# The primal element in integral domain 

Sinan O. Al-Salihi<br>Tikreet University, College of Education for Women, Department of Mathematics


#### Abstract

An element x of an integral domain R is called primal if whenever x divides a product $a_{1} a_{2}$ with $a_{1}, a_{2} \in R$, $x$ can be written as $x=x_{1} x_{2}$ such that $x_{i}$ divides $a_{i}, i=1,2$. We study whenin $\mathrm{X}^{2}$ primal in $\mathrm{A}+\mathrm{XB} \mathrm{B}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{XB} \mathrm{B}[[\mathrm{X}]]$, when $\mathrm{A} \subseteq \mathrm{B}$ be an extension of domains. Also we show that if $A$ is an integral domain and $S \subseteq A$ a splitting multiplicative system, then $A+X A_{s}[X]$ is a semirigid GCD-domain if and only if $A$ is a semirigid GCD-domain and for each two elements of $S$, one of them divides the other.


Keyword: Integral Domain, Primal element, Principle ideal, Semirigid GCDDomains.

## Introduction:

Let $A \subseteq B$ be an extension of integral domain and X an indeterminate. In this paper, we study some arithmetic properties of the subring $\mathrm{A}+\mathrm{X} \mathrm{B}[\mathrm{X}]$ (resp.A + X B $[[\mathrm{X}]]$ ) of $\mathrm{B}[\mathrm{X}]$ (resp. B [[X]]). According to (P. M. Cohn) ${ }^{(1)}$, an element x of an integral domain R is called primal if whenever x divides a product $\mathrm{a}_{1} \mathrm{a}_{2}$ with $\mathrm{a}_{1}, \mathrm{a}_{2} \in \mathrm{R}$, x can be written as $\mathrm{x}=\mathrm{x}_{1} \mathrm{X}_{2}$ such that $\mathrm{x}_{\mathrm{i}}$ divides $a_{i}, i=1,2$ (an element whose divisors are
primal elements is called completely primal). A domain R is called GCDDomain if every pair of elements of R has a greatest common divisor. Let A be a domain and $\mathrm{S} \subseteq \mathrm{A}$ a saturated multiplicative system of A. A nonzero element $\mathrm{a} \in \mathrm{A}$ is said to be LCM-prime to $S^{(2)}$, if $a A \cap t A=$ at $A$ (equivalently $t A$ : $\mathrm{a}=\mathrm{tA})$ for each $\mathrm{t} \in \mathrm{S} . \mathrm{S}$ is said to be a splitting multiplicative system ${ }^{(3)}$, if each nonzero element x of A can be
written as $\mathrm{x}=$ as , where a is LCMprime to $S$ and $s \in S$. As $i n^{(3)}$, an extension of rings $\mathrm{A} \subseteq \mathrm{B}$ is called inert if whenever $x y \in A$ for nonzero $x, y \in$ $B$, then $x u, y u^{-1} \in A$ for some $u \in U(B)$. An element $x$ of an integral domain $R$ is called an extractor ${ }^{(4)}$, if $x R \cap y R$ is a principal ideal for each $y \in R$.

In Section 1, we prove that X is primal in $\mathrm{A}+\mathrm{X} \mathrm{B}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X} \mathrm{B}[[\mathrm{X}]]$ if and only if $\mathrm{B}=\mathrm{A}_{\mathrm{S}}$ and S is good, where $S=U(B) \cap A$ ( we say that $S$ is good if whenever $s \in S, a, b \in A \backslash\{0\}$ and $\mathrm{s} \mid{ }_{\mathrm{a}}^{\mathrm{a}} \mathrm{ab}$, there exists $\mathrm{t} \in \mathrm{S}$ such that $t \mid{ }_{\mathrm{A}} \mathrm{a}$ and $\left.\mathrm{s} \mid{ }_{\mathrm{A}} \mathrm{tb}\right)$. If $\mathrm{n} \geq 2$ and $\mathrm{S}=\mathrm{U}(\mathrm{B})$ $\cap A$, we prove that $X^{n}$ is primal in $A+$ $\mathrm{XB}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X} \mathrm{B}[[\mathrm{X}]]$ if and only if S is good, $A_{s}=B \cap Q(A)$ and for each $b$ $\in B$ there exists $c \in U(B)$ such that $b c \in$ A. We also include some remarks about the goodness of a multiplicative system.

In Section 2 we study when $\mathrm{A}+\mathrm{X}$ $\mathrm{B}[\mathrm{X}]$ is a semirigid GCD-domain. We recall that, according to (M. Zafrullah
$1975,1987,1988)^{(5,6,7)}$, an element $x$ of integral domain R is called rigid if whenever $r, s \in R$ and $r, s \mid x$, we have $s$ $\mid \mathrm{r}$ or $\mathrm{r} \mid \mathrm{s}$. Also R is called semirigid if every nonzero element of R can be expressed as a product of a finite number of rigid elements. We show that if A is an integral domain and $\mathrm{S} \subseteq \mathrm{A}$ a splitting (saturated) multiplicative system, then $A+X A_{S}[X]$ is a semirigid GCD-domain if and only if $A$ is a semirigid GCD-domain and for each two elements of $S$, one of them divides the other.

