

SÉMINAIRE N. BOURBAKI

JACQUES DIXMIER

Solution négative du problème des invariants

Séminaire N. Bourbaki, 1960, exp. n° 175, p. 97-107

http://www.numdam.org/item?id=SB_1958-1960__5__97_0

© Association des collaborateurs de Nicolas Bourbaki, 1960, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

les a_{ij} algébriquement indépendants sur le corps premier. (ce qui exige que k soit assez grand). Soit G l'ensemble des $u(\alpha_1, \dots, \alpha_r)$ tels que

$$(1) \quad a_{i1} \alpha_1 + \dots + a_{ir} \alpha_r = 0 \quad (i = 1, 2, 3).$$

Alors G est un sous-groupe de G_1 . Soit $I \subset S(V)$ l'algèbre des invariants pour G .

Les éléments de $S(V)$ s'identifient aux fonctions polynômes sur V^* . Une fonction rationnelle sur V^* est invariante par G si elle est constante le long des orbites de G . Prenons dans V^* la base duale de la base $(x_1, \dots, t_r)$. Pour que deux points de V^* de coordonnées $(\xi_1, \dots, \xi_r, \tau_1, \dots, \tau_r)$ et $(\xi'_1, \dots, \xi'_r, \tau'_1, \dots, \tau'_r)$ de V^* appartiennent à une même orbite il faut et il suffit qu'il existe $\alpha_1, \dots, \alpha_r$ satisfaisant à (1) tels que

$$\xi'_1 = \xi_1 + \alpha_1 \tau_1, \dots, \xi'_r = \xi_r + \alpha_r \tau_r, \tau'_1 = \tau_1, \dots, \tau'_r = \tau_r.$$

Si $\tau_1 \tau_2 \dots \tau_r \neq 0$, il faut et il suffit que

$$\begin{aligned} \tau'_1 &= \tau_1 \dots \tau'_r = \tau_r \\ a_{i1} \frac{\xi'_1 - \xi_1}{\tau_1} + \dots + a_{ir} \frac{\xi'_r - \xi_r}{\tau_r} &= 0 \quad (i = 1, 2, 3) \end{aligned}$$

ou

$$\begin{aligned} \tau'_1 &= \tau_1 \dots \tau'_r = \tau_r \\ a_{i1} \xi'_1 \tau'_2 \dots \tau'_r + \dots + a_{ir} \xi'_r \tau'_1 \dots \tau'_{r-1} \\ &= a_{i1} \xi_1 \tau_2 \dots \tau_r + \dots + a_{ir} \xi_r \tau_1 \dots \tau_{r-1} \quad (i = 1, 2, 3). \end{aligned}$$

Posons :

$$y_i = a_{i1} x_1 t_2 \dots t_r + \dots + a_{ir} x_r t_1 t_2 \dots t_{r-1} \quad (i = 1, 2, 3).$$

Ce qui précède montre que $t_1, \dots, t_r, y_1, y_2, y_3 \in I$. A cause de l'indépendance des a_{ij} , on a

$$k(x_1, \dots, x_r, t_1, \dots, t_r) = k(y_1, y_2, y_3, x_4, \dots, x_r, t_1, \dots, t_r)$$

et on peut considérer $y_1, y_2, y_3, x_4, \dots, x_r, t_1, \dots, t_r$ comme des

indéterminées, qui sont transformées par G de la manière suivante :

$$t_1 \rightarrow t_1, \dots, t_r \rightarrow t_r, y_1 \rightarrow y_1, y_2 \rightarrow y_2, y_3 \rightarrow y_3,$$

$$x_4 \rightarrow x_4 + \beta_4 t_4, \dots, x_r \rightarrow x_r + \beta_r t_r$$

où $\beta_4, \dots, \beta_r$ sont arbitraires. On en déduit facilement que, dans le corps des quotients de $S(V)$, l'ensemble des invariants est

$$k(t_1, \dots, t_r, y_1, y_2, y_3).$$

CONCLUSION. - $I = k(t_1, \dots, t_r, y_1, y_2, y_3) \cap k[x_1, \dots, x_r, t_1, \dots, t_r]$

