Palestine Journal of Mathematics

Vol. 7(2)(2018) , 363–384

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

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

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 13B99; Secondary 13B21, 13G05.

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

Abstract. Let R be either a Dedekind domain or a special principal ideal ring (SPIR), but not a field. Let $R \subset S$ be a ramified (integral minimal) ring extension with crucial maximal ideal M and $S \subset T$ a decomposed (integral minimal) ring extension with crucial maximal ideal N such that $N \cap R = M$. Then S is the only ring properly contained between R and T if and only if the conductor $(R : T) = M^2$. (The preceding conclusion fails if R is a field.) If R is an SPIR and $(R : T) = M^2$, with either $M^2 = 0$ or $R/M \cong \mathbb{F}_2$, then S and T are determined up to R-algebra isomorphism. For certain SPIRs R, an example is given of such chains $R \subset S_i \subset T_i$ with $(R : T_i) \neq M^2$ (for $i = 1, 2$) while T_1 and T_2 are not R-algebra isomorphic. This work contributes to the characterization of the commutative rings with exactly two proper (unital) subrings.

1 Introduction

All rings and algebras considered below are commutative with identity; all inclusions of rings, ring homomorphisms and algebra homomorphism are unital. If $A \subseteq B$ are rings, then $[A, B]$ denotes the set of "intermediate rings," that is, the set of rings C such that $A \subseteq C \subseteq B$. Recall from [1] that a ring extension $A \subseteq B$ is said to satisfy FIP (or the "finitely many intermediate rings property") if $[A, B]$ is finite. A satisfactory ring-theoretic characterization of FIP was given by the authors in [7]. Central to a study of FIP is the view that any proper ring extension $A \subset B$ which satisfies FIP can be "factored" into a finite chain $A = A_0 \subset \ldots A_i \subset A_{i+1} \subset \ldots \subset A_n = B$ of rings such that $A_i \subset A_{i+1}$ is a minimal ring extension, in the sense of [12], for all $i = 0, \ldots, n-1$. (Background on minimal ring extensions and their "crucial maximal ideals" is given later in this Introduction.) The converse is, however, far from true. Indeed, for minimal ring extensions $R \subset S$ and $S \subset T$, Jay Shapiro and the first-named author gave, in [11, Theorem 4.1], 13 mutually exclusive conditions, dubbed (i)-(xiii), on these minimal ring extensions and their crucial maximal ideals to characterize when $R \subset T$ satisfies FIP. In an increasingly focused series of papers ([3], [4], [5]) that studied more deeply each of these 13 conditions, the first-named author sought first to determine which of the 13 conditions described data such that $|[R, T]| = 3$ (i.e., to determine the data for which S is the only element of $[R, T] \setminus \{R, T\}$; and, secondly, by focusing on the case where R is a prime subring (that is, a ring isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 2$), to characterize the rings T with exactly two proper subrings. It was announced in [3, Theorem 2.9] that the first goal had been achieved. In fact, [3, Theorem 2.9] stated that if the data satisfy either (vi) or (xi), then $|[R, T]| = 3$; if the data satisfy any of (iii), (iv), (vii), (viii), (ix), (x) or (xii), then $|[R, T]| > 3$ (and $|[R, T]| < \infty$); but, for each of the four conditions (i), (ii), (v) and (xiii), there exist data satisfying this condition for which $|[R, T]| = 3$ and there exist other data satisfying this condition for which $|[R, T]| > 3$ (and $|[R, T]| < \infty$). On the basis of this result, it was explained, in [3] and more deeply later in [4], that the characterization of the rings with exactly two proper subrings could be deemed to have been finalized if one could characterize when data satisfying condition (xiii) also satisfies $|[R, T]| = 3$ in case R is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$. Condition (xiii) states that both $R \subset S$ and $S \subset T$ are ramified, their respective crucial maximal ideals M and N satisfy $N \cap R = M$, and the two conditions stated in [11, Proposition 3.5 (b)] hold. In July 2016, the first-named author submitted a manuscript [5] that determined exactly when data satisfying condition (xiii),

with R a prime subring, also satisfy $|[R,T]| = 3$. When a positive referee's report on [5] was received in August 2017, it seemed that the literature would soon record the characterization of the rings with exactly two proper subrings.

