Séminaire Dubreil.
Algèbre et théorie
des nombres

LUC GAUTHIER

Géométrie infinitésimale des courbes algébriques planes ou gauches sur un corps de caractéristique p

Séminaire Dubreil. Algèbre et théorie des nombres, tome 9 (1955-1956), exp. nº 7, p. 1-14
<http://www.numdam.org/item?id=SD_1955-1956__9__A4_0>

Faculté des Sciences de Paris
-:-:-:-

Séminaire P. DUBREIL et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1955/1956
-:-:-:-

19 décembre 1955

Exposé n° 7

GÉOMÉTRIE INFINITÉSIMALE DES COURBES ALGÉBRIQUES PLANES OU GAUCHES SUR UN CORPS DE CARACTÉRISTIQUE p .

par Luc GAUTHIER.

La présente étude de Géométrie Infinitésimale m'a été suggérée par la lecture de la conférence faite au Séminaire d'Algèbre l'an dernier par M. P. SAMUEL, sur les courbes planes en caractéristique 2, et les travaux publiés avec ses élèves : M. P. BOUGHON et Mlle J. NATHAN. La présentation du théorème 2, concernant la classe d'une courbe plane avait beaucoup choqué mon sens géométrique ; bien entendu la définition de l'équation tangentielle, et de la classe en géométrie sur un corps de caractéristique $p \neq 0$ est purement conventionnelle, et le résultat obtenu par M. SAMUEL est incontestablement correct : c'est donc simplement l'habitude de conventions différentes qui a provoqué mon dissentiment. Comme les conventions auxquelles je suis habitué ont l'avantage d'être uniformément les mêmes quelle que soit la caractéristique du corps de base, et quelle que soit la nature du contact envisagé, j'ai pensé qu'il était peut-être intéressant de vous présenter mon point de vue.

Mon exposé comprendra trois parties :

Dans la première partie, je rappellerai les notions d'algèbre qui permettent de définir ce qu'à mon avis il y a lieu d'appeler "Géométrie infinitésimale en caractéristique p".

Dans la seconde partie, je vous exposerai le moyen technique que j'ai mis au point pour l'étudier, c'est une transformation birationnelle que j'ai appelée "perfectionnement" de la courbe.

Dans la troisième partie, j'indiquerai quelques résultats. (Nous retrouverons en particulier, dans le cas de la caractéristique 2 et du contact ordinaire, les résultats de l'Ecole de M. SAMUEL).

Rappel de la notion de Place.-

Considérons dans un plan projectif (x_1 , x_2 , x_3) une courbe algébrique

$$F(x_1 , x_2 , x_3) = 0$$

F étant un polynôme à coefficients dans un corps k .

Nous associons à k le corps $\tilde{k}(t)$ des séries formelles :

$$\tilde{f} = \sum_{h=\omega}^{\infty} a_h t^h$$

où $a_h \in k$, $a_\omega \neq 0$; ω entier rationnel (positif, négatif ou nul) est appelé l'ordre de $\tilde{f}$.

Un ensemble $(\tilde{x}_1 , \tilde{x}_2 , \tilde{x}_3)$ qui vérifie

$$F(\tilde{x}_1 , \tilde{x}_2 , \tilde{x}_3) = \tilde{0}$$

est défini à un facteur $\tilde{\rho}$ près, et donne à toute fraction rationnelle $R \in k(x_1 , x_2 , x_3)$ mod F , définie sur la courbe, une "valeur", $\tilde{R} \in \tilde{k}(t)$ ce qui permet de passer aux courbes gauches.

En prenant pour $\tilde{\rho}$ une puissance convenable de t , on peut faire en sorte que les $\tilde{x}_i \in \tilde{k}[t]$, l'une au moins ayant un ordre nul : soit $\tilde{x}_3$ (permutation éventuelle des indices). En prenant pour $\tilde{\rho}$ son inverse $\tilde{x}_3^{-1}$, on est ramené à la géométrie affine :

$$(\tilde{x} , \tilde{y} , 1)$$

Si $\tilde{x} , \tilde{y} \in k$, on a obtenu un point de la courbe.