Throughout, all rings are commutative with unit element and subrings have the same unit element. If $A$ is a domain, then $U(A)$ denotes the set of invertible elements of A and $\mathrm{A}_{\mathrm{s}}$ denotes the quotient ring of $A$ with respect to the multiplicative $S$. Any unexplained notation or terminology is standard as in (R. Gilmer) $)^{(8,9)}$.

## 1. Primal elements

In this section we study the primality of $X^{n}$ in domain of type $A+X B[X]$ or $\mathrm{A}+\mathrm{X}$ B [[X]]. When $\mathrm{n}=1$, this primality forces B to be a fraction ring of $A$, that is:

Remark 1.1. If $\mathrm{A} \subseteq \mathrm{B}$ is an extension of domains and X is primal in $\mathrm{A}+\mathrm{X}$ $\mathrm{B}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X} \mathrm{B}[[\mathrm{X}]]$, then $\mathrm{B}=\mathrm{A}_{\mathrm{S}}$ where $S=U(B) \cap A$. Indeed, if $R$ denotes $\mathrm{A}+\mathrm{X} \mathrm{B}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X}$ $\mathrm{B}[[\mathrm{X}]]$ and $0 \neq \mathrm{b} \in \mathrm{B}$, then X divides $(b X)^{2}$ in $R$. So, there exist $f, g, u, v \in R$, $f(0) \neq 0$, such that $X=f g$ and $b X=f u=g v$. If $g^{\prime}$ denotes the (formal) derivative of $g$, then $1=f(0) g^{\prime}(0)$, so $f(0) \in S$ and $\mathrm{b}=\mathrm{g}^{\prime}(0) \mathrm{v}(0)=\mathrm{v}(0) / \mathrm{f}(0) \in \mathrm{A}_{\mathrm{s}}$.

The next result describes the primality of X in $\mathrm{A}+\mathrm{XB}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{XB}[[\mathrm{X}]]$. When $f$ is a nonzero power series (polynomial), the order of f is denoted by ord(f).

Theorem 1.2: Let $A$ be a domain and $S$ $\subseteq$ A a saturated multiplicative system. The following assertions are equivalent:
(a). X is primal in $\mathrm{A}+\mathrm{X} \mathrm{A}_{S}[\mathrm{X}]$,
(b) . X is primal in $\mathrm{A}+\mathrm{X} \mathrm{A}_{S}[[\mathrm{X}]]$,
(c). If $s \in S, a, b \in A$ and $s \mid a b$, there exists $t \in S$ such that $t \mid a$ and $s \mid t b$
(let us agree to say that $S$ is good if it satisfies property (c)).

Proof: Set $\mathrm{R}=\mathrm{A}+\mathrm{X} \mathrm{A}_{s}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X}$ $\mathrm{A}_{\mathrm{S}}[[\mathrm{X}]]$. First, we prove that ((a) or (b)) implies (c). Let $s \in S$ and $a, b \in A$ such that $\mathrm{s} \mid \mathrm{A}$ ab. Then $\quad \mathrm{X} \mid \mathrm{R}$ $\mathrm{a}(\mathrm{bX} / \mathrm{s})$, so there exists $\mathrm{t} \in \mathrm{S}$ such that $X=t(X / t),\left.t\right|_{R} a$ and $(X / t) \mid R(b X / s)$. So t|a and s|abt. Conversely, we prove, that (c) implies ((a) and (b)). Assume that $X \mid{ }_{R} f g$ with $f, g \in R \backslash\{0\}$ and ord $(\mathrm{f}) \leq \operatorname{ord}(\mathrm{g})$. If ord $(\mathrm{g}) \geq 2$, then $X \mid R \mathrm{~g}$. If $\operatorname{ord}(\mathrm{f})=\operatorname{ord}(\mathrm{g})=1$, then $0 \neq$ $g^{\prime}(0)=b / s$ with $b \in A, s \in S$, hence $X$ $=\mathrm{s}(\mathrm{X} / \mathrm{s})$ and $\mathrm{s}\left|\mathrm{R}_{\mathrm{R}},(\mathrm{X} / \mathrm{s})\right| \mathrm{R} \mathrm{g}$ (again, $g^{\prime}$ denotes the formal derivative of $g$ ). If $\operatorname{ord}(f)=0$ and $\operatorname{ord}(g)=1$, then $0 \neq f(0)$ $=\mathrm{a} \in \mathrm{A}, 0 \neq \mathrm{g}^{\prime}(0)=\mathrm{b} / \mathrm{s}$ with $\mathrm{b} \in \mathrm{A}, \mathrm{s} \in$ $S$ and $\mathrm{ab} / \mathrm{s} \in \mathrm{A}$. Since S is good, there
exists $t \in S$ such that $a / t, b t / s \in A$. Hence $X=t(X / t)$ and $t|R f,(X / t)| R$ g.

