ON PRIMITIVE ELEMENT AND NORMAL BASIS FOR GALOIS p–EXTENSIONS OF A COMMUTATIVE RING

A. Paques

RELATÓRIO TÉCNICO Nº 23/88

Abstract: In this paper we present some results about the existence of primitive element and of normal basis for Galois p–extensions of a commutative ring R with identity such that $p \in rad(R)$, where p is a prime integer and $rad(R)$ denotes the Jacobson radical of R.

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

Dezembro – 1988

ON PRIMITIVE ELEMENT AND NORMAL BASIS FOR GALOIS p-EXTENSIONS OF A COMMUTATIVE RING

A. PAQUES

IMECC - UNICAMP, Caixa Postal 6065
13.081 - Campinas, SP, Brazil

In this note we are concerned with the existence of primitive element and normal basis for Galois p-extensions of a commutative ring R with identity such that $p \in rad(R)$, where p is a prime integer and rad(R) denotes the Jacobson radical of R. We extend to Galois p-extensions the results obtained in [3] for cyclic p-extensions. We prove that every Galois p-extensions of R has a normal basis (Theorem 1). As a corollary of our Theorem 2 we get the Theorem 2.3 of [3] on primitive elements. We shall assume that all rings are commutative with identity, all modules are unitary and ring homomorphisms map identity on identity.

Let R be a commutative ring with identity and G be a finite group. An overring A of R is called a *Galois extension of* R *with Galois group* G if G is a subgroup of the group Aut(A) of the automorphisms of A and

i) $A^G = \{x \in A \mid \sigma(x) = x, \sigma \in G\} = R$,

ii) for any maximal ideal p of A and any $\sigma \in G$, $\sigma \neq 1$, there exists $x \in A$ such that $\sigma(x) - x \notin p$.

If G is a p-group for some prime integer p we say that A is a *Galois p-extension of* R.

1. NORMAL BASIS

Let R be a commutative ring with identity and A be a Galois extension of R with Galois group G. We say that A *has a normal basis over* R if there exists $\alpha \in A$ such that the set $\{\sigma(\alpha) \mid \alpha \in G\}$ is a basis of A as a free R-module. We also say, in this case, that the element $\alpha \in A$ *generates a normal basis of* A *over* R.

THEOREM 1. Let R be a commutative ring with identity and p be a prime integer such that $p \in rad(R)$. Let A be a Galois p-extension of R with Galois group G and $\alpha \in A$. Then α generates a normal basis of A over R if, and only if, $tr_{A/R}(\alpha) = \sum_{\alpha\in G} \sigma(\alpha)$ is invertible in R. Moreover, every Galois p-extension of R has a normal basis over R.

PROOF. First assume that α generates a normal basis of A over R. Then $\{\sigma(\alpha) \otimes 1 \mid \sigma \in G\}$ is a basis of $A \otimes_R R/$ over $R/_p$ and consequently $tr_{A/R}(\alpha) \not\equiv 0 (\mathrm{mod}\ p)$ for each maximal ideal p of R. Therefore $tr_{A/R}(\alpha)$ is invertible in R.

Conversely, let $\alpha \in A$ be such that $tr_{A/R}(\alpha)$ is invertible in R. So, $tr_{A/R}(\alpha) \otimes 1$ is a non-zero element in $R/_p$ for each maximal ideal p of R. Since, for each maximal ideal p of R, $\overline{A} = A \otimes_R R/_p$ is a Galois p-extension of $\overline{R} = R/_p$ with Galois group $\overline{G} = \{\overline{\sigma} = \sigma \otimes 1 \mid \sigma \in G\}$ ([1], Lemma 1.7) and $tr_{A/R}(\alpha) \otimes 1 = tr_{\overline{A}/\overline{R}}(\overline{\alpha}) \neq 0$ in $\overline{R}$, where $\overline{\alpha} = \alpha \otimes 1$, and $\overline{R}$ is a field of characteristic p (because $p \in rad(R)$) it follows from the Theorem 1 of [2] that $\bar{\alpha}$ generates a normal basis of $\bar{A}$ over $\bar{R}$. Hence α generates a normal basis of A over R. The last claim of the theorem follows now from the Lemma 1.6 of [1]. ∎

REMARK. In [2] Childs and Orzech deal with fields but their Theorem 1 is also true in the general case of Galois p-extension of a field of characteristic p, with the same proof.

2. PRIMITIVE ELEMENT

Let R be a commutative ring with identity and S be an overring of R. We say that S *has a primitive element* x if $S = R[x]$ and $x^n = a_{n-1}x^{n-1} + \dots + a_0$ for some integer $n \geq 1$ and $a_i \in R$, $0 \leq i \leq n-1$.

In general the existence of primitive element is not always valid for Galois extensions of rings. For example, consider $R = \mathbb{F}_p$ the finite field with p elements for a certain prime integer p, G a finite p-group whose order is p^n for a certain integer $n > 1$ and $A = R^{p^n} = \bigoplus_{\sigma \in G} Re_\sigma$ where the elements e_σ are non-zero pairwise orthogonal idempotents of R^{p^n} such that $\sum_{\sigma \in G} e_\sigma = 1$. By considering the action of G on A given by $\tau(\sum_{\sigma \in G} \lambda_\sigma e_\sigma) = \sum_{\sigma \in G} \lambda_\sigma e_{\tau\sigma}$ one can easily see that A is Galois p-extension of R with Galois group G. Now, suppose that A has a primitive element x. So, $x = \sum_{\sigma \in G} x_\sigma e_\sigma$ with $x_\sigma \in R$ and $\tau(x) - x$ is invertible in A for every $\tau \in G$, $\tau \neq 1$ ([4], Corollary 2.2). Thus $\sum_{\sigma \in G} (x_\sigma - x_{\tau\sigma})e_\sigma$

is invertible in A for every $\tau \in G$, $\tau \neq 1$. That implies that $x_\sigma \neq x_\tau$ for all $\sigma, \tau \in G$, $\sigma \neq \tau$ and consequently $\#(R) = p^n > p$ which is a contradiction.

