# Théorème des Syzygies de Hilbert

Gaspard Fougea et Romain Gourvil
sous la direction de Lie Fu

24 juin 2012

# Table des matières

**1 Introduction** **3**

**2 Les outils** **3**
2.1 Les définitions élémentaires . . . . . 3
2.2 Résolutions projectives et injectives . . . . . 4
2.3 Foncteurs dérivés . . . . . 6
2.4 Quelques Exemples . . . . . 8
2.5 Préliminaires sur les modules sur $k[X_0, ..., X_n]$ . . . . . 8

**3 Le Théorème des Syzygies** **9**
3.1 Résolution minimale . . . . . 9
3.2 Énoncé . . . . . 10
3.3 Nombres de Betti . . . . . 11

**4 Bibliographie** **12**

# 1 Introduction

Nous allons donner dans cet exposé l'énoncé et la démonstration d'un théorème dû à Hilbert : le théorème des Syzygies. Mais qu'entend-on par "syzygie" ? Provenant du grec pour "associer", ce terme renvoie aujourd'hui à l'étude des solutions d'une équation linéaire $\alpha(y) = 0$. Le choix de cette terminologie vient du probléme naturel suivant : dans quelle mesure peut-on "associer" une application $\beta$ à $\alpha$ telle que l'on puisse écrire $y = \beta(x)$ ? Ce problème, qui ne se limite pas à l'algèbre linéaire, est en fait à l'origine de l'étude de l'homologie d'un complexe.
Le théorème en question donne une présentation plus simple d'un module $M$ de type fini sur un anneau de polynômes à l'aide d'un nombre fini de modules libres, appelés les modules de syzygie de $M$. Cette présentation fournit entre autres le nombre de générateurs de $M$ ainsi que les relations entre ces générateurs, en plus d'assurer que les éléments annulés par ces relations constituent exactement l'image d'un certain morphisme de modules libres, d'où le nom du théorème.
Commençons maintenant par présenter les outils d'algèbre homologique nécessaires avant de s'intéresser au théorème à proprement parler.

# 2 Les outils

## 2.1 Les définitions élémentaires

Nous allons ici présenter les outils de l'algèbre homologique nécessaires à l'énonciation et la démonstration du Théorème. Nous resterons dans le cadre qui nous intéresse ici, à savoir la catégorie des $A$-modules. Pour une approche plus générale, consulter [3]. Dans toute la suite, $A$ est un anneau commutatif unitaire.

**Définition 2.1 (Complexes)** -Soit $A$ un anneau. Un *complexe de chaines* de $A$-modules est une famille $C = (C_n)_{n\in\mathbb{Z}}$ de $A$-modules représentée telle quelle :

$... \longrightarrow C_{i+1} \longrightarrow C_i \longrightarrow C_{i-1} \longrightarrow ...$

et des applications $d_i : C_i \to C_{i-1}$ telles que $Im(d_{i+1}) \subset Ker(d_i)$ ( ou alors $d^2 = 0$)
Les $C_n$ sont appelées les chaines de degré n, et on note $H_i(C) = Ker(d_i)/Im(d_{i+1})$, que l'on appelle le $n^{ime}$ groupe d'*homologie* du complexe. Les applications $d_n$ sont appelées les *différentielles* du complexe. Les éléments du noyau $Ker(d_i)$ sont des *cycles*, et les éléments de l'image $Im(d_i)$ s'appellent des *bords*. (par ailleurs tout bord est un cycle)

Une suite exacte est un complexe de chaines dans laquelle on a toujours égalité dans la dernière inclusion.

-Soit $A$ un anneau. Un complexe de *cochaines* de $A$-modules est une famille $C = (C_n)_{n\in\mathbb{Z}}$ de $A$-modules représentée telle quelle :

$... \longrightarrow C^{i-1} \longrightarrow Ci \longrightarrow C^{i+1} \longrightarrow ...$

et des applications $d^i : C^i \to C^{i+1}$ telles que $Im(d^{i+1}) \subset Ker(d^i)$ ( ou alors $d^2 = 0$)
Les $C^n$ sont appelées les cochaines de degré n, et on note $H^i(C) = Ker(d_i)/Im(d_{i-1})$, que l'on appelle le $n^{ime}$ groupe de *cohomologie* du complexe. Les applications $d^n$ sont appeles les différentielles du complexe. Les éléments du noyau $Ker(d^i)$ sont des *cocycles*, et les éléments de l'image $Im(d^i)$ s'appellent des *cobords*. (par ailleurs tout cobord est un cocycle). Si $C$

est un complexe de cochaines, on peut obtenir un complexe de chaines en posant $C_i = C^i$. Les deux terminologies existent car elles ont chacune leur utilité.

