Palestine Journal of Mathematics

Vol. 8(2)(2019) , 1–7

On the Number of Intermediate Rings When a Decomposed Extension Lies Atop a Ramified Extension, II

David E. Dobbs, Gabriel Picavet and Martine Picavet-L'Hermitte

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 13B99; Secondary 13B21.

Keywords and phrases: Commutative ring, minimal ring extension, integral, ramified, decomposed, special principal ideal ring, unit, conductor, intermediate ring, FIP.

Abstract. Let (R, M) be a special principal ideal ring (SPIR), but not a field. Fix $p \in M$ so that $Rp = M$, and let Y be an indeterminate over R. Let $R \subset S$ be a ramified (integral minimal) ring extension and $S \subset T$ a decomposed (integral minimal) ring extension. Then S is the only ring properly contained between R and T if and only if T is R-algebra isomorphic to $R[Y]/(Y^2 - Y, p^2Y)$; when these equivalent conditions hold, S is R-algebra isomorphic to the idealization $R(+)R/M$. (This result was already known in case either $M^2 = 0$ or $R/M \cong \mathbb{F}_2$.) This work contributes to the characterization of the finite commutative rings with exactly two proper (unital) subrings.

1 Introduction

This paper is a sequel to [8]. All rings and algebras considered below are commutative with identity; all inclusions of rings, ring homomorphisms and algebra homomorphisms are unital. Except in the concluding results, Corollary 2.5 and Remark 2.6, (R, M) denotes a (nonzero) special principal ideal ring (in short, an SPIR), p denotes a fixed element of M such that $Rp = M$, α denotes the index of nilpotence of M (so that $M^\alpha = 0 \neq M^{\alpha-1}$), $U(R)$ denotes the set of units of R, and Y denotes an indeterminate over R. By definition, an SPIR is a quasi-local principal ideal ring whose unique maximal ideal is nilpotent. By convention in this manuscript, no field is considered to be an SPIR. (So, $\alpha \geq 2$.) Adequate background on SPIRs can be found in [15, page 245] (where, for instance, one can find the fact that p is determined up to a factor from $U(R)$). Our main goal here is to establish the following facts. If $R \subset S \subset T$ are rings such that $R \subset S$ is a ramified (integral minimal) ring extension and $S \subset T$ is a decomposed (integral minimal) ring extension, then S is the only ring properly contained between R and T if and only if T is R-algebra isomorphic to $R[Y]/(Y^2-Y, p^2Y)$; when these equivalent conditions hold, S is R-algebra isomorphic to the idealization $R(+)R/M$. (The required background on idealizations can be found in [12].) These facts were established in [8, Example 2.5 and Theorem 2.6] under the assumption that $\alpha = 2$. Our main goal here is accomplished in Proposition 2.3 and Corollary 2.4.

It will be convenient to let $\mathcal{T}$ denote $R[Y]/(Y^2 - Y, p^2Y)$. Our path to Corollary 2.4 can be summarized as follows. Theorem 2.1 (c) establishes that if $R \subset S$ is a ramified ring extension and $S \subset T$ is a decomposed ring extension such that S is the only ring properly contained between R and T, then (regardless of the value of α) either T is R-algebra isomorphic to $\mathcal{T}$ or T is of the form $T(p, u)$, where $T(p, u)$ denotes a certain kind of R-algebra whose definition via generator-and-relations in Section 2 depends on a parameter $u \in U(R)$. Proposition 2.2 (a) shows that if $u \in U(R)$ with $u - 1 \notin M$, then the second option in the conclusion of Theorem 2.1 (c) cannot arise. The same conclusion is shown in Proposition 2.2 (b) for certain $u \in U(R)$ with $u - 1 \in M$. After a case analysis treating the remaining possible descriptions of $u - 1$ in terms of α, Proposition 2.3 uses all the earlier results in the paper to infer that the first option in the conclusion of Theorem 2.1 (c) must arise.

This paper is built on a long sequence of papers that began with the definition of the FIP

property of ring extensions in [1]. Those papers included a characterization of FIP in [7]; a determination in [9, Theorem 4.1] of necessary and sufficient conditions for a juxtaposition of minimal ring extensions $A \subset B$ and $B \subset C$ to be such that $A \subset C$ satisfies FIP; as an application of [9, Theorem 4.1], an attempted determination in [2, Theorem 2.9] of necessary and sufficient conditions for a juxtaposition of minimal ring extensions $A \subset B$ and $B \subset C$ to be such that C is the only ring properly contained between A and B; as an application of [2] (while its author was unaware of an error in [2, Theorem 2.9 (b)]), a first attempt in [3] to characterize the rings with exactly two proper subrings; and, in [8], a correction to [2, Theorem 2.9 (b)] and the resulting errors that had ensued in [3], one upshot being a (valid) characterization of the rings with exactly two proper subrings, including a classification up to isomorphism in the case of characteristic 0 [8, Corollaries 2.17 and 2.18] (see also [5, Corollaries 2.21 and 3.6]).

