mathfrak{P}_i \cap \mathbf{k}[z_1, \ldots, z_n] = \mathfrak{p}$ et de même rang que $\mathfrak{p}$.

Démonstration – *voir* [3], chap. 7, §11, th. 36 & cor. 2. □

On dit qu'un corps $\mathbf{k}$ est *parfait* si toute extension algébrique finie de $\mathbf{k}$ est séparable.

Corollaire 6 – *Soit R un anneau nœthérien, I un idéal de R engendré par s éléments et $\mathfrak{p}$ un idéal premier de R contenant I alors, si $\varphi : R \to R' = R/I$ est la surjection canonique, l'idéal $\mathfrak{p}' = \varphi(\mathfrak{p})$ de R' est premier et*

$$\operatorname{rg}\mathfrak{p}' + \operatorname{rg} I \leq \operatorname{rg}\mathfrak{p} \leq \operatorname{rg}\mathfrak{p}' + s \ .$$

Démonstration – Si $a', b' \in R'$ satisfont $a'b' \in \mathfrak{p}'$ il existe $a, b \in R$ tels que $a' = \varphi(a)$, $b' = \varphi(b)$ et $\varphi(ab) \in \mathfrak{p}'$. On a $ab \in \varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ car $\ker\varphi = I \subset \mathfrak{p}$ et donc $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ ce qui entraîne $a' \in \mathfrak{p}'$ ou $b \in \mathfrak{p}'$ et montre que cet idéal est premier. Si $\operatorname{rg}\mathfrak{p}' = 0$ alors $\mathfrak{p}$ est un premier isolé associé à I et d'après le théorème de l'idéal principal on a $\operatorname{rg}\mathfrak{p} \leq s$. Si $\operatorname{rg}\mathfrak{p}' = r > 0$ il existe, toujours grâce au théorème principal ci-dessus, $a'_1, \ldots, a'_r \in \mathfrak{p}'$ tels que $\operatorname{rg}(a'_1, \ldots, a'_r) = r$ et $\mathfrak{p}'$ est un premier isolé associé à $(a'_1, \ldots, a'_r)$. Soient $a_1, \ldots, a_r \in \mathfrak{p}$ tels que $\varphi(a_i) = a'_i$ alors $\mathfrak{p}$ est un premier isolé associé à $I + (a_1, \ldots, a_r)$ et cet idéal étant engendré par $r + s$ éléments il suit du théorème de l'idéal principal $\operatorname{rg}\mathfrak{p} \leq r + s$. Pour la minoration, soit $\mathfrak{p}' = \mathfrak{p}'_0 \supset \mathfrak{p}'_1 \supset \ldots \supset \mathfrak{p}'_r$ une suite d'idéaux premiers de R' on en déduit une suite $\mathfrak{p} = \varphi^{-1}(\mathfrak{p}'_0) \supset \ldots \supset \varphi^{-1}(\mathfrak{p}'_r)$ d'idéaux premier de R qui montre $\operatorname{rg}\mathfrak{p} \geq r + \operatorname{rg}\varphi^{-1}(\mathfrak{p}'_r)$, mais $\varphi^{-1}(\mathfrak{p}'_r) \supset I$ et donc $\operatorname{rg}\varphi^{-1}(\mathfrak{p}'_r) \geq \operatorname{rg} I$. □

Soit M un R-module et $a \in R$, on dit que a est *diviseur de zéro sur* M s'il existe $m \in M$, $m \neq 0$ tel que $am = 0$.

Un idéal $\mathfrak{q}$ est primaire si et seulement si tout diviseur de zéro de $R/\mathfrak{q}$ appartient au radical de $\mathfrak{q}$, et $\mathfrak{p}$ est premier si et seulement si $R/\mathfrak{p}$ n'a pas de diviseur de zéro. Si $a \in R$ appartient à un premier associé à $\operatorname{Ann}_R M$ alors a est diviseur de zéro sur M.

On dit qu'une suite $a_1, \ldots, a_s$ d'éléments de R est une *suite régulière sur* M si a_i n'est pas diviseur de zéro sur $M/a_1M + \ldots + a_{i-1}M$ pour $i = 1, \ldots, s$, et $M/(a_1, \ldots, a_s)M \neq 0$. Si tous les éléments $a_1, \ldots, a_s$ appartiennent à un idéal I de R on dit que $(a_1, \ldots, a_s)$ est une suite régulière sur M *dans* I.

On appelle *profondeur* de I sur M, notée $\operatorname{prof}_I(M)$, le nombre d'éléments d'une suite régulière sur M dans I la plus longue possible.

Un anneau nœthérien R est dit *semi-régulier* (ou *Cohen-Macaulay*) si tout idéal de R de rang r engendré par r éléments est pur. Cette propriété est locale, on montre (*cf.* [2], §5.3, thm.11) que R est semi-régulier si et seulement si les localisés $R_\mathfrak{p}$ (obtenus en inversant tous les éléments de $R \setminus \mathfrak{p}$) sont semi-réguliers pour tous les idéaux maximaux $\mathfrak{p}$ de R.

Un anneau local $(R, \mathfrak{p})$ est semi-régulier si et seulement si $\operatorname{prof}_\mathfrak{p}(R) = \dim R$ (*cf.* [2], §5.3, thm.10). Un corps est un anneau semi-régulier de dimension 0.

On dit qu'un anneau local $(R, \mathfrak{p})$ de dimension d est *régulier* si $\mathfrak{p}$ est engendré par d éléments. Un anneau local régulier est semi-régulier (*cf.* [3], chap. VIII, §11 et app. 6).

Si R est un anneau semi-régulier de dimension d alors l'anneau de polynômes $R[z_1, \ldots, z_n]$ est semi-régulier de dimension $d + n$ (*cf.* [2], §§5.4-5.5).

Proposition 7 – *Soient R un anneau semi-régulier, $\mathfrak{p} \subset \mathfrak{p}'$ deux idéaux premiers de R et $a_1, \ldots, a_s$ des éléments de R, alors*

$$\operatorname{rg}\mathfrak{p}' = \operatorname{rg}\mathfrak{p} + \operatorname{rg}(\mathfrak{p}'/\mathfrak{p}) \quad \textit{et} \quad \operatorname{rg}(\mathfrak{p} + (a_1, \ldots, a_s)) \leq \operatorname{rg}\mathfrak{p} + s$$

où $\mathfrak{p}'/\mathfrak{p}$ est considéré comme idéal premier de $R/\mathfrak{p}$.

Démonstration – *voir* [2], §5.3, thm.13, et pour la seconde inégalité on applique la premiére égalité à un idéal $\mathfrak{p}'$ isolé associé à $\mathfrak{p} + (a_1, \ldots, a_s)$. L'idéal $\mathfrak{p}'/\mathfrak{p}$ est premier isolé associé à l'idéal de $R/\mathfrak{p}$ engendré par les images de $a_1, \ldots, a_s$ et est donc de rang $\leq s$ d'après le théorème de l'idéal principal. □

Nous avons déjà vu les localisés $R_\mathfrak{p}$ d'un anneau R, plus généralement si S est un *ensemble multiplicatif* de R (c. à d. $p, q \in S \Rightarrow pq \in S$), *l'anneau* *localisé* de R par rapport à S, noté $S^{-1}R$, est l'anneau des fractions sur R dont les dénominateurs sont dans S (*cf.* [2], chap.3). L'anneau R est unitaire, si $1 \in S$ alors R s'identifie naturellement à un sous-anneau de $S^{-1}R$ et si I est un idéal de R on note $S^{-1}I$ l'idéal engendré par les éléments de I dans $S^{-1}R$. Dans ce cas, si I est premier (resp. primaire d'exposant e et longueur ℓ) et si I ne rencontre pas S, alors $S^{-1}I$ est premier de même rang que I (resp. primaire d'exposant e et longueur ℓ) et $S^{-1}I \cap R = I$. Si I rencontre S alors $S^{-1}I = S^{-1}R$ et en tout cas $S^{-1}\operatorname{Rad} I = \operatorname{Rad} S^{-1}I$. Enfin, si I' est un autre idéal de R on a $S^{-1}(I \cap I') = S^{-1}I \cap S^{-1}I'$.

D'un autre côté, si I est un idéal premier (resp. primaire d'exposant e et longueur ℓ) de $S^{-1}R$ alors $I \cap R$ est un idéal premier de même rang que I (resp. primaire d'exposant e et longueur ℓ) de A et $S^{-1}(I \cap R) = I$.

Si $\mathfrak{p}$ est un idéal premier de R, l'ensemble $R \setminus \mathfrak{p}$ est un ensemble multiplicatif dans R et $R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}R$ est l'anneau localisé correspondant. C'est un anneau local d'idéal maximal $\mathfrak{p}R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$.

§ 3. **Diviseurs et anneaux de Krull**

Une bonne référence pour ce paragraphe est [1], chap. VII, §1.

Supposons l'anneau R intègre de corps de fractions K, et soient M, M' deux R-modules non nuls de type fini, contenus dans K, on écrira $M \preceq M'$ si et seulement si

$$\forall x \in K \quad (Rx \supset M) \Rightarrow (Rx \supset M') \ .$$

Cela définit une relation de préordre sur l'ensemble des sous-R-modules non nuls de type fini de K et on obtient une relation d'équivalence sur ce même ensemble $M \asymp M'$ définie par $M \preceq M'$ *et* $M' \preceq M$. L'ensemble quotient, noté $D(R)$, est appelé l'ensemble des *diviseurs* de R et on notera $\operatorname{div}(M)$ le diviseur associé au sous-module M de type fini dans K. La relation $\preceq$ induit par passage au quotient une relation d'ordre sur les diviseurs.

Le produit dans K induit une structure de monoïde ordonné sur $D(R)$ donnée par $\operatorname{div}(M) + \operatorname{div}(M') = \operatorname{div}(MM')$ dont l'élément neutre est $\operatorname{div}(R)$. Pour que le monoïde $D(R)$ soit un groupe il faut et il suffit que l'anneau R soit *complètement intègralement clos* (*i.e.* tout $x \in K$ dont les puissances x^n $(n \in \mathbf{N})$ appartiennent à un sous-R-module de type fini de K, est dans R), *voir* [1], chap.V, §1.4.

En particulier, un *anneau de Krull* est un anneau complètement intégralement clos où toute famille non vide de diviseurs $\succeq 0$ admet un élément minimal. C'est

équivalent à demander que l'anneau R s'écrive $R = \cap_{v \in \mathcal{V}} R_v$ pour une famille $\mathcal{V}$ de valuations discrètes de K telle que pour tout $x \in K^*$ l'ensemble $\{v \in \mathcal{V};\ v(x) \neq 0\}$ soit fini, *voir* [1], chap.VII, §3. (Ici on note $R_v = \{x \in K;\ v(x) \geq 0\}$ l'anneau de la valuation v).

Par exemple, les anneaux d'entiers des corps de nombres sont des anneaux de Krull, l'anneau d'une sous-variété projectivement normale dans un espace projectif et un anneau de Krull. On retrouve dans ces deux cas les notions de diviseurs de la théorie des nombres et de diviseurs de Weil de la géométrie.

On définit sur $D(R)$ une nouvelle relation d'équivalence, que nous noterons $\sim$. Nous dirons que $d, d' \in D(R)$ satisfont $d \sim d'$ si et seulement s'il existe $x \in K^*$ tel que $d = d' + \operatorname{div}(Rx)$. Les diviseurs de la forme $\operatorname{div}(Rx)$ sont dits *principaux* et forment un groupe ordonné dans $D(R)$. On appelle *monoïde* (*resp. groupe* si R est complétement intégralement clos) *des classes de diviseurs* le monoïde (*resp.* groupe) quotient $C(R) := D(R)/\sim$.

On dit qu'un anneau de Krull R est *factoriel* (*resp. presque factoriel*) si son groupe des classes de diviseurs est réduit à un élément (*resp.* est un groupe de torsion).

Si R est un anneau de Krull de corps des fractions K et K' une extension finie de K, alors la clôture intégrale de R dans K' est un anneau de Krull (*cf.* [1], chap. VII, §1.8, prop. 12).

Si R est un anneau de Krull et S un ensemble multiplicatif de R ne contenant pas 0, alors l'anneau de polynômes $R[z_1, \ldots, z_n]$ et l'anneau local $S^{-1}R$ sont des anneaux de Krull (*cf.* [1], chap.VII, §1.9 et §1.4, prop.6). De plus, $C(R[z_1, \ldots, z_n]) \simeq C(R)$ et $C(R) \twoheadrightarrow C(S^{-1}R)$ (*cf.* [1], chap VII, §1.10, prop. 17 & 18), ce qui montre que si R est factoriel (*resp.* presque factoriel) il en est de même des anneaux $R[z_1, \ldots, z_n]$ et $S^{-1}R$.

Dans un anneau de Krull R, le groupe des diviseurs $D(R)$ est un $\mathbf{Z}$-module libre sur l'ensemble des diviseurs $\succeq 0$ extrémaux. Si on note $E(R)$ l'ensemble des diviseurs extrémaux on a pour tout $x \in K^*$ une décomposition finie

$$\operatorname{div}(x) = \sum_{e \in E(R)} v_e(x).e$$

et les applications $x \mapsto v_e(x)$ sont des valuations discrètes de K. Elles satisfont $R = \cap_{e \in E(R)} R_{v_e}$ et sont appelées les *valuations essentielles* de R (*cf.* [1], chap.VII, §1.4). Plus généralement, si M est un sous-R-module de type fini de K on a

$$\operatorname{div}(M) = \sum_{e \in E(R)} v_e(M).e$$

où $v_e(M) = \sup_{\substack{x \in K \\ Rx \supset M}} (v_e(x))$.

Les idéaux associés aux valuations essentielles de R (*i.e.* $\mathfrak{p}_{v_e} = (x \in R;\ v_e(x) \geq 1)$, $e \in E(R)$) sont exactement les idéaux premiers de rang 1 de R et si $\mathfrak{p}$ est un idéal premier de R de rang >1 alors $\operatorname{div} \mathfrak{p} = 0$ (*cf.* [1], chap. VII, §1.6). Les anneaux localisés $R_{\mathfrak{p}_e}$ ($e \in E(R)$) sont des anneaux de valuations discrètes.

Dans un anneau de valuation discrète l'idéal de la valuation est principal et tout générateur est appelé une *uniformisante* de la valuation.

Références

[1] Bourbaki N. – *Algèbre commutative*, Hermann, Paris, 1969.

[2] Northcott D.G. – *Lessons on rings, modules and multiplicities*, Cambridge Univ. Press, 1968.

[3] Samuel P. & Zariski O. – *Commutative algebra*, I & II, Van Nostrand, Princeton, 1958 & 1960.

Exposé n°2 : Invariants de Fitting

Patrice PHILIPPON

UMR 9994 du CNRS-Problèmes Diophantiens,
Université P. & M. Curie, T.46-56, 5ème ét., F-75252 PARIS cedex 05.

Une excellente référence pour cet exposé est le livre de D.G. Northcott [3]. Nous suivons essentiellement son exposition.

Soit $\mathbf{k}$ un corps commutatif.

Exemple : $\tilde{I} = I(C) = ((2z_1 - 1)^2 + 4z_2^2 - 1; z_1^2 + z_2^2 + z_3^2 - 1)$
$I = I(\pi(C)) = ((2z_1 - 1)^2 + 4z_2^2 - 1) = (p)$

Situation géométrique		*Traduction algébrique*
C courbe de $\mathbf{k}^3$		idéal $I(C) = \tilde{I} \subset \mathbf{k}[z_1, z_2, z_3] = \tilde{R}$
	$\downarrow \pi$ (projection)	$I(\pi(C)) = \tilde{I} \cap R = I \subset \mathbf{k}[z_1, z_2] = R$
$\pi(C)$ courbe de $\mathbf{k}^2$		$M = \tilde{R}/\tilde{I}$ est un $\tilde{R}$- et R-module
		$\operatorname{Ann}_{\tilde{R}} M = \tilde{I}$
		$\operatorname{Ann}_R M = I$

Problème : L'idéal I est premier ($\Rightarrow$ le point générique de $\pi(C)$ est simple), mais on souhaite que "l'image" de π soit formée de deux copies de $\pi(C)$. Plus précisément on veut déduire de $\tilde{I}$ un idéal $I' \subset I$ de radical I avec une composante I-primaire de longueur 2 .

§ 1. **Invariants de Fitting**

Soient R un anneau commutatif unitaire, M un R-module de type fini, et $m_1, \ldots, m_r$ des générateurs de M, on a un homomorphisme surjectif de R-module

$$\varepsilon : R^r \to M$$
$$(a_1, \ldots, a_r) \to a_1 m_1 + \ldots + a_r m_r$$

et si M est libre de rang r (*i.e.* $M \simeq R^r$) alors il n'y a pas de relation entre $m_1, \ldots, m_r$ et $\mathrm{Ann}_R M = (0)$.

L'idée est qu'il y a une étroite relation entre $\mathrm{Ann}_R M$ *et les relations entre* $m_1, \ldots, m_r$ (premier syzygy de Hilbert).

Supposons M de présentation finie, c'est-à-dire qu'il existe s et $\varphi : R^s \to R^r$ tels que

$$R^s \xrightarrow{\varphi} R^r \xrightarrow{\varepsilon} M \to 0 \ .$$

Ainsi une présentation finie de M est la première application d'une résolution libre finie avec $\varepsilon \circ \varphi = 0$, et puisque nous avons des bases naturelles de R^s et R^r en tant que R-modules on écrit la matrice Φ de φ dans ces bases. Les lignes de la matrice forment un système générateur pour le R-module des relations entre $m_1, \ldots, m_r$. La matrice Φ est à coefficients $\Phi_{\alpha,\beta}$ dans R naturellement. Si M n'est pas de présentation finie alors Φ est une suite infinie de vecteurs dans R^r (*i.e.* une matrice $r \times \infty$, à r lignes et une infinité de colonnes).

Tout module projectif de type fini est de présentation finie et si l'anneau R est nœthérien, il en est ainsi pour tout module de type fini (*voir* [1], chap.1, §2.8, lemme 8).

Définition – Nous notons $I_j\varphi$ l'idéal de R engendré par tous les mineurs de Φ de taille $j \leq r$.

Si $F \xrightarrow{\varphi} G \xrightarrow{\varepsilon} M \to 0$ est une présentation finie de M, alors φ induit un homomorphisme $\bigwedge^j \varphi : \bigwedge^j F \to \bigwedge^j G$ de R-modules.

