1. Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **04.06.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

SOMMES DE CARRÉS D'ENTIERS D'UN CORPS p-ADIQUE

par Claude MOSER

RÉSUMÉ

On se propose de présenter, dans cet article, une étude aussi complète et élémentaire que possible de l'anneau formé par les entiers d'un corps p-adique qui sont sommes de carrés d'entiers. Après avoir donné des résultats généraux sur cet anneau, on recherche pour tout $n \geqslant 1$ quels sont les entiers qui sont sommes de n carrés d'entiers, et si un entier est somme de n carrés, on cherche à le représenter comme tel.

1. INTRODUCTION

Le premier intérêt de ce travail est de constituer une étape préliminaire pour l'étude des sommes de carrés d'entiers d'un corps de nombres: on sait qu'une condition nécessaire et suffisante pour qu'un élément totalement positif a d'un corps de nombres K soit somme de n carrés dans K, est que a soit somme de n carrés dans chaque complété p-adique de K; c'est là une application directe du principe de Hasse [1], [4]. Ce principe n'est plus applicable en général lorsqu'il s'agit de représenter un entier comme somme de carrés d'entiers. Il n'en demeure pas moins qu'une condition nécessaire pour qu'un entier a d'un corps de nombres K soit somme de n carrés d'entiers de K, est évidemment que a soit somme de n carrés d'entiers dans chaque complété p-adique de K. Signalons d'ailleurs que la condition est suffisante pour $n = 4$ si le discriminant de $K/\mathbf{Q}$ est impair, cf. [5].

Le second intérêt réside dans le caractère élémentaire de la démarche utilisée: si on peut considérer, en écho aux méthodes générales de C. Riehm sur la représentation d'une forme quadratique par une autre [6], que notre problème est un cas particulier de celui de la représentation entière d'une forme du type aX^2 par une forme $X_1^2 + \ldots + X_n^2$, la recherche explicite d'une telle représentation utilise en fait les calculs que nous faisons.

On conçoit que l'essentiel des difficultés réside dans le comportement des corps dyadiques, c'est-à-dire les extensions finies de $\mathbf{Q}_2$, et que les résul

tats dépendent étroitement de la ramification et de l'extension résiduelle du corps K considéré. Mais ces facteurs ne suffisent pas: intervient aussi la propriété pour -1 d'être « plus ou moins loin » d'être un carré dans K. C'est pourquoi nous utilisons constamment la notion de défaut quadratique introduite par O. T. O'Meara [4].

Nous avons cru intéressant d'étayer les démonstrations de quelques exemples numériques simples qui permettent au lecteur de se rendre compte du caractère effectif de la méthode utilisée.

1.1. *Notations générales et rappels*

K désignera un corps p-adique, d'anneau des entiers A; on notera:

$\mathfrak{P}$	l'idéal maximal de A;
π	une uniformisante de A (choisie une fois pour toutes);
$\dot{K}$	le groupe multiplicatif de K;
$v : \dot{K} \to \mathbf{Z}$	la valuation normalisée de K;
U	le groupe des unités de A;
$\bar{K}$	le corps résiduel de K;
f	le degré résiduel $[\bar{K}:\mathbf{F}_p]$;
e	l'indice de ramification absolu de K sur $\mathbf{Q}_p$;
d	la partie entière de $e/2$;
A_2	le sous-anneau de A formé des sommes de carrés d'éléments de A;
V	le groupe des unités de A_2;
V_n	l'ensemble des unités de A_2 qui sont sommes de n carrés d'éléments de A (pour $n \geqslant 1$);
$s(A)$	la « stufe » de A, c'est-à-dire le plus petit entier n tel que $-1 \in V_n$;
$t(A)$	le plus petit entier n tel que tout élément de A_2 soit somme de n carrés d'éléments de A.

1.1.1. *Lemme de Hensel. Soit $\varphi(X)$ un polynôme à coefficients dans A. Soit $a_0 \in A$ tel que $v(\varphi(a_0))$ soit strictement supérieur à $2v(\varphi'(a_0))$. Alors la suite $\{a_n\}_{n\in\mathbf{N}}$ définie par :*

$$a_{n+1} = a_n - \varphi(a_n)(\varphi'(a_n))^{-1}$$

converge dans A vers un zéro de $\varphi(X)$. De plus si a est la limite de cette suite on a les inégalités :

$$v(a - a_0) \geqslant v(\varphi(a_0)) - 2v(\varphi'(a_0)) > 1 .$$

Pour une démonstration voir [3].