S'il n'en est pas ainsi, on dit que $\tilde{x} , \tilde{y}$ définissent une "représentation paramétrique locale". L'application $\tilde{f} \to a_0$ définit un point de la courbe qu'on appelle "centre" de cette représentation.

La possibilité d'effectuer un changement de variable :

$$\bar{t} = \tilde{g}(t)$$

$\tilde{g}$ appartenant au groupe des séries formelles d'ordre 1, définit une relation d'équivalence dans l'ensemble des représentations paramétriques locales concentriques. On montre qu'on peut toujours trouver un représentant de cette classe, de la forme :

$$\tilde{x} = x_0 + t^n$$
$$\tilde{y} = y_0 + \sum a_i t^{n_i}$$

où

$$1 \leqslant n \leqslant n_1 < n_2 < \cdots\cdots$$

les a_i tous $\neq 0$.

Soit :

$$d = (n , n_1 , n_2 , \cdots\cdots)$$

Si $d = 1$ la représentation est dite irréductible. Si $d > 1$, le changement de variable :

$$\bar{t} = t^d$$

a un sens, et la nouvelle représentation est irréductible.

Ceci étant rappelé, on appelle <u>place</u> une classe d'équivalence de représentations paramétriques locales irréductibles.

On démontre au sujet des places le théorème fondamental suivant :

Sur un corps k algébriquement clos, tout point de la courbe est centre d'au moins une place (et au plus d'un nombre fini).

On appelle Riemannienne de la courbe l'ensemble de ses places. Si $n > 1$, les dérivées partielles premières de F s'annulent au centre de la place, qui est un point singulier. En un point simple on a donc toujours $n = 1$. Une place pour laquelle $n = 1$ est appelée simple : en ramenant l'origine des coordonnées au centre de la place, nous écrirons :

$$\tilde{x} = x$$
$$\tilde{y} = \sum_{h=1}^{\infty} a_h x^h$$

<u>Choix d'une topologie dans le corps des séries formelles.-</u>

Les séries formelles formant un espace vectoriel il suffit de définir un voisinage de zéro. Nous poserons par définition :

$$t^n \longrightarrow 0 \quad \text{quand} \quad n \longrightarrow \infty$$

et nous aurons un système dénombrable de voisinages de zéro, en appelant n-ième voisinage de zéro l'ensemble V_n des séries formelles d'ordre

$$\omega \geqslant n + 1$$

La considération de V_n définit dans $\tilde{k}(t)$ une relation d'équivalence, $\tilde{f}$ et $\tilde{g}$ étant équivalentes si leur différence est dans V_n. La topologie que nous avons définie est compatible avec la structure du corps $\tilde{k}(t)$ car cette équivalence est un homomorphisme : elle conserve en effet l'addition et la multiplication puisqu'on peut encore l'exprimer en disant que $\tilde{f}$ et $\tilde{g}$ sont équivalentes si elles sont congrues modulo t^{n+1}.

Notre topologie est également compatible avec la dérivation : on vérifie en effet aisément que :

$$\frac{\tilde{f}(t+\tilde{\varphi}_n) - \tilde{f}(t)}{\tilde{\varphi}_n} \longrightarrow \tilde{f}'(t)$$

où $\tilde{\varphi}_n \in V_n$ et $n \longrightarrow \infty$.

<u>Elément de contact d'ordre</u> n.

On peut, avec ce qui précède définir le contact de deux courbes algébriques en un point commun A ; je me bornerai, pour les besoins de la suite au cas de deux places simples de centre A.

Soient deux places simples concentriques (appartenant à des courbes distinctes ou non), dont nous prenons le centre comme origine de coordonnées affines, munies d'un paramètre commun x :

$$\begin{cases} \tilde{x}_1 = x \\ \tilde{y}_1 = \sum a_h x^h \end{cases} \qquad \begin{cases} \tilde{x}_2 = x \\ \tilde{y}_2 = \sum b_h x^h \end{cases}$$

Nous dirons que ces deux places ont un contact d'ordre n si la série formelle $\tilde{y}_1 - \tilde{y}_2$ est dans le voisinage V_n de zéro. Deux courbes algébriques sont localement équivalentes (n donné) en un couple de places simples concentriques, si ces deux places ont un contact d'ordre n.