2. Soit $J = k(t_1, \dots, t_r, y_1, y_2, y_3) \cap k[x_1, \dots, x_r, t_1, \dots, t_r, 1/t_1, \dots, 1/t_r]$.

On a $I \subset J$. Par ailleurs, en raison de l'indépendance des a_{ij} , on a

$$\begin{aligned} k[x_1, \dots, x_r, t_1, \dots, t_r, 1/t_1, \dots, 1/t_r] &= \\ &= k[y_1, y_2, y_3, x_4, \dots, x_r, t_1, \dots, t_r, 1/t_1, \dots, 1/t_r]. \end{aligned}$$

Montrons que $J = k[y_1, y_2, y_3, t_1, \dots, t_r, 1/t_1, \dots, 1/t_r]$. Il est clair que $J \supset k[y_1, y_2, y_3, t_1, \dots, t_r, 1/t_1, \dots, 1/t_r]$. Réciproquement, un élément de J s'écrit $P(y_1, y_2, y_3, x_4, \dots, x_r)$, où P est un polynôme dont les coefficients appartiennent à

$$k[t_1, \dots, t_r, 1/t_1, \dots, 1/t_r] \subset k(t_1, \dots, t_r);$$

en même temps, c'est une fraction rationnelle en y_1, y_2, y_3 à coefficients dans $k(t_1, \dots, t_r)$; comme $y_1, y_2, y_3, x_4, \dots, x_r$ sont algébriquement indépendants sur $k(t_1, \dots, t_r)$, on voit que $x_4, \dots, x_r$ ne figurent pas dans P , donc que l'élément considéré de J appartient à

$$k[y_1, y_2, y_3, t_1, \dots, t_r, 1/t_1, \dots, 1/t_r].$$

CONCLUSION. - Tout élément de I s'écrit (de manière unique) sous la forme d'une somme fini

$$(2) \quad Q = \sum_{i_1, \dots, i_r \in \mathbb{Z}} c_{i_1, \dots, i_r} (y_1, y_2, y_3) t_1^{-i_1} \dots t_r^{-i_r}$$

avec $c_{i_1, \dots, i_r} \in k[Y_1, Y_2, Y_3]$ (Y_1, Y_2, Y_3 indéterminées).

3. Pour qu'une expression telle que Q appartienne effectivement à I , il faut et il suffit que Q soit un polynôme en $x_1, \dots, x_r, t_1, \dots, t_r$. Nous allons chercher une condition nécessaire et suffisante, portant sur les $c_{i_1, \dots, i_r}$, pour qu'il en soit ainsi.

Soit $\mathfrak{p}_1$ l'idéal de $k[Y_1, Y_2, Y_3]$ engendré par $a_{11}Y_2 - a_{21}Y_1$, $a_{11}Y_3 - a_{31}Y_1$. C'est un idéal premier homogène. Géométriquement, soit P_1 le point de coordonnées homogènes a_{11}, a_{21}, a_{31} dans le plan projectif (sur k). Alors, $\mathfrak{p}_1$ est l'idéal homogène de P_1 . Si $c \in \mathfrak{p}_1$, alors $c(y_1, y_2, y_3)$ est, en tant que polynôme en $x_1, \dots, x_r, t_1, \dots, t_r$, divisible par t_1 : il suffit de le vérifier pour $a_{11}y_2 - a_{21}y_1$ et $a_{11}y_3 - a_{31}y_1$; or :

$$\frac{a_{11}y_2 - a_{21}y_1}{t_1} = (a_{11}a_{22} - a_{21}a_{12})x_2 t_3 t_4 \dots t_r + (a_{11}a_{23} - a_{21}a_{13})x_3 t_2 t_4 \dots t_r \\ + \dots + (a_{11}a_{2r} - a_{21}a_{1r})x_r t_2 t_3 \dots t_{r-1}$$

$$\frac{a_{11}y_3 - a_{31}y_1}{t_1} = (a_{11}a_{32} - a_{31}a_{12})x_2 t_3 t_4 \dots t_r + (a_{11}a_{33} - a_{31}a_{13})x_3 t_2 t_4 \dots t_r \\ + \dots + (a_{11}a_{3r} - a_{31}a_{1r})x_r t_2 t_3 \dots t_{r-1}$$