Soit $\{g_1, \ldots, g_r\}$ (*resp.*$\{f_1, \ldots, f_s\}$) une base fixée de G (*resp.*F), nous avons ainsi la base suivante pour $\bigwedge^j G$ (*resp.*$\bigwedge^j F$) : $\{g_{\alpha_1} \wedge \ldots \wedge g_{\alpha_j} ; 1 \leq \alpha_1 < \ldots < \alpha_j \leq r\}$ (*resp.*$\{f_{\beta_1} \wedge \ldots \wedge f_{\beta_j} ; 1 \leq \beta_1 < \ldots < \beta_j \leq s\}$). Et les coefficients de la matrice de $\bigwedge^j \varphi$ dans ces bases sont précisément les mineurs de Φ de taille j indexés par $\underline{\alpha}$ et $\underline{\beta}$, notons $\Phi^{(j)}$ (puissance extérieure j-ème) cette matrice. Finalement notre choix de base pour F, G et $\bigwedge^j F, \bigwedge^j G$ induit un

homomorphisme de R-module :

$$\bigwedge^j F^* \otimes \bigwedge^j G \longrightarrow R$$
$$(f_{\beta_1} \wedge \ldots \wedge f_{\beta_j})^* \otimes g_{\alpha_1} \wedge \ldots \wedge g_{\alpha_j} \longrightarrow \Phi^{(j)}_{\underline{\alpha},\underline{\beta}} = |\, \Phi_{\alpha_i,\beta_{i'}} \,|_{1 \leq i,i' \leq j}$$

dont l'image est par définition $I_j\varphi$.

Nota Bene – Nous posons $I_j\varphi = R$ pour $j \leq 0$, et nous avons trivialement $I_j\varphi \subseteq I_{j'}\varphi$ pour $j' \leq j$.

Si M est de présentation finie alors tous les $I_j\varphi$ sont de type fini.

Proposition 1 – *Si* $\omega : R \to S$ *est un homomorphisme d'anneaux alors*

$$\omega(I_j\varphi).S = I_j\varphi_S$$

où $F \otimes_R S \xrightarrow{\varphi_S} G \otimes_R S \xrightarrow{\varepsilon_S} M \otimes_R S \to 0.$

Démonstration – L'exactitude à droite du produit tensoriel (*cf.* [1], chap.I, §2.1, lemme 1) montre que la suite ci-dessus est une présentation de $M \otimes_R S$ et la matrice de φ_S est précisément $\omega(\Phi)$. □

Proposition 2 – *Si* $F' \xrightarrow{\varphi'} G' \xrightarrow{\varepsilon'} M \to 0$ *est une autre présentation de* M, *pour tout* $i \geq 0$, *on a* $I_{r'-i}\varphi' = I_{r-i}\varphi$ *où* $r' = \mathrm{rg}\, G'$ *et* $r = \mathrm{rg}\, G$.

Démonstration – On vérifie que si $G = G'$ a une base fixée les matrices de φ et φ' se déduisent l'une de l'autre par combinaisons linéaires (à coefficients dans R) de leurs colonnes. Ainsi $I_{r-i}\varphi = I_{r-i}\varphi'$ pour tout $i = 0, \ldots, r$ et donc pour tout $i \in \mathbf{N}$ par convention.

Dans le cas général, soient $m_1, \ldots, m_r$ (*resp.* $m'_1, \ldots, m'_{r'}$) les générateurs de M dans chacune des présentations données. Pour tout $i = 1, \ldots, r'$ on a

$$m'_i = \sum_{j=1}^{r} a_{ij}.m_j \qquad a_{i,j} \in R \ ,$$

et donc $e_i = (a_{i1}, \ldots, a_{ir}, 0, \ldots, 0, -1, 0, \ldots, 0)$ est une relation entre $m_1, \ldots, m_r$, $m'_1, \ldots, m'_{r'}$. En fait, on obtient ainsi un système générateur de toutes les relations entre $m_1, \ldots, m_r, m'_1, \ldots, m'_{r'}$ modulo les relations entre $m_1, \ldots, m_r$.

Considérons la présentation suivante :

$$F'' \xrightarrow{\varphi''} G' \oplus G \xrightarrow{\varepsilon'+\varepsilon} M \to 0$$

où $F'' = F \oplus \oplus_{i=1}^{r'} R.e_i$. La matrice de φ'' s'écrit $\begin{pmatrix} \Phi & B \\ 0 & -\mathrm{Id}_{r'} \end{pmatrix}$ où Φ est la matrice de φ et B une matrice $r \times r'$. On en déduit facilement $I_{r''-i}\varphi'' = I_{r-i}\varphi$ pour $i \in \mathbf{N}$ et où $r'' = r + r'$. Par symétrie on a aussi $I_{r''-i}\varphi'' = I_{r'-i}\varphi'$, car on a vu que $I_{r''-i}\varphi''$ ne dépend pas du choix de la présentation lorsqu'une base de $G' \oplus G$ est fixée, d'où le résultat. □

Définition (*voir* **[2])** – On pose $\mathrm{Fitt}_i(M) = I_{r-i}\varphi$ le *i-ème invariant de Fitting de M*. On a

$$(0) \subseteq \mathrm{Fitt}_0(M) \subseteq \mathrm{Fitt}_1(M) \subseteq \ldots \subseteq \mathrm{Fitt}_r(M) = R \ .$$

On appelle encore $\mathrm{Fitt}_0(M)$, *l'invariant de Fitting initial de M*.

Nota Bene – Dans la suite, j'appelle *premier invariant de Fitting de M* le premier idéal $\mathrm{Fitt}_i(M)$ non nul, et le noterai simplement $\mathrm{Fitt}(M)$.

Si M est un module libre fini (*i.e.* $M \simeq R^r$) alors on peut prendre $\varphi = 0$ comme présentation et on calcule

$$\mathrm{Fitt}_i(M) = \begin{cases} (0) & \text{si } i < r \\ R & \text{si } i \geq r \end{cases} .$$

On vérifie aussi avec la proposition 1 ci-dessus $\mathrm{Fitt}_i(M \otimes_R S) = \omega(\mathrm{Fitt}_i(M))$.

§ 2. Quelques propriétés de l'invariant de Fitting initial

Si $s < r$ dans une présentation finie $R^s \xrightarrow{\varphi} R^r \xrightarrow{\varepsilon} M \to 0$ de M alors on a clairement $I_r\varphi = (0)$ et donc $\mathrm{Fitt}_0(M) = (0)$. On a aussi dans ce cas $\mathrm{Ann}_R M = (0)$, car sinon il existe $a \in \mathrm{Ann}_R M \setminus \{0\}$ et au moins r relations de dépendance linéaire indépendantes (*i.e.* $am_i = 0;\ i = 1, \ldots, r$).

Plus généralement on a :

Proposition 3 – *Pour tout R-module M engendré par $\leq r$ éléments on a :*

$$(\mathrm{Ann}_R M)^r \subseteq \mathrm{Fitt}_0(M) \subseteq \mathrm{Ann}_R M \ .$$

En particulier, si M est engendré par un seul élément alors $\mathrm{Fitt}_0(M) = \mathrm{Ann}_R M$.

Démonstration – Supposons $s \geq r$ et prenons une sous-matrice $r \times r$ de Φ arbitraire, disons Φ' , alors on a $(m_1, \ldots, m_r)\Phi' = (0, \ldots, 0)$ dans M . Et en multipliant par la matrice adjointe de Φ' on obtient $\mathrm{Det}\,\Phi'.(m_1, \ldots, m_r) = (0, \ldots, 0)$ dans M (c'est la règle de Kramer). Comme $m_1, \ldots, m_r$ engendre M ceci montre $\mathrm{Det}\,\Phi' \in \mathrm{Ann}_R M$ et (par définition de $I_r\varphi$) $\mathrm{Fitt}_0(M) = I_r\varphi \subseteq \mathrm{Ann}_R M$.

Soient $c_1, \ldots, c_r \in \mathrm{Ann}_R M$ arbitraires, construisons à partir d'une présentation donnée φ de M une présentation φ' de M telle que :

$$R^r \oplus F \xrightarrow{\varphi'} R^r \xrightarrow{\varepsilon} M \to 0$$

où $\varphi' = \varphi'' \oplus \varphi$ avec $\varphi''(a_1, \ldots, a_r) = (c_1a_1, \ldots, c_ra_r)$. Comme $c_1, \ldots, c_r \in \mathrm{Ann}_R M$ on vérifie $\varepsilon \circ \varphi' = 0$. Maintenant

$$\mathrm{Fitt}_0(M) = I_r\varphi' \ni \begin{vmatrix} c_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & c_r \end{vmatrix} = c_1 \cdots c_r$$

ce qui montre que $(\mathrm{Ann}_R M)^r \subseteq \mathrm{Fitt}_0(M)$ car tout élément de $(\mathrm{Ann}_R M)^r$ est une combinaison linéaire de produits $c_1 \cdots c_r$ d'éléments $c_1, \ldots, c_r \in \mathrm{Ann}_R M$. □

Remarque – En fait, l'argument ci-dessus démontre

$$(\mathrm{Ann}_R M)^q.\mathrm{Fitt}_{q+j}(M) \subseteq \mathrm{Fitt}_j(M)$$

pour $j \geq 0$ et $0 \leq q \leq r$.

Corollaire 4 – *Si $M = R/I$ (I idéal de R , i.e. M module cyclique) alors* $\mathrm{Fitt}_0(M) = \mathrm{Ann}_R M = I$.

Démonstration – Clair d'après la proposition 3 avec $r = 1$. □

Exemple (suite) : Considérant $M = \tilde{R}/\tilde{I}$ comme un $\tilde{R}$-module, on obtient $\mathrm{Fitt}_0(M) = \tilde{I}$ mais, regardant M comme R-module, on écrit la présentation suivante $(R = \mathbf{k}[z_1, z_2])$

$$R^2 \xrightarrow{\varphi} R^2 \xrightarrow{\varepsilon} M \to 0$$

où $\varepsilon(a_1, a_2) = a_1 + a_2z_3 (\mathrm{mod}\, \tilde{I})$ et $\varphi(a_1, a_2) = (a_1p, a_2p)$ avec $p = (2z_1 - 1)^2 + 4z_2^2 - 1$. Par conséquent

$$\mathrm{Fitt}_0(M) = I_2\varphi = \begin{vmatrix} p & 0 \\ 0 & p \end{vmatrix} = (p^2)$$

est I-primaire de longueur 2 .

§ 3. Autres propriétés des invariants de Fitting

Proposition 5 – *Soit* $0 \to M' \to M \to M'' \to 0$ *une suite exacte de* R *-modules de type fini. Alors pour* $j', j'' \geq 0$ *on a* $\mathrm{Fitt}_{j'}(M').\mathrm{Fitt}_{j''}(M'') \subseteq \mathrm{Fitt}_j(M)$ *avec* $j = j' + j''$ *et* $\mathrm{Fitt}_j(M) \subseteq \mathrm{Fitt}_j(M'')$ *pour tout* $j \geq 0$ *.*

Démonstration – On peut supposer que M' est un sous-module de M et on choisit des générateurs $g'_1, \ldots, g'_{r'}$ de M' et des éléments $g_1, \ldots, g_{r''} \in M$ tels que leurs images $g''_1, \ldots, g''_{r''}$ engendrent M'' .

Ceci assure que $\{g_1, \ldots, g_r\} = \{g_1, \ldots, g_{r''}, g'_1, \ldots, g'_{r'}\}$ est un système générateur de M , de plus une relation entre $\{g''_1, \ldots, g''_{r''}\}$ de la forme $a_1 g''_1 + \cdots + a_{r''} g''_{r''} = 0$ conduit à $a_1 g_1 + \cdots + a_{r''} g_{r''} \in M'$ et à une relation

$$a_1 g_1 + \cdots + a_{r''} g_{r''} + b_1 g'_1 + \cdots + b_{r'} g'_{r'} = 0$$

dans M . Soit Φ' $(resp. \Phi'')$ une matrice de relations entre les éléments de $\{g'_1, \cdots, g'_{r'}\}$ (*resp.* $\{g''_1, \cdots, g''_{r''}\}$), alors on obtient une matrice $\Phi = \begin{pmatrix} \Phi'' & 0 \\ B & \Phi' \end{pmatrix}$ de relations entre $\{g_1, \cdots, g_r\}$ où B est une certaine matrice.

- Parmi les $(r-j)$-mineurs de Φ , on trouve des mineurs de la forme $\begin{pmatrix} D'' & 0 \\ C & D' \end{pmatrix}$ où D' et D'' sont des mineurs arbitraires de tailles $r' - j'$ et $r'' - j''$ de Φ' et Φ'' respectivement avec $j' + j'' = j$. Ainsi

$$I_{r-j}\varphi \supseteq I_{r'-j'}\varphi''.I_{r''-j''}\varphi''.$$

- Tout $(r-j)$-mineur de Φ non nul est de la forme $\begin{pmatrix} D'' & 0 \\ C & D' \end{pmatrix}$ où D' et D'' sont des sous-matrices $(r'-j') \times (r'-j'-i)$ et $(r''-j'') \times (r''-j''+i)$ de Φ' et Φ'' respectivement, avec $0 \leq j' \leq r'$, $0 \leq i \leq r'-j'$ et $j'+j'' = j$. En effet pour former un $(r-j)$-mineur de Φ non nul on ne peut prendre que $0 \leq r'-j' \leq r'$ lignes de Φ' et donc au moins $r''-j'' \geq r''-j$ lignes de Φ'' , et $0 \leq r'-j'-i \leq r'-j'$ colonnes de Φ' . Ainsi

$$\mathrm{Fitt}_j(M) = I_{r-j}\varphi \subset \sum_{\substack{j'+j'' \leq j \\ 0 \leq j' \leq r'}} I_{r'-j'}\varphi'.I_{r''-j''}\varphi'' \subset I_{r''-j}\varphi'' = \mathrm{Fitt}_j(M'') \ . \ \square$$

Remarquons que dans les hypothèses de la proposition 5 on a $\mathrm{Ann}_R M = \mathrm{Ann}_R M' \cap \mathrm{Ann}_R M''$. Lorsque la suite exacte de la proposition 5 est scindée, on a une formule exacte.

Proposition 6 – *Soient* M', M'' *des* R *-modules de type fini, alors pour tout* $j \geq 0$

$$\mathrm{Fitt}_j(M' \oplus M'') = \sum_{j'+j''=j} \mathrm{Fitt}_{j'}(M').\mathrm{Fitt}_{j''}(M'')$$

En particulier, $\mathrm{Fitt}(M' \oplus M'') = \mathrm{Fitt}(M').\mathrm{Fitt}(M'')$ *.*

Démonstration – Soient $g'_1, \ldots, g'_{r'}$ (*resp.* $g''_1, \ldots, g''_{r''}$) des générateurs de M' (*resp.* M''), une relation entre $\{g_1, \ldots, g_r\} := \{g'_1, \ldots, g'_{r'}, g''_1, \ldots, g''_{r''}\}$ $(r = r' + r'')$ dans $M = M' \oplus M''$ se décompose en une relation entre $\{g'_1, \ldots, g'_{r'}\}$ et une autre entre $\{g''_1, \ldots, g''_{r''}\}$ dans M' et M'' respectivement. Ainsi une matrice Φ de relations entre $\{g_1, \ldots, g_r\}$ a la forme $\begin{pmatrix} \Phi' & 0 \\ 0 & \Phi'' \end{pmatrix}$.

Supposons d'abord $j < r$, alors un $(r-j)$ -mineur de Φ non nul est égal au produit d'un $(r'-j')$ -mineur de Φ' et d'un $(r''-j'')$ -mineur de Φ'' avec $j = j'+j''$, $j' \leq r'$ et $j'' \leq r''$. Ce mineur appartient donc à $I_{r'-j'}\varphi'.I_{r''-j''}\varphi''$, et par conséquent

$$\mathrm{Fitt}_j(M) \subseteq \sum_{j'+j''=j} \mathrm{Fitt}_{j'}(M').\mathrm{Fitt}_{j''}(M'') \ .$$

L'inclusion inverse suit de la proposition 5.

Si $j \geq r$, alors $\mathrm{Fitt}_j(M) = R = \mathrm{Fitt}_{r'}(M') = \mathrm{Fitt}_{j-r'}(M'') = \mathrm{Fitt}_{r'}(M').\mathrm{Fitt}_{j-r'}(M')$ car $j - r' \geq r''$. $\square$

Corollaire 7 – *Soit* $M = \oplus_{i=1}^{r} R/I_i$ *où* I_i *est un idéal de* R *, alors* $\mathrm{Fitt}_0(M) = I_1 \ldots I_r$ *.*

Démonstration – On combine la proposition 6 et le corollaire 4. $\square$

Remarque – Si $I_1 = \ldots = I_r$ alors $\mathrm{Fitt}_0(M) = I^r = (\mathrm{Ann}_R M)^r$ (comparer avec la proposition 3).

§ 4. "Signification" des invariants de Fitting supérieurs

La propriété suivante est claire par définition des invariants de Fitting (et nous l'avons déjà observée).

Scolie – *Si* M *est engendré par* $\leq r$ *éléments alors* $\mathrm{Fitt}_r(M) = R$ *.*

Démonstration – En effet $\mathrm{Fitt}_r(M) = I_0\varphi = R$ par définition. $\square$

Si R est un *anneau local*, c'est-à-dire un anneau commutatif, unitaire, nœthérien n'ayant qu'un seul idéal maximal $\mathfrak{p}$, la réciproque est vraie.

Proposition 8 – *Si* $(R, \mathfrak{p})$ *est un anneau local alors,* $\mathrm{Fitt}_r(M) = R$ *si et seulement si* M *peut-être engendré par* $\leq r$ *éléments.*

Démonstration – L'implication réciproque suit de la scolie. Considérons une présentation minimale de M, c'est-à-dire $R^t \xrightarrow{\varphi} R^s \xrightarrow{\varepsilon} M \to 0$ où les coefficients de la matrice Φ de φ sont dans $\mathfrak{p}$. L'existence d'une telle présentation est assurée par le fait que toute relation entre des générateurs de M faisant intervenir un coefficient qui n'est pas dans $\mathfrak{p}$ (donc inversible dans R) permet d'éliminer un de ces générateurs. Il est alors clair, que $\mathrm{Fitt}_j(M) = I_{s-j}\varphi \subset \mathfrak{p}$ pour $j < s$ par définition . Comme on suppose $\mathrm{Fitt}_r(M) = R$ on a $r \geq s$ ce qui achève la démonstration. $\square$

Pour I idéal de R posons $V(I) = \{\mathfrak{p} \in \mathrm{Spec}\, R;\ I \subset \mathfrak{p}\}$ l'ensemble des “points fermés” de I, alors la proposition 8 se réénonce, grâce à la proposition 1,

$$V(\mathrm{Fitt}_r(M)) = \{\mathfrak{p} \in \mathrm{Spec}\, R\ ; M_\mathfrak{p} \text{ n'est pas engendré sur } R_\mathfrak{p} \text{ par } r \text{ éléments}\},$$

où $R_\mathfrak{p}$ est le *localisé de* R *en* $\mathfrak{p}$ (obtenu en inversant tous les éléments de $R \setminus \mathfrak{p}$) et $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$. Naturellement cet ensemble est fermé pour la topologie de Zariski de $\mathrm{Spec}\, R$. En particulier, la proposition 3 montre que $V(\mathrm{Ann}_R\, M) = V(\mathrm{Fitt}_0 M)$ est égal à l'ensemble des $\mathfrak{p} \in \mathrm{Spec}\, R$ tels que $M_\mathfrak{p} \neq 0$, pour tout R-module M de type fini. On appelle ce sous-ensemble de $\mathrm{Spec}\, R$, le *support* de M.

