Séminaire Dubreil.
Algèbre et théorie
des nombres

F. Châtelet

Quelques propriétés arithmétiques des courbes algébriques

Séminaire Dubreil. Algèbre et théorie des nombres, tome 10 (1956-1957), exp. n° 16, p. 1-8

<http://www.numdam.org/item?id=SD_1956-1957__10__A16_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1956/57
-:-:-:-

Exposé n° 16

QUELQUES PROPRIÉTÉS ARITHMÉTIQUES DES COURBES ALGÉBRIQUES

(Exposé de F. CHÂTELET, le 25.3.1957)

Cet exposé est surtout destiné à attirer l'attention sur un travail de Mlle Elisabeth LUTZ. Ce travail a été fait en 1936 sous la direction de M. André WEIL et publié en 1937 dans le Journal de Crelle [1]. Mlle LUTZ n'a pas poursuivi, depuis, l'étude de ce sujet, bien que son intérêt soit loin d'être épuisé.

H. POINCARÉ [2] a montré l'intérêt d'organiser en groupe abélien l'ensemble des points à coordonnées rationnelles (en abrégé points rationnels) sur une courbe de genre un. Cette organisation en groupe abélien est encore possible pour l'ensemble des points à coordonnées dans un corps k (en abrégé points dans k) situés sur une telle courbe. Le sujet proposé par A. WEIL était l'étude de ce groupe lorsque k est un corps local de Hensel (étude arithmétique locale de la courbe). Mlle LUTZ a bien obtenu une étude complète de ce groupe et a ainsi résolu la question posée.

Mais les méthodes employées donnent aussi des résultats précieux pour l'étude du groupe des points rationnels qui est loin d'être complète (étude arithmétique globale de la courbe). Mlle LUTZ s'est contentée de signaler l'un de ces résultats qui avait d'ailleurs été obtenu antérieurement par M. Tryge NAGELL [3] par une méthode différente. J'en ai signalé quelques autres ultérieurement [4] sans épuiser le sujet. Enfin il y aurait intérêt à généraliser la méthode et les résultats à l'étude des points rationnels de la jacobienne d'une courbe de genre supérieur à un, suivant les suggestions de POINCARÉ.

Considérons une extension p-adique R_p du corps des rationnels et le corps des restes R/p de R_p suivant son idéal premier p. La méthode de Mlle LUTZ consiste essentiellement à comparer le groupe des points dans R_p sur une courbe de genre un à l'ensemble des points dans R/p sur la même courbe.

Pour simplifier les énoncés, limitons nous à la forme normale de Weierstrass d'une courbe de genre un ; une méthode classique de POINCARE montre qu'on peut se ramener à cette forme par une transformation simple. Nous supposerons donc que :

1°) la courbe C peut être définie par une équation de la forme :

$$y^2 = x^3 + Ax + B \quad ,$$

avec A et B entiers p-adiques,

2°) On choisit pour élément neutre ou zéro du groupe le point à l'infini sur C (il est commode de noter le groupe sous forme additive).

Si p ne divise pas $2(4A^3 + 27B^2)$, la courbe C est de genre un dans le corps des restes R/p. L'ensemble des points dans ce corps est formé par les solutions (en nombre fini) de la congruence :

$$y^2 \equiv x^3 + Ax + B \qquad (\text{mod. } p)$$

et le point à l'infini. Cet ensemble peut être organisé en groupe additif en utilisant les 2 règles : la somme de 3 points alignés est nulle ; le zéro est le point à l'infini (en particulier la somme de 2 points alignés avec ce point est nulle). Mlle LUTZ a montré que le groupe des points dans R_p sur C est homomorphe au groupe ainsi construit. Les points correspondants au zéro dans cette homomorphie sont ceux dont les coordonnées x et y peuvent être mises sous la forme du quotient d'un entier p-adique par un multiple de p. Nous dirons qu'un tel point est congru à zéro suivant le module p.

Ainsi, si p ne divise pas $2(4A^3 + 27B^2)$, le groupe des points dans le corps des restes R/p sur C est isomorphe au groupe-quotient du groupe des points dans R_p par le groupe des points congrus au zéro.