Remark 1.3 : Let A be a domain and $S$ $\subseteq$ A a saturated multiplicative system of $A$.
(a). If S is a splitting multiplicative system, then $S$ is good. Indeed, assume that $s \mid a b$ with $s \in S$ and $a, b \in A . W e$ can write $\mathrm{a}=\mathrm{a}^{\prime} \mathrm{t}$ with $\mathrm{t} \in \mathrm{S}$ and $\mathrm{a}^{\prime} \mathrm{LCM}-$ prime to $S$, so $\mathrm{s} \mid \mathrm{bt}$.
(b). If S is consisting of (completely) primal elements, then $S$ is good. Indeed, If $s \mid a b$ with $s \in S$ and $a, b \in A$, then $s=$ tu (so $\mathrm{t}, \mathrm{u} \in \mathrm{S}$ ), such that $\mathrm{t} \mid \mathrm{a}$ and $\mathrm{u} \mid \mathrm{b}$, hence $\mathrm{s} \mid \mathrm{bt}$.
(c). If $A$ is atomic and $S$ is good, then $S$ is splitting. Indeed, it suffices to show that each atom a not belonging to S is LCM-prime to $S$. If $b \in A, \quad s \in S$ and $s \mid a b$, then $s \mid b$, because $S$ is good and a has only unit divisors in S. As a specific example, we can consider the atomic domain $\mathrm{A}=\mathrm{k}\left[\mathrm{X}^{2}, \mathrm{XY}, \mathrm{Y}^{2}\right]$,
where k is a field, $\mathrm{X}, \mathrm{Y}$ are indeterminate and $S$ is the saturated multiplicative system generated by $\mathrm{X}^{2}$. Here the atom XY is not LCM-prime to S , because both $\mathrm{X}^{2}$, XY divide $(\mathrm{XY})^{2}$ but their product does not.
(d). $S$ is good if and only if for each $a \in$ $A, a A_{s} \cap A=\left.U_{t \in s, t}\right|_{a}(a / t) A$. Indeed, to see that the condition is necessary, let x $\in \operatorname{aAs} \cap \mathrm{A}$. Then, there exists $\mathrm{s} \in \mathrm{S}, \mathrm{b} \in$ A such that $s x=a b$, hence $x=a b / s$, so there exists $\quad t \in S$ such that $a / t, t b /$ $s \in A$, therefore $x=(a / t)(b t / s) \in(a /$ t)A. Conversely, if $a, b \in A, s \in S$ such that $x=a b / s \in A$, then $s x=a b \in$ $\mathrm{aA}_{S} \cap \mathrm{~A}$, so there exist $t \in S$ with $t \mid a$ and $c \in A$ such that $x=(a / t) c$, whence $(\mathrm{ab}) / \mathrm{s}=(\mathrm{a} / \mathrm{t}) \mathrm{c}$, therefore $\mathrm{bt} / \mathrm{s}=\mathrm{c} \in \mathrm{A}$. (e). Consequently, S is splitting if and only if S is good and every nonzero a $\in A$ has a divisor $t \in S$, such that any other divisor $w \in S$ of a divides $t$.
(f). Let T be the m-complement of $S^{(4)}$. Then , cf. ${ }^{(10)}$ each nonzero prime ideal P disjoint of $S$ contains an LCM-prime
to $S$ element if and only if the saturation of ST is $\mathrm{A} \backslash\{0\}$ (that is, for each nonzero $x$, there exists $x^{\prime}$ in $A, s \in S, t$ $\in T$ such that $\left.\mathrm{xx}^{\prime}=\mathrm{st}\right)$. If S is good and every prime ideal P disjoint of S contains an LCM-prime to $S$ element, then S is splitting. Indeed, if x is a nonzero element of A , then $\mathrm{xx}^{\prime}=\mathrm{st}$ for some $\quad x^{\prime} \in A, s \in S, t \in T . S o s \mid x x^{\prime}$ and, since S is good, $\mathrm{w} \mid \mathrm{x}$ and $\mathrm{s} \mid \mathrm{wx}$ for some $w \in S$. Now since $T$ is saturated and $t=(x / w)\left(w x^{\prime} / s\right), x / w \in T$, so $x=$ $\mathrm{w}(\mathrm{x} / \mathrm{w})$. That is S is splitting.

Corollary 1.4: Let A be a domain and S a saturated multiplicative system. Then X is completely primal in $\mathrm{A}+\mathrm{X}$ $\mathrm{A}_{s}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X} \mathrm{A}_{s}[[\mathrm{X}]]$ if and only if S is consisting of (completely) primal elements of A.

