Université Grenoble Alpes

RAPPORT DE TER

Sur la Conjecture Jacobienne

Pierre Fromont

Encadrant : Estanislao Herscovich

Janvier 2019 — Mai 2019

Table des matières

1 Introduction

La conjecture Jacobienne a été formulée par le mathématicien allemand Ott-Heinrich Keller en 1939.
Cette conjecture est une généralisation du théorème d'inversion locale dans le cas des applications polynomiales a plusieurs variables. La formulation précise de la conjecture est :
Soit $n > 1$, K un corps de caractéristique 0 et $F = (F_1, ..., F_n)$ une suite de n polynômes en les n variables $X_1, ..., X_n$ sur K, vue comme une application (on appellera ce genre d'application une application polynomiale) de K^n dans K^n. Alors si le jacobien de F : $J = det((\frac{\partial F_i}{\partial X_j})_{1 \leq i,j \leq n})$ est une constante non nulle alors F admet un inverse G qui est aussi une application polynomiale.
A ce jour, cette conjecture n'a toujours pas été prouvée, bien que des avancées majeures ont été réalisées, réduisant considérablement le nombre de cas à étudier.
En effet, en 1980 Wang montra que la conjecture est vérifiée pour les polynômes de degré 2 et en 1982, Bass, Connell et Wright montrèrent que la vérification pour les polynômes de degré 3 entraine la validité de la conjecture Jacobienne.
L'objectif de ce TER est de mettre en relation la conjecture Jacobienne avec deux autres conjectures : La conjecture de Dixmier et la conjecture de Poisson et en montrant que ces trois conjectures sont en fait équivalents.

2 Application polynomiale

On va commencer par introduire plus formellement la conjecture Jacobienne et énoncer quelques résultats sur les applications polynomiales.
Dans toute cette section, K désigne un corps de caractéristique 0 et n et m des entiers non nuls.
De plus on note $X := K^n$, $Y := K^m$, $K[X] := K[x_1, ..., x_n]$ et $K[Y] := K[y_1, ..., y_m]$.

Définition : Soit $F : X \longrightarrow Y$ et $p \in X$, on dit que F est une application polynomiale ou un endomorphisme polynomiale s'il existe $F_1, ..., F_n \in K[X]$ tel que pour tout $p \in X$, $F(p) = (F_1(p), ..., F_n(p))$.

On appelle degré de F, noté deg(F), le maximum des degrés des F_i $(1 \leq i \leq n)$
Si F a un inverse qui est aussi une application polynomiale, on dit que F est un isomorphisme polynomiale.

Remarque : Une application polynomiale peut être bijective et avoir un inverse non polynomiale, C'est le cas pour la fonction définie sur $\mathbb{R}$ par $f(x) = x^3$.

La conjecture jacobienne propose un critère pour qu'une application polynomiale ait un inverse polynomiale :

Conjecture Jacobienne : Pour tout entier $n \geq 1$ et $F := (F_1, ..., F_n) : K^n \longrightarrow K^n$ une application polynomiale tel que $detJF \neq 0$ sur K^n. Alors F admet un inverse polynomiale, ie il existe $G := (G_1, ..., G_n) : K^n \longrightarrow K^n$ une application polynomiale tel que $G.F = (x_1, ..., x_n)$.

Remarque : Comme $detJF$ est un polynôme de $K[X]$ et que K est algébriquement clos, dire que $detJF \neq 0$ sur K^n revient à dire que $detJF$ est une constante non nulle de K.
De plus, cette conjecture est fausse si K n'est pas de caractéristique nulle. En effet, si n=1 et p est un nombre premier alors le polynôme $P = X^p - X$ de $\mathbb{F}_p[X]$ a pour jacobien -1 mais P est nul sur $\mathbb{F}_p$.

K étant de caractéristique nulle, on peut identifier $g \in K[X]$ à l'application qu'on notera aussi g :
$g : X \longrightarrow K$ qui a $p \in X$ associe $g(p)$.
Soit $F : X \longrightarrow Y$ une application polynomiale alors on peut définir le comorphisme $F^* : K[Y] \longrightarrow K[X]$ défini par $F^*(g) = g.F$.
Avec cette définition, F^* est un morphisme de K-algèbre de $K[Y]$ dans $K[X]$. De même, si on a un morphisme de K-algèbre $\phi : K[Y] \longrightarrow K[X]$ on peut définir le comorphisme $\phi_* : X \longrightarrow Y$ défini par $\phi_*(p) = (\phi(y_1)(p), ..., \phi(y_n)(p))$. Et dans ce cas, ϕ_* est une application polynômiale.

Proposition : Soit $F : X \longrightarrow Y$ une application polynomiale, alors $(F^*)_* = F$.
De plus, si $Z = K^r$ et $G : Y \longrightarrow Z$ est une application polynomiale, alors $(G.F)^* = F^*.G^*$.

Preuve : Pour tout i, le polynôme y_i s'identifie en tant qu'application de Y dans K à la i-ème fonction

coordonnée. Ainsi, l'application $F^*(y_i) = y_i.F : X \longrightarrow K$ à $p \in X$ associe $F_i(p)$.
Donc $(F^*)_* : X \longrightarrow Y$ et $\forall p \in X, (F^*)_*(p) = (F_1(p), ..., F_n(p)) = F(p)$.
Donc $(F^*)_* = F$.

L'application $G.F : Y \longrightarrow Z$ à $p \in X$ associe $G.F(p) = (G_1(F(p)), ..., G_r(F(p)))$ et $\forall i, G_i.F : X \longrightarrow K$ qui à $p \in X$ associe $G_i(F_1(p), ..., F_m(p))$ s'identifie bien à un polynôme de $K[X]$. Donc $G.F$ est une application polynômiale.
De plus, $\forall g \in K[X], (G.F)^*(g) = g.(G.F) = (g.G).F = F^*(G^*(g))$.
Donc $(G.F)^* = F^*.G^*$

On a de même le résultat :

Proposition : Si $\phi : K[Y] \longrightarrow K[X]$ est un morphisme de K-algèbre alors $(\phi_*)^* = \phi$.
De plus si $Z = K^r$ et $\psi : K[Z] \longrightarrow K[Y]$ est un morphisme de K-algèbre alors $(\phi.\psi)_* = \psi_*.\phi_*$.

Preuve : L'application $(\phi_*)^* : K[Y] \longrightarrow K[X]$ est définie par $\forall g \in K[Y], (\phi_*)^*(g) = g.\phi_*$
et $g.\phi_* : X \longrightarrow K$, avec $\forall p \in X, g.\phi_*(p) = g(\phi(y_1)(p), ..., (\phi(y_m)(p))$ donc si $g = \sum_\alpha a_\alpha y_1^{\alpha_1}...y_m^{\alpha_m}$ alors $g.\phi_*$ correspond au polynôme $\sum_\alpha a_\alpha \phi(y_1)^{\alpha_1}...\phi(y_m)^{\alpha_m}$.
Or ce polynôme est exactement $\phi(g)$, donc $(\phi_*)^* = \phi$.
On a $\forall p \in X, (\phi.\psi)_*(p) = (\phi.\psi(z_1)(p), ..., \phi.\psi(z_r)(p))$ et
$\psi_*.\phi_*(p) = (\psi(z_1)(\phi_*(p)), ..., \psi(z_r)(\phi_*(p))$.
Or si $\psi(z_i) = \sum_\alpha a_\alpha y_1^{\alpha_1}...y_m^{\alpha_m}$, l'application qui à $p \in X$ associe $\psi(z_i)(\phi_*(p))$ correspond au polynôme $\sum_\alpha a_\alpha \phi(y_1)^{\alpha_1}...\phi(y_m)^{\alpha_m}$ et ce polynôme est exactement $\phi(\psi(z_i))$.

Corollaire : Une application polynômiale $F : X \longrightarrow Y$ est un isomorphisme si et seulement si F^* est un isomorphisme.

Nous allons donner une autre formulation de la conjecture jacobienne avec le comorphisme.

Lemme : Si $F : X \longrightarrow X$ est une application polynomiale avec $detJF \neq 0$ sur X. Alors F^* est surjective.

