Université de Rennes 1

Contre-exemple de Nagata au quatorzième problème de Hilbert

Alice Bouillet

Janvier 2020

Table des matières

Bibliographie

[Ful] : An introduction to Algebraic Geometry, William Fulton.
[Per] : Géométrie Algébrique, une introduction. Daniel Perrin.
[Dolg] : Lectures on Invariant Theory, Igor Dolgachev.
[Hart] : Algebraic Geometry, Robin Hartshorne.

1 Rappels de quelques définitions nécessaires à la compréhension

Définition 1.1. *Soit G un groupe et V un espace vectoriel. Une* ***action linéaire*** *de G sur V est une application :*
$\rho : G \to Gl(V)$ telle que $\forall g_1, g_2 \in G$, $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$.
L'action sous-jacente est alors la suivante :

$$G \times V \to V$$

$$(g, P) \mapsto g.v := \rho(g)(P)$$

On dit que G agit ***linéairement*** *sur V.*

Définition 1.2. *Soient k un corps, G un groupe et V une k-algèbre. On suppose que G agit linéairement sur V. On dit que G agit par* ***automorphismes d'algèbres*** *si $\forall g \in G$, $\rho(g)$ est un automorphisme d'algèbre de V.*

Remarque 1.1. *Soient V une k-algèbre, G un groupe qui agit sur V par automorphismes d'algèbres. Alors $V^G := \{v \in V, \forall g \in G, g.v = v\}$ est naturellement munit d'une structure de k-algèbre. On l'appelle* ***l'algèbre des invariants de V sous G.***

Remarque 1.2. *Soit A une k-algèbre intègre et G agissant par automorphismes d'algèbres sur A. Alors G définit une action naturelle sur $Frac(A)$ par :*
$\forall g \in G$, $\forall \dfrac{P}{Q} \in Frac(A)$, $g.\dfrac{P}{Q} = \dfrac{g.P}{g.Q}$.
L'algèbre des invariants $Frac(A)^G$ est ici munit d'une structure de corps.

2 Présentation du problème

Problème 1. *: Soit k un corps, et $k(t_1, \ldots, t_n)$ son extension transcendante pure.*
Soit K/k une extension de corps, telle que $K \subset k(t_1, \ldots, t_n)$. Est-ce que la k-algèbre $K \cap k[t_1, \ldots, t_n]$ est de type fini sur k ?

Nous allons voir que la réponse à ce problème est en générale négative, en montrant que la réponse à celui-ci l'est :

Problème 2. *Soit k un corps et $k(t_1, \ldots, t_n)$ son extension transcendante pure. Soit G un groupe agissant par automorphismes d'algèbres sur $k[t_1, \ldots, t_n]$. On prend alors $K = k(t_1, \ldots, t_n)^G$. On veut alors savoir si la k-algèbre $K \cap k[t_1, \ldots, t_n] = k[t_1, \ldots, t_n]^G$ est de type fini sur k.*

3 Le contre-exemple de Nagata

Soient $n \in \mathbb{N}$, $(a_{1,1}, \ldots, a_{1,n}), (a_{2,1}, \ldots, a_{2,n})$ et $(a_{3,1}, \ldots, a_{3,n}) \in k^n$.
Soit

$$G' = \{(t_1, \ldots, t_n) \in k^n | \sum_{j=1}^{n} a_{ij} t_j = 0, \text{ pour } i = 1, 2, 3\},$$

G' est un sous-groupe de k^n. Il agit sur k^{2n} par transvection, par la formule :

$$(t_1, \ldots, t_n).(x_1, y_1, \ldots, x_n, y_n) = (x_1 + t_1 y_1, y_1, \ldots, x_n + t_n y_n, y_n)$$

Soit maintenant :

$$C = \{(c_1, \ldots, c_n) \in (k^*)^n | \prod_{i=1}^{n} c_i = 1\}$$

C'est un sous-groupe de $(k^*)^n$, qui agit par dilatation sur k^{2n} par la formule :

$$(c_1, \ldots, c_n).(x_1, y_1, \ldots, x_n, y_n) = (c_1 x_1, c_1 y_1, \ldots, c_n x_n, c_n y_n)$$

On considère enfin $G := G'C$.
G agit alors sur k^{2n} grâce aux formules ci-dessus, et c'est ce groupe qui va nous permettre de montrer que le problème de Hilbert est faux.

Cela nous amène donc à l'énoncé du théorème clé de ce séminaire :

Théorème 1. *Pour un certain choix de $(a_{ij})_{i,j}$ dans la construction du groupe G', et le choix d'un nombre n de variables, l'algèbre des invariants :*

$$k[X_1, Y_1, \ldots, X_n, Y_n]^G$$

*n'est **pas** de type fini sur k.*

Nous avons maintenant besoin de quatre lemmes pour démontrer ce résultat, les deux premiers lemmes étant plus calculatoires, et les deux derniers nécessitant des résultats de géométrie algébrique classique.

