Mathematica Moravica
Vol. **21**, No. **1** (2017), 69–86

# Reduced and irreducible simple algebraic extensions of commutative rings

S.V. Mihovski

Abstract. Let $A$ be a commutative ring with identity and $\alpha$ be an algebraic element over $A$. We give necessary and sufficient conditions under which the simple algebraic extension $A[\alpha]$ is without nilpotent or without idempotent elements.

## 1. Introduction

Let $A$ be a commutative ring with identity element 1. We shall say that $K$ is a commutative ring extension of $A$, or $A$ is a subring of $K$, if $A$ and $K$ are commutative rings with common identity element and $A \subseteq K$.

Suppose that $K$ is a commutative ring extension of $A$ and let $\alpha \in K$ be an algebraic element over$A$. If $\alpha$ is a root of a nonzero polynomial $f(x) \in A[x]$ of a minimal degree $n$, then we shall say that $f(x)$ is a minimal polynomial of $\alpha$ over the ring $A$. The intersection of all subrings of $K$, containing $A$ and $\alpha$, we shall denoted by $A[\alpha]$. The ring $A[\alpha]$ is called a simple algebraic extension of $A$, which is obtained by adjoining $\alpha$ to $A$.

Let $f(x)$ be any nonzero polynomial over the ring $A$. If the leading coefficient of $f(x)$ is $a_0 = 1$, then $f(x)$ is said to be a monic polynomial over $A$. And what is more, if the leading coefficient $a_0$ of $f(x)$ is a regular element in $A$, i.e. $a_0$ is not zero divisor in $A$, then we shall say that $f(x)$ is a regular polynomial over the ring $A$.

Recall that the ring $A$ is called a reduced ring if $A$ has no nonzero nilpotent elements. The ring $A$ is said to be irreducible if $A$ has no nontrivial idempotents.

A main result in [11] asserts that if $A$ is a reduced commutative ring, $f(x)$ is a monic minimal polynomial of $\alpha$ over $A$ and the discriminant $\Delta(f)$ is a regular element in $A$, then the simple algebraic extension $A[\alpha]$ is a reduced ring. Also in [11] is proved that if $A$ is an irreducible ring and the minimal polynomial $f(x)$ of $\alpha$ is monic and irreducible over $A$, then the simple algebraic extension $A[\alpha]$ again is irreducible. So here arises the

---

2010 *Mathematics Subject Classification.* 13B25, 13B02.

*Key words and phrases.* Commutative rings, Polynomials, Discriminants, Resultants, Simple algebraic extensions, Reduced rings, Irreducible rings.

problem to find necessary and sufficient conditions under which the ring $A[\alpha]$ is reduced or irreducible. In this paper we solve these two problems in the parts 3 and 4, respectively.

## 2. PRELIMINARY LEMMAS AND DEFINITIONS

It is well known that every polynomial $f(x)$ of degree $n$ with coefficients from a field $F$ has at most $n$ roots in every field extension of $F$. Moreover, there exists a field extension $\overline{F} \supseteq F$ such that $\overline{F}$ contains exactly $n$ roots of $f(x)$. But this fact does not hold for the ring extensions of $F$. For example, let $G$ be a direct product of $m \geq 2$ cyclic groups of order $n$ and let $K = FG$ be the group ring of the group $G$ over the field $F$. Then $K$ is a ring extension of $F$ and every element of $G$ is a root of the polynomial $f(x) = x^n - 1 \in F[x]$. Thus $f(x)$ has at least $n^m$ roots in $K$.

Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \qquad (n \geq 1) \tag{1}$$

be a polynomial over $A$ of degree $n$. We shall say that the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a canonical system roots of the polynomial $f(x) \in A[x]$ if there exists a commutative ring extension $K \supseteq A$ such that $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ and

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n). \tag{2}$$

Every regular polynomial over $A$ has at last one canonical system roots [9]. But example shows that over some rings $A$ there exist polynomials that have not roots. Moreover, there exist polynomials which have roots, but they have not canonical systems of roots. For more details see [9].

Later on we shall use the following two definitions. A discriminant of the polynomial (1) we shall call the following determinant of order $2n - 1$

$$\Delta(f) = \varepsilon \begin{vmatrix} 1 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_n \\ n & (n-1)a_1 & (n-2)a_2 & \cdots & a_{n-1} & 0 & \ldots & 0 \\ 0 & na_0 & (n-1)a_1 & \ldots & 2a_{n-2} & a_{n-1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & na_0 & (n-1)a_1 & \ldots & a_{n-1} \end{vmatrix},$$

where $\varepsilon = (-1)^{\frac{n(n-1)}{2}}$. So, for $n = 1$ and $n = 2$ we have $\Delta(f) = 1$ and $\Delta(f) = a_1^2 - 4a_0a_2$, respectively. Let

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m \qquad (m \geq 1) \tag{3}$$

be another polynomial over $A$. Then the determinant of order $n + m$

$$R(f,g)=\begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_0 & a_1 & \dots & a_{n-1} & a_n \\ b_0 & b_1 & \dots & b_m & 0 & \dots & 0 & 0 \\ 0 & b_0 & b_1 & \dots & b_m & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_0 & b_1 & \dots & b_{m-1} & b_m \end{vmatrix}$$

is said to be a resultant of the polynomials $f(x)$ and $g(x)$ (see [3, 8, 13]).

If $e_1, e_2, \dots, e_k$ is a full orthogonal system idempotents of the ring $A$, that is the ring $A$ is a direct sum of the ideals $e_iA \quad (i = 1, \dots, k)$, then for the polynomials $f(x), g(x) \in A[x]$ we put $f_i(x) = e_i f(x)$ and $g_i(x) = e_i g(x)$. So from the definition of $R(f, g)$ we conclude that

$$R(f,g) = R(f_1,g_1) + R(f_2,g_2) + \cdots + R(f_k,g_k).$$

Likewise,

$$\Delta(f) = \Delta(f_1) + \Delta(f_2) + \cdots + \Delta(f_k).$$

Later on we shall use these facts without special stipulations.

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be a canonical system roots of the polynomial (1). In [9] it is proved that

$$R(f,g) = a_0^m g(\alpha_1) g(\alpha_2) \cdots g(\alpha_n) \tag{4}$$

for every polynomial $g(x) \in A[x]$, even when $g(x)$ does not have roots. Moreover, if $n \geq 2$ and $f'(x)$ is the prime derivative of $f(x)$, then [10]

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \cdot a_0^{n-2} \cdot f'(\alpha_1) \cdot f'(\alpha_2) \cdots f'(\alpha_n). \tag{5}$$

When $A$ is a field, then (4) and (5) show the well known facts that $R(f, g) = 0$ if and only if $f(x)$ and $g(x)$ have common roots and $f(x)$ has multiple roots if and only if $\Delta(f) = 0$. For arbitrary polynomials $f(x), g(x) \in A[x]$ we have the following.

**Lemma 1.** *(see* [9]*, also* [8] *p.159 and* [13] *p. 130) Let $A$ be any commutative ring with identity. If* (1) *and* (3) *are polynomials over $A$, then*

(i) *There exist polynomials $\varphi(x), \psi(x) \in A[x]$ such that* $\deg \varphi(x) \leq m - 1$, $\deg \psi(x) \leq n - 1$ *and*

$$R(f,g) = \varphi(x) f(x) + \psi(x) g(x).$$

(ii) *If $n \geq 2$, then there exist polynomials $u(x), v(x) \in A[x]$ such that* $\deg u(x) \leq n - 2$, $\deg v(x) \leq n - 1$ *and*

$$\Delta(f) = u(x) f(x) + v(x) f'(x).$$

So we obtain

**Corollary 1.** [9] *Let $f(x)$ and $g(x)$ be polynomials over the ring $A$.*

(i) *If $f(x)$ and $g(x)$ have common roots, then $R(f, g) = 0$.*
(ii) *If $f(x)$ has multiple roots, then $\Delta(f) = 0$.*

Examples show that the converse statements of the preceding corollary in the general case are erroneous [9].