Rappelons qu'un module de présentation finie M est *projectif* si et seulement si il est localement libre (*i.e.* pour tout $\mathfrak{p} \in \mathrm{Spec}\, R$ le $R_\mathfrak{p}$-module $M_\mathfrak{p}$ est libre, [1], chap.II, §5.2). Dans ce cas M est dit de *rang constant* si et seulement si $M_\mathfrak{p} \simeq R_\mathfrak{p}^r$ pour un entier r indépendant de $\mathfrak{p}$. Les invariants de Fitting des modules projectifs, de présentation finie ont une agréable propriété.

Proposition 9 – *Soit* M *un module de présentation finie. Si* M *est projectif alors pour tout* $j \geq 0$ *l'invariant de Fitting* $\mathrm{Fitt}_j(M)$ *est engendré par un idempotent.*

Nota Bene – La réciproque est aussi vraie mais nous ne la démontrerons pas ici (*voir* [3], §4.4, thm.18).

Démonstration – Soit $F \xrightarrow{\varphi} G \xrightarrow{\varepsilon} M \to 0$ une présentation de M avec F, G libres, finis. Comme M est projectif on a $G \simeq \ker\varepsilon \oplus M = \varphi(F) \oplus M$, et $\varphi(F)$ étant facteur direct d'un module libre et également projectif. Ainsi on a un isomorphisme $j : \varphi(F) \oplus \ker\varphi \to F$ et $\varphi \circ j$ est une isomorphisme de $\varphi(F)$, si on appelle ω son inverse la projection $\pi : G \to \varphi(F)$ induit un isomorphisme $j \circ \omega \circ \pi : G \to F$ tel que $\varphi \circ j \circ \omega \circ \pi \circ \varphi = \varphi$. En effet pour $x \in F$, on écrit $\pi \circ \varphi(x) = \varphi(x)$ et $\varphi \circ j \circ \omega \circ \varphi(x) = \varphi(x)$ par définition de ω.

L'homomorphisme $j \circ \omega \circ \pi$ a une matrice Ω et, de $\varphi \circ (j \circ \omega \circ \pi) \circ \varphi = \varphi$ on déduit $\Phi\Omega\Phi = \Phi$. On vérifie que pour tout $j \geq 0$ la puissance extérieure j-ème de Φ et Ω satisfont la même relation $\Phi^{(j)}\Omega^{(j)}\Phi^{(j)} = \Phi^{(j)}$ (en fait $(AB)^{(j)} = A^{(j)}B^{(j)}$ car $(AB)^{(j)}_{\underline{\alpha},\underline{\beta}} = \sum_{|\underline{\gamma}|=j} A^{(j)}_{\underline{\alpha},\underline{\gamma}} B^{(j)}_{\underline{\gamma},\underline{\beta}}$). Maintenant la proposition suit du lemme suivant :

Lemme – *Si* $AB = A$ *où* B *est une matrice carrée* $q \times q$ *et* A, B *sont à coefficients dans* R, *soit* $\mathfrak{A}$ *(resp.* $\mathfrak{B}$*) l'idéal engendré par les coefficients de* A *(resp.* B*) alors il existe* $\beta \in \mathfrak{B}$ *tel que* $(1-\beta)\mathfrak{A} = 0$. *De plus, si* $A\Omega A = A$, *alors* $\mathfrak{A} = R\alpha$ *où* α *est un idempotent de* R *et* $(1-\alpha)\mathfrak{A} = 0$.

Démonstration – On a $A(\mathrm{Id} - B) = 0$ et donc pour toute ligne $(a_{i,1}, \ldots, a_{i,q})$ de A on a $(a_{i,1}, \ldots, a_{i,q}).(\mathrm{Id} - B) = 0$. On vérifie $a_{ij}.\mathrm{Det}(\mathrm{Id} - B) = 0$ par la règle de Kramer. Ainsi $\mathrm{Det}(\mathrm{Id} - B).\mathfrak{A} = 0$ et on écrit $\mathrm{Det}(\mathrm{Id} - B) = 1 - \beta$ avec $\beta \in \mathfrak{B}$.

Posons $B = \Omega A$, alors $(1-\beta)\mathfrak{A} = 0$ pour un certain $\beta \in \mathfrak{B}$. Mais $\beta \in \mathfrak{B} \subset \mathfrak{A}$ car $B = \Omega A$ et on obtient $(1-\beta)\beta = 0$ ce qui est équivalent à $\beta^2 = \beta$. Posons $\alpha = \beta$, on a $R\alpha \subset \mathfrak{A}$ et pour $x \in \mathfrak{A}$ on écrit $x = \alpha x + (1-\alpha)x = \alpha x$ car $(1-\alpha)x = 0$, d'où $\mathfrak{A} = R\alpha$. $\square$

Remarque – Il existe une bijection entre les idempotents de R et les sous-ensembles de $\mathrm{Spec}\, R$ ouverts et fermés, donnée par $\eta \to V(R\eta)$ (*voir* [3], §4.4, thm.17). Ainsi la proposition ci-dessus montre que pour tout module M projectif, de présentation finie, $V(\mathrm{Fitt}_j(M))$ est à la fois ouvert et fermé et la réciproque est également vraie. En particulier, si R n'a pas d'idempotent non trivial (*i.e.* $\mathrm{Spec}\, R$ est connexe) et M est un R-module de type fini alors M est projectif si et seulement si $\mathrm{Fitt}_j(M) = (0)$ si $j < r$ et $= R$ si $j \geq r$ pour un certain r, ce qui s'écrit encore $\mathrm{Fitt}(M) = R$.

Dans la même veine on peut énoncer :

Proposition 10 – *Soit* M *un module de présentation finie. Alors* M *est projectif de rang constant si et seulement si* $\mathrm{Fitt}(M) = R$.

Démonstration – Si M est projectif de rang constant, disons r , alors pour tout premier $\mathfrak{p}$ le $R_\mathfrak{p}$-module $M_\mathfrak{p}$ est isomorphe à $R_\mathfrak{p}^r$. Et donc

$$\operatorname{Fitt}_j(M_\mathfrak{p}) = \operatorname{Fitt}_j(M).R_\mathfrak{p} = \begin{cases} (0) & \text{si } j < r \\ R & \text{si } j \geq r \end{cases} .$$

On en déduit directement

$$\operatorname{Fitt}_j(M) = \begin{cases} (0) & \text{si } j < r \\ R & \text{si } j \geq r \end{cases} ,$$

qui implique $\operatorname{Fitt}(M) = R$.

Supposons $\operatorname{Fitt}_j(M) = \begin{cases} (0) & \text{si } j < r \\ R & \text{si } j \geq r \end{cases}$, localisant à tout premier $\mathfrak{p}$ il suit de la proposition 8 que $M_\mathfrak{p}$ peut être engendré à r éléments et donc à une présentation $F_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} R_\mathfrak{p}^r \to M_\mathfrak{p} \to 0$. Mais $\operatorname{Fitt}_{r-1}(M_\mathfrak{p}) = (0)$ signifie $I_1\varphi_\mathfrak{p} = (0)$, c'est-à-dire que la matrice de $\varphi_\mathfrak{p}$ est nulle et $\varphi_\mathfrak{p} = 0$. Ainsi $M_\mathfrak{p}$ est localement libre de rang r pour tout $\mathfrak{p}$. □

Remarque – La proposition 10 et la remarque précédente entraîne que si R n'a pas d'idempotent non trivial, alors tout R-module de type fini, projectif est de rang constant.

§ 5. **Diviseur attaché à un module**

Etablissons d'abord une propriété de l'idéal de Fitting initial d'un module sur un anneau de Krull.

Proposition 11 – *Soit R un anneau de Krull et M un R-module de type fini alors, si* $\operatorname{Ann}_R M \neq (0)$,

$$\operatorname{div}(\operatorname{Fitt}_0(M)) = \sum_v \ell(M_v).\operatorname{div}(\mathfrak{p}_v)$$

où la somme porte sur les valuations essentielles de R et $M_v = M \otimes_R R_v$.

Démonstration – Soient $R^s \xrightarrow{\varphi} R^r \xrightarrow{\varepsilon} M \to 0$ une présentation finie de M et v une valuation essentielle de R . On en déduit une présentation finie de M_v dont on écrit la matrice $\Phi_v = (a_{ij})_{\substack{1\leq i\leq s \\ 1\leq j\leq r}}$. On choisit i_0, j_0 tels que $v(a_{i_0,j_0}) = \min_{i,j}(v(a_{ij}))$, quitte à permuter lignes et colonnes on peut supposer $i_0 = j_0 = 1$. On a alors $a_{1,j} = a_{1,1}.b_j$ où $b_j \in R_v$ pour $j = 1, \ldots, r$ et, retranchant b_j fois la première ligne de Φ_v à sa j-ème ligne (ce qui correspond à faire un changement de base de R^r) on obtient une matrice de la forme

$$\Phi_v = \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{s,1} \\ 0 & & & \\ \vdots & & \Phi_v^{(1)} & \\ 0 & & & \end{pmatrix} .$$

Itérant la manipulation avec $\Phi_v^{(1)}, \Phi_v^{(2)} \ldots$ On réécrit par changement de base de R^r une matrice de φ_v de la forme

$$\begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & \cdots & \cdots & a_{s,1} \\ 0 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 0 & a_{r,r} & \cdots & a_{s,r} \end{pmatrix}$$

où pour $1 \leq i \leq r$ et $i \leq j \leq s$ on a $v(a_{ij}) \geq v(a_{ii})$. On en déduit $v(I_r\varphi) = v(I_r\varphi_v) = \sum_{i=1}^r v(a_{ii})$. D'un autre côté, cette écriture de la matrice de φ_v montre que

$$M_v \simeq R_v^r/\varphi_v(R_v^s) \simeq \oplus_{i=1}^r R_v/R_v.a_{i,i} \simeq \oplus_{i=1}^r R_v/\mathfrak{p}_v^{v(a_{i,i})}$$

où $\mathfrak{p}_v$ est l'idéal maximal de R_v . Et donc, d'après la proposition 1 de l'exposé 1,

$$\ell(M_v) = \sum_{i=1}^r \ell(R_v/\mathfrak{p}_v^{v(a_{i,i})}) = \sum_{i=1}^r v(a_{ii}) = v(I_r\varphi) ,$$

ce qui entraîne le résultat. □

Définition – On appelle *diviseur attaché* à un R-module M satisfaisant $\operatorname{Ann}_R M \neq (0)$, et on note $\chi(M)$, le diviseur $\operatorname{div}(\operatorname{Fitt}_0(M))$.

Corollaire 12 – *Soient R un anneau de Krull et $0 \to M' \to M \to M'' \to 0$ une suite exacte de R-modules de type fini, alors si $\operatorname{Ann}_R M \neq (0)$ on a*

$$\chi(M) = \chi(M') + \chi(M'') .$$

En particulier, si M et N sont deux R-modules tels que $\operatorname{Ann}_R(M+N) \neq 0$ alors

$$\chi(M+N) + \chi(M \cap N) = \chi(M) + \chi(N) .$$

Démonstration – Pour chaque valuation essentielle v de R on déduit de la suite exacte de R-modules une suite exacte de R_v-modules

$$0 \to M'_v \to M_v \to M''_v \to 0 \ .$$

La proposition 1 de l'exposé 1 montre $\ell(M_v) = \ell(M'_v) + \ell(M''_v)$ et le résultat découle de la proposition 11 car $\mathrm{Ann}_R\, M'$ et $\mathrm{Ann}_R\, M''$ contiennent $\mathrm{Ann}_R\, M \neq (0)$.

On écrit les suites exactes de R-modules

$$0 \to N \to (M+N) \to (M+N)/N \to 0$$

$$0 \to M\cap N \to M \to M/M\cap N \to 0 \ ,$$

et on a $M/(M\cap N) \simeq (M+N)/N$. Comme $\mathrm{Ann}_R(M+N) \neq (0)$ on a $\mathrm{Ann}_R(M) \neq (0)$ et on déduit de ce qui précède

$$\chi(M/M\cap N) = \chi(M) - \chi(M\cap N) = \chi(M+N) - \chi(N) \ . \ \square$$

Références

[1] Bourbaki N. – *Algèbre commutative*, Hermann, Paris, 1969.

[2] Fitting H. – *Jahrbericht. DMV* 46, 1936, 195-228.

[3] Northcott D.G. – *Finite free resolution*, Cambridge Tracts in Math. 71, Cambridge Univ. Press, 1976.

Exposé n°3 : Idéaux éliminants

Patrice PHILIPPON

UMR 9994 du CNRS-Problèmes Diophantiens,
Université P. & M. Curie, T.46-56, 5ème ét., F-75252 PARIS cedex 05.

Soit $\mathbf{k}$ un corps commutatif.

Exemple : $\tilde{I} = I(C) = ((2z_1-1)^2 + 4z_2^2 - 1; (z_1^2+z_2^2)z_3^2 - 1)$
$I = I(\Gamma) = ((2z_1-1)^2 + 4z_2^2 - 1)$

C
courbe de $\mathbf{k}^3$

$\downarrow \pi$ (projection)

Γ
courbe de $\mathbf{k}^2$

$\leftarrow 0$ (point)

Dans cet exemple la surjectivité de π fait défaut. Il n'y a pas de point de C au-dessus du point $0 \in \Gamma$, qui est pourtant bien le lieu des zéros de I . La réponse ici est que le point de C au-dessus de 0 est “à l'infini” de $\mathbf{k}^3$. Mais on sait qu'en rajoutant à $\mathbf{k}^3$ un plan projectif $\mathbf{P}_2(\mathbf{k})$ (à l'infini) on obtient un espace projectif $\mathbf{P}_3(\mathbf{k})$ où le problème disparait. L'espace $\mathbf{P}_3(\mathbf{k})$ est l'espace des directions de $\mathbf{k}^4$ et passer de $\mathbf{k}^3$ à $\mathbf{P}_3(\mathbf{k})$ revient à considérer des cônes épointés dans $\mathbf{k}^4$.

Plus généralement, on considère un anneau commutatif, unitaire, nœthérien R et $A = R[z_0,\dots,z_n]$, notons $\mathfrak{m} = (z_0,\dots,z_n)$ l'idéal maximal trivial de A . Si M est un A-module gradué on écarte les $\mathfrak{m}$-composantes de son annulateur en divisant par les puissances de $\mathfrak{m}$. On pose

$$\tilde{\mathfrak{E}}M = \cup_{k\geq 0} \mathrm{Ann}_R(\mathfrak{m}^k.M)$$

et on appelle cet idéal *l'idéal éliminant de* M . On remarque que les idéaux $\mathrm{Ann}_R(\mathfrak{m}^k M)$ sont emboîtés et que, l'anneau étant nœthérien, cette chaîne croissante est ultimement stationnaire et il existe $k_0 \geq 0$ tel que $\tilde{\mathfrak{E}}M = \mathrm{Ann}_R(\mathfrak{m}^{k_0} M)$. Notons aussi

$$\tilde{\mathfrak{C}}M = \cup_{k\geq 0} \mathrm{Ann}_A(\mathfrak{m}^k M)$$

l'idéal caractéristique de M . C'est un idéal homogène de A et on a trivialement $\tilde{\mathfrak{E}}M = \tilde{\mathfrak{C}}M \cap R$.

Proposition 1 – *Soit M un A-module gradué satisfaisant $\mathfrak{m}^k M \neq 0$ pour tout $k \geq 0$. Si tout diviseur de zéro sur M appartient à $\tilde{\mathfrak{C}}M$ (en particulier si M est simple) alors $\tilde{\mathfrak{C}}M = \operatorname{Ann}_A M$ et $\tilde{\mathfrak{E}}M = \operatorname{Ann}_R M$ sont premiers. Si tout diviseur de zéro sur M appartient au radical de $\tilde{\mathfrak{C}}M$ alors $\tilde{\mathfrak{C}}M = \operatorname{Ann}_A M$ et $\tilde{\mathfrak{E}}M = \operatorname{Ann}_R M$ sont primaires.*

Si R est un anneau semi-régulier et $\tilde{\mathfrak{E}}M$ est premier alors

$$\operatorname{rg} \tilde{\mathfrak{C}}M \leq \operatorname{rg} \tilde{\mathfrak{E}}M + n \ .$$

Démonstration – Soient $a, b \in R$ (*resp.* A) tels que $ab \in \tilde{\mathfrak{E}}M$ (*resp.* $ab \in \tilde{\mathfrak{C}}M$), il existe $k \geq 0$ tel que $ab\mathfrak{m}^k M = 0$, mais aM (*resp.* bM) est un sous-module de M . Si $b \notin \tilde{\mathfrak{E}}M$ (*resp.* $b \notin \tilde{\mathfrak{C}}M$) alors a est diviseur de zéro sur M .

Si tout diviseur de zéro sur M appartient à $\tilde{\mathfrak{C}}M$, on a directement $a \in \tilde{\mathfrak{C}}M \cap R = \tilde{\mathfrak{E}}M$ (*resp.* $a \in \tilde{\mathfrak{C}}M$), ce qui montre que cet idéal est premier.

Si tout diviseur de zéro sur M appartient au radical de $\tilde{\mathfrak{C}}M$, il existe $k' \geq 0$ tel que $a^{k'} \in \tilde{\mathfrak{C}}M \cap R = \tilde{\mathfrak{E}}M$ (*resp.* $a^{k'} \in \tilde{\mathfrak{C}}M$), ce qui montre que cet idéal est primaire.

