Quatorzième problème de Hilbert

sous la direction de Olivier Benoist

Léa Bittmann Olivier Graf

22 novembre 2013

Table des matières

1 Introduction

Le quatorzième problème de Hilbert fait partie des 23 problèmes posés par David Hilbert en 1900 au congrès international des mathématiques à Paris et dont la résolution était censée avoir une grande influence sur les mathématiques du vingtième siècle.
Le quatorzième problème pose la question de savoir si les algèbres d'invariants sont de type fini ou non. Précisons ce que cela signifie, donnons tout d'abord quelques définitions.

1.1 Définitions

Définition 1.1.1. Soit k un corps algébriquement clos, on dit que G est un sous-groupe *algébrique* de $GL_n(k)$ si c'est un sous-groupe de $GL_n(k)$ dont les éléments peuvent être définis comme les zéros d'une famille de polynômes.

Exemple 1.1.2. Les groupes finis sont algébriques.

Exemple 1.1.3. Les groupes :

$$\mathbb{G}_a := (k, +)$$

et :

$$\mathbb{G}_m := (k^*, \times)$$

sont algébriques car :

$$\mathbb{G}_a \simeq \{\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in k\} \subset GL_2(k)$$

et

$$\mathbb{G}_m \simeq GL_1(k).$$

Exemple 1.1.4. Les groupes orthogonaux (resp. symplectiques) sont aussi définis par des équations polynômiales : l'équation ${}^tMAM = A$ où A est la matrice de la forme quadratique (resp. alternée) et M est dans $GL_n(k)$ est clairement polynomiale en M.

Définition 1.1.5. On dit qu'une k-algèbre est de type fini si elle est engendrée comme k-algèbre par un nombre fini d'éléments.

Définition 1.1.6. Soit G un sous-groupe algébrique de $GL_n(k)$ agissant sur une k-algèbre A. On définit A^G par :

$$A^G := \{P \in A \mid \forall g \in G \; g \cdot P = P\}$$

et on l'appelle *algèbre d'invariants de A sous G.*

1.2 Le problème de Hilbert

Le quatorzième problème de Hilbert consiste à savoir si pour tout groupe algébrique et pour toute action algébrique de celui-ci sur une k-algèbre de type fini A, l'algèbre A^G est de type fini ou non.
Un cas particulier d'action d'un groupe algébrique sont les actions *linéaires* :

Définition 1.2.1. Un sous-groupe algébrique G de $GL_n(k)$ a une action naturelle sur $k[X_1, \ldots, X_n]$, que l'on peut expliciter par :

$$g \cdot P(X_1, \ldots, X_n) = P(\sum_{j=1}^{n} (g^{-1})_{1,j} X_j, \ldots, \sum_{j=1}^{n} (g^{-1})_{n,j} X_j)$$

pour tout $g = [g_{i,j}]_{(i,j)\in\{1,\ldots,n\}^2}$ dans G et pour tout P dans $k[X_1, \ldots, X_n]$. Cette action est dite *linéaire.*

Le problème que nous allons traiter par la suite sera de savoir si $k[X_1, \ldots, X_n]^G$ est de type fini, où G agit linéairement sur $k[X_1, \ldots, X_n]$.

C'est Nagata [3] qui en 1959 a trouvé un contre-exemple à ce problème. Nous en présentons ici une version simplifiée par Robert Steinberg [4] et Igor Dolgachev [1].

1.3 Plan

Dans une première partie nous présenterons quelques résultats positifs, à savoir :

Théorème 1.3.1. *Si G est fini et agit sur une k-algèbre A de type fini, alors A^G est de type fini.*

Théorème 1.3.2. *Si $G \simeq \mathbb{G}_m$ et A k-algèbre de type fini telle que l'action de G induit une $\mathbb{Z}$-graduation, alors A^G de type fini.*

Dans une deuxième partie on donnera le contre-exemple de Nagata simplifié par Steinberg :

Théorème 1.3.3. *Il existe un groupe algébrique G sous-groupe de $GL_{18}(\mathbb{C})$ tel que pour son action linéaire, $\mathbb{C}[X_1, \ldots, X_{18}]^G$ n'est pas de type fini.*

Dans une troisième partie on étendra ce contre-exemple, en utilisant des courbes algébriques. Ceci nous amènera à exposer quelques résultats, comme le théorème de Bézout et le théorème fondamental de Max Noether.

2 Des résultats positifs

Dans cette partie, on donnera quelques réponses positives dans des cas particuliers au problème de Hilbert.

2.1 Un exemple : les polynômes symétriques

Commençons par décrire un exemple classique : l'action du groupe symétrique $\mathfrak{S}_n$ sur l'algèbre de polynômes $k[X_1, \ldots, X_n]$.
Pour $\sigma \in \mathfrak{S}_n,\ \sigma \cdot X_i = X_{\sigma(i)}$, et $\mathfrak{S}_n$ agit comme morphisme d'algèbre.
Dans ce cas, l'algèbre d'invariants associée $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est composée des polynômes qui sont symétriques en les différentes indéterminées.
On peut voir qu'elle est engendrée par les polynômes symétriques élémentaires :

$$X_1 + \cdots + X_n\ ;\ X_1X_2 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n; \ldots; X_1X_2 \cdots X_n,$$

qui sont en nombre fini.
La k-algèbre $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est donc dans ce cas de type fini.

2.2 Invariants sous un groupe fini

En fait le cas des polynômes symétriques n'est pas isolé, comme le montre la proposition suivante :

Théorème 2.2.1. *Pour tout groupe G fini agissant sur une k-algèbre de type fini A l'algèbre d'invariants A^G est aussi de type fini.*

On peut montrer ce résultat de plusieurs façons, l'une d'elle est basé sur les mêmes idées que celles utilisées au paragraphe suivant, cf. remarque 2.3.6. On va donc le montrer d'une autre façon.

Démonstration. L'inclusion $A^G \hookrightarrow A$ est une extension d'anneaux entière. En effet, pour tout $a \in A$, on a $P_a = 0$, avec $P_a := \prod_{g \in G}(X - g \cdot a)$. D'après les relations coefficients-racines :

$$P_a = \sum_{k=0}^{|G|} (-1)^k \Big(\prod_{(g_1, \ldots, g_k) \in G^k} g_1 \cdot a \cdots g_k \cdot a \Big) X^k.$$

On voit donc que les coefficients de ce polynôme sont invariants par G. Donc $P_a \in A^G[X]$, unitaire. Ainsi a est entier sur A^G.

L'algèbre A est par hypothèse de type fini, notons $a_1, \ldots, a_n$ des générateurs de A. L'extension d'anneaux $A^G \hookrightarrow A$ est donc engendrée par un nombre fini d'éléments (les $a_1, \ldots, a_n$), qui sont entiers sur A^G, c'est donc une extension finie.
Soit B la sous-algèbre de A engendrée par les coefficients des polynômes P_{a_k}, pour $k \in \{1, \ldots, n\}$.
A est une k-algèbre de type fini, donc aussi une B-algèbre de type fini. De plus, on a montré que l'extension $A^G \hookrightarrow A$ est finie. Donc en appliquant le lemme 2.2.2 suivant avec $C = A^G$, on obtient : A^G est une B-algèbre de type fini, avec B une k-algèbre de type fini.
Ainsi l'algèbre des invariants A^G est une k-algèbre de type fini. □

Lemme 2.2.2. *Soit B un anneau noethérien et soient $B \hookrightarrow C \hookrightarrow A$ des extensions d'anneaux. On suppose que A est une B-algèbre de type fini et une C-algèbre finie. Alors C est une B-algèbre de type fini.*

Démonstration. Soient $a_1, \dots, a_n$ des générateurs de la B-algèbre A et $a'_1, \dots, a'_m$ des générateurs du C-module A. On écrit $a_i = \sum_j c_{ij} a'_j$, avec $c_{ij} \in C$ et $a'_i a'_j = \sum_k c'_{ijk} a'_k$, avec $c'_{ijk} \in C$. Soit $C' \subseteq C$ la sous-B-algèbre engendrée par les c_{ij} et les c'_{ijk}. On a donc la suite d'extensions : $B \hookrightarrow C' \hookrightarrow C \hookrightarrow A$. Comme C' est une B-algèbre de type fini, avec B anneau noethérien, C' est aussi un anneau noethérien.
Montrons que A est une extension finie de C'.
Pour tout $a \in A$, il existe $P \in B[X_1, \dots, X_n]$ tel que $a = P(a_1, \dots, a_n)$. Or, chaque a_i est égal à une combinaison linaire à coefficients dans C' des $a'_1, \dots, a'_m$.
Donc $a = Q(a'_1, \dots, a'_m)$, avec $Q \in C'[X_1, \dots, X_m]$. Or pour tout i, j, le produit $a'_i a'_j$ est égal à une combinaison linéaire à coefficients dans C' des $a'_1, \dots, a'_m$. Donc de même tout monôme $(a'_1)^{\alpha_1} \cdots (a'_m)^{\alpha_m}$ est combinaison linéaire à coefficients dans C' des $a'_1, \dots, a'_m$. Ainsi a est dans le C'-module engendré par $a'_1, \dots, a'_m$.
Alors C est un sous-C'-module du C'-module de type fini A, comme C' est noethérien, C est aussi un C'-module de type fini. Ainsi l'extension $C' \hookrightarrow C$ est finie.
Comme C' est une B-algèbre de type fini, C est aussi une B-algèbre de type fini. □

2.3 Invariants sous le groupe multiplicatif

Soit k un corps. On considère ici une action du groupe multiplicatif $\mathbb{G}_m$, que l'on notera G sur une k-algèbre de type fini A.

Définition 2.3.1. On dit que l'action de G induit une $\mathbb{Z}$-graduation si

$$A = \bigoplus_{i \in \mathbb{Z}} A_i \text{ , avec } A_i = \{a \in A \mid \forall \lambda \in G \ \lambda \cdot a = \lambda^i a\}$$

Remarque 2.3.2. Cette hypothèse n'est en fait pas très restrictive, c'est plutôt une caractérisation du caractère *algébrique* de l'action de G...

Proposition 2.3.3. *Une telle algèbre est munie d'un opérateur appelé opérateur de Reynolds :*

$R_A : \ A \to A^G$, *morphisme de k-espace vectoriel tel que* $R_A(ab) = R_A(a)b$ *si* $a \in A$ *et* $b \in A^G$.

Démonstration. En effet, il suffit de prendre pour R_A la projection sur $A_0 = A^G$. Si $a \in A$, $a = \sum a_i$ avec $a_i \in A_i$ et $b \in A^G$, alors $R_A(ab) = R_A(\sum a_i b) = \sum R_A(a_i b)$. Or, pour tout $i, j \in \mathbb{Z}$, $A_i A_j \subseteq A_{i+k}$. Donc $a_i b \in A_i$.
Ainsi $R_A(ab) = a_0 b = R_A(a)b$. □

Remarque 2.3.4. Avec ces notations on a : $A_0 = A^G$.

Théorème 2.3.5. *L'algèbre d'invariants A^G pour l'action du groupe multiplicatif sur une k-algèbre $\mathbb{Z}$-graduée est de type fini.*

Démonstration. La k-algèbre A est engendrée par un nombre fini de termes $x_1, \dots, x_n$. Chaque x_k peut se décomposer sur la somme directe $\oplus_{i \in \mathbb{Z}} A_i$, donc, quitte à remplacer les x_k par l'ensemble (fini) de leurs coordonnées sur cette décomposition, on peut supposer que pour tout $k \in \{1, \dots, n\}$, il existe $i_k \in \mathbb{Z}$ tel que $x_k \in A_{i_k}$.
On a alors le morphisme de k-algèbres surjectif suivant :

$$\begin{aligned} k[X_1, \dots, X_n] &\xrightarrow{\pi} A \\ X_k &\longmapsto x_k. \end{aligned}$$

L'action de G sur A se relève en une action sur $k[X_1, \dots, X_n]$ préservant le degré, via :

$$\forall k \in \{1, \dots, n\}, \ \lambda \in G, \ \lambda \cdot X_k = \lambda^{i_k} X_k.$$

Et G agit par morphisme d'algèbres sur $k[X_1, \dots, X_n]$.
L'action de G sur $k[X_1, \dots, X_n]$ étant très simple, on a aussi une $\mathbb{Z}$-graduation sur $k[X_1, \dots, X_n]$. Soit $P = \sum_{(\alpha_1, \dots, \alpha_n) = I} c_I X_1^{\alpha_1} \dots X_n^{\alpha_n} \in k[X_1, \dots, X_n]$. Pour tout $\lambda \in G$:

$$\lambda \cdot P = \sum_{(\alpha_1, \dots, \alpha_n) = I} c_I (\lambda \cdot X_1)^{\alpha_1} \dots (\lambda \cdot X_n)^{\alpha_n} = \sum_{(\alpha_1, \dots, \alpha_n) = I} \lambda^{\alpha_1 i_1 + \dots + \alpha_n i_n} c_I X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

Donc

$$P = \sum_{i\in\mathbb{Z}} \underbrace{\sum_{\substack{(\alpha_1,\dots,\alpha_n)=I \\ \alpha_1 i_1+\cdots+\alpha_n i_n=i}} c_I X_1^{\alpha_1}\dots X_n^{\alpha_n}}_{\in k[X_1,\dots,X_n]_i}$$

Alors $k[X_1,\dots,X_n]$ est de la même façon muni d'un opérateur de Reynolds R, et on a $\pi\circ R = R_A\circ\pi$, car π commute à l'action de G.

