Autour du 14ème problème de Hilbert

Marco Maculan

IMJ-PRG

22 avril 2020

Le 14ème problème de Hilbert

- K corps algébriquement clos
- G un groupe qui agit linéairement sur $V := K^n$ via une représentation $G \to \mathrm{GL}(V)$
- $f \in \mathrm{Sym}\, V^* = K[x_1, \ldots, x_n]$ est invariant si $f(gx) = f(x)$ pour tout $g \in G$
- $(\mathrm{Sym}\, V^*)^G = \{f \in \mathrm{Sym}\, V^* : f \text{ invariant}\}$

Question (Hilbert, 1900)

Est-ce que $(\mathrm{Sym}\, V^*)^G$ *est de type fini ? i.e. existe-t-il des polynômes invariants* $f_1, \ldots, f_N$ *tels que tout élément de* $(\mathrm{Sym}\, V^*)^G$ *soit un polynôme en* $f_1, \ldots, f_N$ *?*

Exercice

- $G = \mathrm{GL}_n(K)$ agissant sur $V = \mathrm{M}_n(K)$ par conjugaison
- $A \in \mathrm{M}_n(K)$, $i = 0, \ldots, n-1$,

$$\sigma_i(A) = i\text{-ème coefficient de } \det(A - X\,\mathrm{id})$$

- $(\mathrm{Sym}\, V^*)^G = K[\sigma_0, \ldots, \sigma_{n-1}]$

« Binary quantics »

- $G = \mathrm{SL}_2(K)$ agissant sur l'espace V des polynômes homogènes en 2 variables de degré d

Problème

Exhiber des générateurs de l'algèbre des invariants et décrire les relations entre eux.

On identifie $\mathbb{P}(V)$ avec $\mathbb{P}^1(K)^d/\mathfrak{S}_d$ en associant à un polynôme ses zéros.

- $d = 4$: pour $(x_1, \ldots, x_4) \in \mathbb{P}^1(K)^4$ deux à deux distincts, soit $\lambda \in K \setminus \{0, 1\}$ leur birapport. L'algèbre des invariants « est engendrée » par

$$j(\lambda) = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

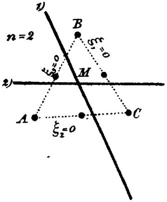
- $d = 5, 6$: chefs d'œuvre du XIXème siècle (Silvester, ...)
- $d \geqslant 11$: inconnu

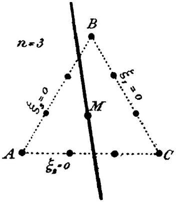
Deux papiers de Hilbert

1890 si $G = \mathrm{SL}_n(K)$ agit sur ses représentations « tensorielles », alors l'algèbre des invariants est de type fini

Theorem V. *Ist ein System von Grundformen mit beliebig vielen Veränderlichenreihen gegeben, welche in vorgeschriebener Weise den nämlichen oder verschiedenen linearen Transformationen unterliegen, so giebt es für dasselbe stets eine* endliche *Zahl von ganzen und rationalen Invarianten, durch welche sich jede andere ganze und rationale Invariante in ganzer und rationaler Weise ausdrücken lässt.*

1893 il introduit un critère (le « critère de Hilbert-Mumford ») pour déterminer les points sur lesquels tout invariant s'annule





Autres résultats de finitude

1916 E. Noether, char $K = 0$ et G fini

1926 E. Noether, char $K > 0$ et G fini

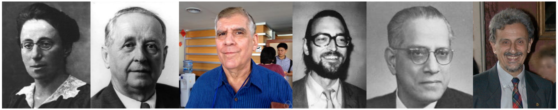
1936 H. Weyl, $K = \mathbb{C}$ et G groupe de Lie complexe connexe semi-simple

1975 W. Haboush, K quelconque et G réductif

sans oublier les contributions de Mumford, Oda, Seshadri, Formanek-Procesi, Humphreys, Jantzen, *et al.*

Exemple (Groupes réductifs)

$\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, K^*, groupes semi-simples, $\mathrm{SO}_n(K)$, ...



