Primes that become primal in a pullback

Tiberiu Dumitrescu Nicolae Radu
Universitatea Bucureşti, Facultatea de Matematică
Str. Academiei 14, Bucureşti, RO 70190, Romania
E-mail: tiberiu@al.math.unibuc.ro radu@al.math.unibuc.ro

Muhammad Zafrullah
Department of Mathematics, Campus Box 8085
Idaho State University, Pocatello, ID 83209, USA
E-mail: zufrmuha@isu.edu

Abstract

Let A be the pullback ring $p^{-1}(A')$, where B is a domain, $M \neq 0$ is a prime ideal of B, $p : B \to B/M$ is the canonical map and A' is a proper subring of $B' = B/M$. Assume that M contains a prime element of B. Set $S = U(B) \cap A$ and $S' = U(B') \cap A'$. We show that A is a GCD domain if and only if the following conditions hold: (a) B is a GCD domain, (b) B' is a quotient ring of A' and $S' = p(S)U(A')$, (c) S' is an lcm splitting multiplicative set of A', and (d) M is a principal ideal of B.

AMS Classification: 13A15; 13F05

1 Introduction

Let $C \subseteq D$ be an extension of integral domains and T the multiplicative set $U(D) \cap C$, where $U(D)$ is the set of units of D. Let E be the polynomial ring $D[X]$ or the power series ring $D[[X]]$. Then $C+XE$ is the ring $C+XD[X]$ of polynomials $f \in D[X]$ with $f(0) \in C$, or its power series analog $C+XD[[X]]$.

By [6, Theorem 1.1] and [4, Theorem 2.11], $C + XE$ is a GCD domain if and only if both of C, E are GCD domains, $D = C_T$ and T is a *splitting* multiplicative set of C [2] (i.e., every principal ideal of C_T contracts to a principal ideal of C). For instance, $\mathbf{Z} + X\mathbf{Q}[X]$ is a GCD domain but $\mathbf{Z} + X\mathbf{R}[X]$ is not.

An element $c \in C$ is called *primal* [5], if $c \mid a_1a_2$ implies that $c = c_1c_2$ such that $c_1 \mid a_1$, $c_2 \mid a_2$; c is called *completely primal* if all its factors are primal. A *pre-Schreier* domain [21] is a domain in which every element is (completely) primal, while a *Schreier* domain [5] is an integrally closed pre-Schreier domain. Obviously, a Schreier domain is pre-Schreier, and, by [5], a GCD domain is Schreier. Examples given in [5], [17] and [21] show that these implications are not reversible. By [8, Theorem 2.7], $C+XE$ is a (pre-) Schreier domain if and only if both of C, E are (pre-) Schreier domains and $D = C_T$. By [3], if $k \subset K$ is a proper field extension, then X is a nonprimal element in $k+XK[X]$ whose square is primal. Motivated by this example, it was shown in [9] that X is primal element of $C + XE$ if and only if $D = C_T$ and T is a *good* multiplicative set of C (i.e., if whenever $s \mid_C ab$ with $s \in T$ and $a, b \in C$, there exists $t \in T$ such that $t \mid_C a$ and $s \mid_C tb$). Also, in [9] it was shown that X^n is a primal element of $C+XE$ for some $n \geq 2$ if and only if T is a good multiplicative set of C, $C_S = D \cap K$ where K is the quotient field of C and, for each $b \in D$, $bU(D) \cap C \neq \emptyset$. Note that $C + XE$ arises as the pullback of the following diagram

$$\begin{array}{ccc} C + XE = q^{-1}(C) & \hookrightarrow & E \\ \downarrow & & \downarrow q \\ C & \hookrightarrow & D \end{array}$$

where q is the map sending f to $f(0)$. The kernel of q is generated by the prime element X.

In this paper, we obtain similar results for domains A arising as pullbacks of canonical homomorphisms

$$\begin{array}{ccc} A = p^{-1}(A') & \hookrightarrow & B \\ \downarrow & & \downarrow p \\ A' & \hookrightarrow & B' = B/M \end{array}$$

where B is a domain, $M \neq 0$ is a prime ideal of B and A' is a subring of $B' = B/M$. Due to its use in constructing examples with prescribed properties, this construction has been extensively studied by several authors (e.g., see [10], [16] and their references), especially when M is a maximal ideal. Instead, we assume that M *contains a prime element of* B. Let us denote the pullback domain A defined above by $B \times_{B/M} A'$. Set $S = U(B) \cap A$ and $S' = U(B') \cap A'$.

In Section 2 we study when a prime element of B (or one of its powers) is a primal element of A. We show that the following assertions are equivalent: (a) there exists an element of M which is prime in B and primal in A, (b) every element of M which is prime in B is primal in A, (c) S is a good multiplicative set of A and B is a quotient ring of A, and (d) S' is a good multiplicative set of A', $S' = p(S)U(A')$ and B' is a quotient ring of A'. In particular, every element $f \in \mathbf{Z} + (X,Y)\mathbf{Q}[[X,Y]]$ with $f(0) = 0$ is primal. If M is principal, say $M = xB$, we show that x^2 is primal in A if and only if x^n is primal in A for some (all) $n \geq 2$.