But there is an error in the literature and it has nothing to do with the "ramified, then ramified" context of condition (xiii) that is addressed in [5]. The same week that the referee reported on [5], the second- and third-named authors sent an email message [18] to the first-named author in which they gave a counter-example to [3, Theorem 2.8]. The existence of this counter-example showed that condition (ix) had been mishandled in the statement of [3, Theorem 2.9]. In conjunction with other material in [3], this counter-example shows that there exist data satisfying (xiii) for which $|[R,T]| = 3$ and there exist other data satisfying (xiii) for which $|[R,T]| > 3$ (and $|[R,T]| < \infty$). Condition (ix) states that the minimal ring extensions $R \subset S$ and $S \subset T$ are respectively ramified and decomposed (these terms will be explained below) and their respective crucial maximal ideals M and N satisfy $N \cap R = M$.

It was clear at once to all three parties that the following three actions had to be taken as soon as possible.

(1): A Corrigendum to [3] must be written and promptly submitted for publication; that document should contain the counterexample from [18] and, if possible, indications of any partial positive results in the spirit of [3, Theorem 2.9].

(2): An intensive study of the "ramified, then decomposed" context of condition (ix) should be undertaken to determine necessary and sufficient conditions for such data to satisfy $|[R,T]| = 3$, at least for the cases needed to supplement [5] and thereby complete the characterization of the rings with exactly two proper subrings; ideally, such a study should include base rings R that are special principal ideal rings (SPIRs), to accommodate rings of the form $\mathbb{Z}/n\mathbb{Z}$, and base rings R that are principal ideal domains but not fields, to accommodate $\mathbb{Z}$.

(3): The revision of [5] that is underway in concordance with the referee's report should clarify the necessary adjustments to background (such as the statement of [3, Theorem 2.8]) and add to the characterizations in [5] concerning condition (xiii) any additional items concerning condition (ix) that are necessitated by the study proposed in (2).

Action (1) has already been taken. Action (3) will be taken as soon as the present manuscript has been submitted; it is anticipated that the impact of adding a study of condition (ix) to the originally submitted form of [5] will be the addition of at most half a dozen lines of text. As for Action (2), the present manuscript presents that proposed study and accomplishes all the *desiderata* noted above. We next summarize its contents.

Theorem 2.2 (resp., Theorem 2.8) shows, in case (R,M) is an SPIR (resp., in case R is a Dedekind domain, but not a field, with M a maximal ideal of R), that $(R:T) = M^2$ is a necessary and sufficient condition for $|[R,T]| = 3$, provided that the data satisfy condition (ix); that is, provided that the minimal ring extensions $R \subset S$ and $S \subset T$ are respectively ramified and decomposed and their respective crucial maximal ideals M and N satisfy $N \cap R = M$. The conclusion of Theorem 2.8 does not apply in case the base ring R is a field. That observation has already been made in the valid part of the published "proof" of [3, Theorem 2.8], and it is generalized in Proposition 2.1 to the situation where the base ring R is a von Neumann regular ring. For that reason, we often point out where our proofs use the assumption that $M \neq 0$. It should be noted that the proofs of Theorems 2.2 and 2.8 owe much to the valid part of the published "proof" of [3, Theorem 2.8]. It is not a coincidence that the final two paragraphs of the proof of Theorem 2.2 follow the lines of how the Corrigendum to [3] has presented a proof of the counter-example that was sent in [18]. We also wish to point out that the reduction to the case of a quasi-local base ring in Theorem 2.8 (without changing the context of condition (ix) or affecting $|[R,T]|$) is due to [11, Proposition 3.1]. We provide a number of examples (satisfying condition (ix)) to illustrate Theorems 2.2 and 2.8. Some of these examples satisfy $|[R,T]| = 3$, while other examples satisfy $|[R,T]| > 3$ (but $|[R,T]| < \infty$). Theorem 2.6 is noteworthy, as it establishes that for two specific classes of SPIRs R, the condition $(R:T) = M^2$ determines S and T up to R-algebra isomorphism. Corollary 2.15 gives the analogous result in case the base ring R is the Dedekind domain $\mathbb{Z}$. Finally, by combining the work in [5] with the relevant impact of Theorem 2.2, Theorem 2.8 and Corollary 2.15, a characterization of the rings with exactly two proper subrings (including a classification of these rings up to isomorphism in the case of characteristic 0) is presented in Corollaries 2.17 and 2.18.

