Séminaire Delange-Pisot-Poitou. Théorie des nombres

Guy Terjanian

Progrès récents dans l'étude de la propriété Ci des corps

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 2 (1966-1967), exp. n° 13, p. 1-7

<http://www.numdam.org/item?id=SDPP_1966-1967__8_2_A4_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
8e année, 1966/67, n° 13

27 février 1967

PROGRÈS RÉCENTS DANS L'ÉTUDE DE LA PROPRIÉTÉ C_i DES CORPS

par Guy TERJANIAN

1. Le problème de Lang.

Rappelons ce qu'est la propriété C_i .

Soient A un anneau intègre, i un nombre réel positif, et $d \geqslant 1$ un entier ; on dit que A a la propriété C_i en degré d , si pour tout entier n tel que $n > d^i$ et pour tout polynôme f homogène de degré d de l'anneau $A[X_1, \ldots, X_n]$, il existe un élément a non nul de A^n tel que $f(a) = 0$.

On dit qu'un anneau intègre a la propriété C_i , s'il a la propriété C_i pour tout degré. Il est clair qu'un anneau intègre a la propriété C_i si, et seulement si, son corps des fractions a cette même propriété.

Dans [5], LANG a posé le problème suivant :

Soit K un corps muni d'une valuation discrète pour laquelle il est complet ; si le corps de restes k de K a la propriété C_i , alors K a-t-il la propriété C_{i+1} ?

Les résultats sur ce problème se partagent, grosso modo, en résultats positifs d'un caractère assez général et en résultats spécifiques aux corps p-adiques, lesquels sont plutôt négatifs.

2. Résultats positifs.

Enonçons un théorème de Greenberg [3].

THÉORÈME 1 (GREENBERG). - *Soient A un anneau de valuation discrète, hensélien, π une uniformisante de A . Soient K le corps des fractions de A , k le corps de restes de A , et soient $\hat{A}$ le complété de A et $\hat{K}$ le complété de K . Supposons $\hat{K}$ séparable sur K .*

Alors, pour tout système de polynômes $F = (F_1, \ldots, F_r)$ de $A[X_1, \ldots, X_n]$ il existe des entiers $N \geqslant 1$, $c \geqslant 1$ et $s \geqslant 0$, tels que si v est un entier supérieur ou égal à N et si $x \in A^n$ est tel que

$$F_i(x) \equiv 0 \quad (\pi^v) \qquad \text{pour chaque } i \ ,$$

alors il existe $y \in A^n$ tel que :

1° $F(y) = 0$,
2° $y \equiv x \ (\pi^{[v/c]-s})$,

où $[a]$ désigne la partie entière de a .

Signalons que ce théorème est le meilleur possible en ce sens que la restriction " $\hat{K}$ séparable sur K " est nécessaire et qu'on ne peut pas non plus y faire $c = 1$.

Signalons encore que la démonstration du théorème 1 contient sans doute les idées nécessaires à la description d'une élimination des quantificateurs dans les corps p-adiques.

Le théorème 1 a les corollaires suivants.

COROLLAIRE 1. - Soit Z un préschéma de type fini sur A , où A satisfait les hypothèses du théorème 1 ; Z a un point dans A si, et seulement si, il a un point dans A/π^v pour chaque v .

COROLLAIRE 2. - Soit Z un préschéma projectif sur un anneau A satisfaisant aux hypothèses du théorème 1, alors Z a un point dans A si, et seulement si, Z a un point primitif dans chaque anneau A/π^v (par point primitif, on désigne un point dont l'image dans A/π n'est pas nulle).

De ce corollaire, on déduit immédiatement le théorème suivant.

THÉORÈME 2. - Soit A un anneau de valuation discrète, hensélien, de corps des fractions K . Soient $\hat{A}$ et $\hat{K}$ les complétés de A et de K , et supposons $\hat{K}$ séparable sur K . Alors A est C_i si, et seulement si, $\hat{A}$ est C_i .

Le corollaire 2 fournit aussi la solution du problème de Lang dans le cas de l'égale caractéristique.

THÉORÈME 3. - Soit K un corps muni d'une valuation discrète pour laquelle il est hensélien. Supposons que $\hat{K}$, le complété de K , soit séparable sur K . Soit k le corps de restes de K , alors si K et k ont la même caractéristique, et si k a la propriété C_i , K a la propriété C_{i+1} .

Démonstration. - Tenant compte du théorème 2, il suffit de montrer que $k[[t]]$ est C_{i+1} . Pour cela, soit f une forme de degré d à coefficients dans $k[[t]]$ en les indéterminées X_1 , ... , X_n avec $n > d$; il s'agit de montrer que f a

un zéro non trivial dans $k[[t]]$. D'après le corollaire 2, il suffit de voir que f a un zéro primitif dans $k[[t]]/t^v$ pour chaque v . Mais on a

$$k[[t]]/t^v = k[t]/t^v \quad ,$$

et il suffit d'utiliser le fait que $k[t]$ est C_{i+1} , fait bien connu par les articles de LANG [5] et NAGATA [6].