Prenons $b = 1$, si $a \notin \operatorname{Ann}_R M$ (*resp.* $a \notin \operatorname{Ann}_A M$) alors tout élément de $\mathfrak{m}^k$ est diviseur de zéro sur M et donc il existe $k' \geq 1$ tel que $\mathfrak{m}^{kk'} \subset \operatorname{Ann}_A M$, contrairement à l'hypothèse. Ainsi, en tout cas, $\tilde{\mathfrak{E}}M = \operatorname{Ann}_R M$ et $\tilde{\mathfrak{C}}M = \operatorname{Ann}_A M$.

Si $\tilde{\mathfrak{E}}M$ est premier, l'anneau $R/\tilde{\mathfrak{E}}M$ est intègre, notons K son corps des fractions. D'après la proposition 7, §2 de l'exposé 1, l'anneau A étant semi-régulier (en tant qu'anneau de polynômes sur R) on a

$$\operatorname{rg} \tilde{\mathfrak{C}}M/\tilde{\mathfrak{E}}M = \operatorname{rg} \tilde{\mathfrak{C}}M - \operatorname{rg} \tilde{\mathfrak{E}}M \ .$$

Notons $\mathfrak{P}$ l'idéal de $K[z_0, \ldots, z_n]$ engendré par les éléments de $\tilde{\mathfrak{C}}M/\tilde{\mathfrak{E}}M$, c'est un idéal premier de même rang que $\tilde{\mathfrak{C}}M/\tilde{\mathfrak{E}}M$ car $\mathfrak{P} \cap (R/\tilde{\mathfrak{E}}M) = (0)$. Mais l'anneau $K[z_0, \ldots, z_n]$ est de dimension $n+1$, $\mathfrak{P}$ est un idéal homogène de cet anneau et $\mathfrak{m} \not\subset \mathfrak{P}$ (car $\mathfrak{m}^k M \neq 0$ pour tout $k \geq 0$) et donc $\operatorname{rg} \mathfrak{P} \leq n$, ce qui entraîne

$$\operatorname{rg} \tilde{\mathfrak{C}}M - \operatorname{rg} \tilde{\mathfrak{E}}M \leq n \ . \ \square$$

En fait on constate que pour tout A-module M on a

$$\tilde{\mathfrak{C}}M = \tilde{\mathfrak{C}}(A/\tilde{\mathfrak{C}}M) \ .$$

En effet, $\tilde{\mathfrak{C}}M = \operatorname{Ann}_A(A/\tilde{\mathfrak{C}}M)$ et si $p \in \operatorname{Ann}_A(\mathfrak{m}^k A/\tilde{\mathfrak{C}}M)$ alors $p\mathfrak{m}^k \subset \tilde{\mathfrak{C}}M$ et il existe $k' \geq 0$ tel que $p\mathfrak{m}^{k+k'} \in \operatorname{Ann}_R M$ d'où $p \in \tilde{\mathfrak{C}}M$.

Pour étudier les idéaux $\tilde{\mathfrak{C}}M$ et $\tilde{\mathfrak{E}}M$ on peut donc se restreindre aux modules de la forme $M = A/I$ avec I idéal homogène de A .

§ 1. Idéaux éliminants

Dans l'exemple du début (et celui de l'exposé 2) la projection est "finie" (*i.e.* au dessus de chaque point de Γ (ou $\pi(C)$) il n'y a qu'un nombre fini de points de C). C'est une condition de l'élimination (si on a plus de variables que d'équations on ne peut en général toutes les éliminer). Pour utiliser l'élimination dans l'étude des variétés projectives on se ramène à ce cas en intersectant la variété donnée par suffisamment d'hyperplans (ou d'hypersurfaces) "génériques". Cette idée remonte aux U-résultants de Kronecker.

Le procédé est le suivant :

$$\begin{array}{lll}
\mathbf{P}_n & & \\
 & C(V) & \\
 & \overset{\pi_1}{\longleftarrow} & \\
V & & \\
 & \downarrow \pi_2 & \\
 & & \mathbf{P}^{\check{}}
\end{array}$$

$\mathbf{P}_n$ espace projectif

V sous-variété projective de $\mathbf{P}_n$

$\mathbf{P}^{\check{}} = \mathbf{P}^{\check{}}_{N_1} \times \ldots \times \mathbf{P}^{\check{}}_{N_h}$
produit d'espaces "duaux" de $\mathbf{P}_n$

$C(V) := \{(x,\mathbf{u}) \in \mathbf{P}_n \times \mathbf{P}^{\check{}};\ x \in V,\ u_1(x) = \ldots = u_h(x) = 0\}$
variété caractéristique de V

$\pi_1(C(V)) = V$

Soient R un anneau commutatif, unitaire et nœthérien, $A = R[z_0, \ldots, z_n]$, $\mathfrak{m} = (z_0, \ldots, z_n)$, $h \in \mathbf{N}$ et $d_1, \ldots, d_h$ des entiers > 0 . On pose $\mathbf{d} = (d_1, \ldots, d_h)$ et $R[\mathbf{d}]$ (*resp.* $A[\mathbf{d}]$) l'anneau des polynômes en les variables

$$\{u_\alpha^{(j)};\ j = 1, \ldots, h \quad \text{et} \quad \alpha \in \mathbf{N}^{n+1},\ |\alpha| = d_j\}$$

à cœfficients dans R (*resp.* A) et où on note $|\alpha| = \alpha_0 + \ldots + \alpha_n$. On considère un idéal homogène I de A et on pose

$$I[\mathbf{d}] = I.A[\mathbf{d}] + A[\mathbf{d}]U_1 + \ldots + A[\mathbf{d}]U_h$$

l'idéal de $A[\mathbf{d}]$ engendré par les éléments de I et les formes

$$U_j = \sum_{|\alpha| = d_j} u_\alpha^{(j)}.z_0^{\alpha_0} \ldots z_n^{\alpha_n} \quad (j = 1, \ldots, n) \ .$$

Si $h = 0$ on a par convention $\mathbf{d} = \emptyset$, $R[\mathbf{d}] = R$, $A[\mathbf{d}] = A$ et $I[\mathbf{d}] = I$.

Définition – On appelle *idéal caractéristique d'indice* $\mathbf{d}$ *de* I l'idéal de $A[\mathbf{d}]$ suivant

$$\mathfrak{C}_{\mathbf{d}} I := \cup_{k\geq 0} \operatorname{Ann}_{A[\mathbf{d}]}(\mathfrak{m}^k.A[\mathbf{d}]/I[\mathbf{d}]) = \tilde{\mathfrak{C}}(A[\mathbf{d}]/I[\mathbf{d}]) \ .$$

On appelle *idéal éliminant d'indice* $\mathbf{d}$ *de* I l'idéal de $R[\mathbf{d}]$

$$\mathfrak{E}_{\mathbf{d}} I := \mathfrak{C}_{\mathbf{d}} I \cap R[\mathbf{d}] = \tilde{\mathfrak{E}}(A[\mathbf{d}]/I[\mathbf{d}]) \ .$$

De façon générale, si B est un sous-anneau d'un anneau A, M un A-module, N un B-module et E un sous-ensemble de A, on notera

$$M :_N E = \{m \in N \ ; \ Em \subset M\}$$

le *transporteur de* M *par* E *dans* N, c'est un sous-module de N. On a, avec cette notation, $\mathfrak{C}_{\mathbf{d}} I = \cup_{k\geq 0} I[\mathbf{d}] :_{A[\mathbf{d}]} \mathfrak{m}^k$ et $\mathfrak{E}_{\mathbf{d}} I = \cup_{k\geq 0} I[\mathbf{d}] :_{R[\mathbf{d}]} \mathfrak{m}^k$.

Pour étudier les décompositions primaires des idéaux $\mathfrak{E}_{\mathbf{d}} I$ il est utile de décrire l'idéal $\mathfrak{C}_{\mathbf{d}} I$ de façon un peu différente. Notons $\mathfrak{S}A[\mathbf{d}]$ l'algèbre des polynômes à cœfficients dans A en les variables

$$\{s^{(j)}_{\alpha,\alpha'}; \ j = 1, \ldots, h \quad \text{et} \quad \alpha, \alpha' \in \mathbf{N}^{n+1}, \ |\alpha| = |\alpha'| = d_j\}$$

modulo les relations

$$s^{(j)}_{\alpha,\alpha'} = 0 \quad \text{et} \quad s^{(j)}_{\alpha,\alpha'} + s^{(j)}_{\alpha',\alpha} = 0 \ .$$

Et considérons le morphisme de A-algèbres suivant

$$\begin{aligned} \mathfrak{d} \ : \ A[\mathbf{d}] &\longrightarrow \ \mathfrak{S}A[\mathbf{d}] \\ u^{(j)}_\alpha &\longrightarrow \sum_{|\alpha'|=d_j} s^{(j)}_{\alpha,\alpha'}.z_0^{\alpha'_0} \ldots z_n^{\alpha'_n} \ . \end{aligned}$$

Lemme 2 – *Soit* M *un* A*-module gradué, de type fini et* N *un sous-module homogène contenant* $M_0 = \cup_{k\geq 0} 0 :_M \mathfrak{m}^k$, $M' = M \otimes_A A[\mathbf{d}]$, $N' = N \otimes_A A[\mathbf{d}]$ *et* $M'' = (M/M_0) \otimes_A \mathfrak{S}A[\mathbf{d}]$. *L'homomorphisme* $\mathfrak{d} : A[\mathbf{d}] \to \mathfrak{S}A[\mathbf{d}]$ *induit un homorphisme* $\mathfrak{d} : M' \to M''$ *dont le noyau satisfait*

$$N' \cap \ker \mathfrak{d} = \cup_{k\geq 0} (U_1 N' + \ldots + U_h N') :_{N'} \mathfrak{m}^k \ .$$

En particulier, si I *est un idéal homogène de* A *et* $p \in A[\mathbf{d}]$, *alors* $p \in \mathfrak{C}_{\mathbf{d}} I$ *si et seulement si* $\mathfrak{d}p \in \mathfrak{C}(I.\mathfrak{S}A[\mathbf{d}])$.

Démonstration – Si $m \in M'$ satisfait $\mathfrak{m}^k.m \in U_1 N' + \ldots + U_h N'$ pour un certain $k \geq 0$ alors $\mathfrak{d}(\mathfrak{m}^k.m) = \mathfrak{m}^k.\mathfrak{d}m = 0$ car

$$\mathfrak{d}U_j = \sum_{|\alpha|=d_j} \mathfrak{d}u^{(j)}_\alpha.z_0^{\alpha_0} \ldots z_n^{\alpha_n} = \sum_{|\alpha|=|\alpha'|=d_j} s^{(j)}_{\alpha,\alpha'}.z_0^{\alpha_0+\alpha'_0} \ldots z_n^{\alpha_n+\alpha'_n} = 0$$

grâce aux relations d'antisymétrie entre les variables $s^{(j)}_{\alpha,\alpha'}$. Et donc $\mathfrak{d}m \in M_0$ est nul dans M''.

Réciproquement, pour tout $i = 0, \ldots, n$ notons S_i l'ensemble multiplicatif formé des puissances positives de z_i, *i.e.* $S_i = \{z_i^m; \ m = 0, 1, \ldots\}$. On définit alors l'homomorphisme de A-algèbres

$$\mathfrak{s}_i : \mathfrak{S}A[\mathbf{d}] \longrightarrow S_i^{-1}.A[\mathbf{d}]$$

par

$$\mathfrak{s}_i(s^{(j)}_{\alpha,\alpha'}) = \begin{cases} u^{(j)}_\alpha / z_i^{d_j} & \text{si } \alpha'_i = d_j \text{ et } \alpha \neq \alpha' \\ -u^{(j)}_{\alpha'} / z_i^{d_j} & \text{si } \alpha_i = d_j \text{ et } \alpha \neq \alpha' \\ 0 & \text{sinon} \end{cases} \ .$$

On vérifie facilement pour tout $j = 1, \ldots, r$ et $|\alpha| = d_j$

$$\mathfrak{s}_i \circ \mathfrak{d}u^{(j)}_\alpha - u^{(j)}_\alpha \in S_i^{-1}(A[\mathbf{d}]U_1 + \ldots + A[\mathbf{d}]U_h) \subset S_i^{-1}.I[\mathbf{d}] \ .$$

Comme N' est engendré par les éléments de N on en déduit, pour tout $m \in N'$,

$$\mathfrak{s}_i \circ \mathfrak{d}m - m \in S_i^{-1}.(M_0 + U_1 N' + \ldots + U_h N') \ .$$

Si on suppose $\mathfrak{d}m = 0$, on a donc $m \in S_i^{-1}.(M_0 + U_1 N' + \ldots + U_h N')$. Ceci étant vrai pour tout $i = 0, \ldots, n$ entraîne l'existence d'un entier $k \geq 0$ tel que $\mathfrak{m}^k.m \subset U_1 N' + \ldots + U_h N'$.

Enfin, on applique ce qui précède aux modules $M = N = A/I$. On a $M'' = \mathfrak{S}A[\mathbf{d}]/\mathfrak{C}(I.\mathfrak{S}A[\mathbf{d}])$ et le noyau de $\mathfrak{d}$ est donc égal à l'image de $\cup_{k\geq 0} I[\mathbf{d}] :_{A[\mathbf{d}]} \mathfrak{m}^k = \mathfrak{C}_{\mathbf{d}} I$ dans $A[\mathbf{d}]/I.A[\mathbf{d}]$. On voit ainsi que $p \in A[\mathbf{d}]$ appartient à $\mathfrak{C}_{\mathbf{d}} I$ si et seulement si $\mathfrak{d}p \in \mathfrak{C}(I.\mathfrak{S}A[\mathbf{d}])$. $\square$

On peut alors établir les propriétés suivantes :

Proposition 3 – *Soit* I *un idéal homogène de* A *:*

(i) $\mathfrak{m} \subset \operatorname{Rad} I \Leftrightarrow \mathfrak{C}_{\mathbf{d}} I = A[\mathbf{d}] \Leftrightarrow \mathfrak{E}_{\mathbf{d}} I = R[\mathbf{d}]$,

(ii) *si* I *est premier (resp. primaire) et* $\mathfrak{m} \not\subset \operatorname{Rad} I$ *alors* $\mathfrak{C}_{\mathbf{d}} I$ *et* $\mathfrak{E}_{\mathbf{d}} I$ *sont premiers (resp. primaires),* $\operatorname{Rad} \mathfrak{C}_{\mathbf{d}} I = \mathfrak{C}_{\mathbf{d}} \operatorname{Rad} I$ *et* $\mathfrak{C}_{\mathbf{d}} I \cap A = I$,

(iii) *si* $I = I_1 \cap \ldots \cap I_m$ *alors* $\mathfrak{C}_{\mathbf{d}} I = \mathfrak{C}_{\mathbf{d}} I_1 \cap \ldots \cap \mathfrak{C}_{\mathbf{d}} I_m$ *et* $\mathfrak{E}_{\mathbf{d}} I = \mathfrak{E}_{\mathbf{d}} I_1 \cap \ldots \cap \mathfrak{E}_{\mathbf{d}} I_m$,

(iv) *si* $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$ *est une décomposition primaire normale de* I *alors* $\mathfrak{C}_{\mathbf{d}} I = \mathfrak{C}_{\mathbf{d}} \mathfrak{q}_1 \cap \ldots \cap \mathfrak{C}_{\mathbf{d}} \mathfrak{q}_m$ *est une décomposition primaire normale de* $\mathfrak{C}_{\mathbf{d}} I$ *dès qu'on omet les facteurs égaux à* $A[\mathbf{d}]$ *(i.e. tels que* $\mathfrak{m} \subset \operatorname{Rad} \mathfrak{q}$ *). Et les premiers isolés non triviaux associés à* I *et* $\mathfrak{C}_{\mathbf{d}} I$ *se correspondent.*

Démonstration – (i) S'il existe $k \geq 0$ tel que $\mathfrak{m}^k \subset I$ alors $1 \in \mathfrak{E}_{\mathbf{d}} I$ et réciproquement.
(ii) Le lemme 4, §1 de l'exposé 1 montre que l'idéal $I.\mathfrak{S}A[\mathbf{d}]$ est premier ou primaire suivant que I est premier ou primaire, il montre également que $\operatorname{Rad}(I.\mathfrak{S}A[\mathbf{d}]) = (\operatorname{Rad} I).\mathfrak{S}A[\mathbf{d}]$ est toujours premier dans ce cas.

De ceci et de l'hypothèse il suit $\mathfrak{m} \not\subset \operatorname{Rad}(I.\mathfrak{S}A[\mathbf{d}])$, et le lemme 2 implique dans ce cas $pq \in \mathfrak{E}_{\mathbf{d}} I$ si et seulement si $\mathfrak{d}(pq) \in I.\mathfrak{S}A[\mathbf{d}]$. En particulier, si $p = 1$ on vérifie $\operatorname{Rad}(\mathfrak{E}_{\mathbf{d}} I) = \mathfrak{E}_{\mathbf{d}} \operatorname{Rad} I$. Mais $\mathfrak{d}(pq) = \mathfrak{d}p\mathfrak{d}q$ et si $\mathfrak{d}p \notin I.\mathfrak{S}A[\mathbf{d}]$ on a nécessairement $\mathfrak{d}q \in (\operatorname{Rad} I).\mathfrak{S}A[\mathbf{d}]$ ce qui équivaut à $q \in \mathfrak{E}_{\mathbf{d}} \operatorname{Rad} I$. Et comme, toujours d'après le lemme 2, $\mathfrak{d}p \notin I.\mathfrak{S}A[\mathbf{d}]$ équivaut à $p \notin \mathfrak{E}_{\mathbf{d}} I$ on a bien montré que $\mathfrak{E}_{\mathbf{d}} I$ est premier (*resp.* primaire) dès que I est premier (*resp.* primaire). L'intersection d'un idéal premier (*resp.* primaire) avec un sous-anneau est premier (*resp.* primaire), d'où le résultat pour $\mathfrak{E}_{\mathbf{d}} I$.