Le contre-exemple de Nagata

- $W := K^n$ qui agit sur $V := W \times W$ par

$$t(x,y) = (x_1, \ldots, x_n, y_1 + t_1 x_1, \ldots, y_n + t_n x_n), \qquad t, x, y \in W$$

Théorème (Nagata, 1958)

Soit $n = 16$. *Si* $\operatorname{degtr} K \geqslant 48$, *il existe un sous-espace vectoriel* $G \subseteq W$ *de codimension* 3 *tel que l'algèbre des invariants* $(\operatorname{Sym} V^*)^G$ *n'est pas de type fini.*

- $G = \operatorname{Ker}(A)$ avec $A \in \mathrm{M}_{3\times 16}(K)$ où A est une matrice dont les coefficients sont algébriquement indépendants

Appendix

A1. Examples of bad Noetherian rings

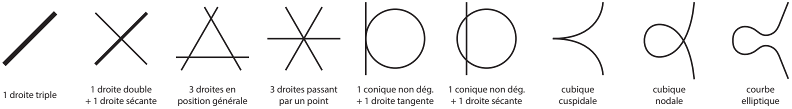
EXAMPLE 1. *A Noetherian ring whose altitude is infinite.*

Let K be a field and let $x_1, \ldots, x_n, \ldots$ be infinitely many algebraically independent elements over K. Let $m_1, \ldots, m_i, \ldots$ be a sequence of natural numbers such that $0 < m_i - m_{i-1} < m_{i+1} - m_i$ for every i. Let $\mathfrak{p}_i$ be the prime ideal of $K[x_1, \ldots, x_n, \ldots]$ generated by all the x_j such that $m_i \leq j < m_{i+1}$, and let S be the intersection of complements of $\mathfrak{p}_i$ in $K[x_1, \ldots, x_n, \ldots]$. Then $R = K[x_1, \ldots, \ldots, x_n, \ldots]_S$ is the required example.

Cubiques planes

Une cubique plane est l'ensemble des zéros d'un polynôme $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ homogène de degré 3 :

$$V(f) = \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(K) : f(x_0, x_1, x_2) = 0\}.$$

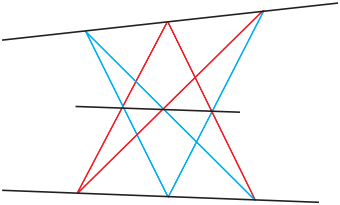


Si char $K \neq 2$ une courbe elliptique a une équation de la forme $y^2 = p(x)$ où $p(x)$ est un polynôme de degré 3 sans racines multiples.

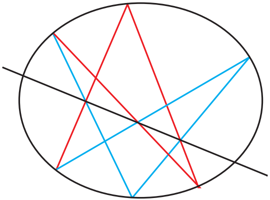
Le théorème de Chasles

Théorème (Chasles)

Soient C_1, C_2 des cubiques planes se rencontrant en 9 points $p_1, \ldots, p_9$ deux à deux distincts. Soit C_3 une cubique passant par $p_1, \ldots, p_8$. Alors, C_3 passe aussi par p_9.



Le théorème de Pappus



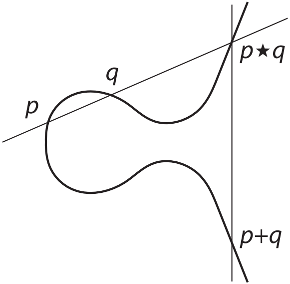
L'hexagone mystique de Pascal

Loi de groupe sur une courbe elliptique I

Soient E une courbe elliptique, $p, q \in E$. On fixe $o \in E$.

$$L_{p,q} = \begin{cases} \text{droite tangente à } E \text{ en } p & \text{si } p = q \\ \text{droite passant par } p \text{ et } q & \text{si } p \neq q. \end{cases}$$

- $p \star q =$ troisième point dans $L_{p,q} \cap E$
- $p + q = (p \star q) \star o$ est une loi de groupe abélien sur E avec élément neutre o