Let $S$ be a multiplicatively closed set of regular elements in $A$, that is $S$ contains the product of every his two elements and every element of $S$ is not zero divisor in $A$. Then there exists a ring of quotients $S^{-1}A$ with respect to $S$ ([12], p. 146). Every element of $S^{-1}A$ is of the form $s^{-1}a$, where $s \in S$, $a \in A$. Thus all elements of $S$ are invertible in $S^{-1}A$. If $S$ is the set of all regular elements in $A$, then $S^{-1}A$ is said to be the classical ring of quotients, that we shall denote by $Q(A)$.

**Lemma 2.** *Let $A$ be a ring with identity and $f(x)$ be a regular polynomial over $A$ of degree $n \geq 1$. Then there exists a ring extension $K \supseteq A$ such that $f(x)$ is a minimal polynomial over $A$ of some element $\alpha \in K$.*

*Proof.* Let (1) be a regular polynomial over $A$. First, suppose that $a_0 = 1$. If $\deg f(x) = n = 1$, then we put $\alpha = -a_1$ and the statements are trivial. If $n \geq 2$, then let $K = A[y]/I$ be the quotient ring of the polynomial ring $A[y]$ modulo the principal ideal $I$, generated by the polynomial $f(y)$. Thus $\bar{A} = \{a + I \mid a \in A\}$ is a subring of $K$ and, because $a_0 = 1$, it is clear that $A$ and $\overline{A}$ are isomorphic rings. So $A$ can be viewed as a subring of $K$. Obviously, $f(x)$ is a minimal polynomial of the element $\alpha = y + I \in K$.

If $a_0 \neq 1$, then let $P = Q(A)$ be the classical ring of quotients of $A$. Now $A \subseteq P$, $f(x) \in P[x]$ and $a_0$ is an invertible element of $P$. Therefore $g(x) = a_0^{-1} f(x)$ is a monic polynomial over $P$ and the statement for $g(x)$ holds. Thus we conclude that there exists a commutative ring extension $K \supseteq P$ such that $g(x)$ is a minimal polynomial over $P$ of some element $\alpha \in K$. Then it is clear that $f(x) = a_0 g(x)$ is a minimal polynomial of $\alpha$ over $A$, as was to be shoved. □

When $\alpha \in K$ and $P = Q(A) \subseteq K$, then by definition there exists the simple ring extensions $P[\alpha]$ with $A[\alpha] \subseteq P[\alpha]$. But, if $P \not\subseteq K$, then $P[\alpha]$ is not defined in the general case. Later on we shall use the following

**Lemma 3.** *Let $K \supseteq A$ be a ring extension and $\alpha \in K$ be an algebraic element over $A$ with a regular minimal polynomial $f(x) \in A[x]$. Then there exists a ring extension $K_1 \supseteq A$ such that $Q(A) \subseteq K_1$, $f(x)$ is a minimal polynomial of some $\beta \in K_1$ and $A[\alpha] \cong A[\beta]$.*

*Proof.* Let (1) be a minimal polynomial over $A$ of the element $\alpha$. If $P = Q(A) \subseteq K$, then we put $K_1 = K$ and $\beta = \alpha$. Suppose that $P \not\subseteq K$. Since $f(x) \in P[x]$, by Lemma 2 it follows that there exists a commutative ring extension $K_1 \supseteq P$ such that $f(x)$ is a minimal polynomial over $P$ of some element $\beta \in K_1$. Since $A \subseteq P$ and $f(x) \in A[x]$, it is clear that $f(x)$ is a minimal polynomial of $\beta$ and over $A$. Now we shall prove that $A[\alpha]$ and $A[\beta]$ are isomorphic.

First we shall show that for $g(x) \in A[x]$ the conditions $g(\alpha) = 0$ and $g(\beta) = 0$ are equivalent. Really, since the leading coefficient $a_0$ is invertible in $P = Q(A)$, we have

$$g(x) = f(x)q(x) + r(x), \qquad \deg r(x) < \deg f(x),$$

where the polynomials $q(x)$ and $r(x)$ are with coefficients in $P$. It is clear that there exists a power $a_0^k$ ($k \geq 1$) of the element $a_0 \in A$ such that $a_0^k q(x)$ and $a_0^k r(x)$ to be elements of $A[x]$. Then

$$a_0^k g(x) = f(x)[a_0^k q(x)] + a_0^k r(x), \qquad \deg(a_0^k r(x)) < \deg f(x).$$

If $g(\alpha) = 0$, then $a_0^k r(\alpha) = 0$ and by the minimum condition of $f(x)$ we conclude that $a_0^k g(x) = f(x)[a_0^k q(x)]$. Therefore $a_0^k g(\beta) = 0$ and so $g(\beta) = 0$, because $a_0^k$ is an invertible element of $P$. In similar way from $g(\beta) = 0$ we receive $g(\alpha) = 0$. Now it is easy to verify that the map $g(\alpha) \mapsto g(\beta)$ for all $g(x) \in A[x]$ is an isomorphism between $A[\alpha]$ and $A[\beta]$, as was to be showed. □

**Lemma 4.** *Let $P = Q(A)$ be the classical ring of quotients of a commutative reduced ring $A$ and let $f(x) \in A[x]$ be a regular minimal polynomial of the algebraic element $\alpha$. Then*

(i) *The rings $A[\alpha]$ and $\overline{A} = A[x]/(A[x] \bigcap f(x)P[x])$ are isomorphic.*

(ii) *The ring $A[\alpha]$ is reduced if and only if the quotient ring $\overline{P} = P[x]/f(x)P[x]$ is reduced.*

*Proof.* In view the preceding lemma we may assume that $Q(A) \subseteq K$ and $\alpha \in K$.

(i) The mapping $\Phi : A[x] \to A[\alpha]$, defined by $\Phi(g(x)) = g(\alpha)$ for all $g(x) \in A[x]$, is a homomorphism of $A[x]$ onto $A[\alpha]$ with $\ker \Phi = A[x] \bigcap f(x)P[x]$. Really, it is clear that $A[x] \bigcap f(x)P[x] \subseteq \ker \Phi$. If $g(x) \in \ker \Phi$, then $g(\alpha) = f(\alpha) = 0$. Moreover, there exist polynomials $q(x), r(x) \in P[x]$, such that

$$g(x) = f(x)q(x) + r(x) \qquad \text{and} \qquad \deg r(x) < \deg f(x).$$

Hence it follows that $r(\alpha) = 0$. Since $P = Q(A)$, for some regular element $a \in A$ we have $\varphi(x) = ar(x) \in A[x]$. But $\varphi(\alpha) = 0$ and $\deg \varphi(x) < \deg f(x)$ imply $\varphi(x) = 0$. So we obtain $r(x) = 0$ and $g(x) \in f(x)P[x]$, as was be shown.