Enfin $(\mathfrak{E}_{\mathbf{d}} I \cap A).\mathfrak{m}^k \subset I.\mathfrak{S}A[\mathbf{d}] \cap A = I$ et $\mathfrak{m}^k \not\subset \operatorname{Rad} I$ entraînent $\mathfrak{E}_{\mathbf{d}} I \cap A \subset I$, l'inclusion inverse étant claire.
(iii) On vérifie avec le lemme 4, §1 de l'exposé 1

$$I_1.\mathfrak{S}A[\mathbf{d}] \cap \ldots \cap I_m.\mathfrak{S}A[\mathbf{d}] = I.\mathfrak{S}A[\mathbf{d}] \ .$$

D'après cette identité et le lemme 2, $p \in \mathfrak{E}_{\mathbf{d}} I$ équivaut à l'existence d'un entier k tel que $\mathfrak{d}p.\mathfrak{m}^k \in I_j.\mathfrak{S}A[\mathbf{d}]$ pour tout $j = 1, \ldots, m$. Et, encore grâce au lemme 2, ceci équivaut à $p \in \mathfrak{E}_{\mathbf{d}} I_j$ pour tout $j = 1, \ldots, m$. L'identité pour les idéaux éliminants se déduit par intersection avec $R[\mathbf{d}]$, ce qui achève d'établir la proposition.
(iv) Si $\mathfrak{E}_{\mathbf{d}} I' \subset \mathfrak{E}_{\mathbf{d}} I$ on a $I' \subset \mathfrak{E}_{\mathbf{d}} I \cap A$ et, si I est primaire et $\mathfrak{m} \not\subset \operatorname{Rad} I$ il suit de (ii) $\mathfrak{E}_{\mathbf{d}} I \cap A = I$. En particulier, si $\mathfrak{m} \not\subset \operatorname{Rad} \mathfrak{q}_j$ et $\mathfrak{E}_{\mathbf{d}} \operatorname{Rad} \mathfrak{q}_i \subseteq \mathfrak{E}_{\mathbf{d}} \operatorname{Rad} \mathfrak{q}_j$ alors $\operatorname{Rad} \mathfrak{q}_i \subseteq \operatorname{Rad} \mathfrak{q}_j$. On en déduit que les premiers $\mathfrak{E}_{\mathbf{d}} \operatorname{Rad} \mathfrak{q}_i$, $(1 \leq i \leq m)$ ne contenant pas $\mathfrak{m}$ sont deux à deux distincts et que $\mathfrak{E}_{\mathbf{d}} \operatorname{Rad} \mathfrak{q}_i$ est un premier isolé associé à $\mathfrak{E}_{\mathbf{d}} I$ si et seulement si $\operatorname{Rad} \mathfrak{q}_i$ est un premier isolé non trivial associé à I. D'autre part, si pour $i_0 \in \{1, \ldots, m\}$ on a

$$\mathfrak{E}_{\mathbf{d}} \mathfrak{q}_{i_0} \supset \cap_{i \neq i_0} \mathfrak{E}_{\mathbf{d}} \mathfrak{q}_i = \mathfrak{E}_{\mathbf{d}} (\cap_{i \neq i_0} \mathfrak{q}_i)$$

on a $\mathfrak{q}_{i_0} \supset \cap_{i \neq i_0} \mathfrak{q}_i$ et, la décomposition de I étant normale, on doit avoir $\mathfrak{m} \subset \operatorname{Rad} \mathfrak{q}_{i_0}$. Ceci montre que la décomposition $\mathfrak{E}_{\mathbf{d}} I = \mathfrak{E}_{\mathbf{d}} \mathfrak{q}_1 \cap \ldots \cap \mathfrak{E}_{\mathbf{d}} \mathfrak{q}_m$ où on omet les facteurs triviaux, est bien normale. □

La proposition 3 montre que si $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$ est une décomposition primaire normale de I on a une décomposition primaire $\mathfrak{E}_{\mathbf{d}} I = \mathfrak{E}_{\mathbf{d}} \mathfrak{q}_1 \cap \ldots \cap \mathfrak{E}_{\mathbf{d}} \mathfrak{q}_m$ de $\mathfrak{E}_{\mathbf{d}} I$, mais celle-ci n'est pas nécessairement normale. En particulier, dans le schéma du début du paragraphe, comme V est irréductible et réduite il en est de même de $C(V)$ et de la projection $\pi_2(C(V))$.

§ 2. **Théorème de l'élimination**

L'interprétation géométrique de l'idéal éliminant est essentiellement contenue dans le théorème dit de l'élimination dont voici une version. Dans la figuration géométrique du §1, ce théorème montre que l'idéal $\mathfrak{E}_{\mathbf{d}} I$ (avec $I = I(V)$) défini bien la projection $\pi_2(C(V))$ dans $\mathbf{P}^{\check{}}$ et que la situation de l'exemple du début du paragraphe n'apparait pas ici.

Théorème de l'élimination – *Soit* $\rho : R[\mathbf{d}] \to \mathbf{k}$ *un homomorphisme de* $R[\mathbf{d}]$ *dans un corps* $\mathbf{k}$ *, les conditions suivantes sont équivalentes :*
(i) $\rho(\mathfrak{E}_{\mathbf{d}} I) = (0)$,
(ii) *il existe une extension* K *de* $\mathbf{k}$ *et un zéro non trivial de* $\rho(I[\mathbf{d}])$ *dans* K^{n+1} *(i.e.* $\exists \mathbf{x} = (x_0, \ldots, x_n) \in K^{n+1} \setminus \{0\}$; $\forall p \in I[\mathbf{d}]$, $\rho(p)(\mathbf{x}) = 0$ *).*

Démonstration – (ii) $\Rightarrow$ (i) Si $a \in \mathfrak{E}_{\mathbf{d}} I$ alors il existe $k \geq 0$ tel que $a.\mathfrak{m}^k \subset I[\mathbf{d}]$ et donc, si $(x_0, \ldots, x_n)$ est un zéro non trivial de $\rho(I[\mathbf{d}])$ dans K^{n+1} et i un indice tel que $x_i \neq 0$, on écrit $\rho(a).x_i^k = 0$ d'où $\rho(a) = 0$.

(i) $\Rightarrow$ (ii) Si ρ est l'homomorphisme nul tout point de $\mathbf{k}^{n+1}$ est zéro de $\rho(I[\mathbf{d}]) = (0)$, en particulier (ii) est satisfaite. Supposons dorénavant que ρ n'est pas l'homomorphisme nul, et montrons que pour tout entier $k \geq 0$ on a $\mathfrak{m}^k \not\subset J$ où J est l'idéal homogène de $\mathbf{k}[z_0, \ldots, z_n]$ engendré par les éléments de $\rho(I[\mathbf{d}])$. Soit $\mathbf{k}_0$ le corps des fractions de $\rho(R[\mathbf{d}])$, c'est un sous-corps de $\mathbf{k}$. Si $\mathfrak{m}^k \subset J$ alors $\mathfrak{m}^k \subset J \cap \mathbf{k}_0[z_0, \ldots, z_n]$, ce qui implique l'existence d'un élément $a \in R[\mathbf{d}]$ tel que $\rho(a).\mathfrak{m}^k \subset \rho(I[\mathbf{d}])$ et $\rho(a) \neq 0$. Il existe donc des éléments $(a_{\alpha,\alpha'})_{|\alpha|=|\alpha'|=k}$ de $\ker \rho \subset R[\mathbf{d}]$ satisfaisant, pour tout $|\alpha| = k$,

$$\sum_{|\alpha'|=k} (a.\delta_{\alpha,\alpha'} + a_{\alpha,\alpha'}).z_0^{\alpha'_0} \ldots z_n^{\alpha'_n} \in I[\mathbf{d}] \ ,$$

où $\delta_{\alpha,\alpha'}$ désigne le symbole de Kronecker. Si Δ est le déterminant de la matrice $(a.\delta_{\alpha,\alpha'} + a_{\alpha,\alpha'})_{|\alpha|=|\alpha'|=k}$ on vérifie sans peine les propriétés suivantes :

$$\Delta.\mathfrak{m}^k \subset I[\mathbf{d}] \quad \text{et donc} \quad \Delta \in \mathfrak{E}_{\mathbf{d}} I \ ,$$
$$\rho(\Delta) = \rho(a)^{\binom{k+n}{n}} \neq 0 \ ,$$

où $\binom{k+n}{n}$ est le nombre de monômes de degré k . Ainsi, lorsque $\mathfrak{m}^k \subset J$ on vérifie $\rho(\mathfrak{E}_{\mathbf{d}} I) \neq (0)$ et donc, sous l'hypothèse (i) on a $\mathfrak{m}^k \not\subset J$.

Soit i un indice dans $\{0, \ldots, n\}$ tel que pour tout entier $k \geq 0$ on ait $z_i^k \notin J$, un tel indice existe d'après ce qui précède et on vérifie que l'élément $1 - z_i$

de $\mathbf{k}[z_0,\ldots,z_n]$ n'est pas inversible modulo J. En effet, si $1-z_i$ est inversible modulo J notons $p_0+\cdots+p_M$ un inverse avec p_j polynôme homogène de degré j. Le polynôme $(1-z_i)(p_0+\cdots+p_M)-1$ appartient à l'idéal homogène J, ce qui entraîne par homogénéité que p_0-1, $z_ip_0-p_1,\ldots,z_ip_{M-1}-p_M$, z_ip_M et donc par télescopage aussi z_i^{M+1} appartiennent à J, contrairement au choix de l'indice i. En conséquence $1-z_i$ appartient à un idéal maximal $\mathfrak{M}$ de $\mathbf{k}[z_0,\ldots,z_n]$ contenant J, donc $\rho(I[\mathbf{d}])$. Et ρ induit un homomorphisme

$$\tilde{\rho}: A[\mathbf{d}] \longrightarrow \mathbf{k}[z_0,\ldots,z_n] \longrightarrow K := \mathbf{k}[z_0.\ldots,z_n]/\mathfrak{M}$$

de $A[\mathbf{d}]$ vers un corps K contenant $\mathbf{k}$, qui satisfait $\tilde{\rho}(z_i)=1\neq 0$ et $\tilde{\rho}(p)=0$ pour tout $p\in I[\mathbf{d}]$. Or $\tilde{\rho}(p)=\rho(p)(\tilde{\rho}(z_0),\ldots,\tilde{\rho}(z_n))$ ce qui permet de conclure que $(\tilde{\rho}(z_0),\ldots,\tilde{\rho}(z_n))$ est bien un zéro non trivial de $\rho(I[\mathbf{d}])$ dans K^{n+1} et achève la preuve du théorème. $\square$

Remarque – On notera que la seconde partie de la démonstration de (i) $\Rightarrow$ (ii) montre une forme faible du théorème dit des zéros de Hilbert : si pour tout $k\geq 0$ $z_i^k\notin J$ alors J a un zéro $(x_0,\ldots,x_n)\in K^{n+1}$ tel que $x_i\neq 0$.

§ 3. Rang des idéaux éliminants

Revenons à notre étude algébrique des idéaux caractéristiques et éliminants.

Lemme 4 – *Soit* $\mathfrak{p}$ *un idéal homogène premier de* A *tel que* $\mathfrak{m}\not\subset\mathfrak{p}$*, alors* $\operatorname{rg}\mathfrak{E}_{\mathbf{d}}\mathfrak{p}=\operatorname{rg}\mathfrak{p}+h$.

Démonstration – Soit r le rang de $\mathfrak{p}$, on a une chaîne d'idéaux premiers emboîtés de A

$$\mathfrak{p}_r\subsetneq\ \ldots\subsetneq\ \mathfrak{p}_0=\mathfrak{p}\ ,$$

qui induit la chaîne de $r+h+1$ idéaux de $A[\mathbf{d}]$ suivante :

$$\mathfrak{p}_r.A[\mathbf{d}]\subsetneq\ \ldots\subsetneq\ \mathfrak{p}_0.A[\mathbf{d}]\subset\mathfrak{E}_{(d_1)}\mathfrak{p}\subset\ldots\subset\mathfrak{E}_{(d_1,\ldots,d_{h-1})}\mathfrak{p}\subset\mathfrak{E}_{\mathbf{d}}\mathfrak{p}\subsetneq A[\mathbf{d}]\ .$$

D'après le lemme 4, §1 de l'exposé 1, les $r+1$ plus petits idéaux de cette chaîne sont premiers et deux à deux distincts. De même, d'après la proposition 3(i) et (ii), §1 les h plus gros idéaux de la chaîne sont premiers et propres. Si pour $i\in\{1,\ldots,h\}$ on a $U_i.\mathfrak{m}^k\subset\mathfrak{p}[(d_1,\ldots,d_{i-1})]$ alors $\mathfrak{m}^{k+d_i}\subset\mathfrak{p}[(d_1,\ldots,d_{i-1})]$ car les générateurs de ce dernier idéal ne font pas intervenir les variables $u_\alpha^{(i)}$, $|\alpha|=d_i$, d'où $\mathfrak{E}_{\mathbf{d}}\mathfrak{p}=A[\mathbf{d}]$. Ceci étant exclu car $\mathfrak{p}\not\supset\mathfrak{m}$ on en déduit $U_i\notin$

$\mathfrak{E}_{(d_1,\ldots,d_{i-1})}\mathfrak{p}$ $(i=1,\ldots,h)$, toutes les inclusions de la chaîne d'idéaux premiers ci-dessus sont strictes, et donc $\operatorname{rg}\mathfrak{E}_{\mathbf{d}}\mathfrak{p}\geq r+h$.

Par ailleurs, on peut trouver grâce au théorème de l'idéal principal, §2, exposé 1, des éléments homogènes $p_1,\ldots,p_r$ dans $\mathfrak{p}$ tels que $\operatorname{rg}(p_1,\ldots,p_r)=r$, l'idéal $\mathfrak{p}$ est alors un premier isolé associé à $(p_1,\ldots,p_r)$. D'après la proposition 3 (ii), $\mathfrak{E}_{\mathbf{d}}\mathfrak{p}$ est un premier isolé associé à $\mathfrak{E}_{\mathbf{d}}(p_1,\ldots,p_r)$ et donc aussi un premier isolé associé à $(p_1,\ldots,p_r,U_1,\ldots,U_h)$ dans $A[\mathbf{d}]$. Il résulte encore du théorème de l'idéal principal, §2, exposé 1, $\operatorname{rg}\mathfrak{E}_{\mathbf{d}}\mathfrak{p}\leq r+h$, ainsi $\operatorname{rg}\mathfrak{E}_{\mathbf{d}}\mathfrak{p}=r+h=\operatorname{rg}\mathfrak{p}+h$. $\square$

Soit $\mathfrak{p}$ un idéal homogène premier de A, on peut se restreindre au cas où l'anneau de base R est intègre pour l'étude de $\mathfrak{E}_{\mathbf{d}}\mathfrak{p}$. En effet, considérons l'homomorphisme $\varphi: R\to R/(\mathfrak{p}\cap R)$ que l'on étend à $A[\mathbf{d}]$ de façon évidente, alors $\mathfrak{E}_{\mathbf{d}}\mathfrak{p}=\varphi^{-1}(\mathfrak{E}_{\mathbf{d}}\varphi(\mathfrak{p}))$ car $\ker\varphi=\mathfrak{p}\cap R\subset\mathfrak{E}_{\mathbf{d}}\mathfrak{p}$.

Nous posons dans toute la suite de ce paragraphe $R':=R/(\mathfrak{p}\cap R)$, $A'=R'[z_0,\ldots,z_n]$ *et* $\varphi: R\to R'$ *le morphisme ci-dessus.*

Théorème 5 – *Soit* $\mathfrak{p}$ *un idéal homogène premier de* A *tel que* $\mathfrak{m}\not\subset\mathfrak{p}$*, on a* $\varphi(\mathfrak{E}_{\mathbf{d}}\mathfrak{p})=\mathfrak{E}_{\mathbf{d}}(\varphi(\mathfrak{p}))$ *et les propriétés suivantes :*

(i) $\mathfrak{E}_{\mathbf{d}}\mathfrak{p}=(\mathfrak{p}\cap R).R[\mathbf{d}]\ \Leftrightarrow\ \operatorname{rg}\varphi(\mathfrak{p})<n+1-h$,

(ii) *si* $\operatorname{rg}\varphi(\mathfrak{p})\geq n+1-h$ *alors* $\operatorname{rg}\mathfrak{E}_{\mathbf{d}}\varphi(\mathfrak{p})=\operatorname{rg}\mathfrak{C}_{\mathbf{d}}\varphi(\mathfrak{p})-n=\operatorname{rg}\varphi(\mathfrak{p})+h-n$.

