

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

YVES POURCHET

Formes cubiques sur les corps locaux

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, n° 2 (1965-1966),
exp. n° 18, p. 1-9

http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A6_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1965-1966, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

FORMES CUBIQUES SUR LES CORPS LOCAUX

par Yves POURCHET

Introduction. - Dans ce qui suit, K désigne un corps local, i. e. un corps commutatif complet pour une valuation non archimédienne discrète (non triviale), \mathcal{O} est l'anneau des entiers, $\mathfrak{P} = (\pi)$ l'idéal premier, $\bar{K} = \mathcal{O}/\mathfrak{P}$ le corps résiduel ; \mathbb{F}_q est le corps fini à q éléments, et k désigne un corps commutatif.

Exemples.

1° $K = \mathbb{Q}_p$.

2° $K = k((Y))$ (corps des fractions de l'anneau $k[[Y]]$ des séries formelles sur k).

Situons le problème par l'énoncé de quelques résultats.

THÉORÈME 1. - f_1, f_2, \dots, f_r étant des polynômes sans terme constant appartenant à $\mathbb{F}_q[X_1, \dots, X_n]$, f_i étant de degré d_i , si $n > \sum_{i=1}^r d_i$, les f_i ont un zéro commun non trivial (i. e. $\neq (0, 0, \dots, 0)$) dans \mathbb{F}_q^n (CHEVALLEY).

THÉORÈME 2A. - Si $K = \mathbb{F}_q((Y))$ et si f_1, f_2, \dots, f_r sont des polynômes homogènes, de degrés d_i , appartenant à $K[X_1, \dots, X_n]$, où $n > \sum_{i=1}^r d_i^2$, les f_i ont un zéro commun non trivial dans K^n (LANG [4]).

Pour $K = \mathbb{Q}_p$ qui est un corps local ayant même corps résiduel \mathbb{F}_p que $\mathbb{F}_p((Y))$, on a seulement le résultat suivant, établi par J. AX et S. KOCHEN [1] et [7], en utilisant le théorème 2A.

THÉORÈME 2B. - Soient d_1, d_2, \dots, d_r , des entiers > 0 ; il existe un ensemble fini de nombres premiers $B(d_1, \dots, d_r)$ tel que, $\forall p$ premier $\notin B$, $\forall f_1, \dots, f_r \in \mathbb{Q}_p[X_1, \dots, X_n]$, f_i étant homogène de degré d_i et $n > \sum_{i=1}^r d_i^2$, les f_i ont un zéro commun non trivial dans \mathbb{Q}_p^n .

Toutefois, on sait (HASSE) que si K est un corps local tel que \bar{K} soit fini, tout $f \in K[X_1, X_n]$ homogène de degré 2 représente 0 (i. e. a un zéro non trivial) dans K si $n > 2^2 = 4$.

L'objet du présent exposé est de démontrer que le résultat analogue, avec $n > 3^2 = 9$, vaut pour le degré 3. Signalons que l'énoncé général relatif à un

polynôme homogène de degré $d \in K[X_1, \dots, X_n]$, avec $n > d^2$, est inexact comme vient de le montrer G. TERJANIAN, qui a construit un polynôme homogène de degré 4 appartenant à $\mathbb{Q}_2[X_1, \dots, X_{18}]$ qui ne représente pas 0 dans \mathbb{Q}_2 [8]. Par contre, il est facile de montrer que, $\forall d, \forall p$, il existe un polynôme homogène de degré d appartenant à $\mathbb{Q}_p[X_1, \dots, X_{d^2}]$ qui ne représente pas 0 sur \mathbb{Q}_p (voir e. g. [4]).

Formes cubiques. - Nous allons démontrer le théorème suivant.

THÉORÈME 3. - K étant un corps local, à corps résiduel fini, et $f \in K[X_1, \dots, X_n]$ un polynôme homogène de degré 3, si $n > 9$, f représente 0 dans K .

Ce résultat a été obtenu d'abord par DEM'JANOV [3] avec la restriction caractéristique de $\bar{K} \neq 3$, que LEWIS [5] a pu ensuite éviter avec une méthode différente. DAVENPORT [2] a donné une nouvelle démonstration et quelques résultats complémentaires dans le cas $K = \mathbb{Q}_p$. Nous suivrons ici la méthode la plus récente, utilisée par SPRINGER [6].

