Math. J. Okayama Univ. **49** (2007), 171–181

A GENERALIZED PRIMITIVE ELEMENT THEOREM

Dirceu BAGIO and Antonio PAQUES

Abstract. We deal with the following variant of the primitive element theorem: any commutative strongly separable extension of a commutative ring can be embedded in another one having primitive element. This statement holds for connected strongly separable extension of commutative rings which are either local or connected semilocal. We show that it holds for a more general family of rings, that is, for connected commutative rings whose quotient ring by the corresponding Jacobson radical is von Neumann regular and locally uniform. Some properties of the (connected) separable closure of such rings are also given as an application of this result.

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.

Let $S \supseteq R$ be a ring extension. We say that S has a *primitive element* over R if there exists $\alpha \in S$ such that $S = R[\alpha]$. The existence of primitive elements for strongly separable extensions has been extensively studied by several authors (see, for instance, [1, 9, 10, 11, 12, 20, 22]). It holds for fields and, more generally, for rings with many units [15] under certain restrictive conditions on the cardinality of their residue fields (see [20]). For instance, any strongly separable extension S of a semilocal ring R, with constant rank over R, has a primitive element over R if and only if $|R/\mathfrak{m}| \geq rank_R S$, for every maximal ideal $\mathfrak{m}$ of R.

Our aim in this paper is concerned with a variant of the primitive element theorem. Indeed, we are interested in the following question: the assertion

($\star$) *every strongly separable extension S of a ring R can be embedded into another one having primitive element*

holds without any restriction on the cardinality of the residue fields of R? This question has been affirmatively answered for connected strongly separable extension of R in the case that R is either local [18] or connected semilocal [2].

We prove in Section 2 that the assertion ($\star$) is also true in a more general situation, that is, for connected strongly separable extensions of a connected

Mathematics Subject Classification. Primary 13B-05; Secondary 12F-10.

Key words and phrases. primitive element, von Neumann regular ring; locally uniform ring; strongly separable extension; separable closure.

ring R whose quotient ring by its Jacobson radical is von Neumann regular and locally uniform. As an application of this main result we present in Section 3 some interesting properties of the (connected) separable closure of such a ring. The notion of locally uniform ring, which we introduce in Section 1, is a slight extension of the notion of uniform ring as considered in [4].

1. Preliminaires

In all of this paper we will be employing freely the ideas and results of [23] on boolean spectrum and boolean localization of a ring (see also [14, 21]). We begin by introducing the terminology we will need.

For any ring R let $B(R)$ denotes the boolean ring of all idempotents of R and $Spec(B(R))$ denotes the boolean spectrum of R consisting of all prime (equivalently maximal) ideals of $B(R)$. 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 $R_x = R/I(x)$ where $I(x)$ denotes the ideal of R generated by the elements of x. By [23, 2.13] R_x is a connected ring. For any R-module M, $M_x = M \otimes_R R_x = M/I(x)M$. 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 $f_x = f \otimes R_x$.

We say that a ring R is *locally uniform* if for each $x \in Spec(B(R))$ and each finite subset F of R there exist an idempotent $e = e(x, F) \in R$ and a collection of ring isomorphisms $\phi_y : R_y \to R_x$ such that $x \in U_e$ and $\phi_y(a_y) = a_x$, for every $a \in F$ and $y \in U_e$. Uniform rings as introduced in [4] are locally uniform but the converse is not true as it will be shown in the following first example. We denote by $J(R)$ the Jacobson radical of the ring R.

Example 1.1 Let R be a semilocal ring with at least two maximal ideals such that the corresponding residue fields are not isomorphic. Put $R' = R/J(R)$. Note that $Spec(B(R'))$ is finite. Thus, in order to verify that R' is locally uniform, given any $x \in Spec(B(R'))$ and any finite subset F of R' it is enough to take $e = e(x, F) \in B(R')$ such that $U_e = \{x\}$ and the identity isomorphism $id_x : R'_x \to R'_x$. On the other hand R'_x is a field. So, $I(x) = \mathfrak{m}/J(R)$ for some maximal ideal $\mathfrak{m}$ of R and $R'_x \simeq R/\mathfrak{m}$. Therefore, it follows from the assumption on the maximal ideals of R that R' is not uniform.

We observe that the semilocal ring given in Example 1.1 is a particular example of rings R such that $R/J(R)$ is von Neumann regular and locally uniform. In the following example we give a way to construct (connected) rings with this same property and with infinitely many maximal ideals.

