GUY TERJANIAN

Équations diophantiennes p-adiques

Séminaire N. Bourbaki, 1966, exp. n° 299, p. 323-335
<http://www.numdam.org/item?id=SB_1964-1966__9__323_0>

Séminaire BOURBAKI
18e année, 1965/66, n° 299 Novembre 1965

ÉQUATIONS DIOPHANTIENNES p-ADIQUES

(d'après J. AX et S. KOCHEN [1])

par Guy TERJANIAN

1. Méthodes et résultats.

Nous désignerons pour un nombre premier p, par F_p le corps fini à p éléments, par Q_p le corps des nombres p-adiques, par S_p le corps des séries formelles à une indéterminée à coefficients dans F_p.

Rappelons qu'un corps k possède la propriété C_r si

" tout polynôme homogène $f \in k[X_1,\dots,X_n]$ de degré d, où $n > d^r > 0$, a un zéro non trivial dans k ".

Artin a conjecturé que les p-adiques sont C_2. Pour $d = 2$ la propriété est classique ; pour $d = 3$, elle a été démontrée par D. Lewis dans [9].

Ax et Kochen ont obtenu récemment le résultat suivant :

" Pour tout entier $d > 0$, il y a un ensemble fini de nombres premiers $A(d)$, tel que si p est un nombre premier $\notin A(d)$, tout polynôme sans terme constant $f \in Q_p[X_1,\dots,X_n]$, de degré d, où $n > d^2$, a un zéro non trivial dans Q_p ".

Ils ont démontré également le résultat suivant, conjecturé par Lang dans [8] et dont N. Greenleaf a donné une démonstration tout à fait différente dans [4] :

" Soit $f \in Z[X_1,\dots,X_n]$, de degré $d > 0$, sans terme constant, où $n > d$, il existe un ensemble fini de nombres premiers B, tel que pour tout nombre premier $p \notin B$, f ait un zéro non trivial dans Q_p ".

Ces deux résultats sont conséquences du principe général suivant :

" Pour toute "propriété élémentaire" Δ , il y a un ensemble fini de nombres premiers $C(\Delta)$, tel que si p est premier et si $p \notin C(\Delta)$, Δ est vraie dans Q_p si et seulement si Δ est vraie dans S_p ".

La démonstration de ce principe, qu'on trouvera ici, est sans doute inspirée d'un travail de logique de Kochen [6] ; elle utilise les notions d'ultraproduit et de propriété élémentaire que nous allons définir, des notions générales de théorie des valuations et l'hypothèse du continu, ce qui n'est pas gênant d'après le résultat de Gödel [3].

2. Ultraproduits et propriétés élémentaires.

Un ultrafiltre U sur un ensemble I sera dit principal, s'il existe un $i \in I$ tel que $U = \{V$ tels que $i \in V\}$. On voit aisément que toute partie infinie d'un ensemble I appartient à un ultrafiltre non principal de I et que toute partie cofinie de I est élément de tout ultrafiltre non principal de I .

On appellera "corps valué" un triplet $\underline{F} = (F, v, \Gamma)$ formé d'un corps F muni d'une valuation v à valeurs dans le groupe Γ . On désignera pour $O_{\underline{F}}$ l'anneau de la valuation, par $k(\underline{F})$ le corps résiduel.

Ainsi on distinguera le corps Q_p du corps valué $\underline{Q}_p$; de même S_p et $\underline{S}_p$.

DÉFINITION.- Soit $(F_i)_{i \in I}$ une famille de corps, U un ultrafiltre sur I , on appelle ultraproduit suivant U des F_i et on note $\prod_U F_i$, le corps obtenu en quotientant l'anneau $\prod_I F_i$ par la relation d'équivalence $\{ i \in I$ tels que $x_i = y_i \} \in U$.

DÉFINITION.- Soit $(\Gamma_i)_{i\in I}$ une famille de groupes totalement ordonnés, U un ultrafiltre sur I, on définit un groupe totalement ordonné, qu'on appelle <u>l'ultraproduit suivant</u> U <u>des</u> Γ_i et qu'on note $\prod_U \Gamma_i$ comme suit :

$\prod_U \Gamma_i$ est le quotient du groupe $\prod_I \Gamma_i$ par la relation d'équivalence $\{i \in I \text{ tels que } x_i = y_i\} \in U$, relation compatible avec la structure de groupe de $\prod_I \Gamma_i$.