Proof: Let R denote $\mathrm{A}+\mathrm{X} \mathrm{A}_{S}[\mathrm{X}]$ or A $+X A_{S}[[X]]$. Notice that, if $s \in S$, $s$ is primal in A if and only if s is primal in $R$. Indeed, if $s$ is primal in $A$ and $\left.s\right|_{R}$ $f g, f, g \in R$, then $\left.s\right|_{A} f(0) g(0)$, hence $s$ can be written as $\mathrm{s}=\mathrm{tu}$ with $\mathrm{t}, \mathrm{u} \in \mathrm{S}$ such
that $\left.t\right|_{A} f(0),\left.u\right|_{A} g(0)$, thus $\left.t\right|_{R} f$ and $\left.u\right|_{R} g$. Since the divisors of $X$ in $R$ are of type $s$ or $X / s$ with $s \in S$ and since $R$ has an automorphism sending $\mathrm{X} / \mathrm{s}$, the assertion of Corollary 1.4 follows from Remark 1.3 (b).

The next result describes the primality of $\mathrm{X}^{\mathrm{n}}$ in $\mathrm{A}+\mathrm{X} \mathrm{B}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{XB} \mathrm{B}[[\mathrm{X}]]$, when $\mathrm{n} \geq 2$. Here, if B is a domain and $b \in B, b U(B)=\{b w ; w \in U(B)\}$.

Theorem 1.5: Let $\mathrm{A} \subseteq \mathrm{B}$ be an extension of domains, $S=U(B) \cap A$ and K the quotient field of A . Let R denote $\mathrm{A}+\mathrm{X} \mathrm{B}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X} \mathrm{B}[[\mathrm{X}]]$. The following statements are equivalent:
(a). $X^{2}$ is primal in $R$,
(b). $\mathrm{X}^{\mathrm{n}}$ is primal in R for some $\mathrm{n} \geq 2$,
(c). $\mathrm{X}^{\mathrm{n}}$ is primal in R for each $\mathrm{n} \geq 2$,
(d). $b \mathrm{U}(\mathrm{B}) \cap \mathrm{A} \neq \emptyset$ for each $\mathrm{b} \in \mathrm{B}$ is good and $\mathrm{As}_{\mathrm{s}}=\mathrm{B} \cap \mathrm{K}$,
(e). $b U(B) \cap A \neq \emptyset$ for each $b \in B$ and whenever $a \in A, b \in B$ are nonzero elements such that $a b \in A$, there exists $t$ $\in S$ such that $\mathrm{at}^{-1}, \mathrm{bt} \in \mathrm{A}$.

Remark 1.6: Let $\mathrm{A} \subseteq \mathrm{B}$ be an extension of domain. If condition (d) of Theorem 1.5 holds, then $\mathrm{A} \subseteq \mathrm{B}$ is an inert extenstion. Indeed, let $\quad b_{1}, b_{2} \in$ $B \backslash\{0\}$ such that $b_{1} b_{2}=a \in A$. Since $b_{1}$ $\mathrm{U}(\mathrm{B}) \cap \mathrm{A}=\varnothing$, there exists $\mathrm{u} \in \mathrm{U}(\mathrm{B})$ such that $a^{\prime}=b_{1} u^{-1} \in A$. Therefore $a=$ $b_{1} b_{2}=\left(b_{1} u^{-1}\right)\left(b_{2} u\right)=a^{\prime}\left(b_{2} u\right)$. Since $(d)$ holds, there exists $t \in S$ such that $b_{1} u^{-1}$ $\mathrm{t}^{-1}=\mathrm{b}_{1}(\mathrm{ut})^{-1} \in \mathrm{~A}$ and $\mathrm{b}_{2}(\mathrm{ut}) \in \mathrm{A}$.