Example 1.2 Let $p \in \mathbb{Z}$ be a prime integer and $R_0 = \mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at $p\mathbb{Z}$. Following Hasse [8] there exists a quadratic extension K_1 of the rational number field $K_0 = \mathbb{Q}$ such that $pR_1 = \mathfrak{q}_1\mathfrak{q}_2$, where R_1 denotes the integral closure of R_0 in K_1 and $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are the unique maximal ideals of R_1 over $\mathfrak{q}_0 = p\mathbb{Z}_{(p)}$. Again by the same result due to Hasse there exists a quadratic extension K_2 of K_1 such that $\mathfrak{q}_iR_2 = \mathfrak{q}_{i1}\mathfrak{q}_{i2}$ where R_2 denotes the integral closure of R_1 in K_2 and $\mathfrak{q}_{i1}$ and $\mathfrak{q}_{i2}$ are the unique maximal ideals of R_2 over $\mathfrak{q}_i$, $i = 1, 2$. Applying this same argument successively we will get a tower of rings $R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R$, where $R = \bigcup_{j\geq 0} R_j$ is the integral closure of R_0 in $K = \bigcup_{j\geq 0} K_j$.

From the construction of R it is easy to see that: (i) R has infinitely many maximal ideals and all of them are over $\mathfrak{q}_0$; (ii) R/pR is a ring of Krull dimension zero and (iii) $R/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ for every prime ideal $\mathfrak{p}$ of R.

It is a consequence of the assertions (i) and (ii) that $R' = R/J(R) \simeq (R/pR)/(J(R)/pR) = (R/pR)/J(R/pR)$ is von Neumann regular by [7, Lemma 1]. And it follows from assertion (iii) that $R'_z \simeq \mathbb{Z}/p\mathbb{Z}$ for all $z \in Spec(B(R'))$. Put $R'_z = \{0_z, 1_z, \ldots, (p-1)_z\}$.

Now take $x \in Spec(B(R'))$ and $F = \{a_1, \ldots, a_n\}$ a finite set of elements of R'. Assume that $(a_j)_x = (i_j)_x$, with $0 \leq i_j \leq p-1$ and $1 \leq j \leq n$. Thus, for each j there is an idempotent $e_j \in R'$ such that $x \in U_{e_j}$ and $(a_j)_y = (i_j)_y$ for every $y \in U_{e_j}$ [23, 2.9]. Let $U_e = \bigcap_{1\leq j\leq n} U_{e_j}$, with $e = \prod_{1\leq j\leq n} e_j$, and $\phi_y : R'_y \to R'_x$ be such that $\phi_y(i_y) = i_x$, for every $y \in U_e$. Clearly ϕ_y is a ring isomorphism and $\phi_y((a_j)_y) = \phi_y((i_j)_y) = (i_j)_x = (a_j)_x$, for all $y \in U_e$ and $1 \leq j \leq n$. Therefore R' is locally uniform.

2. The main theorem

Let $R \subseteq S$ be a ring extension. We say that S is a *strongly separable extension* of R if S is separable as R-algebra and finitely generated and projective as R-module. If for any finite subset $N \subseteq S$ there exists a subalgebra L of S which contains N and is a strongly separable extension of R, we say that S is a *locally strongly separable extension* of R. We say that a connected ring is *separably closed* if its unique connected strongly separable extension is itself. We will denote by $\Omega(R)$, up to isomorphism, the (connected) separable closure of a connected ring R, that is, $\Omega(R)$ is a locally strongly separable extension of R which is connected and separably closed.

For more about the (connected) separable closure of a connected ring we refer to [9, 14].

Theorem 2.1 below provides a generalization of the primitive element theorem and it was already stated for local rings [18] and for connected semilocal rings [2]. In this paper we extend it to the setting of the connected rings R such that $R/J(R)$ is von Neumann regular and locally uniform.

A polynomial $f(X) \in R[X]$ is said to be *separable* over R if it is monic and $R[X]/(f(X))$ 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 $h(X) = 1$.

Theorem 2.1 *Let R be a connected ring and $S \subseteq \Omega(R)$ be a strongly separable extension of R. Assume that $R/J(R)$ is von Neumann regular and locally uniform. Then there exist a polynomial $f(X) \in R[X]$ and $\alpha \in \Omega(R)$ such that:*

(i) *$f(X)$ is separable and indecomposable,*

(ii) *$f(\alpha) = 0$ and $R[\alpha] \simeq R[X]/(f(X))$.*

(iii) *$S \subseteq R[\alpha]$.*

Proof. Let $R' = R/J(R)$, $S' = S/J(S)$. Note that R'_x is a field for every $x \in Spec(B(R'))$. Let $Y = \{x \in Spec(B(R')) \,|\, |R'_x| < \infty\}$. The proof will be divided in two parts.