Si alors $*$ désigne l'application canonique de $\prod_I \Gamma_i$ sur $\prod_U \Gamma_i$, on vérifie qu'il y a une structure d'ordre et une seule sur $\prod_U \Gamma_i$ telle que pour $\alpha, \beta \in \prod_I \Gamma_i$:

$$\alpha^* < \beta^* \iff \{i \in I \text{ tels que } \alpha_i < \beta_i\} \in U .$$

On obtient ainsi un ordre total sur $\prod_U \Gamma_i$.

DÉFINITION.- Soit $(\underline{F}_i)_{i\in I}$ une famille de corps valués, $\underline{F}_i = (F_i, v_i, \Gamma_i)$, U un ultrafiltre sur I, on appelle <u>ultraproduit suivant</u> U <u>des</u> $\underline{F}_i$ et on note $\prod_U \underline{F}_i$ le corps valué $(\prod_U F_i, v, \prod_U \Gamma_i)$ où si l'on désigne par $*$ les applications canoniques de $\prod_I F_i$ (resp. $\prod_I \Gamma_i$) sur $\prod_U F_i$ (resp. $\prod_U \Gamma_i$), l'application v est définie par $v(f^*) = (v_i(f_i))^*$.

PROPOSITION.- Sous les hypothèses précédentes, on a

$$k(\prod_U \underline{F}_i) = \prod_U k(\underline{F}_i) \qquad \text{et} \qquad v(\prod_U \underline{F}_i) = \prod_U v_i(\underline{F}_i) .$$

Nous appellerons corps discret un quadruplet $\underline{F} = (F, v, \Gamma, \pi)$ où (F, v, Γ) est un corps valué, Γ a un plus petit élément strictement positif 1_Γ et $\pi \in F$ est tel que $v(\pi) = 1_\Gamma$.

PROPOSITION.- Soit $(\underline{F}_i)_{i\in I}$ une famille de corps discrets, U un ultrafiltre sur I , $\prod_{U} F_i$ est canoniquement muni d'une structure de corps discret.

Passons aux propriétés élémentaires. Nous décrirons cette notion dans le système formel de Bourbaki. Soit T la théorie des ensembles de Bourbaki, nous désignerons par C , V , D les théories plus fortes que T , obtenues en adjoignant respectivement aux axiomes de T les axiomes

(C) " $\underline{F}$ est un corps " ;

(V) " $\underline{F}$ est un corps valué " ;

(D) " $\underline{F}$ est un corps discret ".

Nous nous contenterons de décrire les propriétés élémentaires pour la théorie D , les changements à apporter dans le cas de C et de V sont faciles.

Les <u>formules atomiques</u> sont les relations $v(f) > v(g)$ où f et g sont des polynômes explicites de l'anneau $Z[\pi][A,B,\dots,L]$.

Les <u>chaînes de type</u> α sont des suites de relations de la théorie D , telles que pour toute relation A de la suite l'une des conditions suivantes soit réalisée :

a) A est une formule atomique.

b) Il y a dans la chaîne une relation B précédant A telle que A soit (non B).

c) Il y a deux relations B et C précédant A telles que A soit (B ou C).

d) Il y a une relation B précédant A et une lettre x qui n'est pas une constante telles que A soit $(\exists x)(x \in F$ et $B)$.

Les <u>relations de type</u> α sont les relations qui figurent dans des chaînes de type α . <u>Les relations de type</u> β sont les relations de type α qui ne contiennent pas d'autres lettres que les constantes. Enfin les propriétés élémentaires sont les relations qui sont équivalentes dans la théorie D à des relations de type β .

Exemples : Les relations suivantes sont équivalentes à des relations de type α : $a = 0$, le polynôme $ax^3 + bx^2 + cx + d$ est irréductible (séparable).

Le principe métamathématique suivant montre l'intérêt de la notion de propriété élémentaire.

PRINCIPE $\prod$.- Soit $(\underline{F}_i)_{i\in I}$ une famille de corps (resp. de corps valués, de corps discrets), U un ultrafiltre sur I , et Δ une propriété élémentaire. Alors Δ est vraie pour $\prod_U \underline{F}_i$ si et seulement si l'ensemble des i tels que Δ soit vraie pour $\underline{F}_i$ est un élément de U .