Proof of Theorem 1.5:For a nonzero $\mathrm{f} \in$ $R$, let $\alpha(\mathrm{f})$ denote the first nonzero coefficient of $f$. In order to show that (e) implies (d), let $a, b \in A$ and $s \in S$, such that $\left.\mathrm{s}\right|_{\mathrm{A}} \mathrm{ab}$. By the second condition of (e) applied for $b / s \in B$, there exists t $\in S$ such that $\mathrm{at}^{-1} \in \mathrm{~A}, \mathrm{bt} / \mathrm{s} \in \mathrm{A}$. Let $\mathrm{b}=$ $c / a \in B$, where $a, c \in A$ are nonzero. So $\mathrm{ba}=\mathrm{c} \in \mathrm{A}$, hence, $\mathrm{by}(\mathrm{e})$, there exists $t \in S$ such that $b t \in A$, thus $b \in A_{s}$. The inclusion $\mathrm{A}_{\mathrm{S}} \subseteq \mathrm{B}$ is obvious. Conversely, let $a \in A, b \in B$ be nonzero elements such that $\mathrm{c}=\mathrm{ab} \in \mathrm{A}$. Then $\mathrm{b}=$ $c / a \in K \cap B=A s$. So there exist $s \in$ $S, d \in A$ such that $\quad b=d / s$. Since
$S$ is good, there exists $t \in S$ such that at ${ }^{-}$ ${ }^{1} \in A$ and $b t=(d / s) t \in A$.
(b) $\Rightarrow$ (e). In order to see that the second part of (e) holds, let $a \in A, \quad b \in B$ nonzero elements such that $\mathrm{ab}=\mathrm{c} \in \mathrm{A}$. Then $\left.X^{n}\right|_{R} a\left(b X^{n}\right)$, , so $X^{n}=f g, a=f f^{\prime}$ , $b X^{n}=g g^{\prime}$ for some $f, f^{\prime}, g^{\prime} \in R$ of order 0 and $g \in R$ of order $n$. Then $t=$ $\alpha(f) \in S$, because $\alpha(f) \alpha(g)=1$. Also $\mathrm{a}=\alpha(\mathrm{f}) \alpha\left(\mathrm{f}^{\prime}\right)$, so $\left.\mathrm{t}\right|_{\mathrm{A}} \mathrm{a}$, and $\mathrm{b}=\alpha(\mathrm{g}) \alpha($ $\left.\mathrm{g}^{\prime}\right)$, hence $\mathrm{bt}=\alpha\left(\mathrm{g}^{\prime}\right) \in \mathrm{A}$. To show the first part of (e), let $0 \neq b \in B$. Then $\left.X^{n}\right|_{R}\left(b X^{n}\right)(b X)$, so $X^{n}=f g, b X^{n}=f f^{\prime}$, $b X=g g^{\prime}$, for some $f, f^{\prime}, g, g^{\prime} \in R$. Then $1=\alpha(\mathrm{f}) \alpha(\mathrm{g})$ and $\mathrm{b}=\alpha(\mathrm{f}) \alpha\left(\mathrm{f}^{\prime}\right)=\alpha$ $(\mathrm{g}) \alpha\left(\mathrm{g}^{\prime}\right)$ with $\alpha\left(\mathrm{f}^{\prime}\right) \in \mathrm{A}$ or $\alpha\left(\mathrm{g}^{\prime}\right) \in \mathrm{A}$. Hence $\alpha(\mathrm{f}), \alpha(\mathrm{g}) \in \mathrm{U}(\mathrm{B})$ and of the elements $b \alpha(f), b \alpha(g)$, belongs to $A$. (a) $\Rightarrow$ (e) can be proved similarly. (c) $\Rightarrow$ (b) and (c) $\Rightarrow$ (a) are trivial . (e) $\Rightarrow$ (c). Assume that $\mathrm{f}, \mathrm{g} \in \mathrm{R}$ are nonzero, $X^{n} \mid{ }_{\mathrm{R}} \mathrm{gg}$ and $\operatorname{ord}(\mathrm{g})=\mathrm{j} \geq \operatorname{ord}(\mathrm{f})=\mathrm{i}$. Obviously, if $j \geq n+1$, then $\left.X^{n}\right|_{R} g$. We consider the following three cases.

If $\mathrm{i}=0$ and $\mathrm{j}=\mathrm{n}$, then $\alpha(\mathrm{f}) \in \mathrm{A}$, $\alpha(\mathrm{g}) \in \mathrm{B}$ and $\alpha(\mathrm{f}) \alpha(\mathrm{g}) \in \mathrm{A} . \mathrm{By}(\mathrm{e})$, there exists $t \in S$ such that $t^{-1} \alpha(f), \operatorname{ta}($ g) $\in$ A. Hence $X^{n}=t\left(t^{-1} X^{n}\right)$ with $\left.t\right|_{R} f$ and $\left.\mathrm{t}^{-1} \mathrm{X}^{\mathrm{n}}\right|_{\mathrm{R}} \mathrm{g}$, because t divides each nonconstant monomial in f. If $i+j=n$ and $i \geq 1$, then $\alpha(f), \alpha(g) \in B$ and $\alpha(f$ ), $\alpha(\mathrm{g}) \in \mathrm{A}$. By Remark 1.6 there exists $w \in U(B)$ such that $w \alpha(f) \in A$ and $\mathrm{w}^{-1} \alpha(\mathrm{~g}) \in \mathrm{A}$. Hence $\mathrm{X}^{\mathrm{n}}=\left(\mathrm{w}^{-1} \mathrm{X}^{\mathrm{i}}\right)($ $\left.w X^{j}\right)$ with $\left.w^{-1} X^{i}\right|_{R} f$ and $\left.w X^{j}\right|_{R} g$. If $i+j \geq n+1$ and $i \geq 1$, then $J \geq 2$ and $\alpha(f$ ), $\alpha(\mathrm{g}) \in \mathrm{B} . \mathrm{By}(\mathrm{e})$, there exists $\mathrm{c} \in$ $\mathrm{U}(\mathrm{B})$ that such $\alpha$ (f)ce A. Hence $\mathrm{X}^{\mathrm{n}}=$ $\left(c^{-1} X^{i}\right)\left(c X^{j-1}\right)$ with $\left.c^{-1} X^{i}\right|_{R} f$ and $c X^{j-}$ ${ }^{1} \mid{ }_{\mathrm{Rg}}$.