Firstly assume that $Y = \emptyset$. Then S'_x has primitive element over R'_x for all $x \in Spec(B(R'))$ [9, Lemma 3.1]. Let $\alpha'(x) \in S'$ be such that $S'_x = R'_x[\alpha'(x)_x] = R'[\alpha'(x)]_x$. So, for each $x \in Spec(B(R'))$ there exists an idempotent $e(x) \in R'$ such that $x \in U_{e(x)}$ and $S'e(x) = R'[\alpha'(x)]e(x)$ [23, 2.8 and 2.11]. Applying compactness arguments we obtain elements $\alpha'_1, \ldots, \alpha'_r \in S'$ and orthogonal idempotents $e_1, \ldots, e_r \in R'$ such that $\sum_{1 \leq i \leq r} e_i = 1$ and $S'e_i = R'[\alpha'_i]e_i$. Then for $\alpha' = \sum_{1 \leq i \leq r} \alpha'_i e_i$ we have $S' = R'[\alpha']$ and by Nakayama's lemma $S = R[\alpha]$ with $\alpha \in S$ such that $\alpha' = \alpha + J(S)$. Finally by [16, Theorem 3.3] there exists a separable and indecomposable polynomial $f(X) \in R[X]$ such that $f(\alpha) = 0$ and $S \simeq R[X]/(f(X))$.

Now consider $Y \neq \emptyset$. Note that S is free as R-module [6, Theorem 2.10] of constant rank n say. Let $p \in \mathbb{Z}$ be a prime integer not divisor of n. From now on we will proceed by steps.

Claim 1. *For each $x \in Spec(B(R'))$ there exist an idempotent $e(x)$ in R' and a monic polynomial $g(X) \in R'[X]$ of degree p such that:*

(i) *$g(X)_z$ is separable over R'_z for all $z \in U_{e(x)}$,*

(ii) $g(X)_z$ *is separable and indecomposable in* $R'_z[X]$ *for all* $z \in U_{e(x)}$, *whenever* $x \in Y$,

(iii) $U_{e(x)} \bigcap U_{e(y)} = \emptyset$ *whenever* $x \notin Y$ *and* $y \in Y$.

Clearly there exists a separable polynomial of degree p in $R'_x[X]$ for every $x \in Spec(B(R'))$. And we may assume that it is also indecomposable if $x \in Y$ because, in this case, R'_x is a finite field.

Take $g(X) = a_0 + a_1X + \cdots + a_{p-1}X^{p-1} + X^p \in R'[X]$ such that $g(X)_x \in R'_x[X]$ is such a polynomial. Consequently the discriminant $d(g(X)_x) = d(g(X))_x$ of $g(X)_x$ is a unit in R'_x. So, $(d(g(X))\lambda)_x = 1_x$ for some $\lambda \in R'$. By [23, 2.9] there exists an idempotent $e_1 \in R'$ such that $x \in U_{e_1}$ and $(d(g(X))\lambda)e_1 = e_1$.

On the other hand, there exist by assumption an idempotent $e_2 \in R'$ and rings isomorphisms $\phi_z : R'_z \to R'_x$ such that $x \in U_{e_2}$ and $\phi_z((a_j)_z) = (a_j)_x$ for all $z \in U_{e_2}$ and $0 \leq j \leq p-1$.

It is enough to take $U_{e(x)} = U_{e_1} \bigcap U_{e_2}$ with $e(x) = e_1e_2$.

Claim 2. *There exists a monic polynomial* $t(X) \in R[X]$ *of degree* p, *which is separable over* R *and indecomposable in* $S[X]$.

By Claim 1 and the usual compactness argument we can insure that there are pairwise orthogonal idempotents $e_1 = e(x_1), \ldots, e_r = e(x_r)$ in R' and monic polynomials of degree p $g_1(X), \ldots, g_r(X)$ in $R'[X]$ such that $\sum_{1 \leq i \leq r} e_i = 1$ and $e_ig_i(X)$ is separable over e_iR' for all $1 \leq i \leq r$. And, in addition, $e_ig_i(X)$ is indecomposable over e_iR' for those i such that $x_i \in Y$.