According to [8, Corollary 2.17] (or [5, Corollary 3.6]), two of the six parts of the above-mentioned characterization in the case of positive characteristic fell short of providing a classification up to isomorphism. Those two parts concerned certain towers $A \subset B$ and $B \subset C$ of integral minimal ring extensions of finite rings, where A is of the form $\mathbb{Z}/p^\alpha\mathbb{Z}$ with p a prime number and $\alpha \geq 2$, $A \subset B$ is ramified, and $B \subset C$ is either ramified or decomposed. In the situation where $B \subset C$ is ramified, apart from the characterization given in [5, Theorem 3.1] and the subcase for which a classification was found in [5, Corollary 3.7], it seems that nothing further is known at this time. As for the situation where $B \subset C$ is decomposed, Proposition 2.3 and Corollary 2.4 settle that question, while Corollary 2.5 and Remark 2.6 explain how the work in this paper contributes to the overall question of classification up to isomorphism.

We assume that the reader has a copy of [8] (and possibly also copies of [7], [9] and [2]) at hand. Nevertheless, for the sale of completeness, we next recall some notation and provide a modicum of background on minimal ring extensions. If $A \subseteq B$ are rings, then $[A, B]$ denotes the set of "intermediate rings," that is, the set of rings D such that $A \subseteq D \subseteq B$. As in [10], a ring extension $A \subset B$ is called a *minimal ring extension* if there does not exist a ring properly contained between A and B. A minimal ring extension $A \subset B$ is either integrally closed (in the sense that A is integrally closed in B) or integral. If $A \subset B$ is a minimal ring extension, it follows from [10, Théorème 2.2 (i) and Lemme 1.3] that there exists a unique maximal ideal M of A (called the *crucial maximal ideal* of $A \subset B$) such that the canonical injective ring homomorphism $A_M \to B_M$ can be viewed as a minimal ring extension while the canonical ring homomorphism $A_P \to B_P$ is an isomorphism for all prime ideals P of A except M. If $A \subset B$ is an integral minimal ring extension with crucial maximal ideal M, there are three possibilities: $A \subset B$ is said to be respectively *inert*, *ramified*, or *decomposed* if $B/MB\,(= B/M)$ is isomorphic, as an algebra over the field $K := A/M$, to a minimal field extension of K, $K[X]/(X^2)$, or $K \times K$.

If A is a ring, then $\mathrm{Spec}(A)$ denotes the set of prime ideals of A. As usual, if A is a ring with E an A-module and $P \in \mathrm{Spec}(A)$, then $E_P := E_{A\setminus P}$; $\mathbb{F}_q$ denotes the finite field of cardinality q; $\subset$ denotes proper inclusion; and $|U|$ denotes the cardinal number of a set U. (In particular, if $A \subset B \subset C$ are rings, then B is the only ring contained properly between A and C if and only if $|[A, C]| = 3$.) The symbols X and Y denote indeterminates over the ambient ring(s). We use the standard notation for conductors and annihilators. Any unexplained material is standard, as in [11], [13].

2 Results

Let (R, M) be an SPIR, with $p \in M$ such that $Rp = M$. If $u \in U(R)$, it will be convenient to say that an R-algebra T is an *R-algebra of the form $T(p, u)$* if there exists $y \in T$ such that $T = R[y]$, $y^2 = y$ and $p^2y = p^2u$ (in T). Notice that R-algebras of the form $T(p, u)$ need not be R-algebra isomorphic. Indeed, 0 is an R-algebra of the form $T(p, u)$, as is the (nonzero) R-algebra $R[X]/(X^2 - X, p^2X - p^2u)$. In particular, if T is an R-algebra of the form $T(p, u)$ whose structure is induced by a ring homomorphism $f : R \to T$, then f need not be an injection. Two relevant situations where such a structure map is shown to not be an injection are given in Proposition 2.2, which considers certain kinds of R-algebras of the form $T(p, u)$. This result allows Proposition 2.3 to focus attention on some relevant different kinds of R-algebras of the form $T(p, u)$. We begin with Theorem 2.1, whose part (c) presents a dichotomy in which R-

algebras of the form $T(p,u)$ play an essential role.