Montrons que les invariants de $k[X_1,\dots,X_n]$ se surjectent dans les invariants de A : $k[X_1,\dots,X_n]^G \twoheadrightarrow A^G$.
Cela découle de l'égalité précédente :
Si $P \in k[X_1,\dots,X_n]^G$ alors $\pi(P) = \pi(R(P)) = R_A(\pi(P)) \in A^G$. Donc $\pi(k[X_1,\dots,X_n]^G) \subseteq A^G$.
Et pour tout $a \in A^G$, $a = \pi(P)$ car π est surjective. Donc $a = R_A(a) = R_A(\pi(P)) = \pi(\underbrace{R(P)}_{\in k[X_1,\dots,X_n]^G})$.
Il suffit donc de montrer que $k[X_1,\dots,X_n]^G$ est une algèbre de type fini, et on peut en déduire directement que A^G aussi (les images par π des générateurs de $k[X_1,\dots,X_n]^G$ donneront des générateurs de A^G).

Notons $k_m[X_1,\dots,X_n]$ l'ensemble des polynômes homogènes de degré $m \geq 0$. On a :

$$k[X_1,\dots,X_n] = \bigoplus_{m=0}^{\infty} k_m[X_1,\dots,X_n]$$

Comme G préserve le degré, il préserve les $k_m[X_1,\dots,X_n]$ et donc on a aussi :

$$k[X_1,\dots,X_n]^G = \bigoplus_{m=0}^{\infty} k_m[X_1,\dots,X_n]^G \tag{1}$$

Soit I l'idéal de $k[X_1,\dots,X_n]$ engendré par les polynômes invariants homogènes de degré $m \geq 1$.
Comme $k[X_1,\dots,X_n]$ est noethérien, il existe $F_1,\dots,F_r$ des générateurs de I.
Pour tout $k \in \{1,\dots,r\}$, $F_k \in I$ donc on peut écrire F_k comme combinaison linéaire de polynômes homogènes invariants. Ainsi, quitte à remplacer $\{F_1,\dots,F_r\}$ par l'ensemble (fini) de leurs coordonnées, on peut supposer qu'ils sont eux-mêmes homogènes et invariants. On note m_k le degré de F_k.

Montrons que $k[X_1,\dots,X_n]^G$ est engendrée en tant que k-algèbre par les polynômes $F_1,\dots,F_r$ et qu'elle est donc de type fini.
Soit $F \in k[X_1,\dots,X_n]^G$, homogène de degré $m \geq 1$. Comme $F \in I$, il existe $P_1,\dots,P_r \in k[X_1,\dots,X_n]$ tels que $F = P_1F_1 + \cdots + P_rF_r$.
Comme F est homogène, les monômes apparaissant dans le terme de droite qui sont de degré différent de m vont se simplifier. On peut donc supposer que pour tout $k \in \{1,\dots,r\}$, P_k est homogène de degré $m - m_k$. Appliquons R, opérateur de Reynolds, à l'expression précédente :

$$\underbrace{R(F)}_{=F} = \underbrace{R(P_1F_1)}_{=R(P_1)F_1} + \cdots + \underbrace{R(P_rF_r)}_{=R(P_r)F_r} \tag{2}$$

car $F, F_1,\dots,F_r \in k[X_1,\dots,X_n]^G$.
Pour tout k, $R(P_k) \in k[X_1,\dots,X_n]^G$ et $R(P_k)$ est toujours homogène de degré $m - m_k (< m)$, car comme dans (1), R préserve la graduation par le degré. Par récurrence sur le degré d'homogénéité, on montre alors que $R(P_k)$ est dans l'algèbre engendrée par $F_1,\dots,F_r$ et donc F aussi, par (2) (les constantes étant évidemment dans l'algèbre).
Soit $F \in k[X_1,\dots,X_n]^G$, quelconque. On décompose F en somme de polynômes homogènes, par (1) encore, ils restent invariants. D'après le résultat précédent, chacun de ces termes sont dans l'algèbre engendrée par $F_1,\dots,F_r$, et donc F aussi.
L'autre inclusion étant évidente, on a montré que la k-algèbre engendrée par $F_1,\dots,F_r$ était $k[X_1,\dots,X_n]^G$. □

Remarque 2.3.6. Si G fini et si $|G|$ est premier avec la caractéristique de k, la même preuve fonctionne avec $R(a) := \frac{1}{|G|} \sum_{g \in G} g \cdot a$ ce qui donne une preuve alternative du théorème 2.2.1 dans ce cas.

3 Un premier contre-exemple

Dans cette partie, nous donnerons le premier contre-exemple (dû à Nagata [3]) au quatorzième problème de Hilbert, en prenant le cas particulier $k = \mathbb{C}$, et où $G \simeq \mathbb{G}_a^6$.

3.1 Action de $\mathbb{G}_a^6$ sur $\mathbb{C}[x_1, \ldots, x_9, t_1, \ldots, t_9]$

Définition 3.1.1. Soient $a_1, \ldots, a_9 \in \mathbb{C}$ deux à deux distincts et tels que : $\sum_{i=1}^9 a_i \neq 0$. Alors on définit :

$$G := \{(c_1, \ldots, c_9) \mid \sum_{i=1}^9 c_i = 0 \text{ et } \sum_{i=1}^9 a_i c_i = 0 \text{ et } \sum_{i=1}^9 a_i^3 c_i = 0\}.$$

En ce sens, G peut être vu comme un sous-espace vectoriel de $\mathbb{C}^9$ de codimension 3 ; il s'identifie donc au groupe additif $\mathbb{G}_a^6$.

Définition 3.1.2. On définit une action linéaire de G sur $\mathbb{C}[x_1, \ldots, x_9, t_1, \ldots, t_9]$ (qu'on nommera par la suite $\mathbb{C}[V]$) par : $x_i \mapsto x_i + c_i t_i$ et $t_i \mapsto t_i$.

On va étudier le groupe H engendré par le groupe G et le tore isomorphe à $\mathbb{G}_m^8$:

Définition 3.1.3. On définit le tore T par : $\{(d_1, \ldots, d_9) \mid d_1 \ldots d_9 = 1\}$. Le groupe $H = GT$ agit sur $\mathbb{C}[V]$ par : $x_i \mapsto d_i x_i + c_i d_i t_i$ et $t_i \mapsto d_i t_i$

Il s'agit à présent de montrer que l'algèbre $\mathbb{C}[V]^G$ n'est pas de type fini. Ce qui fournit un contre-exemple au quatorzième problème de Hilbert.
Pour ce faire on commence par montrer que le l'algèbre $\mathbb{C}[V]^H$ n'est pas de type fini. Nous aurons besoin des deux lemmes présentés dans la suite.

3.2 Description de $\mathbb{C}[V]^H$

Nous allons décrire l'algèbre d'invariants de H, en considérant une situation plus générale.
Soient n points $P_i = [a_{i,1} : a_{i,2} : a_{i,3}]$ non alignés dans $\mathbb{CP}^2$. Les c_i sont alors dans les hyperplans associés aux $a_{i,j}$, i.e.

$$\forall j \in \{1, 2, 3\} \ \sum_{i=1}^n a_{i,j} c_i = 0$$

C'est bien une généralisation puisque l'hypothèse faite sur les a_i originaux garantit que les P_i ne sont pas alignés. En effet, les $P_1, \ldots, P_9$ sont tous de coordonnées $[1 : a_i : a_i^3]$ donc tous dans le plan $x = 1$. Quitte à faire une translation dans ce plan on peut supposer $P_1 = [1 : 0 : 0]$. Si tous les P_i étaient alignés et puisqu'ils sont par hypothèse deux à deux distincts, il existerait pour tout i un α_i dans $\mathbb{C}$ tel que $(a_i, a_i^3) = \alpha_i(a_2, a_2^3)$. Ce qui impliquerait que pour tout i $\alpha_i^3 = \alpha_i$, équation n'ayant que trois solutions dans $\mathbb{C}$ donc les $P_1, \ldots, P_9$ ne seraient pas deux à deux distincts : c'est absurde.
Posons alors :

$$\begin{aligned} t &= t_1 \ldots t_n \\ z_1 &= a_{1,1} x_1 t_2 \ldots t_n + \ldots + a_{n,1} t_1 \ldots t_{n-1} x_n \\ z_2 &= a_{1,2} x_1 t_2 \ldots t_n + \ldots + a_{n,2} t_1 \ldots t_{n-1} x_n \\ z_3 &= a_{1,3} x_1 t_2 \ldots t_n + \ldots + a_{n,3} t_1 \ldots t_{n-1} x_n \end{aligned}$$

Proposition 3.2.1. *Les t, z_1, z_2, z_3 sont invariants sous H et algébriquement indépendants sur $\mathbb{C}$.*

Démonstration. Il résulte d'un simple calcul que les t, z_1, z_2, z_3 sont invariants sous H. Quitte à les échanger on peut supposer que P_1, P_2, P_3 ne sont pas alignés dans $\mathbb{C}P^2$, c'est-à-dire que la matrice $A = [a_{i,j}]_{i,j \in \{1,2,3\}}$ de leurs coefficients dans $\mathbb{C}^3$ est inversible. Posons : $w_i = t_1 \ldots x_i t_{i+1} \ldots t_n$. On

a par définition :

$$z_1 = a_{1,1}w_1 + a_{2,1}w_2 + a_{3,1}w_3 + \dots$$
$$z_2 = a_{1,2}w_1 + a_{2,2}w_2 + a_{3,2}w_3 + \dots$$
$$z_3 = a_{1,3}w_1 + a_{2,3}w_2 + a_{3,3}w_3 + \dots$$

Or les x_i sont indépendants sur $\mathbb{C}[t_1, \dots, t_n]$ donc les $w_i, i = 1, \dots 3$ et les $x_4, \dots, x_n$ sont indépendants sur $\mathbb{C}[t_1, \dots, t_n]$, donc les z_i et $x_4, \dots, x_n$ sont indépendants sur $\mathbb{C}[t_1, \dots, t_n]$. En effet, il existe une matrice B à coefficients dans $\mathbb{C}$ inversible telle que : $(z_1, z_2, z_3, x_4, \dots, x_n) = B(w_1, w_2, w_3, x_4, \dots, x_n)$; il suffit en effet de prendre :

$$B = \begin{pmatrix} A & C \\ (0) & Id \end{pmatrix}$$

où $C = [a_{j,i}]_{1 \leq i \leq 3,\ 4 \leq j \leq n}$. Alors les deux blocs diagonaux sont inversibles puisque la matrice A de base était inversible. Supposons alors qu'il existe P tel que $P(z_1, \dots, x_n) = 0$, alors cela signifie que : $Q(w_1, \dots, x_n) = P(B(w_1, \dots, x_n)) = 0$ donc $Q = 0$, or $P = Q(B^{-1})$, donc $P = 0$ et en particulier les z_i sont algébriquement indépendants sur $\mathbb{C}[t_1, \dots, t_n]$. Donc z_1, z_2, z_3, t sont algébriquement indépendants sur $\mathbb{C}$.

□

Proposition 3.2.2. *L'algèbre d'invariants $\mathbb{C}[V]^H$ coïncide avec $\mathbb{C}[z_1, z_2, z_3, t, t^{-1}] \cap \mathbb{C}[V]$.*

Démonstration. Puisque $x_i = \frac{w_i t_i}{t}$ et que la matrice A vue précédemment est inversible, on a :

$$\mathbb{C}[x_1, \dots, x_n, t_1, \dots, t_n][\frac{1}{t}] = \mathbb{C}[w_1, w_2, w_3, x_4, \dots, x_n, t_1, \dots, t_n][\frac{1}{t}] = \mathbb{C}[z_1, z_2, z_3, x_4, \dots, t_n, \frac{1}{t}]$$

Soit $c \in \mathbb{C}$. On peut résoudre en c_1, c_2, c_3 le système linéaire suivant :

$$0 = a_{1,1}c_1 + a_{2,1}c_2 + a_{3,1}c_3 + a_{4,1}c$$
$$0 = a_{1,2}c_1 + a_{2,2}c_2 + a_{3,2}c_3 + a_{4,2}c$$
$$0 = a_{1,3}c_1 + a_{2,3}c_2 + a_{3,3}c_3 + a_{4,3}c$$

car A est inversible, ce qui nous donne des éléments de G : $(c_1, c_2, c_3, c, 0, \dots, 0)$. Faisons les agir sur $\mathbb{C}[z_1, z_2, z_3, x_4, \dots, t_n, \frac{1}{t}]$ (l'action sur $\frac{1}{t}$ est l'action triviale) :
soit $P \in \mathbb{C}[z_1, z_2, z_3, x_4, \dots, t_n, \frac{1}{t}]$, alors $(c_1, c_2, c_3, c, 0, \dots, 0) \cdot P = P(z_1, z_2, z_3, x_4 + ct_4, x_5, \dots, t_n, \frac{1}{t})$ car les z_i sont invariants. Si P est dans $\mathbb{C}[V]^H$ alors on a : $P(z_1, z_2, z_3, x_4 + ct_4, x_5, \dots, t_n, \frac{1}{t}) = P(z_1, z_2, z_3, x_4, x_5, \dots, t_n, \frac{1}{t})$, quel que soit c dans $\mathbb{C}$. On en déduit donc que P ne dépend pas de x_4. De la même manière, on a P indépendant des autres x_i, pour $i \geq 4$. Donc $\mathbb{C}[z_1, z_2, z_3, x_4, \dots, t_n, \frac{1}{t}]^G = \mathbb{C}[z_1, z_2, z_3, t_1, \dots, t_n, \frac{1}{t}]$.
On en déduit que $\mathbb{C}[z_1, z_2, z_3, x_4, \dots, t_n, \frac{1}{t}]^H = \mathbb{C}[z_1, z_2, z_3, t, \frac{1}{t}]$ car on peut écrire :

$$P = \sum_{i \in \mathbb{Z}, i_1, \dots, i_n \in I} f_{i_1, \dots, i_n}(z_1, z_2, z_3) \frac{t_1^{i_1} \cdots t_n^{i_n}}{t^i},$$

où $I = \{(i_1, \dots, i_n) \in \mathbb{N} \mid \exists k\ i_k = 0\}$ ce qui rend la décomposition unique. Si P est invariant sous H, alors tous les éléments de la somme le sont, et donc on a :

$$\forall (i_1, \dots, i_n), \in I\ d_1^{i_1} \dots d_n^{i_n} = 1.$$

Ce qui implique que $i_1 = \dots = i_n = 0$ car en supposant qu'il existe k tel que $i_k \neq 0$, on peut faire agir l'élément $(1, \dots, 1, \lambda, 1, \dots, \frac{1}{\lambda}, 1, \dots, 1)$ où les λ et $\frac{1}{\lambda}$ sont à la position k et l où $i_l = 0$, et on obtiendrait une absurdité.
Donc, finalement : $\mathbb{C}[z_1, z_2, z_3, x_4, \dots, t_n, \frac{1}{t}]^H = \mathbb{C}[z_1, z_2, z_3, t, \frac{1}{t}]$, et : $\mathbb{C}[V]^H = \mathbb{C}[V] \cap \mathbb{C}[z_1, z_2, z_3, t, \frac{1}{t}]$.
□

Proposition 3.2.3. *Les éléments de* $\mathbb{C}[V]^H = \mathbb{C}[z_1, z_2, z_3, t, t^{-1}] \cap \mathbb{C}[V]$ *sont sommes de* $\frac{f(z_1,z_2,z_3)}{t^m}$ *où* m *est dans* $\mathbb{Z}$, f *est homogène et divisible par* t^m *dans* $\mathbb{C}[V]$.