Let $g(X) = \sum_{1 \leq i \leq r} e_ig_i(X)$ and $t(X) \in R[X]$ be monic and such that $g(X) = t(X)$ modulo $J(R)[X]$. By construction $t(X)$ is of degree p and separable over R.

In order to verify that $t(X)$ is indecomposable in $S[X]$ take $y \in Y$. Note that $g(X)_y = g_i(X)_y$ is indecomposable in $R'_y[X]$ for some i such that $y \in U_{e_i}$. Furthermore, $R'_y = R'/I(y)$ is a field then $I(y) = \mathfrak{m}/J(R)$ for some maximal ideal $\mathfrak{m}$ of R and $R'_y \simeq R/\mathfrak{m}$. So $t(X)$ is indecomposable modulo $\mathfrak{m}[X]$. Let $\mathfrak{M}$ be a maximal ideal of S over $\mathfrak{m}$. Since $rank_{R/\mathfrak{m}}S/\mathfrak{M} = rank_RS = n$ and by assumption p does not divide n then the claim follows.

From now on let $q = min\{|R'_x| \,|\, x \in Y\}$ and assume that the prime integer p above considered also satisfies $\frac{q^p - q}{p} \geq n$. By [9, Theorem 1.1] we can also assume that S is a Galois extension of R in the sense of [3]. Set $T = S[X]/(t(X))$. It easily follows from the properties of $t(X)$ that T is a connected strongly separable extension of R.

Claim 3. *T has a primitive element over R.*

By Nakayama's lemma and boolean localization it is enough to show that T'_x has a primitive element over R'_x for every $x \in Spec(B(R))$, where $T' = T/J(R)T = T/J(T)$.

It is clear that T'_x has a primitive element over R'_x if $x \notin Y$. So let $x \in Y$ and $\mathfrak{M}_1, \ldots, \mathfrak{M}_s$ be the maximal ideals of S over $\mathfrak{m}$, where $\mathfrak{m}$ is such that $R'_x \simeq R/\mathfrak{m}$.

Recall that $t(X) = g(X)$ modulo $J(R)[X]$ as constructed above. By the same arguments used in Claim 2 $t(X)$ is indecomposable in $S/\mathfrak{M}_j[X]$, for all $1 \leq j \leq s$. By [16, Theorem 3.5] there is a unique maximal ideal $\mathfrak{M}'_j$ of T over $\mathfrak{M}_j$ and $\left[T/\mathfrak{M}'_j : S/\mathfrak{M}_j\right] = p$, for each $1 \leq j \leq s$.

On the other hand, we have $S/\mathfrak{M}_j \simeq S/\mathfrak{M}_1$ since as assumed above S is a Galois extension of R. Therefore, $\left[T/\mathfrak{M}'_j : R/\mathfrak{m}\right] = p\,[S/\mathfrak{M}_j : R/\mathfrak{m}] = p\,[S/\mathfrak{M}_1 : R/\mathfrak{m}]$.

Let $\mathbb{F}_q$ denote the finite Galois field with q elements and $N_q(m)$ the number of all monic and indecomposable polynomials of degree m in $\mathbb{F}_q[X]$. By [13, Theorem 3.25] we have $N_q(p) = \frac{q^p - q}{p}$. Hence, if $|R'_x| = q_x$ then $N_{q_x}(p) = \frac{q_x^p - q_x}{p} \geq \frac{q^p - q}{p} = N_q(p)$.

If $[S/\mathfrak{M}_1 : R/\mathfrak{m}] = 1$ then $N_{q_x}\left(p\,[S/\mathfrak{M}_1 : R/\mathfrak{m}]\right) = N_{q_x}(p) \geq N_q(p) \geq n$. If $[S/\mathfrak{M}_1 : R/\mathfrak{m}] \geq 2$ then by [10, Lemma 1.2] we have $N_{q_x}\left(p\,[S/\mathfrak{M}_1 : R/\mathfrak{m}]\right) \geq N_{q_x}(p) N_{q_x}\left([S/\mathfrak{M}_1 : R/\mathfrak{m}]\right) \geq N_{q_x}(p) \geq N_q(p) \geq n$.

Thus $N_{q_x}\left(p\,[S/\mathfrak{M}_1 : R/\mathfrak{m}]\right) \geq n \geq s$ and there exist distinct separable and indecomposable polynomials $h_1(X), \ldots, h_s(X)$ of degree $p\,[S/\mathfrak{M}_1 : R/\mathfrak{m}]$ in $R/\mathfrak{m}[X]$.