La démonstration repose sur le fait suivant :

Fait 6 – *Soit* P *un idéal homogène premier de* A' *tel que* $P\cap R'=(0)$ *et supposons* $z_0\notin P$*. Pour* $t\in\{0,\ldots,h\}$ *on note* $\mathbf{d}_t=(d_1,\ldots,d_t)$ *et* R'_t *le sous-anneau de* $R'[\mathbf{d}]$ *des polynômes à cœfficients dans* $R'[\mathbf{d}_t]$ *en les variables*

$$\{u_\alpha^{(j)}\,;\ j=t+1,\ldots,h\quad\textit{et}\quad|\alpha|=d_j,\ \alpha_0\neq d_j\}\ ,$$

et $A'_t=R'_t[z_0,\ldots,z_n]$*. Alors si* $\operatorname{rg}P<n+1-t$ *avec* $t\leq h$*, on a*

$$\mathfrak{E}_{\mathbf{d}}P\cap A'_t=(\mathfrak{E}_{\mathbf{d}_t}P).A'_t\quad\textit{et}\quad\mathfrak{E}_{\mathbf{d}}P\cap R'_t=(0)\ .$$

Démonstration – L'anneau R' est intègre, considérons le corps des fractions $\mathbf{k}$ de R'_t. On a $P\cap R'_t=P\cap R'=(0)$ et, en notant $\bar{P}$ l'idéal premier engendré dans $B:=\mathbf{k}[z_0,\ldots,z_n]$ par P,

$$\mathfrak{E}_{\mathbf{d}_t}P\subset(\bar{P}+(U_1,\ldots,U_t)):_{\mathbf{k}}\mathfrak{m}^k$$

pour un certain entier $k \in \mathbf{N}$. Le rang de $\bar{P}$ est égal au rang de P car $P \cap R'_t = (0)$ et donc, d'après la proposition 7, §2 de l'exposé 1, $\mathrm{rg}(\bar{P} + (U_1, \ldots, U_t)) \leq \mathrm{rg}\, P + t$. Mais alors, d'après le choix de t , on a $\mathrm{rg}(\bar{P} + (U_1, \ldots, U_t)) < n+1$ et il existe un premier $\mathfrak{P}$ associé à $(\bar{P} + (U_1, \ldots, U_t))$, de rang $< n+1$. En particulier, $\mathfrak{P} \not\supset \mathfrak{m}$ et

$$\mathfrak{E}_{\mathbf{d}_t} P \subset (\bar{P} + (U_1, \ldots, U_t)) :_{\mathbf{k}} \mathfrak{m}^k \subset \mathfrak{P} :_{\mathbf{k}} \mathfrak{m}^k = (0) \ .$$

Soit maintenant $a \in \mathfrak{E}_{\mathbf{d}} P \cap A'_t$, il existe un entier k' tel que

$$a.z_0^{k'} \in P[\mathbf{d}] \ ,$$

et nous considérons l'homomorphisme de A'_t-algèbres

$$\mathfrak{s} : A'[\mathbf{d}] \to A'_t[\frac{1}{z_0}]$$

défini par

$$\mathfrak{s}(u_0^{(j)}) = -\sum u_\alpha^{(j)}.z_0^{\alpha_0 - d_j}.z_1^{\alpha_1} \ldots z_n^{\alpha_n} \quad (j = t+1, \ldots, h)$$

où la somme porte sur les $\alpha \in \mathbf{N}^{n+1}$ tels que $|\alpha| = d_j,\ \alpha_0 \neq d_j$ et où on a posé $u_0^{(j)} = u_\alpha^{(j)}$ pour $\alpha = (d_j, 0, \ldots, 0)$. On vérifie $\mathfrak{s}(P[\mathbf{d}]) \subset P[\mathbf{d}_t].A'_t[\frac{1}{z_0}]$, et a ne dépendant pas de $u_0^{(t+1)}, \ldots, u_0^{(h)}$ on a aussi $\mathfrak{s}(a) = a$, d'où $a.z_0^{k'} \in P[\mathbf{d}_t].A'_t[\frac{1}{z_0}]$. On en déduit l'existence d'un entier k'' tel que

$$a.z_0^{k''} \in P[\mathbf{d}_t].A'_t \subset \big(\mathfrak{E}_{\mathbf{d}_t} P\big).A'_t \ .$$

Comme $z_0 \notin P$ et $\mathfrak{E}_{\mathbf{d}_t} P \cap A' = P$ d'après la proposition 3 (ii), on a encore $z_0 \notin \mathfrak{E}_{\mathbf{d}_t} P$. Ce dernier idéal étant premier d'après la proposition 3(ii), on déduit de la relation précédente $a \in (\mathfrak{E}_{\mathbf{d}_t} P).A'_t$. On a donc $\mathfrak{E}_{\mathbf{d}} P \cap A'_t \subseteq \big(\mathfrak{E}_{\mathbf{d}_t} P\big).A'_t$ et l'inclusion inverse est claire. Intersectant l'égalité ainsi obtenue avec R'_t on obtient $\mathfrak{E}_{\mathbf{d}} P \cap R'_t = \big(\mathfrak{E}_{\mathbf{d}_t} P\big).R'_t = (0)$, ce qui établit le fait 6. □

Démonstration du théorème 5 – Comme $\mathfrak{m} \not\subset \mathfrak{p}$ on peut supposer, quitte à réindexer les variables $z_0, \ldots, z_n$, que $z_0 \notin \mathfrak{p}$. On a déjà remarqué $\mathfrak{E}_{\mathbf{d}} \mathfrak{p} = \varphi^{-1}(\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}))$ car $\ker \varphi = \mathfrak{p} \cap R \subset \mathfrak{E}_{\mathbf{d}} \mathfrak{p}$.
(i) Si $\mathrm{rg}\, \varphi(\mathfrak{p}) < n+1-h$ on applique le fait 6 avec $t = h$, $R'_t = R'[\mathbf{d}]$ et $P = \varphi(\mathfrak{p})$ pour obtenir $\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}) = (0)$ qui équivaut à $\mathfrak{E}_{\mathbf{d}} \mathfrak{p} = \ker \varphi.R[\mathbf{d}] = (\mathfrak{p} \cap R).R[\mathbf{d}]$. Dans l'autre sens, supposons $\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}) = (0)$ et reprenons le corps $\mathbf{k}$ des fractions de $R'[\mathbf{d}]$, l'anneau B , $P = \varphi(\mathfrak{p})$ et l'idéal $\bar{P}$ de la preuve du fait 6 pour $t = h$. Comme $P \cap R'[\mathbf{d}] \subset \mathfrak{E}_{\mathbf{d}} P \cap R'[\mathbf{d}] = \mathfrak{E}_{\mathbf{d}} P = (0)$, on a $\mathrm{rg}\, \bar{P} = \mathrm{rg}\, P$,

$\mathrm{rg}\, \mathfrak{E}(\bar{P}[\mathbf{d}]) = \mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} P$ et $\mathfrak{E}(\bar{P}[\mathbf{d}]) = (0)$. Le théorème de l'élimination avec $\rho = \mathrm{id}$ montre alors qu'il exite un zéro non trivial de $\bar{P}[\mathbf{d}]$ dans K^{n+1} où K est une clôture algébrique de $\mathbf{k}$. On en déduit $\mathrm{Rad}(\bar{P}[\mathbf{d}]) \not\supset \mathfrak{m}$ et donc $\mathrm{rg}\, \mathfrak{E}(\bar{P}[\mathbf{d}]) < n+1$. Mais le lemme 4 entraîne $\mathrm{rg}\, \mathfrak{E}(\bar{P}[\mathbf{d}]) = \mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} P = \mathrm{rg}\, P + h$ et il suit $\mathrm{rg}\, \varphi(\mathfrak{p}) < n+1-h$.
(ii) Choisissons $t = n - \mathrm{rg}\, \varphi(\mathfrak{p}) < h$ et $P = \varphi(\mathfrak{p})$ dans le fait 6, on obtient

$$\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}) \cap R'_t = (0) \ .$$

Soient $\mathbf{k}$ le corps des fractions de R'_t et $B = \mathbf{k}[z_0, \ldots, z_n]$, d'après l'identité précédente l'idéal engendré par les éléments de $\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p})$ dans $\mathbf{k}[u_0^{(t+1)}, \ldots, u_0^{(h)}]$ est premier de rang égal à $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p})$. On déduit immédiatement des propriétés des anneaux semi-réguliers (*cf.* §2, exposé 1)

$$\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}) \leq \dim \mathbf{k}[u_0^{(t+1)}, \ldots, u_0^{(h)}] = h - t = \mathrm{rg}\, \varphi(\mathfrak{p}) + h - n \ .$$

D'un autre coté, l'anneau B étant semi-régulier de dimension n la proposition 1 montre

$$\begin{aligned} \mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}) &= \mathrm{rg}\, \tilde{\mathfrak{E}}(B/\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}).B) \\ &\geq \mathrm{rg}\, \tilde{\mathfrak{E}}(B/\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}).B) - n \\ &\geq \mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p}) - n \\ &\geq \mathrm{rg}\, \varphi(\mathfrak{p}) + h - n \end{aligned}$$

avec le lemme 4. En combinant les estimations ci-dessus on conclut la preuve du théorème 5. □

Soit $\mathfrak{p}$ un idéal homogène premier de A , tel que $\mathrm{rg}\, \varphi(\mathfrak{p}) \leq n+1-h$, si R' est factoriel il suit du théorème 5 que $\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p})$ est principal. Plus généralement, si R' est un anneau de Krull le diviseur associé à $\mathfrak{E}_{\mathbf{d}} \varphi(\mathfrak{p})$ est bien défini lorsque $\mathrm{rg}\, \varphi(\mathfrak{p}) \geq n+1-h$ et trivial dès que $\mathrm{rg}\, \varphi(\mathfrak{p}) > n+1-h$.

Dans la représentation géométrique du §1, le théorème 5 dit que, si $h = \dim V + 1$, la projection $\pi_2(C(V))$ est de codimension 1 dans $\mathbf{P}^{\check{}}$.

Exposé n$^\circ$4 : Idéaux et diviseurs résultants

Patrice PHILIPPON

UMR 9994 du CNRS-Problèmes Diophantiens,
Université P. & M. Curie, T.46-56, 5ème ét., F-75252 PARIS cedex 05.

Nous avons étudié dans l'exposé 3 les annulateurs de modules cycliques d'un anneau de polynômes. Comme nous l'avons indiqué dans l'exposé 2, ceux-ci décrivent une projection schématique grossière ne conservant pas les bonnes multiplicités. Nous allons maintenant utiliser les invariants de Fitting pour décrire les bonnes projections. Lorsque l'anneau de base est factoriel on obtient des formes résultantes (ou de Chow) associées à un idéal dont les propriétés reflètent celles de l'idéal. En particulier, une forme résultante associée à l'idéal nul est le résultant classique de formes homogènes.

Soient R un anneau commutatif, unitaire et nœthérien, $A = R[z_0, \ldots, z_n]$ et M un A-module de type fini, gradué. Pour $k \in \mathbf{N}$ on note $M(k)$ le R-module (de type fini) des éléments homogènes de degré k. On pose

$$\tilde{\mathfrak{F}}M(\delta) = \sum_{k\geq\delta} \mathrm{Fitt}_0 M(k) \qquad \text{et} \qquad \tilde{\mathfrak{F}}M = \bigcap_{\delta} \tilde{\mathfrak{F}}M(\delta)$$

où l'intersection est prise sur les entiers $\delta \geq 0$ tels que M soit engendré par ses éléments de degré $\leq \delta$, et on appelle $\tilde{\mathfrak{F}}M$ l'*idéal résultant de* M. L'anneau R étant nœthérien, pour tout $\delta \geq 0$ il existe $k_0 \geq 0$ tel que $\tilde{\mathfrak{F}}M(\delta) = \sum_{\delta\leq k\leq k_0} \mathrm{Fitt}_0 M(k)$. On remarque que les idéaux $\tilde{\mathfrak{F}}M(\delta)$ forment une chaîne décroissante d'idéaux emboîtés.

Proposition 1 – *Soit M un A-module gradué, de type fini engendré par ses éléments de degré $\leq \delta$. Alors*
(i) $\tilde{\mathfrak{E}}M = \cup_{k\geq\delta} \mathrm{Ann}_R(M(k))$,
(ii) $\mathrm{Rad}(\mathrm{Fitt}_0 M(k)) = \mathrm{Rad}(\mathrm{Ann}_R M(k))$ *pour tout* $k \geq 0$,
(iii) $\tilde{\mathfrak{F}}M \subseteq \tilde{\mathfrak{F}}M(\delta) \subseteq \tilde{\mathfrak{E}}M$,
(iv) *si* $\omega : R \to S$ *est un homomorphisme d'anneaux alors*

$$\tilde{\mathfrak{F}}(M \otimes_R S)(\delta) = \omega(\tilde{\mathfrak{F}}M(\delta)).S \ .$$

Démonstration – (i) Soit $k \geq \delta$, comme M est engendré par des éléments de degré $\leq \delta$ alors $\mathfrak{m}^k M$ est contenu dans le A-module engendré par les éléments de $M(k)$ et donc $\mathrm{Ann}_R M(k) \subset \mathrm{Ann}_R \mathfrak{m}^k M \subset \tilde{\mathfrak{E}}M$. On a aussi $M(k+1) = M(k) \otimes_R A(1)$ et donc $\mathrm{Ann}_R M(k) \subset \mathrm{Ann}_R M(k+1)$. Réciproquement $M(k) \subset \mathfrak{m}^{k-\delta}.M$ et donc $\mathrm{Ann}_R(\mathfrak{m}^{k-\delta}M) \subset \mathrm{Ann}_R M(k)$. Ceci entraîne $\tilde{\mathfrak{E}}M = \mathrm{Ann}_R(\mathfrak{m}^{k-\delta}M) \subset \mathrm{Ann}_R M(k)$ pour tout k assez grand.
(ii) Comme $M(k)$ est de type fini pour tout $k \geq 0$ on a, d'après la proposition 3, §2 de l'exposé 2,

$$\mathrm{Rad}(\mathrm{Fitt}_0 M(k)) = \mathrm{Rad}(\mathrm{Ann}_R M(k)) \ .$$

(iii) L'inclusion $\tilde{\mathfrak{F}}M \subseteq \tilde{\mathfrak{E}}M$ résulte de (i) et de la proposition 3, §2 de l'exposé 2 qui entraînent $\mathrm{Fitt}_0(M(k)) \subset \mathrm{Ann}_R M(k) \subset \tilde{\mathfrak{E}}M$ pour tout $k \geq \delta$ dès que M est engendré par des éléments de degrés $\leq \delta$.
(iv) On a $\mathrm{Fitt}_0(M \otimes_R S)(k) = \omega(\mathrm{Fitt}_0 M(k)).S$ pour tout $k \geq 0$, d'après la proposition 1, §1 de l'exposé 2. $\square$

Proposition 2 – (i) *Si M est un R-module de type fini, simple alors $M \simeq R/\mathrm{Ann}_R M$ et $\mathrm{Ann}_R M = \mathrm{Fitt}_0 M$ est un idéal premier de R.*
(ii) *Soit M un A-module de type fini, gradué. Si M est simple, alors pour tout $k \geq 0$ le R-module $M(k)$ de type fini est aussi simple. Si tout diviseur de zéro sur M appartient au radical de $\tilde{\mathfrak{C}}M$ (resp. à $\tilde{\mathfrak{C}}M$), alors pour tout k assez grand tout diviseur de zéro sur $M(k)$ appartient au radical de $\mathrm{Ann}_R M(k)$ (resp. à $\mathrm{Ann}_R M(k)$).*

Démonstration – (i) Si $M = 0$ alors $\mathrm{Ann}_R M = \mathrm{Fitt}_0(M) = R$, sinon prenons $m \in M$, $m \neq 0$ alors Rm est un sous-module non nul de M et, M étant simple, on a nécessairement $Rm = M$. Ainsi M est engendré par un élément, $M \simeq R/\mathrm{Ann}_R M$ et d'après le corollaire 4, §2 de l'exposé 2 on en déduit $\mathrm{Fitt}_0 M = \mathrm{Ann}_R M$.

De plus, soit $a, b \in R$ tels que $ab \in \mathrm{Ann}_R M$, alors si $bM = 0$ on a $b \in \mathrm{Ann}_R M$ et sinon bM est un sous-module non nul de M donc égal à M. Ainsi $abM = aM = 0$ et $a \in \mathrm{Ann}_R M$, ce qui montre que $\mathrm{Ann}_R M$ est bien premier.
(ii) Supposons M simple, soient $k \geq 0$ et N' un sous-R-module propre de $M(k)$. Considérons le A-module $M' = N' \otimes_R A$, c'est un sous-module gradué de M dont le R-module des éléments de poids k est égal à $N' \subsetneq M(k)$. Donc $M' \subsetneq M$ et comme M est simple on a $M' = 0$ ce qui est équivalent à $N' = 0$ et démontre que $M(k)$ est simple.

Supposons que tout diviseur de zéro sur M appartient au radical de $\tilde{\mathfrak{C}}M$, (*resp.* à $\tilde{\mathfrak{C}}M$). Si $a \in R$ est diviseur de zéro sur $M(k)$ alors a est diviseur de zéro sur M et donc il existe $k' \geq 1$ tel que $a^{k'} \in \tilde{\mathfrak{C}}M \cap R = \tilde{\mathfrak{E}}M$. (*resp.* $a \in \tilde{\mathfrak{C}}M \cap R = \tilde{\mathfrak{E}}M$). Mais, l'anneau R étant nœthérien $\tilde{\mathfrak{E}}M = \mathrm{Ann}_R\, M(k)$ pour tout k assez grand d'après la proposition 1 (i). □

Le lemme suivant établit des relations très utiles pour étudier la variation des idéaux $\mathrm{Fitt}_0 M(k)$ une fonction de k .

Lemme 3 – *Soient M un A-module de type fini, gradué , $p \in A(1)$, $M' = 0 :_M p$ et $M'' = M/pM$. Alors* $\mathrm{Rad}\, \mathfrak{E}(\mathrm{Ann}_A\, M + (p)) \subset \mathrm{Rad}(\tilde{\mathfrak{E}}M' \cap \tilde{\mathfrak{E}}M'')$ *et, pour tout $k \geq 0$ il existe un entier $k' > 0$ tel que*

$$\mathrm{Ann}_R\, M''(k+1)^{k'}.\mathrm{Fitt}_0(M/M')(k) \subset \mathrm{Fitt}_0 M(k+1) \ .$$

Si de plus $\mathrm{Ann}_R\, M(k) \neq (0)$ *et* $\mathrm{Ann}_R\, M(k+1) \neq (0)$ *, alors*

$$\chi(M(k+1)) - \chi(M(k)) = \chi(M''(k+1)) - \chi(M'(k)) \ .$$

Démonstration – Les modules M' et M'' sont clairement annulés par p et $\mathrm{Ann}_A\, M$. Si $a \in \mathrm{Rad}(\mathfrak{E}(\mathrm{Ann}_A\, M + (p)))$ il existe $k, k' \geq 0$ tels que $a^k \mathfrak{m}^{k'} \in (p) + \mathrm{Ann}_A\, M$ et donc $a^k \mathfrak{m}^{k'}$ annule M/pM et $(0 :_M p)$. Ainsi $a^k \in \tilde{\mathfrak{E}}(M/pM) \cap \tilde{\mathfrak{E}}(0 :_M p)$ ce qui montre la première inclusion.

Considérons la suite exacte de R-modules

$$0 \to (M/M')(k) \xrightarrow{\times p} M(k+1) \to M''(k+1) \to 0 \ ,$$

le résultat s'en déduit par les propositions 3, §2 et 5, §3 de l'exposé 2. Si $\mathrm{Ann}\, M(k) \neq (0)$ et $\mathrm{Ann}_R\, M(k+1) \neq (0)$ on applique le corollaire 12, §5 de l'exposé 2 à la suite exacte ci-dessus et à la suivante

$$0 \to M'(k) \to M(k) \to (M/M')(k) \to 0 \ . \ \square$$

Exemple : Considérons les anneaux $R = \mathbf{Z}$, $A = \mathbf{Z}[z_0, z_1]$ $(n = 1)$, l'idéal $I = (6z_0^2, 10z_1)$ et le module $M = A/I$. On a $I(0) = 0$, $I(1) = \mathbf{Z}.10z_1$ et pour $k \geq 2$,

$$I(k) = \mathbf{Z}.6z_0^k \oplus \bigoplus_{i=0}^{k-3} \mathbf{Z}.2z_0^{i+2} z_1^{k-i-2} \oplus \mathbf{Z}.10z_0 z_1^{k-1} \oplus \mathbf{Z}10z_1^k \ .$$

On en déduit $M(0) \simeq \mathbf{Z}$, $M(1) \simeq \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ et pour $k \geq 2$, $M(k) \simeq (\mathbf{Z}/2\mathbf{Z})^{k+1} \oplus (\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})^2$. On calcule alors

$$\tilde{\mathfrak{E}}M = (2.3.5) \quad \text{et} \quad \tilde{\mathfrak{F}}M = (0) \ .$$

En fait, on vérifie pour tout $k \geq 2$ les égalités $\mathrm{Ann}_R\, M(k) = (2.3.5)$ et $\mathrm{Fitt}_0 M(k) = (2^{k+1}.3.5^2)$. L'idéal I est de rang 1 et admet pour décomposition primaire

$$I = (2) \cap (3, z_1) \cap (5, z_0^2) \cap (z_0^2, z_1) \ .$$

§ 1. **Diviseurs résultants**

On reprend les notations de l'exposé 3, mais on se donne maintenant un anneau de Krull R , nœthérien, $A = R[z_0, \ldots, z_n]$ et $\mathbf{d} \in (\mathbf{N}^*)^h$.