Preuve : Par l'absurde, supposons que $F^* : K[X] \longrightarrow K[X]$ n'est pas injective.
Soit $g \in K[X]$ le polynôme de plus petit degré tel que $F^*(g) = 0$, c'est-à-dire que $g.F = 0$.
Posons $g_i = \frac{\partial g}{\partial x_i}$ et $v(g_1(F_1, ..., F_n), ..., g_n(F_1, ..., F_n))$.
Alors en dérivant l'équation $g.F = 0$ on obtient :
$\forall p \in X, v(p).JF(p) = 0$.
Comme $\forall p \in X, detJF(p) \neq 0$, on a $\forall p \in X, v(p) = 0$.
Or g n'est pas constant car F^* est un morphisme d'algèbre, donc il existe un indice i tel que $g_i \neq 0$ et $g_i.F = 0$.
Donc $F^*(g_i) = 0$ et $deg(g_i) < deg(g)$. Ce qui est contraire à l'hypothèse sur g.
Donc F^* est injective.

Si $F = (F_1, ..., F_n) : X \longrightarrow X$ est une application polynomiale, on peut considérer la sous-algèbre $K[F_1, ..., F_n]$ de $K[X]$ engendré par les composantes de F. C'est aussi l'image de $K[X]$ par le comorphisme F^*. Et dire que F^* est surjective revient à dire que $K[F_1, ..., F_n] = K[X]$.
Or, on a vu que si $detJF$ est non nul sur X alors F^* est injective, donc si on a de plus que F^* est surjective alors F^* est un isomorphisme. Et ainsi, F admet un inverse polynomiale.

D'où la reformulation de la conjecture jacobienne :

Conjecture Jacobienne : Si $F : K^n \longrightarrow K^n$ est une application polynomiale vérifiant $detJF \neq 0$ sur K^n. Alors $K[F_1, ...F_n] = K[X_1, ..., X_n]$ (ie F^* est surjective).

3 Algèbre de Weyl

Dans cette partie nous allons introduire l'algèbre de Weyl et formuler la conjecture de Dixmier. On montrera dans une autre partie que cette conjecture est équivalente à la conjecture Jacobienne.
Dans cette partie, K est un corps de caractéristique nulle et on note $K[X]$ l'anneau des polynômes $K[x_1, ..., x_n]$.
Soit $End_K(K[X])$ la K algèbre des endomorphismes linéaires (aussi appelé opérateurs linéaires) de $K[X]$ vu en tant que K espace vectoriel.
Dans cette algèbre, on va considérer deux familles d'endomorphismes :

1. La multiplication par x_i $(1 \leq i \leq n)$, notée aussi par x_i.
2. La dérivation par rapport à x_i $(1 \leq i \leq n)$, qu'on notera ∂_i.

L'algèbre de Weyl est la K sous algèbre de $End_K(K[X])$ engendrée par les opérateurs linéaires $x_1, ..., x_n, \partial_1, ..., \partial_n$.
On note cette algèbre $A_n(K)$ ou A_n lorsque le corps de base est explicite.
Si $P, Q \in A_n$ on note $[P, Q]$ leur commutateur.
$[P, Q] \in A_n$ et est défini par $\forall f \in K[X], [P, Q](f) = P \circ Q(f) - Q \circ P(f)$
Regardons maintenant les commutateurs des générateurs de A_n.

Proposition : Soit $i, j \in \{1, ..., n\}$ alors

1) $[\partial_i, x_j] = \delta_{i,j}1$ (1 est ici l'unité de A_n)
2) $[x_j, \partial_i] = -1\delta_{i,j}$
3) $[x_i, x_j] = [\partial_i, \partial_j] = 0$

Preuve :

1) Soit $f \in K[X]$ alors $[\partial_i, x_j](f) = \partial_i(x_j.f) - x_j.(\partial_i(f))$
et $\partial_i(x_j.f) = \delta_{i,j}f - x_j\partial_i(f)$
2) Cela découle du fait général que pour $P, Q \in A_n, [P, Q] = -[Q, P]$.
3) Il suffit de remarquer les opérateurs x_i et x_j commutent. De même pour ∂_i et ∂_j.

Soit $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, on note $|\alpha|$ la longueur de α défini par $|\alpha| = |\alpha_1| + ... + |\alpha_1|$.
On note x^α le monôme $x_1^{\alpha_1}...x_n^{\alpha_n}$ et le degré de x^α est $|\alpha|$. On définit de la même façon ∂^β pour $\beta \in \mathbb{N}^n$.
Par définition, les éléments de A_n sont les combinaisons linéaires de monômes en $x_1, ..., x_n, \partial_1, ..., \partial_n$.
On va voir qu'on peut en fait regrouper ces monômes et les écrire sous une même forme.

Proposition : L'ensemble $B = \{x^\alpha \partial^\beta : \alpha, \beta \in \mathbb{N}^n\}$ est une base de A_n en tant que K espace vectoriel.

Pour $\alpha \in \mathbb{N}^n$ on définit $\alpha! := \alpha_1!...\alpha_n!$
Pour la preuve de cette proposition, on aura besoin du lemme suivant :

Lemme : Soit $\alpha, \beta \in \mathbb{N}^n$ tel que $|\alpha| \leq |\beta|$ alors $\partial^\beta(x^\alpha) = \beta!$ si $\alpha = \beta$ et 0 sinon.

Preuve du lemme : Il suffit d'utiliser la règle de Leibniz pour remarquer que :
$\partial^\beta(x^\alpha) = \partial_1^{\beta_1}...\partial_n^{\beta_n}(x_1^{\alpha_1}...x_n^{\alpha_n}) = \partial_1^{\beta_1}(x_1^{\alpha_1})...\partial_n^{\beta_n}(x_n^{\alpha_n}) = \beta_1!...\beta_n! = \beta!$ si $|\alpha| \leq |\beta|$ et $\alpha = \beta$ et 0 sinon.

Preuve de la proposition : Comme $\forall f \in K[X], \forall i, \ [\partial_i, f] = \partial_i.f - f.\partial_i = \dfrac{\partial f}{\partial x_i}$.
Cela nous permet de mettre les puissances des x_i à gauche des ∂_i. Ainsi, B génère $A_n(K)$
Il nous faut maintenant montrer que B est libre. Pour cela, soit $D = \sum c_{\alpha\beta} x^\alpha \partial^\beta$ une combinaison linéaire d'éléments de B. On va montrer que $D = 0$ implique que $c_{\alpha\beta} = 0$, $\forall \alpha, \beta$.
Par l'absurde s'il existe un coefficient $c_{\mu\sigma} \neq 0$ pour un certain couple de multi-indices (μ, σ) et en choisissant μ tel que pour tout β vérifiant $|\beta| < |\sigma|$ on ait $c_{\mu\beta} = 0$.
Alors, par le lemme précédent, $D(x^\sigma) = \sigma! \sum\limits_\alpha c_{\alpha\sigma} x^\alpha$.
Donc $D(x^\sigma) \neq 0$ car $c_{\mu\sigma} \neq 0$, et par conséquent $D \neq 0$.
Nous allons maintenant introduire le degré d'un élément de A_n.
Soit $D \in A_n$ alors d'après ce que nous venons de voir, D s'écrit de manière unique comme :
$D = \sum c_{\alpha\beta} x^\alpha \partial^\beta$.

Le degré de D, noté $deg(D)$, est par définition le multi-indices $(\alpha, \beta) \in \mathbb{N}^n \times \mathbb{N}^n$ de longueur maximal tel que $c_{\alpha\beta} \neq 0$

Ainsi, $deg(D) = 0$ implique que $D \in K$ et on convient que $deg(0) = -\infty$
Par exemple si $D = x_1^3 x_2^4 \partial_2 \partial_3^2 - x_1^2 x_3^2 \partial_1^3$ alors $deg(D) = 10$.