Lemme 1. *Supposons $M := (a_{ij})_{1 \leq i,j \leq 3}$ soit inversible. On a alors :*

$$k(X_1, Y_1, \ldots, X_n, Y_n)^G = k(T, Z_1, Z_2, Z_3)$$

où $T := Y_1 \ldots Y_n$ et pour $i = 1, 2, 3$, $Z_i := \sum_{j=1}^{n} a_{ij}(\frac{X_j T}{Y j})$.

Démonstration. Soit $g = (t_1, \ldots, t_n)\dot{(}c_1, \ldots, c_n) \in G$. D'après les formules précédentes, on a

$$g(\frac{X_j}{Y_j}) = \frac{X_j}{Y j} + t_j \, ; \, g(T) = T$$

Et comme $\sum_{j=1}^{n} a_{ij} t_j = 0$, on obtient $g(Z_i) = Z_i$ pour $i = 1, 2, 3$. On montre ainsi que $k(T, Z_1, Z_2, Z_3) \subset k(X_1, Y_1, \ldots, X_n, Y_n)^G$. Montrons l'inclusion réciproque.

Grâce aux hypothèses sur la matrice M, en inversant les équations, on peut écrire $\frac{X_i T}{Y_i}$ pour $i = 1, 2, 3$ comme combinaisons linéaires de $\frac{X_j T}{Y_j}$ pour $j = 4, \ldots, n$ et Z_1, Z_2, Z_3. On obtient alors :

$$k(X_1, Y_1, \ldots, X_n, Y_n) = k(Z_1, Z_2, Z_3, X_4, \ldots, X_n, Y_1, \ldots, Y_n)$$

$$k(X_1, Y_1, \ldots, X_n, Y_n) = k(T, Z_1, Z_2, Z_3, X_4, \ldots, X_n, Y_1, \ldots, Y_{n-1})$$

On sait que le degré de transcendance de $k(X_1, Y_1, \ldots, X_n, Y_n)$ sur k est de $2n$. Ainsi le degré de transcendance de $k(Z_1, Z_2, Z_3, X_4, \ldots, X_n, Y_1, \ldots, Y_n)$ sur k est de $2n$ aussi, ainsi

$Z_1, Z_2, Z_3, Y_1, \ldots, Y_n$ sont algébriquement indépendants sur k. Et donc, T, Z_1, Z_2, Z_3 sont aussi algébriquement indépendants sur k.
Soit H le sous-groupe de G définit par $H = \{\underbrace{(t_1, t_2, t_3, t_4, 0, \ldots, 0)}_{\in G'}(1, \ldots, 1)\}$. On a alors :

$$k(X_1, Y_1, \ldots, X_n, Y_n)^G = k(T, Z_1, Z_2, Z_3, X_4, \ldots, X_n, Y_1, \ldots, Y_{n-1})^G$$

$$k(X_1, Y_1, \ldots, X_n, Y_n)^G \subset k(T, Z_1, Z_2, Z_3, X_4, \ldots, X_n, Y_1, \ldots, Y_{n-1})^H$$

Mais on a

$$k(T, Z_1, Z_2, Z_3, X_4, \ldots, X_n, Y_1, \ldots, Y_{n-1})^H = k(T, Z_1, Z_2, Z_3, X_5, \ldots, X_n, Y_1, \ldots, Y_{n-1})$$

En continuant de cette façon à éliminer les variables X_i, on obtient

$$k(X_1, Y_1, \ldots, X_n, Y_n)^G \subset k(T, Z_1, Z_2, Z_3, Y_1, \ldots, Y_{n-1})$$

Enfin, pour que Y_i soit invariant sous l'action de G, il doit en particulier être invariant par homothétie. Ainsi tout polynôme en Y_i invariant par G est en fait constant.
On obtient alors la preuve du lemme. □

Pour le deuxième lemme, nous avons besoin de la définition suivante, qui généralise la notion de multiplicité d'un polynôme en une variable.

Définition 3.1. *Soit P un polylnôme de $k[T_1, \ldots, T_n]$. On dit que P a une multiplicité m au point $(0, \ldots, 0)$ si, en écrivant P comme somme de polynômes homogènes, il y a un polynôme de degrés m mais aucun de degré plus petit. On dit que P a une multiplicité m au point $(x_1, \ldots, x_n)$ si $P(T_1 + x_1, \ldots, T_n + x_n)$ a une multiplicité de m en $(0, \ldots, 0)$.*

Exemple 3.1. *$P(X, Y, Z) = XYZ + X^3 - 5X^2Y + 3Y^2 - 2XY$ est de multiplicité 2 en $(0, 0, 0)$.*

Proposition 3.1. *Si $char(k) = 0$, alors P est de multiplicité m en $(0, \ldots, 0)$ si et seulement si toutes les dérivées partielles de P de degré $< m$ s'annulent en $(0, \ldots, 0)$.*

Démonstration. Si la multiplicité de P est m, on a trivialement que ses dérivées partielles de degrés $< m$ s'annule car si P_i est homogène de degré i, alors toutes ses dérivées partielles sont homogènes de degré $i - 1$. La réciproque se prouve grâce à la formule de Taylor. □

Maintenant, considérons chaque colonne (a_{1j}, a_{2j}, a_{3j}) de la matrice $(a_{ij})_{1 \leq i,j \leq 9}$ comme les coordonnées d'un point P_j dans le plan projectif $\mathbb{P}^2$. Soit $m \in \mathbb{N}$, et $R(m)$ l'idéal de $k[Z_1, Z_2, Z_3]$ engendré par les polynômes homogènes P de multiplicité au moins m en chaque P_j.
Ces notions nous donnent une description plus précise de l'algèbre des invariants, qui va nous être utile pour prouver que le problème de Hilbert est faux.