Une suite exacte est un complexe de cochaines dans laquelle on a toujours égalité dans la dernière inclusion.

**Exemple 2.2 (Complexes)**

- On prend $C_n = 0$ pour $n < 0$ et $C_n = \mathbb{Z}/8\mathbb{Z}$ pour $n \geq 0$
et $d_n : x \to 4x$. C'est un complexe de chaines.

- Si M est une variété différentielle, on a un complexe de cochaines en posant $C^n$ ={ formes différentielles sur M de degr n } et alors les différentielles sont la différentielle extérieure usuelle. Le $n^{ime}$ groupe de cohomogie du complexe correspond {formes fermées de degré $n$}/{formes exactes de degré $n$}. On l'appelle la cohomologie de Rham.

**Définition 2.3 (Morphisme de Complexes)** Un morphisme de Complexes de chaines $u : C \to D$ est une famille $(u_n)_{n\in\mathbb{Z}}$ d'applications $u_n : C_n \to D_n$ telles que $u_{n-1}d_n = d_{n-1}u_n$
C'est un quasi-isomorphisme si les applications induites $H_n(C) \to H_n(D)$ sont toutes des isomorphismes. (On peut définir de manière équivalente les morphismes de complexes de cochaines.)

**Remarque 2.4** Supposons que l'on a deux complexes de chaines $C$ et $D$, avec des applications $s_n : C_n \to D_{n+1}$, et posons alors le morphisme de chaine $f_n = d_{n+1}s_n + s_{n-1}d_n$. On a aisément $df = fd$

**Définition 2.5 (Homotopies)** On dit que deux applicationt $f$ et $g$ de $C$ vers $D$ sont homotopes s'il existe des applications $(s_n : C_n \to D_{n+1})_n$ telles que $f - g = sd + ds$. Les applications $(s_n)_n$ sont appelées les homotopies de $f$ à $g$. Finalement, on dit que $f : C \longrightarrow D$ est une équivalence de d'homotopie si il existe une application $g : D \longrightarrow C$ telles que $gf$ et $fg$ sont homotopes respectivement aux applications identité de $C$ et $D$.

**Définition 2.6 ( Module Libre )** Un $A$-module $M$ est dit *libre* s'il s'écrit sous la forme $A^{(I)}$, où I est un ensemble fini ou non. Par ailleurs tout module libre possède des bases, qui ont toutes le meme cardinal : le *rang* de M.

## 2.2 Résolutions projectives et injectives

**Définition 2.7 (Module Projectif)** Un $A$-module $M$ est *projectif* s'il vérifie la propriété suivante : Si on a deux $A$-modules B et C, associs un morphisme surjectif $g : B \to C$ et un morphisme $y : M \to C$ Alors il existe au moins un morphisme $\beta : M \to B$ tel que $y = go\beta$

**Proposition 2.8** *Soit $M$ un A-module. Les trois assertions suivantes sont quivalentes :*

*(i) $M$ est projectif*

*(ii) M est facteur direct dans un module libre.*

*(iii) $Hom_A(M, -)$ est un foncteur exact, c'est à dire que pour toute suite exacte courte $0 \longrightarrow F \longrightarrow B \longrightarrow C \longrightarrow 0$, alors $0 \longrightarrow Hom_A(M, F) \longrightarrow Hom_A(M, B) \longrightarrow Hom_A(M, C) \longrightarrow 0$ est exacte*