Nous appellerons "<u>élément de contact d'ordre</u> n" la classe d'équivalence ainsi définie.

<u>Remarque</u> : le contact d'ordre 1, dit ordinaire, signifie que :

$$y'_1 = y'_2$$

c'est-à-dire que les deux places ont la même tangente.

Mais je ne vais pas au-delà de l'ordre 1 dans cette voie, car la définition du contact par l'égalité des dérivées successives, qui est traditionnelle en caractéristique zéro, perd son sens pour $n \geqslant p$ en caractéristique p (en caractéristique 2, par exemple, $\tilde{y}'' = \tilde{0}$).

Les considérations qui précèdent s'étendent sans aucune difficulté aux variétés algébriques de dimensions quelconques, en utilisant des anneaux de séries formelles à plusieurs indéterminées.

L'ordre de contact d'un hyperplan :

$$L = u_1 x_1 + \dots + u_r x_r = 0$$

avec une place simple d'une courbe gauche centrée à l'origine des coordonnées :

$$\begin{cases} \tilde{x}_1 = x \\ \tilde{x}_i = \sum a_{ih} x^h \qquad i = 2, \dots, r \end{cases}$$

est $n = \omega - 1$, où ω est l'ordre de la série :

$$\tilde{L} = u_1 x + \sum u_i \tilde{x}_i$$

<u>Définition</u> :

La géométrie infinitésimale en caractéristique p est l'étude des éléments de contacts de tous ordres, au sens que nous venons de préciser.

- II -

Nous supposerons désormais le corps de base k de caractéristique $p \neq 0$, parfait (tout élément de k est la puissance p-ième d'un élément de k) : en l'absence de cette dernière propriété, il y aurait lieu, dans l'étude de certains polynômes, d'envisager l'extension finie du corps k dans laquelle tous les coefficients sont des puissances p-ièmes.

<u>Perfectionnement d'une courbe algébrique</u> :

Considérons un plan projectif $P : (x_1, x_2, x_3)$: Nous lui associons ν plans $P_i : (x_{i1}, x_{i2}, x_{i3})$ et sur la variété de SEGRE produit de ces $\nu + 1$ plans projectifs, nous envisageons la surface rationnelle (strictement équivalente au plan P) d'équations :

$$\text{Rang} \begin{pmatrix} x_1^{p^\nu} & x_{11}^{p^{\nu-1}} & \cdots\cdots & x_{i1}^{p^{\nu-i}} & \cdots\cdots & x_{\nu 1} \\ x_2^{p^\nu} & x_{12}^{p^{\nu-1}} & \cdots\cdots & x_{i2}^{p^{\nu-i}} & \cdots\cdots & x_{\nu 2} \\ x_3^{p^\nu} & x_{13}^{p^{\nu-1}} & \cdots\cdots & x_{i3}^{p^{\nu-i}} & \cdots\cdots & x_{\nu 3} \end{pmatrix} = 1$$

Toute courbe algébrique

$$F(x_1 , x_2 , x_3) = 0$$

admet sur cette surface une transformée birationnelle, que nous appelons son ν-ième perfectionnement.

Cette transformation, essentiellement liée à la caractéristique du corps de base et à la relation

$$y = x^p$$

fournit pour les courbes algébriques des modèles particulièrement commodes pour l'étude des questions que nous avons en vue.

Pour simplifier, j'exposerai ce point par voie purement algébrique en coordonnées affines.

<u>Prolégomènes</u>.-

I) Si $f(x , y)$ est un polynôme $\in k[x , y]$, alors $f^p = F$ est un polynôme $\in k[\xi, \eta]$, où $\xi = x^p$, $\eta = y^p$, et réciproquement.

En effet :

$$f = \sum M_{\alpha\beta} = \sum a_{\alpha\beta} x^\alpha y^\beta$$

$$F = f^p = (\sum M)^p = \sum M^p = \sum a^p_{\alpha\beta} x^{p\alpha} y^{p\beta}$$

$$= \sum A_{\alpha\beta} \xi^\alpha \eta^\beta$$

où $A_{\alpha\beta} = a^p_{\alpha\beta}$

et réciproquement puisque k est parfait.