In Section 3, we study GCD pullback domains. If $A' \neq B/M$, we show that A is a GCD domain if and only if the following conditions hold: (a) B is a GCD domain, (b) B' is a quotient ring of A' and $S' = p(S)U(A')$, (c) S' is an lcm splitting multiplicative set of A', and (d) M is a principal ideal of B (a splitting multiplicative set T is called *lcm splitting* if $(s) \cap (t)$ is a principal ideal for all $s, t \in T$). For instance, $\mathbf{Z}[X] + (X^2+3)\mathbf{Z}_S[X]$, where $S = \{1, 5, 5^2, ..\}$, or $\mathbf{C}[y,z] + x\mathbf{C}[x,y,z]_{(x,y,z-1)}$, where $x^2+y^2+z^2 = 1$, are GCD domains. Also, if D is a domain and $x, f \in D$ such that x is a prime element of D and $f + xD$ is a prime element of D/xD, then $D + xD_f$ is a GCD domain if and only if D_f is a GCD domain and $\cap_{n\geq 1}(f^nD + xD) = xD$. Similar results describing the pullback semirigid GCD domains (resp., GCD domains of finite t-character) are also obtained.

Throughout, if no explicit mention is made, A denotes the pullback domain $B \times_{B/M} A'$ defined above, $S = U(B) \cap A$ and $S' = U(B') \cap A'$. Our general references for any undefined terminology or notation are [11], [12] and [15].

2 Primal elements

Recall that an element c of a domain is called primal, if $c \mid a_1a_2$ implies that $c = c_1c_2$ such that $c_1 \mid a_1$, $c_2 \mid a_2$ and c is called completely primal if all its factors are primal. Let $A = B \times_{B/M} A'$, $S = U(B) \cap A$ and $S' = U(B') \cap A'$. Clearly, B is a quotient ring of A if and only if $B = A_S$. Also, M is a common ideal of the rings $A \subseteq A_S \subseteq B$ and $A/M = A'$. In the next lemma, we recall some basic properties of the pullback construction.

Lemma 2.1 *Consider the pullback $A = B \times_{B/M} A'$.*

(i) If $s \in S$ and $a \in A$, $s \mid_A a$ if and only if $p(s) \mid_{A'} p(a)$.

(ii) If $p(U(B)) = U(B')$, then $p(S) = S'$ (note that $p(U(B)) = U(B')$, if M is contained in the Jacobson radical of B, e.g. if B is quasilocal with maximal ideal M).

(iii) $A'_{p(S)} = B'$ if and only if $A_S = B$.

Proof. For (i) it suffices to notice that $s \mid_A m$ for each $m \in M$.

(ii) If $b' \in S'$, there exists $b \in U(B)$ such that $p(b) = b'$. Hence $b \in p^{-1}(A') \cap U(B) = S$. The opposite inclusion is obvious.

(iii) We have, $A_S = B$ if and only if $A'_{p(S)} = A_S/M = B/M = B'$. •

We recall from the introduction that a multiplicative set T of a domain D is said to be good, if whenever $s \mid ab$ with $s \in T$, $a, b \in D$, there exists $t \in T$ such that $t \mid a$ and $s \mid tb$. If T is good, then its saturation is $U(D)T$. Indeed, if $s = ab$ with $s \in T$ and $a, b \in D \setminus \{0\}$, there exists $t \in T$ such that $t \mid a$ and $ab = s \mid tb$. Hence a, t are associates in D.

The next lemma collects some properties of the good multiplicative sets in the pullback setup.

Lemma 2.2 *Consider the pullback $A = B \times_{B/M} A'$.*

(i) S is a good multiplicative set of A if and only if $p(S)$ is a good multiplicative set of A'.

(ii) S is a good multiplicative set of A and $A'_{p(S)} = A'_{S'}$ if and only if S' is a good multiplicative set of A' and $S' = p(S)U(A')$.

(iii) If $S' = p(S)U(A')$, every element of S is completely primal in A if and only if S' has the same property in A'.

Proof. (i) It suffices to notice that the goodness of S is given by divisibility relations of type $s \mid_A a$ with $s \in S$ and $a \in A$, so part (i) of Lemma 2.1 applies.

(ii) If $A'_{p(S)} = A'_{S'}$, then the saturation of $p(S)$ is S', because S' is saturated. If, in addition, S is a good multiplicative set of A, then $S' = p(S)U(A')$, by the remark made in paragraph before Lemma 2.2. Conversely, if $S' = p(S)U(A')$ and S' is a good multiplicative set of A', then so is $p(S)$ and $A'_{p(S)} = A'_{S'}$. Hence (i) applies.

(iii) To prove the "if" part, let $s \in S$ and $a, b \in A$ such that $s \mid_A ab$. Then $p(s) \mid_{A'} p(a)p(b)$. Since every element of S' is completely primal and S' is saturated, there exist $u', v' \in S'$ such that $p(s) = u'v'$ and $u' \mid_{A'} p(a)$, $v' \mid_{A'} p(b)$. Since $S' = p(S)U(A')$, there exist $u, v \in S$ and $q, r \in A$ such that $p(q), p(r) \in U(A')$ and $u' = p(uq)$, $v' = p(vr)$. So $p(s) = p(uvqr)$, hence $s - uvqr = m \in M$. Thus $s = uw$, where $w = vqr + u^{-1}m \in S$, because S is saturated. Now, $p(w) = p(v)p(q)p(r) \sim_{A'} v' \mid_{A'} p(b)$ and $p(u) \sim_{A'} u' \mid_{A'} p(a)$. Part (i) of Lemma 2.1 shows that $u \mid_A a$ and $w \mid_A b$.

To prove the "only if" part, let $s' \in S'$ and $a, b \in A$ such that $s' \mid_{A'} p(a)p(b)$. Since $S' = p(S)U(A')$, we may assume that $s' = p(s)$ with $s \in S$. By part (i) of Lemma 2.1, $s \mid_A ab$, so there exist $s, t \in S$ such that $s = tu$ and $t \mid_A a$, $u \mid_A b$. It suffices to apply p. •

Theorem 2.3 *Let $A = B \times_{B/M} A'$ be a pullback such that M contains a prime element of B. The following assertions are equivalent:*

(a) *there exists an element of M which is prime in B and primal in A,*

(b) *every element of M which is prime in B is primal in A,*

(c) *S is a good multiplicative set of A and B is a quotient ring of A,*

(d) *$p(S)$ is a good multiplicative set of A' and $B' = A'_{p(S)}$,*

(e) *S' is a good multiplicative set of A', $S' = p(S)U(A')$ and B' is a quotient ring of A', and*

(f) *S' is a good multiplicative set of A', $U(B') = p(U(B))U(A')$ and B' is a quotient ring of A'.*

PROOF. If $x \in M$ is a prime element of B, every (two-factor) decomposition of x in A has the form $x = s(x/s)$ for some $s \in S$.

