SUR L'EXISTENCE D'ÉLÉMENT PRIMITIF ET BASE NORMALE

Artibano Micali
and
A. Paques

RELATÓRIO TÉCNICO Nº 24/88

Abstract: In this paper we make some considerations about the validity of the Primitive Element and Normal Basis Theorems in the case of commutative rings.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC – UNICAMP
Caixa Postal 6065
13.081 – Campinas – SP
BRASIL

Dezembro – 1988

Sur l'existence d'élément primitif et base normale

Artibano Micali et Antonio Paques

1. Introdução. Le but de cette note est de faire quelques considérations sur la validité, pour des anneaux commutatifs en général, de deux théorèmes classiques de la théorie des corps commutatifs, à savoir, le théorème de l'élément primitif et celui de la base normale.

Théorème de l'élément primitif (TEP). Si K est un corps, toute extension L de K, finie et séparable, possède un élément primitif, c'est-à-dire, il existe un polynôme unitaire f dans $K[X]$ tel que $L = K[X]/(f)$.

Théorème de la base normale (TBN). Si K est un corps, toute extension galoisienne finie L de K possède une base normale, c'est-à-dire, si $G = \{\sigma_1, \ldots, \sigma_n\}$ est le groupe de Galois de L sur K, il existe un élément x de L tel que $\{\sigma_i(x) \mid 1 \leq i \leq n\}$ est une base de L sur K.

Pour des anneaux commutatifs à élément unité, ces deux théorèmes ne sont pas, en général, vrais. Pour les anneaux pour lesquels on a pu démontrer ces deux théorèmes, le TBN maintient la même version mais le TEP a été modifié, sa nouvelle versions étant la suivante:

TEP pour les anneaux. Soit K un anneau commutatif à élément unité. Toute extension séparable L de K de degré n possède un élément primitif si et seulement si $\mathrm{card}(L/\wp) \geq n$ pour tout idéal maximal $\wp$ de K.

Comme exemples d'anneaux pour lesquels on a le TEP et le TBN, citons les anneaux locaux, semi-locaux, absolument plats ainsi que les LG-anneaux. Ceux-ci figurent pour la première fois dans la littérature dans l'article de Estes et Guralnick (cf. [3]). Il s'agit d'anneaux K pour lesquels on a le *principle local-global* suivant: tout polynôme f dans $K[X_1, \ldots, X_n]$ qui représente un élément inversible dans l'anneau $K_\wp$, pour tout idéal maximal $\wp$ de K, représente aussi un élément inversible dans K. Comme exemple de tels anneaux on a ceux cités ci-dessus ainsi que les anneaux K tels que $K/\mathrm{rad}(K)$ soit absolument plat.

Le TEP pour les anneaux a été démontré pour la première fois par Janusz en 1966 das le cas des anneaux locaux (cf. [4]). Le TBN dans le cas des anneaux semi-locaux a été considéré par Chase, Harrison et Rosenberg en 1965 (cf. [1]). Le TBN pour les anneaux absolument plats a été démontré par Kreimer et Cook II (cf. [5]) et le TEP pour les anneaux semi-locaux a été démontré par Thérond (cf. [13]). Ces deux théorèmes pour les LG-anneaux sont dûs à Paques (cf. [10]).

Il est intéressant de remarquer que dans tous ces cas connus les anneaux considérés

sont tels que les deux théorèmes sont vérifiés. Ceci nous conduit, dans une certaine mesure, à la question qui suit.

Soit K un anneau commutatif à élément unité. On se demande sous quelles conditions sur K l'équivalence suivante est vraie pour des extensions galoisiennes finies A de K: (PN) il existe un élément primitif pour A si et seulement si il existe une base normale de A sur K.

Le cas des extensions quadratiques a été considéré par Small (cf. [12]) en 1974. Il démontre que si K est un anneau commutatif à élément unité dans lequel ou bien 2 est inversible ou bien 2 appartient au radical de Jacobson de K, l'équivalence (PN) est vraie pour des extensions quadratiques de K.