Démonstration. Soit $F \in \mathbb{C}[V]^H$. Alors on peut écrire :

$$F = \sum_{m \in \mathbb{Z}} \frac{f_m(z_1, z_2, z_3)}{t^m}$$

On peut également se ramener au cas où F homogène sur $\mathbb{C}[V]$ puisque F se décompose de façon unique en somme de polynômes homogènes et que l'action de H conserve le degré des polynômes homogènes : F est donc dans $\mathbb{C}[V]^H$ si et seulement si tous les polynômes homogènes de sa décomposition le sont.

Notons d son degré. Les z_i et t sont homogènes de degré n sur $\mathbb{C}[V]$, donc : $\frac{z_1^a z_2^b z_3^c}{t^m}$ est de degré $(a+b+c)n-mn$. De plus la décomposition de F sur les $\frac{1}{t^m}$ est unique car les z_i, t sont indépendants et donc aussi les z_i et $\frac{1}{t}$ (supposons le contraire, on pourrait trouver un polynôme de degré δ de $\mathbb{C}[z_1, z_2, z_3]$ annulant $\frac{1}{t}$ et en multipliant par t^δ on obtiendrait un polynôme de $\mathbb{C}[z_1, z_2, z_3]$ annulant t). Il est donc nécessaire que $(a+b+c)n - mn = d$ sans quoi on aurait des polynômes homogènes d'un degré différent dans F. Il n'y a donc dans les f_m que des monômes de degré $a+b+c = \frac{d}{n} + m$, donc les f_m sont homogènes de degré $a+b+c = \frac{d}{n} + m$.

Il reste à prouver que $\frac{f_m}{t^m} \in \mathbb{C}[V]$.

Or les f_m sont homogènes en les x_i de même degré $m + \frac{d}{n}$ que pour les z_i, donc ils sont les polynômes homogènes de la décomposition en polynômes homogènes de F comme élément de $\mathbb{C}[t_1, \ldots, t_n][x_1, \ldots, x_n]$ puisque tous de degrés différents. Finalement : $\frac{f_m}{t^m}$ est dans $\mathbb{C}[V]$. □

On définit la multiplicité pour les polynômes de $\mathbb{C}[z_1, \ldots, z_n]$ comme suit :

Définition 3.2.4. Le polynôme $f \in \mathbb{C}[z_1, \ldots, z_n]$ a une multiplicité m en 0 si et seulement si en écrivant f comme somme de polynômes homogènes, il n'y a pas de terme homogène de degré $\leq m-1$. Et f a une multiplicité m au point $P = (z_{1,0}, \ldots, z_{n,0})$ si $(z_1, \ldots, z_n) \longrightarrow f(z_1 + z_{1,0}, \ldots, z_n + z_{n,0})$ a une multiplicité m en 0.

Remarque 3.2.5. Cela correspond bien à l'idée intuitive de multiplicité d'un polynôme à plusieurs variables qu'on a en remplaçant la dérivation par la différentiation...

Proposition 3.2.6. *Un polynôme* f *homogène et différent de* 0 *dans* $\mathbb{C}[z_1, z_2, z_3]$ *est divisible par* t^m *dans* $\mathbb{C}[V]$ *si et seulement si la courbe projective de* $\mathbb{CP}^2$ *associée a multiplicité au moins* m *en chaque* $P_i = [a_{i,1} : a_{i,2} : a_{i,3}]$.

Démonstration. Prenons $f(z_1, z_2, z_3)$ polynôme homogène de degré d. On a un changement de base de matrice M dans $\mathbb{C}^3$ qui fait que P_1 a pour coordonnées dans cette nouvelle base $[1:0:0]$. Les variables s'expriment en fonction des anciennes : $(z_1', z_2', z_3') = M(z_1, z_2, z_3)$ et les coordonnées des P_i deviennent les $[a'_{i,1} : a'_{i,2} : a'_{i,3}]$, où $(a'_{i,1}, a'_{i,2}, a'_{i,3}) = M(a_{i,1}, a_{i,2}, a_{i,3})$. De plus, on avait $z_i = a_{1,i}x_1t_2 \ldots t_n + \ldots + a_{n,i}x_nt_1 \ldots t_{n-1}$, or puisque on a le même changement de variable M, on a également $z_i' = a'_{1,i}x_1t_2 \ldots t_n + \ldots + a'_{n,i}x_nt_1 \ldots t_{n-1}$, donc $f(z_1, z_2, z_3) = f'(z_1', z_2', z_3')$ vu dans $\mathbb{C}[V]$, où $f' = f(M^{-1})$. Les conditions f a multiplicité m en un point P_i et f' a multiplicité m en ce même point sont équivalentes et de même f divisible par t^m dans $\mathbb{C}[V]$ et f' divisible par t^m sont équivalentes, puisque ce sont les mêmes polynômes vus dans $\mathbb{C}[V]$. Donc on peut se ramener au cas où $P_1 = [1:0:0]$.

Notons p la multiplicité de f en $[1:0:0]$. On a $f \in \mathbb{C}[z_1, z_2, z_3] = \mathbb{C}[z_2, z_3][z_1]$ donc on peut décomposer f sur les z_1^k :

$$f = f_q(z_2, z_3)z_1^{d-q} + f_{q+1}(z_2, z_3)z_1^{d-q-1} + \ldots + f_d(z_2, z_3)$$

où q est positif ou nul car f homogène de degré d et $f_q \neq 0$. De plus les f_i sont homogènes de degré i car tous les monômes intervenant dans f sont de degré d, car f homogène de degré d.

On a alors $q = p$ car $f_k(z_2, z_3)z_1^{d-k}$ est de multiplicité k en $[1:0:0]$: en effet, f_k est de multiplicité k en $(0,0)$ et on en déduit que $f_k(z_2, z_3)z_1^{d-k}$ de multiplicité k en $[1:0:0]$. Donc f est de multiplicité exactement q en $[1:0:0]$, donc $q = p$.

On va maintenant écrire f comme élément de $\mathbb{C}[V]$. Puisque on a pris $P_1 = [1 : 0 : 0]$, on a $z_1 = x_1 t_2 \dots t_n + \dots$, $z_2 = t_1 u_2$ et $z_3 = t_1 u_3$ où $u_j = a_{2,j} x_2 t_3 \dots t_n + \dots + a_{n,j} x_n t_2 \dots t_{n-1}$. Remarquons que t_1 n'intervient pas dans les u_j. On a donc :

$$f = t_1^p f_p(u_2, u_3)(x_1 t_2 \dots t_n)^{d-p} + t_1^{p+1}(\dots)$$

et t^1 n'intervient pas dans $f_p(u_2, u_3)(x_1 t_2 \dots t_n)^{d-p}$ et $f_p(u_2, u_3) \neq 0$ car $f_p \neq 0$ et u_2, u_3 algébriquement indépendants. En effet, $x_2 t_3 \dots t_n, x_3 t_2 t_4 \dots t_n, \dots, x_n t_2 \cdots t_{n-1}$ sont algébriquement indépendants et $(u_2, u_3, x_4 t_2 \cdots t_n, \dots, x_n t_2 \cdots t_{n-1}) = B(x_2 t_3 \dots t_n, x_3 t_2 t_4 \dots t_n, \dots, x_n t_2 \cdots t_{n-1})$ où :

$$B = \begin{pmatrix} A & C \\ (0) & Id \end{pmatrix}$$

où

$$A = \begin{pmatrix} a_{2,2} & a_{3,2} \\ a_{2,3} & a_{3,3} \end{pmatrix}$$

Et $C = [a_{j,i}]_{2 \leq i \leq 3,\ 4 \leq j \leq n}$. Or la matrice :

$$\begin{pmatrix} 1 & a_{2,1} & a_{3,1} \\ 0 & a_{2,2} & a_{3,2} \\ 0 & a_{2,3} & a_{3,3} \end{pmatrix}$$

est inversible car on peut supposer quitte à les échanger que les P_1, P_2, P_3 ne sont pas alignés dans $\mathbb{C}P^2$. On en déduit donc que A est inversible et donc que u_2 et u_3 sont algébriquement indépendants (c'est ensuite la même preuve que lorsqu'on a montré que les z_i, t étaient algébriquement indépendants).
Donc t_1^p divise f dans $\mathbb{C}[V]$ et c'est la plus grande puissance de t_1 divisant f. On peut maintenant conclure.
Si f est de multiplicité m en tous les P_i alors par ce qui précède, pour tout i, t_i^m divise f et donc t^m divise f dans $\mathbb{C}[V]$ car l'anneau $\mathbb{C}[V]$ est factoriel et les t_i sont irréductibles et non associés.
Réciproquement, si t^m divise f alors pour tout i, t_i^m divise f et donc la multiplicité de f en les P_i est supérieure ou égale à m, puisque la multiplicité en P_i est la plus grande puissance de t_i divisant f. Ce qui achève la démonstration de la proposition et caractérise les éléments de $\mathbb{C}[V]^H$. □

On a donc prouvé le lemme suivant :

Lemme 3.2.7. *Les t, z_1, z_2, z_3 sont invariants sous H et algébriquement indépendants sur $\mathbb{C}$ et $\mathbb{C}[V]^H$ correspond aux éléments de $\mathbb{C}[z_1, z_2, z_3, t, t^{-1}]$ qui sont sommes de $\frac{f(z_1,z_2,z_3)}{t^m}$ où $m \in \mathbb{Z}$ tels que f est un polynôme homogène différent de 0 telle que la courbe projective de $\mathbb{C}P^2$ associée a multiplicité au moins m en chaque $P_i = [a_{i,1} : a_{i,2} : a_{i,3}]$.*

3.3 Multiplicité et degré des courbes projectives passant par les P_i

On considère maintenant la cubique dans $\mathbb{C}P^2$ que l'on appelle cuspidale d'équation : $YZ^2 - X^3 = 0$. On se placera ici dans le plan affine $Z = 1$. Les coordonnées sont notées (x, y). On considèrera indifféremment les courbes algébriques et les polynômes de $\mathbb{C}[x, y]$.
L'équation en question est alors $y - x^3$. (On la notera f_0)

Lemme 3.3.1. *Soit $a_1, \dots, a_9 \in \mathbb{C}^9$ tels que $\sum_{k=1}^9 a_k \neq 0$ (distincts).$\forall k \in \{1, \dots, 9\}$, on note P_k le point de la courbe f_0 de coordonnées (a_k, a_k^3).*

(a) Pour tout $m \geq 0$, il existe (à une multiplication par un scalaire près) une unique *courbe de degré $\leq 3m$, de multiplicité $\geq m$ à chaque P_k. Il s'agit de f_0^m.*

(b) Pour tout $d \geq 3m$, les conditions du point (a) sur les multiplicités sont linéairement indépendantes sur l'espace des polynômes de degré $\leq d$.

(c) Il existe un polynôme de degré $3m + 1$ qui a une multiplicité $\geq m$ à chaque P_k et qui n'est pas divisible par f_0.

Démonstration. Montrons tout d'abord que la dimension de l'espace des polynômes de degré $\leq d$ sur $\mathbb{C}[x,y]$ est $\binom{d+2}{2}$.

En effet si on note N_d ce nombre, on a la relation de récurrence suivante :

$$N_d = \underbrace{N_{d-1}}_{\text{poly. de degré } <d} + \underbrace{d+1}_{\text{poly. homogènes de degré } d : \sum_{k=0}^{d} x^k y^{d-k} c_k}$$

donc

$$N_d - \underbrace{N_0}_{=1} = \sum_{k=1}^{d} k+1 = d + \frac{d(d+1)}{2}$$

Ainsi

$$N_d = \frac{2(d+1)+d(d+1)}{2} = \frac{(d+1)(d+2)}{2} = \binom{d+2}{2}$$

De même, les conditions (linéaires) qui indiquent qu'une courbe de degré $\geq m-1$ a une multiplicité $\geq m$ en un point P donné sont au nombre de $\binom{m+1}{2}$ et indépendantes.

Montrons le. On peut se ramener par changement de variables à $P=(0,0)$.
Alors si on écrit $f = \sum c_{ij} x^i y^j$, f a une multiplicité $\geq m$ en $(0,0)$ si et seulement si tous les coefficients c_{ij}, $i+j<m$ sont nuls (il n'y a que des termes de degré au moins m).
En comptant comme précédemment, cela donne $\binom{m+1}{2}$ conditions, qui sont clairement indépendantes, vu comme des formes linéaires par exemple (nullité des coefficients sur une base).