Recall that a ring extension $A \subset B$ is 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 [12, 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 $\mathrm{Spec}(A)$ (resp., $\mathrm{Max}(A)$) denotes the set of prime (resp., maximal) ideals of A. If $A \subseteq B$ are rings, then $^{+}_{B}A$ denotes the seminormalization of A in B, in the sense of [19]. 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; and $|U|$ denotes the cardinal number of a set U. The symbols X, Y and W denote indeterminates over the ambient ring(s). If I is a ideal of a ring A, then $\mathrm{nil}_A(I)$ denotes the radical of I (as an ideal of A), in the sense of [15, page 17]. All the required background on idealizations can be found in [14]. We assume that the reader has a copy of [3] (and possibly also copies of [7] and [11]) at hand. Any unexplained material is either taken from the Introduction of [11] or is standard, as in [13], [15].

2 Results

Although the statement of [3, Theorem 2.8] is incorrect, the initial four paragraphs of its published "proof" are valid, and the reductions and conclusions in those paragraphs will be of use in several of the proofs given below. That reasoning also leads, in Proposition 2.1, to a case in which the conclusion of [3, Theorem 2.8] is correct. Another reason for the inclusion of Proposition 2.1 here is that it serves to explain why the ambient ring R is assumed to not be a field in Theorems 2.2 and 2.8. For an example satisfying the hypotheses of Proposition 2.1 in which the crucial maximal ideals satisfy $N \cap R = M$ and the base ring R is an arbitrary finite field (so that $(R : T) = 0 = M^2$), see [11, Remark 3.4 (f)].

Proposition 2.1. Let R be a von Neumann regular ring (for instance, a field). Let $R \subset S$ be a ramified ring extension and $S \subset T$ a decomposed ring extension. Then S is not the only ring properly contained between R and T; that is, $|[R, T]| > 3$.

Proof. Let M (resp., N) denote the crucial maximal ideal of $R \subset S$ (resp., of $S \subset T$). If $N \cap R \neq M$, the assertion follows from [11, Proposition 3.1 (d)]. Hence, without loss of generality, $N \cap R = M$. We can now repeat the first sentence of the "proof" of [3, Theorem 2.8]: by [11, Proposition 3.1 (a), (c), (d)], we can assume, without loss of generality, that R is quasi-local, with unique maximal ideal M. Recall that a ring A is a von Neumann regular ring if and only if A_P is a field for each $P \in \mathrm{Max}(A)$. Thus, we may assume that R is a quasi-local von Neumann regular ring, that is, a field. For this context, the assertion was established in the fourth paragraph of the "proof" of [3, Theorem 2.8]. □

Theorem 2.2 gives a necessary and sufficient condition for the conclusion of [3, Theorem 2.8] to be correct in case the base ring R is a special principal ideal ring (SPIR). For background on SPIRs, see [20, page 245]. We wish to stress that in this manuscript, our convention is that no field is considered to be an SPIR.

Theorem 2.2. Let R be an SPIR and let M denote the unique maximal ideal (indeed, the unique prime ideal) of R. Let $R \subset S$ be a ramified ring extension and let N denote the unique maximal ideal (indeed, the unique prime ideal) of S. Let $S \subset T$ be a decomposed ring extension (necesarily with crucial maximal ideal N). Then $N \cap R = M$ and the conductor $(R : T)$ is either M or M^2. Moreover, S is the only ring properly contained between R and T (that is, $|[R, T]| = 3$) if and only if $(R : T) = M^2$.

Proof. Since R is an SPIR, $\mathrm{Spec}(R)$ is a singleton set. As $R \subset S$ is ramified, necessarily with crucial maximal ideal M, it follows that only one prime ideal of S can lie over M. Indeed,

since S is integral over R, the lying-over Theorem (cf. [13, Theorem 11.5], [15, Theorem 44]) provides at least one such prime ideal of S; its uniqueness is guaranteed by facts about ramified extensions, as in [7, Theorem 2.2] (when coupled with the incomparability property of integral extensions, as in [13, Corollary 11.2], [15, Theorem 44]). In fact, it is now clear that $\mathrm{Spec}(S)$ must be the singleton set $\{N\}$ and $N \cap R = M$. Now that the parenthetical assertions have been justified, we turn to the (more difficult) "Moreover" conclusion.