Cette assertion de Small est un cas particulier des résultats concernant les extensions p–cycliques de K présentés au paragraphe 2 de cette note si p est un nombre premier dans le radical de Jacobson de K et d'un théorème démontré par Childs (cf. [2]) en 1977 dans le cas où p n'est pas diviseur de zéro dans K et K contient une racine primitive p–ième de l'unité.

L'equivalence (PN) a été encore demontrée par Micali, Paques et Solecki (cf. [8]) pour des extensions cubiques d'un anneau K en supposant que 2 soit inversible dans K.

2. Les cas des extensions p–cycliques. Soient K et A deux anneaux commutatifs à élément unité, A contenant K comme sous–anneau. Si G est un groupe fini de K–automorphismes de A, on dira que A est une *extension galoisienne finie* de K de *groupe de Galois* G si les conditions suivantes sont vérifiées: (i) $A^G = \{x \mid x \in A,\ \sigma(x) = x,\ \forall\ \sigma \in G\} = K$; (ii) pour tout σ dans G, $\sigma \neq 1$, et pour tout idéal maximal $\wp$ de A, il existe un élément x dans A tal que $\sigma(x) - x$ ne soit pas dans $\wp$. On sait que si A est une extension galoisienne finie de K de groupe de Galois G, alors A est un K–module projectif de type fini et rang égal à $|G|$ (cf. [1], Lemme 4.1.). Si G est un groupe cyclique d'ordre $p > 0$ où p est un nombre premier, on dira que A est une *extension p–cyclique* ou *cyclique de degré p* de K.

Nous montrons, dans ce paragraphe, que l'équivalence (PN) est aussi vraie dans le cas des extensions p–cycliques et, tout d'abord, un résultat qui nous sera utile par la suite:

Proposition 2.1. Soient $p > 0$ un nombre entier premier et K un anneau commutatif à élément unité tel que p soit dans le radical de Jacobson $\mathrm{rad}(K)$. Si A est une extension p–cyclique de K de groupe de Galois $G = \langle\sigma\rangle$, un élément α dans A engendre une base normale de A sur K, c'est–à–dire, l'ensemble $\{\sigma^i(\alpha) \mid 0 \leq i \leq p-1\}$ est une base normale de A sur K si et seulement si $\mathrm{tr}(\alpha) = \sum_{i=0}^{p-1} \sigma^i(\alpha)$ est un élément inversible dans K.

Démonstration. Si α dans A est tel que les vecteurs $\sigma^i(\alpha)$, $(0 \leq i \leq p-1)$ forment une base de A sur K alors les vecteurs $\sigma^i(\alpha) \otimes 1$, $(0 \leq i \leq p-1)$, de $A \otimes_K (K/\wp)$ sont linéairement indépendants sur $K/\wp$ pour tout idéal maximal $\wp$ de K. Il s'ensuit que $\mathrm{tr}(\alpha)$ n'appartient à aucun idéal maximal $\wp$ de K donc il est inversible dans K.

Réciproquement, étant donné α dans A tel que $\mathrm{tr}(\alpha)$ soit inversible dans K, alors