PREUVE. Nous prouvons ici $(i) \Leftrightarrow (iii)$. Supposons que $Hom_A(M, -)$ est exact, et supposons que nous avons une surjection $g : B \to C$, et un morphisme $\alpha : M \to C$. L'application induite par g de $Hom(M, B) \to Hom(M, C)$ est aussi surjective. Donc il existe $\beta \in Hom(M, B)$ tel que $\alpha = go\beta$. C'est bien dire que M est projectif.
Supposons que $M$ est projectif. Pour montrer que $Hom(M, -)$ est exact, il suffit de montrer que pour toute surjection $g : B \to C$ comme ci-dessus, l'application induite $g_*$ est galement surjective. Si on a $\alpha \in Hom(M, C)$, la propriété de projectivité de $M$ nous donne $\beta \in Hom(M, B)$ tel que $\alpha = go\beta = g_*(\beta)$. C'est dire que $g_*$ est surjectif. □ □

**Définition 2.9 (Résolution à gauche)** Soit $M$ un $A$-Module. Une *résolution à gauche* de M est un complexe de chaines $P_\bullet$, avec $P_i = 0$ pour $i < 0$, et une application $\alpha : P_0 \to M$ telle que le complexe $... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$

est exact. C'est une résolution projective si tous les $P_i$ sont projectifs.

**Lemme 2.10** *Tout A-module M a une résolution projective.*

PREUVE DU LEMME. On construit la rsolution projective du module par rcurrence sur $n$. Soit un module projectif $P_0$ et une surjection $\alpha_0 : P_0 \to M$. On pose alors $M_0 = Ker(\alpha_0)$. Considérons maintenant un module $M_{n-1}$ on choisit un module projectif $P_n$ et une surjection $\alpha_n : P_n \to M_{n-1}$. On pose $M_n = Ker(\alpha_n)$ et on pose alors $d_n$ comme étant la compose $P_n \longrightarrow M_{n-1} \longrightarrow P_{n-1}$.
Comme $d_n(P_n) = M_{n-1} = Ker(d_{n-1})$, la chaine complexe P est bien une résolution projective de M. □

**Théorème 2.11 (De Comparaison)** Soit $P_\bullet \longrightarrow M$ Une résolution projective de M. (Avec $\epsilon : P_0 \to M$) et $f : M \to N$ Un morphisme.
Alors pour toute résolution projective $Q_\bullet \to N$ (Avec $\eta : Q_0 \to N$) il existe un morphisme de Chaine $f : P_\bullet \to Q_\bullet$ telle que $\eta of = f_0 o\epsilon$. Le morphisme $f$ est alors unique à homotopie de chaine près.

PREUVE DU THÉORÈME On note $(d_n)_n$ les différentielles de P et $(u_n)_n$ les différentielles de Q.
On va construire les $f_n$ et montrer leur unicité par récurrence, en prenant $f_{-1} = f$. Supposons connue $f_i$ pour $i \leq n$ telle que $f_{i-1}d_i = u_i f_i$. Si $n \geq 0$, le fait que $f_{n-1}d = uf_n$ montre que $f_n$ induit une application $f'_n : Ker(d_n) \to Ker(u_n)$. On a alors les suites exactes suivantes :

$$\longrightarrow P_{n+1} \longrightarrow Ker(d_n) \longrightarrow 0 \text{ et } \longrightarrow Ker(d_n) \longrightarrow P_n \longrightarrow P_{n-1}$$

$$\longrightarrow Q_{n+1} \longrightarrow Ker(u_n) \longrightarrow 0 \text{ et } \longrightarrow Ker(u_n) \longrightarrow Q_n \longrightarrow Q_{n-1}$$

La propriété universelle du projectif $P_{n+1}$ cre une application $f_{n+1} : P_{n+1} \to Q_{n+1}$ telle que $uf_{n+1} = f'_n d = f_n d$. On a ainsi construit notre application. Montrons que c'est un quasi-isomorphisme.
Supposons que $g : P \to Q$ est une autre application correspondant aux hypothèses. Posons $h = f - g$. On va construire par récurrence une suite d'applications $(s_n : P_n \to Q_{n+1})_n$ qui

sera une contraction de chaines de $h$.
Si $n < 0$, alors $P_n = 0$. On pose alors $s_n = 0$. Si $n = 0$, notons que comme $\eta h_0 = \epsilon(f - f) = 0$, l'application $h_0$ envoie $P_0$ sur $Ker(u_0) = u(Q_1)$. On utilise la propriété de projectivité de $P_0$ pour obtenir un morphisme $s_0 : P_0 \to Q_1$ telle que $h_0 = us_0 = us_0 + s_{-1}d$
On suppose alors qu'on a les applications $s_i (i < n)$ telles que $us_{n-1} = h_{n-1} - s_{n-2}d$, et on considère l'application $h_n - s_{n-1}d : P_n \to Q_n$. On voit que :

$d(h_n - s_{n-1}d) = dh$ , $-(h_{n-1} - s_{n-2}d)d = (uh - hd) + s_{n-2}dd = 0$.

