Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 15 (1969)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LA GÉOMÉTRIE SUR LES CORPS DE CARACTÉRISTIQUE NON NULLE

Autor: Gauthier, Luc

DOI: https://doi.org/10.5169/seals-43210

LA GÉOMÉTRIE SUR LES CORPS DE CARACTÉRISTIQUE NON NULLE

par Luc GAUTHIER

à la mémoire de Jean Karamata

Lorsque Descartes eut l'idée d'associer à une figure géométrique un repère de coordonnées de façon à substituer au raisonnement basé sur l'intuition de l'espace, un calcul effectué sur les équations correspondantes, il n'avait, je crois, pas d'autre but que de faciliter le progrès de la connaissance géométrique.

Cependant, la géométrie analytique ainsi créée comportait une quantité notable d'équations algébriques, et les mathématiciens sentirent bientôt la nécessité d'élargir les conceptions géométriques traditionnelles pour interpréter les solutions complexes des équations.

Pendant longtemps, cette modification apportée aux notions géométriques n'a été conçue que comme une généralisation inéluctable de la géométrie des Grecs, maintenue enracinée dans ses origines topographiques. C'est probablement la raison pour laquelle on a si souvent mal compris les efforts d'un von Staudt pour introduire les éléments imaginaires en géométrie, indépendamment de la notion de coordonnées: il ne lui aurait pas suffi de constater par un changement de repère le caractère invariant des notions nouvellement introduites. C'est ce que fit plus tard Gaston Darboux, mais von Staudt aurait plutôt souhaité modifier le système des axiomes d'Euclide de façon que la géométrie ainsi constituée soit équivalente à la géométrie analytique complexe.

Cette évolution se poursuivant, la situation est, à notre époque, complètement retournée, et l'on définit abstraitement un espace dont les éléments ont leurs coordonnées extraites d'un ensemble de nombres, par exemple un corps: les propriétés des figures sont alors celles des équations qui les définissent. Une géométrie est, comme l'a montré Félix Klein dans le programme d'Erlangen, l'étude des invariants des figures dans un groupe d'automorphismes de l'espace.

Le présent exposé est une introduction à ces géométries récentes, qui, pour rester bref et suggestif, ne supposera que peu de connaissances d'algèbre dite moderne, et qui, au lieu de dégager celles des propriétés de la géométrie classique qui sont valables quel que soit le corps de base, mettra plutôt en évidence des propriétés étranges, spécifiques de la caractéristique.

C'est ainsi que, commençant par quelques propriétés élémentaires nous n'utiliserons dans le premier paragraphe que la définition de la caractéristique p du corps de base K: si l'on forme la progression arithmétique de premier terme zéro, et de raison $x \neq 0$, définie par

$$u_{n+1} = u_n + x$$

$$u_0 = 0$$

cette progression est périodique

$$u_{n+p} = u_n$$

et ne comporte, comme termes distincts que les termes u_0, u_1, ... u_{p-1}, car

$$u_p = u_0 = 0$$

et le nombre premier p qui a cette propriété est le même pour tous les éléments x non nuls de K.

Nous verrons, par exemple, que lorsque le corps K est de caractéristique $p = 2$, les diagonales d'un quadrilatère complet ne sont jamais linéairement indépendantes. Quel est le professeur de notre enseignement secondaire qui, après avoir dessiné un quadrilatère complet au tableau, a vraiment ressenti le besoin, avant de parler du triangle diagonal, de s'assurer de l'existence de ce triangle?

I. Quelques exemples élémentaires

a) Un plan affine peut être défini sur un corps K de caractéristique $p = 2$ comme l'ensemble des points qui ont deux coordonnées x, y dans K, avec, comme groupe d'automorphismes

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} ax + by + c \\ a'x + b'y + c' \end{pmatrix}$$

dont le sous-groupe

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x + c \\ y + c' \end{pmatrix}$$

est le groupe des translations.

Considérons trois points ABC non alignés: nous pouvons définir un repère en attribuant à ces points les coordonnées $A\,(0, 0)$ $B\,(1, 0)$ $C\,(0, 1)$, c'est-à-dire en prenant AB et AC pour vecteurs de base.

Désignons par X la translation

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x+1 \\ y \end{pmatrix}$$

qui fait passer de A à B. Elle fait passer du point C à un point $D\,(1, 1)$ et nous dirons que le quadrilatère $ABCD$ est un parallélogramme car, à cause de la commutativité de l'addition, la translation

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x \\ y+1 \end{pmatrix}$$

qui fait passer de A à C fait aussi passer de B à D.
Mais du fait que

$$1 + 1 = 0$$

dans le corps K, la translation X transforme aussi B en A et D en C: elle conserve le parallélogramme, et en désignant par I la transformation identique, on a

$$X^2 = I$$

La translation Y conserve elle aussi le parallélogramme en transformant C en A et D en B:

$$Y^2 = I$$

Dans ces conditions la translation

$$Z = XY = YX$$

produit des précédentes:

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x+1 \\ y+1 \end{pmatrix}$$

conserve elle aussi le parallélogramme,

$$Z^2 = I$$

en faisant passer simultanément de A en D et de B en C. On a donc aussi

$$XZ = ZX = Y$$

$$YZ = ZY = X$$

Les segments joignant deux points *quelconques* du parallélogramme définissent les translations d'un groupe G_4 qui conserve le parallélogramme.

On pourrait énoncer ce résultat sous une forme amusante en disant: en géométrie sur un corps de caractéristique $p = 2$ les diagonales d'un parallélogramme sont équipollentes et son centre est à l'infini (l'impossibilité de diviser par 2 entraîne d'ailleurs que le milieu d'un segment n'existe pas).

b) On peut définir un plan projectif sur un corps K comme l'ensemble des points qui ont trois coordonnées homogènes x, y, z dans K (non toutes nulles), avec comme groupe d'automorphismes le groupe linéaire.