$\mathrm{tr}(\alpha) \otimes 1 \neq 0$ dans $K/\wp$ pour tout idéal maximal $\wp$ de K. On note que pour chaque idéal maximal $\wp$ de K, $\overline{K} = K/\wp$ est un corps de caractéristique p car $p \in \mathrm{rad}(K)$ et $\overline{A} = A \otimes_K \overline{K}$ est une extension p-cyclique de $\overline{K}$ de groupe de Galois $\overline{G} = \langle \overline{\sigma} \rangle$ où $\overline{\sigma} = \sigma \otimes 1$. Comme $\overline{G}$ est cyclique d'ordre p, le Lemme 1.2 de [6] nous dit que $\overline{A}$ est un corps ou $\overline{A} = \overline{K} \times \cdots \times \overline{K}$ (p fois) et, dans ce second cas, $\overline{\sigma} : \overline{A} \to \overline{A}$ est défini par $(x_1, \ldots, x_p) \mapsto (x_p, x_1, \ldots, x_{p-1})$. Si $\overline{A}$ est un corps, il résulte du théorème 1 de [11] que $\overline{\alpha} = \alpha \otimes 1$ engendre une base normale de $\overline{A}$ sur $\overline{K}$. Supposons alors que $\overline{A} = \overline{K} \times \cdots \times \overline{K}$ (p fois). Dans ce cas, si $\overline{\alpha} = (a_1, \ldots, a_p)$, il découle de $\mathrm{tr}(\overline{\alpha}) = \mathrm{tr}(\alpha) \otimes 1 \neq 0$ que $a_1 + \cdots + a_p \neq 0$. Nous disons que les vecteurs $\overline{\sigma}^i(\overline{\alpha})$, $(0 \leq i \leq p-1)$, sont linéairement indépendants sur $\overline{K}$ donc ils forment une base de $\overline{A}$ sur $\overline{K}$. En effet, on remarque, tout d'abord, que de $x_1\overline{\alpha} + x_2\overline{\sigma}(\overline{\alpha}) + \cdots + x_p\overline{\sigma}^{p-1}(\overline{\alpha}) = 0$ avec $x_1, \ldots x_p$ dans $\overline{K}$ on a

$$M \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{où} \quad M = \begin{pmatrix} a_1 & a_p & a_{p-1} & \cdots & a_2 \\ a_2 & a_1 & a_p & \cdots & a_3 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_p & a_{p-1} & a_{p-2} & \cdots & a_1 \end{pmatrix}.$$

De plus,

$$M = \sum_{i=1}^{p} a_i M_0^{i-1}, \quad \text{où} \quad M_0 = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & \cdots\cdots & 1 & 0 \end{pmatrix},$$

donc

$$M^p = \left(\sum_{i=1}^{p} a_1\right)^p \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Ceci nous dit que M est inversible donc $x_1 = \cdots = x_p = 0$.

On conclut alors que pour tout idéal maximal $\wp$ de K, l'ensemble $\{\sigma^i(\alpha) \otimes 1 \mid \sigma^i(\alpha) \otimes 1 \in A \otimes_K (K/\wp),\ 0 \leq i \leq p-1\}$ est une base normale de $A \otimes_K (K/\wp)$ sur $K/\wp$ ce qui entraine que $\{\sigma^i(\alpha) \mid 0 \leq i \leq p-1\}$ est une base normale de A sur K.

Corollaire 2.2. Si K est un anneau commutatif à élément unité et A est une extension p-cyclique de K de groupe de Galois $G = \langle \sigma \rangle$ où $p > 0$ est un nombre entier premier appartenant au radical de Jacobson de K, alors A possède une base normale.

Démonstration. Il suffit de remarquer que, puisque A est une extension galoisienne de K, il existe un élément α dans A tel que $\mathrm{tr}(\alpha) = 1$ (cf. [1], Lemme 1.6.).

Théorème 2.3. Soient K un anneau commutatif à élément unité et A une extension p-cyclique de K de groupe de Galois $G = \langle \sigma \rangle$ où $p > 0$ est un nombre entier premier

appartenant au radical de Jacobson de K. Il existe alors des éléments α et x dans A tels que $\mathrm{tr}(\alpha) = 1$, $\sigma(x) = x + 1 - p\alpha$ et $A = K[x] = K[X]/(f)$ où $f = \prod_{i=0}^{p-1}(X - \sigma^i(x))$. De plus, l'élément $y = x^{p-1}$ engendre une base normale de A sur K.

