Algebra and Discrete Mathematics RESEARCH ARTICLE
Number 3. **(2009).** pp. 20 – 26
© Journal "Algebra and Discrete Mathematics"

A variant of the primitive element theorem for separable extensions of a commutative ring

Dirceu Bagio and Antonio Paques

Communicated by guest editors

Abstract. In this article we show that any strongly separable extension of a commutative ring R can be embedded into another one having primitive element whenever every boolean localization of R modulo its Jacobson radical is von Neumann regular and locally uniform.

Dedicated to Professor Miguel Ferrero
on occasion of his 70-th anniversary

Introduction

Throughout this paper by ring we mean a commutative ring with identity element. By a connected ring we mean a ring whose unique idempotents are 0 and 1. Furthermore, $J(R)$ denotes the Jacobson radical of the ring R.

Given a ring extension $S \supseteq R$ we say that S has a *primitive element* over R if there exists $\alpha \in S$ such that $S = R[\alpha]$. As it is well known, any finite separable field extension has a primitive element. Although this assertion is not true in general, several authors has been obtained extensions of it for strongly separable extensions S of a ring R. For instance, in the case that:

— $(R, \mathfrak{m})$ is a local ring with $\left|\frac{R}{\mathfrak{m}}\right| = \infty$ [6];

This paper was partially supported by CAPES (Brazil)
2000 Mathematics Subject Classification: *13B05, 12F10.*
Key words and phrases: *primitive element, separable extension, boolean localization.*

- R is a semilocal ring with $|\frac{R}{\mathfrak{m}}| \geq rank_R S$, for every maximal ideal $\mathfrak{m}$ of R [10];
- R is a ring with many units and such that $|\frac{R}{\mathfrak{m}}| \geq rank_R S$, for every maximal ideal $\mathfrak{m}$ of R [9].

An alternative and also interesting question is to know under what conditions the following variant of the primitive element theorem holds: ($\star$) *any strongly separable extension S of a ring R can be embedded into another one having primitive element.*

The statement ($\star$) is true for connected strongly separable extensions of R in the following cases: R is local [8, Theorem 1.1], R is connected and semilocal [1, Theorem 2.1.1] and R is connected with $\frac{R}{J(R)}$ von Neumann regular and locally uniform [2, Theorem 2.1].

In this paper we show that the statement ($\star$) is valid for any ring R, provided that $\frac{R_x}{J(R_x)}$ is von Neumann regular and locally uniform, for all prime ideal x in the boolean ring $B(R)$ of all idempotents of R.

1. Preliminaries

In this paper we will be employing freely the ideas and results of [12] on boolean spectrum and boolean localization of a ring (see also [7]). We begin by recalling the terminology we will need.

For any ring R let $B(R)$ denote the boolean ring of all idempotents of R and $Spec(B(R))$ the boolean spectrum of R consisting of all prime (equivalently maximal) ideals of $B(R)$ (see [12, 2.1 and 2.2]). A base for a topology on $Spec(B(R))$ is given by the family of basic open sets $\{U_e | e \in B(R)\}$, where $U_e = \{x \in Spec(B(R)) | 1 - e \in x\}$. This base defines a compact, totally disconnected, Hausdorff topology on $Spec(B(R))$.

By localization of R at x, for each $x \in Spec(B(R))$, we mean the quotient ring $R_x = \frac{R}{I(x)}$ where $I(x)$ denotes the ideal of R generated by the elements of x. By [12, 2.13] R_x is a connected ring. For any R-module M, we set $M_x = M \otimes_R R_x = \frac{M}{I(x)M}$. For any element $a \in M$, a_x denotes the image of a in M_x. For every R-module homomorphism $f : M \to N$, the corresponding induced R_x-homomorphism $f_x : M_x \to N_x$ is given by $f_x = f \otimes R_x$.

Following [4] a ring R is called *uniform* if for each $x \in Spec(B(R))$ there exists a collection of isomorphisms (of rings) $\{\phi_y : R_y \to R_x | y \in Spec(B(R))\}$ such that if F is a finite subset of R there exists a neighborhood V of x with $\phi_y(a_y) = a_x$ for all $a \in F$ and $y \in V$.