Lorsque le corps K est de caractéristique $p = 2$, nous avons une géométrie projective dans laquelle il n'y a pas de division harmonique: la valeur $-1 = +1$ du birapport exprime en effet que les points ne sont pas distincts. Cette remarque incite à examiner les propriétés du quadrilatère complet.

Le repère projectif peut toujours être choisi de telle sorte que les côtés du quadrilatère soient

$$x = 0, \quad y = 0, \quad z = 0, \quad x + y + z = 0$$

Dans ces conditions les trois couples des sommets opposés sont

$$\begin{array}{l} (1, 0, 0) \text{ et } (0, 1, 1) \text{ sur la diagonale } y = z \\ (0, 1, 0) \text{ et } (1, 0, 1) \text{ sur la diagonale } z = x \\ (0, 0, 1) \text{ et } (1, 1, 0) \text{ sur la diagonale } x = y \end{array}$$

et les trois diagonales sont concourantes au point unitaire (1, 1, 1).

En géométrie sur un corps de caractéristique deux, tout quadrilatère complet a ses diagonales concourantes.

Bien entendu, ce résultat est l'extension à la géométrie projective de celui obtenu en géométrie affine relativement au parallélogramme dont les diagonales sont parallèles. Cependant nous voyons apparaître ici une symétrie très remarquable: la figure comporte sept droites (quatre côtés et trois diagonales) et sept points (six sommets et le point de concours des diagonales) et chaque point appartient à trois des droites, pendant que chaque droite contient trois points de la figure. Cette symétrie de rôle de tous les éléments tient à ce qu'il s'agit de l'ensemble des points et des droites d'un plan projectif construits sur GF (2).

Lorsqu'un plan projectif est construit sur un corps[1]) *commutatif, s'il contient un quadrilatère complet dont les diagonales sont concourantes, il en*

1) Mais il existe des plans projectifs, non plongeables dans des espaces projectifs plus amples; ils ne peuvent pas être définis par des coordonnées prises dans un corps commutatif. Dans de tels plans, la réciproque que nous énonçons ici n'est pas vraie. cf. Pickert. Projective Ebene.

est de même pour tous les quadrilatères complets, et le corps de base est de caractéristique 2.

Il suffit, en effet, de choisir un repère associé au quadrilatère complet remarquable, de la même manière que ci-dessus: les trois diagonales ont alors pour équations

$$y + z = 0, \quad z + x = 0, \quad x + y = 0$$

système qui entraîne

$$x + x = 0, \quad y + y = 0, \quad z + z = 0$$

de sorte que l'existence du point de concours des diagonales équivaut à l'existence d'un élément non nul du corps de base qui vérifie

$$x + x = 0$$

et la caractéristique est bien $p = 2$.

En revenant à la géométrie affine du triangle de référence nous observons que sur un corps de caractéristique 2, les classiques théorèmes de Menelaus et de Jean de Ceva se confondent en un seul projectif: *la condition nécessaire et suffisante pour que trois droites issues des sommets d'un triangle soient concourantes, est que leurs pieds sur les côtés opposés soient alignés.*

Si l'on songe aux coniques inscrites dans un triangle qui, en géométrie projective classique ont leurs contacts caractérisés précisément par la propriété de concours précédent, on peut être étonné de ne rencontrer en caractéristique 2 que la seule famille des droites doubles, et de devoir conclure qu'*en géométrie sur un corps de caractéristique 2 il n'y a pas de coniques proprement dites inscrites à un triangle.*

c) Cette propriété paradoxale est liée aux vicissitudes de la théorie des formes quadratiques, qui sur un corps de caractéristique 2 ne vérifient pas le théorème de Gauss, de décomposition en carrés. Il est clair en effet que l'identité:

$$x^2 + y^2 = (x+y)^2$$

permet, quitte à introduire, quand cela est nécessaire, les racines carrées des coefficients, de réduire à un seul carré toute combinaison linéaire de carrés. Considérons donc dans le plan une conique

$$Ax^2 + A'y^2 + A''z^2 + Byz + B'zx + B''xy = 0$$

lorsque B, B', B'' sont tous nuls, le premier membre étant le carré d'une forme linéaire, la conique se réduit à une droite double. Lorsqu'il n'en est pas ainsi, nous introduirons comme en géométrie classique, l'application l néaire

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \rightarrow \begin{pmatrix} f'_x \\ f'_y \\ f'_z \end{pmatrix} = \begin{pmatrix} B''y + B'z \\ B''x + Bz \\ B'x + By \end{pmatrix} = \begin{pmatrix} 0 & B'' & B' \\ B'' & 0 & B \\ B' & B & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

qui est intrinsèquement liée à la conique en vertu de l'invariance de la différentielle. La matrice symétrique, est de ce fait antisymétrique, donc irrégulière, et l'application admet un noyau non réduit à zéro. Ainsi s'introduit e point

$$N = \begin{pmatrix} B \\ B' \\ B'' \end{pmatrix}$$

projectivement lié à la conique, et que nous appellerons son « nucléon ».

En choisissant le repère de façon que le nucléon soit le point (0, 0, 1), nous obtenons une première équation réduite:

$$Ax^2 + A'y^2 + A''z^2 + B''xy = 0$$

Si le nucléon appartient à la conique, c'est-à-dire si $A'' = 0$, l'équation homogène en x, y représente deux droites (distinctes) issues de N.