Montrons maintenant le point (a) du lemme. Il s'agit de montrer que pour qu'une courbe passe un certain nombre de fois par des points donnés (qui ne sont pas alignés) elle doit avoir un degré assez élevé.
Considérons une courbe de degré $\leq 3m$ et de multiplicité $\geq m$ en chaque P_k.
On écrit $f(x,y) = c_0(x)y^{3m} + c_1(x)y^{3m-1} + \cdots + c_{3m}(x)$ où chaque c_k est un polynôme en x de degré $\leq k$.
On regarde les points d'intersection de f avec la cubique f_0, cela revient à se placer dans le quotient $\mathbb{C}[x,y]/(y-x^3) \simeq \mathbb{C}[x]$.
Pour tout k, si on écrit $f(x,y) = \sum_{i+j\leq 3m} c_{ij}(x-a_k)^i (y-a_k^3)^j$ avec $c_{ij}=0$ pour $i+j<m$.
Alors le projeté devient

$$\begin{aligned}[f](x) &= \sum_{m+1\leq i+j\leq 3m} c_{ij}(x-a_k)^i (x^3-a_k^3)^j \\ &= \sum_{m+1\leq i+j\leq 3m} c_{ij} \underbrace{(x-a_k)^i (x-a_k)^j}_{i+j>m} (x^2+a_k x+a_k^2)^j\end{aligned}$$

Ainsi $[f]$ est divisible par $(x-a_k)^m$, pour tout k. Donc $[f]$ est divisible par $\prod_{k=1}^{9}(x-a_k)^m$ (par le théorème de Gauss), qui est de degré $9m$.
Comme le degré de $[f]$ est majoré par $9m$, il est nécessairement égal à $9m$, et on a

$$c_0(x)x^{9m} + c_1(x)x^{9m-3} + \cdots + c_{3m}(x) = c_0 \prod_{k=1}^{9}(x-a_k)^m \tag{3}$$

Comme $\deg c_j \leq j$, pour tout j, il n'y a pas de terme de degré x^{9m-1} dans le terme de gauche.
Dans l'expression de droite, le coefficient de x^{9m-1} est $-c_0 m \sum_{k=1}^{9} a_k$. Il est donc nul. Or, $\sum_{k=1}^{9} a_k \neq 0$ par hypothèse, donc à condition que $m\geq 1$, on a $c_0=0$, et donc, par (3), $[f]=0$.
Ainsi f est divisible par f_0.

Pour tout k, f_0 a une multiplicité 1 en P_k, donc la courbe $\frac{f}{f_0}$ a un degré $\leq 3(m-1)$ et une multiplicité $\geq m-1$ en chaque P_k.
En procédant par récurrence on en déduit que $\frac{f}{f_0} = \lambda f_0^{m-1}$, avec $\lambda \in \mathbb{C}$. Donc

$$f = \lambda f_0^m$$

Il ne reste plus qu'à initier la récurrence avec le cas $m = 0$. Par hypothèse f est alors de degré ≤ 0 donc

$$\begin{aligned} f &= \lambda \in \mathbb{C} \\ &= \lambda f_0^0 \end{aligned}$$

Passons maintenant au point (b). Comme on l'a vu, l'espace des polynômes de $\mathbb{C}[x, y]$ de degré $\leq 3m$ est de dimension

$$\binom{3m+2}{2} = \frac{(3m+2)(3m+1)}{2} = \frac{9m^2+9m+2}{2}$$

Pour tout k, avoir une multiplicité $\geq m$ en P_k donne $\binom{m+1}{2}$ conditions. Il y a donc en tout

$$9\binom{m+1}{2} = \frac{9(m+1)m}{2} = \frac{9m^2+9m}{2}$$

conditions, donc exactement une de moins que la dimension de l'espace.
Rappelons qu'on peut voir ces conditions comme l'appartenance à des noyaux de formes linéaires. On a donc l'intersection de $N-1$ noyaux dans un espace de dimension N. Ainsi, ces conditions sont linéairement indépendantes si et seulement si l'espace des solutions est de dimension 1.
C'est exactement ce que l'on a montré au point (a).
Fixons $d \geq 3m$. L'ensemble des polynômes de degré $\leq 3m$ est inclus dans l'ensemble des polynômes de degré $\leq d$, donc les conditions de multiplicité restent indépendantes sur l'ensemble des polynômes de degré $\leq d$.

Il reste à prouver le point (c). D'après (b), l'espace des polynômes de degré $\leq 3m+1$ et de multiplicité $\geq m$ en chaque P_k est de dimension

$$\binom{3m+1+2}{2} - 9\binom{m+1}{2} = \frac{(3m+3)(3m+2)}{2} - \frac{9(m+1)m}{2} = 3(m+1)$$

Quelle dimension obtient-on si on considère uniquement les polynômes qui sont en plus divisible par f_0 ?

$$f = qf_0 \Longrightarrow \begin{cases} q \text{ est de degré } \leq 3m+1-3 = 3(m-1)+1 \\ q \text{ a une multiplicité } \geq m-1 \text{ en chaque } P_k \end{cases}$$

f étant entièrement déterminé par q, la dimension est la même qu'en remplaçant m par $m-1$ dans le résultat précédent, donc $3m$.
Ainsi il existe un polynôme (en fait un sous-espace de dimension 3) de degré $\leq 3m+1$, qui vérifie les conditions de multiplicité en chacun des P_k et qui ne soit pas divisible par f_0.
Par (a), son degré ne peut être que exactement $3m+1$.
On achève là la démonstration du point (c) et donc du lemme. □

3.4 L'algèbre d'invariants de H n'est pas de type fini

Des deux lemmes précédents on va déduire :

Théorème 3.4.1. $\mathbb{C}[V]^H$ *n'est pas de type fini*

Démonstration. Supposons le contraire : il existerait, quitte à prendre les $\frac{f_m}{t^m}$ comme dans le lemme 3.2.7, un nombre fini d'éléments $\frac{f_{m_1}}{t^{m_1}}, \ldots, \frac{f_{m_p}}{t^{m_p}}$ générant l'algèbre $\mathbb{C}[V]^H$. On peut y ajouter $\frac{f_0}{t}$ où $f_0 = z_2^3 - z_3 z_1^2$ qui correspond à l'homogénéisé de la courbe $y - x^3$ dans le plan affine et on peut supposer que les f_{m_j} ne sont pas divisibles par f_0 : sinon on peut remplacer $\frac{f_{m_j}}{t^{m_j}} = \frac{f_0^k g(z_1,z_2,z_3)}{t^k t^{m_j-k}}$ par $\frac{g}{t^{m_j-k}}$, où g n'est pas divisible par f_0. En effet, $\frac{g}{t^{m_j-k}} \in \mathbb{C}[V]$, car g est de multiplicité $\geq m_j - k$, $f_0^k g$ étant de multiplicité $\geq m_j$
Soit $m > m_j$, $\forall j$. Alors d'après le lemme 3.3.1, il existe f homogène de degré $3m+1$ non divisible

par f_0 et de multiplicité $\geq m$ en chaque P_i. Montrons que $\frac{f}{t^m}$ n'est pas un polynôme en les $\frac{f_{m_j}}{t^{m_j}}$. Supposons le contraire :

$$\frac{f}{t^m} = \sum \prod \frac{f_{m_j}}{t^{m_j}}$$

Par unicité de la décomposition de $\frac{f}{t^m}$ sur les $\frac{1}{t^k}$ car les z_i, t sont algébriquement indépendants, il n'apparaît dans la somme que des $\frac{1}{t^m}$. On peut donc la réécrire :

$$\frac{f}{t^m} = \frac{\sum \prod f_{m_j}}{t^m}$$

et donc : $f = \sum \prod f_{m_j}$. f étant homogène de degré $3m+1$ il n'apparaît dans la somme que des éléments homogènes de degré $3m+1$. Or f_0 ne divise pas f donc il existe un élément de cette somme où f_0 n'intervient pas, disons

$$\prod_{j=1}^{p} f_{m_j}^{e_j}$$

Notons d_j le degré de f_{m_j} comme polynôme homogène en les z_i. En égalisant les degrés on a donc :

$$\sum_{j=1}^{p} e_j d_j = 3m+1$$

$$\sum_{j=1}^{p} e_j m_j = m$$

Ce qui nous donne $\sum_{j=1}^{p} e_j(d_j - 3m_j) = 1$. Or $\forall j \geq 1$ les f_{m_j} ne sont pas divisibles par f_0, donc d'après le lemme 3.3.1 $d_j - 3m_j > 0$ si $m_j > 0$. L'inégalité reste vraie si $m_j < 0$ ou $d_j > 0$ et $m_j = 0$.
Finalement il existe un unique j tel que $d_j > 0$ ou $m_j \neq 0$ et $e_j = 1$. Pour ce j, on a alors $m_j = m$, ce qui est une contradiction avec le choix de m. □

3.5 De l'algèbre d'invariants de H à celle de G

On sait maintenant que $\mathbb{C}[V]^H$ n'est pas de type fini, et on va prouver :

Théorème 3.5.1. *L'algèbre d'invariants $\mathbb{C}[V]^G$ n'est pas de type fini*

Démonstration. Remarquons tout d'abord que $\mathbb{C}[V]^H = (\mathbb{C}[V]^G)^T$ où T est le tore défini dans la partie 3.1. Raisonnons par l'absurde et supposons que $\mathbb{C}[V]^G$ est de type fini.
On va montrer en utilisant le théorème 2.3.5 que dans ce cas $\mathbb{C}[V]^H = (\mathbb{C}[V]^G)^T$ est de type fini.
On définit pour $1 \leq i \leq 8$ des sous-groupes T_i (isomorphes à $\mathbb{G}_m$) de T :

$$T_i := \{(1, \ldots, 1, \lambda, 1, \ldots, \frac{1}{\lambda}) \mid \lambda \in \mathbb{C}^*\}$$

ce qui va nous permettre de décomposer l'action de T comme produit d'actions de $\mathbb{G}_m$ et donc d'appliquer le théorème 2.3.5.
Toutes les actions des T_i et de G sur $\mathbb{C}[V]$ commutent. Or pour une action de T_i sur $\mathbb{C}[V]$, il existe une $\mathbb{Z}$-graduation comme définie dans la partie 2.3. En effet, tout polynôme P dans $\mathbb{C}[V]^H$:

$$\begin{aligned} P &= \sum_{k,l,k',l' \in \mathbb{N}} f_{k,l,k',l'}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_8, t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_8) x_i^k t_i^l x_9^{k'} t_9^{l'} \\ &= \sum_{n \in \mathbb{Z}} \sum_{k+l-k'-l'=n} f_{k,l,k',l'}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_8, t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_8) x_i^k t_i^l x_9^{k'} t_9^{l'} \end{aligned}$$

qui nous donne bien une $\mathbb{Z}$-graduation sur $\mathbb{C}[V]$ pour l'action de T_i, avec les notations de la partie 2.3 :

$$\mathbb{C}[V] = \bigoplus_{n\in\mathbb{Z}} \mathbb{C}[V]_n$$

Puisque toutes les actions sont des morphismes d'algèbre et qu'elles commutent on en déduit que : si on fixe i et $i_1, \ldots, i_k$ distincts deux à deux et distincts de i :

$$(\mathbb{C}[V]^{GT_{i_1}\ldots T_{i_k}})_n = ((\mathbb{C}[V])_n)^{GT_{i_1}\ldots T_{i_k}}$$

et :

$$\mathbb{C}[V]^{GT_{i_1}\ldots T_{i_k}} = \bigoplus_{n\in\mathbb{Z}} (\mathbb{C}[V]^{GT_{i_1}\ldots T_{i_k}})_n$$

puisque les actions stabilisent les espaces propres. On a donc une $\mathbb{Z}$-graduation pour toute action de $T_i \simeq \mathbb{G}_m$ sur $\mathbb{C}[V]^{GT_{i_1}\ldots T_{i_k}}$.
Puisque $\mathbb{C}[V]^G$ est supposée de type fini, on a par récurrence en appliquant le théorème 2.3.5 $\mathbb{C}[V]^{GT_1\ldots T_8}$ de type fini.
Or $\mathbb{C}[V]^{GT} = \mathbb{C}[V]^{GT_1\ldots T_8}$, en effet les T_i sont inclus dans T donc $\mathbb{C}[V]^{GT}$ est inclus dans $\mathbb{C}[V]^{GT_1\ldots T_8}$. Réciproquement si $d = (d_1, \ldots, d_8, \frac{1}{d_1\ldots d_8})$ alors pour tout P dans $\mathbb{C}[V]$ on peut décomposer l'action de d comme suit :

$$d \cdot P = (d_1, 1, \ldots, 1, \frac{1}{d_1}) \cdot \ldots \cdot (1, \ldots, 1, d_8, \frac{1}{d_8}) \cdot P$$

donc $\mathbb{C}[V]^{GT_1\ldots T_8}$ est inclus dans $\mathbb{C}[V]^{GT}$.
Finalement $\mathbb{C}[V]^{GT} = \mathbb{C}[V]^H$ est de type fini, ce qui est absurde.
Donc $\mathbb{C}[V]^G$ n'est pas de type fini. □

4 Généralisation du contre-exemple à des points sur une cubique quelconque

L'objectif de cette dernière partie est d'étendre le théorème 3.5.1.
Les points P_i, $1 \leq i \leq 9$, choisis pour construire le groupe G (cf. définition 3.1.1) sont de la forme $[1 : a_i : a_i^3]$. Ils correspondent donc à des points sur la cubique d'équation affine $x = y^3$.
On prouvera deux théorèmes nécessaires, à savoir le théorème de Bézout et le théorème fondamental de Max Noether.
Ensuite, on va montrer que l'on peut choisir plus généralement les P_i sur une cubique irréductible quelconque sous une hypothèse d' *ordre* dans un groupe qui sera explicité dans la partie 4.4.