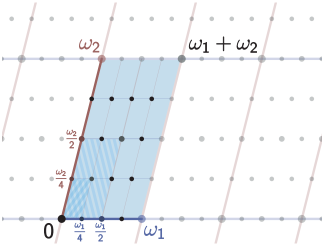


- Théorème de Chasles $\Rightarrow$ associativité

Loi de groupe sur une courbe elliptique II

Si $K = \mathbb{C}$ une courbe elliptique E est de la forme $\mathbb{C}/\Lambda$ pour un réseau $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

- si $z \in \mathbb{Q}\omega_1 \oplus \mathbb{Q}\omega_2$, il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $n[z] = 0_E$
- si $z \notin \mathbb{Q}\omega_1 \oplus \mathbb{Q}\omega_2$, $n[z] \neq 0_E$ pour tout $n \in \mathbb{N} \setminus \{0\}$



$\Rightarrow$ E contient des points d'ordre infini

C'est vrai aussi si $K = \bar{\mathbb{Q}}$!

Le théorème de Mordell-Weil I

- $f(x) \in \mathbb{Q}[x_0, x_1, x_2]$ polynôme homogène de degré 3 tel que $\frac{\partial f}{\partial x_0}, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}$ n'ont pas de zéro commun
- E courbe elliptique d'équation $f(x) = 0$ sur $K = \bar{\mathbb{Q}}$.
- $E(\mathbb{Q}) := E \cap \mathbb{P}^2(\mathbb{Q})$

Théorème (Mordell-Weil)

Si non-vide, $E(\mathbb{Q})$ est un groupe abélien de type fini :

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{\rho}.$$

L'entier ρ est appelé rang de Mordell-Weil de E.

Le théorème de Mordell-Weil II

- K un corps algébriquement clos, $F = K(t)$
- $f_t(x) \in K(t)[x_0, x_1, x_2]$ polynôme homogène de degré 3 tel que $\frac{\partial f_t}{\partial x_0}, \frac{\partial f_t}{\partial x_1}, \frac{\partial f_t}{\partial x_2}$ n'ont pas de zéro commun
- E courbe elliptique d'équation $f_t(x) = 0$ sur $\bar{F}$.
- $E(K(t)) := E \cap \mathbb{P}^2(K(t))$

Théorème (Mordell-Weil)

Supposons que $f_t(x)$ ne soit pas un multiple d'un polynôme dans $K[x_0, x_1, x_2]$. Alors, si non-vide, $E(K(t))$ est un groupe abélien de type fini :

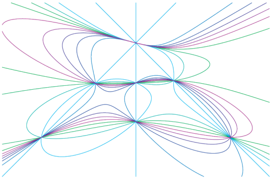
$$E(K(t)) = E(K(t))_{\mathrm{tors}} \oplus \mathbb{Z}^{\rho}.$$

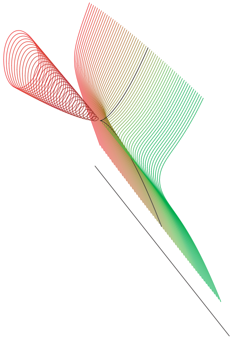
Pinceaux de cubiques

- K corps algébriquement clos
- $i = 1, 2$, $f_i \in K[x_0, x_1, x_2]$ polynôme homogène de degré 3
- $C_i = V(f_i)$ cubique correspondante

Le pinceau des cubiques C_1, C_2 est

$$P = \{([t_1 : t_2], x) \in \mathbb{P}^1(K) \times \mathbb{P}^2(K) : t_1 f_1(x) + t_2 f_2(x) = 0\}.$$





La courbe elliptique générique

- $f_t(x) = f_1(x) + tf_2(x) \in K(t)[x_0, x_1, x_2]$
- $E = V(f_t)$ est une cubique sur $\overline{K(t)}$

Question

Si E est une courbe elliptique, quel est son rang de Mordell-Weil ?