$f(X)$ étant un polynôme homogène de degré 3, appartenant à $k[X_1, \dots, X_n]$, nous introduirons ses polaires $g(X, Y) \in k[X_1, \dots, X_n, Y_1, \dots, Y_n]$, homogène de degré 2 par rapport à X (i. e. à l'ensemble des X_1, \dots, X_n) et de degré 1 par rapport à Y , et $h(X, Y, Z) \in k[X_1, \dots, X_n, Y_1, \dots, Y_n, Z_1, \dots, Z_n]$ de degré 1 par rapport à X , à Y , et à Z , tels que

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

$$f(X + Y + Z) = \sum f(X) + \sum (g(X, Y) + g(Y, X)) + h(X, Y, Z) .$$

Plus généralement, on a :

$$f(Z_1 X^1 + \dots + Z_m X^m)$$

$$= \sum_i Z_i^3 f(X^i) + \sum_{i \neq j} Z_i^2 Z_j g(X^i, X^j) + \sum_{i < j < k} Z_i Z_j Z_k h(X^i, X^j, X^k)$$

où l'on a posé

$$X^i = (X_{1i}, \dots, X_{ni}), \quad Z_i X^i = (Z_i X_{1i}, \dots, Z_i X_{ni}),$$

les deux membres de l'égalité étant contenus dans $k[X_{11}, \dots, X_{nm}, Z_1, \dots, Z_m]$.

Remarque. - Pour $m = 3$, substituons $X^1 = X^2 = X^3 = X$ dans l'égalité précédente.

$$\begin{aligned}
(z_1 + z_2 + z_3)^3 f(X) &= f(z_1 X + z_2 X + z_3 X) \\
&= \sum z_i^3 f(X) + \sum_{i \neq j} z_i^2 z_j g(X, X) + \sum_{i < j < k} z_i z_j z_k h(X, X, X)
\end{aligned}$$

d'où

$$3f(X) = g(X, X), \quad 6f(X) = h(X, X, X).$$

DÉFINITION. - k étant un corps commutatif et E un espace vectoriel de rang n sur k , une application F de E dans k sera dite forme cubique sur E si, pour toute base $B = \{e_1, \dots, e_n\}$ de E , il existe un polynôme homogène de degré 3, $f \in k[X_1, \dots, X_n]$, tel que $\forall x = \sum_{i=1}^n x_i e_i \in E$,

$$F(x) = f(x_1, \dots, x_n).$$

Remarque 1. - B étant donnée, f est unique, $f = F_B$ si, et seulement si, on n'a pas $k = \mathbb{F}_2$ et $n > 1$.

Remarque 2. - Il suffit que la propriété précédente ait lieu pour une base B_0 .

Démonstration du théorème 1. - Compte tenu du théorème de Chevalley, le théorème 1 résultera du lemme suivant.

LEMME 1. - Si t est un entier tel que tout polynôme homogène, de degré 3, appartenant à $\overline{K}[X_1, \dots, X_n]$, où $n > t$ représente 0, alors $s = 3t$ a la même propriété relativement à K .

Démonstration. - Soit $f \in K[X_1, \dots, X_n]$ un polynôme homogène de degré 3, qui ne représente pas 0 dans K . $\{e_i\}_{i=1}^n$ étant la base canonique de $E = K^n$, définissons F, G, H :

$$E \xrightarrow{F} K, \quad E \times E \xrightarrow{G} K, \quad E \times E \times E \xrightarrow{H} K$$

par

$$F(\sum x_i e_i) = f(x_1, \dots, x_n)$$

$$G(\sum x_i e_i, \sum y_i e_i) = g(x_1, \dots, x_n, y_1, \dots, y_n)$$

$$H(\sum x_i e_i, \sum y_i e_i, \sum z_i e_i) = h(x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n)$$

$\forall (x_1, \dots, x_n), (y_1, \dots, y_n), (z_1, \dots, z_n) \in K^n$, g et h étant les polynômes introduits précédemment.

Il est clair que F est une forme cubique, G une forme quadratique à gauche, linéaire à droite et H une forme trilinéaire symétrique.

1. Propriété normique de F .

Soient x, y indépendants, appartenant à E et

$$\phi(T) = F(x)T^3 + G(x, y)T^2 + G(y, x)T + F(y)T^3 \in K[T] ;$$

$\forall \lambda \in K$,

$$\phi(\lambda) = F(\lambda x + y) ,$$

ϕ , de degré 3 , n'a pas de zéro dans K , donc est irréductible dans $K[T]$ (cette conclusion n'est plus légitime pour un degré ≥ 4) , donc (lemme de Hensel) :

$$(1) \quad \max(|G(x, y)| , |G(y, x)|) \leq \max(|F(x)| , |F(y)|) ,$$

par suite

$$(2) \quad |\phi(1)| = |F(x + y)| \leq \max(|F(x)| , |F(y)|) .$$

Si $|F(x)| > |F(y)|$, $|F(x)| > \max(|G(x, y)| , |G(y, x)|)$, donc

$$(3) \quad |F(x)| > |F(x + y) - F(x)| .$$

En outre, $\forall \lambda \in K$, $|1 + \lambda|^3 \leq \max(1 , |\lambda|^3)$, et si $|\lambda| < 1$,

$$|(1 + \lambda)^3 - 1| < 1 ,$$

les inégalités (2) et (3) sont donc vérifiées également quand x et y sont dépendants. Elles sont donc vraies sans restriction.