<u>Corollaire</u> : Cette propriété est également vraie pour une fraction rationnelle

$$r(x , y) \in k(x , y) : r^p \in k(\xi, \eta) .$$

II) Soit $f(x , y)$ un polynôme de $k[x , y]$:

$$f = \sum_{i,j} A_{ij} x^i y^j$$

effectuons la division par p des exposants :

$$i = p\,q + \alpha \qquad 0 \leq \alpha < p$$
$$j = p\,q' + \beta \qquad 0 \leq \beta < p$$

On peut mettre f sous la forme :

$$f = \sum_{\alpha,\beta} \Big(\sum_{q,q'} A_{ij}\, \xi^{q}\, \eta^{q'}\Big)\, x^{\alpha}\, y^{\beta} = \sum_{\alpha,\beta} B_{\alpha,\beta}\, x^{\alpha}\, y^{\beta}$$

c'est-à-dire d'un polynôme à coefficients $B_{\alpha,\beta} \in k[\xi, \eta]$ et à exposants dans le corps des restes modulo p.

III) Soit $r(x, y)$ une fraction rationnelle de $k(x, y)$:

$$r = \frac{f}{g} = \frac{fg^{p-1}}{g^{p}} = \sum_{\alpha,\beta} C_{\alpha,\beta}\, x^{\alpha}\, y^{\beta}$$

est un polynôme à coefficients $C_{\alpha,\beta} \in k(\xi, \eta)$ et à exposants dans le corps des restes modulo p.

<u>Théorème de Clôture</u> :

<u>Lemme</u> : Si x est algébrique sur k et si $f(x)$ est son polynôme minimal

$$f'(x) \neq 0$$

En effet : si $f(x) = 0$, avec $f'(x) \not\equiv 0$, l'équation $f'(x) = 0$ est une équation de degré moindre vérifiée par x, en contradiction avec le fait que $f(x)$ est minimal. Si $f'(x) \equiv 0$, l'utilisation du prolégomène II montre que $f(x) \in k[\xi]$, et d'après I c'est une puissance p-ième : même contradiction.

<u>Théorème</u> : Si x est algébrique sur k, il est rationnel sur $k(\xi)$.

Ce théorème requiert quelque minutie : je ne donnerai ici qu'une brève indication sur sa démonstration.

Soit $f(x)$ le polynôme minimal de x.

En caractéristique $p = 2$, le prolégomène II permet d'écrire $f(x)$ sous la forme d'un polynôme à coefficients dans $k[\xi]$, dont les exposants de x sont 1 et 0 ; le coefficient de x n'est pas nul car c'est $f'(x) \neq 0$ d'après le lemme.

En caractéristique $p > 2$, il y a lieu de déterminer un multiplicateur $g(x)$ tel que :

$$f(x)\ \ g(x) = A(\xi)\, x + B(\xi)$$

et on montre que ce multiplicateur $g(x)$ a les propriétés suivantes : (application du théorème de Wilson)

$$g(x) = f'^{p-2} \mod f$$

$$A(\xi) = f'^{p-1} \mod f$$

Il résulte alors du lemme que l'équation $fg = 0$ définit bien x rationnel sur $k(\xi)$. Bien entendu l'existence du facteur g introduit, en caractéristique $p > 2$ des solutions étrangères, mais cela est sans importance et signifie seulement qu'il y a plusieurs polynômes $f(x)$ qui conduisent à la même expression rationnelle sur $k(\xi)$ pour exprimer leurs racines.

<u>Exemple</u> : Considérons l'équation

$$x^2 - a = 0 \qquad (1)$$

en caractéristique $p = 5$.
On écrit successivement :

$$x^4 = a^2$$

$$x^5 = a^2 x$$

$$x = \frac{\xi}{a^2} \qquad (2)$$

l'équation (2) est vérifiée non seulement par les solutions $x = \pm\sqrt{a}$ de (1) mais aussi par $x = 0$ et $x = \pm\sqrt{-a}$.