Si le nucléon n'appartient pas à la conique, on peut choisir la droite double

$$Ax^2 + A'y^2 + A''z^2 = 0$$

comme côté opposé à N dans le repère et le choix du point unitaire, arbitrairement, sur la conique donne l'équation réduite définitive

$$xy = z^2$$

On vérifie immédiatement sur cette équation que l'intersection de la conique avec la droite

$$ux + vy + wz = 0$$

est formée de deux points distincts si $w \neq 0$ et de deux points confondus si $w = 0$.

Une conique non décomposée a ses tangentes concourantes, au nucléon de la conique.

C'est pour cette raison qu'on ne trouve aucun triangle proprement dit, circonscrit à une conique.

Dans ces conditions, il est peut-être utile d'indiquer brièvement comment se présente la discussion des différents types de faisceaux linéaires de coniques. Dans le cas général, un faisceau de coniques ne contient aucune droite double. Il y a quatre points bases, qui, joints deux à deux, définissent six droites constituant les coniques décomposées du faisceau. Les nucléons des coniques décrivent la septième droite du plan projectif défini ainsi sur le corps des restes modulo 2.

Lorsque le nombre des points de base est réduit à trois ou à deux, l'un de ces points étant un contact bi ou tri-ponctuel, il n'y a pas de droite double dans le faisceau et les nucléons décrivent la tangente fixe.

Lorsque dans un faisceau il y a une droite double, les coniques du faisceau ont un nucléon fixe: si ce nucléon n'appartient pas à la droite double, il s'agit d'un faisceau de coniques bitangentes. Si le nucléon fixe appartient à la droite double, c'est l'unique point base, et les coniques ont en ce point un contact quadriponctuel.

Enfin, lorsque deux coniques d'un faisceau sont des droites doubles, le premier membre de l'équation est une combinaison linéaire de carrés, donc un carré, et toutes les coniques du faisceau sont les droites issues du point base, comptées doubles: *en géométrie sur un corps de caractéristique deux, il n'y a pas de faisceau involutif, mais des faisceaux de droites doubles.*

d) Nous allons maintenant nous intéresser à la division harmonique dans la géométrie sur un corps de caractéristique $p = 3$. La relation entre les coordonnées de quatre points alignés en division harmonique:

$$\frac{x_3 - x_1}{x_3 - x_2} : \frac{x_4 - x_1}{x_4 - x_2} = -1$$

se transforme par un calcul facile en

$$x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 = 0$$

qui montre qu'*en géométrie sur un corps de caractéristique trois les quatre points d'une division harmonique ne sont pas distingués en deux paires, mais jouent le même rôle.* C'est pourquoi nous l'appellerons une *division symétrique.* Deux points choisis arbitrairement dans la division sont conjugués par rapport aux deux points restants.

On peut éviter le calcul précédent en plaçant trois des points en ∞, 0, 1, en utilisant la triple transitivité du groupe projectif. Le conjugué de chaque point, par rapport aux deux autres est, successivement

$$\frac{1}{2}, \quad 2, \quad -1$$

et sur le corps des restes modulo 3, ces trois nombres sont égaux. Sous cette forme réduite, on peut dire: *en géométrie affine sur le corps des restes modulo 3 chacun des trois points d'une droite est le milieu des deux autres.*

Il résulte de cette symétrie que si, en géométrie projective plane sur un corps de caractéristique trois, nous associons à un quadrangle $ABCD$, de points diagonaux I, J, K, la conique sur laquelle les points A, B, C, D forment une division symétrique, nous obtenons une figure dans laquelle les propriétés classiques du quadrangle harmonique se retrouvent, symétrisées. Les tangentes a, b, c, d en A, B, C, D sont intrinsèquement déterminées par le birapport -1, sans qu'il soit nécessaire d'ordonner les points: a, AB, AC, AD forment un faisceau symétrique. Les trois diagonales du quadrilatère $abcd$ sont, comme en géométrie classique, les côtés du triangle IJK: par I passent deux côtés du quadrangle $ABCD$ et deux diagonales du quadrilatère $abcd$, et ces quatre droites forment un faisceau symétrique.

En outre, l'intersection des côtés a, b du quadrilatère appartient à CD conjuguée de AB de même que l'intersection des côtés c, d appartient à AB conjuguée de CD, ces points étant, sur JK, conjugués par rapport à J et K. Cette propriété, symétrique, est valable pour tous les sommets du quadrilatère. *Le quadrilatère abcd est non seulement circonscrit au quadrangle ABCD* (chaque côté contenant le sommet de même nom) *mais il lui est en même temps inscrit*, en ce sens que les six sommets du quadrilatère appartiennent respectivement aux six côtés du quadrangle.

On peut donner de cette propriété une forme réduite affine, en plaçant JK à l'infini, et en disant: en géométrie affine sur un corps de caractéristique trois, la figure obtenue en joignant les milieux des côtés d'un parallélogramme est un parallélogramme et chacun est à la fois inscrit et circonscrit à l'autre.

La configuration projective ainsi associée à quatre points d'un plan comporte 13 points et 13 droites; elle est telle que toute droite contient quatre points en division symétrique et que par tout point passent quatre droites formant un faisceau symétrique: c'est un plan projectif construit sur le corps des restes modulo 3.

Cette propriété pourrait, comme précédemment, servir à caractériser la géométrie projective dont nous nous occupons.

e) Sans vouloir multiplier les exemples élémentaires nous remarquerons encore cette propriété de la droite projective sur le corps des restes modulo cinq: *les six points d'une telle droite projective forment trois couples deux à deux en division harmonique.*

En effet, en choisissant trois points quelconques de l'ensemble comme repère $(\infty, 0, 1)$ les autres ont pour coordonnées $2, -1, -2$: les deux couples $(\infty, 0)$ $(1, -1)$ et les deux couples $(\infty, 0)$ $(2, -2)$ sont évidemment harmoniques. Et le conjugué de 2 par rapport $(-1, 1)$ est

$$\frac{1}{2} = -2$$

nous ne nous appesantirons pas sur les propriétés de commutation liées à cette figure.