Si p divise $2(4A^3 + 27B^2)$, la courbe C est unicursale dans le corps des restes R/p ; l'ensemble de ses points ne peut plus être organisé en groupe additif. Néanmoins Mlle LUTZ a encore construit une image du groupe-quotient du groupe des points dans R_p sur C par le groupe des points congrus au zéro (en conservant la même définition de ce groupe que dans le cas où p ne divise pas $2(4A^3 + 27B^2)$). Je ne donnerai pas le détail de cette construction qui est assez délicate. L'essentiel de la méthode consiste à utiliser les solutions des congruences :

$$y^2 \equiv x^3 + A x + B \qquad (\text{mod. } p^n)$$

pour les premières puissances de p ; mais pour chacune de ces congruences, on ne considère que les solutions qui peuvent être considérées comme des points simples sur C suivant le module p^n et comme des points multiples sur C suivant les diviseurs de ce module. Le groupe obtenu est un groupe fini dont la construction peut être effectuée au moyen d'un nombre fini d'opérations. Nous appelerons ce groupe "groupe de Lutz sur C dans R/p" .

Pour obtenir une étude plus complète du groupe des points dans R_p sur C , il est utile d'introduire des sous-groupes convenablement choisis du groupe des points congrus à zéro. Pour celà, on peut utiliser la transformation :

$$x = x_1 \, p^{-2a} \qquad , \qquad y = y_1 \, p^{-3a}$$

avec a entier positif. Elle transforme la courbe C en la courbe C_a :

$$y_1^2 = x_1^3 + A \, p^{4a} \, x_1 + B \, p^{6a} \quad .$$

L'étude détaillée du groupe de Lutz de cette nouvelle courbe montre que certains de ces éléments correspondent aux solutions de la congruence :

$$y^2 \equiv x^3 + A x + B \quad , \quad (\text{mod. } p^{a+1}) \; .$$

Les autres éléments correspondent à des sous-ensembles du groupe des points de C congrus au zéro suivant le module p . On est ainsi conduit à dire que les points de C qui correspondent au points de C_a congrus au zéro suivant le module p sont congrus au zéro sur C suivant le module p^{a+1} . Ces points sont ceux dont les coordonnées sont de la forme :

$$x = x_1 \, p^{-2n} \qquad , \qquad y = y_1 \, p^{-3n}$$

avec x_1 et y_1 unités p-adiques et n supérieur ou égal à $a + 1$. Ils forment un sous-groupe du groupe des points congrus sur C au zéro suivant le module p .

Le groupe-quotient du groupe des points sur C congrus au zéro suivant le module p par le groupe des points congrus au zéro suivant le module p^{a+1} est isomorphe à un sous-groupe du groupe de Lutz. Les éléments de ce sous-groupe correspondent aux solutions des congruences :

$$y^2 \equiv x^3 \qquad (\text{mod. } p^b)$$

pour des valeurs convenables de b . Chacune de ces congruences est unicursale et peut être étudiée à l'aide de la représentation paramétrique :

$$x = t^{-2} \quad , \quad y = t^{-3} \quad .$$

Dans cette représentation, la somme de 2 solutions correspond à la somme de leurs paramètres. Ce qui permet de montrer que :

Le groupe quotient du groupe des points sur C congrus au zéro suivant le module p par le groupe des points congrus au zéro suivant le module p^{a+1} est isomorphe au groupe additif des restes d'entiers p-adiques suivant le module p^a . C'est donc un groupe cyclique d'ordre p^a ; il peut être engendré par l'un quelconque des points de C congrus au zéro suivant le module p , mais non congru à ce point suivant le module p^2 .

Les résultats précédents se transposent facilement à l'étude du groupe des points rationnels sur C (lorsque A et B sont des entiers rationnels), mais ne donnent ainsi que des renseignements beaucoup moins précis :

Le groupe-quotient du groupe des points rationnels sur C par le groupe des points congrus au zéro suivant le module p est isomorphe à un sous-groupe du groupe de Lutz.

Le groupe-quotient du groupe des points rationnels congrus au zéro suivant le module p par le groupe des points congrus au zéro suivant le module p^{a+1} est un groupe cyclique d'ordre 1 ou p^a .