Consider the conductor $C := (R : T)$. Of course, $C \subseteq (R : S)$. But since M is the crucial maximal ideal of the integral minimal ring extension $R \subset S$, it follows from [12, Théorème 2.2 (ii)] that $(R : S) = M$. Consequently, $C \subseteq M$. Also, by the (valid) first two paragraphs of the "proof" of [3, Theorem 2.8], $|[R/C, T/C]| = |[R, T]|$, $R/C \subset S/C$ is ramified with crucial maximal ideal M/C, and $S/C \subset T/C$ is decomposed with crucial maximal ideal N/C. In addition, by the (valid) third paragraph of the "proof" of [3, Theorem 2.8], $M^2 \subseteq C$.

Suppose first that $C = M$. As R/C is then a field, it follows from Proposition 2.1 (when applied to the chain $R/C \subset S/C \subset T/C$) that $|[R/C, T/C]| > 3$. Thus, by the above comments, $|[R, T]| > 3$. Therefore, to prove the "Moreover" conclusion in case $C = M$, it suffices to show that $M^2 \neq M$. But this, in turn, is a standard fact about any SPIR with (nonzero) maximal ideal M [20, page 245]. (For an alternate proof that $M \neq M^2$, apply the Krull Intersection Theorem [15, Theorem 79], bearing in mind that any SPIR is a Noetherian ring by virtue of Cohen's Theorem [15, Theorem 8]). As we have seen that $M^2 \subseteq C \subseteq M$ and every proper ideal of (the SPIR) R must be a power of M, it follows (cf. [20, page 245]) that C is either M or M^2. It also follows that in proving the asserted equivalence, we may assume henceforth that $C \subset M$; that is, that $C = M^2$.

Now, since $C \neq M$, the ring R/C is an SPIR (with nonzero maximal ideal M/C). Hence (cf. the above comments), it follows as in the first two paragraphs of the "proof" of [3, Theorem 2.8] that we can, without loss of generality, replace the chain $R \subset S \subset T$ with $R/C \subset S/C \subset T/C$, so that we can also assume that R, S and T are Artinian rings such that $C = 0$. As the original data satisfy $M^2 \subseteq C$, we are now assuming, *inter alia*, that $M^2 = C = 0$. Therefore, to complete the proof, it suffices to show that $|[R, T]| = 3$.

Since R/C ($\cong R$) is an Artinian ring and T is a finitely generated R-module, it follows from [7, Theorem 4.2 (a)] that $R \subset T$ satisfies the FCP property; that is, each chain in (the poset) $[R, T]$ is finite. In addition, it follows from basic facts about ramified extensions and decomposed extensions (as in [7, Theorem 2.2]) that the extension $R \subset T$ is infra-integral (that is, for each $P \in \mathrm{Spec}(T) = \mathrm{Max}(T)$, the canonical map $R/(P \cap R) \to T/P$ is an isomorphism of fields). Furthermore, the above-cited basic facts about ramified extensions give $MN \subseteq N^2 \subseteq M$ and $\dim_{R/M}(S/M) = 2$. Hence, since $0 \subset N/M \subset S/M$, the length of N/M as an R-module is $\mathrm{L}_R(N/M) = \dim_{R/M}(N/M) = 1$. Therefore, it follows from [7, Lemma 5.4] that each maximal chain in $[R, T]$ has length

$$\mathrm{L}_R(N/M) + \mathrm{Max}(T) - 1 = 1 + 2 - 1 = 2.$$

It suffices to get a contradiction from the supposed existence of some $S' \in [R, T] \setminus \{R, S, T\}$. By the above conclusion about length, $R \subset S'$ must be a (necessarily integral) minimal ring extension. We claim that $R \subset S'$ is not an inert extension. If this claim fails, M is a common maximal ideal of distinct members (namely R and S') of $[R, T]$, which is a contradiction to [7, Lemma 5.2] (which applies since $R \subset T$ is an integral infra-integral extension). This proves the claim. Since $R \subset S'$ is not inert, it must be either ramified or decomposed. Suppose, for the moment, that $R \subset S'$ is ramified. Then $R \subset S'$ is subintegral and so, by [7, Proposition 4.5 (b)], $S' \subseteq {}^{+}_{R}T$. Note that this seminormalization (of R in T) contains S (also by [7, Proposition 4.5 (b)]) but cannot be T. (Indeed, $R \subset T$ is not subintegral because the "decomposed" hypothesis ensures that two distinct prime ideals of T meet S in N and, hence, meet R in M.) Therefore, since $S \subset T$ is a minimal ring extension, ${}^{+}_{R}T = S$, and so $S' \subseteq S$. Since $R \subset S$ is a minimal extension, S' must be either R or S, a contradiction to the choice of S'. Therefore, $R \subset S'$ is not ramified. Hence, $R \subset S'$ is decomposed.