Example 1.7: (i).Let A be a domain and $S \subseteq A$ a multiplicative system. In A+X As [X], X is primal if and only if $\mathrm{X}^{2}$ is primal.
(ii).Let K be a field and A a subring of K . Then $\mathrm{X}^{2}$ is primal in $\mathrm{A}+\mathrm{X} \mathrm{K}[\mathrm{X}]$, but $X$ is primal in $A+X K[X]$ if and only if $\mathrm{K}=\mathrm{Q}(\mathrm{A})$. For instance, in the ring $\mathrm{Z}+$
$\mathrm{X} R[\mathrm{X}], \mathrm{X}^{2}$ is primal, but X is not primal.
(iii). $\mathrm{X}^{2}$ is not primal in $\mathrm{Z}+\mathrm{X}$ $\mathrm{Z}[\sqrt{2}][\mathrm{X}]$.
(iv). If $\mathrm{A}^{\prime} \subseteq \mathrm{B}$ is an extension of domains such that $\mathrm{bU}(\mathrm{B}) \cap \mathrm{A}^{\prime} \neq \emptyset$ for each $b \in B$, then $X^{2}$ is primal in $A+X$ $B[X]$, where $A=Q\left(A^{\prime}\right) \cap B$. Indeed, $\mathrm{Q}(\mathrm{A}) \cap \mathrm{B}=\mathrm{A}$, whence $\mathrm{U}(\mathrm{B}) \cap$ $A=U(A)$.

We recall that an element $x$ of integral domain in R is said to be an extractor if $R x \cap R y$ is principal for each $y \in R \backslash\{0\}$. Obviously each extractor is primal. By (D. D. Anderson et al 1995, Theorem 4.1) ${ }^{(4)}$ if x is an extractor, then so is every divisor of x . By the proof of [T. Dumitrescu, Proposition 2.11$]^{(11)}$, a completely primal element x is an extractor if and only if for each y , the elements $\mathrm{x} . \mathrm{y}$ have a maximal common divisor (abbrev.MCD), that is, a common
divisor z such that $\mathrm{x} / \mathrm{z}$ and $\mathrm{y} / \mathrm{z}$ are relatively prime.

Proposition 1.8: Let A be a domain and $\mathrm{S} \subseteq \mathrm{A}$ a saturated multiplicative system of A . Then X is an extractor in $\mathrm{A}+\mathrm{X}$ $\mathrm{A}_{S}[\mathrm{X}]$ or $\mathrm{A}+\mathrm{X} \mathrm{A}_{S}[[\mathrm{X}]]$ if and only if S is splitting and consists of extractors.

Proof:Let R denote $\mathrm{A}+\mathrm{X} \mathrm{A}_{\mathrm{s}}[\mathrm{X}]$ or $\mathrm{A}+$ X $\mathrm{A}_{s}[[\mathrm{X}]]$. Assume that X is an extractor in R. By the above remark, the elements of $S$ are extractors in $R$, hence extractors in A. By Remark 1.3 (b), S is good. Let $\mathrm{a} \in \mathrm{A}$ be nonzero and $\mathrm{f}=$ $\operatorname{GCD}_{\mathrm{R}}(\mathrm{X}, \mathrm{a})$. Then $\mathrm{f}(0)=\mathrm{t} \in \mathrm{S}$ and if $\left.w\right|_{\text {a }}$ with $w \in S$, then $\left.w\right|_{R} a, X$, so $\mathrm{w} \mid \mathrm{R} \mathrm{t}$, hence $\left.\mathrm{w}\right|_{\mathrm{A}} \mathrm{t}$. By Remark1.3(e), $S$ is splitting.

Conversely, assume that $S$ is splitting and consists of extractors. By Corollary 1.4, , X is completely primal in R . So, by the remarks made before Proposition 1.8 , it suffices to see that $\mathrm{X}, \mathrm{f}$ have an MCD , for each nonzero $\mathrm{f} \in \mathrm{R}$. If $\mathrm{a}=$ $\mathrm{f}(0) \neq 0$, a can be written $\mathrm{a}=\mathrm{bs}$ with s
$\in S$ and $b$ LCM-prime to $S$. Thus $s$ is an MCD of $X$ and $f$ in $R$. If $\operatorname{ord}(f)=1$, say $f=(a / t) X+c_{2} X^{2}+c_{3} X^{3}+\ldots$ with $a \in$ $\mathrm{A}, \mathrm{t} \in \mathrm{S}$, we write again $\mathrm{a}=\mathrm{bs}$ with $\mathrm{s} \in$ S and b LCM-prime to S. Since s,t are extractors, there exists $w \in S$ such that $(\mathrm{s}, \mathrm{t})_{\mathrm{v}}=\mathrm{Aw}$. Then $(\mathrm{w} / \mathrm{t}) \mathrm{X}$ is an MCD of X and f in R .

Corollary 1.9: Let A be a domain and $\mathrm{S} \subseteq \mathrm{A}$ a saturated multiplicative system of A . Then $\mathrm{A}+\mathrm{X} \mathrm{A}_{s}[\mathrm{X}]$ is GCDdomain if and only if X is an extractor in $\mathrm{A}+\mathrm{X} \mathrm{A}_{s}[\mathrm{X}]$ and $\mathrm{A}_{s}$ is a GCDdomain.