The notion of uniform rings was generalized in [2]. A ring R is called *locally uniform* if for each $x \in Spec(B(R))$ and each finite subset F of

R there exist a neighborhood $U = U(x, F)$ of x and a collection of ring isomorphisms $\{\phi_y : R_y \to R_x | y \in U\}$ such that $\phi_y(a_y) = a_x$, for every $a \in F$ and $y \in U$. Consequently, if R is locally uniform then there exist an idempotent $e = e(x, F) \in R$ and a collection of ring isomorphisms $\{\phi_y : R_y \to R_x | y \in U_e\}$ such that $x \in U_e$ and $\phi_y(a_y) = a_x$, for every $a \in F$ and $y \in U_e$.

A ring R is called *von Neumann regular* if for every element a in R there exists an element b in R such that $a = a^2 b$, which is equivalent to say that each element in R is a product of an idempotent by a unit. In particular, von Neumann regular connected rings are fields.

Examples of connected rings such that every boolean localization modulo its Jacobson radical is von Neumann regular and locally uniform can be seen in [2]. In the sequel we present a ring with the above conditions that is not connected.

Example. Let S be a connected ring and $R = \prod_{n \geq 0} S_n$, where $S_n = S$ for all $n \geq 0$. Observe that the elements in $B(R)$ are all of the type $(a_n)_{n \in \mathbb{N}}$ with $a_n = 0$ or 1. By [12, 2.2] one can easily see that $Spec(B(R)) = \{x_i | i \in \mathbb{N}\}$, where x_i denotes the set of all elements $(a_n)_{n \in \mathbb{N}} \in B(R)$ such that $a_i = 0$ and for every $j \neq i$ there exists an element in x_i whose j^{th}-coordinate is equal to 1. Consequently, $R_x \simeq S$ for all $x \in Spec(B(R))$, and in order to get the required it is enough to take S such that $S/J(S)$ is von Neumann regular and locally uniform.

2. Main result

A ring extension $S \supset R$ is called *separable* if the multiplication map $m_S : S \otimes_R S \to S$ is a splitting epimorphism of S-bimodules, which is equivalent to say that there exists an element $x \in S \otimes_R S$ which is S-central (i.e., $xs = sx$ for all $s \in S$) and satisfies the condition $m_S(x) = 1_S$. Also, we say that S is a *strongly separable extension* of R if S is a separable extension of R and S is a finitely generated projective R-module.

A polynomial $f(X) \in R[X]$ is said to be *separable* over R if it is monic and $\frac{R[X]}{(f(X))}$ is a separable R-algebra. A monic polynomial $f(X) \in R[X]$ is defined to be *indecomposable* in $R[X]$ if whenever there exist monic polynomials $g(X), h(X) \in R[X]$ such that $f(X) = g(X)h(X)$ it follows that $g(X) = 1$ or $h(X) = 1$.

The purpose of this article is to prove the next theorem and its proof will be divided in two parts: the connected and the general case.

Theorem 2.1. *Let R be a ring such that $\frac{R_x}{J(R_x)}$ is von Neumann regular and locally uniform, for every $x \in Spec(B(R))$, and S a strongly separable* *extension of R. Then, there exist a strongly separable extension T of R and an element α in T such that $T = R[\alpha]$ and $S \subseteq T$. If, in addition, T has constant rank over R, then there exists a separable polynomial $f(X) \in R[X]$ of degree $rank_R T$ such that $f(\alpha) = 0$ and $T \simeq \frac{R[X]}{(f(X))}$.*

Connected case

Theorem 2.2. *Let R be a connected ring such that $\frac{R}{J(R)}$ is von Neumann regular and locally uniform, and S a strongly separable extension of R. Then, there exist a strongly separable extension T of R, an element α in T and a separable polynomial $f(X) \in R[X]$ such that:*

(i) $S \subseteq T$;

(ii) $f(\alpha) = 0$ and $T = R[\alpha] \simeq \frac{R[X]}{(f(X))}$;

(iii) $B(S) = B(T)$.