Since $R \subset S'$ is decomposed (necessarily with crucial maximal ideal M), it follows that $\mathrm{Spec}(S') = \mathrm{Max}(S') = \{N_1, N_2\}$ with $N_1 \neq N_2$ and $M = N_1 \cap N_2 = N_1 N_2$. Without loss of generality, we can take N_1 to be the crucial maximal ideal of $S' \subset T$. Then $N_1 = (S' : T)$ by [12, Théorème 2.2 (ii)]. Thus N_1 is an ideal of T, and so $N_1 T = N_1$. Hence $M = N_1 N_2 = (N_1 T) N_2 = N_1 (T N_2)$, which is a product of ideals of T. Thus M is an ideal of T, and so

$MT = M \subseteq R$. Hence $M \subseteq (R : T) = C = 0$, and so $M = 0$, the desired contradiction. □

The necessary and sufficient condition in Theorem 2.2 is not automatically satisfied. Indeed, Example 2.3 presents data, with R an arbitrary SPIR, satisfying the hypotheses of Theorem 2.2 and $|[R, T]| > 3$.

Example 2.3. Let (R, M) be an SPIR. Then there exist a ramified extension $R \subset S$ (necessarily with crucial maximal ideal M) and a decomposed extension $S \subset T$ with crucial maximal ideal N such that $N \cap R = M$ and $|[R, T]| > 3$. One way to construct such data is the following. Take $S := R(+)R/M$ and denote its unique maximal ideal by N $(= M(+)R/M$, noting also that the canonical map $R/M \to S/N$ is an isomorphism which will be viewed henceforth as an identification); then take $T := S \times S/N$ $(= S \times R/M$, where S is viewed as a subring of T via the injective R-algebra homomorphism $R \to T$ that is given by the universal mapping property of the direct product T in conjunction with the identity map $S \to S$ and the canonical projection map $S \to S/N)$.

Proof. By [2, Corollary 2.5], $R \subset S$ is a minimal ring extension (where R is viewed as a subring of S via the injective R-algebra homomorphism given by $r \mapsto (r, r + M)$ for all $r \in R$). As R is quasi-local, the crucial maximal ideal of $R \subset S$ must be M. Moreover, by the proof of [10, Corollary 2.5] (cf. also [17, Lemma 2.1]), $R \subset S$ is ramified. A standard fact about idealizations shows that N is the unique prime ideal of S. It is evident that $N \cap R = M$. Hence, the canonical map $R/M \to S/N$ is indeed an isomorphism (cf. [7, Theorem 2.2]), a conclusion that can also be easily verified directly. It also follows from the proof of [10, Corollary 2.5] that $S \subset T$ is a decomposed (minimal ring) extension; its crucial maximal ideal must be N since S is quasi-local.

By Theorem 2.2, it suffices to show that $(R : T) \neq M^2$. Recall that the third paragraph of the proof of Theorem 2.2 recorded two proofs that $M \neq M^2$; that is, $M^2 \subset M$. Therefore it suffices to show that $M \subseteq (R : T)$; that is, that if $p \in M$ and $\tau \in T$, then $p\tau \in R$. To that end, observe that p has been identified with $(p, 0 + M) \in S$ and, hence, with the element

$$((p, 0 + M), (p, 0 + M) + N) = ((p, 0 + M), 0 + N) \in S \times S/N$$

and thus with the element $((p, 0 + M), 0 + M) \in S \times R/M = T$. On the other hand,

$$\tau = ((r_1, r_2 + M), r_3 + M) \in S \times R/M = T,$$

for some elements $r_1, r_2, r_3 \in R$. So, working with the multiplication in the direct product T, with "$*$" denoting the multiplication in the idealization S, we see that $p\tau$ is viewed (in T) as the element

$$((p, 0 + M) * (r_1, r_2 + M), (0 + M)(r_3 + M)) =$$

$$((pr_1, pr_2 + 0r_1 + M), 0r_3 + M) = ((pr_1, 0 + M), 0 + M) \in T.$$

(The last step in the last display used the fact that $pr_2 \in MR = M$.) This means that $p\tau = pr_1 \in M \subseteq R$, which completes the proof. □

One may ask if there was any flexibility in the construction of the R-algebra T in Example 2.3. We next answer that question in the affirmative, at least in case the base ring R is taken from a certain class of SPIRs.