(ii) Let $\overline{P}$ be a reduced ring. Since

$$\overline{A} = A[x] \Big/ (A[x] \bigcap f(x)P[x]) \cong (A[x] + f(x)P[x]) / f(x)P[x] \subseteq \overline{P},$$

so we conclude that $\overline{A}$ is a reduced ring. Now by (i) we obtain that the ring $A[\alpha]$ is reduced. Conversely, suppose that $A[\alpha]$ is reduced. If $\overline{P}$ is not reduced and $\varphi(x) + f(x)P[x]$ is its nontrivial nilpotent element, then we may assume that $0 \neq \varphi(x) \in P[x]$, $\deg \varphi(x) < \deg f(x)$ and $\varphi^k(x) \in f(x)P[x]$ for some integer $k > 1$. Let $a \in A$ be a nonzero regular element such that $0 \neq a\varphi(x) \in A[x]$. Then it is clear that $a\varphi(x) + A[x] \bigcap f(x)P[x]$ is a nonzero nilpotent element of $\overline{A}$. This shows that $\overline{A}$ is not reduced ring and by (i) we receive that $A[\alpha]$ is not reduced, which is a contradiction. So the proof is completed. $\square$

**Corollary 2.** *If the leading coefficient of the polynomial $f(x) \in A[x]$ is an invertible element of $A$ and $f(x)$ is a minimal polynomial of $\alpha$, then the rings $A[\alpha]$ and $A[x]/f(x)A[x]$ are isomorphic.*

*Proof.* Let $P$ be as above. Since the leading coefficient of the polynomial $f(x)$ is invertible in $A$, it is easy to verify that $f(x)A[x] \subseteq A[x] \bigcap f(x)P(x) \subseteq f(x)A[x]$. Then the statement follows by Lemma 4(i). $\square$

## 3. SIMPLE ALGEBRAIC EXTENSIONS OF REDUCED RINGS

Now let $A$ be a reduced commutative ring and let $f(x) \in A[x]$ be a minimal polynomial of the algebraic element $\alpha$. It is clear that $A[\alpha]$ is reduced if and only if the ring $B[\alpha]$ is reduced for every finitely generated subring $B \subseteq A$ such that $f(x) \in B[x]$. Therefore it is sufficient to find necessary and sufficient conditions $A[\alpha]$ to be reduce when $A$ is a noetherian ring. First we shall consider the case when $A$ is a field.

Recall that a field $F$ of characteristic $p \geq 0$ is said to be perfect if $p = 0$, or $p > 0$ and $F^p = F$ ([2], p. 137). So every finite field and every algebraically closed field is perfect.

If $F$ is a field and $f(x), g(x) \in F[x]$, then as ever, by $(f, g)$ we shall denote the monic greatest common divisor over $F$ of the polynomials $f(x)$ and $g(x)$. Moreover, $f(x)$ and $g(x)$ are associated if $f(x) = ag(x)$ for some non zero element $a \in F$.

**Lemma 5.** *Let $F$ be a field of characteristic $p \geq 0$ and let $f(x)$ be a nonzero polynomial over $F$. Then the following conditions are equivalent:*

(i) *The quotient ring $F[x]/f(x)F[x]$ is reduced.*
(ii) *The polynomial $f(x)$ is a product of distinct non associated irreducible polynomials over the field of $F$.*
(iii) *Either $(f, f') = 1$, or $F$ is not perfect field of characteristic $p \neq 0$ and $(f, f')$ is a products of distinct non associated irreducible polynomials of the form $\varphi(x^p) \in F[x]$.*

*Proof.* Let $f(x) = af_1^{k_1}(x)f_2^{k_2}(x) \cdots f_s^{k_s}(x)$ be a factorization of $f(x)$ over $F$, where $f_1(x), \dots, f_s(x)$ are distinct non associated irreducible polynomials over $F$ and $a \in F$. Since $(f_i, f_j) = 1$ for all $i \neq j$, by the Chinese theorem ([8], p.88) we have

$$F[x] \Big/ f(x)F[x] \cong \sum_{i=1}^{s} \oplus F[x] \Big/ f_i^{k_i}(x)F[x].$$

It is clear that $F[x]/f(x)F[x]$ is reduced if and only if $k_1 = k_2 = \cdots = k_s = 1$. So we obtain that (i) and (ii) are equivalent.

Further, let $f(x) = f_1(x)f_2(x)\cdots f_s(x)$ be a product of distinct non associated irreducible polynomials over $F$. Denote by $g(x) = f_1(x)\cdots f_k(x)$ the product of all factors of $f(x)$, not having multiple roots. When $k = 0$ we put $g(x) = 1$. If $k < s$, let $d(x) = f_{k+1}(x)f_{k+2}(x)\cdots f_s(x)$ be the product of all factors of $f(x)$ which have multiple roots. This happens if $p > 0$ and $F$ is not perfect field (see ([2] p. 138). In such case $f_i(x) = \varphi_i(x^p)$, where $\varphi_i(x) \in F[x]$ for $i = k+1, k+2, \ldots, s$. When $k = s$ we put $d(x) = 1$. Thus $f(x) = g(x)d(x)$ and either $d(x) = 1$, or $d(x) = \varphi(x^p)$ with $\varphi(x) \in F[x]$ and $\deg\varphi(x) \geq 1$ (see [6] p. 162). Therefore we have $d'(x) = 0$. Since $f'(x) = g'(x)d(x)$ and $(g, g') = 1$, it is clear that $d(x) = (f, f')$. So we see that (ii) and (iii) are equivalent, as was to be shown. □

As an immediate consequence we obtain

**Corollary 3.** *Let $F$ be a field and let $f(x) \in F[x]$ be a nonzero polynomial.*

(i) *If $\Delta(f) \neq 0$, then the quotient ring $F[x]/f(x)F[x]$ is reduced.*

(ii) *If $F$ is a perfect field, then the ring $F[x]/f(x)F[x]$ is reduced if and only if $\Delta(f) \neq 0$.*

Really, it is sufficient to observe that the conditions $(f, f') = 1$ and $\Delta(f) \neq 0$ are equivalent.

Now let $A$ be a reduced commutative ring and let $f(x) \in A[x]$ be a minimal polynomial of the algebraic element $\alpha$. As was mentioned above, it is sufficient to find necessary and sufficient conditions under which $A[\alpha]$ is reduce, when $A$ is a noetherian ring.

**Theorem 1.** *Let $A$ be a reduced commutative noetherian ring with classical ring of quotients $P = Q(A)$ and let $\alpha$ be an algebraic element over $A$ with a minimal polynomial $f(x) \in A[x]$. If $f(x)$ is a regular polynomial over $A$, then the following statements are equivalent:*

(i) *The ring $A[\alpha]$ is reduced.*

(ii) *For every regular element $a \in A$ the polynomial $af(x)$ is not divisible by squares of polynomials over $A$ of degree $t \geq 1$.*

(iii) *For every minimal idempotent $e \in P$ the polynomial $ef(x)$ is a product of distinct non associated irreducible polynomials over the field $eP$.*

(iv) *For every minimal idempotent $e \in P$, either $(ef, ef') = e$, or $eP$ is a field of characteristic $p > 0$, $eP$ is not a perfect field and $(ef, ef')$ is a product of distinct non associated irreducible polynomials of the form $\varphi(x^p) \in eP[x]$.*

*Proof.* Suppose that $A \subseteq K$ and $\alpha \in K$. By Lemma 3, without loss of generality, we may assume that $P = Q(A) \subseteq K$. Since $A$ is a reduced commutative notherian ring, by Goldie's Theorem (see [1], Corollary 2, p. 323), the ring $P$ is a finite direct sum

$$P = A_1 \oplus A_2 \oplus \cdots \oplus A_k$$

of fields $A_i$ with identity elements $e_i$ ($i = 1, \dots, k$). Then $A_i = e_i P$ and it is clear that $f_i(x) = e_i f(x)$ is a minimal polynomial of $\alpha$ over the field $A_i$ for $i = 1, \dots, k$. Moreover,

$$A[\alpha] \subseteq P[\alpha] = A_1[\alpha] \oplus A_2[\alpha] \oplus \cdots \oplus A_k[\alpha]$$

and $P[\alpha] \cong P[x]/f(x)P[x]$. Thus, by Lemma 4(ii) we obtain that $A[\alpha]$ is reduced if and only if the rings $A_1[\alpha], A_2[\alpha], \dots, A_k[\alpha]$ are reduced. Hence, by Lemma 5 we conclude that the statements (i), (iii) and (iv) are equivalent. Therefore it is sufficient to prove that (i) and (ii) are equivalent.