Proof. This proof is quite similar to that of [2, Theorem 2.1]. Let $R' = \frac{R}{J(R)}$ and $S' = \frac{S}{J(S)}$. Note that R'_x is a connected and von Neumann regular ring, so it follows that R'_x is a field, for all $x \in Spec(B(R'))$.

Firstly assume that R'_x is infinite, for every $x \in Spec(B(R'))$. Thus each S'_x has a primitive element over R'_x [6, Lemma 3.1] and, consequently, there exist $\alpha'(x) \in S'$ and an idempotent $e(x) \in R'$ such that $x \in U_{e(x)}$ and $S'e(x) = R'[\alpha'(x)]e(x)$ [12, 2.8 and 2.11]. By compactness arguments we obtain elements $\alpha'_1, \dots, \alpha'_n \in S'$ and orthogonal idempotents $e_1, \dots, e_n \in R'$ such that $\sum_{1 \le i \le n} e_i = 1$ and $S'e_i = R'[\alpha'_i]e_i$. Taking $\alpha' = \sum_{1 \le i \le n} \alpha'_i e_i$ we have $S' = R'[\alpha']$ and by Nakayama's lemma $S = R[\alpha]$ for some $\alpha \in S$ such that $\alpha' = \alpha + J(S)$. Finally, (iii) is obvious and (ii) follows from [6, Theorem 2.9].

Now put $Y = \{x \in Spec(B(R')) | R'_x \text{ is finite}\}$ and assume that $Y \neq \emptyset$. By [11, Proposition 1.3] we can assume that $S = S_1 \oplus \cdots \oplus S_n$, with S_i a connected and strongly separable extension of R. Moreover, by [6, Theorem 1.1] we may also assume that each S_i is a connected Galois extension of R in the sense of [3].

On the other hand, it follows from the proof of [2, Theorem 2.1] that for each $1 \le i \le n$ there exists a connected and strongly separable extension T_i of R such that $S_i \subseteq T_i$ and $rank_{S_i} T_i = p_i$, for some prime integer p_i satisfying $\frac{q^{p_i} - q}{p_i} \ge rank_R S_i$, where $q = min\{|R'_x| | x \in Y\}$.

Taking $T = T_1 \oplus \cdots \oplus T_n$ we have that T is a strongly separable extension of R, $S \subseteq T$, $B(S) = B(T)$. It remains to show that T also satisfies (ii).

Put $T' = \frac{T}{J(R)T} = \frac{T}{J(T)}$. By boolean localization and Nakayama's lemma it is enough to prove that T'_x has a primitive element over R'_x, for every $x \in Spec(B(R'))$. If $x \notin Y$ then T'_x is an extension of R'_x with primitive element [6, Lemma 3.1].

If $x \in Y$, then R'_x is a finite field and $R'_x = R'/I(x)$ with $I(x) = \mathfrak{m}/J(R)$ for some maximal ideal $\mathfrak{m}$ of R. Again as in the proof of [2, Theorem 2.1] (see Claim 3), we have $\frac{T_i}{\mathfrak{m}T_i} \simeq \frac{R/\mathfrak{m}[X]}{(f_i(X))}$, where each $f_i(X) \in R/\mathfrak{m}[X]$ is separable over $R/\mathfrak{m}$, of degree $p_i(rank_R S_i)$ and every indecomposable factor of $f_i(X)$ in $R/\mathfrak{m}[X]$ has the same degree $p_i d_i$ with d_i a divisor of $rank_R S_i$.

Furthermore, each p_i can be chose such that $p_i d_i \neq p_j d_j$ if $i \neq j$. Therefore, the polynomials $f_i(X)$ are pairwise coprimes and $\frac{T}{\mathfrak{m}T} \simeq \frac{T_1}{\mathfrak{m}T_1} \oplus \cdots \oplus \frac{T_n}{\mathfrak{m}T_n} \simeq \frac{R/\mathfrak{m}[X]}{(f(X))}$, with $f(X) = \prod_{1 \leq i \leq n} f_i(X)$. Since $T'_x = T'/I(x)T' = \frac{T/J(T)}{\mathfrak{m}T/J(T)} \simeq T/\mathfrak{m}T$, the proof is complete. □

The following example illustrates the type of construction considered in the proof of Theorem 2.2.