Mais on ne connait pas encore de moyen pour reconnaitre, à l'intérieur du groupe de Lutz, le sous-groupe des éléments qui représentent effectivement des points rationnels. On ne connait pas de moyen pour reconnaitre s'il existe des points rationnels congrus au zéro suivant le module p et non congrus suivant le module p^a .

J'ai énoncé les résultats précédents pour le corps des nombres rationnels et ses extensions p-adiques. Mais ils peuvent être étendus à un corps algébrique fini k et à ses extensions $\mathfrak{p}$-adiques. Toutefois, le groupe additif des entiers $\mathfrak{p}$-adiques suivant le module $\mathfrak{p}^a$ est le produit direct de plusieurs groupes cycliques d'ordres différents. Ce qui complique le second énoncé.

Ces résultats ont permis d'obtenir des propriétés des points exceptionnels rationnels sur une cubique de Weierstrass : on appelle ainsi un point qui est d'ordre fini dans le groupe des points rationnels sur C .

Supposons qu'un tel point M soit congru au zéro suivant le module p . Décomposons son ordre en le produit d'une puissance p^b de p et d'un entier a premier à p . Si a est différent de 1 , il est possible de choisir une puissance p^n de p suffisamment élevée pour que p^b M ne soit pas congru au zéro suivant le module p^n. Mais, puisque a est premier à p , le second résultat montre que a p M n'est pas congru au zéro suivant le module p^{n+1} , et a fortiori est différent de cet élément. Cette contradiction exige que a soit égal à 1 . Si b est différent de 0 , on peut choisir une puissance p^n de p telle que M ne soit pas congru au zéro suivant le module p^n . Les propriétés du groupe-quotient du groupe des points congrus au zéro suivant le module p^n par le groupe des points congrus au zéro suivant le module p^{n+m} montrent que l'ordre de M est divisible par p^m , aussi grand que soit m . Cette nouvelle contradiction exige que b soit nul. Il n'y a donc pas de point rationnel exceptionnel congru au zéro suivant le module p , sauf le zéro lui-même.

En comparant les propriétés analogues pour tous les nombres premiers, on obtient le théorème de Nagell-Lutz :

Les coordonnées d'un point rationnel exceptionnel sur une cubique de Weierstrass sont des entiers rationnels.

On peut encore étendre ce résultat aux points exceptionnels dans un corps algébrique fini k ; mais son énoncé est plus compliqué. On sait construire effectivement tous les points exceptionnels sur une cubique de Weierstrass donnée dans un corps algébrique fini.

Pour construire le groupe des points rationnels sur une cubique de Weierstrass, il reste à construire les points d'ordre infini. On sait que ces points peuvent être obtenus à partir d'un nombre fini d'entre eux qui forment une base du groupe. Mais on ne sait pas construire une pareille base.

Les méthodes classiques de MM. MORDELL [5] et WEIL [6] introduisent les différentes classes du groupe des points rationnels sur C par rapport au sous-groupe formé par les produits par 2 des points rationnels. A chacune de

ces classes, on fait correspondre une courbe de genre un et de degré 4 . On sait construire toutes ces courbes, qui sont en nombre fini, sans connaitre une base du groupe des points rationnels ; mais on construit en même temps d'autres courbes qui ne contiennent aucun point rationnel et qui correspondent aux groupes des points sur C dans certains corps quadratiques. Il reste donc à reconnaître, parmi l'ensemble des courbes ainsi construites et que j'appellerai courbes de Weil de C , celles qui contiennent effectivement des points rationnels.

Or une condition nécessaire pour qu'une courbe contienne des points rationnels est qu'elle contienne des points dans chaque corps des restes suivant un module premier. Un résultat de F.K. SCHMIDT [7] montre d'ailleurs qu'une courbe indécomposable dans un corps de restes et dans ses extensions algébriques contient des points dans ce corps. Il n'y a qu'un nombre fini de modules premiers pour lesquels une courbe donnée se décompose dans une extension du corps des restes suivant ce module. Les méthodes de Mlle LUTZ permettent d'étudier les courbes de Weil dans les corps de restes correspondants.