Ainsi $h_n - s_{n_1}d$ a son image dans $Ker(d_n)$, un quotient de $Q_{n+1}$. La propriété de projectivité de $P_n$ nous donne l'application voulue $s_n : P_n \to Q_{n+1}$ telle que $us = h - sd$. □

**Définition 2.12 (Module Injectif)** Un $A$-module M est *injectif* s'il vérifie la propriété suivante :
Si on a deux $A$-modules $B$ et $C$, associs un morphisme injectif $f : C \to B$ et un morphisme $\alpha : C \to M$, alors il existe au moins une application $\beta : B \to M$ telle que $\alpha = \beta of$

**Remarque 2.13** Dans le cas injectif, les démonstrations étant similaires au cas projectif, nous ne les ferons pas.

**Définition 2.14 (Résolution injective)** Soit $M$ un $A$-Module. Une *résolution droite* de $M$ est un complexe de cochaines $I^\bullet$, avec $I^i = 0$ pour $i < 0$, et une application $\alpha : M \to I^0$ telle que le complexe $0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow ...$

est exacte. C'est une résolution injective si tous les $I^i$ sont injectifs.

**Lemme 2.15** Tout $A$-Module $M$ possde une résolution injective.

**Remarque 2.16** *La catégorie des A-modules a assez de projectif, et assez d'injectifs, c'est dire que pour tout object B de cette catégorie, il existe une injection $B \to I$, avec I injectif, et il existe une surjection $P \to B$, avec P projectif. Ce sont ces propriétés qui sont l'origine de l'existence de résolutions injectives et projectives pour des modules.*

**Théorème 2.17 (De Comparaison)** Soit $N \longrightarrow I^\bullet$ Une résolution injective de N. et $f : M \to N$ un morphisme.
Alors pour toute résolution injective $M \to E$ il existe un morphisme de complexe de cochaine $F : E \to I$ . Le morphisme $F$ est alors unique à homotopie de chaine près.

## 2.3 Foncteurs dérivés

**Définition 2.18**

1. Soit $F : A \to B$ un foncteur entre deux catégories additives A et B. On dit que :
2. F est *exact* si pour toute suite exacte courte $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, alors $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$ est exacte
3. F est *exact à droite* si pour toute suite exacte courte $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, alors $F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$ est exacte
4. F est *exact à gauche* si pour toute suite exacte courte $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, alors $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$ est exacte

**Définition 2.19** Soit $F : A - mod \to Ab$ un foncteur exact à droite ($Ab$ tant une catgorie ablienne). Comme $A - mod$ est une catégorie possdant assez de projectifs, si $M \in A - mod$, on peut définir le *foncteur dérivé gauche* $L_iF(i \geq 0)$ de F comme suit :
On choisit une résolution projective (une fois pour toutes) $P_\bullet \longrightarrow M$ et on définit $L_iF(M) = H_i(F(P_\bullet))$ Noter que l'on a toujours $L_0F(M) = F(M)$

**Lemme 2.20** Les objects $L_iF(M)$ sont bien définis à isomorphisme près. C'est à dire que si $Q_\bullet \longrightarrow M$ est une autre résolution de $M$, il y a un isomorphisme canonique $H_i(F(P_\bullet)) \to H_i(F(Q_\bullet))$

Preuve du Lemme. D'aprs le théorème de comparaison énoncé plus haut, il y a un morphisme de chaines $f : P_\bullet \to Q_\bullet$ qui prolonge l'application $id_M$ aux résolutions $P$ et $Q$. (Avec les notations du théorème, on prend ici $M = N$), et f induit une application $f_*$ de $H_iF(P_\bullet)$ vers $H_iF(Q_\bullet)$. Tout autre morphisme de chaine $f'$ qui vérifie ces conditions est homotope à $f$. Donc $f_* = f'_*$.
De la meme manière, il y a une application $g : Q_\bullet \to P_\bullet$ qui prolonge $id_M$ et induit $g_*$. Comme $gf$ et $id_{P_\bullet}$ sont deux applications qui prolongent $id_M$, on a :

$g_*f_* = (gf)_* = (id_{P_\bullet})_*$ =morphisme identité sur $H_iF(P_\bullet)$.