Example 2.4. Let p be a prime number and X an indeterminate over $\mathbb{F}_p$. Put $R := \mathbb{F}_p[X]/(X^2)$ and $x := X + (X^2) \in R$. (It is well known that R is an SPIR with unique maximal ideal $M := \mathbb{F}_p x$ satisfying $M \neq 0 = M^2$ and $R = \mathbb{F}_p(+)M \cong \mathbb{F}_p(+)\mathbb{F}_p$.) As in Example 2.3, take $S := R(+)R/M$, denote its unique maximal ideal by N $(= M(+)R/M)$, and recall that a canonical identification permits us to view $R/M = S/N$. Let T_1 denote the ring T from Example 2.3; that is, $T_1 := S \times S/N$ $(= S \times R/M)$, where S is viewed as a subring of T_1 as in Example 2.3. (Recall from Example 2.3 that $R \subset S$ is a ramified extension with crucial maximal ideal M, $S \subset T_1$ is a decomposed extension with crucial maximal ideal N, $N \cap R = M$, and $|[R, T_1]| > 3$.) Let S^* be the ring that was denoted by R_1 in [4, Proposition 2.11]. (Recall from [4, Proposition 2.11] that S^* can be constructed as the R-algebra whose additive structure as a

vector space over $\mathbb{F}_p$ is given by $R \oplus \mathbb{F}_p z$ for some nonzero element z and whose multiplication is determined by the relations $xz = 0$ and $z^2 = x$ (and $x^2 = 0$); the unique maximal ideal of S^* is $Q := M \oplus \mathbb{F}_p z = \mathbb{F}_p x \oplus \mathbb{F}_p z$; $Q \cap R = M$; $R \subset S^*$ is a ramified extension with crucial maximal ideal M; and S^* is not isomorphic to S, as S^* has only two proper subrings.) Put $T_2 := S^* \times S^*/Q$, which we identify with $S^* \times \mathbb{F}_p$. (Note that $S^*/Q \cong R/M \cong \mathbb{F}_p$.) We view $S^* \subseteq T_2$ via the injective S^*-algebra map given by the universal mapping property of the direct product T_2, in conjunction with the identity map $S^* \to S^*$ and the canonical projection map $S^* \to S^*/Q$. Then:

(a) $S^* \subset T_2$ is a decomposed extension whose crucial maximal ideal lies over M, and $|[R, T_2]| > 3$.

(b) T_1 and T_2 are not isomorphic as R-algebras.

Proof. (a) Note that $y := (0, 1) \in T_2 \setminus S^*$. It is straightforward to use the criteria in [7, Theorem 2.3] to verify that $S^* \subset T_2$ is a decomposed extension, necessarily with crucial maximal ideal Q. (In detail, $T_2 = S^*[y]$ (since the S^*-module structure of T_2 is given by $S^* \oplus \mathbb{F}_p = S^* \oplus \mathbb{F}_p y$), $y^2 - y = 0 \in Q$, and $yQ = \{0\} \subseteq S^*$. For an alternative explanation, using the criterion in [7, Theorem 2.2], note that Q is viewed in T_2 as $Q \times \{0\}$, so that $T_2/Q \cong S^*/Q \times S^*/Q$.) It remains only to show that $|[R, T_2]| > 3$ or (equivalently, by Theorem 2.2) that $(R : T_2) \neq M^2$ $(= 0)$. That, in turn, can be done by producing the ring $R \times \mathbb{F}_p \in [R, T_2] \setminus \{R, S^*, T_2\}$. (Verifying that $R \times \mathbb{F}_p \neq S^*$ is somewhat tedious. Indeed, to obtain a contradiction from $z = (r, \alpha)$ with $r \in R$ and $\alpha \in \mathbb{F}_p$, use $xz = 0$ to get $r \in (0 :_R x) = M$ and then use $z^2 = x$ to get $x = r^2 \in M^2 = 0$, a contradiction. The following alternate argument, using the criterion in Theorem 2.2, seems faster. We have that $(0 \neq)\ x \in (R : T_2)$, since $xT_2 = xS^* + x\mathbb{F}_p y$, with $xS^* \subseteq MS^* = M \subseteq R$ and $xy = 0 \in R$.)