Really, suppose that $A[\alpha]$ is a reduced ring but $af(x) = p^2(x)q(x)$ for some regular element $a \in A$, where $p(x)$, $q(x) \in A[x]$ and $\deg p(x) \geq 1$. Then

$$p(x) = e_1 p(x) + e_2 p(x) + \cdots + e_k p(x)$$

and without loss of generality we may assume that $\deg e_1 p(x) \geq 1$. Thus the equality $af(x) = p^2(x)q(x)$ shows that

$$e_1 a f(x) = (e_1 p(x))^2 e_1 q(x)$$

and

$$1 \leq \deg(e_1 p(x) q(x)) < \deg(e_1 a f(x)) = \deg f_1(x),$$

where $f_1(x) = e_1 f(x)$. Therefore, $e_1 p(x) q(x) + f_1(x) A_1[x]$ is a nonzero nilpotent element of the quotient ring $A_1[x]/f_1(x)A_1[x]$. As far as $f_1(x)$ is a minimal polynomial of $\alpha$ over $A_1$, by Corollary 2 we receive that $A_1[\alpha]$ is not reduced, which is impossible. Conversely, if $A[\alpha]$ is not reduced ring, then $P[\alpha]$ is not reduced and without loss of generality we may assume that $A_1[\alpha]$ is not reduced. Then by Corollary 2 and Lemma 5 we obtain that $f_1(x) = p_1^2(x) q_1(x)$, where $p_1(x)$, $q_1(x) \in A_1[x]$ and $\deg p_1(x) \geq 1$. Now we put

$$p(x) = p_1(x) + e_2 + \cdots + e_k,$$
$$q(x) = q_1(x) + f_2 + \cdots + f_k$$

and thus we receive $f(x) = p^2(x)q(x)$, where $p(x)$, $q(x) \in P[x]$ and $\deg p(x) \geq 1$. Since P is a ring of quotients, it follows that there exist regular elements $b, c \in A$ such that $bp(x)$ and $cq(x)$ are elements of $A[x]$. Then $a = b^2 c$ is a regular element in $A$ and $af(x)$ is divisible by the square of $bp(x) \in A[x]$, as was to be showed.

As was mentioned above, the main result of [11] asserts that if $\Delta(f)$ is a regular element in $A$, then $A[\alpha]$ is a reduced ring. But $A[\alpha]$ may be reduced even when $\Delta(f) = 0$. Indeed, let $\alpha$ be a root of the polynomial $f(x) = x^p - y \in A[x]$, where $A = F(y)$ is the ring of quotients of the polynomial ring $F[y]$ over a field $F$ of characteristic $p > 0$. Then $\Delta(f) = 0$,

$f(x)$ is irreducible over $A$ (see [2], p. 165) and $A[\alpha]$ is reduced by Corollary 2 and Lemma 5. □

We shall say that the reduced commutative ring $A$ is locally perfect if for every finitely generated subring $B \subseteq A$ and every minimal idempotent $e \in Q(B)$ the field $eQ(B)$ is perfect. If the additive group of the reduced ring $A$ is either torsion free, or locally finite, then $A$ is a locally perfect ring. Thus we have the following

**Corollary 4.** *Let $\alpha$ be an algebraic element over the commutative ring $A$ with a regular minimal polynomial $f(x) \in A[x]$ and let $\Delta(f)$ be the discriminant of $f(x)$.*

(i) *If $\Delta(f)$ is a regular element in $A$, then the ring $A[\alpha]$ is reduced if and only if $A$ is reduced.*

(ii) *If $A$ is a reduced locally perfect ring, then $A[\alpha]$ is reduced if and only if $\Delta(f)$ is a regular element in $A$.*

*Proof.* (i) Assume that $A$ is reduced and $\Delta(f)$ is regular in $A$, but $A[\alpha]$ is not reduced. If $\beta$ is a nonzero nilpotent element of $A[\alpha]$, then let $B$ be the subring of $A$, generated by the coefficients of $\beta$ and $f(x)$. Thus $f(x) \in B[x]$ and $\beta \in B[\alpha]$. Hence by the preceding theorem it follows that for some minimal idempotent $e \in Q(B)$ the polynomial $ef(x)$ has multiple roots and therefore $\Delta(ef) = 0$. Since $\Delta(ef) = e\Delta(f)$, we obtain that the element $\Delta(f)$ is a proper divisor of zero, which is a contradiction. As far as the converse statement is trivial, the part (i) is proved.

(ii) In view of (i) it is sufficient to prove that if $A[\alpha]$ is reduced, then $\Delta(f)$ is regular. Assume for moment that $\Delta(f)a = 0$ and $0 \neq a \in A$. Let $B$ be the finitely generated subring of $A$, generated by the coefficients of $f(x)$ and the element $a \in A$. Thus $f(x) \in B[x]$ and $a \in B$. Let $e_1, e_2, \ldots, e_n$ be a full orthogonal system minimal idempotents of $Q(B)$. Then

$$\Delta(f) = \Delta(e_1 f) + \Delta(e_2 f) + \cdots + \Delta(e_n f),$$

where $\Delta(e_i f) \in e_i Q(B)$ for $i = 1, 2, \ldots, n$. Since each $e_i Q(B)$ is a field and $\Delta(f)$ is a proper divisor of zero in $B$, we conclude that for some $i$ $(1 \leq i \leq n)$ we have $\Delta(e_i f) = 0$. This implies that $e_i f(x)$ has multiple roots. But $e_i Q(B)$ is a perfect field and by Corollary 2 and Lemma 5 we obtain that $e_i Q(B)[\alpha]$ is not reduced and therefore $Q(B)[\alpha]$ is not reduced ring, which is a contradiction. So the proof is completed. □

Let $K$ be any ring extension of the commutative ring $A$ where $K$ is not necessary commutative. If the element $\alpha \in K$ centralizes $A$, that is $\alpha.a = a.\alpha$ for all $a \in A$, then we may to consider the simple commutative ring extension $A[\alpha]$. So we have the following

**Corollary 5.** *Let $F$ be a perfect field and let $S$ be an element of the $n \times n$ matrix ring $M(n, F)$. If $F$ contains all characteristic values of $S$, then the* *ring $F[S]$ is reduced if and only if for some non-singular matrix $T \in M(n, F)$ the matrix $TST^{-1}$ is diagonal.*

*Proof.* By Corollary 2 and Corollary 3(ii) the ring $F[S]$ is reduced if and only if $\Delta(f) \neq 0$ where $f = f(\lambda)$ is the minimal polynomial of $S$ in $F[\lambda]$. Since $f(\lambda)$ is the last invariant factor of the characteristic matrix $S - \lambda E$ (see [5], p. 389), this condition is equivalent with the condition the Jordan's normal form of $S$ to be diagonal. □

## 4. SIMPLE ALGEBRAIC EXTENSIONS OF IRREDUCIBLE COMMUTATIVE RINGS

In this part we shall study the problem who the ring $A[\alpha]$ contains nontrivial idempotent elements. Later on we shall say that the idempotent $E$ of the ring $A[\alpha]$ (respectively of $A[x]/f(x)A[x]$) is a trivial idempotent if $E$ is an element of the subring $A$ (respectively of the subring $(A+f(x)A[x])/f(x)A[x]$).