<u>Premier perfectionnement (en projection) d'une courbe plane.</u>

Soit $f(x, y) = 0$ une courbe plane, éventuellement réductible, mais privée de composante p-uple. On a alors grad $f \not\equiv 0$ (démonstration analogue au lemme précédent). En un point non singulier grad $f \neq 0$, il existe au moins une des coordonnées pour laquelle la dérivée partielle de f n'est pas nulle, soit y .

D'après le théorème de clôture, on peut tirer

$$y = R(x)$$

où $R \in k(x, \eta)$ est rationnelle en x à coefficients dans $k(\eta)$. D'après le prolégomène III on peut l'exprimer sous la forme :

$$y = P(x)$$

où P est un polynôme en x , à exposants dans le corps des restes mod p , et à coefficients dans le corps $k(\xi, \eta)$.

C'est cette représentation de y comme polynôme en x de degré $p - 1$ au plus, dont les coefficients sont des puissances p-ièmes parfaites de fractions rationnelles, qui constitue le premier perfectionnement de la courbe.

Réitération du processus.-

Considérons un coefficient $A(\xi, \eta)$ de P ; en élevant l'expression perfectionnée de y à la puissance p, on obtient (prolégomène I) :

$$\eta = P^p(x) = P^*(\xi)$$

où $P^* \in k(\xi^p ; \eta^p)[\xi]$.

En reportant dans A, on obtient une expression rationnelle en ξ, à coefficients dans $k(\xi^p ; \eta^p)$, qui d'après le prolégomène III peut encore être mise sous la forme d'un polynôme en ξ, à coefficients dans ce même corps, et à exposants pris dans les restes modulo p.

En posant $\xi^p = \xi'$, $\eta^p = \eta'$ dans les coefficients, puis $\xi = x^p$ l'expression de y prend alors la forme d'un polynôme $\in k(\xi', \eta')[x]$ à exposants pris dans l'anneau des restes modulo p^2.

Ceci est le principe d'une récurrence qui conduit au résultat suivant :

Il est possible de représenter la courbe plane :

$$f(x , y) = 0$$

par une équation de la forme :

$$y = P(x)$$

où P est un polynôme en x de degré $p^\nu - 1$, au plus, à coefficients dans le corps $k(x^{p^\nu} , y^{p^\nu})$.

Perfectionnement des courbes gauches.

Nous définirons une courbe gauche comme transformée rationnelle d'une courbe plane :

$$\begin{cases} x_i = R_i(u , v) & i = 1 , 2 , \ldots\ldots , r \\ f(u , v) = 0 & \end{cases}$$

où $f \in k[u , v]$ et les $R_i \in k(u , v)$.

En effectuant un perfectionnement réitéré de f et en raisonnant sur les fractions rationnelles R_i comme nous venons de le faire sur $A(\xi, \eta)$ on obtient la représentation :

$$\begin{cases} v = P(u) \\ x_i = P_i(u) \end{cases}$$

où P et les P_i sont des polynômes en u de degré $p^\nu - 1$ au plus, à coefficients dans $k(u^{p^\nu}, v^{p^\nu})$.

Remarque :

Il n'y a pas de difficulté essentielle à étendre le processus précédent aux variétés algébriques de dimension quelconque.

- III -

Courbes planes en caractéristique 2.-

Nous utiliserons le premier perfectionnement pour étudier le contact du premier ordre. L'équation d'une courbe s'écrit :

$$y = M x + N$$

où $M, N \in k(x^2, y^2)$; ou bien, en rendant l'équation entière et en tenant compte du prolégomène I :

$$A^2 x + B^2 y + C^2 = 0 \qquad (1)$$

où $A, B, C \in k[x, y]$.

L'équation de la tangente au point (x_0, y_0) de la courbe est

$$A_0^2 x + B_0^2 y + C_0^2 = 0$$

ses coordonnées tangentielles sont des carrés parfaits : nous retrouvons le résultat de SAMUEL sur le point dual.