By [16, Theorem 2.1] $\mathfrak{m}T = \bigcap_{1 \leq j \leq s} \mathfrak{M}'_j$. Also $T/\mathfrak{M}'_j \simeq R/\mathfrak{m}[X]/(h_j(X))$ for all $1 \leq j \leq s$. So by chinese remainder theorem we have $T/\mathfrak{m}T = \bigoplus_{1 \leq j \leq s} T/\mathfrak{M}'_j \simeq R/\mathfrak{m}[X]/(h(X))$, with $h(X) = h_1(X) \cdots h_s(X)$.

Finally, by observing that $T'_x = T'/I(x)T' = (T/J(T))/(\mathfrak{m}T/J(T)) \simeq T/\mathfrak{m}T$ the claim follows.

The conclusion of the proof of Theorem 2.1 follows now from Claim 3 and [16, Theorem 3.3]. □

Remark 2.2 In Theorem 2.1 the ring extension $T = R[\alpha] \supseteq S$ also satisfies $rank_R T = p^{\epsilon} rank_R S$, with p a prime integer and either $\epsilon = 0$ or $\epsilon = 1$, in the following two cases: R is semilocal [2, Theorem 2.1.1] or S is a Galois extension of R.

Remark 2.3 Corollaries 1.2 and 1.4 of [18] have natural corresponding extensions, with similar proofs, to the setting of connected rings R such that $R/J(R)$ is von Neumann regular and locally uniform.

3. More about separable closures

For any ring R we will denote by $Max(R)$ the set of all maximal ideals of R.

Our purpose in this section is twofold. Firstly we will give necessary and sufficient conditions in order to $Max(R)$ and $Max(\Omega(R))$ have the same cardinality (Theorem 3.1). Secondly we will present an interesting characterization of $\mathrm{Aut}_R(\Omega(R))$ (Corollary 3.6). We will do that in the setting of connected rings R such that $R/J(R)$ is von Neumann regular and locally uniform. In particular, our first result is an improved and generalized version of Theorem 1.5 of [17].

Given a ring extension $S \supseteq R$ and a maximal ideal $\mathfrak{M}$ of S we denote by $D(\mathfrak{M})$ the decomposition group of $\mathfrak{M}$, that is, $D(\mathfrak{M}) = \{\sigma \in \mathrm{Aut}_R(S) \,|\, \sigma(\mathfrak{M}) = \mathfrak{M}\}$. For S integral over R let ψ denotes the contraction map from $Max(S)$ onto $Max(R)$, that is, $\psi(\mathfrak{M}) = \mathfrak{M} \bigcap R$ for all $\mathfrak{M} \in Max(S)$.

Theorem 3.1 *Let R be a connected ring such that $R/J(R)$ is von Neumann regular and locally uniform. Then the following statements are equivalent:*

(i) *The map $\psi : Max(\Omega(R)) \to Max(R)$ is bijective.*

(ii) *$D(\mathfrak{M}) = Aut_R(\Omega(R))$, for every $\mathfrak{M} \in Max(\Omega(R))$.*

(iii) *If $f(X)$ is separable and indecomposable in $R[X]$ then $\overline{f(X)} = f(X) + \mathfrak{m}R[X]$ is separable and indecomposable in $R/\mathfrak{m}[X]$ for every $\mathfrak{m} \in Max(R)$.*

Proof. (i)⇒(ii) Take $\mathfrak{M} \in Max(\Omega(R))$ and $\sigma \in \mathrm{Aut}_R(\Omega(R))$. Then $\sigma(\mathfrak{M}) \bigcap R = \sigma(\mathfrak{M} \bigcap R) = \mathfrak{M} \bigcap R$ and consequently $\sigma(\mathfrak{M}) = \mathfrak{M}$.

(ii)⇒(i) If $\mathfrak{M}_1, \mathfrak{M}_2 \in Max(\Omega(R))$ satisfy $\mathfrak{M}_1 \bigcap R = \mathfrak{M}_2 \bigcap R$ then there exists $\sigma \in \mathrm{Aut}_R(\Omega(R))$ such that $\sigma(\mathfrak{M}_1) = \mathfrak{M}_2$ [16, Lemma 2.2]. The result follows by the assumption.