Introduisons de même l'idéal premier homogène $\mathfrak{p}_i$ de $k[Y_1, Y_2, Y_3]$ engendré par $a_{i1}Y_2 - a_{2i}Y_1$, $a_{i1}Y_3 - a_{3i}Y_1$, c'est-à-dire l'idéal homogène du point $P_i(a_{i1}, a_{2i}, a_{3i})$ dans le plan projectif. Soit

$$(3) \quad m_{i_1, \dots, i_r} = \mathfrak{p}_1^{i_1} \cap \dots \cap \mathfrak{p}_r^{i_r}$$

qui est un idéal homogène de $k[Y_1, Y_2, Y_3]$. Alors, si $c \in m_{i_1, \dots, i_r}$, $c(y_1, y_2, y_3)$ est divisible par $t_1^{i_1} t_2^{i_2} \dots t_r^{i_r}$. Nous étendons la définition des $m_{i_1, \dots, i_r}$ au cas des indices entiers < 0 en convenant que, dans la formule (3), $\mathfrak{p}_\ell^{i_\ell} = k[Y_1, Y_2, Y_3]$ si $i_\ell < 0$.

CONCLUSION. - Si, dans l'expression (2) $c_{i_1, \dots, i_r} \in m_{i_1, \dots, i_r}$ pour chaque système $i_1, \dots, i_r$, alors $Q \in I$.

4. Nous allons voir que les conditions $c_{i_1}, \dots, c_{i_r} \in \mathfrak{m}_{i_1}, \dots, \mathfrak{m}_{i_r}$ sont, non seulement suffisantes, mais aussi nécessaires pour que $Q \in I$.

Considérons, dans $k(x_1, \dots, x_r, t_1, \dots, t_r)$, l'anneau local $V_1 = k[x_1, \dots, x_r, t_1, \dots, t_r]_{(t_1)}$, d'idéal maximal $t_1 V_1$. C'est l'anneau d'une valuation discrète v_1 (qui donne l'ordre de divisibilité par t_1 d'une fraction rationnelle). Le quotient $V_1/t_1 V_1$ s'identifie canoniquement à $k(x_1, \dots, x_r, t_2, \dots, t_r)$, et les images canoniques dans ce quotient de

$$y_1, z_1 = \frac{a_{11}y_2 - a_{21}y_1}{t_1}, \quad z_2 = \frac{a_{11}y_3 - a_{31}y_1}{t_1}, \quad t_2, t_3, \dots, t_r$$

sont algébriquement indépendantes sur k comme on le voit facilement.

LEMME A. - Soient K une extension de k , v une valuation discrète de K triviale sur k , τ un élément de K de valuation 1, $\zeta_1, \dots, \zeta_\ell$ des éléments de K de valuation 0 dont les classes dans le corps résiduel sont algébriquement indépendantes sur k . Alors, si

$$\xi = \sum_{n_1, \dots, n_\ell, m} c_{n_1, \dots, n_\ell, m} \zeta_1^{n_1} \dots \zeta_\ell^{n_\ell} \tau^m \in K \quad (c_{n_1, \dots, n_\ell, m} \in k^*),$$

on a

$$v(\xi) = \inf v(c_{n_1, \dots, n_\ell, m} \zeta_1^{n_1} \dots \zeta_\ell^{n_\ell} \tau^m) = \inf m.$$

DEMONSTRATION. - On a évidemment $v(\xi) \geq \inf m$. Pour montrer l'égalité, on peut supposer (quitte à multiplier par une puissance de t) que $\inf m = 0$, et on doit alors voir que $v(\xi) = 0$, c'est-à-dire que la classe de ξ dans le corps résiduel est $\neq 0$; or ceci résulte de l'hypothèse faite sur les ζ_i .

REMARQUE. - Si, dans l'expression de ξ , on regroupe certains des termes, on a encore $v(\xi) = \inf v$ (sommes partielles) : ceci résulte du lemme lui-même.

Nous revenons maintenant aux notations qui précèdent le lemme A.