Lemme 2.

$$k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]^G = \{\sum_{m=0}^{N} F_m(Z_1, Z_2, Z_3)T^{-m} | N \in \mathbb{N}\ ; F_m \in R(m)\}.$$

Démonstration. Utilise le lemme 1. Voir [Dolg] lemme 4.3 chapitre 3 p 55. □

Maintenant, nous avons besoin de notions de géométrie algébrique.

4 Géométrie algébrique

4.1 Multiplicités et anneaux locaux

Définition 4.1. *Soit V un ensemble algébrique affine de k^n irréductible et $P \in V$. On utilise les notations $k[V]$ ou $\Gamma(V)$ pour désigner $k[X_1, \ldots, X_n]/I(V)$.*
*Une **fonction rationnelle** sur V est un élément f du corps de fraction de $k[V]$.*
*On dit que f est **régulière** en $P \in V$ si on peut écrire $f = g/h$ avec $g, h \in k[V]$ et $h(P) \neq 0$.*
On désigne par $\mathscr{O}_P(V)$ l'ensemble des fonctions rationnelles sur V qui sont régulières en P.
On désigne par $\mathfrak{m}_P(V)$ l'ensemble des fonctions régulières en P qui s'annulent en P.
On note $\mathfrak{m} := \{f \in k[V], f(P) = 0\}$.

Proposition 4.1. *$\mathscr{O}_P(V) = k[V]_{\mathfrak{m}}$*
Et de plus, $\mathfrak{m}_P(V) = \mathfrak{m}k[V]_{\mathfrak{m}}$

Démonstration. Par définition, on a :
$f \in \mathscr{O}_P(V) \Leftrightarrow \exists g, h \in k[V], f = g/h, h(P) \neq 0$
$\Leftrightarrow \exists g, h \in k[V], f = g/h, h \notin \mathfrak{m}) \Leftrightarrow f \in k[V]_{\mathfrak{m}}$
De plus on a :
$f \in \mathfrak{m}_P(V) \Leftrightarrow \exists g, h \in k[V], f = g/h, h(P) \neq 0, g(P) = 0$
$\Leftrightarrow \exists g, h \in k[V], h \notin \mathfrak{m}, g \in \mathfrak{m}$ et $f = g/h$
$\Leftrightarrow f \in \mathfrak{m}k[V]_{\mathfrak{m}}$ □

Remarque 4.1. *On voit alors que $\mathscr{O}_P(V)$ est un anneau local intègre noethérien.*

Théorème 2. *Soit $C = V(F)$ une courbe irréductible plane et $P \in C$. Alors il existe un unique $m \in \mathbb{N}$, tel que :*
$\forall n \geq m$, $\dim_k \left(\dfrac{\mathfrak{m}_P(C)^n}{\mathfrak{m}_P(C)^{n+1}} \right) = m.$

Démonstration. Admise. □

Définition 4.2. *Cet entier m s'appelle la **multiplicité** de P dans C, on le note $mult_{P,C}$. On voit en particulier que cette notion ne dépend que de $\mathscr{O}_P(V)$.*

Définition 4.3. *On appelle point singulier P d'une courbe affine C un point qui annule aussi les dérivées partielles. C'est équivalent à dire que la multiplicité de $mult_{P,C} > 1$.*

Théorème 3. *Soit C une courbe irréductible. P est un point non singulier (i.e de multiplicité 1) si et seulement si $\mathscr{O}_P(C)$ est un anneau de valuation discrète.*

Démonstration. On a déjà que $\mathscr{O}_P(C)$ est un anneau local, intègre et noethérien. Puisque P est de multiplicité 1 l'espace vectoriel sur k, $\dfrac{\mathfrak{m}_{C,P}}{\mathfrak{m}_{C,P}^2}$ est de dimension 1. Montrons que les idéaux de $\mathscr{O}_P(C)$ sont exactement (0) et les puissance de $\mathfrak{m}_{C,P}$.
Soit t dans $\mathfrak{m}_{C,P}$ dont la classe modulo $\mathfrak{m}_{C,P}^2$ engendre $\dfrac{\mathfrak{m}_{C,P}}{\mathfrak{m}_{C,P}^2}$. Alors

$$\mathfrak{m}_{C,P} = t\mathscr{O}_P(C) + \mathfrak{m}_{C,P}^2.$$

D'après le lemme de Nakayama, on a alors :