As usually we shall say that the polynomial $p(x) \in A[x]$ divides the polynomial $f(x) \in A[x]$ over the ring $A$ if there exists a polynomial $q(x) \in A[x]$ such that $f(x) = p(x)q(x)$. The polynomial $p(x) \in A[x]$ is said to be a trivial divisor of $f(x)$ if $p(x)$ divides $f(x)$ and there exists an element $a \in A$ such that

$$p(x) + f(x)A[x] = a + f(x)A[x],$$

that is $f(x)$ divides $p(x) - a$ over $A$. For example, if $e \in A$ is a nontrivial idempotent of $A$, then every polynomial $f(x) \in A[x]$ has a trivial decomposition

$$f(x) = [ef(x) + (1 - e)][e + (1 - e)f(x)].$$

The decomposition $f(x) = p(x)q(x)$ over $A$ is said to be nontrivial decomposition if over $A$ the polynomials $p(x)$ and $q(x)$ are nontrivial divisors of $f(x)$. Also, the decomposition $f(x) = p(x)q(x)$ is an essential decomposition over $A$ if $p(x)$ and $q(x)$ are nontrivial divisors of $f(x)$ and $\deg p(x) < \deg f(x)$, $\deg q(x) < \deg f(x)$. We shall say that the polynomial $f(x)$ is irreducible over the ring $A$ if $f(x)$ has no nontrivial decomposition over $A$.

Recall that if $F$ is a field and $\varphi(x), \psi(x) \in F[x]$, then for the greatest common divisor $(\varphi, \psi)$ there exist polynomials $u(x), v(x) \in F[x]$ such that

$$(\varphi, \psi) = u(x)\varphi(x) + v(x)\psi(x)$$

and $\deg u(x) < \deg \psi(x)$, $\deg v(x) < \deg \varphi(x)$. Likewise, if $A$ is any commutative ring and $\varphi(x), \psi(x) \in A[x]$, then by Lemma 1 it follows that for the resultant $R(\varphi, \psi)$ there exist polynomials $u(x), v(x) \in A[x]$ such that

$$R(\varphi, \psi) = u(x)\varphi(x) + v(x)\psi(x) \in A$$

and $\deg u(x) < \deg \psi(x)$, $\deg v(x) < \deg \varphi(x)$. From here on we shall use these facts without special stipulations.

Let $f(x)$ be a minimal polynomial over the field $F$ of the algebraic element $\alpha$. Since the rings $F[\alpha]$ and $F[x]/f(x)F[x]$ are isomorphic, by Chain's theorem it follows that $F[\alpha]$ contains nontrivial idempotents if and only if $f(x)$ is not associated with a power of some irreducible polynomial over $F$. Now we shall prove the following lemma, which gives the idempotents of $F[\alpha]$ in explicit form.

**Lemma 6.** *Let $\alpha$ be an algebraic element over the field $F$ with a minimal polynomial $f(x) \in F[x]$. Then*

(i) *The ring $F[\alpha]$ is irreducible if and only if $f(x)$ is associated with a power of an irreducible polynomial of $F[x]$.*

(ii) *The elements $E_1(\alpha)$ and $E_2(\alpha)$ of $F[\alpha]$ form a full orthogonal system idempotents if and only if over $F$ there exists a decomposition $f(x) = \varphi(x)\psi(x)$ such that*

$$(\varphi, \psi) = u(x)\varphi(x) + v(x)\psi(x) = 1,$$

*where* $\deg(u(x)\varphi(x)) < \deg f(x)$ *and*

$$E_1(\alpha) = u(\alpha)\varphi(\alpha), \qquad E_2(\alpha) = v(\alpha)\psi(\alpha).$$

(iii) *The elements $E_1(\alpha)$ and $E_2(\alpha)$ of $F[\alpha]$ form a nontrivial full orthogonal system idempotents if and only if over $F$ there exists an essential decomposition $f(x) = \varphi(x)\psi(x)$ such that*

$$R(\varphi, \psi) = u_1(x)\varphi(x) + v_1(x)\psi(x) \neq 0$$

*and*

$$E_1(\alpha) = R(\varphi, \psi)^{-1}u_1(\alpha)\varphi(\alpha), \qquad E_2(\alpha) = R(\varphi, \psi)^{-1}v_1(\alpha)\psi(\alpha).$$

*Proof.* (i) Let $F[\alpha]$ be an irreducible ring and let

$$f(x) = ap_1^{k_1}(x)p_2^{k_2}(x)\cdots p_s^{k_s}(x)$$

be the canonical decomposition of $f(x)$ over the field $F$. Since $F[\alpha]$ and $F[x]/f(x)F[x]$ are isomorphic rings, by the Chinese theorem we obtain that $f(x) = ap_1^{k_1}(x)$ and therefore $f(x)$ is associated with a power of irreducible polynomial over $F$. Conversely, if $f(x)$ is associated with a power of an irreducible polynomial over $F$ and $f(x) = ap^k(x)$, then $f(x)F[x] = p^k(x)F[x]$ and $p(x)F[x]/p^k(x)F[x]$ is a nilideal of $F[x]/p^k(x)F[x]$. Since

$$\left(F[x]\Big/p^k(x)F[x]\right)\Big/\left(p(x)F[x]\Big/p^k(x)F[x]\right) \cong F[x]/p(x)F[x]$$

and $F[x]/p(x)F[x]$ is a field, by [4], Proposition 11.5.1 we conclude that (i) follows.

(ii)Suppose that the elements $E_1(\alpha)$ and $E_2(\alpha)$ form a full orthogonal system idempotents of $F[\alpha]$. Since the rings $F[\alpha]$ and $\bar{F}[x] = F[x]/f(x)F[x]$ are isomorphic, it follows that in $\bar{F}[x]$ there exist elements

$$\bar{E}_1(x) = e_1(x) + f(x)F[x], \qquad \bar{E}_2(x) = e_2(x) + f(x)F[x]$$

such that $\bar{E}_1(x)$ and $\bar{E}_2(x)$ form a full orthogonal system idempotents of $\bar{F}[x]$ and $e_1(\alpha) = E_1(\alpha)$, $e_2(\alpha) = E_2(\alpha)$. Without loss of generality we may to assume that $\deg e_i(x) < \deg f(x)$ for $i = 1, 2$. Obviously, $\bar{E}_1(x)$ and $\bar{E}_2(x)$ form a full orthogonal system idempotents if and only if $e_1(x) + e_2(x) = 1$ and $e_1(x)e_2(x) = f(x)q(x)$ for some $q(x) \in F[x]$. If $\bar{E}_1(x)$ and $\bar{E}_2(x)$ form a trivial system orthogonal idempotents of $\bar{F}[x]$ and $e_1(x) = 0$, $e_2(x) = 1$, then we put $\varphi(x) = f(x)$, $\psi(x) = 1$ and $u(x) = 0$, $v(x) = 1$. Suppose that $\bar{E}_1(x)$ and $\bar{E}_2(x)$ form a nontrivial system orthogonal idempotents. Since $F[x]$ is a factorial ring (see [8], p. 142), we conclude that

$$f(x) = \varphi(x)\psi(x), \qquad e_1(x) = u(x)\varphi(x), \qquad e_2(x) = v(x)\psi(x),$$

where $\varphi(x) = (e_1, f)$ and $\psi(x) = (e_2, f)$. Moreover, the polynomials $u(x)$ and $v(x)$ in $F[x]$ are uniquely determined. Since the converse statement is trivial, so (ii) is proved.