4.1 Multiplicité de l'intersection de deux courbes

Dans ce paragraphe, nous devons introduire une nouvelle notion qui précise la façon dont deux courbes planes s'intersectent. Soient C_1, C_2 deux courbes de $\mathbb{C}P^2$, *sans composantes communes*, donc si C_1 et C_2 sont les zéros respectifs de f_1 et $f_2 \in \mathbb{C}[x, y]$ dans une carte affine, alors f_1 et f_2 sont premiers entre eux, d'après 4.2.6.

Définition 4.1.1. On définit la multiplicité de l'intersection en un point P par :

$$\text{mult}(P; C_1, C_2) = \dim O_P/(f_1, f_2)_P$$

où O_P désigne l'anneau local $S^{-1}\mathbb{C}[x, y]$, avec S la partie multiplicative des polynômes ne s'annulant pas en P, ou encore $O_P = \mathbb{C}[x, y]_{(x-a,y-b)}$ si $P = (a, b)$.
Et $(f_1, f_2)_P$ désigne l'idéal engendré par f_1 et f_2 dans O_P.

Remarque 4.1.2. Le fait de localiser au point P revient à regarder les germes de fonctions définies en P. En quotientant par l'idéal (f_1, f_2) on regarde les fonctions définies sur l'intersection $C_1 \cap C_2$. Donc l'espace vectoriel $O_P/(f_1, f_2)_P$ représente les germes de fonctions en P définies sur l'intersection. On voit donc que si l'intersection est "franche", il s'agit des fonctions définies en un point, donc un espace vectoriel de dimension 1.

Remarque 4.1.3. En fait $O_P/(f_1, f_2)_P = (\mathbb{C}[x, y]/(f_1, f_2))_P$: les opérations de quotientage et localisation commutent.

Regardons maintenant quelques propriétés liées à cette définition, résumées dans la proposition suivante :

Proposition 4.1.4. *(1) mult$(P; C_1, C_2) \geq 1$ si et seulement si $P \in C_1 \cap\ C_2$*

(2) Si C_2' représente les zéros de $f_2 + hf_1$, avec $h \in \mathbb{C}[x, y]$ quelconque, alors mult$(P; C_1, C_2') =$ mult$(P; C_1, C_2)$.

(3) Si $f_2 = gh$ et que C_2', C_2'' sont les courbes associées aux polynômes g et h, alors mult$(P; C_1, C_2) =$ mult$(P; C_1, C_2') +$ mult$(P; C_1, C_2'')$.

Démonstration. Montrons (1) :

$$\begin{aligned} P \in C_1 \cap\ C_2 &\Leftrightarrow f_1(P) = f_2(P) = 0 \\ &\Leftrightarrow \forall f \in (f_1, f_2), f \text{ n'est pas inversible dans le localisé } O_P \\ &\Leftrightarrow (f_1, f_2)_P \text{ ne contient pas d'inversible de } O_P \\ &\Leftrightarrow (f_1, f_2)_P \neq O_P \\ &\Leftrightarrow O_P/(f_1, f_2)_P \neq \{0\}. \end{aligned}$$

Comme $(f_1, f_2 + hf_1) = (f_1, f_2)$, le point (2) est clair.
Pour montrer (3), dans la cas où f_1 a une composante commune avec g ou g, l'égalité donne $\infty = \infty$ et est trivialement vérifiée. Regardons le cas où f_1 est premier avec h et g. Il suffit de voir qu'on a une suite exacte courte :

$$0 \to O_P/(f_1, h)_P \xrightarrow{*g} O_P/(f_1, gh)_P \xrightarrow{\pi} O_P/(f_1, g)_P \to 0$$

où $*g$ est définie par $*g(\bar{z}) = \bar{g}z$.
$*g$ est injective : Soit $z \in O_P$ tel que $*g(\bar{z}) = 0$. Il existe donc u et $v \in O_P$ tels que $gz = uf_1 + vgh$. On choisit $s \in \mathbb{C}[x,y]$ tel que $s(P) \neq 0, su = a, sv = b, sz = c$, avec $a, b, c \in \mathbb{C}[x,y]$ (on multiplie par les dénominateurs). On obtient $gc = af_1 + bgh$ dans $\mathbb{C}[x,y]$, donc g divise af_1, or g et f_1 sont premiers entre eux. Donc g divise a. Ainsi $c = (\frac{a}{g})f_1 + bh \in (f_1, h)$. Donc $z = \frac{c}{s} = (\frac{a}{q})(\frac{f_1}{s}) + (\frac{b}{s})h \in (f_1, h)_p$, et donc $\bar{z} = 0$.
π est une projection donc elle est surjective.
$Im(*g) = Ker(\pi)$: Il est clair que $\pi \circ *g = 0$ donc $\mathrm{Ker}(\pi) \subseteq \mathrm{Im}(*g)$.
Soit $z \in O_P$ tel que $\pi(\bar{z}) = 0$. Alors il existe $a, b \in O_P$ tels que $z = af_1 + bg$. Donc $\bar{z} = \bar{b}g$. Ainsi $\bar{z} = (*g)(b)$ et $\bar{z} \in \mathrm{Im}(*g)$.
Le fait que cette suite soit exacte implique que :
$\dim O_P/(f_1, gh)_P = \dim O_P/(f_1, h)_P + \dim O_P/(f_1, g)_P$. □

Exemple 4.1.5. Soit $f = y$ et $g = y - x^2$, et $P = (0,0)$. On veut calculer $\mathrm{mult}(P; C_1, C_2)$, où C_1 et C_2 sont les courbes associées à f et g.
Regardons l'application : $\begin{array}{ccccc} \Phi & : & \mathbb{C}^2 & \to & O_P/(f,g)_P \\ & & (a,b) & \mapsto & \overline{ax+b} \end{array}$, Φ est surjective :
Soit $F \in O_P/(f,g)_P$, alors F s'écrit :

$$\begin{aligned} F &= \frac{\overline{A(x)}}{\overline{B(x)}} = \frac{ax+b}{1+cx} \text{ car } B(0) \neq 0 \text{ et on peut multiplier en haut et en bas par un scalaire} \\ &= \frac{1-cx}{1-cx}\frac{ax+b}{1+cx} = \frac{(a-bc)x+b}{1-c^2x^2} \\ &= (a-bc)x + b. \end{aligned}$$

Ainsi $F \in \mathrm{Im}(\Phi)$.
Φ est injective :
Si $\overline{ax+b} = \overline{cx+d}$ alors $ax + b = cx + d + yP + (y - x^2)Q$. Pour des raisons de degré, $P = Q = 0$. Donc $a = c$ et $b = d$.
Conclusion : $\mathrm{mult}(P; C_1, C_2) = \dim O_P/(f,g)_P = 2$.

Exemple 4.1.6. *Multiplicité de l'intersection d'une courbe et d'une droite :*
Soit f une droite et g une courbe de $\mathbb{C}P^2$ s'intersectant en un point P. En choisissant le bon repère du plan projectif, on peut supposer que $P = (0,0)$ et $f(x,y) = x$. On peut aussi écrire $g(0,y) = y^r h(y)$, avec $r \geq 1$ car g est nulle en 0, et $h(0) \neq 0$. Alors :
$\mathrm{mult}(P; f, g) = \mathrm{mult}(0; x, y^r h(y))$ car tous les termes faisant apparaitre x dans $g(x,y)$ sont dans l'idéal engendré par x. Donc
$\mathrm{mult}(P; f, g) = \mathrm{mult}(0; x, y^r) + \underbrace{\mathrm{mult}(0; x, h(y))}_{=0 \text{ car } h(0)\neq 0} = r$. En particulier, si f est la tangente au point P de g, alors dans le repère choisit, l'équation de g sera : $g(x,y) = x + ax^2 + by^2 + cxy + \cdots$. Et donc $r \geq 2$.
Ainsi, la multiplicité entre une courbe et sa tangente en un point est supérieure ou égale à deux.

On prouve une autre propriété qui servira pour le théorème 4.5.1 final :

Proposition 4.1.7. *Soient C_1 et C_2 deux courbes de multiplicité respectivement 1 et m en un point P. Alors : mult$(P; C_1, C_2) \geq m$.*

Démonstration. On peut quitte à faire un changement de variables se ramener à $P = (0,0)$. Les équations f_1 et f_2 associées à C_1 et C_2 n'ont donc dans leur décomposition en polynômes homogènes que des polynômes de degré respectivement ≥ 1 et $\geq m$. Notons g le polynôme homogène de plus petit degré de f_1. Pour $0 \leq k \leq m-1$, notons F_k un polynôme homogène de degré k non divisible par g (on peut en trouver car g est de degré strictement positif). Dans $(\mathbb{C}[x,y]/(f_1, f_2))_{(0,0)}$ la famille des $\frac{F_k}{1}$ est libre : soient $a_k \in \mathbb{C}$ tels que :

$$0 = \sum a_k \frac{F_k}{1} = \frac{\sum a_k F_k}{1}$$

Alors il existe u tel que $u(0,0) \neq 0$ et $a, b \in \mathbb{C}[x,y]$ tels que :

$$u \sum a_k F_k = af_1 + bf_2$$

Notons k_0 le plus petit k tel que $a_k \neq 0$. Alors

$$u(0,0) a_{k_0} F_{k_0} = \alpha(x,y) g$$

par unicité de la décomposition en somme de polynômes homogènes. C'est absurde. La famille est donc libre, $\text{mult}(P; C_1, C_2) \geq m$. □

4.2 Théorème de Bézout

Pour prouver les théorèmes de Bézout et Max Noether, on aura besoin de résultats sur les modules de longueur finie :

Définition 4.2.1. Soit A un anneau. On dit qu'un A-module M est simple si il ne contient pas de sous-module non trivial.

Remarque 4.2.2. Dans ce cas, soit $m \in M$ différent de 0. Alors $A \cdot m = M$ donc $M \simeq A/I$ où I est un idéal maximal sans quoi A/I aurait des sous-modules stricts. En particulier M a une structure de corps induite par le choix de m dans M.

Définition 4.2.3. On dit qu'un A-module M est de longueur finie s'il existe une suite finie de sous-modules M_i tels que $M_0 = M$ et $M_n = 0$ et pour tout $0 \leq i \leq n-1$ $M_{i+1} \subset M_i$ et M_i/M_{i+1} est simple.

Exemple 4.2.4. Un espace vectoriel de dimension finie est un module de longueur finie.

Proposition 4.2.5. *Si M est un A-module de longueur finie, on a la somme finie :*

$$M \simeq \bigoplus_{\mathfrak{p}\ maximal} M_{\mathfrak{p}}$$

où $M_{\mathfrak{p}}$ désigne le module localisé en $\mathfrak{p}$.

Démonstration. La démonstration se fait par récurrence sur la longueur de M. Supposons M de longueur 1. Fixons $m \in M$ non nul, l'application :

$$\begin{array}{rccc} \pi_m & : & A & \to & M \\ & & \lambda & \mapsto & \lambda \cdot m \end{array}$$

est surjective car le module est simple. Notons I son noyau. Alors I est maximal sans quoi on aurait des sous-modules non triviaux de $A/I \simeq M$. Considérons l'application canonique :

$$\begin{array}{rccc} \psi & : & M & \to & M_I \\ & & m' & \mapsto & \frac{m'}{1}. \end{array}$$

C'est un isomorphisme de modules : elle est injective car $\frac{m'}{1} = 0$ si et seulement si il existe $\lambda \in A - I$ tel que $\lambda \cdot m' = 0$. Or si $m' \neq 0$, il existe $\lambda' \in A - I$ tel que $\lambda' m = m'$ soit $\lambda\lambda' m = 0$ ce qui est absurde car puisque I est maximal, $\lambda\lambda' \in A - I$. L'application canonique est également surjective : pour tout $\beta \in A$, pour tout $\lambda \in A - I$ on veut trouver $\alpha \in A$ tel que $\frac{\alpha m}{1} = \frac{\beta m}{\lambda}$. Or A/I est un corps donc il existe $\alpha \in A$ tel que $\alpha\lambda = \beta + i$ où $i \in I$, ce qu'on voulait.
Considérons un autre idéal maximal I'. Alors $M_{I'} = 0$, car il existe $x \in I - I'$ donc pour tout $m' \in M$ et pour tout $\lambda \in A - I'$, $\frac{m'}{\lambda} = \frac{0}{x} = 0$. On a donc bien : $M \simeq \bigoplus M_{\mathfrak{p}}$ et ce par le morphisme canonique entre M et $M_{\mathfrak{p}}$. De plus on remarque bien que la somme est finie, ce qui amorce la récurrence.
Maintenant si M est de longueur finie, il existe un sous-module N de longueur strictement inférieure tel que M/N est simple. On remarque tout d'abord que pour tout idéal maximal $\mathfrak{p}$ de A, on a un morphisme canonique entre M et $M_{\mathfrak{p}}$ donné par $\psi : m \mapsto \frac{m}{1}$. On a de plus une suite exacte :

$$0 \to N_{\mathfrak{p}} \to M_{\mathfrak{p}} \to (M/N)_{\mathfrak{p}} \to 0$$

En effet, un morphisme de A-modules ϕ entre B et C peut se "prolonger" en un morphisme $\phi_{\mathfrak{p}}$ de A-modules entre les modules localisés, en posant simplement $\phi_{\mathfrak{p}}(\frac{m}{\lambda}) := \frac{\phi(m)}{\lambda}$, et c'est chose facile que de vérifier que cela définit bien une application et que c'est un morphisme de modules. Ce prolongement donne le diagramme commutatif suivant :

$$\begin{array}{ccc} B & \xrightarrow{\phi} & C \\ {\scriptstyle \psi_B}\downarrow & & \downarrow{\scriptstyle \psi_C} \\ B_{\mathfrak{p}} & \xrightarrow[\phi_{\mathfrak{p}}]{} & C_{\mathfrak{p}} \end{array}$$

où ψ_B et ψ_C sont les morphismes canoniques entre les modules et leur localisé. De plus, on a les deux relations suivantes :

$$(\mathrm{Ker}(f))_{\mathfrak{p}} = \mathrm{Ker}(f_{\mathfrak{p}})$$
$$(\mathrm{Im}(f))_{\mathfrak{p}} = \mathrm{Im}(f_{\mathfrak{p}}).$$