$$\mathfrak{m}_{C,P} = t\mathscr{O}_P(C).$$

Cela montre que $\mathfrak{m}_{C,P}$ n'est pas nilpotent. Or dans un anneau local noethérien, l'intersection des puissances de $\mathfrak{m}_{C,P}$ est nulle. Donc pour tout idéal I propre et non nul, on dispose d'un entier maximal n tel que $I \subset \mathfrak{m}_{C,P}^n$, en effet le lemme de Krull assure que $I \subset \mathfrak{m}_{C,P}$.
Ainsi le sous-espace $\dfrac{I + \mathfrak{m}_{C,P}^{n+1}}{\mathfrak{m}_{C,P}^{n+1}}$ de $\dfrac{\mathfrak{m}_{C,P}^{n}}{\mathfrak{m}_{C,P}^{n+1}}$ est non-nul et puisque le second quotient est de dimension 1, ces deux espaces sont égaux i.e. :

$$I + \mathfrak{m}_{C,P}^{n+1} = \mathfrak{m}_{C,P}^{n}.$$

Enfin le lemme de Nakayama nous assure que :

$$I = \mathfrak{m}_{C,P}^{n}.$$

Cette propriété montre que l'inclusion est un ordre total sur les idéaux de $\mathscr{O}_P(C)$ ce qui en fait un anneau de valuation, notons la ν. De plus, $\mathscr{O}_P(C)$ étant noethérien l'ensemble $\nu(\mathfrak{m}_{C,P})$ admet un élément minimal et donc la valuation ν est bien discrète.

□

4.2 Théorème de Bézout projectif

4.2.1 Multiplicité d'intersection

Soient F et G deux courbes affines, et $P \in k^2$. On veut définir la multiplicité d'intersection de F et G en P, que l'on va écrire $I(P, F \cap G)$.
On dit que F et G s'intersectent **proprement** en P si F et G n'ont pas de composantes communes qui passe par P.

Théorème 4. *Il existe un unique nombre $I(P, F \cap G)$ défini pour toute courbe plane F, G et tout point $P \in k^2$, que l'on appelle* ***multiplicité d'intersection de F et G en P*** *tel que :*
1) $I(P, F \cap G)$ est un entier positif ou nul pour tout P tel que F et G s'intersectent proprement en P. Sinon, on a $I(P, F \cap G) = \infty$.
2) $I(P, F \cap G) = 0$ si et seulement si $P \notin F \cap G$.
3) $I(P, F \cap G)$ est invariant par changement affine de coordonnée.
4) $I(P, F \cap G) = I(P, G \cap F)$.
5) $I(P, F \cap G) \leq mult_{P,F} \times mult_{P,G}$, avec égalité lorsque F et G n'ont pas de tangente commune en P.
6) Si $F = \prod F_i^{r_i}$ et $G = \prod G_j^{s_j}$, alors $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.
7) $I(P, F \cap G) = I(P, F \cap (G + AF))$, pour tout $A \in k[X, Y]$.

Ce nombre est donnée par : $I(P, F \cap G) = \dim_k \left(\dfrac{\mathscr{O}_P(k^2)}{(F, G)} \right)$.

Démonstration. Voir [*Ful*], théorème 3 chapitre 3, p 75. □

Remarque 4.2. *On a ce résultat (Voir [Per] chapitre 8, lemme 2.8 page 166) : Soit A une k-algèbre qui est un anneau de valuation discrète, de valuation ν. On suppose $A/m \simeq k$, où m est l'idéal maximal de A. Alors, on a pour tout $a \in A$, $\nu(a) = dim_k(A/(a))$.*
Soit $C = V(g)$ une courbe irréductible et $P \in C$ non singulier. On applique ce résultat avec $A = \mathscr{O}_P(C)$ dont on note la valuation ord_P. On a alors que pour toute fonction régulière $f = f_1/f_2$ sur C,
$ord_P(f) = ord_P(f_1) + ord_P(1/f_2) = ord_P(f_1)$ car $1/f_2$ est inversible dans $\mathscr{O}_P(C)$. Donc,

$ord_P(f) = dim_k(\mathscr{O}_P(g)/(f_1))$. Or, $\mathscr{O}_P(g)/(f_1) \simeq \mathscr{O}_P(k^2)/(g)/(f_1) \simeq \mathscr{O}_P(k^2)/(f_1, g)$. On voit alors que $ord_P(f) = I(P, f_1 \cap g)$ donc la valuation sur $\mathscr{O}_P(C)$ généralise la notion de multiplicité d'un point à une fonction régulière sur une courbe.

4.2.2 Lien affine/projectif

On va maintenant voir la version projective des définitions vues précédemment. Tout d'abords on identifie $\mathbb{P}^n$ avec k^n.
Pour tout $i \in [1, \dots, n+1]$, on note

$$\phi_i : k^n \to U_i$$

$$(x_1, \dots, x_n) \mapsto (x_1, ...x_{i-1}, 1, x_{i+1}, \dots, x_n)$$

où $U_i = \{[x_1 : \dots : x_{n+1}] \in \mathbb{P}^n \ , \ x_i \neq 0\}$
Dans ce qui suit, on va souvent considérer ϕ_{n+1} mais tout reste vrai pour tout i.

Définition 4.4. *Soit $P = P(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$. On appelle $\overline{P}$ **l'homogénéisé** de P par rapport à X_{n+1} défini ainsi :*

$$\overline{P}(X_1, \dots, X_{n+1}) = X_{n+1}^d P(\frac{X_1}{X_{n+1}}, \dots, \frac{X_n}{X_{n+1}})$$

où d est le degré de P.