1.2. *Extensions cycliques de corps locaux*

1.2.1. *Proposition. Soit L une extension finie et cyclique d'un corps local K et soit $N_{K/L} : \dot{L} \to \dot{K}$ l'application norme. On a les égalités :*

$$(\dot{K} : N_{L/K}(\dot{L})) = [L : K],$$
$$(U(K) : N_{L/K}(U(L))) = e(L/K).$$

Pour une démonstration voir [7], ou [4] pour le cas particulier d'une extension de degré 2.

1.2.2. *Proposition. Soit p un nombre premier. Pour tout $n \geqslant 1$ il existe une extension non ramifiée (unique à isomorphisme près) de degré n de $\mathbf{Q}_p$. Cette extension peut etre décrite comme étant le corps de décomposition sur $\mathbf{Q}_p$ du polynôme $X^{p^n} - X$. Elle est cyclique.*

Pour une démonstration voir également [4] et [7].

1.3. *Le défaut quadratique (cas dyadique, $p = 2$)*

Dans tout ce paragraphe on considère des corps dyadiques, c'est-à-dire des extensions finies du corps $\mathbf{Q}_2$, complété 2-adique du corps des rationnels. La notion de défaut quadratique et les résultats qui la concernent sont dus à O'Meara (cf. [4]).

1.3.1. *Définition. Soit u une unité de A qui n'est pas un carré dans A. On appelle défaut quadratique de u, et on note $\delta(u)$, le plus grand entier n tel que la congruence*

$$u \equiv x^2 \pmod{\mathfrak{P}^n}$$

ait une solution dans A. (Si u est un carré dans A, on convient de poser $\delta(u) = +\infty$).

1.3.2. *Proposition. Soit u une unité de A.*

1. *Pour que u soit un carré dans A, il faut et il suffit que la congruence $u \equiv x^2 \pmod{4\mathfrak{P}}$ ait une solution dans A ; (autrement dit la condition $\delta(u) \geqslant 2e + 1$ équivaut à la condition $\delta(u) = +\infty$).*

2. *Si u satisfait à $\delta(u) < 2e$, alors $\delta(u)$ est un nombre impair.*

3. *L'extension quadratique $K(\sqrt{u})/K$ est non ramifiée si et seulement si on a $\delta(u) = 2e$. De plus, si deux unités ont pour défaut quadratique $2e$, leur produit est un carré.*

4. *Soit a un élément de A tel que $v(a)$ soit impair. Alors $\delta(1+a) = v(a)$.*

Remarquons d'abord que toute unité u a un défaut quadratique car du fait que $\overline{K} = \overline{K}^2$, toute congruence $u \equiv x^2 \pmod{\mathfrak{P}}$ a une solution dans A. De plus le défaut quadratique d'une unité u ne dépend que de sa classe modulo les carrés d'unités. Soit u une unité telle que $\delta(u) = m$ et soit $y \in U$. Posons $\delta(uy^2) = n$. A partir des représentations: $u = x^2 + x_1\pi^m$ et $y^2u = z^2 + z_1\pi^n$ on déduit les égalités:

$y^2u = x^2y^2 + x_1y^2\pi^m$, ce qui implique $m \leqslant n$;
$u = (zy^{-1})^2 + z_1y^{-2}\pi^n$, ce qui implique $n \leqslant m$; d'où $m = n$.

1. Soit u une unité de A telle que $\delta(u) \geqslant 2e + 1$. Quitte à multiplier u par le carré d'une unité, on peut supposer qu'on a:

$$u = 1 + 4\pi b\,, \quad \text{avec} \quad b \in A\,.$$

Dans l'anneau de séries formelles $\mathbf{Q}[[T]]$ l'élément $1 + 4T$ est le carré de l'élément:

$$(1+4T)^{1/2} = 1 + \sum_{n=1}^{\infty} \frac{1}{n!}\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)4^nT^n\,;$$

on vérifie sans peine que pour tout $n \geqslant 1$ on a:

$$\frac{1}{n!}\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)4^nT^n = (-1)^{n-1}\binom{2n}{n}T^n\,.$$