Les tangentes issues d'un point (x_1, y_1) ont leurs contacts qui doivent vérifier, outre l'équation (1) de la courbe, l'équation de sa première polaire:

$$A^2 x_1 + B^2 y_1 + C^2 = 0 \qquad (2)$$

Cette courbe est "double" et passe par les éventuels points singuliers de la courbe donnée, qui vérifient $A = B = C = 0$.

On peut convenir, avec SAMUEL, en spécialisant (x_1 , y_1) dans le corps de base, ou en adjoignant les racines de ses coordonnées, que la classe d'une courbe de degré n sans singularité est $\frac{1}{2} n (n - 1)$; on peut aussi lui conserver la valeur $n(n - 1)$ obtenue en caractéristique $p \neq 2$ et convenir, conformément au caractère "double" de la polaire que dans le faisceau des tangentes issues d'un point, toutes les tangentes ont une multiplicité paire.

Avec cette convention, la forme adjointe (équation tangentielle) est toujours un carré parfait en caractéristique 2.

Exemple :

Reprenons le calcul classique de l'équation tangentielle d'une conique :

$$a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + b_1 x_2 x_3 + b_2 x_3 x_1 + b_3 x_1 x_2 = 0$$

Les coordonnées tangentielles de la tangente au point courant :

$$\begin{aligned} b_3 x_2 + b_2 x_3 &= \rho u \\ b_3 x_1 + \qquad + b_1 x_3 &= \rho v \\ b_2 x_1 + b_1 x_2 \qquad &= \rho w \\ u x_1 + v x_2 + w x_3 &= 0 \end{aligned}$$

sont liées par la condition exprimant que ces équations sont compatibles pour les valeurs (x_1 , x_2 , x_3 , ρ) non toutes nulles. Le déterminant classique, symétrique, est en caractéristique 2, en même temps, antisymétrique, donc carré parfait :

$$D \equiv (b_1 u + b_2 v + b_3 w)^2 = 0$$

Courbes planes en caractéristique 3.-

Dans le but d'étudier les points d'inflexion en caractéristique 3, nous utiliserons le premier perfectionnement. Une courbe de degré n , dont l'équation réduite d'après le prolégomène II est :

$$A_{n-2} y^2 + B_{n-1} y + C_n = 0$$

où $A , B , C \in k [x , y^3]$ avec des degrés égaux aux indices (en variables homogènes) s'exprime successivement sous les formes :

$$(A y - B)^2 = B^2 - A C$$

puis, par élévation au carré et réarrangement des termes :

$$(A\ y - B)^3\ y = A^2\ B\ y^3 + B^2\ C + C^2\ A$$

et, le second membre étant à son tour réduit en x, nous obtenons en coordonnées homogènes :

$$(A\ y - B)^3\ y = H^3_{n-2}\ x^2\ z^2 + M^3_{n-1}\ x + N^3_{n-1}\ z$$

Par deux dérivations successives nous obtenons :

$$(A\ y - B)^3\ y' = - H^3\ x + M^3$$

$$(A\ y - B)^3\ y'' = - H^3$$

Ainsi les points d'inflexion sont obtenus, (les points singuliers éventuels étant mis à part), par l'intersection de la courbe donnée, avec sa Hessienne :

$$H^3_{n-2} = 0$$

Cette courbe est "triple" : nous conviendrons de dire qu'il y a encore, comme en caractéristique $p \neq 3$,

$$i = 3n\ (n - 2)$$

points d'inflexion, chacun ayant une multiplicité multiple de 3.

La tangente en un point d'inflexion $(x_0\ ;\ y_0)$ a pour équation :

$$(A_0\ y_0 - B_0)^3\ y = M^3_0\ x + N^3_0\ z$$

ses coordonnées tangentielles appartiennent au corps $k(x^3_0\ ,\ y^3_0)$.

Nous voyons ici apparaître une première généralisation des résultats de M. SAMUEL on peut, en effet démontrer le théorème suivant :

<u>Théorème</u> : Dans un espace projectif à p coordonnées homogènes, une courbe algébrique sans singularité, d'ordre n, de genre g, admet des hyperplans osculateurs à contact d'ordre $p - 1$, en nombre :

$$p\left[n + (p - 1)\ (g - 1)\right]$$

et si la caractéristique du corps de base est p, ils ont tous la multiplicité p (ou un multiple de p), et leurs coordonnées tangentielles appartiennent au corps $k(x^p_i)$. Il peut également arriver, que le contact d'ordre $p - 1$ ait lieu en tous les points de la courbe.