Démonstration. En effet, comme A est une extension galoisienne de K, il existe un élément α dans A tel que $\mathrm{tr}(\alpha) = 1$ (cf. [1], Lemme 1.6.). Si l'on pose $x = \sum_{i=1}^{p-1}(p-i)\sigma^{i-1}(\alpha)$ on a $\sigma(x) = x + 1 - p\alpha$ donc $\sigma^i(x) = x + i - p\sum_{j=0}^{i-1}\sigma^j(\alpha)$ et, par suite, $\sigma^i(x) - x = i - p\sum_{j=0}^{i-1}\sigma^j(\alpha)$ est inversible dans A pour tout i tel que $1 \leq i \leq p-1$, car $p \in \mathrm{rad}(K)$. D'après la Proposition 1.1 de [7], x est un élément primitif de A sur K ou encore, $A = K[x]$. Le fait que $A = K[X]/(f)$ avec $f = \prod_{i=0}^{p-1}(X - \sigma^i(x))$ découle de ce que l'application $K[X]/(f) \to K[x]$ définie par $h(X) \bmod(f) \to h(x)$ est bien définie et est un morphisme surjectif de K-algèbres qui sont des K-modules projectifs de type fini et de même rang p. Finalement, étant donné $y = x^{p-1}$, on a $\mathrm{tr}(y) = x^{p-1} + (x+1-p\alpha)^{p-1} + \cdots + (x + p - 1 - p\sum_{j=0}^{p-2}\sigma^j(\alpha))^{p-1}$. Comme $p \in \mathrm{rad}(K)$, pour tout idéal maximal $\wp$ de K on a dans $A \otimes_K (K/\wp)$, $\mathrm{tr}(\overline{y}) = \overline{x}^{p-1} + (\overline{x}+1)^{p-1} + \cdots + (\overline{x}+(p-1))^{p-1}$ où $\overline{x} = x \otimes 1$ et $\overline{y} = y \otimes 1$. Or, de $\mathrm{tr}(\overline{y}) \in K/\wp$ on a nécessairement $\mathrm{tr}(\overline{y}) = 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} = p - 1 = -1$ où encore, $\mathrm{tr}(\overline{y}) \neq 0$ dans $K/\wp$ pour tout idéal maximal $\wp$ de K et, par suite, $\mathrm{tr}(y)$ est inversible dans K. D'après la Proposition 2.1, l'élément y engendre une base normale de A sur K.

Corollaire 2.4 (cf. [9], Théorème 1.2). Si K est un anneau commutatif à élément unité de caractéristique première $p > 0$, toute extension p-cyclique A de K de groupe de Galois $G = \langle\sigma\rangle$ est de la forme $A = K[x] = K[X]/(X^p - X - c)$ avec c dans K et $x = X \bmod(X^p - X - c)$ avec $\sigma(x) = x + 1$.

Bibliographie

[1] S. U. CHASE, D. K. HARRISON, A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, Mem. Am. Math. Soc. 52 (1965), 15-33.

[2] L. N. CHILDS, The group of unramified Kummer extensions of prime degree, Proceedings of the London Math. Soc. 35 (1977), 407-422.

[3] D. R. ESTES, E. M. GURALNICK, Module equivalences: local to global when primitive polynomials represent units, J. of Algebra 77 (1982), 138-157.

[4] G. J. JANUSZ, Separable algebras over commutative rings, Trans. Am. Math. Soc. 122 (1966), 461-479.

[5] H. F. KREIMER, P. M. COOK II, Galois theories and normal basis, J. of Algebra 43 (1976), 115-121.

[6] A. MICALI, A. PAQUES, Sur le groupe des extensions cycliques, J. of Algebra 63 (1980), 268-278.

[7] A. MICALI, A. PAQUES, A. SOLECKI, Sur le groupe des extensions cubiques, Proceedings of an International Conference on Ring Theory held in Antwerp, April 1985, Lecture Notes in Math. 1197, Springer Verlag (1986), 134-148.

[8] A. MICALI, A. PAQUES, A. SOLECKI, Extensions cubiques à base normale, J. of Algebra (à paraitre).

[9] T. NAGAHARA, A. NAKAJIMA, On cyclic extensions of commutative rings, Math. J. of Okayama Univ. 15 (1971), 81-90.

[10] A. PAQUES, On the Primitive Element and Normal Basis Theorems, Comm. in Algebra, 16 (1988), 443-455.