De la meme manière, $fg$ et $id_{Q_\bullet}$ prolongent $id_M$, dont $f_*g_*$ est l'identité. Cela prouve que $f_*$ et $g_*$ sont des isomorphismes. □

□

**Définition 2.21** *Si $M$ et $N$ sont des $A$-modules, $Tor_n(M,N)$ correspond au foncteur dérivé à gauche de $M$ pour $T(-) = - \bigotimes_A N$ qui est un foncteur exact à droite.*

$Tor_n(M,N) = L_nT(M)$

***Remarque 2.22*** Pour définir $Tor$, on peut également prendre une résolution injective de N, et appliquer la meme méthode que pour les foncteurs dérivés droite. Il y a un isomorphisme canonique entre les deux objects.

***Définition 2.23*** Soit $F : A - mod \to Ab$ un foncteur exact à gauche. Comme $A - mod$ est une catégorie possédant assez d'injectifs. Si $M \in A - mod$, on peut définir le *foncteur dérivé à droite* $R^iF(i \geq 0)$ de F comme suit :
On choisit une résolution injective (une fois pour toutes) $M \longrightarrow I^\bullet$ et on définit

$R^iF(M) = H^i(F(I^\bullet))$

*Ainsi, si $M$ et $N$ sont deux $A$-modules, on pose $F(N) = Hom_A(M,N)$ qui est un foncteur exact à gauche. Son foncteur dérivé à droite est, par dfinition :*

$Ext^i_A(M,N) = R^iHom_A(M,-)(N)$

***Remarque 2.24*** Pour définir $Ext$, on peut également prendre une résolution projective de N, et appliquer la meme méthode que pour les foncteurs dérivés à gauche. Il y a un isomorphisme canonique entre les deux objects.

## 2.4 Quelques Exemples

***Proposition 2.25*** *Soient $m$ et $n \in \mathbb{N}*$. Alors, si $d = pgcd(m,n)$*
$Tor_0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \bigotimes \mathbb{Z}/m\mathbb{Z}$
$Tor_1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$

PREUVE. *On construit la résolution projective de $\mathbb{Z}/n\mathbb{Z}$ suivante :*
$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$
*dans laquelle la flèche $\mathbb{Z} \longrightarrow \mathbb{Z}$ correspond la multiplication par $n$. On applique le foncteur $T$ décrit plus haut, et on obtient :*
$0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \bigotimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$
*Alors, on a automatiquement $Tor_0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \bigotimes \mathbb{Z}/m\mathbb{Z}$*
*. On note $\phi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ tel que $\forall k \in \mathbb{Z}/m\mathbb{Z}, \phi(k) = nk$. $Tor_1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = Ker(\phi)$. On note $k^*$ un reprsentant de $k$ dans $[[0,m]]$*
*$\phi(k) = 0 \Rightarrow \exists l \in \mathbb{Z}$ tel que $nk^* = lm$. On note $m = di$ et $n = dj$. Or,*
*$nk^* = lm = ldi \Rightarrow jk^* = li$. Or, comme $i$ et $j$ sont premiers entre eux, d'après le lemme de Gauss, $i$ divise $k^*$. Réciproquement, si $k^* = ai$ ($a$ étant un entier), alors, $nk^* = djai = maj \in m\mathbb{Z}$. On a donc montré que $Ker(\phi) = \{0, i, 2i, 3i, ..., (d-1)i\}$, qui est un groupe cyclique à $d$ lments. On a donc $Tor_1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$* □

***Lemme 2.26*** *Si $M$ et $N$ sont deux $A$-modules tel que au moins l'un deux est libre, alors $\forall n \geq 1$, $Tor_n(M,N) = 0$*