Proposition : Soit $D, D' \in A_n$, alors on a :

1)$deg(D + D') \leq max\{deg(D), deg(D')\}$

2)$deg(DD') = deg(D) + deg(D')$

3)$deg([D, D']) \leq deg(D) + deg(D') - 2$

Preuve : 1) Si D et D' sont écrits dans la base canonique B alors il en est de même pour $D + D'$ et la propriété découle directement.
Nous allons prouver 2) et 3) en même temps. On note e_i l'élément de $\mathbb{N}^n$ dont tous les termes sont nuls sauf le i-ème qui vaut 1.
On procède par récurrence sur $deg(D) + deg(D')$.
Si $deg(D) = 0$ ou $deg(D') = 0$ alors 2) et 3) sont vraies. On suppose par la suite que $deg(D), deg(D') \geq 1$ et que la propriété est vraie lorsque $deg(D) + deg(D') < k$
Par 1) et le fait que B est une base de A_n, il suffit de vérifier la propriété pour les monômes de la forme $x^\alpha \partial^\beta$.
Considérons d'abord $D = \partial^\beta$ et $D' = x^\alpha$, avec $|\alpha| + |\beta| = k$.
Comme $deg(D') = |\beta| \geq 1$, il existe un indice i tel que $\beta_i \neq 0$.
Or, $[\partial^\beta, x^\alpha] = \partial^\beta x^\alpha - x^\alpha \partial^\beta = \partial_i \partial^{\beta - e_i} x^\alpha - \partial_i x^\alpha \partial^{\beta - e_i} + \partial_i x^\alpha \partial^{\beta - e_i} - x^\alpha \partial_i \partial^{\beta - e_i} = \partial_i [\partial^{\beta - e_i}, x^\alpha] + [\partial_i, x^\alpha] \partial^{\beta - e_i}$.
Par notre hypothèse de récurrence, nous avons :
$deg([\partial^{\beta - e_i}, x^\alpha] \leq |\alpha| + |\beta| - 3$.
et $deg([\partial_i, x^\alpha]) \leq |\alpha| - 1$.
On a de plus par l'hypothèse de récurrence que :
$deg(\partial_i [\partial^{\beta - e_i}, x^\alpha]), deg([\partial_i, x^\alpha] \partial^{\beta - e_i}) \leq |\alpha| + |\beta| - 2$.
Or, $\partial^\beta x^\alpha = [\partial^\beta, x^\alpha] + x^\alpha \partial^\beta$.
Et $deg(x^\alpha \partial^\beta) = |\alpha| + |\beta|$ et $deg([\partial^\beta, x^\alpha]) \leq |\alpha| + |\beta| - 2$.
Par conséquent, $deg(\partial^\beta x^\alpha) = deg(x^\alpha x^\alpha) = |\alpha| + |\beta| - 2$.
On peut enfin considérer des éléments de B.
Soit $D = x^\sigma \partial^\beta$ et $D' = x^\alpha \partial^\eta$.
Si $|\alpha| = |\beta| = 0$ alors la propriété est évidente. Supposons donc que ce ne soit pas le cas.
Comme $\partial^\beta x^\alpha = x^\alpha \partial^\beta + P$. Avec $P = [\partial^\beta, x^\alpha]$ et $deg(P) \leq |\alpha| + |\beta| - 2$.
Nous avons, $DD' = x^\sigma \partial^\beta x^\alpha \partial^\eta = x^\sigma (x^\alpha \partial^\beta + P) \partial^\eta = x^{\sigma + \alpha} \partial^{\beta + \eta} + x^\sigma P \partial^\eta$.
Par hypothèse de récurrence,
$deg(x^\sigma P \partial^\eta) = deg(x^\sigma [\partial^\beta, x^\alpha] \partial^\eta) = deg(x^\sigma) + deg([\partial^\beta, x^\alpha]) + deg(\partial^\eta) \leq |\sigma| + \leq |\eta| + \leq |\beta| + \leq |\alpha| - 2$.
Donc $deg(x^\sigma P \partial^\eta) \leq deg(D) + deg(D') - 2$.
Ainsi, par la propriété 1), $deg(DD') = deg(x^{\alpha + \sigma} \partial^{\beta + \eta} = deg(D) + deg(D')$.
De plus nous avons vu que $DD' = x^{\alpha + \sigma} \partial^{\beta + \eta} + Q_1$, $D'D = x^{\alpha + \sigma} \partial^{\beta + \eta} + Q_2$.
Avec $Q_1, Q_2 \in A_n$ et $deg(Q_i) \leq deg(D) + deg(D') - 2$ pour $i = 1, 2$.
De ce fait,$[D, D'] = Q_1 - Q_2$ et en utilisant la propriété 1) nous avons :
$deg[D, D'] \leq deg(D) + deg(D') - 2$.
Ce qui complète la preuve.

Corollaire : L'anneau A_n est intègre.

Preuve : En effet, en utilisant la propriété 2), si $DD' = 0$ avec $D, D' \in A_n$. Alors, $deg(D) + deg(D') = -\infty$, donc $D = 0$ ou $D' = 0$.

Nous arrivons à la propriété cruciale de l'anneau A_n.

Définition : Un anneau A est dit simple si ses seuls idéaux bilatères sont $\{0\}$ et A.

Théorème : L'anneau A_n est simple.

Preuve : Soit I un idéal bilatère non nul de A_n. Soit $D \in I$, non nul et de degré minimal. Si $deg(D) = 0$ alors $D \in K$ et donc $I = A_n$.

Par l'absurde, si $deg(D) = k > 0$. On peut écrire D sous la forme,
$D = \sum c_{\alpha\beta} x^\alpha \partial^\beta$ avec $c_{\alpha\beta} \in K$.
Comme $deg(D) = k$, il existe un multi-indice (α, β) de longueur k tel que $c_{\alpha\beta} \neq 0$.
Soit β_i un indice non nul de β alors $[x_i, D]$ est non nul.
En effet, $[x_i, D] = x_i D - D x_i = \sum c_{\alpha\beta} x^{\alpha+e_i} \partial^\beta - \sum c_{\alpha\beta} x^\alpha \partial^\beta x_i$.
De plus, $\partial^\beta x_i = [\partial^\beta, x_i] + x_i \partial^\beta$.
Si bien que $[x_i, D] = \sum c_{\alpha\beta} x^\alpha [\partial^\beta, x_i]$.
Il nous suffit donc de monter que $[\partial^\beta, x_i] \neq 0$. Et cela se voit en appliquant $x^{\beta - e_i}$ à cet élément et en utilisant le lemme précédent pour trouver $\beta! \neq 0$.
Comme I est bilatère, $[x_i, D] \in I$ et $deg([x_i, D]) \leq k - 1$. Cela contredit notre hypothèse sur D. Donc $\beta = (0, ..., 0)$
Comme $k > 0$, il existe un indice $\alpha_i \neq 0$. Mais alors, par le même raisonnement, $[\partial_i, D]$ est un élément non nul de I et est de degré plus petit que $k-1$. Ce qui contredit encore une fois l'hypothèse sur D. Donc $I = \{0\}$.

Corollaire : Tout endomorphisme de la K algèbre $A_n(K)$ est injectif.

Preuve : En effet, si φ est un tel morphisme alors $Ker\varphi$ est un idéal bilatère de $A_n(K)$. Or en tant que morphisme d'anneaux, $\varphi(1) = 1$. Donc par le théorème précédent, $Ker\varphi = \{0\}$.
Par conséquent, φ est injectif.

Nous pouvons maintenant nous demander si tout endomorphisme de A_n est aussi surjectif et cela est précisément la conjecture de Dixmier.

Conjecture de Dixmier : Soit K un corps de caractéristique nulle et $A_n(K)$ son algèbre de Weyl.
Alors tout endomorphisme de $A_n(K)$ est surjectif (et donc tout endomorphisme est un automorphisme).

4 Algèbre de Poisson

Soit n un entier positif non nul et R un anneau commutatif. On notera dans cette partie $A = R^{[2n]}$ pour désigner $R[x_1, ..., x_{2n}]$. L'algèbre de Poisson $P_n(R)$ est l'anneau A muni du crochet de Poisson défini par :
$\forall f, g \in R^{[2n]}, \{f, g\} = \sum_{i=0}^{n} (\frac{\partial f}{\partial x_i} \frac{\partial g}{\partial x_{i+n}} - \frac{\partial f}{\partial x_{i+n}} \frac{\partial g}{\partial x_i})$.
Par la suite on notera $\partial_i f$ pour $\frac{\partial f}{\partial x_i}$.
Un endomorphisme ϕ de $P_n(R)$ est un R-endomorphisme de A tel que
$\forall f, g \in A, \{\phi(f), \phi(g)\} = \{f, g\}$.
Soit $(e) = (e_1, ..., e_{2n})$ la base canonique du A module libre $E := A^{2n}$ et $(e^*) = (e_1^*, ..., e_{2n}^*)$ la base duale de (e).
La forme forme symplectique canonique sur E est la forme bilinéaire $w := \sum_{i=0}^{n} e_i^* \wedge e_{i+n}^*$ où $e_i^* \wedge e_{i+n}^*$ est la forme 2-linéaire alternée sur E définie par $\forall p, q \in \mathbb{N}$, $1 \leq p < q \leq 2n$, $e_i^* \wedge e_{i+n}^*(e_p, e_q) = 1$ si $i = p$ et $i + n = q$ et 0 sinon.
Si L est un endomorphisme A linéaire de E alors on définit $L^* w := w \circ (L, L)$.
De plus, on dit que L est symplectique si $L^* w = w$.
Enfin, si on a une application polynômiale $F = (F_1, ..., F_{2n}) \in E$ alors on dit que F est symplectique si l'endomorphisme A linéaire de E définit par la matrice $(JF)^t$ est symplectique. (JF désigne la matrice jacobienne de F).