Theorem 2.1. Let (R,M) be an SPIR. Fix $p \in M$ so that $Rp = M$, and let Y be an indeterminate over R. Let $R \subset S$ be a ramified ring extension and $S \subset T$ a decomposed ring extension such that $|[R,T]| = 3$. Let α (≥ 2) denote the index of nilpotence of M, and let N denote the unique prime ideal of S. Then:

(a) There exists a (necessarily nonunit) element y of T such that $T = R[y]$, $y^2 = y$, and either $p^2y = 0$ or $p^2y = p^2u$ for some $u \in U(R)$. For any such element y, the element $py \in N \setminus R = N \setminus M$; moreover, $S = R[py]$, $(py)^2 \in M$ and $(py)^3 \in M$.

(b) If there exists $y \in T$ such that $T = R[y]$, $y^2 = y$ and $p^2y = 0$, then T is R-algebra isomorphic to $\mathcal{T}$ $(:= R[Y]/(Y^2 - Y, p^2Y))$.

(c) Either T is R-algebra isomorphic to $\mathcal{T}$ or T is an R-algebra of the form $T(p,u)$ for some $u \in U(R)$.

(d) If T is an R-algebra of the form $T(p,1)$ (that is, $T(p,u)$ with $u = 1$), then T is R-algebra isomorphic to $\mathcal{T}$.

Proof. We assume familiarity with the basic properties and characterizations of ramified extensions and decomposed extensions that were collected in [7, Theorems 2.2 and 2.3]. As in the first paragraph of the proof of [8, Theorem 2.2], the hypothesis that $R \subset S$ is ramified and the fact that M is the only prime ideal of R combine to show that S has a unique prime ideal, say, N. (We will not explicitly mention appeals to standard facts about the behavior of prime ideals in integral extensions, such as the Lying-over Theorem, as we assume familiarity with those facts, as in [11], [13].) Then, necessarily, N is the crucial maximal ideal of $S \subset T$, and so $(S : T) = N$ by [10, Théorème 2.2 (ii)]. In particular, $yN \subseteq N$. Also, the hypothesis that $S \subset T$ is decomposed and the fact that N is the only prime ideal of S combine to show that T has only two (distinct) prime ideals, say, Q_1 and Q_2; and that $Q_1Q_2 = Q_1 \cap Q_2 = N$; moreover, there exists $y \in T$ such that $T = S[y]$, $y^2 - y \in N$ and, of course, $yN \subseteq N$. It follows easily that $T = S + Sy$. Note also that $y \in Q_1 \cup Q_2$ (for if y were a unit of T, then $y - 1 = y^{-1}(y^2 - y) \in TN = N \subseteq S$ and $T = S[y-1] \subseteq S$, a contradiction to the fact that $S \subset T$). In addition, the hypothesis that $R \subset S$ is ramified (necessarily with crucial maximal ideal M) provides $x \in N$ such that $S = R[x]$, $x^2 \in N^2 \subseteq M$ and, similarly, $x^3 = x^2x \in M$, so that $S = R + Rx$. Furthermore, if y is as above, then, since $xy \in NT = N \subseteq S$, we see that $T = S + Sy = (R + Rx) + (R + Rx)y = R + Rx + Ry$. It will be useful to observe that py has all the above-mentioned properties of x. (Here is how to see the most important of those facts, with the others following as above. Since $|[R,T]| = 3$ and [8, Theorem 2.2] yield that $(R : T) = M^2$, the hypothesis that R is an SPIR then ensures that $p \notin M^2 = (R :_R y)$, so that $py \in N(Q_1 \cup Q_2) \setminus R \subseteq N \setminus R = N \setminus M$, whence $S = R[py]$ by the minimality of $R \subset S$.) Next, observe that it is clear from the construction of $\mathcal{T}$ that, if T is R-algebra isomorphic to $\mathcal{T}$, then there exists $w \in T$ such that $T = R[w]$, $w^2 = w$ and $p^2w = 0$. For the case $\alpha = 2$, Example 2.5 and Theorem 2.6 of [8] can be combined to show that T *is* R-algebra isomorphic to $\mathcal{T}$. Thus, it follows from the above comments that, in the proofs of (a)-(d), we may suppose henceforth that $\alpha \geq 3$.