II. Propriétés hermitiennes

Nous avons rencontré dans l'étude des formes quadratiques en caractéristique deux, l'identité

$$x^2 + y^2 = (x+y)^2$$

cette propriété s'étend à toute caractéristique finie, sous la forme

$$x^p + y^p = (x+y)^p$$

plus généralement

$$x^q + y^q = (x+y)^q$$

où $q = p^k$ est une puissance de p: liée au « petit » théorème de Fermat, elle tient à la divisibilité par p des coefficients binômiaux. Elle montre que dans un corps de caractéristique p, l'opération

$$x \to x^p$$

est un automorphisme, qui engendre un groupe.

De même que l'automorphisme du corps complexe

$$z = x + iy \to \bar{z} = x - iy$$

avait permis à Hermite de définir les formes, puis la géométrie qui porte son nom, de même, il est possible de définir, en caractéristique p, *les formes sesquilinéaires.*

Considérons un espace vectoriel, sur un corps de caractéristique p, et une forme $f(x, y)$ qui à un couple de vecteurs X, Y associe un nombre du corps de base, avec les propriétés suivantes:

a) la forme est linéaire par rapport à X:

$$f(\lambda X, Y) = \lambda f(X, Y)$$

$$f(X' + X'', Y) = f(X', Y) + f(X'', Y)$$

b) la forme est semilinéaire par rapport à Y:

$$f(X, \lambda Y) = \lambda^q f(X, Y)$$

$$f(X, Y' + Y'') = f(X, Y') + f(X, Y'')$$

Il est clair que lorsqu'on passe de l'espace vectoriel à l'espace projectif par la traditionnelle relation d'homogénéité, une telle forme, dite sesquilinéaire, possède, pour le couple de points correspondants, les propriétés d'une fonction caractéristique. En désignant toujours par X, Y les points correspondant aux deux vecteurs de mêmes noms, la relation

$$f(X, Y) = 0$$

est une propriété géométrique de l'espace projectif, que nous appellerons une *sesquipolarité.*

Pour en montrer brièvement les propriétés, je supposerai que l'espace vectoriel étant à trois dimensions, nous traitons de géométrie projective plane.

Lorsque le point $Y = A$ est donné, le lieu des points X qui lui correspondent

$$f(X, A) = 0$$

est une droite que nous appellerons la polaire de A. En faisant décrire à Y une droite

$$Y = A + tB$$

la polaire

$$f(X, A) + t^q f(X, B) = 0$$

décrit un faisceau linéaire de droites. Le birapport r de quatre points alignés est celui des t, le birapport des polaires est celui des t^q. Comme l'expression du birapport est rationnelle, et que l'élévation à la puissance q est un homomorphisme, le birapport des quatre polaires est r^q.

De même lorsque le point $X = A$ est donné, le lieu des points Y qui lui correspondent a pour équation

$$f(A, Y) = 0.$$

Sous réserve d'étendre éventuellement le corps de base (comme on le fait en géométrie réelle lorsqu'on introduit des éléments imaginaires conjugués), le premier membre est la puissance q-ème d'une forme linéaire: le lieu est une droite (multiple) que nous appellerons la semi-polaire de A. En faisant décrire à X une droite

$$X = A + tB$$

la semi-polaire

$$f(A, Y) + tf(B, Y) = 0$$

décrit un faisceau linéaire de droites, et en utilisant comme plus haut l'homomorphisme fondamental, on voit que le birapport de quatre semi-polaires est la racine q-ème du birapport r des quatre points correspondants.

Pour alléger cet exposé, nous nous limiterons au cas où la correspondance entre un point et sa polaire, est biunivoque. Nous voyons ainsi comment la notion de sesquipolarité généralise la notion classique de transformation par polaires réciproques, associée aux formes bilinéaires. Cette théorie classique est immédiatement liée à celle des formes quadratiques, et il s'introduit ici toute une série de courbes (et de variétés dans les espaces projectifs de dimension quelconque), lieu des points qui appartiennent à leur polaire, et par conséquent aussi à leur semi-polaire:

$$f(X, X) = 0$$

Ce sont ces courbes et variétés que, en accord avec M. Beniamino Segre, nous nommerons *variétés hermitiennes* [1]).

Le dédoublement de la polarité pose cependant la question de la recherche des couples point-droite pour lesquels il y a réciprocité, c'est-à-dire des points pour lesquels la polaire est en même temps la semi-polaire. Dans le cas régulier, auquel nous nous sommes limités, on obtient une configuration très simple: *les éléments pour lesquels il y a réciprocité sont les points et les droites d'un plan projectif sous-jacent au plan donné dans lequel les coordonnées sont prises dans le corps à q^2 éléments.*

Ce résultat est important car, de même qu'en géométrie classique des formes quadratiques, la recherche d'un repère conjugué est équivalente à la décomposition en carrés de Gauss, de même, ici, l'obtention d'un repère

[1]) Cf. L. Gauthier: *Géométrie hermitienne généralisée.* Bulletin Académie Royale de Belgique 1966, p. 421. Dans ce mémoire, ces variétés étaient désignées, pour une autre raison, sous le nom de variétés de Fermat. Cf. B. Segre: *Hermitian geometries, with special regard to the finite case.* Actas Coloquio Internacional Geometria Algebraica Madrid 1965.