Définition 4.5. *Soit $P(X_1, \dots, X_{n+1})$ un polynôme homogène de $K[X_1, \dots, X_{n+1}]$. On appelle le **déshomogénéisé** de P par rapport à X_{n+1} le polynôme suivant :*

$$\widetilde{P}(X_1, \dots, X_n) = P(X_1, \dots, X_n, 1)$$

Définition 4.6. *Soit V un ensemble algébrique projectif irréductible dans $\mathbb{P}^n$.*
On définit $I(V) := \{F \in k[X_1, \dots, X_{n+1}] \mid \forall P \in V \ , \ F(P) = 0\}$ l'idéal associé à V, où $P = [x_1, \dots, x_{n+1}]$ est un zéro de F si F est nul pour tout système de coordonnées homogène de P. C'est équivalent à demander que chaque polynôme homogène dans la décomposition de F s'annule sur P.
*On appelle **l'anneau de coordonnée homogène de V** l'anneau $\Gamma_h(V) := \dfrac{k[X_1, \dots, X_{n+1}]}{I(V)}$*

Définition 4.7. *Soit $C = V(G)$ une courbe plane projective. On dit que f est une **fonction rationnelle** sur C si $f = \dfrac{P}{Q}$, où P et Q sont des polynômes homogènes de $k[X, Y, Z]$ de même degré, et G ne divise pas Q.*

Les fonctions rationnelles sur C forment un corps, noté $k(C)$. On l'appelle aussi le corps des fonctions de C.

Définition 4.8. *Soit C une courbe plane projective irréductible et $P \in C$, et $f \in k(C)$. On dit que f est **régulière** en P si f peut être écrit sous la forme $f = \dfrac{G}{H}$ où G et H sont homogènes de même degré et $H(P) \neq 0$.*
Soit $\mathscr{O}_P(C)$ l'ensemble de ces fonctions. $\mathscr{O}_P(C)$ est un sous anneau local de $k(C)$, d'idéal maximal $\mathfrak{m}_P(C) = \{f = \dfrac{G}{H}, H(P) \neq 0, G(P) = 0\}$.

Définition 4.9. *Soit $V \in k^n$ un ensemble algébrique. Soit $I = I(V)$. Soit $\overline{I} = \{\overline{F}, \ , \ F \in I\}$. On définit $\overline{V} = V(\overline{I})$.*
Réciproquement, soit $V \subset \mathbb{P}^n$ un ensemble algébrique projectif. Soit $I = I(V)$. Soit $\widetilde{I} = \{\widetilde{F} \ , \ F \in I\}$. On définit $\widetilde{V} = V(\widetilde{I})$.

Proposition 4.2. *1) Si $V \subset k^n$, $\phi_{n+1}(V) = \overline{V} \cap U_{n+1}$, et $\widetilde{\overline{V}} = V$.*
2) Si V est irréductible dans k^n, alors $\overline{V}$ l'est dans $\mathbb{P}^n$.
3) Si $V = V(F) \subset k^n$, alors $\overline{V} = V(\overline{F})$.
4) On a une bijection entre les variété affines, et les projectives non inclues dans le plan à l'infini.

Proposition 4.3. *Soit V un ensemble algébrique affine irréductible, et $P \in V$. Alors*

$$\mathscr{O}_P(V) \simeq \mathscr{O}_{\phi_{n+1}(P)}(\overline{V})$$

Démonstration. Si $f \in \Gamma_h(\overline{V})$ est la classe d'un polynôme homogène F, on définit $f_* \in \Gamma(V)$ en la classe de $\widetilde{F}$ modulo $I(V)$. On vérifie que cette application est bien définie, et on obtient alors un isomorphisme : $\alpha : k(\overline{V}) \to k(V)$, $\alpha(f/g) = f_*/g_*$. Si $P \in V$, on peut considérer $P \in \overline{V}$ grâce à ϕ_{n+1} par exemple, et α induit un isomorphisme de $\mathscr{O}_P(\overline{V})$ sur $\mathscr{O}_P(V)$. □

Proposition 4.4. *De la même manière, soit V un ensemble algébrique projectif irréductible, et $P \in V$. Alors soit i tel que $P \in V \cap U_i$. On a alors :*

$$\mathscr{O}_P(V) \simeq \mathscr{O}_{\phi_i^{-1}(P)}(\widetilde{V})$$

Définition 4.10. *Soit $P = [x, y, z] \in \mathbb{P}^2$, avec $P \in C = V(F)$. Il existe $i = 1, 2$ ou 3 tel que $P \in U_i$. On définit alors la **multiplicité** de C en P comme étant la multiplicité du point (x, y) sur la courbe définie par $\widetilde{F} = 0$, où $\widetilde{F}$ est le déshomogénéisé de F. On vérifie que cette notion est indépendante du choix de U_i.*

Définition 4.11. *Soient F et G deux polynômes homogènes non nuls de $k[X, Y, Z]$ sans facteur commun, de degrés respectifs m et n.*
Soit $P = (x, y, z) \in \mathbb{P}^2$. L'une des coordonnées est non nulles, on peut alors supposer que $z = 1$. On considère alors les polynômes $\widetilde{F}$ et $\widetilde{G}$ les déhomogénéisés par rapport à Z, et on définit la multiplicité d'intersection de F et G en P par $I_P(P, F \cap G) := I((x, y), \widetilde{F} \cap \widetilde{G})$.