(a) Suppose, for the moment, that we have been able to choose the (necessarily nonunit) element y so that $T = R[y]$ and $y^2 = y$. In that case, the above comments allow us to choose $x = py$. Then $px = p^2y = p^2y^2 = (py)^2 = x^2$. In addition, the assertions in the final sentence of the statement of (a) then follow from the preceding paragraph. Thus, having momentarily assumed that $y^2 = y$, we may also assume, without loss of generality, that $p^2y \neq 0$. Since $p^2y = p(py) \in N^2 \subseteq M$, the hypothesis that R is an SPIR provides a positive integer $k \leq \alpha - 1$ and $u \in U(R)$ such that $p^2y = p^ku$. As in the beginning of the fourth paragraph of the proof of [8, Theorem 2.6], the hypotheses ensure that $k \neq 1$. Hence, without loss of generality, $3 \leq k$ (and $\alpha \geq 4$). Then, by reworking the subsequent part of the fourth paragraph of the proof of [8, Theorem 2.6], we can construct an element $z \in T$ such that $T = R[z]$, $z^2 = z$ and $p^2z = 0$. Thus, to complete the proof of (a), it will suffice to prove that we can indeed find an element y so that $T = R[y]$ and $y^2 = y$.

As noted above, we do have an element y such that $T = S[y]$ and $y^2 - y \in N$. Hence $y \notin S$ (for otherwise, $T = S[y] = S$, a contradiction); *a fortiori*, $y \notin R$. Since $R[y] \in [R,T] = \{R, S, T\}$, it follows by the process of elimination that $R[y] = T$. We now proceed with an indirect argument; that is, we suppose that a satisfactory replacement for y cannot be found (and

we seek a contradiction).

Since N is the unique prime ideal of S, N is a nil ideal (cf. [11, Corollary 2.10]). As idempotents can be lifted modulo any nil ideal (cf. [14, Proposition 1, page 72]), there exists $e = e^2 \in T$ such that $\zeta := y - e \in N$. It is known that $N = M + Rx$ (see, for instance, the first paragraph of the proof of [8, Theorem 2.6]). Now, if $m \in M$, we have $T = R[y - m]$ and $(y-m)^2-(y-m) \in N$, the latter point following since $y^2-y \in N$, $M \subseteq N$ and $2my \in NT = T$. Thus, by harmlessly modifying y (and ζ) by subtracting an element of M, we can assume that $\zeta \in Rx$. Choose $r \in R$ such that $\zeta = rx$. Observe that $Mx \subseteq N^2 \subseteq M$. So if $r \in M$, then $y - e \in M$ and, harmlessly modifying y (and ζ) by subtracting an element of M, we would be able to replace y with the idempotent e (and we would have the desired contradiction). Thus, without loss of generality $r \in R \setminus M = U(R)$. Then there is no harm in replacing x with rx, and so we can assume that $\zeta = x$; that is, $y = e + x$. Then $T = S[y] = S[e + x] = S[e]$, the last equation holding since $x \in S$. But $R[e] \neq S$ since $e \notin S$ (for otherwise, $y = \zeta + e \in N + S = S$ and $T = S[y] \subseteq S$, a contradiction); *a fortiori*, $R[e] \neq R$. By another application of the process of elimination, $R[e] = T$. Thus, e has the properties that no element y was supposed to have. This (desired) contradiction completes the proof of (a).

(b) By hypothesis, there exists (a nonunit element) $z \in T$ such that $T = R[z]$, $z^2 = z$ and $p^2z = 0$. By the final assertion in (a), we may redefine $x := pz \in N \setminus R$, with the upshot that $x^2 = p^2z = px = 0$ and $S = R[x] = R + Rx = R + Rpz$. But we can say more, by using a set $\mathfrak{S}$ that figured prominently in several proofs in [5] and [8].

Considering M as an additive subgroup of R, choose a set $\mathfrak{S}$ of coset representatives of M in R with the property that $\{0, 1\} \subseteq \mathfrak{S}$. As in the proof of [8, Theorem 2.6], we have $T = R + \mathfrak{S}pz+\mathfrak{S}z$, in the sense that each element of T can be uniquely expressed in the form $a+\sigma pz+\tau z$ where $a \in R$ and $\sigma, \tau \in \mathfrak{S}$. Note that when the elements of T are expressed in this way, the addition and multiplication tables for T are determined (with answers unambiguously expressed in the form $a + \sigma pz + \tau z$), essentially for the following reasons: the arithmetic operations on R are given; each element of R is of the form $\lambda + \mu$ for some uniquely determined $\lambda \in \mathfrak{S}$ and $\mu \in M$; $z^2 = z$; $(pz)^2 = 0$; $(pz)z = pz$; and $Mpz = Rp^2z = 0$.