Théorème : On a une équivalence entre
i) F est symplectique.
ii) $F^* : A \longrightarrow A, p \longmapsto p(F)$ est un endomorphisme de $P_n(R)$.
De plus si une de ces conditions est vérifiée et que $n!$ est inversible dans R alors $det JF = 1$.

Pour montrer ce résultat, nous allons nous servir du lemme suivant :
Pour une forme bilinéaire B sur E on note $Mat(B)$ la matrice de B dans la base (e).

Lemme : Si $F = (F_1, ..., F_{2n}) \in E$ alors $Mat(((JF)^t)^* w) = (\{F_i, F_j\})_{1 \leq i,j \leq 2n}$

Preuve : Soit $1 \leq p, q \leq 2n$ et $L := (JF)^t$ alors $(L^* w)(e_p, e_q) = w(Le_p, Le_q)$.
Or $Le_p = \sum_{i=0}^{2n} \partial_i(F_p) e_i$.
Donc $(e_i^* \wedge e_{i+n}^*)(Le_p, Le_q) = (e_i^* \wedge e_{i+n}^*)(\partial_i(F_p) e_i, \partial_{i+n}(F_q) e_{i+n}) - (e_i^* \wedge e_{i+n}^*)(\partial_i(F_q) e_i, \partial_{i+n}(F_p) e_{i+n})$.
Ainsi, $(e_i^* \wedge e_{i+n}^*)(Le_p, Le_q) = \partial_i(F_p)\partial_{i+n}(F_q) - \partial_{i+n}(F_p)\partial_i(F_q)$.
Donc $Mat(((JF)^t)^* w) = (\{F_i, F_j\})_{1 \leq i,j \leq 2n}$

Corollaire : Soit $F = (F_1, ..., F_{2n}) \in E$, on a l'équivalence entre les assertions suivantes :
i) F est symplectique ($((JF)^t)^* w = w$)
ii) $\{F_i, F_j\} = \{x_i, x_j\}$ pour tout $1 \leq i, j \leq 2n$
iii) F^* est un endomorphisme de $P_n(R)$

Preuve : Si $F = (x_1, ..., x_{2n}) \in E$, alors $(JF)^t = I_{2n}$ et $(JF)^t)^* w = w$.
Donc d'après le lemme précédent,
$Mat((JF)^t)^* w) = (\{F_i, F_j\})_{1 \leq i,j \leq 2n} = (\{x_i, x_j\})_{1 \leq i,j \leq 2n} = Mat(w)$.
Ainsi, i) implique ii). De plus si on a ii) alors $Mat((JF)^t)^* w) = Mat(w)$ donc $(JF)^t)^* w = w$ et F est symplectique. Donc ii) implique i).
Montrons maintenant l'équivalence entre ii) et iii).
Si on a iii) alors $F^* : A \longrightarrow A, p \longmapsto p(F)$ est un endomorphisme de $P_n(R)$ et comme $F^*(x_i) = F_i$.
Donc $\{F^*(x_i), F^*(x_j)\} = \{F_i, F_j\} = \{x_i, x_j\}$ pour tout $1 \leq i, j \leq 2n$. Ainsi, ii) est vérifié.
Enfin, pour iii) implique ii). Il faut remarquer avec la formule :
$\{f, g\} = \sum_{i=0}^{n} (\frac{\partial f}{\partial x_i} \frac{\partial g}{\partial x_{i+n}} - \frac{\partial f}{\partial x_{i+n}} \frac{\partial g}{\partial x_i})$
que le crochet de poisson est bilinéaire, antisymétrique et vérifie la règle de Leibniz :
$\forall f, g, h \in A, \{fg, h\} = f\{g, h\} + g\{f, h\}$ (Cela se voit en utilisant le fait que les ∂_i vérifient cette règle).

Preuve du théorème : L'équivalence entre i) et ii) a été prouvée dans le corollaire précédent.

Supposons donc que F est symplectique et que $n!$ est inversible dans R pour montrer que $detJF = 1$.
Notons L l'application A -linéaire de $E := A^{2n}$ défini par la matrice $(JF)^t$.
Soit $v := e_1^* \wedge ... \wedge e_{2n}^*$la forme volume canonique sur E. Alors $w^n = n!(-1)^{\frac{n(n-1)}{2}}v$.
Comme $n!$ est inversible, w^n est une forme volume sur E, et F étant symplectique,ie $L^*w = w$, on a : $L^*(w^n) = (L^*(w))^n = w^n$.
Mais comme w^n est une forme volume sur E, on a aussi $L^*(w^n) = (detL)w^n$. Or $v(e_1, ..., e_{2n}) = 1$ et $n!$ est inversible donc $det(L) = 1$. De plus, $det(L) = det(JF)^t = det(JF)$.
Ainsi $det(JF) = 1$.

5 Équivalence des conjectures

Dans cette partie, nous allons démontrer l'équivalence sur $\mathbb{C}$ entre la conjecture Jacobienne, la conjecture de Dixmier et la conjecture de Poisson.
On rappelle d'abord les trois conjectures :

Conjecture Jacobienne : Pour tout entier $n \geq 1$, l'assertion suivante est vraie $JC(n, \mathbb{C})$: si $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ est une application polynomiale et $detJF \in \mathbb{C}^*$ alors F admet un inverse polynomiale.

Conjecture de Dixmier : Pour tout entier $n \geq 1$, l'assertion suivante est vraie $DC(n, \mathbb{C})$: Tout $\mathbb{C}$- endomorphisme de $A_n(\mathbb{C})$ est surjectif et est donc un $\mathbb{C}$- automorphisme.

Conjecture de Poisson : Pour tout corps K de caractéristique nulle et pour tout entier $n \geq 1$, l'assertion suivante est vraie $PC(n, K)$: Tout endomorphisme de $P_n(K)$ est un automorphisme.

Avec ces notations, nous allons montrer :
$\forall n \geq 1, JC(n, \mathbb{C}) \iff \forall n \geq 1, DC(n, \mathbb{C}) \iff \forall n \geq 1, PC(n, \mathbb{C})$

Montrons d'abord que la conjecture de Dixmier implique la conjecture Jacobienne.

Proposition : Pour tout entier $n \geq 1, DC(n, \mathbb{C})$ implique $JC(n\mathbb{C}$.

Preuve : Soit $F = (F_1, ..., F_n) : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ une application polynomiale avec $detJF \in \mathbb{C}^*$.
Posons,

$$\begin{pmatrix} \dfrac{\partial}{\partial F_1} \\ \vdots \\ \dfrac{\partial}{\partial F_n} \end{pmatrix} = ((JF)^{-1})^t \begin{pmatrix} \partial_1 \\ \vdots \\ \partial_n \end{pmatrix}. \tag{1}$$

Comme $A_n(\mathbb{C})$ est un anneau, les $\dfrac{\partial}{\partial F_i}$ sont des dérivations sur $\mathbb{C}[x]$ et vérifient de plus les propriétés suivantes :

i)$\dfrac{\partial}{\partial F_i}(F_j) = \delta_{i,j}, \forall i, j$
ii)$\dfrac{\partial}{\partial F_1}, ..., \dfrac{\partial}{\partial F_n}$ est une base du $\mathbb{C}[X]$ module $Der_{\mathbb{C}}\mathbb{C}[X]$.
iii)$[\dfrac{\partial}{\partial F_i}, \dfrac{\partial}{\partial F_j}] = 0, \forall i, j,$