conjugué (avec réciprocité) permet de définir une *forme réduite, de Fermat :*

$$x^{q+1} + y^{q+1} + z^{q+1} = 0$$

Pour donner un exemple simple d'étude de courbe hermitienne, prenons le cas $q = p = 3$. La quartique Q

$$x^4 + y^4 + z^4 = 0$$

est coupée par toutes les droites du plan en des points formant des divisions symétriques, comme on le voit après avoir remarqué que

$$(x_0 + \lambda x_1)^4 = x^4{}_0 + \lambda x_0^3 x_1 + \lambda^3 x_0 x_1^3 + \lambda^4 x_1^4$$

ne contient pas de terme en λ^2. Pour cette raison, nous dirons que la quartique Q est *totalement symétrique.*

En particulier, si le point (x_0, y_0, z_0) appartient à Q, la tangente en ce point, définie, suivant l'habitude classique des géomètres algébristes, comme la droite exceptionnelle, pour laquelle $\lambda = 0$ est racine multiple de l'équation d'intersection, a pour équation:

$$x_0^3 X + y_0^3 Y + z_0^3 Z = 0$$

le premier membre est précisément la forme sesquilinéaire associée à l'équation de Q, et la *tangente est la polaire du point de contact.*

Cette remarque associée aux propriétés d'alignement montre que *quatre points alignés sur Q ont des tangentes concourantes suivant un faisceau symétrique.* Ces quatre tangentes recoupent d'ailleurs Q en quatre points alignés.

D'autre part, la racine $\lambda = 0$ est dans ce cas une racine au moins triple, le contact de la tangente avec la courbe est au moins triponctuel, et *la courbe Q est totalement inflexionnelle* c'est-à-dire que tous ses points sont d'inflexion.

Les points pour lesquels il y a réciprocité polaire sont ceux dont les coordonnées sont des entiers de Gauss: $a + bi$ (où a, b sont des restes modulo 3 et $i^2 = -1$). Il y a 91 tels points dont 28 sont sur la courbe Q, la tangente ayant alors un contact quadriponctuel, et il y en a 63 qui n'appartiennent pas à Q. Une étude approfondie de cette question et des fonctions modulaires en caractéristique trois [1]) rapproche ces deux nombres de la détermination des 28 bitangentes et des 63 familles de coniques quadritangentes, donnée par F. Klein dans son étude de la quartique canonique en géométrie complexe.

---

[1]) Cf. Luc Gauthier: *L'invariant modulaire dans la géométrie sur un corps de caractéristique trois.* Journal de mathématiques pures et appliquées 1957, p. 117.

La détermination de la tangente courante à la quartique totalement symétrique Q, associée à l'homomorphisme d'élévation au cube, montre que l'équation tangentielle de Q est

$$u^4 + v^4 + w^4 = 0$$

cette courbe est donc *autoduale.*

D'un point P quelconque du plan on mène quatre tangentes à Q, formant un faisceau symétrique: leurs contacts sont alignés sur la semipolaire de P. Lorsque P est sur la quartique Q, sa semipolaire passe par P et est tangente à Q en un point P': le faisceau est alors formé de PP' triple et de la tangente en P simple.

Comme la quartique Q ne comporte aucune singularité ponctuelle, elle est de genre 3. En géométrie projective complexe les quartiques de genre 3 sont de classe 12. Nous rencontrons ici, pour la seconde fois, le fait qu'en géométrie sur un corps de caractéristique p les propriétés tangentielles sont profondément différentes de celles de la géométrie complexe classique. Dans la théorie des coniques, pour $p = 2$ nous avons trouvé que l'enveloppe des tangentes n'est pas du tout la conique elle-même, mais le nucléon de la conique, qui est de classe 1. Dans la présente étude, en caractéristique $p = 3$, la quartique Q est bien l'enveloppe de ses tangentes, mais le point caractéristique d'une tangente:

$$X = u^3 \qquad Y = v^3 \qquad Z = w^3$$

n'est pas le point de contact, puisque

$$u = x_0^3 \qquad v = y_0^3 \qquad w = z_0^3$$

C'est le point déduit du point de contact par l'homomorphisme $x \to x^9$: c'est le tangentiel du point de contact.

Nous verrons plus loin comment peut être élaborée non seulement la géométrie tangentielle, mais toute la géométrie infinitésimale.

III. Quelques questions de géométrie algébrique

Pour rester fidèle au but que je me suis proposé, je me bornerai ici à indiquer quelques théorèmes classiques de la géométrie complexe qui perdent leur validité en géométrie sur un corps de caractéristique p.

Nous avons montré, comme conséquence de l'homomorphisme fondamental, qu'il n'y a pas, en géométrie sur un corps de caractéristique deux, de faisceaux involutifs, mais qu'en revanche il existe des faisceaux de droites doubles:

$$y^2 - \lambda x^2 = 0$$

Plus généralement, sur un corps de caractéristique p

$$y^p - \lambda x^p = 0$$

représente un faisceau linéaire de droites p-uples.

Le théorème classique de Bertini assurant que la courbe générale d'un système linéaire privé de composante fixe ne peut avoir de point multiple variable est donc essentiellement lié à l'absence d'extensions inséparables et appartient au seul domaine de la géométrie sur un corps de caractéristique zéro (ou infinie, suivant les notations du lecteur).

La quartique totalement symétrique que nous avons présentée en géométrie sur un corps de caractéristique 3 fournit, elle aussi, en tant que courbe totalement inflexionnelle, un contre-exemple au *théorème complémentaire de Weierstrass*: Le théorème des lacunes, dont on peut donner une démonstration valable en toute caractéristique, affirme que toute place d'une courbe de genre g peut être l'unique pôle d'une fraction rationnelle définie sur la courbe, l'ordre de multiplicité de ce pôle prenant toute valeur entière, à part g lacunes inférieures à $2g$. Le théorème complémentaire affirme que sauf en un nombre fini de places exceptionnelles, les lacunes sont 1, 2, ..., g.