C'est ce qui aurait lieu, en caractéristique 3, pour les courbes vérifiant $H \neq 0$, dont tous les points sont d'inflexion.

Courbes gauches en caractéristique 2.-

Dans le but d'étudier des contacts dont l'ordre dépasse la caractéristique du corps de base, nous utiliserons le second perfectionnement. Considérons dans l'espace à trois dimensions la courbe :

$$\begin{cases} y = A^4 x^3 + B^4 x^2 + C^4 x + D^4 \\ z = L^4 x^3 + M^4 x^2 + N^4 x + P^4 \end{cases} \qquad (1)$$

que nous allons couper par le plan

$$u(x - x_0) + v(y - y_0) + w(z - z_0) = 0$$

passant par le point (x_0 , y_0 , z_0) de la courbe. En prenant pour paramètre local :

$$\tilde{x} = x_0 + t$$

les premiers termes des séries formelles $\tilde{y}$, $\tilde{z}$ sont :

$$\tilde{y} = y_0 + (A_0^4 x_0^2 + C_0^4)\, t + (A_0^4 x_0 + B_0^4)\, t^2 + A_0^4 t^3 + \ldots\ldots$$

et analogues. Ils permettent de former sans difficulté l'équation du plan osculateur au point (x_0 , y_0 , z_0) et de constater que ce plan a en général un contact du second ordre avec la courbe.

Les points où le plan est surosculateur, c'est-à-dire présente un contact d'ordre 3 au moins sont obtenus en associant aux équations de la courbe (1) la condition :

$$\begin{vmatrix} A^4 x + B^4 & L^4 x + M^4 \\ A^4 & L^4 \end{vmatrix} = (A\,M + B\,L)^4 = 0 \qquad (2)$$

et si (x_0 , y_0 , z_0) est un tel point, le plan osculateur a pour équation :

$$(A_0 N_0 + C_0 L_0)^4 x + L_0^4 y + A_0^4 z + (A_0 P_0 + D_0 L_0)^4 = 0$$

Ainsi les éléments de contact d'ordre 3 ont leurs coordonnées tangentielles qui appartiennent au corps $k(x_0^4 , y_0^4 , z_0^4)$, et la surface quadruple (2) qui les détermine (en supposant $A\,M + B\,L \neq 0$) montre que leur nombre, déterminé par un procédé canonique valable en toute caractéristique, est donné par une formule valable en toute caractéristique, à condition de convenir qu'en caractéristique 2, ils ont tous la multiplicité $2^2 = 4$.

Ce résultat fait apparaître une nouvelle généralisation des résultats précédents ; on peut, en effet, démontrer le théorème suivant :

Théorème : Si une courbe algébrique définie sur un corps de caractéristique p admet un nombre fini d'éléments de contact d'ordre n, et si p^ν est la plus haute puissance de p qui divise $n+1$, ces éléments de contact ont tous la multiplicité p^ν (ou un multiple de p^ν), et leurs coordonnées tangentielles (ou grassmanniennes) appartiennent au corps $k(x_i^{p^\nu})$.

Ce résultat généralise à une courbe de genre quelconque celui obtenu sur ce même sujet par HASSE, pour les courbes de genre un.

BIBLIOGRAPHIE

P. SAMUEL : Courbes planes en caractéristique 2. Séminaire P. DUBREIL, Algèbre et Théorie des Nombres, 8, 1954/55, exposé 13.

P. BOUGHON. J. NATHAN. P. SAMUEL : Courbes planes en caractéristique 2, Bulletin Société mathématique de France, T. 83 (1955) p. 275.

H. HASSE : Zur Theorie der abstrakten elliptischen Funktionenkörper, Journal für die reine und angewandte Mathematik (Crelle), t. 175 (1936) p. 55, 65, 193.