Il en est de même de (1), car $G(x, x) = 3F(x)$, et

$$\max(|3\lambda| , |3\lambda^2|) \leq \max(1 , |\lambda|^3) .$$

Soient $x, y, z \in E$, on a

$$\begin{aligned} F(x + y + z) = F(x) + F(y) + F(z) + G(x, y) + G(y, x) + G(y, z) + G(z, y) \\ + G(z, x) + G(x, z) + H(x, y, z) \end{aligned}$$

d'où, compte tenu de (1),

$$(4) \quad |H(x, y, z)| \leq \max(|F(x)| , |F(y)| , |F(z)|) .$$

Remarque. - De (2), on déduit que $x \rightarrow |F(x)|^{1/3}$ est une norme ultramétrique sur E .

2.

$$\forall i \in \mathbb{Z} , \text{ soit } M_i = \{x ; x \in E , |F(x)| \leq |\pi|^i\}$$

- d'après (1), M_i est un \mathcal{D} -module,
- $M_{i+1} \subset M_i$,
- $M_{i+3} = \pi M_i$.

Si $i < j \leq i + 3$, M_i/M_j est un \mathcal{D} -module annihilé par \mathfrak{P} , donc muni canoniquement d'une structure de $\overline{K} = \mathcal{D}/\mathfrak{P}$, espace vectoriel.

Soient $E_i = M_i/M_{i+1}$, $n_i = \dim_{\overline{K}} E_i$ ($0 \leq d_i \leq \infty$), $F_i = \left(\frac{1}{\pi^i}\right)|_{M_i}$, $F_i(M_i) \subset \mathcal{D}$ et, d'après (2), $x \equiv x' \pmod{M_{i+1}} \implies F_i(x) \equiv F_i(x') \pmod{\mathfrak{P}}$, donc il existe \overline{F}_i unique telle que

$$\begin{array}{ccc} M_i & \xrightarrow{F_i} & \mathcal{D} \\ \downarrow & \searrow \overline{F}_i & \downarrow \\ E_i & \xrightarrow{\overline{F}_i} & \overline{K} \end{array}$$

soit commutatif.

Remarquons, bien que cela ne nous soit pas directement utile, que de $M_{i+3} = \pi M_i$, on tire un isomorphisme évident de (E_i, \overline{F}_i) sur (E_j, \overline{F}_j) lorsque $i \equiv j \pmod{3}$.

Nous allons démontrer que :

- (a) $\dim_{\overline{K}} M_i/M_{i+3} = \dim_{\overline{K}} E_i$.
- (b) \overline{F}_i est une forme cubique.

Le lemme en résultera car :

- (a) il est clair que $n_i + n_{i+1} + n_{i+2} = \dim_{\overline{K}} E_i/E_{i+3}$,
- (b) par construction, \overline{F}_i ne représente pas 0, donc d'après l'hypothèse $d_i \leq t$, $\forall i$, par suite $n = n_0 + n_1 + n_2 \leq 3t = s$.

Q. E. D.

(a) résulte du lemme suivant.

LEMME 2. - E étant un K -espace vectoriel de dimension finie d , et M un \mathcal{D} -module tel que $\bigcap_{n \in \mathbb{N}} \pi^n M = \{0\}$, alors M est un \mathcal{D} -module libre.

Démonstration. - Remarquons d'abord que pour la topologie d'espace vectoriel topologique séparé de E , un \mathcal{D} -module M est fermé. Soient en effet e_1, \dots, e_ν K indépendants appartenant à M , ν étant maximum pour cette propriété ($\nu \leq d$) alors

$$\bigoplus_{i=1}^{\nu} \mathcal{D}e_i \subset M \subset \bigoplus_{i=1}^{\nu} Ke_i ,$$

M est un sous-groupe ouvert, donc fermé de $\bigoplus_{i=1}^{\nu} Ke_i$, lequel est fermé dans E .