Soit M un A-module gradué, de type fini, pour $k \in \mathbf{N}$ on note $M(k)$ le R-module (de type fini) des éléments homogènes de degré k de M . On pose $M' = M \otimes_A A[\mathbf{d}]$ et $M[\mathbf{d}] = M'/U_1 M' + \ldots + U_h M'$, c'est un $A[\mathbf{d}]$-module gradué de type fini et on désigne pour $M[\mathbf{d}](k)$ le $R[\mathbf{d}]$-module (aussi de type fini) des éléments homogènes de degré k .

Si I est un idéal homogène de A alors $(A/I)[\mathbf{d}] = A[\mathbf{d}]/I[\mathbf{d}]$ avec les notations de l'exposé 3. Mais on fera attention que la notation $I[\mathbf{d}]$ représente des idéaux différents selon qu'on considère I comme idéal ou comme A-module.

On a en tout cas $\mathrm{Ann}_{A[\mathbf{d}]}\, M' = (\mathrm{Ann}_A\, M).A[\mathbf{d}] \subset \mathrm{Ann}_{A[\mathbf{d}]}\, M[\mathbf{d}]$.

Lemme 4 – *Soit M un A-module gradué, de type fini, alors pour $h \geq 0$ et $\mathbf{d} \in (\mathbf{N}^*)^h$ on a*

$$\tilde{\mathfrak{C}}M[\mathbf{d}] = \mathfrak{C}_{\mathbf{d}}(\mathrm{Ann}_A\, M) \qquad \textit{et} \qquad \tilde{\mathfrak{E}}M[\mathbf{d}] = \mathfrak{E}_{\mathbf{d}}(\mathrm{Ann}_A\, M) \ .$$

Démonstration – Soit $a \in R[\mathbf{d}]$, on a $a \in \tilde{\mathfrak{C}}M[\mathbf{d}]$ si et seulement s'il existe $k \geq 0$ tel que $a\mathfrak{m}^k \in \mathrm{Ann}_{A[\mathbf{d}]}\, M[\mathbf{d}]$, c'est-à-dire $a\mathfrak{m}^k M' \subset U_1 M' + \ldots + U_h M'$, par définition de $M[\mathbf{d}]$. Appliquons l'opérateur $\mathfrak{d}$ du §1 de l'exposé 3, comme $\mathfrak{d}U_i = 0$ $(i = 1 \ldots, h)$ on obtient $\mathfrak{d}(a).\mathfrak{m}^k.M'' = 0$ où $M'' = M \otimes_A \mathfrak{S}A[\mathbf{d}]$, c'est-à-dire $\mathfrak{d}(a)\mathfrak{m}^k \in \mathrm{Ann}_A\, M.\mathfrak{S}A[\mathbf{d}]$. On déduit du lemme 2, §1 de l'exposé 3 $a \in \mathfrak{C}_{\mathbf{d}}(\mathrm{Ann}_A\, M)$. Réciproquement, si $a \in \mathfrak{C}_{\mathbf{d}}(\mathrm{Ann}_A\, M)$ alors il existe $k \geq 0$ tel que $a\mathfrak{m}^k \subset \mathrm{Ann}_{A[\mathbf{d}]}\, M' + (U_1, \ldots, U_h)$ d'où $a\mathfrak{m}^k M' \subset U_1 M' + \ldots + U_h M'$, c'est-à-dire $a \in \tilde{\mathfrak{C}}M[\mathbf{d}]$. Le résultat pour les idéaux éliminants s'obtient en intersectant avec $R[\mathbf{d}]$. □

Définition – Soit M un A-module gradué de type fini tel que $\tilde{\mathfrak{E}}(\mathrm{Ann}_A\, M) \neq (0)$, on note $\tilde{\chi}(M)$ et on appelle *diviseur résultant de* M , la borne supérieure des diviseurs $\mathrm{div}(\tilde{\mathfrak{F}}M(\delta))$ $(\delta \geq 0)$. Si I est un idéal de A et $\mathbf{d} \in (\mathbf{N}^*)^h$, on note $\chi_{\mathbf{d}}(I)$ et on appelle *diviseur résultant d'indice* $\mathbf{d}$ *de* I le diviseur $\tilde{\chi}(M[\mathbf{d}])$ où $M = A/I$.

Avec cette définition, le diviseur résultant $\tilde{\chi}(M)$ est la “limite inférieure” des diviseurs $\chi(M(k))$ pour $k \geq \delta$ où δ est le plus petit entier tel que M soit engendré par ses éléments de degrés $\leq \delta$. On notera qu'on a toujours $\mathrm{div}(\tilde{\mathfrak{F}}M) \succeq \tilde{\chi}(M)$, mais cette inégalité est stricte en général.

Le diviseur résultant de M n'est pas trivial si et seulement si les idéaux $\mathrm{Fitt}_0 M(k)$ sont de rang 1 pour tout k assez grand. Dans le cas général, on considère le diviseur résultant du module $M[\mathbf{d}]$ pour $\mathbf{d} \in (\mathbf{N}^*)^h$ avec h convenablement choisi. Posons $I = \mathrm{Ann}_A M$ et $r = \mathrm{rg}\, I$, la définition ci-dessus nous amène à préciser les idéaux premiers (isolés) associés à $\tilde{\mathfrak{F}} M[\mathbf{d}]$, de rang 1. On sait que les idéaux premiers associés à $\mathfrak{E}_{\mathbf{d}} I$ sont de la forme $\mathfrak{E}_{\mathbf{d}} \mathfrak{P}$ avec $\mathfrak{P} \in \mathrm{Ass}\, I$ (*cf.* prop. 3, §1, exposé 3).

Proposition 5 – *Soient* R *un anneau de Krull, nœthérien,* $A = R[z_0 \dots, z_n]$ *et* $\mathfrak{P}$ *un idéal homogène premier de rang* r *de* A *. Soit* $h \geq n+1-r$, $\mathbf{d} \in (\mathbf{N}^*)^h$, *alors* $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \mathfrak{P} \geq 1$ *avec égalité si et seulement si* $\mathrm{rg}\, \mathfrak{P} = r = n+1-h$ *.*

Démonstration – Posons $\mathfrak{p} = \mathfrak{P} \cap R$, c'est un idéal premier de R contenu dans $\mathfrak{E}_{\mathbf{d}} \mathfrak{P}$. Si $\mathrm{rg}\, \mathfrak{p} > 1$ alors $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \mathfrak{P} > 1$ et si $\mathrm{rg}\, \mathfrak{p} = 0$ (*i.e.* $\mathfrak{p} = (0)$) alors, d'après le théorème 5, §3 de l'exposé 3 on a $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \mathfrak{P} = \mathrm{rg}\, \mathfrak{P} + h - n$. En particulier, si $\mathrm{rg}\, \mathfrak{p} = 0$ alors $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \mathfrak{P} = 1$ si et seulement si $\mathrm{rg}\, \mathfrak{P} = r = n+1-h$. Finalement, si $\mathrm{rg}\, \mathfrak{p} = 1$ alors $\mathfrak{p}$ est l'idéal d'une valuation essentielle de R, l'anneau localisé $R_{\mathfrak{p}}$ est un anneau de valuation discrète, $\mathfrak{p}.R_{\mathfrak{p}}$ est un idéal principal et $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ est un corps. On déduit du corollaire du théorème de l'idéal principal, §2 ,exposé 1, en notant $A_{\mathfrak{p}} = R_{\mathfrak{p}}[z_0, \dots, z_n]$ et $\varphi_{\mathfrak{p}} : R_{\mathfrak{p}} \to R_{\mathfrak{p}}/\mathfrak{p}.R_{\mathfrak{p}}$,

$$r \leq \mathrm{rg}\, \mathfrak{P} = \mathrm{rg}(\mathfrak{P}.A_{\mathfrak{P}}) = \mathrm{rg}\, \varphi_{\mathfrak{p}}(\mathfrak{P}) + 1$$

car $\mathrm{rg}\, \mathfrak{p} = 1$. Le théorème 5, §3 de l'exposé 3 montre encore que, si $\mathrm{rg}\, \mathfrak{P} > n+1-h$,

$$\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \mathfrak{P} > \mathrm{rg}\, \mathfrak{E}_{\mathbf{d}} \varphi_{\mathfrak{p}}(\mathfrak{P}.A_{\mathfrak{p}}) = \mathrm{rg}\, \varphi_{\mathfrak{p}}(\mathfrak{P}.A_{\mathfrak{P}}) + h - n = \mathrm{rg}\, \mathfrak{P} + h - n - 1 \geq 1 \;,$$

et si $\mathrm{rg}\, \mathfrak{P} = r = n+1-h$ alors $\mathrm{rg}\, \varphi_{\mathfrak{p}}(\mathfrak{P}.A_{\mathfrak{P}}) < n+1-h$ et $\mathfrak{E}_{\mathbf{d}} \mathfrak{P} = \mathfrak{p}$ est de rang 1. □

Proposition 6 – *Soit* R *un anneau de Krull, nœthérien,* $A = R[z_0, \dots, z_n]$ *et* M *un* A*-module gradué, de type fini.*
(i) *On note* $r = \mathrm{rg}\, \mathrm{Ann}_A M$ *, on se donne* $h \geq n+1-r$ *et* $\mathbf{d} = (d_1, \dots, d_h) \in (\mathbf{N}^*)^h$ *. Alors, pour tout* k *assez grand on a*

$$\chi(M[\mathbf{d}](k)) = \chi(M[\mathbf{d}](k+1)) \;.$$

En particulier, $\tilde{\chi}(M[\mathbf{d}]) = \chi(M[\mathbf{d}](k))$ *pour tout* k *assez grand et* $\tilde{\chi}(M[\mathbf{d}]) = 0$ *dès que* $\mathrm{rg}\, \mathrm{Ann}_A M > n+1-h$ *.*
(ii) *On note* $N = \cup_{k \geq 0} (0 :_M \mathfrak{m}^k)$ *, alors pour tout* k *assez grand on a*

$$\mathrm{Fitt}_0 M(k) = \mathrm{Fitt}_0 (M/N)(k) \;.$$

Démonstration – (i) Notons $\mathbf{d}_1 = (d_1, \dots, d_h, 1) \in (\mathbf{N}^*)^{h+1}$ et $M_1 = M[\mathbf{d}] \otimes_{A[\mathbf{d}]} A[\mathbf{d}_1]$, d'après le lemme 3 avec $p = U_{h+1}$ il suffit de montrer

$$\chi((M_1/U_{h+1}M_1)(k)) = \chi((0 :_{M_1} U_{h+1})(k)) = 0$$

pour tout k assez grand. Cela se ramène, d'après la proposition 1 (ii) à montrer que les idéaux $\mathrm{Ann}_{R[\mathbf{d}_1]}(M_1/U_{h+1}M_1)(k)$ et $\mathrm{Ann}_{R[\mathbf{d}_1]}(0 :_{M_1} U_{h+1})(k)$ sont de rangs > 1.

Mais l'anneau R étant nœthérien il suit de la proposition 1 (i) que ces annulateurs sont égaux pour k assez grand à $\tilde{\mathfrak{E}}(M_1/U_{h+1}M_1) = \tilde{\mathfrak{E}} M[\mathbf{d}_1]$ et $\tilde{\mathfrak{E}}(0 :_{M_1} U_{h+1})$ respectivement. On sait par le lemme 3 que les radicaux de ces idéaux contiennent $\mathfrak{E}((U_{h+1}) + \mathrm{Ann}_{A[\mathbf{d}_1]} M_1) \supseteq \mathfrak{E}_{\mathbf{d}_1}(\mathrm{Ann}_A M)$, et comme $\mathrm{rg}\, \mathrm{Ann}_A M = r \geq n+1-h > n-h$ on a, d'après la proposition 5, $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}_1}(\mathrm{Ann}_A M) > 1$.

On a par définition et avec ce qui précède

$$\chi(M[\mathbf{d}]) = \sup_{\delta} \inf_{k' \geq \delta} \chi(M[\mathbf{d}](k')) = \chi(M[\mathbf{d}](k))$$

pour tout k assez grand. Et, avec les propositions 1(i) & (ii) et 5, on sait que $\mathrm{rg}(\mathrm{Fitt}_0 M[\mathbf{d}](k)) = \mathrm{rg}\, \tilde{\mathfrak{E}} M[\mathbf{d}] > 1$ dès que $\mathrm{rg}\, \mathrm{Ann}_A M > n+1-h$.
(ii) D'après la proposition 5, §3 de l'exposé 2 il suffit de montrer que $\mathrm{Fitt}_0 N(k) = \mathrm{Ann}_R N(k) = R$ pour tout k assez grand. Mais M étant de type fini il existe k tel que $\mathfrak{m}^k.R$ annule N et donc $\tilde{\mathfrak{E}} N = R$, le résultat suit de la proposition 1(i) & (ii). □

Exemple : Supposons $R = K$ un corps algébriquement clos et $M = A/\mathfrak{P}$ où $\mathfrak{P}$ est un idéal premier de rang n de $A = K[z_0, \dots, z_n]$. Alors la variété des zéros de $\mathfrak{P}$ dans $\mathbf{P}_n(K)$ est réduite à un point, de coordonnées projectives $(x_0, \dots, x_n) \in K^{n+1} \setminus \{0\}$, disons. Quitte à permuter les x_i et à multiplier par un scalaire non nul, on peut supposer $x_0 = 1$, et alors $\mathfrak{P} = (z_1 - x_1 z_0, \dots, z_n - x_n z_0)$. Soit $k \geq 0$, choisissons comme générateurs de $M(k)$ les images des monômes (unitaires) de degré k de A, une base des relations entre ces générateurs est $\{z^\alpha - x^\alpha z_0^k;\quad \alpha \in \mathbf{N}^{n+1},\quad |\alpha| = k,\quad \alpha_0 \neq k\}$ où $z^\alpha = z_0^{\alpha_0} \dots z_n^{\alpha_n}$.

Soient $h = 1$, $d \in \mathbf{N}^*$, l'image des monômes de degré k dans $M[d]$ engendrent le R-module $M[d](k)$, satisfont les relations précédentes et, si $k \geq d$ la relation $U = 0$. On a ainsi une base de relations et on écrit la présentation

$$R[d]^{\binom{k+n}{n}} \xrightarrow{\varphi} R[d]^{\binom{k+n}{n}} \to M[d] \to 0$$

où φ est défini par $\varphi((a_\alpha)_{|\alpha|=k}) = a_{\alpha_0} U + \sum_{\substack{|\alpha|=k \\ \alpha \neq \alpha_0}} a_\alpha (z^\alpha - x^\alpha z_0^k)$ avec $\alpha_0 = (k, 0, \dots, 0)$. La matrice Φ de φ est carrée, ce qui montre que l'idéal

$\mathrm{Fitt}_0 M[d](k)$ est principal engendré par le déterminant de Φ pour tout $k \geq d$. Mais on voit facilement, par manipulation de colonnes, que le déterminant de Φ est égal à celui de la matrice $\begin{pmatrix} U(x) & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \mathrm{Id} & \\ 0 & & & \end{pmatrix}$, et donc égal à $U(x) = \sum_{|\alpha|=d} u_\alpha . x^\alpha$. Cette forme linéaire étant irréductible dans $R[d]$ on en déduit du même coup que $\tilde{\mathfrak{F}}M[d] = \tilde{\mathfrak{E}}M[d] = \mathfrak{E}_d\mathfrak{P} = (U)$ est premier dans $R[d]$.

§ 2. **Propriétés des diviseurs résultants**

Nous montrons dans cette section que les diviseurs résultants des A-modules gradués ont le même type de décomposition que les diviseurs attachés aux R-modules.

Théorème 7 – *Soit R un anneau de Krull, nœthérien, $A = R[z_0, \ldots z_n]$ et M un A-module gradué, de type fini. On note $I = \mathrm{Ann}_A M$, $r = \mathrm{rg}\, I$ et on se donne $h \geq n+1-r$ et $\mathbf{d} \in (\mathbf{N}^*)^h$. Alors*

$$\tilde{\chi}(M[\mathbf{d}]) = \sum_{\mathfrak{P}} \ell(M_{\mathfrak{P}}).\chi_{\mathbf{d}}(\mathfrak{P})$$

où la somme est prise sur $\mathfrak{P} \in \mathrm{Ass}\, I$, $\mathrm{rg}\, \mathfrak{P} = n+1-h$ et $\mathfrak{m} \not\subset \mathfrak{P}$, avec la convention $\tilde{\chi}(M[\mathbf{d}]) = 0$ si la somme est vide.