LEMME B. - Si les $c_{i_1}, \dots, c_{i_r}$ sont dans $k[Y_1, Y_2, Y_3]$, on a

$$\begin{aligned} v_1 \left(\sum c_{i_1, \dots, i_r} (y_1, y_2, y_3) t_1^{-i_1} \dots t_r^{-i_r} \right) \\ = \inf v_1 (c_{i_1, \dots, i_r} (y_1, y_2, y_3) t_1^{-i_1} \dots t_r^{-i_r}) \end{aligned}$$

DEMONSTRATION. - Posant $u_1 = a_{11}y_2 - a_{21}y_1 = z_1t_1$, $u_2 = a_{11}y_3 - a_{31}y_1 = z_2t_1$, on a

$$\begin{aligned} \sum c_{i_1, \dots, i_r}(y_1, y_2, y_3)t_1^{-i_1} \dots t_r^{-i_r} &= \sum c_{i_1, \dots, i_r}^*(y_1, u_1, u_2)t_1^{-i_1} \dots t_r^{-i_r} \\ &= \sum c_{i_1, \dots, i_r, n_1, n_2, n_3} y_1^{n_1} u_1^{n_2} u_2^{n_3} t_1^{-i_1} \dots t_r^{-i_r} \\ &= \sum c_{i_1, \dots, i_r, n_1, n_2, n_3} y_1^{n_1} z_1^{n_2} z_2^{n_3} t_1^{-i_1+n_2+n_3} t_2^{-i_2} \dots t_r^{-i_r} \end{aligned}$$

et il suffit d'appliquer le lemme A et la remarque qui le suit.

LEMME C. - Si $c \in k[Y_1, Y_2, Y_3]$, on a

$$v_1(c(y_1, y_2, y_3)) \geq m \Leftrightarrow c \in \mathfrak{P}_1^m$$

DEMONSTRATION. - On a

$$c(y_1, y_2, y_3) = c^*(y_1, u_2, u_3) = \sum c_{n_1, n_2, n_3} y_1^{n_1} u_2^{n_2} u_3^{n_3}$$

D'après le lemme A, $v_1(c(y_1, y_2, y_3)) = \inf(n_2 + n_3)$. Donc

$$v_1(c(y_1, y_2, y_3)) \geq m \Leftrightarrow c^*(Y_1, U_2, U_3) \in (U_2, U_3)^m \Leftrightarrow c(Y_1, Y_2, Y_3) \in \mathfrak{P}_1^m$$

On définit les v_ℓ comme v_1 en remplaçant t_1 par t_ℓ .

Ceci dit, supposons que $Q = \sum c_{i_1, \dots, i_r}(y_1, y_2, y_3)t_1^{-i_1} \dots t_r^{-i_r}$

soit un polynôme en $x_1, \dots, x_r, t_1, \dots, t_r$. Alors $v_\ell(Q) \geq 0$, donc

$v_\ell(c_{i_1, \dots, i_r}(y_1, y_2, y_3)t_1^{-i_1} \dots t_r^{-i_r}) \geq 0$ d'après le lemme B, donc

$v_\ell(c_{i_1, \dots, i_r}(y_1, y_2, y_3)) \geq i_\ell$, donc $c_{i_1, \dots, i_r} \in \mathfrak{P}_\ell^{i_\ell}$ d'après le lemme C.

Ceci étant vrai pour tout ℓ , on a $c_{i_1, \dots, i_r} \in \mathfrak{M}_{i_1, \dots, i_r}$.

CONCLUSION. - Pour que $Q = \sum c_{i_1, \dots, i_r}(y_1, y_2, y_3)t_1^{-i_1} \dots t_r^{-i_r}$ appartienne à I, il faut et il suffit que $c_{i_1, \dots, i_r} \in \mathfrak{M}_{i_1, \dots, i_r}$ pour chaque système $(i_1, \dots, i_r)$.

5. Supposons l'algèbre I de type fini. Alors I est engendrée par un nombre fini d'éléments du type $c_{i_1, \dots, i_r} (y_1, y_2, y_3) t_1^{-i_1} \dots t_r^{-i_r}$ ($c_{i_1, \dots, i_r}$ homogène, $c_{i_1, \dots, i_r} \in \mathfrak{M}_{i_1, \dots, i_r}$). Pour chacun de ces éléments, formons le nombre

$$\frac{\text{degré de } c_{i_1, \dots, i_r}}{i_1 + i_2 + \dots + i_r}$$

Soit d le plus petit de ces nombres.