(i)⇒(iii) Let $f(X) \in R[X]$ be separable and indecomposable. The separability of $\overline{f(X)}$ over $R/\mathfrak{m}$ is clear, for all $\mathfrak{m} \in Max(R)$. Put $T = R[X]/(f(X))$. Clearly T is a connected strongly separable extension of R and by [5, Theorem III.3.3] we may assume that T is contained in $\Omega(R)$. Thus it follows by the assumption that for each $\mathfrak{m} \in Max(R)$ there exists a unique $\mathfrak{M} \in Max(T)$ such that $\mathfrak{M} \bigcap R = \mathfrak{m}$. Consequently $\overline{f(X)}$ is indecomposable in $R/\mathfrak{m}[X]$ for all $\mathfrak{m} \in Max(R)$ by [16, Theorem 3.5].

(iii)⇒(i) Let $\mathfrak{M}_1, \mathfrak{M}_2 \in Max(\Omega(R))$ such that $\mathfrak{M}_1 \bigcap R = \mathfrak{M}_2 \bigcap R = \mathfrak{m}$. By [16, Theorem 2.1] we have $\mathfrak{m}\Omega(R) \subseteq \mathfrak{M}_1 \bigcap \mathfrak{M}_2$. Thus, if $\mathfrak{m}\Omega(R) = \mathfrak{M}_1$ the result follows. Assume that $\mathfrak{m}\Omega(R) \subsetneq \mathfrak{M}_1$. Then there exist $z \in \mathfrak{M}_1 \backslash \mathfrak{m}\Omega(R)$ and a strongly separable extension S of R such that $z \in S \subseteq \Omega(R)$. Note that

$z \in (S \bigcap \mathfrak{M}_1) \setminus \mathfrak{m}S$, so $\mathfrak{m}S \subsetneq S \bigcap \mathfrak{M}_1$. Since $S \bigcap \mathfrak{M}_1$ is a maximal ideal of S over $\mathfrak{m}$ it follows from [16, Theorem 2.1] that S contains at least two maximal ideals over $\mathfrak{m}$. On the other hand $R/J(R)$ is von Neumann regular and locally uniform, so there exist $\alpha \in \Omega(R)$ and a separable and indecomposable polynomial $f(X) \in R[X]$ such that $f(\alpha) = 0$ and $S \subseteq R[\alpha] \simeq R[X]/(f(X))$ by Theorem 2.1. Consequently it follows from [16, Theorem 3.5] that $R[\alpha]$ contains a unique maximal ideal over $\mathfrak{m}$, which is a contradiction. □

For our second result mentioned above we need some preparation and we start with the following lemmas.

Lemma 3.2 *Let R be a von Neumann regular ring. Then every locally strongly separable extension of R is von Neumann regular.*

Proof. Let T be a locally strongly separable extension of R. Take $a \in T$. Thus T contains a strongly separable extension S of R such that $a \in S$. Note that if S is von Neumann regular then $a = a^2b$ for some $b \in S$ and consequently T is also von Neumann regular. Hence, it is enough to prove that S is von Neumann regular. For every maximal ideal $\mathfrak{m}$ of R, $S_{\mathfrak{m}}$ is a separable extension of $R_{\mathfrak{m}}$ and $R_{\mathfrak{m}}$ is a field. So $S_{\mathfrak{m}}$ is a finite direct sum of fields and consequently a von Neumann regular ring. The required follows from [7, Lemma 1]. □

Lemma 3.3 *Let R be a connected ring, $I \subseteq R$ an ideal and T a locally strongly separable extension of R. Then $IT \bigcap R = I$.*

Proof. Clearly $I \subseteq IT \bigcap R$. Now take $c \in IT \bigcap R$. Then $c \in R$ and $c = \sum_{1 \leq i \leq n} a_i b_i \in R$ with $a_i \in I$ and $b_i \in T$. Consider $S \subseteq T$ a strongly separable extension of R containing b_i, $1 \leq i \leq n$. So $c \in IS \bigcap R$. Since R is a direct summand of S [5, Corollary III.2.3] we have $IS = I \bigoplus IN$ for some R-module N and $c = a + b$ with $a \in I$ and $b \in IN$. Consequently $b = c - a \in R \bigcap N = 0$ and $c \in I$. □

Lemma 3.4 *Let R be a connected ring, $I \subseteq R$ an ideal such that R/I is von Neumann regular. Then $\Omega(R)/I\Omega(R)$ also is von Neumann regular.*