Similarly, combining [8, Example 2.5] and the proof of [8, Theorem 2.6], $y_1 := Y + (Y^2 - Y, p^2Y) \in \mathcal{T}$ and $x_1 := py_1$ are such that $\mathcal{T} = R[y_1]$, $y_1^2 = y_1$, $p^2y_1 = 0$, $x_1^2 = 0$ and $x_1 \in N_1 \setminus R$, where N_1 denotes the unique prime ideal of the unique element S_1 of $[R, \mathcal{T}] \setminus \{R, \mathcal{T}\}$; and $\mathcal{T} = R + \mathfrak{S}x_1 + \mathfrak{S}y_1$, in the sense that each element of $\mathcal{T}$ can be uniquely expressed in the form $a + \sigma x_1 + \tau y_1$ where $a \in R$ and $\sigma, \tau \in \mathfrak{S}$. As above, the addition and multiplication tables for T are determined. Define a function $g : \mathcal{T} \to T$ as follows. If $\xi \in \mathcal{T}$, express ξ as $a + \sigma x_1 + \tau y_1$ where $a \in R$ and $\{\sigma, \tau\} \subseteq \mathfrak{S}$; then let

$$g(\xi) = g(a + \sigma x_1 + \tau y_1) := a + \sigma pz + \tau z.$$

By the above comments about unique expressibility, it is clear that g is a bijection. Moreover, since the addition (resp., multiplication) tables for $\mathcal{T}$ and T are completed in essentially the same way, it is also clear that g is an R-algebra homomorphism. (For a more formal proof of the preceding assertion, one can repeat *verbatim* the thirteenth through the sixteenth paragraphs of the proof of [8, Theorem 2.6].) Therefore, g is an R-algebra isomorphism from $\mathcal{T}$ (on)to T.

(c) It suffices to combine (a) and (b) with the definition of an R-algebra of the form $T(p, u)$.

(d) Since T is an R-algebra of the form $T(p, 1)$, there exists $y \in T$ such that $T = R[y]$, $y^2 = y$ and $p^2y = p^2$ (in T). Then $z := 1 - y \in T$ satisfies $R[z] = R[y] = T$, $z^2 = 1 - 2y + y^2 = 1 - 2y + y = 1 - y = z$ and $p^2z = p^2 - p^2y = 0$. Replacing y with z, we now see that an application of (b) completes the proof. □

We show next that if the second option in the conclusion of Theorem 2.1 (c) holds and $M^2 \neq 0$, some important necessary conditions are imposed on the unit u.

Proposition 2.2. Let (R, M) be an SPIR. Let α denote the index of nilpotence of M, and suppose that $\alpha \neq 2$ (that is, $\alpha \geq 3$). Fix $p \in M$ so that $Rp = M$. Let $u \in U(R)$. Let T be an R-algebra of the form $T(p, u)$ whose structure is induced by a ring homomorphism $f : R \to T$. Suppose that either (a) $u - 1 \notin M$ (that is, $u - 1 \in U(R)$) or (b) $0 \neq u - 1 \in M^k \setminus M^{k+1}$ with $1 \leq k < \alpha - 2$. Then f is not an injection.

Proof. (a) Set $b_0 := b_1 := b_2 := 1,\ b_3 := (1-u)^{-1}(p-1) - 2$, $a_0 := p^2(1-u),\ a_1 := -p^2[p-2(1-u)]$ and $a_2 := -p^2[(1-u)^{-1}(p-1)-2] = -p^2 b_3$. Since T is an R-algebra of the form $T(p,u)$, we have $T = R[y]$ and $y^2 - y = 0 = p^2 y - p^2 u$. Thus

$$0 = (y^2 - y)(a_2 y^2 + a_1 y + a_0) + (p^2 y - p^2 u)(b_3 y^3 + b_2 y^2 + b_1 y + b_0).$$

It is straightforward to check that the displayed expression simplifies to $0 = p^3 y^2 - p^2 u$. Hence $p^3 y = p^3 y^2 = p^2 u = p^2 y$. Then $p^3 y - p^2 y = 0$, and so $(p-1)p^2 y = 0$. Since $p - 1 \in U(R)$, multiplication by $(p-1)^{-1}$ gives $p^2 y = 0$. Thus $p^2 u = 0$ in T, whence $p^2 = 0$ in T; that is, $f(p^2) = 0$. But $p^2 \neq 0$ in R since $\alpha \neq 2$, and so f is not an injection.