$(b) \Rightarrow (a)$ is obvious.

$(a) \Rightarrow (c)$. Suppose that $x \in M$ is prime in B and primal in A. Clearly $A_S \subseteq B$. Let $b \in B$. If $b \in xB$, then $b \in A$. Assume that $b \notin xB$. Since x is primal in A and $x \mid_A (bx)^2$, we get $(x/t) \mid_A bx$ for some $t \in S$, so $bt \in A$. In order to prove that S is a good multiplicative set of A, let $s \mid_A ab$ with $s \in S$, $a, b \in A$. When $a \in xB$ (resp., $b \in xB$) we may take $t = s$ (resp., $t = 1$). Suppose that $a, b \notin xB$. Since $x \mid_A a(bx/s)$ and x is primal in A, x can be written as $x = tu$, with t or u in S, such that $t \mid_A a$ and $u \mid_A (bx/s)$. If $u \in S$, then $a \in tB = (x/u)B = xB$, a contradiction. It follows that $t \in S$, so $(x/t) \mid_A (bx/s)$, that is $s \mid_A tb$.

$(c) \Rightarrow (b)$. Assume that $x \in M$ is a prime element of B. Let $x \mid_A ac$ with $a, c \in A \setminus \{0\}$. Since x is prime in B, we may assume that $x \mid_B c$, so

$c = x(b/s)$ for some $b \in A$ and $s \in S$. Then $sc = bx \mid_A abc$, so $s \mid_A ab$. Since S is good, there exists $t \in S$ such that $t \mid_A a$ and $s \mid_A tb$. So, $x = t(x/t)$, $t \mid_A a$ and $(x/t) \mid_A (bx/s) = c$.

$(c) \Leftrightarrow (d)$ cf. Lemmas 2.1 and 2.2.

$(d) \Leftrightarrow (e)$. Obviously, $A'_{p(S)} \subseteq A'_{S'} \subseteq B'$. So, $A'_{p(S)} = B'$ if and only if $A'_{p(S)} = A'_{S'}$ and $A'_{S'} = B'$. We apply parts (i) and (ii) of Lemma 2.2.

$(e) \Rightarrow (f)$. We have $U(B') = S'S'^{-1} = p(S)p(S)^{-1}U(A')$, so $U(B') = p(SS^{-1})U(A') = p(U(B))U(A')$.

$(f) \Rightarrow (e)$. Let $q' \in S'$. There exist $c \in U(A')$, $b \in U(B)$ such that $q'c = p(b)$. So $b \in p^{-1}(A') \cap U(B) = S$. Thus $q' = p(b)c^{-1} \in p(S)U(A')$. •

Remark 2.4 (i) In Theorem 2.3, the hypothesis that M contains a prime element of B is not needed for proving the equivalence of assertions (c)-(f).

(ii) If $A = B \times_{B/M} A'$ is a pullback and B has no prime element, A may be a pre-Schreier domain without B being a quotient ring of A. Indeed, in the last paragraph of [17], it is pointed out that for a rank one non-discrete valuation domain of type $K + M$, $F + M$ is a pre-Schreier domain for each subfield F of K.

(iii) Taking $B = \mathbf{Z}[X]$, $M = (2X-1)B$, $B' = \mathbf{Z}[1/2]$ and $A' = \mathbf{Z}$, we get the pullback $A = B \times_{B/M} A' = \mathbf{Z} + (2X-1)\mathbf{Z}[1/2][X]$. Here, $S = U(A') = \{1, -1\}$ and $S' = \{2^n;\ n \geq 0\}$. Hence $S' \neq p(S)U(A')$, so A is not a pre-Schreier domain, cf. Theorem 2.3.

Corollary 2.5 *Let $A = B \times_{B/M} A'$ be a pullback and $x \in M$ a prime element in B. The following assertions are equivalent:*

(a) *x is a completely primal element of A,*

(b) *every element of S is (completely) primal in A and B is a quotient ring of A, and*

(c) *every element of S' is (completely) primal in A', $S' = p(S)U(A')$ and B' is a quotient ring of A'.*

Proof. We use Theorem 2.3 and the following facts. 1) $s \mid_A x$ for each $s \in S$. 2) If x is primal in A, then so is x/s for each $s \in S$, cf. Theorem 2.3. 3) If every element of S is completely primal in A, then S is a good multiplicative set of A. Indeed, if $s \mid_A ab$ with $s \in S$ and $a, b \in A$, there exist $t, u \in S$ such that $s = tu$ and $t \mid_A a$, $u \mid_A b$. Since S is saturated, $t \in S$. Also, $s = tu \mid_A tb$. 4) Part (iii) of Lemma 2.2. •

Corollary 2.6 ([9, Theorem 2, Corollary 4]) *Let D be a domain, $T \subseteq D$ a saturated multiplicative set and let R denote $D + XD_T[X]$ or $D + XD_T[[X]]$.*

(a) X is primal in R if and only if T is a good multiplicative set of D.

(b) X is completely primal in R if and only if every element of T is (completely) primal in D.