Le principe $\prod$ résulte du lemme plus précis suivant :

LEMME.- Soient $(\underline{F}_i)_{i\in I}$ une famille de corps (resp. de corps valués, de corps discrets), U un ultrafiltre sur I , $R\{a,b,\dots,\ell;\underline{F}\}$ une relation de type α . Soient alors A,B,...,L de nouvelles lettres. Sous l'hypothèse $A \in \prod_I \underline{F}_i$, $B \in \prod_I \underline{F}_i$,..., $L \in \prod_I \underline{F}_i$, on a l'équivalence des conditions :

a) $R\{A^*,B^*,\dots,L^*\,;\,\prod_U \underline{F}_i\}$

b) $\{\,i \text{ tels que } R\{A_i\,,B_i\,,\dots,L_i\,;\underline{F}_i\}\} \in U$.

La démonstration facile, dans la chaîne de type α où figure la relation R , on le démontre de proche en proche pour toutes les relations.

DÉFINITION.- On dit qu'un corps valué $\underline{F} = (F,v,\Gamma)$ possède la propriété de Hensel-Rychlik, si pour tout polynôme unitaire $J \in 0_{\underline{F}}[X]$ tel qu'il existe un $f \in 0_{\underline{F}}$ tel que $v(J(f)) > v(D(J))$ où D désigne le discriminant, il existe $f' \in 0_{\underline{F}}$ tel que $J(f') = 0$.

PROPOSITION.- Si tout élément d'une famille $(\underline{F}_i)_{i \in I}$ de corps valués possède la propriété de Hensel-Rychlik, tout ultraproduit $\prod_U \underline{F}_i$ de ces corps la possède.

En effet, Hensel-Rychlik est une propriété élémentaire.

Nous appellerons corps résoluble un corps dont toutes les extensions galoisiennes de degré fini ont un groupe de Galois résoluble.

PROPOSITION.- Si les corps $(\underline{F}_i)_{i \in I}$ sont résolubles, tout ultraproduit de ces corps est résoluble.

On vérifie en effet que la résolubilité est une propriété élémentaire.

On dira qu'un corps valué $\underline{F} = (F, v, \Gamma)$ a la propriété d'unicité si la valuation ne s'étend que d'une seule manière à une clôture algébrique de F .

PROPOSITION.- Si $(\underline{F}_i)_{i \in I}$ est une famille de corps valués, si chaque $\underline{F}_i$ a la propriété d'unicité, tout ultraproduit de ces corps possède la propriété d'unicité.

En effet, on démontre en utilisant la théorie du polygone de Newton [Bourbaki, Alg. Comm., Chap. VI, § 4, exerc. 11] que la propriété d'unicité équivaut à la suivante :

" Si $X^n + a_1 X^{n-1} + \dots + a_n$ est un polynôme irréductible, on a

$$j\, v(a_n) \leq n\, v(a_j) \qquad \text{pour tout } j \text{ tel que } 1 \leq j \leq n \text{ " ,}$$

ce qui est une propriété élémentaire.

DÉFINITION.- Soit $\underline{F} = (F, v, \Gamma, \pi)$ un corps discret, on appelle section de $\underline{F}$ un homomorphisme s du groupe Γ dans le groupe multiplicatif du corps F tel que :

1°) $v \circ s$ soit l'identité de Γ ;

2°) $v(1_\Gamma) = \pi$.

PROPOSITION.- Soit $(\underline{F}_i)_{i\in I}$ une famille de corps discrets possédant des sections, tout ultraproduit des $\underline{F}_i$ possède une section.

Passons à une notion relative au groupe des valeurs.

On appelle Z-groupe, un groupe abélien, totalement ordonné ayant un plus petit élément strictement positif et tel que $(G : nG) = n$ pour tout entier $n > 0$.

LEMME.- Soit $(G_i)_{i\in I}$ une famille de Z-groupes.

a) Tout ultraproduit des G_i est un Z-groupe.

b) Si $\mathrm{Card}\,(G_i) \leq 2^{\aleph_0}$ pour tout i, si $\mathrm{Card}\,(I) = \aleph_0$ et si U est un ultrafiltre non principal

$$\mathrm{Card}\,(\prod_U G_i) = 2^{\aleph_0} .$$

(Ici $\aleph_0 = \mathrm{Card}\,(N)$.)