En effet, $f_{\mathfrak{p}}(\frac{m}{\lambda}) = 0$ implique qu'il existe $s \in A - \mathfrak{p}$ tel que $sf(m) = 0$. Donc $sm \in \mathrm{Ker}(f)$, donc $\frac{m}{\lambda} \in (\mathrm{Ker}(f))_{\mathfrak{p}}$. L'inclusion réciproque étant évidente, ainsi que la relation sur les images.
On en déduit donc que la localisation transforme une suite exacte en une suite exacte : si

$$N \xrightarrow{f} M \xrightarrow{g} P$$

est une suite exacte, alors $\mathrm{Ker}(g) = \mathrm{Im}(f)$. Or $\mathrm{Im}(f_{\mathfrak{p}}) = (\mathrm{Im}(f))_{\mathfrak{p}} = (\mathrm{Ker}(g))_{\mathfrak{p}} = \mathrm{Ker}(g_{\mathfrak{p}})$, donc

$$N_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} M_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} P_{\mathfrak{p}}$$

est exacte.
On a un morphisme entre M et la somme finie $\bigoplus_{\mathfrak{p}} M_{\mathfrak{p}}$. Celle-ci est bien finie par récurrence, car par hypothèse de récurrence il n'y a qu'un nombre fini de $\mathfrak{p}$ maximaux tels que $N_{\mathfrak{p}}$ et $(M/N)_{\mathfrak{p}}$ soient non nuls. Et pour les autres, l'exactitude de la suite :

$$0 \to 0 = N_{\mathfrak{p}} \to M_{\mathfrak{p}} \to (M/N)_{\mathfrak{p}} = 0 \to 0$$

nous donne que $M_{\mathfrak{p}} = 0$, donc la somme est finie.
Cela nous donne finalement une suite exacte sur les sommes finies :

$$0 \to \bigoplus_{\mathfrak{p}} N_{\mathfrak{p}} \to \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}} \to \bigoplus_{\mathfrak{p}} (M/N)_{\mathfrak{p}} \to 0$$

On en déduit le diagramme commutatif (commutatif car la localisation des morphismes de modules était commutative avec les morphismes canoniques entre le module et son localisé) suivant où les suites du haut et du bas sont exactes et où la première et la dernière flèche descendantes sont des isomorphismes par récurrence :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus N_{\mathfrak{p}} & \longrightarrow & \bigoplus M_{\mathfrak{p}} & \longrightarrow & \bigoplus (M/N)_{\mathfrak{p}} & \longrightarrow & 0 \end{array}$$

Ceci nous donne le diagramme commutatif suivant où les suites en haut et en bas sont exactes :

$$\begin{array}{ccccccc} & & & & M & & & & \\ & & & {\scriptstyle i}\nearrow & & \searrow{\scriptstyle p} & & & \\ 0 & \longrightarrow & N & & {\scriptstyle \phi}\downarrow & & M/N & \longrightarrow & 0 \\ & & & {\scriptstyle j}\searrow & & \nearrow{\scriptstyle q} & & & \\ & & & & \bigoplus M_{\mathfrak{p}} & & & & \end{array}$$

Montrons que cela implique que ϕ est un isomorphisme. Tout d'abord, $\mathrm{Ker}(q \circ \phi) = i(N)$ donc $\mathrm{Ker}(\phi) \subset N$ or $\phi \circ i = j$ donc $\phi \circ i$ injective, donc $\mathrm{Ker}(\phi) = 0$. De plus, si ϕ n'était pas surjective, il existerait x dans $\bigoplus M_{\mathfrak{p}} - \mathrm{Im}(\phi)$. Montrons qu'alors $q(x)$ n'est pas atteint par $q \circ \phi$ ce qui contredira $q \circ \phi = p$ surjective. On a $\mathrm{Ker}(q) = \phi(i(N))$, or les y tels que $q(y) = q(x)$ s'écrivent $x = y + h$ où $h \in \mathrm{Ker}(q)$. Or si un tel y est dans $\mathrm{Im}(\phi)$, alors $y + h$ est dans $\mathrm{Im}(\phi)$ ce qui contredit le fait que x ne soit pas dans $\mathrm{Im}(\phi)$. Ce qui achève la démonstration de la proposition. □

Pour prouver le théorème de Bézout nous aurons encore besoin d'un résultat reliant divisibilité et intersection de courbes :

Lemme 4.2.6. *Soient $A, B \in \mathbb{C}[x, y]$ deux courbes. Alors les trois propriétés suivantes sont équivalentes :*

(a) A, B sont premières entre elles dans $\mathbb{C}[x, y]$

(b) A, B n'ont pas de composante commune

(c) $A \cap B$ est finie

Démonstration. Il est tout d'abord évident que (c) implique (b) et que (b) implique (a) car si A et B ne sont pas premières entre elles, alors elles sont divisées par un polynôme de degré strictement positif de $\mathbb{C}[x, y]$ et ont donc une composante commune.
Réciproquement, raisonnons par l'absurde et supposons que $A \cap B$ est infinie et qu'elles sont premières entre elles. Alors elles sont premières entre elles dans $\mathbb{C}(x)[y]$ et dans $\mathbb{C}(y)[x]$. En effet, prenons Q un diviseur de A et B dans $\mathbb{C}(x)[y]$. On a alors : $A = A'Q$ et $B = B'Q$. En multipliant par les dénominateurs des coefficients de A', B' et Q vu comme polynômes de $\mathbb{C}(x)[y]$, on obtient deux relations : $F(x)A(x, y) = A''(x, y)q(x, y)$ et $G(x)B(x, y) = B''(x, y)q(x, y)$. Supposons que Q soit de degré strictement positif. Alors y intervient dans q et donc si l'on regarde les décompositions en irréductibles dans $\mathbb{C}[x, y]$ (qui est un anneau factoriel), on obtient qu'il existe des facteurs irréductibles identiques dans $\mathbb{C}[x, y]$ dans les décompositions de A et B, ce qui contredit le fait que A et B soient premiers entre eux dans $\mathbb{C}[x, y]$. Donc A et B sont premiers entre eux dans $\mathbb{C}(x)[y]$ et dans $\mathbb{C}(y)[x]$. On peut donc appliquer le théorème de Bézout, en multipliant par les dénominateurs comme précédemment : il existe des polynômes non nuls $a, b, a', b' \in \mathbb{C}[x, y]$ et $c, c' \in \mathbb{C}[x]$ non nuls tels que :

$$\begin{cases} a(x, y)A(x, y) + b(x, y)B(x, y) = c(x) \\ a'(x, y)A(x, y) + b'(x, y)B(x, y) = c'(y). \end{cases}$$

Or $A \cap B$ est infinie, donc il existe au moins une infinité de x ou une infinité de y annulant A et B, ce qui est absurde puisque c et c' ont un nombre fini de racines. Donc A et B ne sont pas premières entre elles, ce qui achève la démonstration du lemme. □

Théorème 4.2.7 (Bézout)**.** *Soient C_1, C_2 deux courbes de $\mathbb{C}P^2$ de degrés d_1 et d_2 sans composante commune, alors :*

$$\sum_{P \in C_1 \cap C_2} mult(P; C_1, C_2) = d_1 d_2.$$

Démonstration. Les idées de la preuve viennent de M. Hindry [2].
Notons f_1 et f_2 les équations polynomiales associées à C_1 et C_2 dans une carte affine quelconque. On a montré que $C_1 \cap C_2$ est fini par le lemme 4.2.6, donc quitte à changer de coordonnées projectives, on peut supposer que la droite à l'infini ne rencontre pas $C_1 \cap C_2$ (la droite infinie devient donc $(X : Y : 0)$ dans ces coordonnées). Montrons que cela implique que $f_1^{(d_1)}$ et $f_2^{(d_2)}$, les parties homogènes de plus haut degré respectives de f_1 et f_2 sont premières entre elles.
En écrivant f_1 et f_2 comme des polynômes homogènes en $[X, Y, Z]$, les monômes $f_i^{(d_i)}$ ne feront pas apparaitre Z, et il existe $U, V \in \mathbb{C}[X, Y, Z]$ tels que :
$f_1(X, Y, Z) = f_1^{(d_1)}(X, Y, Z) + ZU(X, Y, Z)$
$f_2(X, Y, Z) = f_2^{(d_2)}(X, Y, Z) + ZV(X, Y, Z)$.
Pour tout point $(X : Y : 0)$ de la droite infinie, on a $f_1(X, Y, 0) \neq 0$ ou $f_2(X, Y, 0) \neq 0$. Ainsi pour tout $(x, y) \in \mathbb{C}^2$, $f_1^{(d_1)}(x, y) \neq 0$ ou $f_2^{(d_2)}(x, y) \neq 0$.
Supposons qu'il existe un diviseur commun à $f_1^{(d_1)}$ et $f_2^{(d_2)}$, alors si (x, y) est un zéro de ce diviseur, il annule les $f_i^{(d_i)}$, ce qui est absurde, donc $f_1^{(d_1)}$ et $f_2^{(d_2)}$ sont premiers entre eux.

En reprenant les notations du paragraphe 3.3, on a A_d, l'ensemble des polynômes de $\mathbb{C}[x,y]$ de degré $\leq d$, qui est de dimension $N_d = \binom{d+1}{2}$.

L'application de $A_d \xrightarrow{\phi} \mathbb{C}[x,y]/(f_1,f_2)$ est surjective pour d assez grand. En effet, les polynômes c et c' dans 4.2 peuvent être choisis unitaires, et si on note r et r' leurs degrés, on a une relation entre x^r et les puissances inférieures de x, dans le quotient $\mathbb{C}[x,y]/(f_1,f_2)$, et de même pour y. Ainsi le degré des polynômes de $\mathbb{C}[x,y]/(f_1,f_2)$ est majoré par $r+r'-2$. Donc en prenant $d \geq r+r'-2$, l'application ϕ sera bien surjective.
Son noyau est $B_d = A_d \cap (f_1,f_2)$ et contient $I_d := A_{d-d_1}f_1 + A_{d-d2}f_2$. Montrons que $I_d = B_d$, lorsque $d \geq d_1 + d_2$.
On prend $f = g_1f_1 + g_2f_2 \in B_d$, en supposant que les degrés e_1 et e_2 de g_1 et g_2 sont minimaux pour une telle écriture. On veut montrer que $e_1 \leq d - d_1$ et $e_2 \leq d - d_2$.
Supposons par exemple que $e_1 > d - d_1$. Considérons les parties homogènes de plus haut degré, nécessairement $e_1 + d_1 = e_2 + d_2$ et $g_1^{(e_1)}f_1^{(d_1)} + g_2^{(e_2)}f_2^{(d_2)} = 0$ car $\deg f \leq d$.
Ainsi $f_1^{(d_1)}$ divise $g_2^{(e_2)}f_2^{(d_2)}$. Or, on a montré que $f_1^{(d_1)}$ et $f_2^{(d_2)}$ sont premiers entre eux, donc il existe h tel que $f_1^{(d_1)}h = g_2^{(e_2)}$. En remplaçant dans l'égalité précédente, on obtient $g_1^{(e_1)}f_1^{(d_1)} + f_1^{(d_1)}hf_2^{(d_2)} = 0$, donc $g_1^{(e_1)} = -hf_2^{(d_2)}$.
Ainsi $f = f_1(g_1 + f_2h) + f_2(g_2 - f_1h)$ donne une autre écriture de f, avec $\deg(g_1 + f_2h) < e_1$, ce qui contredit la minimalité de e_1.
On a donc montré que $e_1 \leq d - d_1$ et $e_2 \leq d - d_2$, et donc que $f \in I_d$.
Ainsi, pour d assez grand, on a :

$$A_d/I_d \cong \mathbb{C}[x,y]/(f_1,f_2) \tag{4}$$

De plus $A_{d-d_1}f_1 \cap A_{d-d_2}f_2 = A_{d-d_1-d_2}f_1f_2$.
En effet, l'inclusion de droite à gauche est claire, et si $f \in A_{d-d_1}f_1 \cap A_{d-d_2}f_2$, alors $f = g_1f_1 = g_2f_2$. Donc f_1 divise g_2 (car f_1 et f_2 sont premiers entre eux). On peut écrire $g_2 = hf_1$,avec $\deg h \leq d - d_1 - d_2$. Et donc : $f = hf_1f_2 \in A_{d-d_1-d_2}f_1f_2$.
Exprimons (4) en terme de dimensions :

$$\begin{aligned}
\dim \mathbb{C}[x,y]/(f_1,f_2) &= \dim A_d/I_d = \dim A_d - \dim A_{d-d_1}f_1 - \dim A_{d-d_2}f_2 + \dim A_{d-d_1-d_2}f_1f_2 \\
&= N_d - N_{d-d_1} - N_{d-d_2} + N_{d-d_1-d_2} \\
&= \binom{d+2}{2} - \binom{d-d_1+2}{2} - \binom{d-d_2+2}{2} + \binom{d-d_1-d_2+2}{2} \\
&= d_1d_2
\end{aligned}$$

On sait donc maintenant que $\dim \mathbb{C}[x,y]/(f_1,f_2) = d_1d_2$. Il suffit donc de montrer que

$$\dim \mathbb{C}[x,y]/(f_1,f_2) = \sum_{P \in C_1 \cap C_2} \mathrm{mult}(P; C_1, C_2)$$

Or cela est une conséquence de la proposition 4.2.5 appliquée au $\mathbb{C}[x,y]$-module $\mathbb{C}[x,y]/(f_1,f_2)$ vu comme un $\mathbb{C}$-espace vectoriel. En effet, un $\mathbb{C}[x,y]$-module qui est un $\mathbb{C}$-espace vectoriel de dimension finie est de longueur finie, ce qui se prouve par récurrence sur la dimension de l'espace vectoriel. Si la dimension est 1 alors il n'existe pas de sous-espace vectoriel strict donc a fortiori pas de sous-$\mathbb{C}[x,y]$-module strict. Si la dimension est supérieure à 1 : si l'espace n'admet pas de sous-module strict, alors il est simple et c'est fini. Sinon il admet un sous-module strict, qui sera en particulier un sous-espace vectoriel de dimension strictement inférieure et on peut donc appliquer la récurrence au sous-module strict et au sous-module quotient. De plus les idéaux maximaux de $\mathbb{C}[x,y]$ sont les $\mathfrak{p} = (X-a, Y-b)$ où $a,b \in \mathbb{C}$. Ce qui achève la preuve du théorème de Bézout. □

4.3 Théorème fondamental de Max Noether

On présente ici un autre résultat sur les courbes algébriques qui sera utilisé dans la généralisation à une cubique quelconque.