Corollary 2.7 *Consider the pullback $A = B \times_{B/M} A'$, where B' is the quotient field of A' and B is a quasilocal domain. If B is a UFD, then every element of M is primal in A. In particular, if D is a domain with quotient field L and $C = D + (X_1, .., X_n)L[[X_1, .., X_n]]$ with $n \geq 1$, then every $f \in C$ with $f(0) = 0$ is primal in C.*

Proof. Note that B' is a field, $p(U(B)) = U(B')$ and $S' = A' \setminus \{0\}$ is a good multiplicative set of A'. Since B is a quasilocal UFD, every element of M is a products of prime elements of B and these are in M. So, Theorem 2.3 applies. •

Proposition 2.8 *Let $A = B \times_{B/M} A'$ be a pullback such that $S' = p(S)U(A')$ and $B' = A'_{S'}$.*

(a) If A' and B are pre-Schreier domains, then so is A.

(b) If A and B' are pre-Schreier domains, then so is A'.

Proof. Note that $B' = A'_{p(S)}$. So $B = A_S$, cf. part (iii) of Lemma 2.1. As noticed in [22, Corollary 8] the proof of [5, Theorem 2.6] shows that if D is a domain and $T \subseteq D$ a multiplicative set consisting of completely primal elements such that D_T is a pre-Schreier domain, then D is a pre-Schreier domain. So, we may apply part (iii) of Lemma 2.2. •

Corollary 2.9 ([8, Corollary 2.9]) *Let D be a pre-Schreier domain and $T \subseteq D$ a multiplicative set. Let E denote $D_T[X]$ or $D_T[[X]]$. If E is a pre-Schreier domain, then so is $D + XE$.*

If D is a domain and $b \in D$, let $bU(D)$ denote $\{bw; w \in U(D)\}$.

Theorem 2.10 *Let $A = B \times_{B/M} A'$ be a pullback such that M is a principal nonzero ideal of B, say $M = xB$. Set $T = A \setminus xB$. The following assertions are equivalent:*

(a) x^2 is a primal element of A,

(b) x^n is a primal element of A for some $n \geq 2$,

(*c*) x^n *is a primal element of* A *for all* $n \geq 2$,

(*d*) $bU(B) \cap A \neq \emptyset$ *for each* $b \in B$, $A_S = B \cap A_T$ *and* S *is a good multiplicative set of* A,

(*e*) $b'p(U(B)) \cap A' \neq \emptyset$ *for each* $b' \in B'$, $A'_{S'} = B' \cap Q(A')$, $S' = p(S)U(A')$ *and* S' *is a good multiplicative set of* A',

(*f*) $bU(B) \cap A \neq \emptyset$ *for each* $b \in B$ *and for each* $a \in T$, $b \in B$ *such that* $ab \in A$, *there exists* $t \in S$ *such that* at^{-1}, $bt \in A$, *and*

(*g*) $b'p(U(B)) \cap A' \neq \emptyset$ *for each* $b' \in B'$, $S' = p(S)U(A')$ *and for each* $a \in A' \setminus \{0\}$, $b \in B'$ *such that* $ab \in A'$, *there exists* $t \in S'$ *such that* at^{-1}, $bt \in A'$.

PROOF. Obviously $(c) \Rightarrow (a) \Rightarrow (b)$. We shall use freely the following remark. Since x is prime in B, every decomposition of x^n, $n \geq 1$ has the form $x^n = (tx^r)(t^{-1}x^q)$ with $t \in U(B)$, $q + r = n$, $r, q \geq 0$ and $t \in S$ if $r = 0$.

$(b) \Rightarrow (d)$. Let $n \geq 2$ such that x^n is primal in A. Let $b \in B$. To show that $bU(B) \cap A \neq \emptyset$, we may assume that $b \in B \setminus A$, so $b \in B \setminus xB$. Since x^n is primal in A and $x^n \mid_A (bx^n)(bx)$, there exist $t \in U(B)$, $0 \leq q \leq n$, $0 \leq r \leq 1$, $q + r = n$ such that $(t^{-1}x^q) \mid_A bx^n$ and $(tx^r) \mid_A bx$. If $r = 0$, $bt \in A$, if $r = 1$ $bt^{-1} \in A$. Obviously, $A_S \subseteq B \cap A_T$. Conversely, let $b = a/t$ with $b \in B$, $a \in A$ and $t \in T$. Since x^n is primal in A, $t \notin xB$ and $x^n \mid_A (bt)x^n = t(bx^n)$, there exists $s \in S$ such that $s \mid_A t$ and $(s^{-1}x^n) \mid_A bx^n$, so $bs \in A$, that is $b \in A_S$. In order to prove that S is a good multiplicative set of A, let $s \mid_A ab$ with $s \in S$, $a, b \in A$. When $a \in xB$ we may take $t = s$. Suppose that $a \notin xB$. Since x^n is primal in A and $x^n \mid_A (ab/s)x^n = a(x^nb/s)$, there exists $t \in S$ such that $t \mid_A a$ and $(t^{-1}x^n) \mid_A x^nb/s$, so $s \mid_A tb$.