[C'est un bon exercice de montrer que le coefficient binomial $\binom{2n}{n}$ est toujours pair, et qu'il est multiple de 4 si et seulement si n n'est pas une puissance de 2]. Maintenant, dans l'espace ultramétrique complet A, la série de terme général $a_0 = 1$ et $a_n = (-1)^{n-1}\binom{2n}{n}\pi^nb^n$ $(n \geqslant 1)$ est convergente. On conclut à l'égalité:

$$(CAR.)\ 1 + 4\pi b = \{1 + \sum_{n=1}^{\infty}(-1)^{n-1}\binom{2n}{n}\pi^nb^n\}^2\,.$$

Cette formule rend « explicite » l'extraction de la racine carrée, en ce sens qu'il est possible, pour tout $n \geqslant 0$, de trouver le terme de rang n du développement de Hensel d'une racine carrée de $1 + 4\pi b$.

Réciproquement, si u est un carré d'unité, il est clair que la congruence: $u \equiv x^2 \pmod{4\,\mathfrak{P}}$ a une solution dans A.

[Pour une autre démonstration de cette assertion voir [4] pp. 160-163 à qui sont empruntées les démonstrations des assertions 2) à 4).]

2. Il suffit de montrer que si la congruence $u \equiv x^2 \pmod{\mathfrak{P}^{2a}}$ $(a<e)$ a une solution dans A, il en est de même de la congruence: $u \equiv x^2 \pmod{\mathfrak{P}^{2a+1}}$. Quitte, encore, à multiplier u par le carré d'une unité, on peut supposer qu'on a $u = 1 + y\pi^{2a}$ avec $y \in A$. Si y n'est pas une unité, il n'y a rien à démontrer. Au contraire si y est une unité, il existe une unité w et un entier $t \in A$ tels que $y = w^2 + \pi t$ et $u = 1 + w^2\pi^{2a} + t\pi^{2a+1}$, c'est-à-dire

$$u = (1+w\pi^a)^2 + t\pi^{2a+1} - 2w\pi^a \equiv (1+w\pi^a)^2 \pmod{\mathfrak{P}^{2a+1}},$$

car on a $v(t\pi^{2a+1} - 2w\pi^a) \geqslant \min\{2a+1, e+a\} \geqslant 2a+1$. On a donc $\delta(u) \geqslant 1 + 2a$.

3. Si $u = y^2 + 4z$ est une unité de A telle que $\delta(u) = 2e$, alors z est une unité et u n'est pas un carré dans A. De plus, $\frac{1}{2}(y+\sqrt{u})$ est entier sur A. Son polynôme irréductible sur A est $X^2 - yX - z$ dont le discriminant est u. C'est dire que $K(\sqrt{u})$ est une extension quadratique non ramifiée de K.

Réciproquement, soit u une unité non carrée de A telle que $K(\sqrt{u})$ soit non ramifiée sur K. Quitte à multiplier u par le carré d'une unité, ce qui ne change pas l'extension $K(\sqrt{u})$, on peut supposer qu'on a $u = 1 + \pi^a b$ avec $a = \delta(u)$ et $b \in U$. Posons $c = -1 + \sqrt{u}$ et désignons par $\hat{v} : (K(\sqrt{u})) \to \mathbf{Z}$ la valuation normalisée de $K(\sqrt{u})$. Puisque l'extension $K(\sqrt{u})/K$ est non ramifiée, $\hat{v}$ coïncide avec v sur K. Si on avait $\hat{v}(c) < e$ on aurait $a = 2\hat{v}(c) < 2e$, ce qui est impossible d'après l'assertion 2. ci-dessus. Par conséquent on a $\hat{v}(c) \geqslant e$ et $a \geqslant 2e$. Ceci implique $a = 2e$ puisque u n'est pas un carré dans A.

La dernière partie de 3. résulte de l'unicité de l'extension non ramifiée de degré 2 de K.

4. Si $a \in A$ est de valuation impaire $v(a) < 2e$, il est clair qu'on a $\delta(1+a) \geqslant v(a)$. Raisonnons par l'absurde et supposons qu'existe $b \in A$ tel que $1 + a$ soit congru à $(1+b)^2$ modulo $\mathfrak{p}^{1+v(a)}$. On aurait $v(b(b+2)) = v(a)$. L'hypothèse $v(b) \geqslant e$ implique $v(a) \geqslant 2e$ tandis que l'hypothèse $v(b) < e$ implique $v(a) = 2v(b)$. Ces deux hypothèses contredisent la définition de a. Par conséquent, on a $\delta(1+a) \leqslant v(a)$.