Mais les résultats ainsi obtenus restent insuffisants. On sait qu'une courbe de genre supérieur à zéro peut contenir des points dans tous les corps de restes sans contenir des points rationnels [7] .

Or on peut appliquer la méthode de Mordell-Weil en remplaçant le sous-groupe des produits par 2 des points rationnels par le sous-groupe des produits par un autre entier n . Il semble que l'étude des courbes de Weil correspondantes dans les corps des restes donnent des résultats différents suivant le choix de cet entier n . Les méthodes de Mlle LUTZ devraient permettre de déterminer l'entier n pour lequel on obtient les résultats les plus complets ; ce serait un progrès important.

Si on considère une courbe C de genre g supérieur à un, on ne peut plus organiser les points rationnels sur C en groupe abélien. Mais POINCARE a montré qu'on peut organiser en groupe abélien les points rationnels de sa jacobienne ou, ce qui revient au même, les ensembles rationnels de g points sur C . La méthode de Mordell-Weil permet encore de montrer que le groupe ainsi formé peut être engendré au moyen d'une base finie.

Il y aurait donc intérêt à transposer à ces groupes les méthodes et les

résultats de Mlle LUTZ. Mais cette généralisation est loin d'être immédiate. En effet, la forme normale de Weierstrass pour une courbe de genre un joue un rôle certain dans les démonstrations de Mlle LUTZ et ce rôle est peut être essentiel pour certains résultats. Or on ne connait pas d'équivalent à cette forme pour la jacobienne d'une courbe de genre supérieur à un . Il faudrait donc déterminer quelles sont exactement les propriétés de la forme normale de Weierstrass qui sont utiles dans les démonstrations de Mlle LUTZ pour généraliser ces propriétés aux jacobiennes.

La propriété que le zéro est le point à l'infini de la courbe peut d'abord sembler importante. Mais l'utilisation convenable de coordonnées homogènes permet de réduire la distinction entre les points à distance finie et à l'infini, dans les corps de restes comme dans le corps des rationnels. La propriété que la somme de trois points alignés est nulle est certainement plus importante ; remarquons qu'elle a pour conséquence que le zéro est un point d'inflexion de la courbe. Il n'est pas impossible toutefois d'utiliser une définition géométrique plus générale de l'opération d'addition sur une courbe de genre un. La propriété qui me semble la plus essentielle est qu'une cubique de Weierstrass à coefficients rationnels est indécomposable dans tous les corps des restes et leurs extensions. Il est également possible que les représentations des courbes unicursales dans un corps de restes ait une certaine importance.

C'est donc l'étude des dégénérescences d'une jacobienne dans un corps de restes qui doit être la première difficulté d'une généralisation du travail de Mlle LUTZ.

En terminant, je souhaite vivement que les problèmes que j'ai évoqués intéressent quelque jeune mathématicien et que celui-ci apporte une contribution décisive à leurs solutions.

BIBLIOGRAPHIE

[1] E. LUTZ : Sur l'équation $y^2 = x^3 - A x - B$ dans les corps p-adiques. J.f. Math., t. 177 (1937).

[2] H. POINCARÉ : Sur les propriétés arithmétiques des courbes algébriques. J. de Math., t. 7 (1901).

[3] T. NAGELL : Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. Vid. Akad. Skrifter Oslo, 1 (1935).

[4] F. CHÂTELET : Points exceptionnels des cubiques. Colloque d'algèbre et de théorie des nombres. Paris 1949.

[5] L.J. MORDELL: On the rational solutions of the indeter minate equations of the third and fourth degrees. Proc. of the Cambridge phil. Soc., t. 21 (1922).

[6] A. WEIL : Sur un théorème de MORDELL. Bull. des Sc. math., t. 54 (1930).

[7] F.K. SCHMIDT: Analytische Zahlentheorie in Körpern der Charakteristik p. Math. Zeit., t. 33 (1931). Voir aussi S. LANG : Algebraic groups over finite fields. Am. J. of Math., t. 78 (1956).

[8] Voir par exemple : E.S. SELMER : On Cassels conditions for rational solubility of the diophantine equation $\eta^2 = \xi^3 - D$ Archiv f. Mat. of Naturw., t. 53 (1956).