Example 2.3. Let $R = \mathbb{Z}_{(2)}$ be the localization of $\mathbb{Z}$ at $2\mathbb{Z}$ and $S = R \oplus R \oplus R$. Clearly, S is a strongly separable extension of R and S does not have a primitive element over R. Take $\mathfrak{m} = 2R$, $h_1(X), h_2(X), h_3(X) \in R/\mathfrak{m}[X]$ separable and indecomposable polynomials with degrees $2, 3$ and 5 respectively, and $f_i(X) \in R[X]$ monic polynomials such that $h_i(X) = f_i(X)$ modulo $\mathfrak{m}[X]$, $1 \leq i \leq 3$. Taking $T_i = \frac{R[X]}{(f_i(X))}$ and $T = T_1 \oplus T_2 \oplus T_3$ then $\frac{T}{\mathfrak{m}T} \simeq \frac{R/\mathfrak{m}[X]}{(h(X))}$ with $h(X) = h_1(X)h_2(X)h_3(X)$. Therefore, $S \subseteq T$ and T is a strongly separable extension of R with primitive element, by Nakayama's lemma.

General case

It is easy to check that a strongly separable extension $S \supseteq R$ has a primitive element if and only if $S_x \supseteq R_x$ has a primitive element for all $x \in Spec(B(R))$. A similar result is valid when we consider the variant $(\star)$ of the primitive element theorem.

Lemma 2.4. *Let R be a ring. Then the following statements are equivalent:*

(i) $(\star)$ is true for R.

(ii) $(\star)$ is true for R_x, for all $x \in Spec(B(R))$.

Proof. (i)⇒(ii) Let $x \in Spec(B(R))$ and L be a strongly separable extension of R_x. By [7, II.24] there exists a strongly separable extension T of

R such that $T_x = L$. Thus T is contained in a strongly separable extension T' of R having a primitive element, by assumption. Consequently T'_x is a strongly separable extension of R_x having a primitive element and $L \subseteq T'_x$.

(ii)⇒(i) Let S be a strongly separable extension of R and assume that for each $x \in Spec(B(R))$ there exists a strongly separable extension $L_{(x)}$ of R_x, having a primitive element over R_x, such that $S_x \subseteq L_{(x)}$. Then, there exist a strongly separable extension $T_{(x)}$ of R and an element $\alpha_{(x)} \in T_{(x)}$ such that $(T_{(x)})_x = L_{(x)} = (R[\alpha_{(x)}])_x$ [7, II.24]. Consequently, there exists an idempotent $e(x) \in R$ such that $x \in U_{e(x)}$ and $T_{(x)}e(x) = R[\alpha_{(x)}]e(x)$ [12, 2.11].

By compactness arguments we get pairwise orthogonal idempotents $e_1, \dots, e_n$ of R, strongly separable extensions $T_1, \dots, T_n$ of R and elements $\alpha_i \in T_i$ such that $\sum_{1 \le i \le n} e_i = 1$ and $T_i e_i = R[\alpha_i]e_i$, $1 \le i \le n$. Taking $T = T_1e_1 \oplus \cdots \oplus T_ne_n$ and $\alpha = \alpha_1e_1 + \cdots + \alpha_ne_n$ we have that T is a strongly separable extension of R and $T = R[\alpha]$.

It remains to prove that $S \subseteq T$. Take $s \in S$ and $x \in Spec(B(R))$. By construction $S_x \subseteq T_x$, so there exists $t \in T$ such that $s_x = t_x$ and consequently $s - t \in I(x)T \subseteq T$. □

Corollary 2.5. *Let R be a ring. If $\frac{R_x}{J(R_x)}$ is von Neumann regular and locally uniform for any $x \in Spec(B(R))$, then $(\star)$ is true for R.*

Proof. It follows from Theorem 2.2 and Lemma 2.4. □

Corollary 2.6. *If the prime spectrum $Spec(R)$ of a ring R is totally disconnected then $(\star)$ is true for R.*

Proof. Indeed, in this case R_x is semilocal for all $x \in Spec(B(R))$ [5]. Then the result follows by Corollary 2.5. □

Now we are able to prove Theorem 2.1.