(iii) When $\bar{E}_1(x)$ and $\bar{E}_2(x)$ form a nontrivial system orthogonal idempotents of $\bar{F}[x]$, it is clear that $0 < \deg e_i(x) < \deg f(x)$ for $i = 1, 2$. Thus we obtain that the decomposition $f(x) = \varphi(x)\psi(x)$ is nontrivial and therefore $\deg \varphi(x) \geq 1$, $\deg \psi(x) \geq 1$. As far $e_1(x) + e_2(x) = 1$, we have $(\varphi, \psi) = 1$ and hence we receive

$$R(\varphi, \psi) = u_1(x)\varphi(x) + v_1(x)\psi(x) \neq 0,$$

where, by Lemma 1, $\deg u_1(x) < \deg \psi(x)$ and $\deg v_1(x) < \deg \varphi(x)$. Now it is easy to verify that $u(x) = R(\varphi, \psi)^{-1}u_1(x)$ and $v(x) = R(\varphi, \psi)^{-1}v_1(x)$. So we prove and the statement (iii). □

The following lemma is an analog of the parts (ii) and (iii) of the preceding lemma for commutative artinian rings.

**Lemma 7.** *Let $\alpha$ be an algebraic element over the reduced commutative artinian ring $A$ with a regular minimal polynomial $f(x) \in A[x]$. Then*

(i) *The element $E(\alpha)$ is a nontrivial idempotent in $A[\alpha]$ if and only if over $A$ there exists a nontrivial decomposition $f(x) = \varphi(x)\psi(x)$ such that*

$$u(x)\varphi(x) + v(x)\psi(x) = 1$$

*for some polynomials $u(x)$ and $v(x)$ of $A[x]$, where* $\deg(u(x)\varphi(x)) < \deg f(x)$ *and $E(\alpha) = u(\alpha)\varphi(\alpha)$.*

(ii) *The ring $A[\alpha]$ contains nontrivial idempotents if and only if for some nonzero idempotent $e \in A$ over the ring $eA$ there exists an essential decomposition $ef(x) = \varphi(x)\psi(x)$ such that $R(\varphi, \psi)$ is a nonzero element of $eA$.*

*Proof.* By Wedderburn-Artin theorem, $A = F_1 \oplus F_2 \oplus \cdots \oplus F_m$ is a finite direct sum of fields $F_i$ with identity elements $e_i$ $(i = 1, \ldots, m)$. So we have the decomposition

$$A[\alpha] = F_1[\alpha] \oplus F_2[\alpha] \oplus \cdots \oplus F_m[\alpha].$$

(i) Suppose that $E(\alpha)$ is a nontrivial idempotent of $A[\alpha]$. Then the elements $E_1(\alpha) = E(\alpha)$ and $E_2(\alpha) = 1 - E(\alpha)$ have the decompositions

$$E_k(\alpha) = E_{k1}(\alpha) + E_{k2}(\alpha) + \cdots + E_{km}(\alpha) \qquad (k = 1, 2), \tag{6}$$

where $E_{1i}(\alpha)$ and $E_{2i}(\alpha)$ form a full orthogonal system idempotents of $F_i[\alpha]$. Obviously $f_i(x) = e_i f(x)$ is a minimal polynomial of $\alpha$ over the field $F_i = e_i A$ for all $i = 1, 2, \ldots, m$. By Lemma 6(ii) it follows that over $F_i$ there exists a decomposition $e_i f(x) = \varphi_i(x)\psi_i(x)$ such that

$$(\varphi_i, \psi_i) = u_i(x)\varphi_i(x) + v_i(x)\psi_i(x) = e_i,$$

where $\deg(u_i(x)\varphi_i(x)) < \deg f(x)$ and

$$E_{1i}(\alpha) = u_i(\alpha)\varphi_i(\alpha), \qquad E_{2i}(\alpha) = v_i(\alpha)\psi_i(\alpha)$$

for $i = 1, 2, \ldots, m$. Then $f(x) = \varphi(x)\psi(x)$, where

$$\varphi(x) = \varphi_1(x) + \varphi_2(x) + \cdots + \varphi_m(x),$$
$$\psi(x) = \psi_1(x) + \psi_2(x) + \cdots + \psi_m(x).$$

Moreover, $u(x)\varphi(x) + v(x)\psi(x) = 1$, where

$$u(x) = u_1(x) + u_2(x) + \cdots + u_m(x),$$
$$v(x) = v_1(x) + v_2(x) + \cdots + v_m(x).$$

Obviously, $\deg(u(x)\varphi(x)) < \deg f(x)$ and $E(\alpha) = u(\alpha)\varphi(\alpha)$. Since the converse statement is evident, so (i) is proved.

(ii) If $E(\alpha)$ is a nontrivial idempotent of $A[\alpha]$, then again we put $E_1(\alpha) = E(\alpha)$ and $E_2(\alpha) = 1 - E(\alpha)$. Suppose that $E_1(\alpha)$ and $E_2(\alpha)$ have the decompositions (6). Without loss of generality we may to assume that $E_{11}(\alpha)$ and $E_{21}(\alpha)$ form a full nontrivial orthogonal system idempotents of $F_1[\alpha]$, where $f_1(x) = ef(x)$ is a minimal polynomial of $\alpha$ over the field $F_1 = eA$ and $e = e_1$. Then by Lemma 6(ii), over $F_1$ there exists an essential decomposition $ef = \varphi(x)\psi(x)$ such that $R(\varphi, \psi) \neq 0$.

Conversely, if for some idempotent $e \in A$ over the ring $eA$ there exists an essential decomposition $ef(x) = \varphi(x)\psi(x)$ such that $R(\varphi, \psi) \neq 0$, we shall have the decompositions

$$\varphi(x) = \varphi_1(x) + \varphi_2(x) + \cdots + \varphi_m(x),$$
$$\psi(x) = \psi_1(x) + \psi_2(x) + \cdots + \psi_m(x),$$

where $\varphi_i(x) = e_i\varphi(x)$ and $\psi_i(x) = e_i\psi(x)$ for $i = 1, \ldots, m$. Since

$$R(\varphi, \psi) = R(\varphi_1, \psi_1) + R(\varphi_2, \psi_2) + \cdots + R(\varphi_m, \psi_m) \neq 0,$$

it follows that for some $k\,(1 \leq k \leq m)$ we have $R(\varphi_k, \psi_k) \neq 0$. Then

$$e_k e f(x) = e_k f(x) = \varphi_k(x)\psi_k(x)$$

is an essential decomposition over the field $F_k$ and by Lemma 6(ii) it follows that $F_k[\alpha]$ contains nontrivial idempotents. Since $F_k[\alpha] \subseteq A[\alpha]$, we conclude that $A[\alpha]$ contains nontrivial idempotents, as was to be shoved. □

Let $I$ be an ideal of $A$ and let $I[\alpha]$ be the simple algebraic extension of $I$, which is obtained by adjoining of $\alpha$ to $I$. As for $A[x]/f(x)A[x]$, we shall say that an idempotent $E$ of the ring $A[\alpha]/I[\alpha]$ is trivial if $E$ is an element of the subring $(A + I[\alpha])/I[\alpha]$.