Proof: Apply proposition $1.8^{(8,12)}$

## 2. SEMIRIGID GCD-DOMAINS

Let R be an integral domain. We recall that a element $x \in R$ is said to be rigid, if whenever $r, s \in R$ and $r, s \mid x$, we have $r \mid s$ or $s \mid r$. so an irreducible element is obviously rigid ( we recall that a nonzero nonunit $\mathrm{x} \in \mathrm{R}$ is called irreducible if whenever $y \in R$ and $y \mid x$, we have $y \mid 1$ or $x \mid y$. Then $R$ is called
semirigid if every nonzero element of $R$ can be expressed as a product of a finite number of rigid elements. So, each atomic domain, that is a domain in which every nonzero nonunit element is a product of irreducible elements, is semirigid.

Lemma 2.1: Let A be a domain, $\mathrm{S} \subseteq \mathrm{A}$ a saturated multiplicative system and R $=\mathrm{A}+\mathrm{x} \mathrm{A}_{\mathrm{s}}[\mathrm{X}]$.
(a). X is rigid in R if and only if for every $r, s \in S,\left.r\right|_{A S}$ or $\left.s\right|_{A r}$. If $X$ is rigid in $R$ and $s \in S$, then $X / s$ is rigid in $R$.
(b). A nonzero element $\mathrm{a} \in \mathrm{A}$ is rigid in A if and only if a is rigid in $R$.

Proof:Is a consequence of the following remarks. The set of all divisors of X in $R$ is $S \cup\{X / s ; s \in S\}$ and any nonzero $\mathrm{a} \in \mathrm{A}$ has the same divisors in $A$ and $R$. Also if $b, c \in A$, then $\left.b\right|_{A} c$ if and only if $b \mid R c$. When $s \in S, R$ has an A-algebra automorphism sending X into $\mathrm{X} / \mathrm{s}$.

Let A be a domain and $\mathrm{S} \subseteq \mathrm{A}$ a saturated multiplicative system. In [D. Costa et al. , Theorem 1.1] ${ }^{(12)}$, is show that $\mathrm{A}+\mathrm{X} \mathrm{A}_{s}[\mathrm{X}]$ is a GCD-domain if and only if A is a GCD-domain and S is splitting. Our next result characterizes the semirigid GCD-domain of type A + X As $[\mathrm{X}]$.

Theorem 2.2: Let A be a domain and $S$ $\subseteq A \quad \mathrm{a} \quad$ splitting $\quad(\quad$ saturated $)$ multiplicative system. Then $\mathrm{A}+\mathrm{X}$ $\mathrm{As}_{\mathrm{s}}[\mathrm{X}]$ is a semirigid GCD-domain if and only if A is a semirigid GCDdomain and for every $s, t \in S,\left.s\right|_{A} t$ or $t \|_{\mathrm{A}} \mathrm{S}$.

Proof: Set $\mathrm{R}=\mathrm{A}+\mathrm{X} \mathrm{As}_{\mathrm{s}}[\mathrm{X}]$. Using Lemma 2.1, and the comments above, it suffices to show that R is semirigid provided A is a semirigid GCD-domain and $X / s$ is rigid in $R$ for each $s \in S$. We use freely Lemma 2.1. Let $f \in R$ be a nonzero polynomial of minimal degree among all nonzero polynomials of R which cannot be written as product of
rigid elements of R . Then any divisor of f in R is constant or have the same degree with $f$. Since a rigid element of A is still rigid in $R$, it follows that $\mathrm{f} \notin \mathrm{A}$. If $f(0)=0$, then $f=(X / s)$ a for some $s$ $\in S$ and $a \in A$. This contradicts the choice of $f$ because $X / s$ is rigid and $A$ semirigid. If $\mathrm{f}(0) \neq 0$, then factoring out from f an appropriates element of A , we may assume that

$$
\mathrm{f}=\mathrm{a}_{0}+\left(\mathrm{a}_{1} / \mathrm{s}\right) \mathrm{X}+\ldots+\left(\mathrm{a}_{\mathrm{n}} / \mathrm{s}\right) \mathrm{X}^{\mathrm{n}}
$$

with $a_{i} \in A, s \in S$ and $\operatorname{GCD}\left(a_{0}, \cdots a_{n}\right)$ $=1$. Moreover, since $S$ is splitting, we may assume that $\mathrm{a}_{0}$ is LCM-prime to S . Then f has no nonunit factor in A , thus f is irreducible, a contradiction.

There is as certain resemblance between the proofs of Theorem 2.2 and [T. Dumitrescu, Corollary 1.8$]^{(11)}$.

Corollary 2.3: If A is a semirigid GCDdomain, so is the polynomial ring A [X].

Corollary 2.4:[M. Zafrullah, Example $4]{ }^{(6)}$. If V is a valuation domain with quotient field $K$, then $V+X K[X]$ is a semirigid GCD-domain.