Pour le i), si l'on applique F_i dans l'équation (1) et que nous transposons, nous obtenons :
$(\dfrac{\partial F_i}{\partial F_1}, ...\dfrac{\partial F_i}{\partial F_n}) = (\dfrac{\partial F_i}{\partial x_1}, ...\dfrac{\partial F_i}{\partial x_n})(JF)^{-1}$.
Or,$(\dfrac{\partial F_i}{\partial x_1}, ...\dfrac{\partial F_i}{\partial x_n})$ est la i-ième colonne de JF donc le deuxième membre de l'équation ci-dessus est la i-ième colonne de $JF.JF^{-1} = I_n$.
Le ii) vient du fait que $((JF) \in GL_n(\mathbb{C}[X])$, donc $((JF)^{-1})^t$ aussi. Ainsi, $((JF)^{-1})^t$ transforme une base du $\mathbb{C}[X]$ module $Der_{\mathbb{C}}\mathbb{C}[X]$ en une autre base.
Pour le iii), si l'on pose $D = [\dfrac{\partial}{\partial F_i}, \dfrac{\partial}{\partial F_j}]$ alors d'après le ii), $D = \sum_k a_k \dfrac{\partial}{\partial F_k}$ avec $a_k \in \mathbb{C}[X]$.
Et en utilisant i), $D(F_l) = a_l = 0, \forall l$. Donc $a_k = 0, \forall k$ et donc $D = 0$.
De plus, $\forall i, j$, $[\dfrac{\partial}{\partial F_i}, F_j] = \delta_{i,j}$.
En effet, si l'on pose $D = [\dfrac{\partial}{\partial F_i}, F_j] = \dfrac{\partial}{\partial F_i}F_j - F_j\dfrac{\partial}{\partial F_i}$.
Donc $\forall P \in \mathbb{C}[x], D(P) = \dfrac{\partial}{\partial F_i}(F_j.P) - F_j\dfrac{\partial}{\partial F_i}(P) = F_j\dfrac{\partial}{\partial F_i}(P) + P\dfrac{\partial}{\partial F_i}(F_j) - F_j\dfrac{\partial}{\partial F_i}(P)$.
Donc $\forall P \in \mathbb{C}[x], D(P) = \delta_{i,j}P$, d'où le résultat.

Ainsi, si on définit $\varphi : A_n(\mathbb{C}) \longrightarrow A_n(\mathbb{C})$, par$\varphi(x_i) = F_i$ et $\varphi(\partial_i) = \dfrac{\partial}{\partial F_i}$ alors φ est un endomorphisme de $A_n(\mathbb{C})$.
Comme nous avons supposé $DC(n, \mathbb{C})$, φ est surjective et donc $\mathbb{C}[F_1, ..., F_n, \dfrac{\partial}{\partial F_1}, ..., \dfrac{\partial}{\partial F_1}] = A_n(\mathbb{C})$
En particulier, si $g \in \mathbb{C}[x]$ alors on peut voir g comme un élément de $A_n(\mathbb{C})$ et donc on peut écrire g sous la forme : $g = \sum_\alpha a_\alpha(F)(\dfrac{\partial}{\partial F})^\alpha$ avec $a_\alpha(F) \in \mathbb{C}[F] := \mathbb{C}[F_1, ..., F_n]$.
Alors en appliquant g à 1 on obtient $g.1 = a_0(F) = g$. Donc $g \in \mathbb{C}[F]$. On a donc montré que $\mathbb{C}[x] \subseteq \mathbb{C}[F]$.
Et on a clairement l'inclusion $\mathbb{C}[F] \subseteq \mathbb{C}[x]$.
Or l'assertion : Pour toute application polynomiale $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$,tel que $detJF \in \mathbb{C}^*$ alors $\mathbb{C}[x] = \mathbb{C}[F]$ est équivalente à $JC(n, \mathbb{C})$.
On rappelle le théorème énoncé dans la partie sur l'algèbre de Poisson en le voyant maintenant sur $\mathbb{C}$.

Théorème P : Si φ est un endomorphisme de $P_n(\mathbb{C})$ alors $detJ\varphi_* = 1$.

Ce théorème nous donne directement

Corollaire : Pour tout entier naturel $n \geq 1$, $JC(2n, \mathbb{C})$ implique $PC(n, \mathbb{C})$.

Preuve : En effet, si φ est un endomorphisme de $P_n(C)$, alors φ_* est une application polynomiale (symplectique) de $\mathbb{C}^{2n}$.
Comme nous supposons $JC(2n, \mathbb{C})$ et que nous avons $detJ\varphi_* = 1$, φ_* admet un inverse polynomiale. Donc le morphisme φ est aussi inversible. Ce qui signifie qu'il existe un endomorphisme ψ de $\mathbb{C}^{[2n]}$ tel que $\psi \circ \varphi = (x_1, ..., x_{2n}$.
Par conséquent, $\{\psi \circ \varphi(f), \psi \circ \varphi(g)\} = \{f, g\} = \{\psi(f), \psi(g)\}$.
De ce fait, ψ est un endomorphisme de $P_n(\mathbb{C})$, inverse de ψ. Donc tout endomorphisme de $P_n(\mathbb{C})$ est un automorphisme.

Il nous reste donc plus qu'à montrer que $PC(n, \mathbb{C})$ implique $DC(n, \mathbb{C})$.
L'idée pour montrer cette implication est de remplacer $\mathbb{C}$ par un anneau R/pR avec R un sous anneau de $\mathbb{C}$ et p un nombre premier.
Dans cette partie, nous allons regarder $A_n(\mathbb{C})$ comme la $\mathbb{C}$ algèbre avec $2n$ générateurs $y_1, ..., y_{2n}$ et les relations $[y_i, y_{i+n}] = 1$ pour tout $1 \leq i \leq n$ et $[y_i, y_j] = 0$ sinon. Pour ce passer de montrer que cela caractérise bien $A_n(\mathbb{C}$, on peut supposer que pour tout $1 \leq i \leq n$, $y_i = x_i$ (multiplication par x_i) et $y_{i+n} = \partial_i$.
Soit φ un $\mathbb{C}$-endomorphisme de $A_n(\mathbb{C})$ alors en tant que morphisme d'algèbre, φ est entièrement déterminé par l'image des $\varphi(y_i)$.
On définit le degré de φ par le maximum des degrés des $\varphi(y_i)$.
On remarque que cette définition est cohérente avec la définition du degré d'une application polynomiale car si l'on considère φ_*, qui est une application polynomiale sur $\mathbb{C}^{2n}$ alors ses composantes sont les $\varphi(y_i)$.
En outre, φ est surjective si et seulement si il existe $\psi_1, ..., \psi_{2n} \in A_n(\mathbb{C})$ tel que pour tout i, $\varphi(\psi_i) = y_i$. Si tel est le cas et que les ψ_i sont tous de degré $\leq N$ alors on dit que φ est N-surjective.

En supposant $PC(n, \mathbb{C})$ on va montrer un résultat plus fort que $DC(n, \mathbb{C}$:
Pour tout entier $d \geq 1$, tout $\mathbb{C}$-endomorphisme de $A_n(\mathbb{C})$ est D-surjectif, avec $D = d^{2n-1}$.
Par l'absurde, si φ est un $\mathbb{C}$-endomorphisme de $A_n(\mathbb{C}$ de degré d mais qui n'est pas D-surjectif.
Alors il n'existe pas $\psi_1, ..., \psi_{2n} \in A_n(\mathbb{C})$ de degré $\leq D$ tel que pour tout i, $\varphi(\psi_i) - y_i = 0$.
Considérons les éléments universels de $A_n(\mathbb{C})$ de degré $\leq D$, c'est-à-dire les éléments :
$\psi_i^U = \sum_{|\alpha| \leq D} c_\alpha^{(i)} y^\alpha$, où les $c_\alpha^{(i)}$ sont des variables distinctes.
Ainsi, $\varphi(\psi_i^U) - y_i = \sum_{|\alpha| \leq D} c_\alpha^{(i)} \varphi(y_1)^{\alpha_1} ... \varphi(y_{2n})^{\alpha_{2n}} - y_i$.
Soit C l'ensemble des $c_\alpha^{(i)}$ (C est un ensemble fini) et $P_1(C), ..., P_s(C) \in \mathbb{C}[C]$ les coefficients des monômes y^α apparaissant dans les expressions des $\varphi(\psi_i^U) - y_i$.
Alors les $P_i(C)$ n'ont pas de zéros communs dans $\mathbb{C}^C$ (sinon φ serait D-surjective). Donc par le nullstellensatz, il existe $Q_1(C), ..., Q_s(C) \in \mathbb{C}[C]$ tel que :
$1 = \sum Q_j(C) P_j(C)$ (2).

Corollaire (1) : Soit φ un $\mathbb{C}$-endomorphisme de $A_n(\mathbb{C})$ de degré d, non D-surjectif. R un sous anneau de $\mathbb{C}$ contenant les coefficients des monômes y^α apparaissant dans les $\varphi(y_i)$ et tous les coefficients des P_j et Q_j.
Si $\mathfrak{a}$ est un idéal de propre de R ($\mathfrak{a} \neq R$) et $\bar{\varphi}$ est l'endomorphisme induit par φ sur $A_n(R/\mathfrak{a})$. Alors $\bar{\varphi}$ n'est pas D-surjectif.