Pour une courbe de genre $g = 3$, le modèle canonique est une quartique plane; en un point ordinaire les lacunes sont 1, 2, 3: les points exceptionnels de Weierstrass sont les points d'inflexion. La quartique totalement symétrique Q admet tous ses points comme points d'inflexion, donc comme points exceptionnels de Weierstrass. Il est d'ailleurs facile de vérifier que les lacunes sont 1, 2, 4 sauf lorsqu'on choisit l'un des 28 points de la configuration de réciprocité, pour lesquels les lacunes sont 1, 2, 5.

Considérons maintenant, dans un espace projectif à trois dimensions, sur un corps de caractéristique trois, la surface

$$xy^3 + yz^3 + zt^3 + tx^3 = 0$$

c'est une variété hermitienne, dont nous allons obtenir une représentation paramétrique rationnelle en posant:

$$z = u^3 x$$

$$y + ut = vx$$

On obtient, effectivement

$$x = u^{10} - 1$$

$$y = -v(uv^2 + 1)$$

$$z = u^3(u^{10} - 1)$$

$$t = v(v^2 + u^9)$$

Comme u est défini par son cube, il a, pour un point donné, une valeur unique: cette représentation rationnelle biunivoque ne peut cependant pas être modifiée en une représentation birationnelle, car une surface du quatrième ordre sans singularité a tous ses genres égaux à 1. Nous obtenons ainsi un contre-exemple au *théorème classique de Castelnuovo* relatif aux surfaces rationnelles.

Les variétés hermitiennes fournissent des exemples en toute dimension (exception faite des courbes) de variétés admettant des représentations rationnelles biunivoques, mais non birationnelles, avec des genres non bornés.

IV. La géométrie infinitésimale

Nous avons rencontré, en géométrie sur un corps de caractéristique trois, une quartique dont tous les points sont inflexionnels. C'est un exemple de courbe dont tous les points sont singuliers du point de vue tangentiel. Le fait, que nous avons rencontré également, que l'enveloppe des tangentes à une courbe n'est pas la courbe elle-même, montre, lui aussi, la nécessité de préciser les fondements de la géométrie infinitésimale.

a) Il faut d'abord donner une signification claire aux notions de voisinages d'un point sur une courbe (plus généralement sur une variété). C'est une question de nature topologique, et tant que l'on considère les points d'une courbe à coordonnées prises dans un corps fini, ils forment un ensemble discret qui n'est naturellement muni que de la topologie discrète. Mais, dès que l'on effectue des extensions infinies du corps de base, c'est-à-dire dès que l'on associe à une courbe la connaissance de son équation, on peut associer à chaque point des représentations paramétriques locales, et définir des voisinages de tous ordres.

Soit a une coordonnée quelconque d'un point. On la remplace par la série formelle

$$x = a + a_1 t + \dots + a_n t^n + \dots$$

qui admet pour spécialisation a, lorsque $t = 0$. Les coefficients successifs de la série seront déterminés par un processus récurrent, qui est justifié par une topologie très simple dont on munit l'anneau des séries formelles. On sait que l'on appelle ordre ω d'une série formelle le numéro du premier coefficient non nul. Cet entier associé à la série possède, vis-à-vis des opérations sur les séries, des propriétés valuatives très simples, de sorte que l'on définit un système dénombrable de voisinages de zéro, en appelant n-ème voisinage de zéro l'ensemble V_n des séries formelles d'ordres

$$\omega \geqslant n + 1$$

Ces voisinages sont emboîtés, et transportés par translation dans tout l'espace vectoriel des séries formelles. Dans la topologie ainsi définie, la limite de t^n pour n augmentant indéfiniment est zéro, et on dispose ainsi d'une technique tout à fait analogue à celle classique des développements limités, pour écrire que le premier membre d'une équation appartient à un voisinage de zéro donné a priori.

b) Voici, à titre d'exemple l'étude du contact, en géométrie sur un corps de caractéristique deux, de la cubique

$$y^2 z = x^3$$

avec une conique. La cubique admet le point R (0, 0, 1) comme point singulier et le point I (0, 1, 0) comme point d'inflexion. La conique sera définie paramétriquement:

$$x = x_0 + x_1 t + x_2 t^2$$

$$y = y_0 + y_1 t + y_2 t^2$$

$$z = z_0 + z_1 t + z_2 t^2$$

le point $(x_0\, y_0\, z_0)$ étant un point courant de la cubique. Les coefficients des puissances successives de t dans l'équation d'intersection sont

$$y_0^2 z_0 + x_0^3$$

$$y_0^2 z_1 + x_0^2 x_1$$

$$y_0^2 z_2 + y_1^2 z_0 + x_0^2 x_2 + x_1^2 x_0$$

$$y_1^2 z_1 + x_1^3$$

$$y_2^2 z_0 + y_1^2 z_2 + x_2^2 x_0 + x_1^2 x_2$$

$$y_2^2 z_1 + x_2^2 x_1$$

$$y_2^2 z_2 + x_2^3$$

L'équation

$$y_0^2 z + x_0^2 x = 0$$

est l'équation de la tangente à la cubique au point courant: cette tangente passe par le point fixe I où elle recoupe la cubique. On voit ainsi que les coniques qui ont, au point considéré, un contact quadriponctuel avec la cubique, ont pour nucléon I:

$$x_1 = z_1 = 0$$

La conique osculatrice a pour équation

$$x^2 x_0 z_0 + y^2 z_0^2 + z^2 y_0^2 + xz x_0^2 = 0$$

elle admet avec la cubique un contact 6-ponctuel.