(b) Since R is an SPIR, the hypothesis allows us to write $1 - u = p^k v$ for some $1 \leq k < \alpha - 2$ and $v \in U(R)$. Consequently $p^{k+2} \neq 0$, since $k+2 < \alpha$. Set $b_0 := p^k v$, $b_1 := b_2 =: 0$, $b_3 := -1$, $a_0 := a_1 := p^{k+2} v$ and $a_2 = p^2$. Since T is an R-algebra of the form $T(p,u)$, we have $T = R[y]$ and $y^2 - y = 0 = p^2 y - p^2 u = p^2 y - p^2 + p^{k+2} v$. Thus

$$0 = (y^2 - y)(a_2 y^2 + a_1 y + a_0) + (p^2 y - p^2 u)(b_3 y^3 + b_2 y^2 + b_1 y + b_0).$$

It is straightforward to check that the displayed expression simplifies to $0 = -uvp^{k+2}$ (in T); that is, $f(-uvp^{k+2}) = 0$. Hence $f(p^{k+2}) = (-uv)^{-1} f(-uvp^{k+2}) = 0$. But $p^{k+2} \neq 0$ in R, and so f is not an injection. □

In view of Theorem 2.1 and Proposition 2.2, one should study more deeply R-algebras T of the form $T(p,u)$ for units u such that $u - 1 \in M$. For that context, Proposition 2.3 gives the final steps in resolving our main question.

Proposition 2.3. Let (R, M) be an SPIR. Let α denote the index of nilpotence of M. Fix $p \in M$ so that $Rp = M$. Let $R \subset S$ be a ramified ring extension and $S \subset T$ a decomposed ring extension such that $|[R,T]| = 3$. Then T is R-algebra isomorphic to $\mathcal{T}$.

Proof. By [8, Theorem 2.6], parts (c) and (d) of Theorem 2.1, and Proposition 2.2, we may assume, without loss of generality, that T is an R-algebra of the form $T(p,u)$ for some $u \in U(R)$ such that $0 \neq u - 1 \in M^k \setminus M^{k+1}$ with $1 \leq \alpha - 2 \leq k \leq \alpha - 1$. By the definition of an R-algebra of the form $T(p,u)$, we have $T = R[y]$, with $y^2 = y$ and $p^2 y = p^2 u$. Since R is an SPIR, the hypothesis allows us to write $1 - u = p^k v$, with ($1 \leq \alpha - 2 \leq k \leq \alpha - 1$ and) $v \in U(R)$. Then, since $k + 2 \geq \alpha$ ensures that $p^{k+2} = 0$,

$$p^2 y = p^2 u = p^2(1 - p^k v) = p^2 - p^{k+2} v = p^2.$$

Thus, without loss of generality, $u = 1$. Therefore, an application of Theorem 2.1 (d) completes the proof. □

We can now extend the first assertion in [8, Theorem 2.6] from the case $\alpha = 2$ to the general case.

Corollary 2.4. Let (R, M) be an SPIR. Fix $p \in M$ so that $Rp = M$. Let α denote the index of nilpotence of M, and let Y be an indeterminate over R. Then:

(a) Let $R \subset S$ be a ramified ring extension and $S \subset T$ a decomposed ring extension. Then $|[R,T]| = 3$ if and only if T is R-algebra isomorphic to $R[Y]/(Y^2 - Y, p^2 Y)$; when these equivalent conditions hold, S is R-algebra isomorphic to the idealization $R(+)R/M$.

(b) Let T be a ring having R as a subring. Then T is R-algebra isomorphic to $R[Y]/(Y^2 - Y, p^2 Y)$ if and only if there exists $S \in [R,T]$ such that $R \subset S$ is a ramified ring extension, $S \subset T$ is a decomposed ring extension and $|[R,T]| = 3$.

Proof. According to [8, Example 2.5], $\mathcal{T} := R[Y]/(Y^2 - Y, p^2 Y)$ has a subring, say S_1, such that $R \subset S_1$ is ramified, $S_1 \subset \mathcal{T}$ is decomposed, $|[R,\mathcal{T}]| = 3$, and S_1 is R-algebra isomorphic to $R(+)R/M$. Now, consider any ring extension $R \subseteq T$ such that there exists an R-algebra isomorphism $g : \mathcal{T} \to T$. Then the assignment $E \mapsto g(E)$ determines a bijection $[R,\mathcal{T}] \to [R,T]$, and so $|[R,T]| = |[R,\mathcal{T}]| = 3$. In addition, $S^* := g(S_1)$ is such that $R \subset S^*$ is a ramified ring extension and $S^* \subset T$ a decomposed ring extension. (Indeed, $R \subset S^*$ (resp., $S^* \subset T$)

inherits the property of being a minimal ring extension from $R \subset S$ (resp., $S \subset T$), by [4, Lemma 2.1 (a)]; it is also straightforward to see that ring isomorphisms preserve the "ramified" and "decomposed" (and "inert") properties.) Thus, S^* is the unique element of $[R,T] \setminus \{R,T\}$. Also, since $g|_{S_1} : S_1 \to S^*$ is an R-algebra isomorphism, we get that $S^* \cong (S_1 \cong) R(+)R/M$ as R-algebras.