Preuve : Il suffit de réduire l'équation (1) modulo $\mathfrak{a}$ ($1 \notin \mathfrak{a}$) et d'utiliser le fait que $\{y^\alpha | \alpha \in \mathbb{N}^{2n}\}$ est une base de $A_n(\mathbb{C})$ car on a vu dans la partie sur l'algèbre de Weyl que $\{x^\alpha \partial^\beta | \alpha, \beta \in \mathbb{N}^n\}$ en est une. Donc on a précisément que φ est D-surjectif si et seulement si les $P_j(C)$ n'ont pas de zéros communs.

On va réécrire l'hypothèse$PC(n, \mathbb{C})$ en termes d'équation polynomiales.
Pour cela, on considère pour tout entier $d \geq 1$, l'assertion $P(n, \mathbb{C}, d)$ signifiant que la conjecture de Poisson est vraie pour tout endomorphisme de $P_n(\mathbb{C}$ de degré $\leq d$.
Du fait de la correspondance entre les endomorphismes de la $\mathbb{C}$-algèbre $C[x]^{[2n}$ et les applications polynomiales sur $\mathbb{C}^{2n}$, en terme polynomiale cette assertion signifie que pour tout application polynomiale $F := (F_1, ..., F_{2n}$ de $\mathbb{C}^{2n}$ de degré $\leq d$, ie $\forall i$, $deg(F_i) \leq d$, et vérifiant $\{F_i, F_j\} = \{x_i, x_j\}$ pour tout $1 \leq i, j \leq 2n$. Alors F a un inverse polynomiale de degré $\leq d^{2n-1}$ par la propriété (D).
Encore une fois, on va considérer des éléments universels en ajoutant de nouvelles variables puis utiliser le Nullstellensatz pour obtenir des informations sur un tel F.
Ainsi, soit $F^U := (F_1^U, ..., F_{2n}^U)$ l'application polynomiale universelle de degré d en $2n$ variables $(x_1, ..., x_{2n})$ avec
$F_i^U = \sum_{|\alpha| \leq d} A_\alpha^{(i)} x^\alpha$, où les $A_\alpha^{(i)}$ sont des variables distinctes.
Soit A l'ensemble des $A_\alpha^{(i)}$ (A est fini) et $\mathbb{C}[A]$ l'algèbre des polynômes engendrée par A sur $\mathbb{C}$.
Enfin, pour tout $1 \leq i, j \leq 2n$, on définit $P_{ij} = \{F_i^U, F_j^U\} - \{x_i, x_j\}$.
Soit $g_1(A), ..., g_r(A)$ les coefficients des monômes en x^α apparaissant dans les expressions des P_{ij} et $J := (g_1(A), ..., g_r(A))$, l'idéal de $\mathbb{C}[A]$ engendré par ces éléments.
Par définition de J, l'image de F^U par la projection canonique dans $L := (\mathbb{C}[A])[x]^{[2n]}$, est une application polynomiale symplectique de L. Donc son jacobien est 1.
Par le théorème (FI), F^U a un inverse formel dans $\mathbb{C}[A][[x]]^{[2n]}$.
Soit $G(A)$ un un représentant de cet inverse dans $\mathbb{C}[A][x]^{[2n]}$ et I l'idéal de $\mathbb{C}[A]$ généré par les coefficients de x^α avec $|\alpha| > D := d^{2n-1}$ de $G(A)$.
Comme $\mathbb{C}[A][x]^{[2n]}$ est noethérien (car $\mathbb{C}[A]$ l'est), on peut trouver $h_1(A), ..., h_t(A) \in \mathbb{C}[A][x]^{[2n]}$ tel que $I = (h_1(A), ..., h_t(A))$.

Proposition (2) Si $P(n, \mathbb{C}, d)$ est vraie alors il existe des $b_j^{(i)} \in \mathbb{C}[A]$ et un entier $k \geq 1$ tel que
$\forall 1 \leq i \leq t, h_i(A) = \sum_j b_j^{(i)}(A) g_j(A) \qquad (3).$
Preuve : Soit $a \in \mathbb{C}^A$ un zéro de J.Comme $F^U(A = a)$ est de degré $\leq d$ et $detJF^U(A = a) = 1$, par hypothèse,$F^U(A = a)$ est inversible, d'inverse $G(A = a)$.
D'après la propriété(D), $degG(A = a) \leq D$.
Par notre construction de I, cela implique que a est un zéro de I.
Donc { zéros de J} $\subseteq$ { zéros de I}.
Et par le Nullstellensatz, on a $\sqrt{I} \subseteq \sqrt{J}$. Or, $I \subseteq \sqrt{I}$. Donc $I \subseteq \sqrt{J}$, ce qui nous donne le résultat.
On en déduit le fait suivant :

Corollaire (3) Soit R un sous-anneau de $\mathbb{C}$ contenant les coefficients des polynômes $h_i(A), b_j^{(i)}(A)$ et $g_j(A)$.
Si $\mathfrak{a}$ est un idéal propre de R et f un endomorphisme de $P_n(R/\mathfrak{a})$ de degré $\leq d$. Alors, f a un inverse de degré $\leq D := d^{2n-1}$.

Nous pouvons maintenant prouver que $P(n, \mathbb{C}, d)$ implique $D(n, \mathbb{C}, d)$.
Pour cela, supposons $P(n, \mathbb{C}, d)$ et prenons φ un $\mathbb{C}$-endomorphisme de $A_n(\mathbb{C})$ de degré $\leq d$. On suppose que φ est n'est pas surjectif.
Par ce que nous venons de voir, nous avons les équations :
$1 = \sum Q_j(C) P_j(C) \qquad (2).$
$\forall 1 \leq i \leq t, h_i(A) = \sum_j b_j^{(i)}(A) g_j(A) \qquad (3).$

Soit R la $\mathbb{Z}$ sous algèbre de $\mathbb{C}$ engendré par $\dfrac{1}{n!}$ et tous les coefficients des monômes y^α apparaissant dans les $h_i(A), g_j(A), b_j^{(i)}(A), Q_j(C)$ et $P_j(C)$.
Alors, φ est un R endomorphisme de $A_n(R)$ et R est une $\mathbb{Z}$ algèbre de type fini sans $\mathbb{Z}$-torsion (car $R \subseteq \mathbb{C}$).
Ainsi, par le théorème(D), il existe un nombre premier p non inversible dans R.
En réduisant modulo pR, on obtient un R/pR endomorphisme $\bar{\varphi}$ de $A_n(R/pR)$ or par le corollaire (1), $\bar{\varphi}$ n'est pas D-surjective.
Mais nous allons voir maintenant que si $P(n, \mathbb{C}, d)$ est vraie alors $\bar{\varphi}$ est D-surjective.
Pour cela, nous avons besoin des deux théorèmes suivants, que l'on énonce avec les notations adoptées ci-dessus.

Théorème 1 : Le centre de $A_n(R/pR)$, noté Z, est un anneau polynomial en les variables $y_1^p, ..., y_{2n}^p$ sur R/pR.
De plus, nous avons :
i) $\bar{\varphi}(Z) \subseteq Z$, donc $\bar{\varphi}(Z)$ induit une application polynomiale de $R/pR[y_1^p, ..., y_{2n}^p]$ dans lui-même, que l'on note $\bar{\varphi}_{pol}$.
ii)Si $\bar{\varphi}_{pol}$ est surjective alors $\bar{\varphi}$ est surjective. Plus précisément, si $\bar{\varphi}_{pol}$ est N-surjective, pour un certain entier $N \geq 1$, alors $\bar{\varphi}$ est aussi N-surjective.

Théorème 2 : $\bar{\varphi}_{pol}$ est un endomorphisme de $P_n(R/pR)$ de degré $\leq d$.

Avec ces théorèmes, prouvons la surjectivité de $\bar{\varphi}$.
Par le théorème 2, $\bar{\varphi}_{pol}$ est un endomorphisme de $P_n(R/pR)$ de degré $\leq d$.
Donc d'après le théorème(P), l'hypothèse sur $P(n, \mathbb{C}, d)$ et en réduisant l'équation (3) modulo pR alors $\bar{\varphi}_{pol}$ a un inverse de degré $\leq D := d^{2n-1}$.
Donc $\bar{\varphi}_{pol}$ est D-surjective et donc d'après le point ii) du théorème 1, $\bar{\varphi}$ est D-surjective.
Ce qui achève de montrer que $P(n, \mathbb{C}, d)$ implique $D(n, \mathbb{C}, d)$.
Ainsi, pour tout $n \geq 1$, $PC(n, \mathbb{C}) \Rightarrow DC(n, \mathbb{C})$.
Et par conséquent, les trois conjectures sont équivalentes.