En géométrie sur un corps de caractéristique deux, la cubique à point de rebroussement admet tous ses points simples comme points sextactiques.

c) J'ai défini [1]) un procédé de transformation des équations, que j'ai appelé le « perfectionnement », et qui a l'avantage de présenter l'étude d'une variété algébrique sous une forme tout à fait analogue à l'étude d'une fonction polynôme. Voici, en nous limitant à la géométrie affine plane, en quoi il consiste:

Considérons un polynôme à deux variables $f(x, y)$, à coefficients dans un corps K parfait, de caractéristique p. Lorsqu'il est exprimé au moyen de ses monômes

$$f(x, y) = \sum M_{kh} = \sum a_{kh} x^k y^h$$

l'homomorphisme fondamental fournit sa puissance p-ème

$$F = f^p = (\sum M)^p = \sum M^p = \sum a_{kh}^p x^{pk} y^{ph}$$

sous forme d'un polynôme par rapport à

$$\xi = x^p \qquad \eta = y^p$$

à coefficients dans K. La réciproque est évidente puisque dans K parfait les coefficients ont une racine p-ème. Cette propriété s'étend sans difficulté aux fractions rationnelles.

Revenons alors au polynôme

$$f(x, y) = \sum a_{kh} x^k y^h$$

---

[1]) Luc Gauthier: *Géométrie infinitésimale des courbes algébriques planes ou gauches sur un corps de caractéristique p*, Séminaire P. Dubreil et Ch. Pisot, décembre 1955, exposé 7 (Faculté des Sciences de Paris).

et modifions les exposants modulo p, par exemple en choisissant comme système de représentants les entiers $0, 1, ..., p - 1$:

$$k = pq + \alpha$$

$$h = pq' + \beta$$

ceci nous permet de mettre f sous la forme

$$f(x, y) = \sum_{\alpha,\beta} (\sum_{q,q'} a_{kh} \xi^q \eta^{q'}) x^\alpha y^\beta = \sum A_{\alpha,\beta} x^\alpha y^\beta$$

c'est-à-dire sous la forme d'un polynôme à exposants pris dans les restes modulo p, les coefficients étant des polynômes en ξ et η.

Cette propriété s'étend immédiatement aux fractions rationnelles

$$r = \frac{f}{g} = \frac{f g^{p-1}}{g^p} = \sum B_{\alpha,\beta} x^\alpha y^\beta$$

qui peuvent être écrites sous forme de polynômes à exposants pris dans les restes modulo p, les coefficients étant rationnels en ξ et η.

Lorsque le choix des représentants pris comme exposants est précisé, la représentation est unique et il en résulte qu'*une condition nécessaire et suffisante pour qu'une expression ait sa différentielle identiquement nulle est qu'elle appartienne au sous-corps des puissances p-èmes.*

Pour cette raison, nous désignerons désormais les puissances p-èmes sous le nom de quasi-constantes.

Considérons alors, maintenant, une quantité z, algébrique sur le corps K, et son polynôme minimal $f(z)$. Lorsqu'on écrit

$$f^{p-1} = A_1 z^{p-1} + ... + A_p$$

où les A_i sont des polynômes en $\zeta = z^p$, le premier coefficient non nul A_k ne peut être le dernier car

$$ff' = 0$$

est contradictoire avec le fait que f est minimal. En dérivant $p-2$ fois

$$z^{k-1} f^{p-1}$$

on obtient

$$fg = - A_k z + A_{k+1}$$

où g est un polynôme de l'idéal engendré par f et f'.

L'équation

$$f(z) = 0$$

entraîne que *z est rationnel en* ζ.

Cette propriété de clôture est importante car elle montre que toute courbe

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

peut, en un point ou F'_y n'est pas nul, être mise sous forme résolue

$$y = P(x;\xi,\eta)$$

dans laquelle le second membre est un polynôme de degré p-1 au plus en x, à coefficients quasi-constants.

Cette propriété s'étend d'ailleurs aux variétés de toutes dimensions, et aux homomorphismes

$$x \to \xi = x^q$$

($q=p^k$) engendrés par l'homomorphisme fondamental.

d) Voici un exemple simple d'application de la méthode de transformation précédente:

Sur un corps de caractéristique trois l'équation affine d'une courbe peut être mise sous la forme

$$y = Ax^2 + Bx + C$$

où A, B, C sont des quasi constantes: Si A est identiquement nulle, la courbe a tous ses points simples comme points d'inflexion. Si A n'est pas identiquement nulle, on obtient les points d'inflexion en coupant la courbe proposée par

$$A = 0$$

et comme A est un cube, les points obtenus ont chacun une multiplicité d'intersection multiple de 3 [1]).

C'est ainsi que la cubique

$$y^2 = x^3$$

---

[1]) Dans l'étude des cubiques, A est le cube d'une forme linéaire. La classification projective se présente ainsi: Si A est identiquement nulle, la cubique est totalement inflexionnelle (cf. exemple qui suit).

Si $A = 0$ est une droite sécante ou tangente à la cubique, contenant éventuellement un point double, il y a trois, un ou zéro point d'inflexion (cf. exemple du § e).

Le cas où il y a un seul point d'inflexion, de multiplicité 9, correspond à l'annulation de l'invariant de Hasse.

peut, sauf à l'origine qui est un point singulier, être écrite

$$\xi y = \eta$$

y est une quasi constante: les tangentes à la courbe sont les droites

$$y = y_0$$

et l'intersection

$$(x - x_0)^3 = 0$$

montre bien que tous les points simples sont inflexionnels.