PREUVE DU LEMME. Si $M$ est libre, il est par conséquent projectif, et sa résolution projective $P_\bullet$ est triviale : $\forall n \geq 1, P_n = 0$. Le résultat en découle immédiatement.
Si $N$ est libre, le foncteur $- \bigotimes_A N$ est exact. On en déduit donc que le complexe de chaines $(P_n \bigotimes_A N)_{n \geq 1}$ est une suite exacte. On en dduit donc que $\forall n \geq 1$, $Tor_n(M,N) = 0$. □

## 2.5 Préliminaires sur les modules sur $k[X_0, ..., X_n]$

*Soit $k$ un corps. On travaille désormais sur l'anneau $S = k[X_0, X_1, ..., X_n]$ l'anneau des polynomes en $n+1$ variables. On considère que c'est une algèbre graduée, dans laquelle chaque variable est de degré 1. On peut donc écrire $S = \bigoplus_{n \in \mathbb{N}} S_n$, où chaque $S_n$ est homogène de degré $n$.*

***Définition 2.27*** On définit alors le tordu comme tel : pour $a \in Z$, on pose $S(a) = k[X_0, X_1, ..., X_n]$ tel que $\forall n \in Z, S(a)_n = S_{n+a}$

**Définition 2.28** Un module gradué sur S est un module qui se décompose sous la forme : $M = \bigoplus_{n \in \mathbb{N}} M_n$, tel que $\forall (i,j) \in \mathbb{N}^2$, $S_i M_j \subseteq M_{i+j}$ On définit alors de la meme manière le tordu d'un module gradué : on note $\forall (a,n) \in \mathbb{Z}^2, M(a)_n = M_{n+a}$

**Définition 2.29** Un morphisme de la catégorie des modules gradués, (ou morphisme homogène) est un morphisme $\phi : \bigoplus_{n \in \mathbb{N}} M_n \to \bigoplus_{n \in \mathbb{N}} N_n$ tel que pour tout $n \in \mathbb{N}$, $\phi(M_n) \subset N_n$. Autrement dit, $\phi$ préserve le degré.

**Remarque 2.30** Grace aux tordus, toute résolution projective, ou injective d'un $S$-module peut etre graduée, i.e. que tous les morphismes sont homogènes (cela sera prouvé plus tard). Cela fournit ainsi $Ext$ et $Tor$ des structures de modules gradués. C'est grace à cela que l'on pourra définir les Syzygies.

# 3 Le Théorème des Syzygies

Dans toute cette partie, $M$ désignera un $S$-module gradué, où $S = k[X_0, ..., X_n]$ et $k$ est un corps.
On note : $M = \oplus_d M_d$

## 3.1 Résolution minimale

**Lemme 3.1 (Lemme de Nakayama)** *(cas d'un module gradué) Soit $M$ un $S$-module gradué de type fini. Soit $\mathfrak{m} = (X_0, ..., X_n)$. Si $m_1, ..., m_r$ engendrent $M/\mathfrak{m}M$, alors $m_1, ..., m_r$ engendrent $M$.*

PREUVE. *On pose $N = M/(\sum S m_i)$. On veut montrer que $N = 0$. Comme les $m_i$ engendrent $M/$, $N/\mathfrak{m}N = 0$. Supposons par l'absurde $N \neq 0$. Comme $M$ est de type fini, $N$ aussi, donc il existe un élément non nul de $N$ de degré minimal $x$. Mais alors tous les éléments de $\mathfrak{m}N$ sont de degré supérieur à $deg(x) + 1$, contredisant le fait que $N = \mathfrak{m}N$.* □

**Définition 3.2 (Résolution minimale)** On se donne une résolution libre de $M$ :
$... \xrightarrow{\delta_{r+1}} F_r \xrightarrow{\delta_r} ... \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \to 0$
Cette résolution est dite minimale si :
$\forall i \in \mathbb{N}, Im(\delta_i) \subseteq \mathfrak{m}F_{i-1}$, où $\mathfrak{m} = (X_0, ..., X_n)$ est l'idéal des éléments de $S$ sans coefficient constant.