Proof of Theorem 2.1. The first assertion follows by Corollary 2.5. For the second assume that $T = R[\alpha]$ has constant rank n over R. Then $T_x = (R[\alpha])_x = R_x[\alpha_x]$ and by [6, Theorem 2.9] there exists a monic polynomial $f_{(x)}(X)$ in $R[X]$ of degree n, such that $(f_{(x)}(X))_x$ is separable over R_x and $(f_{(x)}(\alpha))_x = 0$ for each $x \in Spec(B(R))$.

The separability of $(f_{(x)}(X))_x$ implies that $(\lambda_{(x)}d(f_{(x)}(X)))_x = 1_x$ for some $\lambda_{(x)} \in R$, where $d(f_{(x)}(X))$ denotes the discriminant of $f_{(x)}(X)$. By [12, 2.9] there exists an idempotent $e(x) \in R$ such that $x \in U_{e(x)}$, $f_{(x)}(\alpha)e(x) = 0$ and $(\lambda_{(x)}d(f_{(x)}(X)))e(x) = e(x)$, which means that $f_{(x)}(X)e(x)$ is separable over $Re(x)$.

By compactness arguments we get orthogonal idempotents $e_1, \ldots, e_m$ of R and monic polynomials $f_1(X), \ldots, f_m(X) \in R[X]$ of degree n such that $\sum_{1\leq i\leq m} e_i = 1$, $f_i(X)e_i$ is separable over Re_i and $f_i(\alpha)e_i = 0$. Put $f(X) = \sum_{1\leq i\leq m} f_i(X)e_i$. Thus, $f(X)$ is a polynomial of degree n, separable over R and $f(\alpha) = 0$.

Finally the canonical map $\varphi : R[X] \to R[\alpha]$, $h(X) \mapsto h(\alpha)$, is an epimorphism of R-algebras whose kernel contains $f(X)$. Hence, it induces an epimorphism from $R[X]/(f(x))$ onto $R[\alpha]$. Since $rank_R R[\alpha] = n = rank_R(R[X]/(f(X)))$ it follows that φ is an isomorphism. □

References

[1] D. Bagio, I. Dias and A. Paques, *On self-dual normal bases*, Indag. Math. 17 (2006), 1-11.

[2] D. Bagio and A. Paques, *A generalized primitive element theorem*, Math. J. Okayama Univ. 49 (2007), 171-181.

[3] S.U. Chase, D.K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. **52** (1968), 1-19.

[4] F. DeMeyer, *Separable polynomials over a commutative ring*, Rocky Mountain J. of Math. 2 (1972), 299-310.

[5] F. DeMeyer, *On separable polynomials over a commutative ring*, Pacific J. Math. 51 (1974), 57-66.

[6] G. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. 122 (1966) 461-479.

[7] A.R. Magid, *The Separable Galois Theory of Commutative Rings*, Marcel Dekker, NY, 1974.

[8] T. McKenzie, *The separable closure of a local ring*, J. of Algebra 207 (1998), 657-663.

[9] A. Paques, *On the primitive element and normal basis theorems*, Comm. in Algebra 16 (1988), 443-455.

[10] J-D. Therond, *Le théorème de l'élément primitif pour un anneau semilocal*, J. of Algebra 105 (1987), 29-39.

[11] O.E Villamayor and D. Zelinsky, *Galois theory with finitely many idempotents*, Nagoya Math. J. 27 (1966), 721-731.

[12] ______, *Galois theory with infinitely many idempotents*, Nagoya Math. J. 35 (1969), 83-98.

Contact information

D. Bagio

Departamento de Matemática
Universidade Federal de Santa Maria
97105-900, Santa Maria, RS, Brazil
E-Mail: bagio@smail.ufsm.br

A. Paques

Instituto de Matemática
Universidade Federal do Rio Grande do Sul
91509-900, Porto Alegre, RS, Brazil
E-Mail: `paques@mat.ufrgs.br`

Received by the editors: 12.08.2009
and in final form 25.09.2009.