Q. E. D.

Soit $\{e_i\}_{i \in I}$; $e_i \in M$, $\forall i \in I$, tels que $\{\overline{e_i}\}_{i \in I}$ soit une base du \overline{K} -espace vectoriel $\overline{M} = M/\pi M$. Je dis que $\{e_i\}_{i \in I}$ est une \mathcal{D} -base de M .

- $\{e_i\}_{i \in I}$ est \mathcal{D} -libre, car $\sum \lambda_i e_i = 0$ et $|\lambda_{i_0}| = \max_{i \in I} |\lambda_i| > 0$ entraînent, en posant $\mu_i = \frac{\lambda_i}{\lambda_{i_0}}$,

$$\sum \overline{\mu_i} \overline{e_i} = 0 ,$$

d'où $\overline{\mu_i} = 0$, $\forall i$, contradictoirement avec $\mu_{i_0} = 1$, en particulier $\text{card } I \leq d$, I est fini.

- Les e_i \mathcal{D} -engendrent M : Soit $x \in M$; il existe des $\lambda_i^0 \in \mathcal{D}$ et $x_1 \in M$ tels que

$$x = \sum_{i \in I} \lambda_i^0 e_i + \pi x_1 ,$$

en itérant, on obtient

$$\begin{aligned} x_1 &= \sum_{i \in I} \lambda_i^1 e_i + \pi x_2 \\ &\vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \\ x_{n-1} &= \sum_{i \in I} \lambda_i^{n-1} e_i + \pi x_n \end{aligned}$$

d'où

$$x = \sum_{i \in I} \left(\sum_{k=0}^{n-1} \lambda_i^k \pi^k \right) e_i + \pi^n x_n .$$

Posons $\lambda_i = \sum_{k=0}^{\infty} \lambda_i^k \pi^k$, cette série étant convergente, car $\lambda_i^k \in \mathcal{D}$, $\forall i$, $\forall k$, I étant fini, on en déduit que $\pi^n x_n$ a une limite, quand $n \rightarrow \infty$, qui est $x - \sum \lambda_i e_i$, mais les $\pi^n M$ étant fermés décroissants, cette limite est dans

$$\bigcap_{n \in \mathbb{N}} \pi^n M = \{0\} \implies x = \sum_{i \in I} \lambda_i e_i .$$

Q. E. D.

Dans le cas présent, $x \in \bigcap_{n \in \mathbb{N}} \pi^n E_i \implies F(x) = 0$, donc $x = 0$, en outre,

$\forall x \in E$, $\exists \lambda \in K - \{0\}$ tel que $\lambda x \in E_i$, donc E_i K -engendre E , donc $\dim_{\mathbb{D}} E_i = \dim_{\mathbb{D}} E$, et comme

$$\dim_{\overline{K}} E_i / E_{i+3} = \dim_{\overline{K}} E_i / \pi E_i = \dim_{\mathbb{D}} E_i,$$

(a) est démontré.

(b) En remplaçant F par $\frac{1}{\pi^i} F$, on se ramène à démontrer que \overline{F}_0 est une forme cubique. Soient $\varepsilon_1, \dots, \varepsilon_{n_0} \in M_0$ tels que $\varepsilon_1, \dots, \varepsilon_{n_0} \in M_0/M_1 = E_0$ forment une \overline{K} -base de E_0 . Soit

$$\begin{aligned} \varphi(X_1, \dots, X_{n_0}) \\ = \sum_{i=1}^{n_0} F(\varepsilon_i) X_i^3 + \sum_{i \neq j} G(\varepsilon_i, \varepsilon_j) X_i^2 X_j + \sum_{i < j < k} H(\varepsilon_i, \varepsilon_j, \varepsilon_k) X_i X_j X_k, \end{aligned}$$

d'après les inégalités (1) et (4) du § 1, et la définition de M_0

$$\varphi \in \mathbb{D}[X_1, \dots, X_{n_0}]$$

et il est clair que, $\forall (\xi_1, \dots, \xi_{n_0}) \in \overline{K}^{n_0}$,

$$\overline{F}_0(\sum \xi_i \varepsilon_i) = \overline{\varphi}(\xi_1, \dots, \xi_{n_0}) \quad \text{où } \overline{\varphi} \in \overline{K}[X_1, \dots, X_{n_0}].$$

Le théorème 3 est donc établi.

Q. E. D.

COROLLAIRE. - Soit $f(X_1, \dots, X_n)$ un polynôme homogène de degré 3 appartenant à $\mathbb{Z}[X_1, \dots, X_n]$. Si $n > 9$, la congruence

$$f(x_1, \dots, x_n) \equiv 0 \pmod{m}, \quad \forall m \in \mathbb{Z} - \{0\}$$

possède une solution non triviale (i. e. telle que $(x_1, \dots, x_n) = 1$).