Soit maintenant c un élément homogène de $\mathfrak{M}_{j_1, \dots, j_r}$. On a $c(y_1, y_2, y_3) t_1^{-j_1} \dots t_r^{-j_r} \in I$, donc $c(y_1, y_2, y_3) t_1^{-j_1} \dots t_r^{-j_r}$ s'exprime comme polynôme par rapport aux $c_{i_1, \dots, i_r} (y_1, y_2, y_3) t_1^{-i_1} \dots t_r^{-i_r}$ envisagés précédemment. Considérant les termes en $t_1^{-j_1} \dots t_r^{-j_r}$, $c(y_1, y_2, y_3) t_1^{-j_1} \dots t_r^{-j_r}$ est somme de produits

$$c_{i_1, \dots, i_r} (y_1, y_2, y_3) t_1^{-i_1} \dots t_r^{-i_r} \dots c_{i'_1, \dots, i'_r} (y_1, y_2, y_3) t_1^{-i'_1} \dots t_r^{-i'_r}$$

avec $i_1 + \dots + i'_1 = j_1, \dots, i_r + \dots + i'_r = j_r$. Donc :

$$\frac{\deg c}{j_1 + \dots + j_r} = \frac{\deg c_{i_1, \dots, i_r} + \dots + \deg c_{i'_1, \dots, i'_r}}{i_1 + \dots + i_r + \dots + i'_1 + \dots + i'_r} \geq d$$

CONCLUSION. - Si I est de type fini, l'expression $\frac{\deg c}{j_1 + \dots + j_r}$, ($c \in \mathfrak{M}_{j_1, \dots, j_r}$, c homogène) atteint son minimum quand $j_1, \dots, j_r, c$ varient.

6. Montrons que la borne inférieure des nombres $\frac{\deg c}{j_1 + \dots + j_r}$ ($c \in \mathfrak{M}_{j_1, \dots, j_r}$, c homogène) est $\leq \frac{1}{\sqrt{r}}$. Pour cela, donnons une interprétation géométrique qui sera aussi utile plus loin. L'équation $c = 0$ est l'équation homogène d'une courbe algébrique (ou plutôt d'un diviseur positif) C du plan projectif. Dire que $c \in \mathfrak{M}_{j_1, \dots, j_r}$ signifie que C passe par P_1 avec une multiplicité $\geq j_1, \dots$, par P_r avec une multiplicité $\geq j_r$. Les nombres $j_1, \dots, j_r$ étant donnés, on pourra trouver une telle courbe C de degré d pourvu que

$$\frac{(d+1)(d+2)}{2} - 1 \geq \frac{j_1(j_1+1)}{2} + \dots + \frac{j_r(j_r+1)}{2}$$

Si $j_1 = j_2 = \dots = j_r = j$, cette inégalité s'écrit

$$d^2 + 3d \geq rj(j+1)$$

ou

$$\frac{d}{rj} \sqrt{\frac{1+3/d}{1+1/j}} \geq \frac{1}{\sqrt{r}} ;$$

pour d et j assez grand, on peut y satisfaire avec un rapport $\frac{d}{rj} = \frac{d}{j_1 + \dots + j_r}$ aussi voisin qu'on veut de $\frac{1}{\sqrt{r}}$. D'où le résultat annoncé.

CONCLUSION. - Supposons prouvée l'assertion suivante :

(*) Si une courbe C de degré d passe par chaque P_ℓ avec une multiplicité $\geq j_\ell$, alors

$$\frac{d}{j_1 + \dots + j_\ell} > \frac{1}{\sqrt{r}}$$

Alors, d'après ce qui précède, les nombres $\frac{d}{j_1 + \dots + j_\ell}$ n'atteignent pas leur minimum, donc, d'après 5, I n'est pas de type fini.