Grâce à ces identifications, on se placera facilement dans le cas affine dans la suite.

Tout cela nous ammène donc au théorème de Bézout :

Théorème 5. *Soit $k = \overline{k}$. Soient F et G deux courbes projectives sans composantes communes, de degré respectivement m et n. Alors :*

$$\sum_{P \in F \cap G} I(P, F \cap G) = mn$$

Démonstration. Voir [Ful], chapitre 5, 3) p 112. □

4.3 Diviseurs d'une fonction rationnelle

On se place sur une courbe projective irréductible et non singulière. Grâce à la correspondance affine/projective, on adopte le point de vue affine. On a vu alors que $\forall P \in C, \mathscr{O}_P(C)$ est un anneau de valuation discrète. On appelle $ord_P(C)$, ou ord_P quand il n'y a pas d'ambigüité, la valuation de cet anneau. Comme $k(C) = Frac(\mathscr{O}_P(C))$, on étend cette valuation à $k(C)$ en posant $ord_P(g/h) = ord_P(g) - ord_P(h)$.

Proposition 4.5. *Soit $P \in C$ comme ci-dessus, et $f \in k(C)$. Alors :*
$ord_P(f) < 0 \Leftrightarrow P$ est un pôle pour $f \Leftrightarrow f \notin \mathcal{O}_P(C)$
$ord_P(f) \geq 0 \Leftrightarrow f$ est régulière en $P \Leftrightarrow f \in \mathcal{O}_P(C)$
$ord_P(f) = 0 \Leftrightarrow f$ est régulière en P et $f(P) \neq 0 \Leftrightarrow f \in \mathcal{O}_P^\times(C)$
$ord_P(f) > 0 \Leftrightarrow P$ est un zéro de $f \Leftrightarrow f \in \mathfrak{m}_P(C)$

Démonstration. Découle directement des définitions et du lemme de la remarque 4.1. □

Définition 4.12. *Soit $z \in k(C)$. On définit le **diviseur** de z, $div(z)$, comme étant la somme formelle suivante : $\sum_{P \in C} ord_P(z)P$. Grâce au théorème de Bezout, on sait que z a un nombre fini de zéros et de pôles, cette somme est donc une somme finie.*
Si on écrit $(z)_0 = \sum_{ord_P(z)>0} ord_P(z)P$ et $(z)_\infty = \sum_{ord_P(z)<0} -ord_P(z)P$, on a $div(z) = (z)_0 - (z)_\infty$.

Cette notion est primordiale dans la preuve de notre théorème. Pour finir, nous avons besoin d'étudier des courbes projectives particulières : celles de degré 3.

4.4 Les cubiques

Définition 4.13. *Une cubique sur k est une courbe projective plane $C = V(F)$, où le polynôme $F \in k[X, Y, Z]$ correspondant est de degré 3.*
*Un point $P \in P^2$ d'une cubique $C = V(F)$ est dit **singulier***
si la multiplicité de P en C est > 1.

Remarque 4.3. *Toute cubique admet une tangente en un point P non singulier.*

On a alors un résultat fondamental : l'ensemble des points non singuliers d'une cubique lisse est munit d'une **loi de groupe**. On appelle E cet ensemble.
On la décrit ci-dessous :

Définition 4.14. *On peut définir **une loi de groupe** sur E, munit d'un point $O \in E(k)$. Soient P, Q deux points distincts de E. La droite joignant P à Q coupe la cubique en un troisième point de E (Théorème de Bézout). Soit R le troisième (éventuellement égal à P ou Q). On note $R = P \circ Q$. Si $P = Q$, on effectue la même opération avec la tangente de C en P. On définit alors l'addition en utilisant le point origine $O \in E(K)$, puis en posant $O' = O \circ O$ et enfin*

$$P \oplus Q := O \circ (P \circ Q)$$

et

$$-P := O' \circ P$$

Théorème 6. *La loi définit précédemment est une **loi de groupe** sur E, dont l'élément neutre est O. E munit de cette loi est un groupe abélien.*

Démonstration. Admise (seule l'associativité est non triviale). Voici une illustration pour l'associativité.

$= F$

□

Armé.es de ces nouvelles notions, nous sommes maintenant pret.es à comprendre le contre-exemple de Nagata.

4.5 Retour au contre-exemple de Nagata

On se place maintenant sur un corps k algébriquement clos, de caractéristique nulle.