$(f) \Rightarrow (c)$. Let $n \geq 2$. To show that x^n is primal in A, let $x^n \mid_A fg$ with $f, g \in A \setminus \{0\}$. We may assume that $x^{n+1} \nmid_B f, g$, otherwise x^n divides f or g in A. We write $f = Fx^i$, $g = Gx^j$ with $F, G \in B \setminus xB$, $0 \leq i \leq j \leq n$ and $i + j \geq n$. We consider the following three cases. If $i = 0$, so $j = n$, we get $F \in A \setminus xB$ and $FG \in A$. By (*f*), there exists $t \in S$ such that $t^{-1}F, tG \in A$. Hence $x^n = t(t^{-1}x^n)$ with $t \mid_A f$ and $t^{-1}x^n \mid_A g$. If $i + j = n$ and $i \geq 1$, then $F, G \in B \setminus xB$ and $FG \in A$. Since $FU(B) \cap A \neq \emptyset$, there exists $u \in U(B)$ such that $Fu^{-1} \in A$. Note that $Fu^{-1} \notin xB$. By applying (*f*) to $FG = (Fu^{-1})(Gu) \in A$, we get $Fu^{-1}s^{-1}, Gus \in A$, for some $s \in S$. So, $w = u^{-1}s^{-1} \in U(B)$ and $wF, w^{-1}G \in A$. Hence $x^n = (w^{-1}x^i)(wx^j)$ with $w^{-1}x^i \mid_A f$ and $wx^j \mid_A g$. If $i + j \geq n + 1 \geq 3$ and $i \geq 1$, then $j \geq 2$. Since $FU(B) \cap A \neq \emptyset$, there exists $c \in U(B)$ such that $Fc \in A$. Hence

$x^n = (c^{-1}x^i)(cx^{j-1})$ with $c^{-1}x^i \mid_A f$ and $cx^{j-1} \mid_A g$.

$(d) \Rightarrow (f)$. Let $a \in T$, $b \in B$ such that $ab \in A$. Then $b \in A_T \cap B = A_S$. So, $b = d/s$ for some $d \in A$ and $s \in S$. Since S is good, there exists $t \in S$ such that $at^{-1}, t(d/s) = tb \in A$.

For $(d) \Leftrightarrow (e)$, first note that, taking modulo $M = xB$, we see that $A_S = B \cap A_T$ if and only if $A'_{p(S)} = B' \cap Q(A')$.

$(d) \Rightarrow (e)$. Since $A'_{p(S)} \subseteq A'_{S'} \subseteq B' \cap Q(A')$, we get $A'_{p(S)} = A'_{S'}$, so part (ii) of Lemma 2.2 applies.

$(e) \Rightarrow (d)$ follows from part (ii) of Lemma 2.2.

$(f) \Rightarrow (g)$. That $S' = p(S)U(A')$ follows from $(f) \Leftrightarrow (e)$. The rest is straightforward.

$(g) \Rightarrow (f)$. Let $a \in T$, $b \in B$ such that $ab \in A$. Then $p(a) \neq 0$ and $p(a)p(b) \in A'$. So, there exists $s' \in S'$ such that $p(a)s'^{-1}, p(b)s' \in A'$. Since $S' = p(S)U(A')$, we may assume that $s' = p(s)$ for some $s \in S$. Consequently, $as^{-1}, bs \in A$. •

Corollary 2.11 ([9, Theorem 5]) *Let $C \subseteq D$ be an extension of domains, $S = U(D) \cap C$ and K the quotient field of C. Let B denote $D[X]$ or $D[[X]]$ and $A = C + XB$. The following statements are equivalent:*

(a) X^2 is a primal element of A,

(b) X^n is a primal element of A for some $n \geq 2$,

(c) X^n is a primal element of A for all $n \geq 2$,

(d) $bU(D) \cap C \neq \emptyset$ for each $b \in D$, S is a good multiplicative set of C and $C_S = D \cap K$, and

(e) $bU(D) \cap C \neq \emptyset$ for each $b \in D$ and whenever $ab \in C$ with $a \in C$, $b \in D$ nonzero elements, there exists $t \in S$ such that at^{-1}, $bt \in C$.

3 GCD domains

Let D be a domain. According to [3], a nonzero element $x \in D$ is called an *extractor*, if $xD \cap yD$ is a principal ideal (that is, $LCM(x, y)$ exists), for each $y \in D$. By [1], a splitting multiplicative set S of D is said to be *lcm splitting*, if every element of S is an extractor. By [3, Theorem 3.1], every extractor is completely primal. The next lemma gives a kind of converse. Recall from [18], that a maximal common divisor (MCD) of two elements $x, y \in D$ is a common factor d of x, y such that $x/d, y/d$ are coprime. Also, two nonzero elements x, y of a domain are called *v-coprime* if $(x) \cap (y) = (xy)$. In a GCD domain, two nonzero elements are v-coprime if and only if they are coprime.

Lemma 3.1 *Let D be a domain, x a nonzero completely primal element of D and $y \in D$. Then x, y have an LCM if and only if x, y have an MCD.*

Proof. The "only if" part is clear. Conversely, dividing x, y by an MCD of them, we may assume that x, y are coprime. Assume that $x \mid yy'$, with $y' \in D$. Since x is primal, x can be written as $x = zz'$ with $z \mid y$, $z' \mid y'$. It follows that $z \mid x, y$, so z is a unit, hence $x \mid y'$. Consequently, x, y are v-coprime, that is, their LCM is xy. •

Remark 3.2 Let D be a domain and $T \subseteq D$ a saturated multiplicative set consisting of completely primal elements of D.

(i) By Lemma 3.1, T is splitting if and only if every nonzero element $a \in D$ has a maximal divisor in T (i.e. an $t \in T$ such that $t \mid a$ and w does not divide a/t for each nonunit $w \in T$).

(ii) By Lemma 3.1 and [1, Proposition 2.4], T is lcm splitting if and only if T is splitting and every two elements of T have an MCD.