**Proposition 3.3** *La résolution est minimale si et seulement si pour tout $i \in \mathbf{N}$, $F_i$ est engendré par un nombre minimal de générateurs de $Ker(\delta_i)$.*

PREUVE. *Par le lemme de Nakayama, $F_i$ est engendré par un nombre minimal de générateurs de $Ker(\delta_i)$ si et seulement si $\delta_i$ induit un isomorphisme $\delta_i^*$ entre $F_i/\mathfrak{m}F_i$ et $Im(\delta_i)/\mathfrak{m}Im(\delta_i)$. En effet, un système* minimal *de générateurs est inclus dans $F_i/\mathfrak{m}F_i$, et un générateur $x$ qui serait envoyé dans $\mathfrak{m}Im(\delta_i)$ serait dans $Ker(\delta_i)$ (car $M$ est de type fini). Réciproquement, si on a un générateur indispensable de plus dans $F_i$, alors quitte à changer d'ensemble de générateurs, $\delta_i^*$ annule un des générateurs $x$ de $F_i$ (les deux modules ont même rang). Il existe donc $m \in \mathfrak{m}$ et $v \in F_i$ tels que $x = mv$, contredisant la minimalité du système de générateurs choisi.*
*Or $F_{i+1} \to F_i \to Im(\delta_i) \to 0$ est exacte, donc :*
*$F_{i+1}/\mathfrak{m}F_{i+1} \to F_i/\mathfrak{m}F_i \to Im(\delta_i)/\mathfrak{m}Im(\delta_i) \to 0$ l'est également*
*On en déduit que $\delta_i^*$ est un isomorphisme si et seulement si l'application induite par $\delta_{i+1}$ est nulle, i.e. $Im(\delta_{i+1}) \subseteq \mathfrak{m}F_i$.* □

**Remarque 3.4** *La proposition précédente nous assure l'existence et l'unicité d'une résolution minimale.*

**Exemple 3.5 (Résolution de Koszul)** *On a une résolution minimale de k[x,y] :*
$0 \to k[x](-2) \xrightarrow{\phi} k[x,y](-1)^2 \xrightarrow{\psi} k[x,y] \to 0$
*où $\phi(P) = (XP, YP) et \psi(P, Q) = YP - XQ$.*
*De manière plus générale, si $R$ est un module et $x, y \in R$, on a un diagramme commutatif*

*pour les multiplications par x et y :*

$$\begin{array}{ccccc} 0 & \longrightarrow & R & \xrightarrow{x} & R \\ & & \downarrow{\scriptstyle y} & & \downarrow{\scriptstyle y} \\ 0 & \longrightarrow & R & \xrightarrow{x} & R \end{array}$$

*Ceci nous permet de construire le complexe suivant :*

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \xrightarrow{x} & R & & \\ & & & \searrow^{y} \quad \oplus \quad \searrow^{y} & & & \\ 0 & \longrightarrow & R & \xrightarrow[-x]{} & R & \longrightarrow & 0 \end{array}$$

*On retrouve ainsi la résolution précédente. Mieux : on a donné un algorithme fournissant une résolution minimale de $k[X_0, ..., X_n]$ pour tout $n$.*
*Pour une définition précise et une discussion approfondie sur les résolutions de Koszul, voir [2] .chap17*

## 3.2 Énoncé

[Théorème des Syzygies] Soit $M$ un $S$-module gradué de type fini, alors il admet une résolution libre minimale (nécessairement unique) *finie*
$0 \to F_r \to ... \to F_1 \to F_0 \to M \to 0$
On a de plus $r \leq n+1$. On appelle alors $F_p$ la p-ème *syzygie* de M.

**Lemme 3.6** *Soit $M$ un $S$-module gradué de type fini. Alors $M$ projectif $\implies$ $M$ libre*

PREUVE. *On a une résolution projective de $M$ :*

$0 \to M \to M \to 0$
*On en déduit que $Tor_1(M,k) = 0$ où $k = S/\mathfrak{m}$.*
*Soit $F$ un module libre gradué tel que $F \xrightarrow{\phi} M \to 0$ donne un système minimal de générateurs de $M$. On pose $N = Ker(\phi)$. Montrons que $N = 0$.*
*Par définition d'un foncteur dérivé, la suite exacte $0 \to N \to F \to M \to 0$ donne une suite exacte :*
$0 = Tor_1(M,k) \to N \otimes_S k \to F \otimes_S k \to M \otimes_S k \to 0$
*donc $0 \to N/\mathfrak{m}N \to F/\mathfrak{m}F \xrightarrow{\psi} M/\mathfrak{m}M \to 0$ est exacte.*
*Or $F$ est engendré par un nombre minimal de générateurs de $M$, donc $\psi$ est un isomorphisme par le lemme de Nakayama. On en déduit que $N/\mathfrak{m}N = 0$, et donc $N = 0$ d'après le lemme de Nakayama.* □