Théorème 4.3.1 (Max Noether)**.** *Soient F, G et H des courbes algébriques telles que F et G n'ont pas de composantes communes,* $\deg H - \deg F > 0$ *et* $\deg H - \deg G > 0$*. Alors on a l'équivalence suivante :*

(i) Pour tout $P \in F \cap G, h \in (f,g)_P$*, avec* f, g *et* h *les polynômes de* $\mathbb{C}[x,y]$ *associés à* F, G *et* H*.*

(ii) Il existe $a, b \in \mathbb{C}[x,y]$ *tels que* $h = af + bg$*, avec* $\deg a = \deg h - \deg f$ *et* $\deg b = \deg h - \deg g$*.*

Remarque 4.3.2. (ii) signifie que $h \in (f,g)$ dans $\mathbb{C}[x,y]$. Il s'agit d'une condition globale ; alors que (i) concerne des conditions locales.

Démonstration. Si $h = af + bg$ alors cette égalité reste vraie dans O_P, pour tout $P \in F \cap G$. Donc $(ii) \Rightarrow (i)$ est claire.
Supposons maintenant que les conditions (i) sont vérifiées. Alors pour tout $P \in F \cap G$, h, la classe de h dans le quotient $O_P/(f,g)_P$ est nulle. or, comme on l'a vu dans la preuve du théorème de Bézout

$$\mathbb{C}[x,y]/(f,g) \xrightarrow{\sim} \bigoplus_{P \in F \cap G} O_P/(f,g)_P.$$

Ainsi la classe de h est nulle dans le quotient $\mathbb{C}[x,y]/(f,g)$, ce qui signifie qu'il existe $a, b \in \mathbb{C}[x,y]$ tels que $h = af + bg$. Les monômes de a de degré strictement supérieur à $\deg h - \deg f$ vont se simplifier avec des termes du produit bg (provenant nécessairement de monômes de b de degré strictement supérieur à $\deg h - \deg g$), donc on peut supposer que $\deg a = \deg h - \deg f$ et $\deg b = \deg h - \deg g$. □

4.4 Lois de groupes sur les courbes cubiques

Les courbes dites *cubiques* sont des courbes du plan projectif $\mathbb{C}P^2$ définies par un polynôme homogène de degré 3.

Définition 4.4.1. Une cubique est dite *irréductible* si le polynôme dont elle représente les zéros est irréductible.

Définition 4.4.2. On dit qu'un point de C est *régulier* si la tangente à la courbe en ce point est définie. Si $F(X,Y,Z) = 0$ est l'équation de C, cela revient à dire que $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}) \neq 0$.

On peut trouver une structure de groupe sur l'ensemble des points réguliers d'une cubique.

Définition 4.4.3. Soit P et Q deux points réguliers distincts de la cubique C. La droite qui relie P et Q coupe la cubique en 3 points (avec multiplicités éventuelles), d'après le théorème de Bézout 4.2.7. Il existe donc un troisième point R dans l'intersection de C avec la droite. On notera $R = P \circ Q$.
Si les deux points choisis sont confondus, la tangente à la courbe en ce point intersecte C avec une multiplicité au moins 2 (voir l'exemple 4.1.6), encore par théorème de Bézout, il existe un troisième point R dans l'intersection (qui peut être égal à P aussi), on notera encore $R = P \circ P$. On fixe une origine quelconque O parmi les points réguliers, et on pose $O' := O \circ O$. la loi est alors définie par :

$$P + Q := O \circ (P \circ Q) \quad \text{et} \quad -P := O' \circ P.$$

Proposition 4.4.4. *Si* C *est irréductible, on a ainsi défini une loi de groupe abélien sur l'ensemble des points réguliers de* C*.*

Démonstration. Loi interne :
Il faut commencer par montrer que la somme de deux points réguliers est bien un point régulier. Pour cela il suffit de montrer que pour toute droite intersectant la cubique en deux points réguliers, le troisième point d'intersection est régulier.
Supposons qu'il existe R et Q deux points réguliers distincts de C telle que la droite L qu'ils définissent intersecte C en un troisième point P, non régulier. D'après le théorème de Bézout, la multiplicité de l'intersection entre la droite et C est 1 en P. Or, comme P est irrégulier $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}) = 0$ en P. Donc si on se place dans une carte telle que $P = (0,0)$ et L est la droite $x = 0$, alors $F(x,y) = ax^2 + by^2 + cxy + dx^3 + \cdots$. Donc $\text{mult}(P; L, C) \geq 2$, comme dans l'exemple 4.1.6. Ceci est absurde.
Si les deux points sont confondus, et L est la tangente en ce point R à C, comme on l'a vu dans l'exemple 4.1.6, la multiplicité de l'intersection entre L et C en R est ≥ 2. Donc L ne peut pas

intersecter C en un point irrégulier,en plus de R, comme précédemment, car la multiplicité de cette intersection serait de 1.
Ainsi la loi + définie sur l'ensemble des points réguliers de C est bien une loi de composition interne.
Élément neutre :

$$P + O = O \circ (P \circ O) = P = O \circ (O \circ P) = O + P$$

En effet, la droite passant par O et P coupe C en un troisième point R. C'est la même droite qui passa par O et R et le troisième point d'intersection est donc P.
Symétrique :

$$P + (-P) = O \circ (P \circ -P) = O \circ (\underbrace{P \circ (O' \circ P)}_{=O'}) = O \circ (O \circ O) = O.$$

$$(-P) + P = O \circ (-P \circ P) = O \circ (\underbrace{(O' \circ P) \circ P}_{=O'}) = O \circ (O \circ O) = O.$$

Commutativité :
Clairement pour tous points P et Q, $P \circ Q = Q \circ P$, la commutativité pour + en découle.
Associativité :
Montrer que cette loi est associative est plus compliqué, c'est là que l'irréductibilité de C est nécessaire. On utilisera deux lemmes explicités dans la suite.
(Pour cette démonstration, on renvoie le lecteur aux deux figures en annexe.) Soit P, Q et R trois points distincts de la cubique C. La droite $L_1 = (P, Q)$ coupe C en P, Q et T. La droite $L_2 = (T, O)$ coupe C en T, O et T'. La droite $L_3 = (R, T')$ coupe C en R, T' et U. Et la droite $L_4 = (U, O)$ coupe C en U, O et U', de sorte que : $(P + Q) + R = U'$.
La droite $M_1 = (Q, R)$ coupe C en Q, R et S. La droite $M_2 = (S, O)$ coupe C en S, O et S'. La droite $M_3 = (P, S')$ coupe C en P, S' et V. Et la droite $M_4 = (V, O)$ coupe C en V, O et V', de sorte que : $P + (Q + R) = V'$.
On veut montrer que $U' = V'$, et pour cela il suffit de montrer que $U = V$, ou encore $L_4 = M_4$.
On considère les cubiques $C_1 := L_1 \star M_2 \star L_3$ et $C_2 := M_1 \star L_2 \star M_3$, où $F \star G$ désigne la courbe décrivant les zéros du polynôme homogène fg, avec f et g les polynômes homogènes associés à F et G.
On a alors :

$$\begin{cases} C \cap C_1 = \{P, Q, R, O, T, T', S, S', U\} \\ C \cap C_2 = \{P, Q, R, O, T, T', S, S', V\}. \end{cases}$$

Si les points P, Q, R, O, T, T', S et S' sont distincts, le lemme 4.4.6, appliqué à C, C_1 donne bien $U = V$.
C'est le cas en général. L'égalité $(P + Q) + R = P + (Q + R)$ se prolonge par continuité dans les cas où certains points sont confondus (car la courbe est lisse en dehors du nombre fini de points singuliers). □

Lemme 4.4.5. *Soit $P_1, \ldots, P_8$ huit points distincts de $\mathbb{C}P^2$. On suppose que parmi eux il n'existe pas quatre points alignés, ni sept sur une même conique. Alors l'espace vectoriel des polynômes homogènes de degré 3 s'annulant en $P_1, \ldots, P_8$ est de dimension 2.*

Démonstration. Notons n la dimension cherchée. L'espace vectoriel des polynômes homogènes de degré 3 est de dimension 10, car $\{XYZ, XY^2, XZ^2, YX^2, YZ^2, ZX^2, ZY^2, X^3, Y^3, Z^3\}$ en est une base. Comme on l'a vu dans la partie 3.3, les conditions d'annulation en des points distincts sont linéaires et indépendantes. Donc $n \geq 10 - 8 = 2$.
Si P_1, P_2, P_3 sont alignés, on choisit P_9 sur la même droite et on note $L(X, Y, Z)$ son équation. Toute cubique F passant par $P_1, \ldots, P_9$ intersecte la droite définie par L en au moins quatre points, d'après le théorème de Bézout 4.2.7 F et L ont une composante commune. Donc il existe Q tel que $F = LQ$, d'après le lemme 4.2.6. Nécessairement Q passe par $P_4, \ldots, P_8$ (L ne peut passer par aucun de ces points dans les huit points de départ il n'y en a pas quatre qui soient alignés).

Montrons que par cinq points dont quatre ne sont pas alignés il ne passe qu'une conique.
Supposons trois des points soient alignés, par exemple P_4, P_5, P_6. Alors la conique contient nécessairement la droite D définie par ces trois points (par théorème de Bézout). On a alors : $S_2(P_4, \dots, P_8) = LS_1(P_7, P_8)$, où $S_d(Q_1, \dots, Q_r)$ désigne l'espace des polynômes homogènes de degré $\leq d$ s'annulant en $Q_1, \dots, Q_r$, car ni P_7 ni P_8 n'est sur L.
Or, il n'y qu'une droite passant par P_7 et P_8, donc $\dim S_1(P_7, P_8) = 1$. Ainsi $\dim S_2(P_4, \dots, P_8) = 1$, ce qui correspond au résultat cherché.
Traitons maintenant le cas où aucun triplet de $P_4, \dots, P_8$ n'est aligné, et supposons que $\dim S_2(P_4, \dots, P_8) > 1$. On choisit P_9' sur le droite D définie par P_7, P_8. L'annulation d'un polynôme en P_9' correspond à l'appartenance au noyau d'une forme linéaire sur $S_2(P_4, \dots, P_8)$, donc $\dim S_2(P_4, \dots, P_9') \geq 1$. Or une telle conique contient les trois points aligné P_7, P_8, P_9, donc nécessairement la droite entière. C'est donc le produite de deux droites D et D', et comme ni P_4 ni P_5 ni P_6 ne sont sur D, ils sont tous sur D' et donc alignés. Ceci contredit l'hypothèse faite et on a donc le résultat.

Soit donc Q_0 le polynôme associé à l'unique cubique passant par $P_4, \dots, P_8$, et F est un multiple de LQ_0. Ainsi la dimension n_0 de l'espace des cubiques passant par $P_1, \dots, P_9$ est égale à 1. Or $n \leq n_0 + 1 = 2$, donc on a bien $n = 2$.
On suppose maintenant que $P_1, \dots, P_6$ soit sur une même conique d'équation $Q = 0$, et on choisit P_9 sur cette conique. Toute cubique F s'annulant sur $P_1, \dots, P_9$, intersecte la cubique en 7 points, donc d'après le théorème de Bézout, elles ont une composante commune. Si cette composante était une droite D, on aurait $F = DC$, où C est une cubique et $Q = DT$, où T est une droite. Or D contient au maximum trois des six points $P_1, \dots, P_6$, donc C en contient au moins trois, ces trois points étant aussi sur D. Donc Card $C \cap T \geq 3$, et T divise C : $C = TL$. Donc $F = DC = DTL = QL$. Dans tous les cas, Q divise F.
De plus la droite L passe par P_7 et P_8 car aucun de ces points ne peut appartenir à la cubique Q. La dimension n_0 de l'espace des cubiques passant par $P_1, \dots, P_9$ est donc égale à 1. Ainsi $n \leq n_0 + 1 = 2$. Donc $n = 2$.
Passons au cas général : aucun triplet de points alignés, aucun sextuplet coconique. On choisit P_9 et P_{10} sur la droite $(P_1, P_2$ d'équation $L = 0$. Supposons que $n \geq 3$, le fait qu'une cubique passant par $P_1, \dots, P_8$ passe aussi par P_9 et P_{10} correspond à l'appartenance à l'intersection de deux formes linéaires. Donc $\dim S_3(P_1, \dots, P_{10}) \geq \dim S_3(P_1, \dots, P_8) - 2 \geq 1$. Donc il existe une cubique F passant par $P_1, \dots, P_{10}$. Alors, il y au moins quatre points (P_1, P_2, P_9, P_{10}) dans l'intersection entre F et L. D'après le théorème de Bézout, il existe Q une cubique telle que $F = LQ$. Mais alors, aucun des $P_3, \dots, P_8$ ne peut être sur L, car on aurait trois points alignés, donc tous sont sur Q. On a donc six points de $P_1, \dots, P_8$ coconiques, ceci est absurde. □

On va considérer maintenant deux cubiques C_1 et C_2, on sait par le théorème de Bézout 4.2.7 qu'il y a neufs points (avec multiplicités) dans leur intersection.