(iii) Let $A = B \times_{B/M} A'$ be a pullback such that $S' = p(S)U(A')$ and S consists of completely primal elements of A (hence so does S' in A', cf. part (iii) of Lemma 2.2). Let $s \in S$ and $a \in A \setminus M$. By Lemma 3.1 and part (i) of Lemma 2.1, $LCM_A(a, s)$ exists if and only if so does $LCM_{A'}(p(s), p(a))$. In particular, every two elements of S have an LCM in A if and only if S' has the same property in A'. •

Proposition 3.3 *Let $A = B \times_{B/M} A'$ be a pullback such that $A' \neq B/M$ and $x \in M$ a prime element of B. Then x is an extractor in A if and only if $M = xB$, B' is a quotient ring of A', $S' = p(S)U(A')$ and S' is an lcm splitting multiplicative set in A'.*

Proof. By Corollary 2.5, we may assume that x is completely primal in A, every element of S (resp. S') is (completely) primal in A (resp. A') $S' = p(S)U(A')$ and $B = A_S$ (resp. $B' = A'_{S'}$). We also note that, if $y \in M \setminus xB$, then S is the set of all common divisors of x, y in A, so x, y have no GCD in A. So, we may also assume that $M = xB$. Let $y \in A \setminus M$. Then every common divisor of x, y in A belongs to S. By Lemma 3.1, $LCM_A(x, y)$ exists if and only if y has a maximal divisor in S, if and only if $p(y)$ has a maximal divisor in S', cf. part (i) of Lemma 2.1. By part (i) of Remark 3.2, $LCM_A(x, y)$ exists for each $y \in A \setminus M$ if and only if S' is a splitting multiplicative set of A'. Now, let $y \in M$, say, $y = bx$ with $b \in B$. If $b \in M$, then $LCM_A(x, y) = y$. If not, we can write $b = a/s$ with $a \in A \setminus M$ and $s \in S$. Using well known properties of the LCM symbol, we see that $LCM_A(x, y)$ exists if and only if so does $LCM_A(s, a)$ if and only if so does $LCM_{A'}(p(s), p(a))$, cf. part (iii) of Remark 3.2. Consequently, x is an extractor in A if and only if S' is an lcm splitting multiplicative set in A'. •

The next theorem is the main result of this paper.

Theorem 3.4 *Let $A = B \times_{B/M} A'$ be a pullback such that $A' \neq B/M$ and M contains a prime element of B. Then A is a GCD domain if and only if the following conditions hold:*

(a) *B is a GCD domain,*

(b) *B' is a quotient ring of A' and $S' = p(S)U(A')$,*

(c) *S' is an lcm splitting multiplicative set in A', and*

(d) *M is a principal ideal of B.*

PROOF. The "only if" part follows from Proposition 3.3.

The "if" part. Let x be a generator of M in B. By (c), every element of S' is an extractor, so a completely primal element of A'. By Corollary 2.5, $B = A_S$ and every element of S is completely primal in A. As argued in the proof of Proposition 2.8, A is a pre-Schreier domain. Let $a, b \in A \setminus \{0\}$. According to Lemma 3.1, in order to prove that $GCD(a, b)$ exists, it suffices to see that a, b become coprime in A after multiplying them by a nonzero element of A and/or factoring out a common divisor of them, several times. Let $d = GCD_B(a, b)$. Multiplying with some $s \in S$, we may assume that $d, a/d, b/d \in A$. Factoring out d, we may assume that a, b are coprime in B. Consequently, every common divisor of a, b in A belongs to S. In particular, $x \not|_B a$ or $x \not|_B b$. We separate two cases.

Case 1: $x \not|_B a$, $x |_B b$. Since $S' = p(S)U(A')$ is splitting in A', there exist $s \in S$, $c \in A$ such that $p(a) = p(s)p(c)$ and $p(c)$ is v-coprime to every element of S'. By Lemma 2.1, $s |_A a$. Also, $s |_A b$, because $b \in M$. Dividing a, b by s, we may assume that $p(a)$ is v-coprime to every element of S'. We claim that a, b are coprime in A. Indeed, if $w |_A a, b$, then $w \in S$ and $p(w) |_{A'} p(a)$, so $p(w) |_{A'} 1$, hence $w |_A 1$, by Lemma 2.1.

Case 2: $x \not|_B a$, $x \not|_B b$. Since $S' = p(S)U(A')$ is splitting in A', there exist $s, t, c, d \in A$ such that $p(a) = p(s)p(c)$, $p(b) = p(t)p(d)$ and

$p(c), p(d)$ are v-coprime to every element of $p(S)$. Let $k \in S$, such that $p(k) = GCD_{A'}(p(s), p(t))$. Since $p(k) \mid_{A'} p(a), p(b)$, we get $k \mid_A a, b$, cf. part (i) of Remark 2.1. Factoring out k from a, b, we may assume that $p(s)$, $p(t)$ are v-coprime in A'. We claim that a, b are coprime in A. Indeed, let $w \in A$ such that $w \mid_A a, b$. By a previous reduction, $w \in S$. Hence $p(w) \mid_{A'} p(s), p(t)$, because $p(c), p(d)$ are v-coprime to $p(w)$. So $p(w) \mid_{A'} p(1)$, thus $w \mid_A 1$. •

Corollary 3.5 ([6, Theorem 1.1], [4, Theorem 2.11]) *Let $C \subseteq D$ be an extension of domains, set $T = U(D) \cap C$ and let E denote $D[X]$ or $D[[X]]$. Then $C + XE$ is a GCD domain if and only if both of C, E are GCD domains, $D = C_T$ and T is a splitting multiplicative set of C.*

Remark 3.6 We keep the notations of Theorem 3.4 and assume that A is a GCD domain.

(i) By [13, Theorem 3.1], A' is a GCD domain if and only if so is B'.