(a) In view of the above comments, it remains only to prove that if $|[R,T]| = 3$, then T is R-algebra isomorphic to $\mathcal{T}$. This, in turn, follows from Proposition 2.3.

(b) The "only if" assertion follows from the above comments, while the "if" assertion was established in (a). □

We can now deduce the following improvement of [8, Corollary 2.17] (equivalently, of [5, Corollary 3.6]).

Corollary 2.5. Up to isomorphism, the rings R of positive characteristic that have exactly two proper subrings can be characterized as follows. The prime ring of R is (isomorphic to) the direct product $\prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, where $p = p_1, p_2, \ldots, p_k$ are pairwise distinct prime numbers for some positive integer k and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers (and possibly $\alpha_i = \alpha_j$ for some $i \neq j$). Then (up to isomorphism), R is the direct product $E \times \prod_{i=2}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, where E is a ring satisfying (exactly) one of the following six conditions:

(a) $E = \mathbb{F}_{p^{q^2}}$, where q is a prime number (which is possibly equal to p);

(b) $E = \mathbb{F}_{p^q} \times \mathbb{F}_p$, where q is a prime number (which is possibly equal to p);

(c) $E = R_1$, the ring that was constructed (in terms of any given prime number p) in [3, Proposition 2.11];

(d) $\alpha \geq 2$ and $E = \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{F}_{p^q}$, where q is a prime number (which is possibly equal to p);

(e) $\alpha \geq 2$, there exists a (local) ring (B,N) such that both $A := \mathbb{Z}/p^\alpha\mathbb{Z} \subset B$ and $B \subset E$ are ramified extensions, and there exists an element y such that $E = B[y]$, $y^2 \in B$, $y^3 \in B$, $yN \subseteq N$ and either $y^2 \notin A$ or $py \notin A$.

(f) $E = R[Y]/(Y^2 - Y, p^2Y)$, where $R := \mathbb{Z}/p^\alpha\mathbb{Z}$ with p a prime number, $\alpha \geq 2$ an integer, and Y an indeterminate over R.

Furthermore, for each prime number p and each integer $\alpha \geq 2$, there exist at least two, but only finitely many, isomorphism classes of rings R that form part of a set of data satisfying the above condition (e).

Proof. The statement of this corollary has been obtained by replacing condition (f) of [8, Corollary 2.17] with the above condition (f). For the sake of completeness, we recall that condition (f) of [8, Corollary 2.17] states the following: "$\alpha \geq 2$, there exists a (local) ring (B,N) such that $A := \mathbb{Z}/p^\alpha\mathbb{Z} \subset B$ is a ramified extension, $B \subset E$ is a decomposed extension, and the maximal ideal M of A satisfies $(A : E) = M^2$." In the just-quoted condition, the clause "the maximal ideal M of A satisfies $(A : E) = M^2$" can be replaced by "$|[A,E]| = 3$", in view of [8, Theorem 2.2]. It now follows from Corollary 2.4 (b) that the two conditions (f) are equivalent. □

Remark 2.6. (a) As noted in the Introduction, one has yet to classify up to isomorphism the rings E satisfying condition (e) in Corollary 2.5. If/when that classification will be completed, one will have a classification up to isomorphism of the rings having exactly two proper subrings. Indeed, we noted earlier that [5] and [8] provided such a classification for the case of characteristic 0, and so we need only indicate why a satisfactory handling of condition (e) would suffice to give a corresponding classification for positive characteristic. This fact can perhaps be seen on the basis of category theory, building on the fact that if Λ_1 and Λ_2 are rings, then the category of $(\Lambda_1 \times \Lambda_2)$-modules is equivalent to the product of the category of Λ_1-modules and the category of Λ_2-modules. But more prosaic methods can be used to show that isomorphisms of relevant algebras over rings of the form $\prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ can be characterized by "coordinatewise isomorphisms": see [6, Remark 2.5]. Moreover, other prosaic methods can be used to establish a more general result, namely, that isomorphisms of relevant algebras can be characterized by "coordinatewise isomorphisms" when working over base rings that are arbitrary (possible infinite) direct products of rings: see [6, Theorem 2.2 or Corollary 2.3].