C'est vrai en effet pour $m = p^t$ primaire, d'après le théorème 3.

Avec pour K les hypothèses du théorème 1, nous avons en outre le théorème suivant.

THÉORÈME 4. - Si $f \in K[X_1, \dots, X_n]$ est un polynôme homogène de degré 3, si $n > 3$, alors f représente 0 dans l'extension non ramifiée de degré 3 de K .

Démontrons d'abord le lemme suivant.

LEMME 3. - Si $C(X_1, \dots, X_n)$ est un polynôme homogène de degré 3 appartenant à $\mathbb{F}_q[X_1, \dots, X_n]$ qui ne représente pas 0 dans \mathbb{F}_q , et si $n \geq 2$, C

a un zéro non singulier dans \mathbb{F}_q^3 .

Il suffit de le démontrer pour $n = 2$, et d'appliquer le résultat à $C(X_1, X_2, 0)$ [d'après CHEVALLEY $n = 2$ ou 3].

$C(X_1, 1)$ est un polynôme de degré 3 (car $C(1, 0) \neq 0$), appartenant à $\mathbb{F}_q[X_1]$, qui n'a pas de zéro dans \mathbb{F}_q , donc est irréductible dans $\mathbb{F}_q[X_1]$.
 $\exists \delta \in \mathbb{F}_q^3$ tel que $C(\delta, 1) = 0$ et, \mathbb{F}_q étant parfait,

$$\frac{\partial}{\partial X_1} C(\delta, 1) \neq 0.$$

Q. E. D.

Soit L l'extension cubique non ramifiée de K , et supposons que F (notation précédente) ne représente pas zéro dans $E \subset L^n$. Soit F_L la forme cubique sur L^n , définie par f , dans la base canonique; F_L prolonge F . Considérons la situation décrite dans la démonstration du théorème 3: $n_0 + n_1 + n_2 > 3$, donc $\exists i, 0 \leq i \leq 2$, tel que $n_i \geq 2$; remplaçant F par $\frac{1}{\pi^i} F$, on peut supposer $i = 0$ d'après le lemme 3, le polynôme $\bar{\varphi}(X_1, \dots, X_{n_0}) \in \bar{K}[X_1, \dots, X_{n_0}]$ a un zéro non singulier dans l'extension cubique de \bar{K} , corps résiduel de L qui se relève (HENSEL) en un zéro non trivial de φ dans L . Donc F_L représente 0 dans L^n .

Q. E. D.

Remarque. - D'après le résultat de G. TERJANIAN, on ne peut espérer appliquer le raisonnement du théorème 3 pour un degré > 3 .

Effectivement, le polynôme

$$f(X) = (X_1^2 - pX_2^2)(X_3^2 - pX_4^2)$$

ne représente pas zéro sur \mathbb{Q}_p et ne vérifie pourtant pas l'inégalité normique

$$|f(1, 0, 0, 1)| = |f(0, 1, 1, 0)| = |p|, \quad |f(1, 1, 1, 1)| = 1 > |p|.$$

BIBLIOGRAPHIE

- [1] AX (James) and KOCHEN (Simon). - Diophantine problems over local fields L , Amer. J. of Math., t. 87, 1965, p. 605-630.
- [2] DAVENPORT (H.). - Cubic forms in thirty-two variables, Phil. Trans. Royal Soc. of London, Series A, t. 251, 1958/59, p. 193-232.
- [3] DEM'JANOV (V. B.). - O kubičeskikh formakh v diskretno normirovannykh poljakh, Doklady Akad. Nauk SSSR, N. S., t. 74, 1950, p. 889-891

- [4] LANG (Serge). - On quasi algebraic closure, *Annals of Math.*, Series 2, t. 55, 1952, p. 373-390.
 - [5] LEWIS (D. J.). - Cubic homogeneous polynomials over p -adic number fields, *Annals of Math.*, Series 2, t. 56, 1952, p. 473-478.
 - [6] SPRINGER (T. A.). - Some properties of cubic forms over fields with a discrete valuation, *Koninkl. nederl. Akad. van Wet.*, Proc. Series A, t. 58, 1955, p. 512-516.
 - [7] TERJANIAN (Guy). - Equations diophantiennes p -adiques, *Séminaire Bourbaki*, 18e année, 1965/66, n° 299, 13 p.
 - [8] TERJANIAN (Guy). - Un contre-exemple à une conjecture d'Artin, *C. R. Acad. Sc. Paris*, t. 262, 1966, p. 612.
-