6 Annexes

6.1 Annexe 1 : Le Nullstellensatz

Dans la suite, nous aurons besoin de deux versions du théorème des zéros de Hilbert, aussi appelé Nullstellensatz, qui permet dans sa version faible, de décrire les idéaux maximaux de l'anneau $K[X_1, ..., X_n]$ lorsque K est un corps algébriquement clos.
Nous commençons par rappeler un fait essentiel sur les idéaux de la forme $(X_1 - a_1, ..., X_n - a_n)$ avec $(a_1, ..., a_n) \in K^n$.

Proposition : Soit $(a_1, ..., a_n) \in K^n$ alors l'idéal $(X_1 - a_1, ..., X_n - a_n)$ est maximal dans $K[X_1, ..., X_n]$

Démonstration : Considérons le morphisme d'anneaux $\varphi : K[X_1, ..., X_n] \longrightarrow K$ défini par $\varphi(X_i) = a_i$.
On voit directement que φ est surjectif et que l'idéal $I = (X_1 - a_1, ..., X_n - a_n) \subseteq ker\varphi$.
Montrons maintenant l'autre inclusion.
Soit $P \in ker\varphi$ alors en effectuant la division euclidienne de P par $X - 1 - a_1$ on obtient :
$P = (X_1 - a_1)Q_1 + R_1$ avec $deg_{X_1} R_1 < 1$. En effectuant la division euclidienne de R_1 par $X_2 - a_2$ on trouve :
$P = (X_1 - a_1)Q_1 + (X_2 - a_2)Q_2 + R_2$ avec $deg_{X_1} R_2 < 1$ et $deg_{X_2} R_2 < 1$.
En itérant ce procédé on obtient :
$P = (X_1 - a_1)Q_1 + ... + (X_n - a_n)Q_n + R_n$ avec $R_n \in K$
Or $P(a_1, ..., a_n) = 0$ donc $R_n = 0$.
Ainsi $P \in I$ donc $\ker \varphi = I$.
Et $K[X_1, ..., X_n]/I \cong \mathbb{K}$.
Donc I est un idéal maximal de $K[X_1, ..., X_n]$.
Nous allons maintenant montrer un lemme qui nous donnera le résultat voulu.

Lemme de Zariski : Soit $K \subseteq F$ une extension de corps avec K non dénombrable. Si F est une K algèbre de type fini alors l'extension $K \subseteq F$ est finie

Démonstration : D'après l'hypothèse sur F, F est finiment engendrée en tant qu'extension de corps. On doit prouver que l'extension $K \subseteq F$ est finie ou de manière équivalente d'après ce que l'on vient de dire que l'extension $K \subseteq F$ est algébrique.
Soit $a \in F$ - K et montrons que a est algébrique sur K. Comme F est une K algèbre de type fini, F est le quotient de $K[X_1, ...X_n]$ par un idéal de $K[X_1, ...X_n]$. On a donc un morphisme d'anneaux surjectif de $K[X_1, ...X_n]$ dans F.
De plus, comme $K[X_1, ...X_n]$ admet une base dénombrable en tant que K espace vectoriel, il en est de même pour F.
Considérons $\{\dfrac{1}{a-c}\}_{c \in K}$, cette partie est non dénombrable dans F et est donc linéairement indépendante. Il existe donc $c_1, ..., c_m \in K$ et des coefficients non nuls $\lambda_1, ..., \lambda_m \in K$ tel que :
$\frac{\lambda_1}{a-c_1} + ... + \frac{\lambda_m}{a-c_m} = 0$
On peut exprimer le membre de gauche en mettant les fractions sur le même dénominateur pour obtenir :
$\frac{P(a)}{Q(a)} = 0$ avec $P, Q \in K[X]$ et $P \neq 0$ et $Q(a) \neq 0$
Ainsi, $P(a) = 0$ et donc a est algébrique sur K.
On peut maintenant montrer le résultat qui nous intéresse :

Nullstellensatz (version faible) : Soit K un corps algébriquement clos et I un idéal de $K[X_1, ..., X_n]$. Alors I est maximal si et seulement si il existe $c_1, ..., c_n \in K$ tel que $I = (X_1 - c_1, ..., X_n - c_n)$.

Démonstration : Nous avons déjà vu que les idéaux de la forme $(X_1 - c_1, ..., X_n - c_n)$ sont maximaux dans $K[X_1, ..., X_n]$.
Réciproquement, soit M un idéal maximal de $K[X_1, ..., X_n]$. Alors $L = K[X_1, ..., X_n]/M$ est une extension de corps de K.
Or L est une K algèbre de type fini. Donc d'après le Lemme de Zariski, $K \subseteq L$ est une extension algébrique.
Mais comme K est algébriquement clos, $K = L$.
On a donc un morphisme d'anneaux surjectif $\varphi : K[X_1, ..., X_n] \longrightarrow K$ ayant pour noyau M.
Soit $c_i = \varphi(X_i)$ alors $(X_1 - c_1, ..., X_n - c_n) \subseteq ker\varphi = M$.
Mais $(X_1 - c_1, ..., X_n - c_n)$ est maximal donc $M = (X_1 - c_1, ..., X_n - c_n)$.
On en tire facilement un corollaire qui nous servira plusieurs fois par la suite :

Corollaire : Soit $P_1, ..., P_m \in \mathbb{C}[X_1, ..., X_n]$ n'ayant pas de zéros communs dans $\mathbb{C}^n$. Alors il existe $Q_1, ..., Q_m \in \mathbb{C}[X_1, ..., X_n]$ tel que $1 = P_1Q_1 + ... + P_mQ_m$.

Démonstration : Soit $I = (P_1, ..., P_m)$ alors si $I \neq \mathbb{C}[X_1, ..., X_n]$ le théorème de Krull affirme qu'il existe un idéal maximal $M \subseteq \mathbb{C}[X_1, ..., X_n]$ tel que $I \subseteq M$.
Mais d'après le théorème précédent, il existe $c_1, ..., c_n \in \mathbb{C}$ tel que $M = (X_1 - c_1, ..., X_n - c_n)$. Mais alors, $(c_1, ..., c_n)$ est un zéro commun de $P_1, ..., P_m$, d'où une contradiction.
Ainsi, $I = \mathbb{C}[X_1, ..., X_n]$, $1 \in I$ et donc il existe $Q_1, ..., Q_m$ tel que $1 = P_1Q_1 + ... + P_mQ_m$.
Nous pouvons maintenant démontrer la version forte du Nullstellensatz. Pour cela, nous allons avoir besoin de quelques définitions.

Définition : Soit A un anneau commutatif et I un idéal de A. Alors le radical de I est défini par :
$\sqrt{I} = \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$.

Proposition : Avec ces notations, $\sqrt{I}$ est un idéal de A.

Preuve : Rappelons que le nilradical de A : $nil(A) = \{a \in A | \exists n \in \mathbb{N}^*, a^n = 0\}$ est un idéal de A.
Ainsi, si π est la projection canonique de A sur A/I, alors $\sqrt{I} = \pi^{-1}(nil(A/I))$.
Donc $\sqrt{I}$ est bien un idéal de A.

On observe facilement que $I \subseteq \sqrt{I}$.
Retournons dans le corps algébriquement clos K et notons $A := K[X_1, ...X_n]$.

Définition : Soit S une partie de A on définit son ensemble de zéros par $Z(S) := \{x \in K^n | \forall f \in S, f(x) = 0\}$.

Définition : Si M est une partie de K^n on définit $I(M) := \{f \in A | \forall x \in M, f(x) = 0\}$.

On observe que $I(M)$ est un idéal de A.
On peut enfin énoncer la version forte du Nullstellensatz :

Théorème : Soit $\mathfrak{a}$ un idéal de A, alors $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Preuve : Soit $f \in I(V(\mathfrak{a}))$, et rajoutons une variable à A en définissant $R := A[T]$.
Soit $\mathfrak{b} := (\mathfrak{a}, 1 - Tf)$, l'idéal de R engendré par $\mathfrak{a}$ et l'élément $1 - Tf$.
Alors $V(\mathfrak{b}) = \emptyset$. Donc d'après le Nullstellensatz faible, $\mathfrak{b} = R$ car sinon $\mathfrak{b}$ serait inclus dans un idéal maximal de R et d'après la forme des idéaux maximaux de R on aurait au moins un zéro de $\mathfrak{b}$.
Donc $1 \in \mathfrak{b}$ et on peut donc trouver une équation de la forme :
$\sum_i h_i f_i + h(1 - Tf) = 1 \qquad (*)$
Avec des éléments $f_i \in \mathfrak{a}$ et $h_i, h \in R$.
En substituant T par $\frac{1}{f}$ dans (*) on obtient :
$\sum_i h_i(X_1, ..., X_n, \frac{1}{f}) f_i = 1$
Enfin, en multipliant par une puissance adéquate de f on trouve :
$\sum_i \tilde{h_i} f_i = f^m$, avec $\tilde{h_i} = f^m.h_i$.
Ce qui est bien le résultat voulu.