Proposition 4.6. *Soit $C = V(G)$ une cubique irréductible. Soient P et Q deux points non singuliers de C. Alors $P \oplus Q$ est l'unique point R tel qu'il existe une fonction rationnelle sur C avec un diviseur égal à $P + Q - R - O$.*

Démonstration. Par construction, il existe une droite projective, d'équation $L_1 = 0$, qui coupe la cubique en P, Q et $P \circ Q$, et une autre, d'équation $L_2 = 0$, qui la coupe en O, R et $P \circ Q$. Le quotient L_1/L_2 représente une fonction rationnelle sur la cubique C. Maintenant, pour toute représentation F_1/F_2 d'une fonction rationnelle non nulle sur la cubique C (en particulier, G, ne divise ni F_1 ni F_2) son diviseur est la somme des points d'intersection de $F_1 = 0$ avec C (chaque point d'intersection étant affecté du coefficient égal à la multiplicité d'intersection) moins la somme des points d'intersection de $F_2 = 0$ avec C (chaque point d'intersection étant affecté, là encore, du coefficient égal à la multiplicité d'intersection). La fonction rationnelle recherchée ici est donc L_1/L_2, d'où l'existence.
Pour l'unicité, voir [Dolg], Lemme 4.4 page 57. □

Pour notre contre-exemple, le groupe G recherché utilisera une cubique, et les notions expiquées précédemment. On peut par exemple prendre celle-ci :
On fixe C la cubique définie par $F = Y^2Z - X^3$. Son seul point singulier est en $(0, 0)$. On note C^o sa partie non singulière. Le résultat suivant nous montre que la loi de groupe sur C^o est ici très simple. Dans la suite, on note O son élément neutre.

Théorème 7. $(C^o, \oplus) \simeq (k, +)$

Comme on considère cette cubique sur un corps de caractéristique nulle, on a alors l'existence d'un point P non singulier sur la courbe, qui ne soit pas de torsion. Cela nous amène alors au résultat suivant :

Lemme 3. *Soient $P_1, \dots, P_9 \in C^o$. Alors l'ordre de $P_1 \oplus \cdots \oplus P_9$ dans C^o est égal à $m > 0$ si et seulement si il existe un polynôme homogène G de degré $3m$ qui n'est pas nul sur C, avec multiplicité m en chaque P_i.*

Démonstration. Soient $P, Q \in C^o$. Alors $P \oplus Q$ est l'unique point R tel qu'il existe une fonction rationnelle sur C avec comme diviseur $P+Q-R-O$. Par récurrence, ça implique que $P_1 \oplus \cdots \oplus P_n$ est l'unique point T tel que il existe une fonction rationnelle sur C dont le diviseur $div(f)$ est égal à $P_1 + \cdots + P_n - T - (n-1)O$. En particulier, on obtient que $P_1 \oplus \cdots \oplus P_n$ est de m torsion si et seulement si $m(P_1 + \cdots + P_n) - mnO$ est le diviseur d'une fonction rationnelle. On prend maintenant $n = 9$.
On suppose qu'il existe un polynôme G_{3m} comme dans l'énoncé. Grâce au théorème de Bézout, on a que l'intersection de G_{3m} avec la cubique est exactement constituée des points P_i. Soit $L = 0$ l'équation de la tangente à la courbe C au point O. Alors la droite intercepte la courbe en O avec multiplicité 3. On restreint la fonction rationnelle G_{3m}/L_{3m} à la courbe C, on a donc l'existence d'une fonction rationnelle f telle que $div(f) = m(P_1 + \cdots + P_9) - 9mO$. D'après ce que l'on vient de faire, $P_1 \oplus \cdots \oplus P_9$ est de m-torsion.
Pour la réciproque, voir [Dolg], lemme 4.4 chapitre 4 page 57 (nous ne l'utilisons pas ici). □

Lemme 4. *Soient $P_1, \dots, P_9$ des points non singuliers sur C, tels que $P_1 \oplus \cdots \oplus P_9$ ne soit jamais de torsion. Alors :*
1) Un polynôme homogène G de degré $\leq 3m$ qui a une multiplicité $\geq m$ en chaque P_i est divisible par F^m.
2) La dimension de l'espace vectoriel V_d des polynômes homogènes de degré $d \geq 3m$ qui ont une multiplicité $\geq m$ en chaque P_i est égal à $\binom{d+2}{2} - 9\binom{m+1}{2}$.

Démonstration. 1) Notons $deg(G) = 3l + r$ avec $l \leq m$ et $r \in [0, 1, 2]$. Supposons que G ne soit pas divisible par F. Grâce au théorème de Bézout, on a $deg(G) * deg(F) \geq 9m$, donc $deg(G) = 3m$, donc G a une multiplicité m en chaque P_i et alors on obtient une contradiction grâce au lemme 3. Donc on peut écrire $G = FG'$ avec G' un polynôme homogène de degré $\leq 3m - 3$. On recommence ce raisonnement sur G'. Par récurrence, on obtient que $G = F^l H$, avec $deg(H) \leq 2$. De plus, on a $m \leq mult_{P_i}(G) = mult_{P_i}(F) * l + mult_{P_i}(H) = l + mult_{P_i}(H)$. Si $\forall i, mult_{P_i}(H) \geq 1$, on aurait au moins neuf points d'intersections entre H et C, mais Bézout nous dit qu'il y en a au plus six. Donc $\exists i$ tel que $mult_{P_i}(H) = 0$ et donc $m = l$. Ainsi, F^m divise G.
2) On peut supposer que nos P_i appartiennent à la partie affine $\{Z \neq 0\}$.
Soient $\phi_i^j, i = 1, \dots, 9\ , j = 1, \dots, \binom{m+1}{2}$ les fonctions linéaires définies sur l'espace $k[X, Y, Z]_d$ des polynômes homogènes de degré d, qui à un polynôme P associe la valeur au point P_i de la j-ième dérivée partielle du déshomogénéisé de P en Z, où on ordonne arbitrairement les $\binom{m+1}{2}$ dérivées partielles du polynôme $\widetilde{P}$ (en deux variables) d'ordre inférieur strictement à m.
Alors, $V_d = \bigcap_{i,j} Ker(\phi_i^j)$. Or les bases de Taylor sont indépendantes quand on les prend à des points différents, donc les ϕ_i^j sont linéairement indépendantes, on obtient alors la formule voulue. □