Théorème (Shioda-Tate)

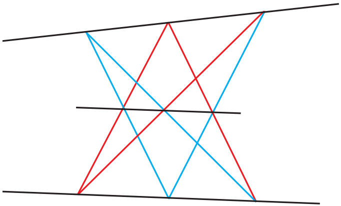
On suppose que C_1 et C_2 se rencontrent en 9 points $p_1, \ldots, p_9$ deux à deux distincts. Soient

$$a := \#\{\text{triplets colinéaires dans } p_1, \ldots, p_9\}$$
$$b := \#\{\text{partitions de } p_1, \ldots, p_9 \text{ en triplets colinéaires}\}$$

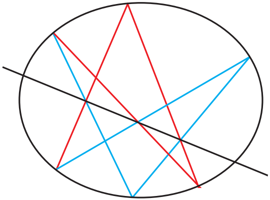
Alors, E est une courbe elliptique et son rang de Mordell-Weil est

$$\rho = 8 - a + b.$$

Exemples



Pappus
$a = 9$
$b = 1$
$\rho = 0$



Pascal
$a = 7$
$b = 0$
$\rho = 1$

Une variante du contre-exemple de Nagata ($n = 9$)

- $W := K^9$ agissant sur $V := W \times W$ par

$$t(x, y) = (x_1, \dots, x_9, y_1 + t_1 x_1, \dots, y_9 + t_9 x_9), \qquad t, x, y \in W$$

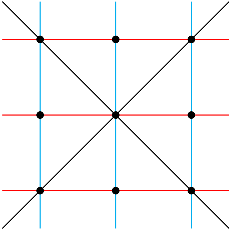
- C_1, C_2 deux cubiques se rencontrant en 9 points deux à deux distincts $p_i = [p_{i0} : p_{i1} : p_{12}]$ $(i = 1, \dots, 9)$
- $A = \begin{pmatrix} p_{10} & p_{20} & \cdots & p_{90} \\ p_{11} & p_{21} & \cdots & p_{91} \\ p_{12} & p_{22} & \cdots & p_{92} \end{pmatrix} \in \mathrm{M}_{3\times 9}(K)$
- $G = \mathrm{Ker}(A)$

Théorème (Totaro, 2008)

L'algèbre $(\mathrm{Sym}\, V^*)^G$ *est de type fini si et seulement si le rang de Mordell-Weil de la cubique générique (du pinceau déterminé par* C_1 *et* C_2*) est* 0.

Exemple (Totaro, 2008)

- char $K \neq 2, 3$
- $C_1 : x(x-1)(x+1) = 0$
- $C_2 : y(y-1)(y+1) = 0$



- $a = 8,\ b = 2,\ \rho = 2$
- $A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & -1 \\ 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 \end{pmatrix}$

$\Rightarrow$ $(\mathrm{Sym}\, V^*)^G$ n'est pas de type fini

Commentaires

Le contre-exemple précédent est une action de $G = K^6$ sur $V = K^{18}$.

Question

Peut-on prendre G plus petit ? Peut-on prendre V plus petit ?

- Les invariants de $G = K$ sont de type fini (Weitzenbock)
- Voici une liste des contre-exemples « petits » :

G	$\dim V$	K	
K^3	9	$\operatorname{degtr} K \gg 0$	Mukai (2001)
$K^4 \rtimes K$	11	$\operatorname{char} K = 0$	Freudenburg (2007)
K^3	18	quelconque	Totaro (2008)
K^4	16	quelconque	Totaro (2008)

References

- Shigeru Mukai, *Counterexample to Hilbert's fourteenth problem for the 3-dimensional additive group*, RIMS Preprint **1343** (2001).
- Masayoshi Nagata, *Lectures on the fourteenth problem of Hilbert*, Tata Institute of Fundamental Research, Bombay, 1965.
- Burt Totaro, *Hilbert's 14th problem over finite fields and a conjecture on the cone of curves*, Compos. Math. **144** (2008), no. 5, 1176–1198.