7. Il est facile de voir que, pour les petites valeurs de r (au moins jusqu'à 9 inclus), (*) n'est pas satisfaite. On va prouver (*) pour $r = 25$. (En fait, NAGATA affirme que (*) est vrai pour $r = s^2$, $s \geq 4$).

Supposons qu'il existe une courbe C de degré d passant par chaque P_ℓ avec la multiplicité j_ℓ , et $\frac{d}{j_1 + \dots + j_r} \leq \frac{1}{\sqrt{r}}$. Vu l'indépendance des a_{ij} , on en déduit, par spécialisation, une courbe de degré d passant par chaque P_ℓ avec la multiplicité $j_{\sigma(\ell)}$, où σ est une permutation arbitraire de $\{1, 2, \dots, r\}$.

En prenant la réunion de ces courbes, on a une courbe de degré d' passant par chaque P_ℓ avec une même multiplicité j' , et $\frac{d'}{rj'} \leq \frac{1}{\sqrt{r}}$. Il suffit donc d'établir le résultat suivant :

(**) Si une courbe C de degré d du plan projectif passe par 25 points algébriquement indépendants avec une multiplicité $\geq m$, alors $\frac{d}{m} > 5$.

2e partie : Constructions de courbes.

1. Soit C une courbe irréductible non singulière de degré n dans le plan projectif. Si $n \geq 3$, la jacobienne J de C n'est pas réduite à l'élément neutre. Le sous-groupe J_t de J formé des points d'ordre fini est dénombrable. Donc toute application rationnelle d'une variété algébrique dans J , qui n'est pas une constante, a une image non contenue dans J_t (on se place, pour simplifier, sur le corps complexe).

Soit a un diviseur ≥ 0 sur C , de degré $n\delta$ multiple de n . Soit d'autre part h le diviseur $C.D$, où D est une droite du plan. Le diviseur $a - \delta.h$ est de degré 0, donc définit un élément de J qu'on notera $\theta(a)$. Si a est de la forme $C.C'$, où C' est un diviseur positif du plan de degré δ , on a $\theta(a) = 0$ (car, si $f' = 0$ et $t = 0$ sont les équations de C' et D , la restriction à C de $f' t^{-\delta}$ a pour diviseur $a - \delta.h$). Donc :

Si $\theta(a) \notin J_t$, aucun multiple de a n'est l'intersection avec C d'un diviseur du plan.

2. Soit C_5 une courbe irréductible non singulière de degré 5. Soit $a = Q_1 + Q_2 + \dots + Q_5$ un diviseur de C_5 tel que $\theta(a) \notin J_t$. (Pour le construire, on choisit arbitrairement $Q_1, \dots, Q_4$; pour Q variable sur C_5 , l'image $f(Q)$ dans J du diviseur $h - Q_1 - Q_2 - Q_3 - Q_4 - Q$ n'est pas fixe, car les $f(Q) - f(Q')$ engendrent J ; cette image est donc hors de J_t pour Q bien choisi).

Soient C_3, C'_3 des cubiques passant par $Q_1, \dots, Q_5$. Posons

$$C_3.C_5 = Q_1 + \dots + Q_5 + R_1 + \dots + R_{10}, \quad C'_3.C_5 = Q_1 + \dots + Q_5 + S_1 + \dots + S_{10}.$$

LEMME D. - Il n'existe pas de courbe E de degré $5m - 1$ passant $m - 1$ fois au moins par chaque Q_i et m fois au moins par chaque R_i et chaque S_i .

Si $E \supset C_5$, on remplace E par $E - C_5$, et on est ramené à la situation analogue pour $m - 1$. On peut donc supposer que $E \not\supset C_5$ et $E.C_5$ est défini. On a $E.C_5 \geq (m - 1) \sum Q_i + m \sum (R_i + S_i)$; ces deux diviseurs ont même degré donc sont égaux. D'où $(m - 1)\theta(a) + m \theta(\sum R_i) + m \theta(\sum S_i) = 0$. Par ailleurs $\theta(a) + \theta(\sum R_i) = 0$, $\theta(a) + \theta(\sum S_i) = 0$. Donc $(m + 1)\theta(a) = 0$, contrairement au choix de a .