Démonstration – Etablissons d'abord l'identité lorsque $h = 0$. Soit $0 = N_0 \subset \ldots \subset N_s = M$ la suite de sous-modules fournie par la proposition 2, §1 de l'exposé 1, on a pour tout $k \geq 0$ des suites exactes courtes de R-modules

$$0 \to N_i(k) \to N_{i+1}(k) \to (N_{i+1}/N_i)(k) \to 0$$

et le corollaire 12, §5 de l'exposé 2 entraîne

$$(*) \qquad \chi(N_{i+1}(k)) - \chi(N_i(k)) = \chi((N_{i+1}/N_i)(k)) \ .$$

Mais $N_{i+1}/N_i \simeq A/\mathfrak{P}_i$ par un isomorphisme de degré disons δ_i, ainsi $(N_{i+1}/N_i)(k) \simeq (A/\mathfrak{P}_i)(k-\delta_i)$ pour tout $k \geq \delta_i$ et en sommant les identités $(*)$ sur $i = 0, \ldots, s-1$ on obtient

$$\chi(M(k)) = \sum_{i=0}^{s-1} \chi((A/\mathfrak{P}_i)(k-\delta_i)) \ .$$

Par hypothèse on a $I = \mathrm{Ann}_A M$ et $r = \mathrm{rg}\, I \geq n+1$, et donc $\mathrm{rg}\, \mathfrak{P}_i \geq r \geq n+1$ pour tout $i = 0, \ldots, s-1$, grâce à la proposition 2, §1 de l'exposé 1. La proposition 6(i) montre alors que pour k assez grand on a $\chi(M(k)) = \tilde{\chi}(M)$ et, pour $i = 0, \ldots s-1$, $\chi((A/\mathfrak{P}_i)(k-\delta_i)) = \chi(\mathfrak{P}_i)$, on a de plus $\chi(\mathfrak{P}_i) = 0$ si $\mathrm{rg}\, \mathfrak{P}_i > n+1$. D'après la proposition 2, §1 de l'exposé 1, les $\mathfrak{P}_i$ de rang $n+1$ sont les premiers isolés associés à I de rang $n+1$ (s'il n'y en a aucun on trouve $\tilde{\chi}(M) = 0$) et le nombre de ces $\mathfrak{P}_i$ égaux à un même premier $\mathfrak{P}$ est égal à $\ell(M_{\mathfrak{P}})$. Enfin, si $\mathfrak{m} \subset \mathfrak{P}$ on a clairement $(A/\mathfrak{P})(k) = 0$ pour tout k assez grand et $\chi(\mathfrak{P}) = 0$.

Lorsque $h = 0$ on applique ce qui précède au $R[\mathbf{d}]$-module $M[\mathbf{d}]$, en remarquant que les premiers associés à $\mathrm{Ann}_{A[\mathbf{d}]} M[\mathbf{d}]$ de rang $n+1$ et ne contenant pas $\mathfrak{m}$ sont les idéaux $\mathfrak{C}_{\mathbf{d}}\mathfrak{P}$ avec $\mathfrak{P} \in \mathrm{Ass}\, I$ et $\mathrm{rg}\, \mathfrak{P} = n+1-h$. On a donc

$$\chi(\mathfrak{C}_{\mathbf{d}}\mathfrak{P}) = \tilde{\chi}(A[\mathbf{d}]/\mathfrak{C}_{\mathbf{d}}\mathfrak{P}) = \tilde{\chi}((A/\mathfrak{P})[\mathbf{d}]) = \chi(\mathfrak{P}) \ ,$$

car $\mathfrak{C}_{\mathbf{d}}\mathfrak{P}(k) = \mathfrak{P}[\mathbf{d}](k)$ pour tout k assez grand. Il suffit maintenant de vérifier $\ell(M[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}}) = \ell(M_{\mathfrak{P}})$. Soit $0 = N_0 \subset \ldots \subset N_s = M_{\mathfrak{P}}$ une suite de composition du $A_{\mathfrak{P}}$-module $M_{\mathfrak{P}}$. On a donc $s = \ell(M_{\mathfrak{P}})$ et $N_{i+1}/N_i \simeq A_{\mathfrak{P}}/\mathfrak{P}.A_{\mathfrak{P}}$. Posons $N'_i = N_i \otimes_{A_{\mathfrak{P}}} A_{\mathfrak{P}}[\mathbf{d}]$, comme $\mathfrak{m} \not\subset \mathfrak{P}$ le lemme 2, §1 de l'exposé 3 montre

$$N'_i \cap (U_1 M + \ldots + U_h M) = U_1 N'_i + \ldots + U_h N'_i$$

et on a donc une suite de $A_{\mathfrak{P}}[\mathbf{d}]$-modules emboîtés

$$0 = N_0[\mathbf{d}] \subset \ldots \subset N_s[\mathbf{d}] = M_{\mathfrak{P}}[\mathbf{d}]$$

où $N_i[\mathbf{d}] = N'_i/(U_1 N'_i + \ldots + U_h N'_i)$. Posons $N''_i = N_i[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}}$, la suite de $A[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}}$-modules

$$0 = N''_0 \subset \ldots \subset N''_s = M[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}}$$

est une suite de composition de $M[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}}$ car, pour tout $i = 0, \ldots, s-1$, le module

$$\begin{aligned} N''_{i+1}/N''_i &\simeq ((N'_{i+1}/N'_i)/U_1(N'_{i+1}/N'_i) + \ldots + U_h(N'_{i+1}/N'_i))_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}} \\ &\simeq (N_{i+1}/N_i)[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}} \\ &\simeq (A_{\mathfrak{P}}/\mathfrak{P}.A_{\mathfrak{P}})[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}} \\ &\simeq (A[\mathbf{d}]/\mathfrak{C}_{\mathbf{d}}\mathfrak{P})_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}} \end{aligned}$$

est simple. Ainsi $\ell(M[\mathbf{d}]_{\mathfrak{C}_{\mathbf{d}}\mathfrak{P}}) = s = \ell(M_{\mathfrak{P}})$ ce qui achève la démonstration du théorème 7. □

Le théorème 7 ramène la détermination des diviseurs résultants des A-modules gradués de type fini à celle des diviseurs résultants des idéaux premiers. Nous allons voir au paragraphe suivant que ceux-ci ont d'agréables propriétés.

§ 3. Formes résultantes

Dans tout ce paragraphe R désigne un anneau de Krull, nœthérien et $A = R[z_0, \dots, z_n]$. Rappelons pour commencer que la *fonction de Hilbert* d'un A-module gradué M, de type fini est définie par

$$H(M; k) = \ell_R(M(k)) \ .$$

En particulier, il résulte des propositions 1 & 2, §1 de l'exposé 1 qu'il existe des idéaux premiers $\mathfrak{P}_0, \dots, \mathfrak{P}_{s-1}$ de A et des entiers $\delta_0, \dots, \delta_{s-1}$ tels que $H(M; k) = \sum_{i=0}^{s-1} H(A/\mathfrak{P}_i; k - \delta_i)$ pour tout k assez grand.

Proposition 8 – *Soit* $\mathfrak{P}$ *un idéal homogène premier de* A *de rang* $r \leq n+1$. *On suppose* $\mathrm{rg}(\mathfrak{P} \cap R) = 1$, *alors pour tout* k *assez grand*

$$\chi((A/\mathfrak{P})(k)) = H((A/\mathfrak{P}) \otimes_R \mathbf{k}; k). \operatorname{div}(\mathfrak{P} \cap R)$$

où $\mathbf{k}$ *est le corps des fractions de* $R/(\mathfrak{P} \cap R)$.

Démonstration – On a $\mathrm{rg}(\mathfrak{P}/\mathfrak{P} \cap R) < n+1$ et donc d'après le théorème 5, §3 de l'exposé 3 $\mathfrak{E}\mathfrak{P} = \mathfrak{P} \cap R \neq (0)$. Mais $(A/\mathfrak{P})(k)_{\mathfrak{P} \cap R}$ est un $R_{\mathfrak{P} \cap R}$-module de longueur égale à la dimension du $\mathbf{k}$-espace vectoriel $(A/\mathfrak{P})(k) \otimes_R \mathbf{k}$ car $\mathfrak{P} \cap R \subset \mathrm{Ann}_R(A/\mathfrak{P})(k)$ et $R_{\mathfrak{P} \cap R}/(\mathfrak{P} \cap R).R_{\mathfrak{P} \cap R} = \mathbf{k}$, le résultat découle alors de la proposition 11, §5 de l'exposé 2. □

Remarque – Si $R = \mathbf{Z}$, le diviseur $\operatorname{div}(\mathfrak{P} \cap R)$ est principal, disons égal à $\operatorname{div}(p)$ $(p \in \mathbf{Z})$. E.Lasker (Zur Theorie der Moduln und Ideale, *Math. Ann.* 60, 1905, 20-116) appelle *fonction de Dedekind* l'application

$$k \mapsto p^{H((A/\mathfrak{P}) \otimes_{\mathbf{Z}} \mathbf{F}_p; k)} \ .$$

Si $r = n+1$, la proposition 6 montre que $H((A/\mathfrak{P}) \otimes_R \mathbf{k}; k)$ est indépendant de k assez grand. Si $r = n+1-h < n+1$ et $\mathbf{d} \in (\mathbf{N}^*)^h$ (et toujours $\mathrm{rg}(\mathfrak{P} \cap R) = 1$) on a $\mathrm{rg}\, \mathfrak{E}_{\mathbf{d}}\mathfrak{P} = n+1$ et on peut appliquer la proposition 8 au $A[\mathbf{d}]$-module $A[\mathbf{d}]/\mathfrak{E}_{\mathbf{d}}\mathfrak{P}$ pour obtenir

$$\chi_{\mathbf{d}}(\mathfrak{P}) = H((A/\mathfrak{P})[\mathbf{d}] \otimes_{R[\mathbf{d}]} \mathbf{k}; k). \operatorname{div}(\mathfrak{P} \cap R)$$

pour tout k assez grand et où $\mathbf{k}$ est le corps des fractions de $R[\mathbf{d}]/(\mathfrak{P} \cap R).R[\mathbf{d}]$.

Si K est un corps algébriquement clos et I un idéal homogène de A, on note $\mathcal{Z}(I)$ l'ensemble des zéros de I dans $\mathbf{P}_n(K)$. Pour chaque élément de $\mathcal{Z}(I)$ on choisit alors un système de coordonnées projectives $x \in K^{n+1} \setminus \{0\}$, deux tels choix diffèrent par multiplication par un élément de K^*.

Rappelons encore que dans un anneau de polynômes à coefficients dans un anneau factoriel on appelle *contenu* d'un polynôme tout pgcd de ses coefficients.

Proposition 9 – *On suppose l'anneau* R *factoriel de corps des fractions parfait et on note* K *une clôture algébrique de ce corps. Soit* $\mathfrak{P}$ *un idéal homogène premier de rang* n *de* A *tel que* $\mathfrak{P} \cap R = (0)$ *et* $d \in \mathbf{N}^*$, *alors* $\chi_d(\mathfrak{P}) = \operatorname{div}(\mathfrak{E}_d\mathfrak{P})$ *est le diviseur principal déterminé par toute forme*

$$F_{\mathfrak{P},d} = \lambda. \prod_{x \in \mathcal{Z}(\mathfrak{P})} U(x)$$

où $\lambda \in K^*$ *est choisi fonction des coordonnées projectives* x *des points de* $\mathcal{Z}(\mathfrak{P})$ *dans* $K^{n+1} \setminus \{0\}$, *tel que la forme* $F_{\mathfrak{P},d} \in R[\mathbf{d}]$ *soit de contenu une unité de* R.

Démonstration – D'après le lemme 4, §2 de l'exposé 1 on a, en notant $B = K[z_0, \dots, z_n]$,

$$\mathfrak{P}.B = \mathfrak{P}_1 \cap \ldots \cap \mathfrak{P}_s$$

où $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ sont les premiers de B de rang n tels que $\mathfrak{P}_i \cap A = \mathfrak{P}$. Le théorème 7 entraîne, dans $D(K[d])$,

$$\chi_d(\mathfrak{P}) = \sum_{i=1}^{s} \chi_d(\mathfrak{P}_i) \ .$$

Mais, d'après l'exemple à la fin du §1 on sait que, pour $i = 0, \dots, s$, les idéaux éliminant et résultant d'indice d de $\mathfrak{P}_i$ sont égaux à l'idéal principal engendré par une forme $U(x_i)$ où $x_i \in K^{n+1} \setminus \{0\}$ est un système de coordonnées projectives du zéro de $\mathfrak{P}_i$ dans $\mathbf{P}_n(K)$. On en déduit que, dans $D(K[d])$, les diviseurs $\chi_d(\mathfrak{P}_i)$ sont principaux et donc $\chi_d(\mathfrak{P})$ est aussi principal et déterminé par le produit $\prod_{i=1}^{s} U(x_i)$. On choisit des systèmes de coordonnées projectives $x_1, \dots, x_s$ conjugués sur le corps des fractions de R et on pose λ^{-1} un contenu de la forme $\prod_{i=1}^{s} U(x_i)$, alors, le corps des fractions de R étant parfait, la forme $F_{\mathfrak{P},d} = \lambda. \prod_{i=1}^{s} U(x_i)$ irréductible, de contenu 1, appartient à $R[d]$ et engendre $\mathfrak{E}_d\mathfrak{P}$. On en déduit

$$\chi_d(\mathfrak{P}) = \operatorname{div}(\mathfrak{E}_d\mathfrak{P}) = \operatorname{div}((F_{\mathfrak{P},d})) \ . \ □$$

Dans les hypothèses de la proposition 9, lorsque $\mathfrak{P}$ est de rang $r = n+1-h < n$ et $\mathbf{d} \in (\mathbf{N}^*)^h$ on peut appliquer la proposition à l'idéal $\mathfrak{E}_{\mathbf{d}'}\mathfrak{P}$ de $A[\mathbf{d}']$ avec $\mathbf{d}' = (d_1, \dots, d_{h-1})$. C'est un idéal de rang n d'après le lemme 4, §3 de l'exposé 3, et $\mathfrak{E}_{\mathbf{d}'}\mathfrak{P} = (0)$ d'après le fait 6, §3 de l'exposé 3.

Lorsque l'anneau R est factoriel il en est de même de $R[\mathbf{d}]$ et tous les diviseurs de $D(R[\mathbf{d}])$ sont principaux. On appelle *forme résultante* (*resp. éliminante*) tout générateur d'un idéal résultant (*resp.* éliminant). La proposition 9 montre que si le corps des fractions de R est parfait et si $\mathfrak{P}$ est un idéal premier, de rang $n+1-h$, de A tel que $\mathfrak{P} \cap R = (0)$, le degré en les coefficients de U_h d'une forme résultante, d'indice $\mathbf{d}$ de $\mathfrak{P}$ est égal au nombre de points de $\mathcal{Z}(\mathfrak{C}_{\mathbf{d}'}\mathfrak{P})$. Lorsque $d_1 = \ldots = d_{h-1} = 1$ ce nombre est le *degré* de l'idéal $\mathfrak{P}$, il est aussi égal à $\lim_{k\to\infty} \frac{H((A/\mathfrak{P})\otimes_R \mathbf{k};k)}{k^{h-1}/(h-1)!}$ où $\mathbf{k}$ est le corps des fractions de R. Plus généralement, si M est un A-module satisfaisant $\operatorname{rg}\operatorname{Ann}_A M = n+1-h < n$, le théorème 7 et la propriété des fonctions de Hilbert mentionnée au début du paragraphe montrent que le degré en les coefficients de U_1 d'une forme résultante de $M[\mathbf{d}]$ est égal à $H(M[\mathbf{d}'] \otimes_{R[\mathbf{d}']} \mathbf{k}; k)$ pour tout k assez grand et où $\mathbf{d}' = (d_2, \ldots, d_h)$ et $\mathbf{k}$ le corps des fractions de $R[\mathbf{d}']$.

Exemple : En prenant $R = \mathbf{Z}$ et $\mathfrak{P} = (0)$ le diviseur $\chi_{\mathbf{d}}((0))$ détermine au signe près une forme, qui n'est autre que le *résultant* $\operatorname{Res}(U_1, \ldots, U_{n+1})$ des $n+1$ formes “génériques” $U_1, \ldots, U_{n+1}$. On définit le résultant $\operatorname{Res}(p_1, \ldots, p_{n+1})$ de $n+1$ formes particulières de degrés $d_1, \ldots, d_{n+1}$ respectivement, en spécialisant les formes $U_1, \ldots, U_{n+1}$ en $p_1, \ldots, p_{n+1}$ dans le résultant générique. On fixe le signe du résultant Res en imposant $\operatorname{Res}(z_0^{d_1}, \ldots, z_n^{d_{n+1}}) = 1$.

On notera que, par définition, le résultant et, plus généralement, les formes résultantes et éliminantes ne dépendent que du module $M[\mathbf{d}]$. Ces formes sont donc invariantes par toutes les transformations des $U_1, \ldots, U_h$ qui laissent invariant $M[\mathbf{d}]$ (permutations, combinaisons linéaires triangulaires, ...).

Proposition 10 – *On suppose que* $R = \mathbf{k}$ *est un corps parfait. Soient* M *un* A*-module,* $\mathbf{d} \in (\mathbf{N}^*)^h$ *et* $p \in A$ *un élément homogène de degré* d_h*, non diviseur de zéro sur* M*. On suppose* $r = \operatorname{rg}\operatorname{Ann}_A M = n+1-h$*, on note* $\mathbf{d}' = (d_1, \ldots, d_{h-1})$ *et* $\varrho : R[\mathbf{d}] \to R[\mathbf{d}']$ *défini par* $\varrho(U_h) = p$*. Alors, si* F *est une forme résultante de* $M[\mathbf{d}]$ *et* F' *une forme résultante de* $M'[\mathbf{d}']$ *où* $M' = M/pM$*, il existe* $\lambda \in \mathbf{k}^*$ *tel que*

$$F' = \lambda.\varrho(F) \ .$$

Démonstration – Si $h \leq 1$ le résultat découle du théorème de l'élimination, §2 de l'exposé 3. Supposons $h > 1$, on sait par la proposition 1 que, pour δ assez grand,

$$\tilde{\mathfrak{F}}(M'[\mathbf{d}'])(\delta) = \varrho(\tilde{\mathfrak{F}}(M[\mathbf{d}])(\delta)) \ ,$$

et donc $\operatorname{div}((F')) = \tilde{\chi}(M'[\mathbf{d}']) = \operatorname{div}(\varrho(\tilde{\mathfrak{F}}(M[\mathbf{d}])(\delta))) \succeq \operatorname{div}(\varrho(F))$, c'est-à-dire $F' \mid \varrho(F)$. D'un autre côté, le degré en les coefficients de U_1 de F' est égal à $H(M'[(d_2, \ldots, d_{h-1})]; k)$ et celui de $\varrho(F)$ est égal à $H(M[(d_2, \ldots, d_h)]; k)$, pour tout k assez grand. Posons $\mathbf{d}'' = (d_2, \ldots, d_{h-1})$, les suites exactes

$$0 \to M[\mathbf{d}''](k-d_h) \xrightarrow{\times p} M[\mathbf{d}''](k) \to M'[\mathbf{d}''](k) \to 0$$

$$0 \to M[\mathbf{d}''](k-d_h) \xrightarrow{\times U_h} M[\mathbf{d}''](k) \to M[(d_2, \ldots, d_h)](k) \to 0$$

montrent

$$H(M[(d_2, \ldots, d_h)]; k) = H(M'[\mathbf{d}'']; k) = \ell(M[\mathbf{d}''](k)) - \ell(M[\mathbf{d}''](k-d_h)) \ .$$

On en conclut que les formes F' et $\varrho(F)$ sont bien proportionnelles. $\square$

Ouf !