Proof. By Lemma 3.2 it is enough to prove that $\Omega(R)/I\Omega(R)$ is a locally strongly separable extension of R/I. It follows from Lemma 3.3 that $\Omega(R)/I\Omega(R)$ is an extension of R/I. Let $a_1 + I\Omega(R), \ldots, a_n + I\Omega(R) \in \Omega(R)/I\Omega(R)$. Then there exists a strongly separable extension S of R such that $a_1, \ldots, a_n \in S \subseteq \Omega(R)$. Clearly S/IS is a strongly separable extension of R/I. On the other hand, $\Omega(R)$ is a locally strongly separable extension of S [19, Proposition 2] and so $I\Omega(R) \bigcap S = (IS)\Omega(R) \bigcap S = IS$ by

Lemma 3.3. Therefore $\Omega(R)/I\Omega(R)$ is an extension of S/IS and the result follows. □

Theorem 3.5 *Let R be a connected ring such that $R/J(R)$ is von Neumann regular and $\mathfrak{m} \in Max(R)$. Then $\Omega(R/\mathfrak{m}) = \Omega(R)/\mathfrak{M}$ for all $\mathfrak{M} \in Max(\Omega(R))$ such that $\mathfrak{M} \bigcap R = \mathfrak{m}$.*

Proof. Let $\mathfrak{M} \in Max(\Omega(R))$ such that $\mathfrak{M} \bigcap R = \mathfrak{m}$.

Claim 1. *$\Omega(R)/\mathfrak{M}$ is a locally strongly separable extension of $R/\mathfrak{m}$.*

Take $a_1 + \mathfrak{M}, \dots, a_n + \mathfrak{M} \in \Omega(R)/\mathfrak{M}$. Then $a_1, \dots, a_n \in S$ for some strongly separable extension S of R contained in $\Omega(R)$. Note that $\Omega(R)$ is integral over S, so $\mathfrak{M} \bigcap S$ is a maximal ideal of S over $\mathfrak{m}$. Moreover, $S_{\mathfrak{m}}$ is a strongly separable extension of $R_{\mathfrak{m}}$ and consequently a semilocal ring whose maximal ideals are in bijective correspondence with the maximal ideals of S over $\mathfrak{m}$. Hence there is only finitely many maximal ideals of S over $\mathfrak{m}$ and $S/\mathfrak{M} \bigcap S$ is a direct summand of $S/\mathfrak{m}S$ by [16, Theorem 2.1] and chinese remainder theorem. Therefore $S/\mathfrak{M} \bigcap S$ is a strongly separable extension of $R/\mathfrak{m}$ and the claim follows.

Claim 2. *$\Omega(R)/\mathfrak{M}$ is separably closed.*

Put $R' = R/J(R)$, $\Omega(R)' = \Omega(R)/J(R)\Omega(R)$ and $\mathfrak{M}' = \mathfrak{M}/J(R)\Omega(R)$. By Lemma 3.4 $\Omega(R)'$ is von Neumann regular, so $\mathfrak{M}' = I(x)$ for some $x \in Spec(B(\Omega(R)'))$. Therefore $\Omega(R)'_x = \Omega(R)'/\mathfrak{M}' \simeq \Omega(R)/\mathfrak{M}$.

Let T be a connected and strongly separable extension of $\Omega(R)/\mathfrak{M}$. Then $T \simeq \Omega(R)'/\mathfrak{M}'[X]/(f(X))$ for some separable and indecomposable polynomial $f(X) \in \Omega(R)'/\mathfrak{M}'[X]$.

Let $g_1(X) \in \Omega(R)'[X]$ be a monic polynomial such that $g_1(X)_x = f(X)$. It follows from the separability of $g_1(X)_x$ and from [23, 2.9] that there exists an idempotent $e_1 \in \Omega(R)'$ such that $x \in U_{e_1}$ and $e_1 g_1(X)$ is separable over $e_1\Omega(R)'$.

Put $Y = Spec(B(\Omega(R)')) \backslash U_{e_1}$ and take $g(X) \in \Omega(R)'[X]$ a monic polynomial such that $deg(g(X)) = deg(f(X))$ and $g(X)_y \in \Omega(R')_y[X]$ is separable, for each $y \in Y$. Since Y is an open set, it follows again from the separability of $g(X)_y$ and from [23, 2.9] that there exists for each $y \in Y$ an idempotent $e(y) \in \Omega(R)'$ such that $y \in U_{e(y)} \subseteq Y$ and $e(y)g(X)$ is separable over $e(y)\Omega(R)'$.