En géométrie projective, la quartique qui a trois rebroussements, a pour équation

$$x^2y^2 + y^2z^2 + z^2x^2 = 0$$

en faisant $z = 1$ et en multipliant par xy, on obtient l'équation « perfectionnée »:

$$\eta x + \xi y + \xi\eta = 0$$

qui montre que (pour $p = 3$ encore), cette courbe est, elle aussi, totalement inflexionnelle.

e) En géométrie sur un corps de caractéristique trois, les cubiques à point de rebroussement ne forment pas une seule famille projective: nous venons de montrer que la courbe

$$y^2 = x^3$$

est totalement inflexionnelle. Considérons ensuite la cubique

$$y^2 + x^2y + x^3 = 0$$

qui admet un point singulier unique à l'origine

$$(y - x^2)^2 = x^4 - x^3$$

Pour formei l'équation « perfectionnée », élevons les deux membres au carré

$$(y - x^2)^3 (y - x^2) = x^8 + x^7 + x^6$$

c'est-à-dire

$$(\eta - \xi^2)\, y = \eta x^2 + \xi^2 x + \xi^2$$

Les points d'inflexion sont obtenus en annulant le terme du second degré

$$\eta = 0$$

mais nous avons déjà exclu l'origine comme point singulier.

La cubique considérée n'admet aucun point d'inflexion véritable. En revanche elle admet un point de rebroussement d'une nature plus subtile que ceux de la géométrie classique : il ne vérifie pas le théorème de Puiseux.

Mais je ne veux pas, dans ce travail qui vise seulement à présenter quelques aspects de la géométrie sur un corps de caractéristique p, entrer dans l'étude, d'ailleurs délicate, des singularités des courbes et variétés algébriques.

f) Sans donner non plus de développement au sujet d'une étude dont je me suis occupé récemment, je voudrais cependant signaler que la géométrie infinitésimale en caractéristique p, dispose actuellement de moyens suffisants pour qu'on puisse analyser complètement la structure d'une variété en un point, et lui associer *un repère projectif mobile* intrinsèquement défini. Je renverrai seulement, sur ce sujet, à deux publications en cours, l'une à Bologne (Luc Gauthier: *Adaptation d'une méthode de Bompiani à la géométrie infinitésimale sur les corps de Galois,* Colloque de géométrie différentielle, fin septembre 1967), l'autre dans le volume jubilaire dédié à M. Lucien Godeaux (Luc Gauthier: *Géométrie projective infinitésimale sur les corps de Galois).*

V. Essai de géométrie métrique

Lorsqu'on dispose d'une géométrie projective, et par conséquent, en faisant choix d'un hyperplan à l'infini, d'une géométrie affine, il vient naturellement à l'idée d'introduire une forme quadratique définie positive, à laquelle on associera une distance, pour fabriquer une géométrie métrique.

Malheureusement, dans les corps finis l'absence de relation d'ordre permettant de définir le qualificatif « positif » détruit cet espoir.

Cependant, dans l'intention de donner des applications en astronomie, à l'étude des amas d'étoiles, P. Kustaanheimo [1]) et G. Järnefelt [2]), ont montré que pour des valeurs particulières, (mais non bornées) de la caractéristique p, il est possible d'extraire de l'espace affine construit sur le corps

---

[1]) Kustaanheimo: *One the fundamental prime of a finite world.* Annales Academiae scientiarum fennicae, 1952.

[2]) Järnefelt: *Reflections on a finite approximation to euclidean geometry...* Ibidem 1951.

des restes modulo p un domaine (dont le nombre des points pourra, avec p, croître indéfiniment) que l'on peut munir d'une structure métrique euclidienne.

Je voudrais indiquer rapidement ici les idées directrices qui ont fait le succès de cette étude si originale.

On commence par donner du qualificatif « positif » une signification compatible avec la seule structure multiplicative du corps des restes modulo p. On sait que, en se bornant au cas de p impair, et au groupe multiplicatif des restes non nuls, la théorie de la racine carrée conduit à considérer deux classes d'entiers:

a) les restes quadratiques, c'est-à-dire ceux a pour lesquels la congruence

$$x^2 = a \ mod. \ p$$

admet des solutions.

b) les non-restes quadratiques, c'est-à-dire ceux b pour lesquels la congruence

$$x^2 = b \ mod \ p$$

n'a pas de solution.

Chaque classe contient le même nombre d'éléments.

Le produit de deux restes est un reste. Le produit d'un reste et d'un non-reste est un non-reste. Le produit de deux non-restes est un reste. L'application qui, à tout élément non nul du corps, fait correspondre le symbole $+$ si c'est un reste, et le symbole $-$ si c'est un non-reste, a donc les qualités multiplicatives de la « règle des signes ».

Il faut ensuite transporter cette qualification, par translation, dans le domaine, de façon à pouvoir dire que l'inégalité

$$x \succ y$$

signifie que $x - y$ est un reste quadratique, modulo p. Comme la somme de deux restes n'est pas toujours un reste, c'est ce point qui introduit les limitations du domaine de validité. Kustaanheimo a montré que si ϖ est le produit des k premiers nombres premiers impairs, en choisissant

$$p = -1 \text{ mod } 8\varpi$$

il existe une « chaîne euclidienne »

$$-M, \ldots, -2, -1, 0, 1, 2, \ldots, +M$$

de $2M + 1$ entiers tels que, modulo p, tous les nombres $1, 2, \ldots M$ soient des restes quadratiques et tous les nombres $-1, -2, \ldots -M$ soient des non-restes. Le pavé affine formé des points dont les coordonnées sont prises dans une telle chaîne euclidienne est alors susceptible d'être muni de la métrique dans laquelle la distance est donnée par la règle de Pythagore.

Je renverrai, pour le développement de cette question, aux auteurs eux-mêmes.

(Achevé à Novosibirsk le 9 février 1968)

L. Gauthier
Professeur à la Faculté
des Sciences de Paris

vide-leer-empty