(ii) In the following example, A' is not a GCD domain. We take $B = \mathbf{Z}[X]_S$, where $S = \{1, 5, 5^2, ..\}$, $B' = \mathbf{Z}[\sqrt{-3}]_S$, $p : B \to B'$ is the $\mathbf{Z}$-algebra homomorphism sending X into $\sqrt{-3}$ and $A' = \mathbf{Z}[\sqrt{-3}]$. Note that $B/M = B'$, where $M = (X^2 + 3)\mathbf{Z}_S[X]$. We may apply Theorem 3.4, because S' is generated by a prime element of the Noetherian domain A' and $p(U(B)) = U(B')$. By pullback, we obtain the GCD domain $A = B \times_{B/M} A' = \mathbf{Z}[X] + (X^2 + 3)\mathbf{Z}_S[X]$.

(iii) If M does not contain prime elements, Theorem 3.4 fails, as the next example shows. We take the pullback $A = B \times_{B/M} A'$, where $B = \mathbf{Z}[Y/2] + X\mathbf{Z}[Y/2]_S[X]$ with $S = \{1, 2, 4, ..., 2^n, ..\}$, $B' = \mathbf{Z}[Y/2]$, M the kernel of the canonical homomorphism $B \to B'$ and $A' = \mathbf{Z}[Y]$. So, $A = B \times_{B/M} A' = \mathbf{Z}[Y] + X\mathbf{Z}[Y]_S[X]$. All the rings A, A', B, B' are GCD domains, but B' is not a quotient ring of A'.

(iv) In [10, Theorem 4.2] and [16, Corollaries 3.4 and 3.5], there are given necessary and sufficient conditions for A to be a GCD domain, in the case when M is a maximal ideal, not necessarily containing prime elements.

Corollary 3.7 *Let D be a domain, Q a prime ideal of D and $x \in Q$ a prime element. If D/xD is a UFD and D_Q is a GCD domain, then $D + xD_Q$ is a GCD domain.*

Proof. By [6, Corollary 1.2], every multiplicative set of a UFD is splitting, hence good. We can apply Theorem 3.4 for the pullback $D + xD_Q =$

$D_Q \times_{D_Q/xD_Q} D/xD$, cf. part (ii) of Lemma 2.1 and "$(e) \Leftrightarrow (f)$" in Theorem 2.3. $\bullet$

Cf. [11, Proposition 11.8], $D= \mathbf{C}[X,Y,Z]/(X^2+Y^2+Z^2-1)=\mathbf{C}[x,y,z]$ is not a UFD, but D/XD is so. Hence we may apply the preceding corollary for D, $Q=(X,Y,Z-1)D$ and $x=X$ (note that D_Q is a regular local ring). We obtain the GCD domain $\mathbf{C}[y,z]+x\mathbf{C}[x,y,z]_{(x,y,z-1)}$, where $x^2+y^2+z^2=1$.

Corollary 3.8 *Let D be a domain and $x,f \in D$ such that x is a prime element of D and $f+xD$ is a prime element of D/xD. Then $D+xD_f$ is a GCD domain if and only if D_f is a GCD domain and $\cap_{n\geq 1}(f^nD+xD)=xD$.*

PROOF. We apply Theorem 3.4 for the pullback $D+xD_f = D_f \times_{D_f/xD_f} D/xD$. Since $f+xD$ is prime in D/xD, we get that $S'=p(S)U(A')$ and S' is consisting of extractors. So, $D+xD_f$ is a GCD domain if and only if so is D_f and S' is splitting in A'. Apply [2, Proposition 1.6]. Notice that the example in part (ii) of Remark 3.6 is of this type. $\bullet$

We intend to specialize Theorem 3.4 to the case of semirigid domains and then for the GCD domains of finite t-character. We bring in some new terminology. Let D be an integral domain. Cf. [19], we recall that an element $x \in D$ is said to be *rigid*, if whenever $r,s \in D$ and $r,s \mid x$, we have $r \mid s$ or $s \mid r$. Then D is called *semirigid* if every nonzero nonunit element of D can be expressed as a product of a finite number of rigid elements. Any UFD or valuation domain is a GCD semirigid domain.

Proposition 3.9 *Let $A=B\times_{B/M} A'$ be a pullback such that $A' \neq B/M$, $M=xB$ is a principal nonzero ideal of B and $\cap_{n\geq 1}M^n=0$. Assume that A is a GCD domain. Then A is a semirigid domain if and only if so is B and for every two elements of S' one of them divides the other in A'.*

PROOF. By part (i) of Lemma 2.1, the last part of the condition is equivalent to the same condition for S in A. Assume that A is a semirigid domain. Then so is A_S, cf. [20, Remark 1]. Since each decomposition of x in A is of type $x=s(x/s)$ for some $s\in S$, some x/s has to be rigid. But the elements of S are divisors of x/s, so for every two elements of S one of them has to divide the other. Conversely, assume that S satisfies this condition and B is semirigid. Then $s, x/s$ are rigid elements for every $s\in S$. Let f be a nonzero nonunit of A. We show that f is a product of rigid elements. If $f\in M$, we write $f=x^i(a/s)$ for some $i\geq 1$, $a\in A\setminus M$ and $s\in S$. Since

$f = x^{i-1}(x/s)a$, it suffices to consider only the case $f \notin M$. Since $B = A_S$ is semirigid, there exist $s, t \in S$ and $h_1, ..., h_n \in A \setminus M$ such that $sf = th_1...h_n$ and $h_1, ..., h_n$ are rigid in A. Since S' is splitting in A' and $S' = p(S)U(A')$, we may assume that $s = t = 1$ and $f, h_1, ..., h_n$ are coprime to every element of S. Then every h_i is rigid in A. Indeed, if $q, r \mid_A h_i$, then, say, $q \mid_B r$, hence $q \mid_A rw$ for some $w \in S$. But q is also coprime to every element of S, so $q \mid_A r$. •

Corollary 3.10 *Let $C \subseteq D$ be an extension of domains, set $T = U(D) \cap C$ and let E denote $D[X]$ or $D[[X]]$. Assume that $C + XE$ is a GCD domain. Then $C + XE$ is a semirigid domain if and only if E semirigid and for every two elements of T one of them divides the other in D.*