Now by compactness arguments we get pairwise orthogonal idempotents $e_2, \dots, e_n \in \Omega(R)'$ and polynomials $g_2(X), \dots, g_n(X) \in \Omega(R)'[X]$ such that $e_1 + e_2 + \cdots + e_n = 1$, $deg(g_i(X)) = deg(f(X))$ and $e_i g_i(X)$ is separable over $e_i\Omega(R)'$, for all $2 \leq i \leq n$. Consequently $g(X) = e_1 g_1(X) + e_2 g_2(X) + \cdots +$

$e_n g_n(X)$ is separable over $\Omega(R)'$ and $deg(g(X)) = deg(f(X))$. Furthermore, $e_1 g_1(X)$ (and, consequently, also g(X)) is indecomposable in $\Omega(R)'[X]$.

Let $h(X) \in \Omega(R)[X]$ a monic polynomial such that $g(X) = h(X)$ modulo $J(R)\Omega(R)$. By construction $h(X)$ is separable and indecomposable in $\Omega(R)[X]$. So $\Omega(R)[X]/(h(X))$ is a connected strongly separable extension of $\Omega(R)$. Hence $deg(f(X)) = deg(h(X)) = 1$ and $T = \Omega(R)/\mathfrak{M}$. The proof is complete. □

Corollary 3.6 *Let R be a connected ring such that $R/J(R)$ is von Neumann regular, $\mathfrak{m} \in Max(R)$ and $\mathfrak{M} \in Max(\Omega(R))$ satisfying $\mathfrak{M} \bigcap R = \mathfrak{m}$. Then $D(\mathfrak{M}) \simeq Aut_{R/\mathfrak{m}}(\Omega(R/\mathfrak{m}))$. If in addition $R/J(R)$ is locally uniform then $Aut_R(\Omega(R)) \simeq Aut_{R/\mathfrak{m}}(\Omega(R/\mathfrak{m}))$, for all $\mathfrak{m} \in Max(R)$.*

Proof. It follows from [16, Theorem 2.7] and Theorems 3.1 and 3.5. □

Acknowledgement

This paper was partially supported by CNPQ and FAPERGS, Brazil

References

[1] A. G. Aramova, *Primitive elements for cyclic p^n-extensions of commutative rings*, Math. J. Okayama Univ. **34** (1992), 13-20.

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

[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. Math **2** (1972), 299-310.

[5] F. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings*, LNM 181, Springer Verlag, NY, 1970.

[6] D. R. Estes and R. M. Guralnick, *Module equivalence: local to global when primitive polynomials represent units*, J. of Algebra **77** (1982), 138-157.

[7] K. R. Goodearl and R. B. Warfield, *Algebras over zero-dimensional rings*, Math. Ann. **223** (1976), 157-168.

[8] H. Hasse, *Zwei existenszätze über algebraische zahlkörper*, Math Ann. **95** (1926), 229-238.

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

[10] I. Kikumasa, *On primitive elements of Galois extensions of commutative semilocal rings II*, Math. J. Okayama Univ. **31** (1989), 57-71.

[11] I. Kikumasa and T. Nagahara, *Primitive elements of cyclic extensions of commutative rings*, Math. J. Okayama Univ. **29** (1987), 91-102.

[12] I. Kikumasa, T. Nagahara and K. Kishimoto, *On primitive elements of Galois extensions of commutative semilocal rings*, Math. J. Okayama Univ. **31** (1989), 31-35.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1986.

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

[15] B. R. McDonald and W. C. Waterhouse, *Projective modules over rings with many units*, Proc. Amer. Math. Soc. **83** (1981), 455-458.

[16] T. McKenzie, *Separable polynomials and weak henselizations*, Rings, Extensions and Cohomology (Evenston. IL, 1993), 165-179, LN in Pure and Appl. Math. 159, Marcel Dekker, NY, 1994.

[17] ______, *Weakly hensilian rings*, Math. J. Okayama Univ. **38** (1996), 47-51.

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

[19] T. Nagahara, *On separable extensions of domains*, Math. J. Okayama Univ. **14** (1970), 145-151.

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

[21] R. S. Pierce, *Modules over commutative regular rings*, Mem. AMS 70, 1967.

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

[23] O. E. Villamayor, D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J. **35** (1969), 83-98.

Dirceu Bagio
Departamento de Matemática
Universidade Federal de Santa Maria
Santa Maria, RS, 97105-900 Brazil
e-mail address: bagio@smail.ufsm.br

Antonio Paques
Instituto de Matemática
Universidade Federal do Rio Grande do Sul
Porto Alegre, RS, 91509-900 Brazil
e-mail address: paques@mat.ufrgs.br

(*Received June 12, 2006*)
(*Revised May 8, 2007*)