Nous pouvons maintenant démontrer le contre-exemple de Nagata.

Théorème 8. *En reprenant les définitions de la première partie, pour un certain choix de $(a_{ij})_{i,j}$ dans le groupe G', et le choix d'un nombre n de variables, l'algèbre des invariants :*

$$k[X_1, Y_1, \ldots, X_n, Y_n]^G$$

n'est ***pas*** *de type fini sur k.*

Démonstration. On prend $n = 9$, et on prend $(a_{1,i}, a_{2,i}, a_{3,i})$ comme étant les coordonnées de points non singuliers P_i sur notre cubique C tels que : leur somme ne soit pas de torsion et tels que les trois premiers points ne sont pas alignés. C'est possible car on peut supposer que dans nos P_i, quatre au moins soient distincts deux à deux. Si on suppose que dès que l'on en prend trois, ils sont alignés, alors prenons-en trois distincts, et un quatrième point distinct des trois autres, alors trois d'entre eux sont alignés, c'est-à-dire les quatre sont alignés. Donc ils sont tous alignés. Ceci est impossible grâce au théorème de Bézout. On suppose donc que P_1, P_2 et P_3 ne sont pas alignés. Le lemme 1 est donc satisfait. Supposons par l'absurde que $k[X_1 \ldots, X_9, Y_1, \ldots, Y_9]^G$ soit de type fini. Par le lemme 2, on peut trouver un système de générateurs de la forme F_{n_j}/T^{m_j} , $j = 1, \ldots, N$, où F_{n_j} est un polynôme de degré n_j qui a une multiplicité m_j en chaque point $P_1, \ldots, P_9$. Par le lemme 4, 1), on a $n_j \geq 3m_j$. Soit $m > m_j$ pour tout j. Par le lemme 4, 2), l'espace V_{3m+1} des polynômes de degré $3m + 1$ qui ont une multiplicité $\geq m$ en chaque P_i est de dimension $\binom{3m+3}{2} - 9\binom{m+1}{2} = 3m + 3$. De plus, le sous espace de V_{3m+1} des polynômes qui de plus s'annulent sur C est isomorphe à $V_{3(m-1)+1}$, et donc par le même lemme, est de dimension $\binom{3m}{2} - 9\binom{m}{2} = 3m$. Il existe alors un polynôme dans V_{3m+1} qui ne s'annule pas sur C.
Soit G un tel polynôme. On va montrer que G/T^m ne peut pas être exprimé comme un polynôme en les F_{n_j}/T^{m_j}, ce qui contredira le fait que cette algèbre soit de type fini.
On suppose par l'absurde que $G/T^m = Q(F_{n_1}/T^{m_1}, \ldots F_{n_N}/T^{m_N})$. Soit alors un monôme de la forme $U_1^{d_1} \ldots U_N^{d_N}$ dans l'anneau des polynômes en les variables F_{n_j}/T^{m_j}. Alors le degré de ce monôme en Z_1, Z_2 et Z_3 est égal à $\sum_{j=1}^{N} n_j d_j$. De même, son degré en T est égal à $\sum_{j=1}^{N} m_j d_j$.
Prenons maintenant un monôme de Q. Alors, en identifiant les dégrés, on a $3m + 1 = \sum n_j d_j$ et $m = \sum m_j d_j$. Alors

$$\sum_j (n_j - 3m_j) d_j = 1$$

Comme G n'est pas nul sur C, on peut choisir un monôme tel que, $\forall j$ tels que $n_j = 3m_j$, alors $d_j = 0$. En effet par l'absurde, supposons que dans tous les monômes de Q, on a l'existence d'un j tel que $n_j = 3m_j$ et d_j non nul, alors pour ce j, on aurait F_{n_j} s'annule sur C, et donc on pourrait toujours mettre un F en facteur, donc G s'annulerait sur C, ce qui est exclu. Donc dans ce même monôme, on a $n_j > 3m_j$ dès que $d_j \neq 0$, et donc les seuls cas possibles sont $d_j = 1, n_j = 3m_j + 1$ pour un j, et les autres d_j sont nuls. Ainsi, $m = \sum_j m_j d_j = m_k$ pour un k. Ceci est impossible par choix de m. □

Cette preuve conclut mon séminaire.