LEMME.- Soient I un ensemble infini et dénombrable, U un ultrafiltre non principal sur I ; soit $(\underline{F}_i)_{i\in I}$ une famille de corps discrets, alors l'ultraproduit $\prod_U \underline{F}_i$ est ω-pseudo-complet au sens de Kaplansky [5], si l'on pose $\omega = \mathrm{Ord}(N)$.

3. L-corps.

DÉFINITION.- On appelle L-corps un quintuplet $\underline{F} = (F,v,\Gamma,\pi,C)$ où

(i) (F,v,Γ,π) est un corps discret de caractéristique zéro ;

(ii) Γ est un Z-groupe et $v(F) = \Gamma$;

(iii) C est un sous-corps de F sur lequel la valuation est impropre et tel que

$$k(C) = k(F) \;;$$

(iv) il existe une clôture algébrique F' de F , une clôture algébrique C'

de C et une suite $\pi_1, \pi_2, \ldots$ d'éléments de F' tels que $(\pi_i)^i = \pi$ pour tout i et que

$$F' = F(C', \pi_1, \pi_2, \ldots) .$$

On démontre facilement, dans l'ordre, les faits suivants :

PROPOSITION.- Soit $\underline{F} = (F, v, \Gamma, \pi, C)$ un L-corps, (F, v, Γ) a la propriété d'unicité.

PROPOSITION.- Si $\underline{F}$ est un corps valué de caractéristique zéro, si $\underline{F}$ a la propriété d'unicité, alors $\underline{F}$ a la propriété de Hensel-Rychlik.

PROPOSITION.- Soit $\underline{F} = (F, v, \Gamma, \pi, C)$ un L-corps, (F, v, Γ) a la propriété de Hensel-Rychlik.

PROPOSITION.- Soit $\underline{F} = (F, v, \Gamma, \pi, C)$ un L-corps, F_0 un sous-corps de F algébriquement fermé dans F et contenant $C(\pi)$, alors $(F_0, v|F_0, v(F_0), \pi, C)$ est un L-corps.

Enonçons le résultat principal relatif aux L-corps.

THÉORÈME 1.- Soient $\underline{F} = (F, v, \Gamma, \pi, C)$ et $\underline{F}' = (F', v', \Gamma, \pi', C)$ deux L-corps, de même groupe des valeurs, de même corps résiduel, tels que :

a) Card $(\Gamma) = \aleph_1$ (le successeur de $\aleph_0$) ;

b) $\underline{F}$ et $\underline{F}'$ sont pseudo-complets (Kaplansky [5]) ;

c) $\underline{F}$ et $\underline{F}'$ possèdent des sections.

$\underline{F}$ et $\underline{F}'$ sont alors des L-corps isomorphes.

La démonstration est un peu longue ; nous donnerons les définitions nécessaires et nous en indiquerons la marche.

DÉFINITION.- Soit $\underline{F} = (F, v, \Gamma, \pi, C)$ un L-corps ; un sous-corps E de F est dit $\underline{F}$-complet, si E contient $C(\P)$ et si $(E,v|E,v(E))$ n'a pas d'extension immédiate dans (F,v,Γ).

Notation : Si $H \subset K$ est un sous-groupe du groupe commutatif K, $[H|K]$ sera le sous-groupe des $x \in K$ tels que $mx \in H$ pour un entier m.

DÉFINITION.- Soit $\underline{F} = (F,v,\Gamma)$ un corps valué et E un sous-corps de F. On dira qu'un sous-corps E' de F est une fermeture de E dans $\underline{F}$ si E' est maximal pour la propriété " K est un sous-corps de F et $v(K) \subset [v(E)|\Gamma]$ ".

On démontre alors les propositions suivantes.

PROPOSITION.- Soit $\underline{F} = (F,v,\Gamma,\P,C)$ un L-corps, ω-pseudo-complet. Soit E un sous-corps de F, $\underline{F}$-complet tel que $v(E)$ soit un sous-groupe dénombrable et pur de Γ. Alors $(E,v|E,v(E))$ est maximal au sens de Kaplansky [5], E est algébriquement fermé dans F et $(E,v|E,v(E),\P,C)$ est un L-corps.