(b) It may be helpful to recast some of the above comments here. The sharpening of condition (f) from [8, Corollary 2.17] that was given in condition (f) of Corollary 2.5 can be combined with the comments in (a) in order to classify up to isomorphism the rings $\mathcal{E}$ of (positive) characteristic

$n := \prod_{i=1}^{k} p_i^{\alpha_i}$, where $p_1, p_2, \ldots, p_k$ is a nonempty finite list of pairwise distinct prime numbers and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers (and possibly $\alpha_i = \alpha_j$ for some $i \neq j$), such that there exist a ramified extension $\mathcal{A} \cong \mathbb{Z}/n\mathbb{Z} \subset \mathcal{B}$ and a decomposed extension $\mathcal{B} \subset \mathcal{E}$ with $|[\mathcal{A}, \mathcal{E}]| = 3$. Similarly, if/when the classification up to isomorphism of the rings E satisfying condition (e) in Corollary 2.5 will be completed, the upshot will be the classification up to isomorphism of the rings $\mathcal{E}$ of (positive) characteristic n such that there exist a ramified extension $\mathcal{A} \cong \mathbb{Z}/n\mathbb{Z} \subset \mathcal{B}$ and a ramified extension $\mathcal{B} \subset \mathcal{E}$ with $|[\mathcal{A}, \mathcal{E}]| = 3$. If/when that will be achieved, it will follow from the work in [3], [5], [8] and this paper that the rings with exactly two proper subrings will have been classified up to isomorphism.

References

[1] D. D. Anderson, D. E. Dobbs and B. Mullins, The primitive element theorem for commutative algebras, Houston J. Math. **25** (1999), 603–623.

[2] D. E. Dobbs, When the juxtaposition of two minimal ring extensions produces no new intermediate rings, Pales. J. Math. **6** (1) (2017), 31-44. Corrigendum, Pales. J. Math. **7** (1) 2018, 32–34.

[3] D. E. Dobbs, On the commutative rings with at most two proper subrings, Int. J. Math. Math. Sci., volume 2016, Article ID 6912360, 13 pages, 2016. doi:10.1155/2016/6912360.

[4] D. E. Dobbs, Commutative rings with a prescribed number of isomorphism classes of minimal ring extensions, pp. 145–158, in Rings, Polynomials, and Modules (ed. by M. Fontana, S. Frisch, S. Glaz, P. Zanardo and F. Tartarone), Springer, 2017.

[5] D. E. Dobbs, Certain towers of ramified minimal ring extensions of commutative rings, Comm. Algebra **46** (8) (2018), 3461–3495. doi:10.1080/00927872.2017.1412446.

[6] D. E. Dobbs, Is $A \times B$ isomorphic to $B \times A$?, Far East J. Math. Sci. **108** (2) (2018), 217–228.

[7] D. E. Dobbs, G. Picavet, and M. Picavet-L'Hermitte, Characterizing the ring extensions that satisfy FIP or FCP, J. Algebra **371** (2012), 391–429.

[8] D. E. Dobbs, G. Picavet, and M. Picavet-L'Hermitte, On the number of intermediate rings when a decomposed extension lies atop a ramified extension, Pales. J. Math. **7** (2) (2018), 363–384.

[9] D. E. Dobbs and J. Shapiro, When only finitely many intermediate rings result from juxtaposing two minimal ring extensions, Pales. J. Math. **5** (Spec1) (2016), 13–31.

[10] D. Ferrand and J.-P. Olivier, Homomorphismes minimaux d'anneaux, J. Algebra **16** (1970), 461–471.

[11] R. Gilmer, Multiplicative Ideal Theory, Dekker, New York, 1972.

[12] J. A. Huckaba, Commutative Rings with Zero Divisors, Dekker, New York, 1988.

[13] I. Kaplansky, Commutative Rings, rev. ed., Univ. Chicago Press, Chicago, 1974.

[14] J. Lambek, Lectures on Rings and Modules, Blaisdell, Waltham (MA)-Toronto-London, 1966.

[15] O. Zariski and P. Samuel, Commutative Algebra, Volume I, Van Nostrand, Princeton-Toronto-London, 1958.

Author information

David E. Dobbs, Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1320, USA.
E-mail: dedobbs@comporium.net

Gabriel Picavet, Laboratoire de Mathématiques, Université Blaise Pascal, UMR6620 CNRS, Les Cézeaux, 24, avenue des Landais, BP 80026, 63177 Aubière CEDEX, France.
E-mail: Gabriel.Picavet@math.univ-bpclermont.fr, picavet.gm(at)wanadoo.fr

Martine Picavet-L'Hermitte, Laboratoire de Mathématiques, Université Blaise Pascal, UMR6620 CNRS, Les Cézeaux, 24, avenue des Landais, BP 80026, 63177 Aubière CEDEX, France.
E-mail: Martine.Picavet@math.univ-bpclermont.fr

Received: May 2, 2018.
Accepted: October 21, 2018