Lemme 4.4.6. *Soient $P_1, \dots, P_9$ les points d'intersections de deux cubiques C_1 et C_2 dont l'une au moins est irréductible. On suppose que $P_1, \dots, P_8$ sont distincts. Alors toute cubique C passant par $P_1, \dots, P_8$ passe aussi par P_9.*

Démonstration. Supposons par exemple C_1 irréductible. Alors, elle ne peut contenir ni quatre points alignés, ni sept points coconiques. En effet, si c'était le cas, l'intersection avec la deuxième courbe contiendrait trop de points et donc les deux courbes auraient une composante commune par Bézout. Comme le degré de la deuxième courbe est 1 ou 2, on aurait un diviseur de C_1, ce qui est absurde. Donc on peut appliquer le lemme précédent aux points $P_1, \dots, P_8$. L'espace des cubiques s'annulant sur $P_1, \dots, P_8$ est de dimension 2, donc engendré par C_1 et C_2. Ainsi, toute cubique s'annulant sur $P_1, \dots, P_8$ s'annule aussi en P_9. □

4.5 Conclusion

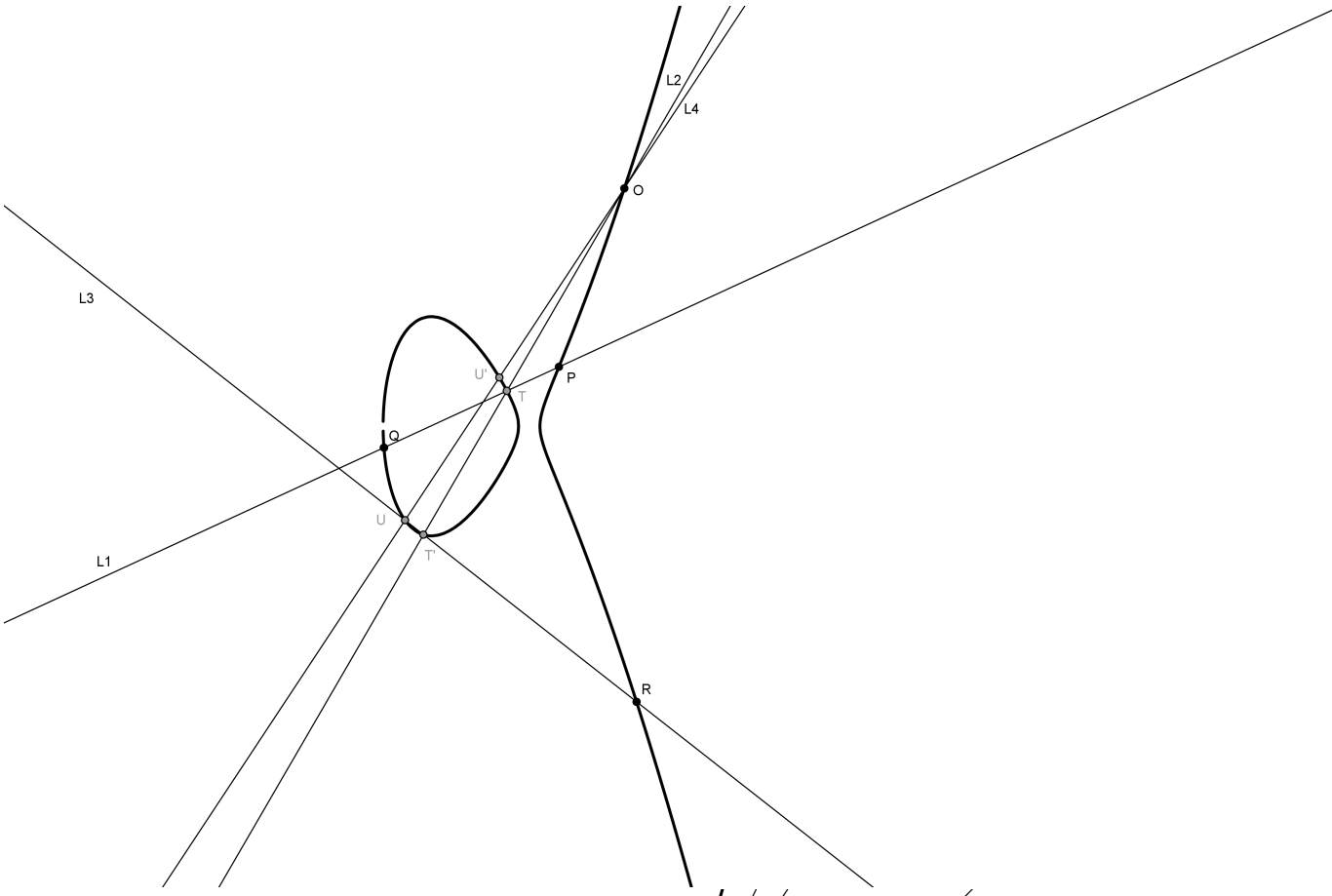
Théorème 4.5.1. *Remplaçons les $[1 : a_i : a_i^3]$, pour $1 \leq i \leq 9$, dans la définition 3.1.1 de G par neuf points réguliers P_i sur une cubique irréductible quelconque. Supposons que dans le groupe des points réguliers de la cubique, $\sum_{i=1}^{9} P_i$ ne soit pas d'ordre fini. Alors : la $\mathbb{C}$-algèbre $\mathbb{C}[V]^G$ n'est pas de type fini.*

Remarque 4.5.2. Ce résultat généralise bien le théorème 3.5.1. En effet, considérons la cubique irréductible d'équation affine $y = x^3$, et prenons pour élément neutre le point $(0, 0)$. Explicitons la loi de groupe : $(a, a^3) + (b, b^3) = (a + b, (a + b)^3)$ car par le calcul, on trouve que le troisième point d'intersection de la droite passant par (a, a^3) et (b, b^3) est de coordonnées $(-a - b, -(a + b)^3)$. Or le troisième point d'intersection de la droite passant par $(0, 0)$ et par ce point est l'opposé de ce point, d'où le résultat. On en déduit que $m \sum_{i=1}^{9} P_i = (m \sum_{i=1}^{9} a_i, (m \sum_{i=1}^{9} a_i)^3)$ donc $m \sum_{i=1}^{9} P_i = 0$ si et seulement si $\sum_{i=1}^{9} a_i = 0$. Or on avait justement choisi les a_i pour éviter ce cas.

Démonstration. On remarque tout d'abord que tous les résultats de la partie précédente ont été prouvés pour des P_i sur une cubique irréductible quelconque, mis à part le point (a) du lemme 3.3.1. En effet l'hypothèse de la partie 3.2 était que les points soient non alignés. Ce qui est le cas, puisque l'intersection d'une droite et d'une cubique est de cardinal 3 si la droite n'est pas inclue dans la cubique par théorème de Bézout, et ne peut donc contenir 9 points distincts sans que la droite soit une partie de la cubique, or celle-ci est irréductible. Les autres résultats ne dépendent pas de la cubique, ni des points P_i.
Notons C la cubique passant par les P_i. Il faut prouver que pour tout m il existe une unique courbe à multiplication par un scalaire près de degré $3m$ et de multiplicité $\geq m$ en les P_i, à savoir : C^m. On va utiliser le lemme 4.5.3 prouvé ci-dessous et on va procéder par récurrence sur m. Pour $m = 0$, le lemme est trivialement vérifié. Soit maintenant F une courbe de degré $3m$ passant par les P_i. Par récurrence, il suffit de montrer que C divise F, ce qui revient à dire que la courbe C est une composante de F, par le lemme 4.2.6 car C est irréductible. Raisonnons par l'absurde et supposons que C et F n'ont pas de composante commune (ce qui revient au même que de supposer que C n'est pas une composante de F car C est irréductible). Alors, grâce au lemme 4.1.7, on sait que l'ensemble des points d'intersection de C et F est les P_i chacun compté avec multiplicité m. En appliquant le lemme 4.5.3, car les P_i sont des points réguliers de C, on obtient que $m \sum_{i=1}^{9} P_i = 0$ dans C. Ce qui contredit l'hypothèse faite sur les P_i et achève la démonstration du théorème. □

Lemme 4.5.3. *Soit C une cubique irréductible et F une courbe de degré n, n'intersectant C qu'en des points réguliers de C. Alors les $3n$ points de $C \cap F$ sont de somme nulle dans le groupe associé à C.*

Démonstration. Raisonnons par récurrence sur le degré n de F.
Si $n = 1$, F est une courbe et par construction de la loi de groupe sur C, la somme des points de l'intersection est nulle.
Si $n \geq 2$, supposons n pair. Notons $S = F \cap C$. Alors S est constitué de $3n$ points par théorème de Bézout. Rassemblons ces points en $3n/2$ paires arbitraires. Notons G le produit des droites passant par les paires de points (si une paire de points est constituée de deux mêmes points, on prend la droite tangente à C passant par ce point). C'est une courbe de degré $3n/2$. Notons T l'ensemble des points d'intersection des droites passant par les paires de points et C. On a alors : $S \cup T = G \cap C$. Puisque G passe par les points de $F \cap C$ on peut appliquer le théorème de Max Noether : il existe $A, B \in \mathbb{C}[x, y]$ tels que : $G = AF + BC$ et l'unicité nous donne que A est de degré $\frac{3n}{2} - n = \frac{n}{2}$. On a donc $T = A \cap C$ et par hypothèse de récurrence la somme des points dans T est nulle. Or la somme des points dans $S \cup T$ est nulle puisque on a à chaque fois les trois points d'intersection (qui éventuellement peuvent être un ou deux points) entre une droite et C. Donc la somme des points dans S est nulle, ce qu'il fallait démontrer. Maintenant si n est impair, on prend pour G le produit des $(3n - 1)/2$ droites et une autre droite quelconque passant par le point restant. On obtient alors avec les notations précédentes, une courbe A de degré $(n + 1)/2$ et on applique la récurrence. □



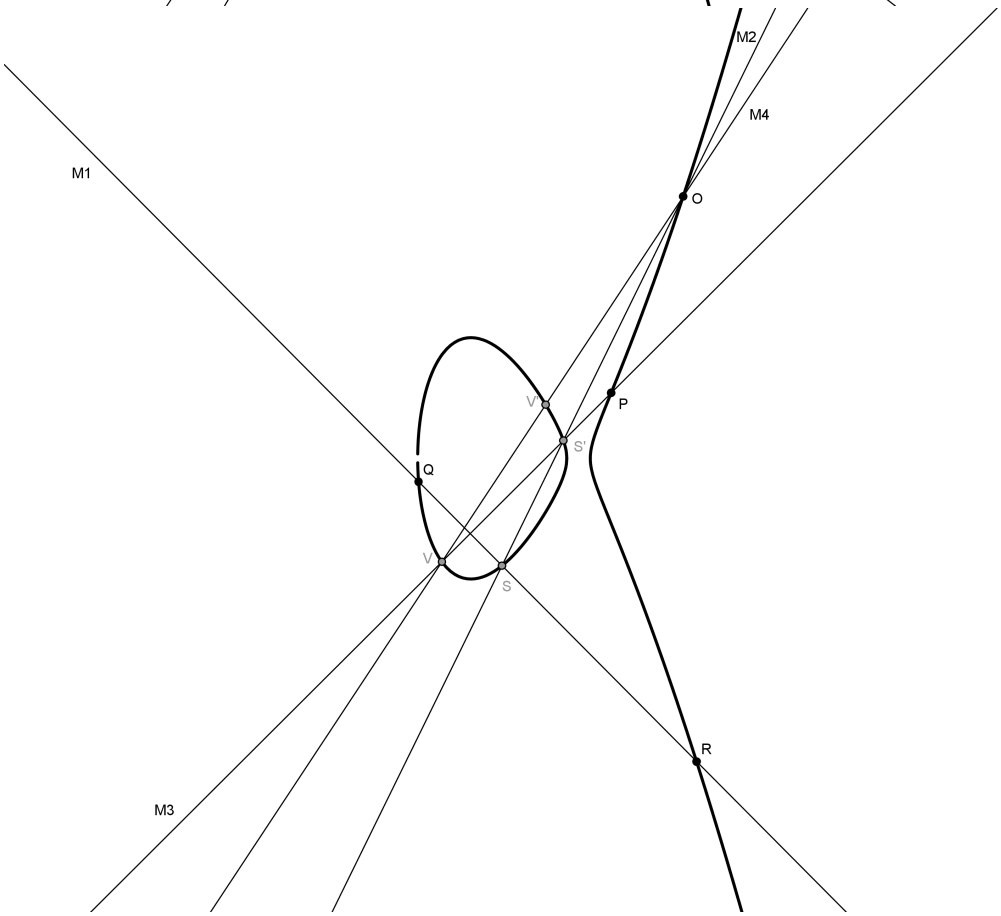


FIGURE 26 – Annexe

Références

[1] I. Dolgachev. *Lectures on invariant theory*, volume 296 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.

[2] M. Hindry. *Arithmétique*. Tableau noir. Calvage et Mounet, Paris, 2008.

[3] M. Nagata. On the fourteenth problem of Hilbert. In *Proc. Internat. Congress Math. 1958*, pages 459–462. Cambridge Univ. Press, New York, 1960.

[4] R. Steinberg. Nagata's example. In *Algebraic groups and Lie groups*, volume 9 of *Austral. Math. Soc. Lect. Ser.*, pages 375–384. Cambridge Univ. Press, Cambridge, 1997.