3. Soient C_5, C_3, C'_3 trois courbes du plan de degrés 5, 3, 3, dont les équations ont des coefficients algébriquement indépendants. Choisissons une spécialisation de ces 3 courbes sur les 3 courbes de 2, et prenons des points $Q_1, \dots, Q_5$ dans $C_3 \cdot C'_3$, $R_1, \dots, R_{10}$ dans $C_3 \cdot C_5$, $S_1, \dots, S_{10}$ dans $C'_3 \cdot C_5$ qui viennent se spécialiser aux points correspondants de 2. Nous allons montrer qu'il n'y a pas de courbe E' de degré $5(m+1)$ passant par chacun des points $Q_1, \dots, Q_5, R_1, \dots, R_{10}, S_1, \dots, S_{10}$ avec une multiplicité $\geq m+1$. (Ceci achèvera la démonstration, car, a fortiori, il n'existera pas de courbe de degré $5(m+1)$ passant par 25 points algébriquement indépendants avec une multiplicité $\geq m+1$). Raisonnant par l'absurde, supposons qu'il existe une telle courbe E' . La courbe E' contient C_3 , car, sinon, $E' \cdot C_3$ serait un diviseur de degré $15(m+1)$ supérieur à $(m+1)(\sum Q_1 + \sum R_1)$, donc égal à ce dernier, donc $(m+1)\theta(\sum Q_1 + \sum R_1) = 0$ dans la jacobienne de C_3 , donc (si on identifie C_3 à sa jacobienne par choix d'un point de base algébrique sur le corps premier) le point $\sum Q_1 + \sum R_1$ de C_3 serait algébrique sur le corps premier, et on va voir plus bas que ceci est impossible. De même, E' contient C'_3 . Alors $E = E' - C_3 - C'_3$ est une courbe de degré $5m-1$ passant $m-1$ fois au moins par chaque Q_1 et m fois au moins par chaque R_1 et chaque S_1 . Spécialisant $C_5, C_3, C'_3, Q_1, R_1, S_1$, E sur la situation de 2, on aboutit à une contradiction.

Nous sommes donc ramenés à prouver que le point $\sum Q_1 + \sum R_1$ de C_3 ne peut pas être algébrique sur le corps premier. Fixons C_3, C_5 et les R_1 . On va montrer (ce qui achèvera la démonstration) que, quand on fait varier la cubique C'_3 , le point $\sum Q_1$ peut être un point arbitraire de C_3 . On va même montrer mieux :

LEMME E. - Soient C une cubique fixe de genre 1, rationnelle sur un corps K , C' une cubique générique sur K , et $(Q_1, \dots, Q_5)$ cinq des points d'intersection de C et C' . Alors $(Q_1, \dots, Q_5)$ est un point générique de $C \times \dots \times C = C^5$.

DEMONSTRATION. - Soit P l'espace projectif de toutes les cubiques. Dans $P \times C^5$, considérons les systèmes (c, z) tels que z soit formé de 5 des points d'intersection de c et C . Ces systèmes forment un fermé F de $P \times C^5$. L'adhérence de $(C', (Q_1, \dots, Q_5))$ pour la K -topologie est une variété irréductible $V \subset F$. La projection $\text{pr}_1 : V \rightarrow P$ est surjective, donc

$\dim V \geq 9$. On va montrer, ce qui achèvera la démonstration, que la projection $\text{pr}_2 : V \rightarrow \mathbb{C}^5$ est surjective. S'il n'en était pas ainsi, $\text{pr}_2(V)$ serait de dimension ≤ 4 , donc les images réciproques des points de $\text{pr}_2(V)$ dans V seraient de dimension $\geq 9 - 4 = 5$. Autrement dit, il existerait 5 points $A_1, \dots, A_5$ sur C tels que la variété (linéaire) des cubiques passant par $A_1, \dots, A_5$ soit de dimension ≥ 5 . Par $A_1, \dots, A_5$ et par 3 points A_6, A_7, A_8 de C , il passerait ∞^2 cubiques, ce qui est absurde (si on impose un 9^e point distinct du point associé sur C à $A_1, \dots, A_8$, on sait qu'on obtient une seule cubique).