C. Q. F. D.

Le corollaire 2 donne aussi le théorème ci-après.

THÉORÈME 4. - Soit K un corps muni d'une valuation discrète pour laquelle il est hensélien. Soit $\hat{K}$ le complété de K , et supposons $\hat{K}$ séparable sur K , alors si le corps de restes de K est algébriquement clos, K a la propriété C_1.

Démonstration. - C'est celle de LANG [5] à ceci près qu'on y remplace le "corollaire du théorème 9" par le corollaire 2 ci-dessus, substitution qui simplifie beaucoup la démonstration.

Montrons comment on peut, à partir du théorème 3, obtenir une variante d'un résultat de AX et KOCHEN [1].

Désignons par X_i la propriété suivante du couple (K , v) :

K est un corps, muni d'une valuation discrète v , pour laquelle K est hensélien, et le corps de restes de K a la propriété C_i .

Désignons encore par Y_p , pour p premier ou nul, la propriété suivante du couple (K , v) :

K est un corps, muni de la valuation discrète v , dont le corps de restes est de caractéristique p .

Le théorème 3, en caractéristique zéro, peut se formuler :

$$X_i \text{ et } Y_0 \Longrightarrow K \text{ est } C_{i+1} \ .$$

Soit alors $d \geqslant 1$ un entier, on a, a fortiori,

$$X_i \text{ et } Y_0 \Longrightarrow K \text{ est } C_{i+1} \text{ en degré } d \ .$$

Maintenant, dans le langage de la théorie des corps valués, ou plus précisément des corps munis d'une valuation discrète et normée, X_i s'exprime comme la conjonction d'une infinité de formules, au sens de [4]. D'autre part, Y_0 est la conjonction des formules non Y_2 , non Y_3 , non Y_5 , ...

Or " K est C_{i+1} en degré d " est une formule, donc en vertu du théorème de finitude du calcul des prédicats ([4], page 35 et aussi page 9), il existe une partie finie P de l'ensemble des formules dont X_i et Y_0 sont la conjonction telle que

$$P \Longrightarrow K \text{ est } C_{i+1} \text{ en degré } d .$$

On a $P = U$ et V, où U est une sous-famille finie de X_i, et V une sous-famille finie de Y_0, donc on a, a fortiori,

$$X_i \text{ et } V \Longrightarrow K \text{ est } C_{i+1} \text{ en degré } d .$$

Ceci se traduit par le théorème suivant.

THÉORÈME 5. - Soient $d \geqslant 1$ un entier, et $i \geqslant 0$ un nombre réel. Il existe un entier $\varphi(i , d)$ tel que si p est un nombre premier et si on a $p \geqslant \varphi(i , d)$, alors :

Si K est un corps, muni d'une valuation discrète, hensélien, et si le corps de restes de K est de caractéristique p et a la propriété C_i, K a la propriété C_{i+1} en degré d .

Utilisant le théorème de Chevalley qui dit que les corps finis sont C_1, on en déduit que, pour un entier d donné, les corps p-adiques Q_p sont C_2 en degré d, sauf pour un nombre fini d'entre eux.

La même méthode que celle qui permet de démontrer le théorème 5 fournit le résultat suivant :

Soit d un entier $\geqslant 1$, si le nombre premier p est assez grand, pour tout polynôme f sans terme constant de $Z_p[X_1 , \ldots , X_{2d+1}]$, il existe un x de Z_p, non divisible par p, tel que

$$f(x) \equiv 0 \quad (p^2) .$$

3. Le cas des corps p-adiques.

Commençons par des résultats négatifs dus à BROWKIN [2] et à moi-même [7].

On dira qu'une forme $f \in Z_p[X_1 , \ldots , X_n]$ vaut a modulo p^r, où a est un élément de Z_p, si pour tout x de Z_p, non divisible par p, on a

$$f(x) \equiv a \text{ modulo } p^r .$$

On s'intéressera particulièrement aux formes qui valent 1 modulo une puissance de p.

On voit facilement que pour que le mônôme X^d vaille 1 modulo p^r, il faut et il suffit que d soit divisible par $(p-1)p^{r-1}$; il en résulte que si une forme de degré d vaut 1 modulo p^r, son degré est divisible par $(p-1)p^{r-1}$.

Donnons des exemples simples de formes valant 1 modulo p^2 :

$(X^p - YX^{p-1})^{p-1} + Y^{p(p-1)}$ pour $p \geqslant 3$,

$X^4 + Y^4 + Z^4 + 3X^2Y^2 + 3X^2Z^2 + 3Y^2Z^2 + 3X^2YZ + 3Y^2XZ + 3Z^2XY$ pour $p = 2$.