6.2 Annexe 2 : Dérivation sur un Anneau

Dans cette partie, A désigne un anneau et R un anneau commutatif. Une dérivation sur A est une application $D \longrightarrow A$ telle que D est additive :$\forall a, b \in A, D(a+b) = D(a) + D(b)$
D vérifie la règle de Leibniz : $\forall a, b \in A, D(ab) = aD(b) + bD(a)$
On notera $DerA$ l'ensemble des dérivations sur A.
Si A est une R-algèbre, une R- dérivation sur A est une dérivation D sur A telle que D soit nulle sur R
Soit $a \in A$ et $r \in R$ alors $D(ra) = rD(a) + aD(r) = rD(a)$ car $D(r) = 0$
Ainsi, une R-dérivation est une application R-linéaire sur A.
L'ensemble des R dérivations sur A sera noté $Der_R A$.
Si D et D' sont deux dérivations sur A, on définit le crochet de Lie de D et D' par
$[D, D'] = D \circ D' - D' \circ D$ On vérifie facilement que $[D, D']$ est une dérivation sur A et que si D et D' sont des R-dérivations sur A alors il en est de même pour $[D, D']$.
De plus, du fait de la règle de Leibniz et du fait qu'une R-dérivation soit R-linéaire, une R-dérivation est entièrement déterminée par ses valeurs sur une partie génératrice de A (en tant que R-algèbre).

Proposition : Soit $R[X] = R[X_1, ..., X_n]$ alors
a) $Der_R R[X]$ est un module libre sur $R[X]$ de base $(\partial_1, ..., \partial_n)$ avec ∂_i la dérivation par rapport à X_i.
b) $[\partial_i, \partial_j] = 0 \forall i, j$

Preuve : a)Il est facile de voir que $Der_R R[X]$ est un module sur $R[X]$ (car $R[X]$ est commutatif).
De plus, rappelons que la R-algèbre $R[X]$ est engendrée par $X_1, ..., X_n$.
Soit $D \in Der_R R[X]$ et notons $D' = D - \sum D(X_i)\partial_i$, alors $\forall i$, $D'(X_i) = 0$ donc $D' = 0$ et $D = \sum D(X_i)\partial_i$.
En outre, si $D = \sum a_i \partial_i = 0$ avec $ai \in R[X]$ alors $D(X_i) = a_i = 0 \forall i$ donc $Der_R R[X]$ est bien un module libre sur $R[X]$ de base $(\partial_1, ..., \partial_n)$.
b)De la même façon si $D = [\partial_i, \partial_j]$, on voit que $\forall k, D(X_k) = 0$. Donc $[\partial_i, \partial_j] = 0$

6.3 Annexe 3 : Formes alternées

Soit A un anneau et $E = A^{2n}$ le A-module de base canonique $(e) := (e_1, ..., e_{2n})$. Et $(e^*) := (e_1^*, ..., e_{2n}^*)$ la base duale de (e).

Pour tout $1 \leq i, j\ 2n$ et $i \neq j$, on définit la 2-forme alternée $e_i^* \wedge e_j^*$ comme l'unique 2-forme alternée vérifiant :
$(e_i^* \wedge e_j^*)(e_i, e_j) = 1$
$(e_i^* \wedge e_j^*)(e_j, e_i) = -1$
$(e_i^* \wedge e_j^*)(e_k, e_l) = 0$, pour tout $k, l \in \{1, , , 2n\} \setminus \{i, j\}$

On voit donc que $(e_i^* \wedge e_j^*) = -(e_j^* \wedge e_i^*)$.
De plus pour que notre définition soit cohérente, $e_i^* \wedge e_i^* = 0$.
Si i, j, k, l sont des indices distincts, on définit le produit extérieur (encore noté $\wedge$) de deux 2-forme alternées par :
$(e_i^* \wedge e_j^*) \wedge (e_k^* \wedge e_l^*) := e_i^* \wedge e_j^* \wedge e_k^* \wedge e_l^*$
la 4-forme linéaire alternée valant 1 en (e_i, e_j, e_k, e_l).

Encore une fois, $e_i^* \wedge e_j^* \wedge e_k^* \wedge e_l^* = 0$, si deux indices sont les mêmes.

On procède de la même manière pour le produit de deux formes alternées quelconques et on admettra que ce produit extérieur est associatif.

Si $v = e_i^*, v' = e_j^*, w = e_k^*, w' = e_l^*$ alors $v \wedge v' \wedge w \wedge w' = w \wedge w' \wedge v \wedge v'$
En effet en utilisant l'associativité et le fait que $v \wedge v' = -v' \wedge v$, on a :
$v \wedge v' \wedge w \wedge w' = -v \wedge w \wedge v' \wedge w'$
$= w \wedge v \wedge v' \wedge w'$
$= -w \wedge v \wedge w' \wedge v'$
$= w \wedge w' \wedge v \wedge v'$

On sait qu'il existe une unique 2n-forme alternée sur E à multiplication par une constante près. Une 2n-forme alternée non nulle sur E est appelée forme volume.
La forme volume canonique est $v := e_1^* \wedge ... \wedge e_{2n}^*$, $v(e_1, ...e_{2n}) = 1$.
De plus, si f est un endomorphisme de E, on définit le determinant de f par :
$det(f) := v(f(e_1), ..., f(e_{2n})$.

Soit $w := \sum_{i=0}^{n} e_i^* \wedge e_{i+n}^*$, montrons que $w^n = n!(-1)^{\frac{n(n-1)}{2}} v$.
En développant w^n et en utilisant le fait qu'un terme comportant deux indices identiques est nul et le fait que l'on peut permuter deux 2-forme alternées côte à côte, on voit que
$w^n = n!(e_1^* \wedge e_{1+n}^* \wedge e_n^* \wedge e_{2+n}^* \wedge ... \wedge e_n^* \wedge e_{2n}^*$
Maintenant pour se ramener à v, on va regarder la suite $(1\ n+1\ 2\ n+2\ ...\ n\ 2n)$.
Il faut faire une transposition pour ramener le 2 à coté du 1.
Puis 2 transpositions pour ramener le 3 à coté du 2.
Et ainsi de suite jusqu'à n-1 transpositions pour ramener le n à coté du n-1.
A la fin de ce procédé, on s'est ramené à $(1\ 2\ 3\ ...\ 2n-1\ 2n)$ et on a fait apparaitre $1+2+...+n-1 = \frac{n(n-1)}{2}$ signe moins.
D'où le résultat.

6.4 Annexe 4 : Principaux résultats

Dans cette annexe, nous allons énoncer (ou rappeler) les résultats nécessaires à la preuve des trois conjectures.

Proposition D : Soit K un corps et F un K-automorphisme de $K[x] := K[x_1, ..., x_n]$ alors $degF^{-1} \leq (degF)^{n-1}$.

Théorème P : Soit R un anneau et φ un endomorphisme de $P_n(R)$. Si $n!$ est inversible dans R alors $detJ\varphi = 1$.

Théorème R : Soit A une $\mathbb{Z}$-algèbre de type fini sans torsion. Alors pour presque tout nombre premier p, il existe un idéal maximal $\mathfrak{m}$ de A contenant p tel que $A/\mathfrak{m}$ soit un corps fini.

Théorème FI : Soit K un corps et $F = (F_1, ..., F_n)$ avec pour tout $1 \leq i \leq n$, $F_i \in K[[x_1, ..., x_n]]$. Si $detJF(0) \neq 0$ et $F(0) = 0$. Alors il existe $G = (G_1, ..., G_n)$ avec pour tout $1 \leq i \leq n$, $G_i \in K[[x_1, ..., x_n]]$ tel que $G.F = (x_1, ..., x_n)$.

7 Bibliographie

1 S. C. Coutinho, A Primer of Algebraic D-Modules.

2 A. van den Essen, Polynomial automorphisms and the Jacobian conjecture.

3 Polynomial automorphisms and related topics. Lecture notes of the international school and workshop ICPA2006, Hanoi, Vietnam, October 9–20, 2006