PROPOSITION.- Soient $\underline{F} = (F,v,\Gamma,\P,C)$ et $\underline{F'} = (F',v',\Gamma',\P',C')$ deux L-corps. Supposons que $\underline{F}$ et $\underline{F'}$ soient ω-pseudo-complets et possèdent des sections. Soient alors E (resp. E') un sous-corps de F (resp. F'), $\underline{F}$-complet (resp. $\underline{F'}$-complet) tel que $v(F)$ (resp. $v'(F')$) soit un sous-groupe pur et dénombrable de Γ (resp. Γ'). Soient $\underline{E} = (E,v|E,v(E),\P,C)$ et $\underline{E'} = (E',v|E',v(E'),\P',C')$ les L-corps construits à partir de E et de E' et $\varphi : \underline{E} \longrightarrow \underline{E'}$ un isomorphisme de L-corps. Alors, pour un x quelconque de F, non dans E, il existe une fermeture $\bar{E}$ de $E(x)$ dans $\underline{F}$ telle que $\underline{\bar{E}} = (\bar{E},v|\bar{E},v(\bar{E}),\P,C)$ soit un L-corps et que φ se prolonge en un isomorphisme de $\underline{\bar{E}}$ sur un sous-L-corps $\underline{\bar{E}'}$ de $\underline{F'}$ et que de plus on ait $v(\bar{E}) = [v(E(x))|\Gamma]$.

Le théorème 1 se démontre par utilisation transfinie de la proposition précédente.

4. Applications.

Soit U un ultrafiltre non principal sur l'ensemble des nombres premiers, on pose

$$\underline{Q} = \prod_U \underline{Q}_p \qquad \text{et} \qquad \underline{S} = \prod_U \underline{S}_p .$$

Appliquons à $\underline{Q}$ et $\underline{S}$ les résultats du n° 2, on a :

PROPOSITION.- $\underline{Q}$ et $\underline{S}$ sont des corps discrets, ont pour corps résiduel $\prod_U F_p$, qui est de caractéristique zéro, pour groupe de valeurs $\prod_U Z$ qui est un Z-groupe de cardinal $2^{\aleph_0}$; $\underline{Q}$ et $\underline{S}$ sont résolubles, possèdent la propriété d'unicité, possèdent des sections et sont ω-pseudo-complets.

Le fait que $\underline{Q}$ et $\underline{S}$ sont des L-corps résulte du lemme suivant.

LEMME.- Soit $\underline{F} = (F,v,\Gamma)$ un corps valué tel que

1) $k(\underline{F})$ est de caractéristique zéro ;

2) Γ est un Z-groupe et $v(F) = \Gamma$;

3) $\underline{F}$ est résoluble et possède la propriété d'unicité.

Alors, il existe un (ou plusieurs) sous-corps C de F et un (ou plus) élément $\pi \in F$ tels que la valuation soit impropre sur C, que $k(C) = k(F)$ et que $v(\pi) = 1_\Gamma$; soit (C,π) un tel couple (F,v,Γ,π,C) est un L-corps.

THÉORÈME 2.- Sous l'hypothèse du continu, $\underline{Q}$ et $\underline{S}$ sont isomorphes.

Cela résulte du théorème 1 et de ce qui précède.

THÉORÈME 3.- Pour toute propriété élémentaire Δ, il existe un ensemble fini de nombres premiers $C(\Delta)$, tel que si p est un nombre premier n'appartenant pas à $C(\Delta)$, Δ est vraie pour Q_p si et seulement si Δ est vraie pour S_p.

Démontrons le, Soit X (resp. Y) l'ensemble des nombres premiers p tels que Δ soit vraie dans Q_p (resp. S_p). Supposons que contrairement à l'énoncé $(X - Y) \cup (Y - X)$ soit infini. Soit alors U un ultrafiltre non principal sur l'ensemble P des nombres premiers dont $(X - Y) \cup (Y - X)$ soit un élément. Appliquant le principe Π , on voit que Δ est vraie pour l'un des corps $\underline{Q}$ et $\underline{S}$ mais non pour l'autre, ce qui est absurde.