Donnons maintenant les exemples de BROWKIN, p est un nombre premier quelconque, $r \geqslant 1$ est un entier, et on suppose $p^r \geqslant 2r + 1$.

Soient $a_1 , \ldots , a_{r+1}$ les éléments de Z qui sont solutions du système :

$$a_1 + \ldots + a_{r+1} = 1$$

$$(r+1)a_1 + \ldots + (2r+1)a_{r+1} = 0$$

$$(r+1)^r a_1 + \ldots + (2r+1)^n a_{r+1} = 0 \quad .$$

Désignons par n la partie entière de $p^r/(2r+1)$, et posons, pour K entier compris entre 1 et n,

$$\psi_K = \sum_1^{r+1} a_i X_1^{p^r-(r+i)(k-1)} (X_2 , \ldots , X_K)^{r+i} \quad ,$$

$$\varphi_K = \sum_{1 \leqslant i_1 \leqslant i_2 \leqslant \ldots \leqslant i_K \leqslant n} \psi_K(X_{i_1} , \ldots , X_{i_K}) \quad ,$$

$$f = \sum_1^n (-1)^{K+1} \varphi_K \quad ,$$

$$g = f(X_1^{p-1} , \ldots , X_n^{p-1}) \quad .$$

On vérifie que g vaut 1 modulo p^{r+1} .

Voyons comment on utilise les formes de valeur 1 pour construire des formes sur Z_p qui n'ont pas de zéro dans Z_p .

Soit f une forme de degré d, valant 1 modulo p^r, posons

$$F = (f + \ldots + f) + p^r(f + \ldots + f) + \ldots + p^{qr}(f + \ldots + f) \quad ,$$

où $q + 1$ est la partie entière de d/r et où, dans chaque parenthèse, f est répété $p^r - 1$ fois, et où chaque terme f a de nouvelles indéterminées.

Il est facile de voir que F n'a pas de zéro dans Z_p. Utilisant les exemples de BROWKIN, on a le théorème suivant.

THÉORÈME 6. - Soient p un nombre premier, et ε un nombre réel strictement positif ; Q_p n'est pas $C_{3-\varepsilon}$.

La technique développée ci-dessus ne peut guère donner mieux que le théorème 6, car on peut majorer le nombre des indéterminées d'une forme de Z_p, qui n'a pas de zéro primitif modulo une puissance de p, à l'aide du lemme suivant qu'on démontre facilement en considérant des vecteurs de Witt.

LEMME. - Si f est un polynôme sans terme constant de degré d de l'anneau $Z_p[X_1, \ldots, X_n]$, et si l'on a $n > (1 + p + \ldots + p^r)d$, il existe un x de Z_p, non divisible par p, tel que

$$f(x) \equiv 0 \quad (p^{r+1}) \quad .$$

On remarquera que dans les formes de Q_p sans zéro, construites plus haut, le degré est un multiple de $(p - 1)p$ si $p \geqslant 3$, et est un multiple de 4 pour $p = 2$.

On peut se demander, par exemple, si la conjecture d'Artin n'est pas vraie pour le corps Q_2 pour des polynômes de degré impair. A cet égard, je viens d'obtenir le résultat partiel suivant :

Soient $d \geqslant 1$ un entier impair, et $f \in Z_2[X_1, \ldots, X_{2d+1}]$ une forme de degré d ; il existe un x de Z_2, non divisible par 2, tel que $f(x) \equiv 0 \quad (p^2)$.

L'énoncé précédent est faux si d est un multiple de 4. Ce résultat est à comparer avec le dernier énoncé du numéro 2.

BIBLIOGRAPHIE

[1] AX (J.) and KOCHEN (S.). - Diophantine problems over local fields, I., II., Amer. J. of Math., t. 87, 1965, p. 605-628 ; III., Annals of Math., Series 2, t. 83, 1966, p. 437-456.

[2] BROWKIN (J.). - On forms over p-adic fields, Bull. Acad. polon. Sc., t. 14, 1966, p. 489-492.

[3] GREENBERG (J. M.). - Rational points in henselian discrete valuation rings. - Paris, Presses universitaires de France, 1967 (Institut des Hautes Etudes Scientifiques, Publications mathématiques, 31).

[4] KREISEL (G.) et KRIVINE (J.-L.). - Eléments de logique mathématique. - Paris, Dunod, 1967 (Monographies de la Société mathématique de France, 3).

[5] LANG (S.). - On quasi algebraic closure, Annals of Math., Series 2, t. 55, 1952, p. 373-390.

[6] NAGATA (M.). - Note on a paper of Lang concerning quasi algebraic closure, Mem. Coll. Sc. Univ. Kyoto, Series A, t. 30, 1956/57, p. 237-241.

[7] TERJANIAN (G.). - Un contre-exemple à une conjecture d'Artin, C. R. Acad. Sc. Paris, t. 262, 1966, Série A, p. 612.