Nevertheless we have the following Theorem and Corollary.

THEOREM 2. Let R be a commutative ring with identity and p be a prime integer such that $p \in \mathrm{rad}(R)$. Let A be a Galois p-extension of R with Galois group G whose order is p^n for some integer $n \geq 1$. Let $H \subset G$ be a normal subgroup of G of order p and τ be a generator of H. Let $B = A^H$ and $G/_H = \{H\sigma_1, \ldots, H\sigma_{p^{n-1}}\}$. Then,

i) A is a Galois p-extension of B with Galois group H and B is a Galois p-extension of R with Galois group $G/_H$;

ii) there exists $\alpha \in A$ such that $tr_{A/R}(\alpha) = \sum_{\rho \in G} \rho(\alpha) = 1$ and α generates a normal basis of A over R;

iii) the element $\beta = \sum_{i=1}^{p^{n-1}} \sigma_i(\alpha)$ generates a normal basis of A over B and the element $\gamma = tr_{A/B}(\alpha) = \sum_{i=0}^{p-1} \tau^i(\alpha)$ generates a normal basis of B over R;

iv) there exists $x \in A$ such that $\tau(x) = x + 1 - p\beta$ and $A = B[x] \cong B[X]/_{(f)}$ where $f = \prod_{i=0}^{p-1} (X - \tau^i(x)) \in B[X]$;

v) the element γx^{p-1} generates a normal basis of A over R.

Moreover if G is cyclic and σ is a generator of G then $\sigma(x) = x + \gamma - p\alpha$.

PROOF. i) and ii) follow from the Galois theory of commutative rings [1] and from the Theorem 1 above.

iii) It is enough to remark that $tr_{A/B}(\beta) = \sum_{i=0}^{p-1}\tau^i(\beta) = \sum_{i=0}^{p-1}\sum_{j=0}^{p^{n-1}}\tau^i\sigma_j(\alpha) = tr_{A/R}(\alpha) = 1$ and that $tr_{B/R}(\gamma) = tr_{B/R}tr_{A/B}(\alpha) = tr_{A/R}(\alpha) = 1$. Now the result follows from the Theorem 1.

iv) Let $x = \sum_{i=1}^{p-1}(p-i)\tau^{i-1}(\beta)$. Since $tr_{A/B}(\beta) = 1$ it follows that $\tau(x) = x + 1 - p\beta$. So, $\tau^i(x) = x + i - p(\sum_{j=0}^{i-1}\tau^j(\beta))$ and consequently $\tau^i(x) - x = i - p(\sum_{j=0}^{i-1}\tau^j(\beta))$ is invertible in A, for $1 \le i \le p-1$, since $p \in rad(R)$. Then, $A = B[x]$ ([4], Corollary 2.2). To prove that $A \cong B[X]/_{(f)}$ where $f = \prod_{i=0}^{p-1}(X - \tau^i(x)) \in B[X]$ it is enough to remark that A and $B[X]/_{(f)}$ are projective B-modules of same rank p and that the mapping $B[X]/_{(f)} \longrightarrow A$, $g + (f) \longmapsto g(x)$ is a surjective homomorphism of B-algebras.

v) It is enough to prove that $tr_{A/R}(\gamma x^{p-1})$ is invertible in R or, equivalently, that $tr_{A/R}(\gamma x^{p-1}) \not\equiv 0 \pmod{\mathfrak{p}}$ for each maximal ideal $\mathfrak{p}$ of R. Since $tr_{A/R}(\gamma x^{p-1}) = tr_{B/R}tr_{A/B}(\gamma x^{p-1}) = tr_{B/R}(\gamma tr_{A/B}(x^{p-1}))$ and $tr_{A/B}(x^{p-1}) \equiv -1 \pmod{\mathfrak{p}B}$ we have $tr_{A/R}(\gamma x^{p-1}) \equiv tr_{B/R}(-\gamma) \equiv -tr_{B/R}tr_{A/B}(\alpha) \equiv -tr_{A/R}(\alpha) \equiv -1 \pmod{\mathfrak{p}}$ for each maximal ideal $\mathfrak{p}$ of R and the result follows.

Finally if G is cyclic and σ is a generator of G, by considering $\tau = \sigma^{p^{n-1}}$ and $\sigma_i = \sigma^{i-1}$, $1 \le i \le p^{n-1}$, the last claim of the theorem can be readily checked by a direct computation. ∎

COROLLARY. Let R be a commutative ring with identity and p be a prime integer such that $p \in \text{rad}(R)$. Let A be a Galois p-extension of R with Galois group G whose order is p. Then A has a primitive element. In particular, if $p = 0$ in R then $A = R[X]/_{(X^p - X - c)}$ for some $c \in R$.

PROOF. Immediate.

REFERENCES.

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

[2] L. CHILDS, M. ORZECH; On modular group rings, normal bases and fixed points, Am. Math. Montly 88 (1981), 142-145.

[3] A. MICALI. A. PAQUES, Sur l'existence d'élément primitif et base normale, Bull. Soc. Math. Belgique (to appear).

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

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. Faria-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 - *Luiz San Martin.*

06/88 - A Geometrical Theory of non Topological Magnetic Monopoles - *Marcio A. Faria-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 - *Aloísio 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.*