[11] S. PERLIS, Normal bases of cyclic fields of prime-power degree, Duke Math. J. (1942), 507-517.

[12] Ch. SMALL, Normal bases for quadratic extensions, Pacific Journal, 50 (1974), 601-611.

[13] J. D. THÉROND, Le théorème de l'élément primitif pour un anneau semi-local, J. of Algebra, 105 (1987), 29-39.

Institut de Mathématiques
Université de Nontpellier II
Place Eugène Bataillon
34.060 Nontpellier, France

IMECC
Universidade Estadual de Campinas
Caixa Postal 6065
13.081 Campinas, SP, Brasil.

RELATÓRIOS TÉCNICOS — 1988

01/88 – **A Linear Continuous Transportation Problem** – *Enrique D. Andjel, Tarcísio L. Lopes* and *José Mario Martínez*.

02/88 – **A Splitting Theorem for Complete Manifolds With Non–Negative Curvature Operator** – *Maria Helena Noronha*.

03/88 – **Mathematical Physics of the Generalized Monopole without String** – *W. A. Rodrigues Jr., M. A. Paris–Rosa, A. Maia Jr.* and *E. Recami*.

04/88 – **A Family of Quasi–Newton Methods with Direct Secant Updates of Matrix Factorizations** – *José Mário Martínez*.

05/88 – **Rotation Numbers of Differential Equations. A Framework in the Linear Case** – *Luis San Martin*.

06/88 – **A Geometrical Theory of non Topological Magnetic Monopoles** – *Marcio A. Paris–Rosa* and *Waldyr A. Rodrigues Jr.*

07/88 – **Cosmic Walls and Axially Symmetric Sigma Models** – *Patricio S. Letelier* and *Enric Verdaguer*.

08/88 – **Verificação do Nível de Enlace do Protocolo X–25** – *Célio C. Guimarães e Edmundo R. M. Madeira*.

09/88 – **A Numerically Stable Reduced–Gradient Type Algorithm for Solving Large–Scale Linearly Constrained Minimization Problems** – *Hermínio Simões Gomes* and *José Mário Martínez*.

10/88 – **On Integral Bases of Some Ring of Integers** – *Nelo D. Allan*.

11/88 – **Generating Inexact–Newton Methods Using Least Change Secant Update Procedures** – *José Mario Martínez*.

12/88 – **Polarized Partition Relations of Higher Dimension** – *Walter Alexandre Carnielli* and *Carlos Augusto Di Prisco*.

13/88 – **Teoria e Prática no Planejamento de Experimentos** – *Armando M. Infante*.

14/88 – **On Closed Twisted Curves** – *Sueli I. R. Costa*.

15/88 – **Green's Function and Isotropic Harmonic Oscillator** – *E. Capelas de Oliveira*.

16/88 – **A Hopf Bifurcation Theorem for Evolution Equations of Hyperbolic Type** – *Aloisio Freiria Neves* and *Hermano de Souza Ribeiro*.

17/88 – **Nonnegatively Curved Submanifolds in Codimension Two** – *Maria Helena Noronha*.

18/88 – **A Comment on the Twin Paradox and the Hafele–Keating Experiment** – *W. A. Rodrigues Jr.* and *E. C. Oliveira*.

19/88 – **Limiting Properties of the Empirical Probability Generating Function of Stationary Random Sequences and Processes** – *Mauro S. Marques* and *Victor Pérez-Abreu*.

20/88 – **Linearization of Bounded Holomorphic Mappings on Banach Spaces** – *Jorge Mujica*.

21/88 – **Quasi-Newton Methods for Solving Underdetermined Nonlinear Simultaneous Equations** – *José Mario Martínez*.

22/88 – **Fifth Force, Sixth Force, and all that: a Theoretical (Classical) Comment** – *Erasmo Recami* and *Vilson Tonin-Zanchin*.

23/88 – **On Primitive Element and Normal Basis for Galois p–Extensions of a Commutative Ring** – *A. Paques*.