**Lemma 8.** *Let $A[\alpha]$ be any simple ring extension of the commutative ring $A$ and let $I$ be a nil-ideal of $A$.*

(i) *All idempotents of $A[\alpha]$ are trivial if and only if all idempotents of the quotient ring $A[\alpha]/I[\alpha]$ are trivial.*

(ii) *If $\alpha$ is an algebraic element over the ring $A$ with a regular minimal polynomial*

$$f\,(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \qquad (n \geq 1),$$

*then there exists a simple algebraic extension $\bar{A}[\beta]$ of the quotient ring $\bar{A} = A/I$, such that $A[\alpha]/I[\alpha] \cong \bar{A}[\beta]$ and*

$$\bar{f}(x) = \bar{a}_0x^n + \bar{a}_1x^{n-1} + \cdots + \bar{a}_{n-1}x + \bar{a}_n \qquad (\bar{a}_k = a_k + I)$$

*is a regular minimal polynomial over $\bar{A}$ of the element $\beta$.*

*Proof.* (i) Suppose that all idempotents of $A[\alpha]$ are trivial and let $E(\alpha) = u(\alpha) + I[\alpha]$ be an idempotent of $A[\alpha]/I[\alpha]$. Then $u(\alpha)^2 - u(\alpha) \in I[\alpha]$ and, since $I[\alpha]$ is a nil-ideal of $A[\alpha]$, by ([4], Proposition 11.5.1) it follows that there exists an idempotent $e(\alpha) \in A[\alpha]$ such that $e(\alpha) - u(\alpha) \in I[\alpha]$. Therefore $E(\alpha) = e(\alpha) + I[\alpha]$ and, since all idempotents of $A[\alpha]$ are trivial, we have $e(\alpha) = e \in A$. So we conclude that all idempotents of $A[\alpha]/I[\alpha]$ are trivial. Conversely, assume that all idempotents of $A[\alpha]/I[\alpha]$ are trivial. If $e(\alpha)$ is an idempotent of $A[\alpha]$, then $e(\alpha) + I[\alpha]$is a trivial idempotent of $A[\alpha]/I[\alpha]$ and hence for some element $a \in A$ we have $e(\alpha) + I[\alpha] = a + I[\alpha]$. Since $e(\alpha)^2 - e(\alpha) = 0$, we obtain that $a^2 - a \in I$. Then again by ([4], Proposition 11.5.1) we obtain that there exists an idempotent $e \in A$, such that $a - e \in I$. As far $I \subseteq I[\alpha]$, we receive

$$e(\alpha) + I[\alpha] = e + I[\alpha].$$

Suppose that $e(\alpha) = e + v(\alpha)$, where $v(\alpha) \in I[\alpha]$ is a nilpotent element. Then $e(\alpha)e = e + v(\alpha)e$ is an invertible element of the ring $eA[\alpha]$. But $e(\alpha)e$ is simultaneously an idempotent of $eA[\alpha]$. Thus we obtain that $e(\alpha)e = e$ and $v(\alpha)e = 0$. Now $e(\alpha)(1 - e) = v(\alpha)(1 - e)$ is simultaneously an idempotent

and a nilpotent element of $(1-e)A[\alpha]$. So we conclude that $v(\alpha)(1-e)=0$ and hence
$$v(\alpha)=v(\alpha)e+v(\alpha)(1-e)=0.$$
Therefore $e(\alpha)=e$ is a trivial idempotent of $A[\alpha]$ and thus (i) is proved.

(ii) Obviously, $A[\alpha]\Big/I[\alpha]=\tilde{A}[\tilde{\alpha}]$ is a simple ring extension of the subring $\tilde{A}=(A+I[\alpha])/I[\alpha]$, obtained by adjoining of the element $\tilde{\alpha}=\alpha+I[\alpha]$ to $\tilde{A}$ . Since $f(\alpha)=0$, it is clear that $\tilde{\alpha}$ is a root of
$$\tilde{f}(x)=\tilde{a}_0x^n+\tilde{a}_1x^{n-1}+\cdots+\tilde{a}_{n-1}x+\tilde{a}_n \qquad (\tilde{a}_k=a_k+I[\alpha]).$$
Therefore $\tilde{A}[\tilde{\alpha}]$ is a simple algebraic extension of $\tilde{A}$. If
$$\tilde{g}(x)=\tilde{b}_0x^m+\tilde{b}_1x^{m-1}+\cdots+\tilde{b}_{m-1}x+\tilde{b}_m \qquad (\tilde{b}_k=b_k+I[\alpha]\in\tilde{A})$$
is a minimal nonzero polynomial of $\tilde{\alpha}$ over $\tilde{A}$, then $b_0\notin I$ and $m\le n$. Suppose that $m<n$. As far $\tilde{g}(\tilde{\alpha})=g(\alpha)+I[\alpha]=I[\alpha]$, we conclude that
$$\begin{aligned} g(\alpha)&=b_0\alpha^m+b_1\alpha^{m-1}+\cdots+b_{m-1}\alpha+b_m\\ &=c_0\alpha^s+c_1\alpha^{s-1}+\cdots+c_{s-1}\alpha+c_s \qquad (c_k\in I),\end{aligned}$$
where $b_0\ne c_0$. Now we use the fact that $a_0$ is an invertible element in the ring of quotients $Q(A)$ and $f(\alpha)=0$. So without loss of generality we may to suppose that $s<n$ and $c_0,c_1,\dots,c_s\in\mathfrak{Nil}Q(A)$. Therefore there exists a regular element $a\in A$ such that $ab_i\in A$ $(i=1,\dots,m)$ and $ac_j\in I$ $(j=1,\dots,s)$. Thus we obtain that $\alpha$ is a root of a nonzero polynomial of degree $t=\min\{m,s\}<n$, which is impossible. Hence $m=n$ and $\tilde{f}(x)$ is a minimal polynomial of $\tilde{\alpha}$ over$\tilde{A}$. By a similar way we prove that $A\bigcap I[\alpha]=I$. Then it is easy to verify that $\tilde{a}_0$ is a regular element of $\tilde{A}$. Moreover,
$$\tilde{A}=(A+I[\alpha])/I[\alpha]\cong A\Big/(A\bigcap I[\alpha])=A/I=\bar{A}.$$
Let $\bar{f}(x)$ be a minimal polynomial of some element $\beta$ over the ring $\bar{A}$. Then the mapping $\tilde{A}[\tilde{\alpha}]\to\bar{A}[\beta]$, defined by $\tilde{\alpha}\mapsto\beta$ and $a+I[\alpha]\mapsto a+I$ for $a\in A$ is an isomorphism, as was to be showed. □

Now by Lemma 8(ii) we shall prove following theorem.

**Theorem 2.** *Let $\alpha$ be an algebraic element over an artinian commutative ring $A$ with a regular minimal polynomial $f(x)\in A[x]$. If $\bar{A}=A/\mathfrak{Nil}A$ and $\bar{f}(x)$ is the natural image of $f(x)$ into $\bar{A}[x]$, then*

(i) *$A[\alpha]$ is irreducible if and only if $\bar{A}$ is a field and $\bar{f}(x)$ is associated with a power of some irreducible polynomial over $\bar{A}$.*

(ii) *$A[\alpha]$ contains only trivial idempotents if and only if for every minimal idempotent $\bar{e}\in\bar{A}$ the polynomial $\bar{e}\bar{f}(x)$ is associated with a power of some irreducible polynomial over the field $\bar{e}\bar{A}$.*

*Proof.* If $A$ is an artinian commutative ring, then $\bar{A} = A/\mathfrak{Nil}A$ is a finite direct sum of fields [6, 7]. Since $A$ is irreducible if and only if $\bar{A}$ is irreducible, by Lemma 8 we obtain that $A[\alpha]$ is irreducible if and only if $\bar{A}[\beta]$ is irreducible, where $\bar{A}$ is a field and $\bar{f}(x)$ is a regular minimal polynomial of $\beta$ over the field $\bar{A}$. Then the statement (i) follows by Lemma 7(i). Again by Lemma 8 it follows that $A[\alpha]$ contains only trivial idempotents if and only if $\bar{A}[\beta]$ contains only trivial idempotents. Since $\bar{A}$ is a finite direct sum of fields, by Lemma 7(i) we conclude that for every minimal idempotent $\bar{e} \in \bar{A}$ the ring $\bar{e}\bar{A}[\beta]$ contains only trivial idempotents. So by Lemma 8 we obtain and the statement (ii). □