Recall that an ideal I of a domain D is called a t-ideal if for every finitely generated ideal $J \subseteq I$, $(J^{-1})^{-1} \subseteq I$. If D is a GCD-domain, then I is a t-ideal of D if and only if $GCD(x, y) \in I$ for every $x, y \in I$. A maximal ideal in the set of all proper t-ideals is called a *maximal t-ideal*. It is well known that a maximal t-ideal is a prime ideal. A domain D is called a domain of finite t-character, if every nonzero nonunit element of D belongs to finitely many maximal t-ideals. As a consequence of the main result of [7], it follows that a GCD-domain is of finite t-character if and only if for every infinite sequence $(x_n)_n$ of mutually v-coprime nonunits of D, $\cap_n \sqrt{x_n D} = 0$.

Proposition 3.11 *Let $A = B \times_{B/M} A'$ be a pullback such that $A' \neq B/M$, $M = xB$ is a principal nonzero ideal of B and $\cap_{n \geq 1} M^n = 0$. Assume that A is a GCD domain. Then A is of finite t-character if and only if so is B and there is no infinite sequence of elements of S' which are mutually v-coprime in A'.*

Proof. By Lemma 2.1, Remark 3.2 and Lemma 3.1, the last part of the condition is equivalent to the same condition for S in A. The "only if" part is a consequence of [14, Theorem 7 and Proposition 12] and of the fact that every element of S divides x. Conversely, assume there exists a nonzero nonunit $f \in A$ and an infinite sequence $(g_n)_n$ of mutually coprime nonzero nonunits of A such that $f \in \cap_n \sqrt{g_n A}$. In both cases below we shall contradict the assumption made on S. If $f \in S$, then each g_n is in S. If not, then all but finitely many of $g_n s$ are in S. Indeed, the elements g_n remain mutually coprime in B and B is a domain of finite t-character. •

Corollary 3.12 *Let $C \subseteq D$ be an extension of domains, set $T = U(D) \cap C$ and let E denote $D[X]$ or $D[[X]]$. Assume that $C + XE$ is a GCD domain. Then $C + XE$ is a domain of finite t-character if and only if E semirigid and if and only if so is E and there is no infinite sequence of elements of T which are mutually coprime in D.*

Acknowledgement. The first author gratefully acknowledges the hospitality of The University of Arkansas at Fayetteville during his three-day visit in April, 2000.

References

[1] D.D. Anderson, D.F. Anderson and M. Zafrullah, Splitting the t-class group, *J. Pure Appl. Algebra* 74, 17-37(1991).

[2] D.D. Anderson, D.F. Anderson and M. Zafrullah, Factorization in integral domains II, *J. Algebra* 152, 78-93(1992).

[3] D. D. Anderson and M. Zafrullah, P.M. Cohn's completely primal elements. *In Lecture Notes in Pure and Applied Mathematics*, vol. 171, pp. 115-123. Marcel Dekker, New York (1995).

[4] D.F. Anderson and D. Nour El Abidine, The $A + XB[X]$ and $A + XB[[X]]$ constructions from GCD domains, to appear in *J. Pure Appl. Algebra.*

[5] P.M. Cohn, Bézout rings and their subrings, *Math. Proc. Cambridge Philos. Soc.* 64, 251-264(1968).

[6] D. Costa, J. Mott and M. Zafrullah, The construction $D+XD_S[X]$, *J. Algebra* 53, 423-439(1978).

[7] T. Dumitrescu, Y. Lequain, J. Mott and M. Zafrullah, Almost GCD domains with a finiteness condition, submitted.

[8] T. Dumitrescu, N. Radu, S.I. Al-Salihi and T. Shah, Some factorization properties of composite domains $A+XB[X]$ and $A+XB[[X]]$, *Comm. Algebra* 28, (2000).

[9] T. Dumitrescu and S.I. Al-Salihi, A note on composite domains $A+XB[X]$ and $A+XB[[X]]$, to appear in *Stud. Cerc. Math.*

[10] M. Fontana and S. Gabelli, On the class group and the local class group of a pullback, *J. Algebra* 181, 803-835(1996).

[11] R. Fossum, *The Divisor Class Group of a Krull Domain,* Springer, New York (1973).

[12] R. Gilmer, *Multiplicative Ideal Theory,* Marcel Dekker, New York (1972).

[13] R. Gilmer and T. Parker, Divisibility properties in semigroup rings, *Michigan J. Math.* 21, 65-86(1974).

[14] M. Griffin, Some results on v-multiplication rings, *Canad. J. Math.* 19, 710-722(1967).

[15] I. Kaplansky, *Commutative Rings* (Revised Edition), The University of Chicago Press, Chicago and London (1974).

[16] M. Khalis and D. Nour El Abidine, On the class group of a pullback. *In Lecture Notes in Pure and Applied Mathematics*, vol. 185, pp. 377-386. Marcel Dekker, New York (1997).

[17] S. McAdam and D.E. Rush, Schreier rings, *Bull. London Math. Soc.* 10, 77-80(1978).

[18] M. Roitman, Polynomial extensions of atomic domains, *J. Pure Appl. Algebra* 87, 187-199(1993).

[19] M. Zafrullah, Semirigid GCD-domain elements, *Manuscripta Math.* 17, 55-66(1975).

[20] M. Zafrullah, Rigid elements in GCD-domains, *J. Natur. Sci. Math.* 17, 7-14(1977).

[21] M. Zafrullah, On a property of pre-Schreier domains, *Comm. Algebra* 15, 1895-1920(1987).

[22] M. Zafrullah, On Riesz Groups, *Manuscripta Math.* 80, 225-238(1993).