Corollary 2.5: If $A$ is a semirigid GCDdomain and $p \in A$ a prime element such that $\bigcap_{n \geq 1} p^{n} A=0$, (e.g. if $A$ is a factorial domain and $\mathrm{p} \in \mathrm{A}$ a prime), then $\mathrm{A}+\mathrm{X}$ $\mathrm{A}[1 / \mathrm{p}][\mathrm{X}]$ is a semirigid GCD-domain. Proof: The saturated multiplicative system generated by p is splitting $\mathrm{cf}^{(3)}$.

Example 2.6: Iterating the preceding corollary, we obtain successively that the following rings are semirigid GCDdomains

$$
\mathrm{A}_{1}=\mathrm{Z}+\mathrm{XZ}[1 / 2]\left[\mathrm{X}_{1}\right], \mathrm{A}_{2}=\mathrm{A}_{1}+\mathrm{X}_{2}
$$

$$
\mathrm{A}[1 / 3]\left[\mathrm{X}_{2}\right], \cdots,
$$

$$
\mathrm{A}_{\mathrm{n}}=\mathrm{A}_{\mathrm{n}-1}+\mathrm{X}_{\mathrm{n}} \mathrm{~A}_{\mathrm{n}-1}\left[1 / \mathrm{p}_{\mathrm{n}-1}\right]\left[\mathrm{X}_{\mathrm{n}}\right],
$$

Where $\mathrm{p}_{\mathrm{n}}$ is the nth prime number. Indeed, if q is a prime distinct from $\mathrm{p}_{1}$ , $\mathrm{p}_{2}, \cdots, \mathrm{p}_{\mathrm{n}}$, then

$$
\begin{gathered}
\mathrm{A}_{\mathrm{n}} / \mathrm{qA} \mathrm{~A}_{\mathrm{n}} \simeq\left(\mathrm{~A}_{\mathrm{n}-1} / \mathrm{qA} \mathrm{~A}_{\mathrm{n}-1}\right)\left[\mathrm{X}_{\mathrm{n}}\right] \simeq \cdots \simeq(\mathrm{Z} \\
\quad \mathrm{qZ})\left[\mathrm{X}_{1}, \mathrm{X}_{2}, \cdots, \mathrm{X}_{\mathrm{n}}\right] \text { and }
\end{gathered}
$$

$\cap_{k \geq 1} q^{k} A_{n} \subseteq \cap_{k \geq 1} q^{k} Z\left[1 / p_{1}, 1 / p_{2}, \cdots, 1 /\right.$

$$
\left.\mathrm{p}_{\mathrm{n}}\right]\left[\mathrm{X}_{1}, \mathrm{X}_{2}, \cdots, \mathrm{X}_{\mathrm{n}}\right]=0
$$

## REFERENCES:

(1) P. M. Cohn, Bezout rings and their subring. Proc. Cambridge Philios. Soc. 64 (1968), 251264.
(2) M. Roitman, Polynomial extensions of atomic domains. J. Pure and Appl. Algebra, 87 (1993), 187-199.
(3) D. D. Anderson, D. F. Anderson and M. Zafrullah, Factorization in integral domains,II. J. Algebra, 152 (1992), 78-93.
(4) D. D. Anderson and M. Zafrullah, P. M. Cohn s completely primal elements, Zero dimensional Commutative Rings, pp. 115-123. Lecture Notes in Pure and Appl. Math. 171, Marcel Dekker, Inc., New York, 1995.
(5) M. Zafrullah, Semirigid GCDdomain elements. Manuscripta Math. 17 (1975), 55-66.
(6) M. Zafrullah, On a property of preSchreier domains. Comm. Algebra, 15 (1987), 1895-1920.
(7) M. Zafrullah, The $\mathrm{D}+\mathrm{XD}_{\mathrm{S}}[\mathrm{X}]$ construction from GCD domains. J, Pure Appl. Algebra, 50(1988), 93-107.
(8) R. Gilmer, Multiplicative Ideal Theory. Marcel Dekker, New York, 1972.
(9) R. Gilmer and T. Parker, Divisibility properties in semigroup rings. Michigan J. Math 21 (1974), 65-86.
(10) V. Barucci, L. Izelgue and S, Kabbaj, Some factorization properties of $\mathrm{A}+\mathrm{XB}[\mathrm{X}]$ domains. In: Commutative Ring Theory. 6978. Lecture Notes in Pure and Appl. Math., 185, Marcel Dekker, New York, 1997.
(11) T. Dumitrescu, On some examples of atomic domains and of G-rings. To appear $n$ Comm. Algebra.
(12) 6-D. Costa, J. Mott and M. Zafrullah, The construction $\mathrm{D}+\mathrm{XD}_{\mathrm{S}}[\mathrm{X}] . \quad$ J. Algebra, 53 (1978), 423-439.

# العنصر الاسـاسي في الساحة العددية <br> سنـان عمر ابراهيم 

جامعة تكريت ـ كلية التربية للبنات - قسم الرياضيات

## الملخص

 ويمكن كتابة x كالثشكل x=x
 عددية و A

شبه صـارم ولكل عنصرين في S احدهما يقسم الاخر.