**Theorem 3.** *Let $\alpha$ be an algebraic element over a commutative noetherian ring $A$ with a monic minimal polynomial $f(x) \in A[x]$ and let $P = Q(\bar{A})$ be the ring of quotients of $\bar{A} = A/\mathfrak{Nil}A$. The ring $A[\alpha]$ contains nontrivial idempotents if and only if over the ring $\bar{P}$ there exists a nontrivial decomposition $\bar{f}(x) = \bar{\varphi}(x)\bar{\psi}(x)$ such that $\bar{u}(x)\bar{\varphi}(x) + \bar{v}(x)\bar{\psi}(x) = \bar{1}$ for some polynomials $\bar{u}(x), \bar{v}(x) \in P[x]$, where $\deg(\bar{u}(x)\bar{\varphi}(x)) < \deg \bar{f}(x)$ and $\bar{u}(x)\bar{\varphi}(x) \in \bar{A}[x]$.*

*Proof.* Suppose that $A[\alpha]$ contains a nontrivial idempotent $E(\alpha)$. Then by Lemma 8(i) it follows that $E(\alpha) + I[\alpha]$ is a nontrivial idempotent of $A[\alpha]/I[\alpha]$, where $I = \mathfrak{Nil}A$. Now by Lemma 8(ii) we conclude that there exists a nontrivial idempotent $\bar{E}(\beta)$ of the ring $\bar{A}[\beta]$, where $\bar{f}(x) \in \bar{A}[x]$ is a minimal polynomial of $\beta$. Without loss of generality, by Lemma 3 we may assume that $\bar{E}(\beta)$ is a nontrivial idempotent of $P[\beta]$. Since $P$ is a reduced artinian ring, by Lemma 7(i) we conclude that over the ring $P$ there exists a nontrivial decomposition $\bar{f}(x) = \bar{\varphi}(x)\bar{\psi}(x)$ such that $\bar{u}(x)\bar{\varphi}(x) + \bar{v}(x)\bar{\psi}(x) = \bar{1}$ for some polynomials $\bar{u}(x)$ and $\bar{v}(x)$ of $P[x]$, where $\deg(\bar{u}(x)\bar{\varphi}(x)) < \deg \bar{f}(x)$ and $\bar{E}(\beta) = \bar{u}(\beta)\bar{\varphi}(\beta) \in \bar{A}[\beta]$. Since $\bar{f}(x) \in \bar{A}[x]$ is a monic minimal polynomial of $\beta$ over $\bar{A}$ and $\deg(\bar{u}(x)\bar{\varphi}(x)) < \deg \bar{f}(x)$, it is clear that $\bar{E}(\beta) = \bar{u}(\beta)\bar{\varphi}(\beta) \in \bar{A}[\beta]$ implies $\bar{u}(x)\bar{\varphi}(x) \in \bar{A}[x]$.

Conversely, suppose that the polynomial $f(x) \in A[x]$ satisfy the conditions of the theorem and let $g(x)$ be a polynomial in $A[x]$ such that $\bar{g}(x) = \bar{u}(x)\bar{\varphi}(x)$. If $\beta$ is an algebraic element over $\bar{A}$ with a minimal polynomial $\bar{f}(x) \in \bar{B}[x]$, then by Lemma 8(ii) it follows that $A[\alpha]/I[\alpha]$ and $\bar{A}[\beta]$ are isomorphic rings. Since $\bar{g}(\beta) = \bar{u}(\beta)\bar{\varphi}(\beta)$ is a nontrivial idempotent in $\bar{A}[\beta]$, the element $g(\alpha) + I[\alpha]$ is a nontrivial idempotent in $A[\alpha]/I[\alpha]$ (see the proof of Lemma 8(ii)). If $u = g^2(\alpha) - g(\alpha)$, then by Proposition 3.6.1 [7] we conclude that $E(\alpha) = g(\alpha) - x[1 - 2g(\alpha)]$ is a nontrivial idempotent of $A[\alpha]$, where

$$x = \frac{1}{2}\left(2u - \begin{pmatrix} 4 \\ 2 \end{pmatrix} u^2 + \begin{pmatrix} 6 \\ 3 \end{pmatrix} u^3 - \cdots\right).$$

So the theorem is proved. □

It is easy to verify that in the preceding theorem the condition $f(x)$ to be a monic polynomial is not necessary. Really, let $f(x) = 4x^2 - 1$ be a minimal polynomial of the algebraic element $\alpha$ over the integer ring $\mathbb{Z}$. Then $f(x) = (2x-1)(2x+1)$ is a nontrivial decomposition over the field $\mathbb{Q} = Q(\mathbb{Z})$ and $2^{-1}(2x+1) - 2^{-1}(2x-1) = 1$. Thus $e(x) = 2^{-1}(2x+1) = x + 2^{-1}$ is not element of $\mathbb{Z}[x]$, but

$$e(\alpha) = \alpha + 2^{-1} = \alpha + 2\alpha^2$$

is an idempotent of $\mathbb{Z}[\alpha]$.

For regular minimal polynomials we have the following

**Corollary 6.** *Let $A$ be a commutative noetherian ring and let $P = Q(\bar{A})$ be the ring of quotients of $\bar{A} = A/\mathfrak{Nil}A$. Suppose that $f(x)$ is a regular minimal polynomial of an algebraic element $\alpha$ over the ring $A$. If for every minimal idempotent $e \in P$ the polynomial $ef(x)$ is associated with a power of some irreducible polynomial over the field $eP$, then all idempotents of the ring $A[\alpha]$ are trivial.*

The proof of this corollary is as the proof of Theorem 3.

## References


[1] V. A. Andrunakievič and J. M. Rjabuhin, *Radikaly algebr i strukturnaya teoriya*, Sovremennaya Algebra [Contemporary Algebra], "Nauka", Moscow, 1979.

[2] N. Burbaki, *Algebra. Mnogochleny i polya. Uporyadochennye gruppy.* Elements of Mathematics, Translated from the French by V. E. Govorov, J u. I. Manin, A. V. Mihalev, A. L. Šmelkin, Edited by Jr. I. Manin, Izdat. "Nauka", Moscow, 1965.

[3] P. M. Gudivok, V. P. Rudko, and V. A. Bovdi. *Kristalografichni grupi*, Uzhgorodskiĭ Natsionalniĭ Universitet, Uzhgorod, 2006.

[4] F. Kasch, *Moduli i koltsa*, "Mir", Moscow, 1981. Translated from the German by E. N. Zaharova and M. I. Ursul, With a preface by L. A. Skornjakov.

[5] A. G. Kurosh, *Lectures in general algebra*, Translated by Ann Swinfen; translation edited by P. M. Cohn. International Series of Monographs in Pure and Applied Mathematics, Vol. 70. Pergamon Press, Oxford, 1965.

[6] T. Y. Lam, *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Math- ematics*. Springer-Verlag, New York, 1991.

[7] J. Lambek, *Lectures on rings and modules*, Chelsea Publishing Co., New York, second edition, 1976.

[8] S. Lang, *Algebra*, Addison-Wesley Publishing Co., Inc., Reading, Mass., 1965.

[9] S. V. Mihovski, Roots of polynomials over commutative rings, Nauk. *Visn. Uzhgorod. Univ. Ser. Mat. Inform.*, (17):161-169, 2008.

[10] S. V. Mihovski, Simple algebraic extensions of commutative rings without nilpotent or idempotent elements, *C. R. Acad. Bulgare Sci.*, 65(12):1631-1640, 2012.

[11] N. A. Nachev, Nilpotent elements and idempotents in commutative group rings, *Comm. Algebra*, 33(10):3631-3637, 2005.

[12] D. S. Passman, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York, 1977.

[13] B. L. van der Varden, *Algebra*, "Nauka", Moscow, second edition, 1979. Translated from the German by A. A. Belskiĭ, With a foreword by Yu. I. Merzlyakov.

**S.V. MIHOVSKI**
UNIVERSITY OF PLOVDIV "P.HILENDARSKI"
TSAR ASSEN STR. 24
PLOVDIV 4000
BULGARIA
*E-mail address*: mihovski@uni-plovdiv.bg