THÉORÈME 4.- Soient $f_1,\dots,f_r$ des polynômes de $Z[X_1,\dots,X_n]$. Il existe un ensemble fini de nombres premiers $A(f_1,\dots,f_r)$, tel que si $p \notin A$, toute solution de $\bar{f}_1 = \bar{f}_2 = \dots = \bar{f}_r = 0$ dans F_p est l'image d'une solution de $f_1 = f_2 = \dots = f_r = 0$ dans l'anneau Z_p des entiers p-adiques.

Dans S_p , c'est en effet l'image d'une solution pour tout p .

THÉORÈME 5.- Soient $f_1,\dots,f_r$ des polynômes sans termes constants de $Z[X_1,\dots,X_n]$. Si d_i est le degré de f_i et si $n > \sum_1^r d_i$, il existe un ensemble fini de nombres premiers $B(f_1,\dots,f_r)$, tel que si le nombre premier p n'appartient pas à B , les f_i ont un zéro commun non trivial dans l'anneau Z_p des entiers p-adiques.

Ce théorème est un corollaire du précédent, compte tenu du théorème de Chevalley [2].

THÉORÈME 6.- Soient $d_1,\dots,d_r$ des entiers strictement positifs. Il existe un ensemble fini de nombres premiers $B(d_1,\dots,d_r)$ tel que pour tout nombre premier $p \notin B(d_1,\dots,d_r)$, tout système de polynômes $f_1,\dots,f_r$ de $Q_p[X_1,\dots,X_n]$, de degrés d_i , sans termes constants, à $n > \sum d_i^2$ indéterminées, a un zéro non trivial dans Q_p .

L'analogue pour S_p est dans la thèse de Lang [7].

5. Un résultat apparenté.

On sait qu'un corps C_1 a une dimension cohomologique inférieure ou égale à 1 , et que la dimension cohomologique des p-adiques est 2 . Ces résultats permettaient d'envisager une solution cohomologique à la conjecture d'Artin. Or Ax vient de construire :

Un corps de caractéristique zéro, quasi-fini au sens de Serre [10], de dimension cohomologique 1 , qui n'est pas C_1 , ni même C_r pour aucun r .

-:-:-:-

BIBLIOGRAPHIE

[1] J. AX et S. KOCHEN - Diophantine problems over local fields I. Amer. J. of Math., 87, 1965, p. 605-630.

[2] C. CHEVALLEY - Démonstration d'une hypothèse de M. Artin. Abh. Math. Sem. Hausischen Univ. vol. 11 (1935).

[3] K. GODEL - The consistency of the continuum hypothesis. Princeton (1940).

[4] N. GREENLEAF - Irreducible subvarieties and rational points. Amer. J. of Math. (janvier 1965).

[5] I. KAPLANSKY - Maximal fields with valuations. Duke Math. J., vol. 9, (1942).

[6] S. KOCHEN - Ultraproducts in the theory of models. Ann. of Math., vol. 74, (1961).

[7] S. LANG - On quasi algebraic closure. Ann. of Math., vol. 55, (1952).

[8] S. LANG - Theorems and conjectures in diophantine equations. Bull. Amer. Math. Soc., vol. 66 (1960).

[9] D. LEWIS - Cubic homogeneous polynomials over p-adic number fields. Ann. of Math., vol. 56 (1952).

[10] J.-P. SERRE - Corps locaux. Publ. de l'Institut de Math. de Nancago, Hermann, Paris (1962).

-:-:-:-

<u>N. B.</u>- Indiquons que la partie II du travail d'Ax et Kochen, contient des résultats de logique importants. Citons les suivants :

THÉORÈME.- Pour toute propriété élémentaire Δ , l'ensemble des nombres premiers p tels que Δ soit vraie dans Q_p est récursif.

THÉORÈME.- La théorie du corps Q_p est décidable.

ERRATA

<u>Page 299-01</u> - Fin de la ligne 7 et début de la ligne 6 du bas, remplacer "sans terme constant" par "homogène".

<u>Page 299-11</u> - Ligne 3 du bas, remplacer "sans termes constants" par "homogènes".

-:-:-:-

Note du Secrétariat, juin 1966 - Depuis cet exposé, G. TERJANIAN a montré que la conjecture d'Artin est fausse ; cf. C.R. Acad. Sci. Paris, t. 262, 1966, p. 612.

-:-:-:-