On obtient ainsi l'existence d'une unique résolution libre minimale, éventuellement infinie. Afin de prouver la finitude, nous allons maintenant nous intéresser à une manière pratique de décrire une résolution minimale : les nombres de Betti.

### 3.3 Nombres de Betti

Le lecteur intéressé par des applications pratiques des nombres de Betti pourra consulter les deux premiers chapitres de [1] .

**Définition 3.7** *Soit* $... \to F_i \to ... \to F_0 \to M \to 0$ *la résolution libre minimale d'un* $S$*-module gradué de type fini* $M$*. On pose* $F_i = \bigoplus_{j\in\mathbb{Z}} S(-j)^{\beta_{ij}}$*. Les* $\beta_{ij}$ *sont appelés les nombres de Betti de* $M$*.*

**Lemme 3.8** *1.* $\beta_{i0} = ... = \beta_{ik} = 0 \implies \beta_{i+1,0} = ... = \beta_{i+1,k+1} = 0$

2. $\beta_{ij} = dim((Tor_i(M,k))_j)$ *où* $A_j$ *désigne l'ensemble des éléments homogènes de degré* $j$ *d'une algèbre extérieure* $A$*.*
3. $Tor_i(M,k) = H_i((M(-p) \otimes_k \Lambda^p(k^{n+1})(-p))_{p\in\mathbb{N}})$
   $Tor_i(M,k)_j = H_i((M_{j-p} \otimes_k \Lambda^p(k^{n+1})(-p))_{p\in\mathbb{N}})$

PREUVE. *1. Conséquence de la minimalité.*

2. *On a montré que l'ième homologie du complexe* $(F_i \otimes_S k)i \in \mathbb{N}$ *est égale à* $F_i \otimes_S k$*. On a donc :*
   $Tor_i(M,k) = F_i/\mathfrak{m}F_i = \oplus_j k(-j)^{\beta_{ij}}$
3. *On pose* $V = k^{n+1}$*. On a une résolution (dite de Koszul) de* $k$ *:*
   $0 \to \Lambda^{n+1}V \otimes_k S(-n-1) \to ... \to \Lambda^2 V \otimes_k S(-2) \to V \otimes_k S(-1) \to k \to 0.$
   *Comme* $N \otimes_S S(-j) = N(-j)$ *pour tout* $S$*-module* $N$*, on a* $Tor_i(M,k) = H_i((M(-p) \otimes_k \Lambda^p(k^{n+1})(-p))_{p\in\mathbb{N}})$*.*
   *L'égalité suivante en découle, car comme toutes les applications préservent le degré, on obtient une somme directe de complexes à partir de* $M = \oplus_j M_j$*.*

□

D'après le lemme, $\beta_{ij} \leq dim(\Lambda^i V \otimes_k M_{j-i}) = dim(M_{j-i}) \times C^i_{r+1}$.
En particulier, $\beta_{ij} = 0\ \forall i > r+1$, ce qui achève la preuve du théorème.

On termine par un résultat reliant la fonction de Hilbert aux nombres de Betti.

**Définition 3.9** *On définit la* fonction de Hilbert *de* $M$ *par :*
$H_M(d) = dim_k(M_d)$

**Proposition 3.10** $H_M(d) = \sum_i (-1)^i \sum_{j=0}^{n+1} \beta_{ij} C^n_{n+d-j}$

PREUVE. *Cela découle de la suite exacte exhibée au lemme 2.7* □

*Les nombres de Betti forment donc un invariant plus fin que la fonction de Hilbert.*

# 4 Bibliographie

## Références


[1] David Eisenbud. *Geometry of Syzygies.* Springer, 2002.

[2] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer, 2004.

[3] Charles A. Weibel. *An Introduction to Homological Algebra.* Cambridge University, 1994.