(b) It suffices to infer a contradiction from the assumption that there exists an R-algebra isomorphism $g : T_1 \to T_2$. Recall that if $A \subseteq B$ are rings, then ${}^+_B A$, the seminormalization of A in B, is the largest element of $[A, B]$ which is subintegral over A (cf. [7, Proposition 4.5 (b)]). It follows from standard homomorphism theorems that the isomorphism g carries ${}^+_{T_1} R$ onto ${}^+_{T_2} R$. Thus ${}^+_{T_1} R \cong {}^+_{T_2} R$ as R-algebras. Note that $R \subseteq S$ is subintegral, $S \subset T_1$ is a minimal ring extension, and $R \subseteq T$ is not subintegral; the last of these assertions holds since the "decomposed" condition ensures that T_1 has two distinct prime ideals that lie over N (and hence lie over M). It follows that ${}^+_{T_1} R = S$. In view of (a), we can prove similarly that ${}^+_{T_2} R = S^*$. Therefore, $S \cong S^*$ as R-algebras. But this contradicts what was shown in [4, Proposition 2.11]. □

As counterpoint to Examples 2.3 and 2.4, we next present an example of data, with (R, M) an arbitrary SPIR, satisfying the hypotheses of Theorem 2.2 and $|[R, T]| = 3$.

Example 2.5. Let (R, M) be an SPIR. Then there exist a ramified extension $R \subset S$ (necessarily with crucial maximal ideal M) and a decomposed extension $S \subset T$ with crucial maximal ideal N such that $N \cap R = M$ and $|[R, T]| = 3$. One way to construct such data is the following. Fix $p \in M$ so that $Rp = M$. With Y an indeterminate over R, put $T := R[Y]/(Y^2 - Y, p^2 Y)$ and $y := Y + (Y^2 - Y, p^2 Y) \in T$. Also put $x := py \in T$ and $S := R[x]$, with N denoting the unique prime ideal of S.

Proof. If $r \in R \cap (Y^2 - Y, p^2 Y)R[Y]$, we see, by expressing r as an $R[Y]$-linear combination of $Y^2 - Y$ and $p^2 Y$ and then equating constant terms, that $r = 0$. Consequently, the R-algebra homomorphism $f : R \to T$ is an injection. We view $R \subseteq T$ via f.

We claim that $x \notin R$. Suppose, on the contrary, that the claim fails. Then $py - a = 0$ for some $a \in R$, so that

$$pY - a = (Y^2 - Y)g(Y) + p^2 Y h(Y)$$

for some $g, h \in R[Y]$. Applying the R-algebra homomorphism $R[Y] \to R[Y]$ determined by $Y \mapsto 0$ leads to $a = 0$, and so

$$pY = (Y^2 - Y)g(Y) + p^2 Y h(Y).$$

Hence $p = (Y - 1)g(Y) + p^2 h(Y)$. Then $Y \mapsto 1$ gives $p = p^2 h(1)$, a contradiction, since, as we recalled in the proof of Theorem 2.2, $M \not\subseteq M^2$ in an SPIR, (R, M). This proves the claim that $x \notin R$.

As $x \notin R$, it follows that $R \subset S$. As $px = p^2y = 0$, we have $M = Rp \subseteq (0 :_R x)$. However, $1 \notin (0 :_R x)$ since $x \neq 0$. Since $M \in \mathrm{Max}(R)$, it follows that $(0 :_R x) = M$. Thus, $Rx \cong R/(0 :_R x) = R/M$ as R-modules. Next, we claim that $R \cap Rx = 0$. To prove this, it suffices to show that if $b \in R \cap Rx$, then $b = 0$. By hypothesis, $b = cx$ for some $c \in R$. Note that c cannot be a unit of R (lest $x = c^{-1}b \in R$, a contradiction). Thus $c \in M$, and so $c = dp$ for some $d \in R$. Then $b = cx = dpx = dp^2y = d \cdot 0 = 0$, thus proving the claim.

Observe that $x^2 = p^2y^2 = (p^2y)y = 0 \cdot y = 0$. Thus, $S \cong R(+)Rx \cong R(+)R/M$ as R-algebras. As recalled in the proof of Example 2.3, it follows from [2], [10] and [17] that $R \subset R(+)R/M$ is a ramified extension with crucial maximal ideal M. Therefore, the same is true of $R \subset S$. As a standard fact about idealizations shows that $R(+)R/M$ has a unique prime ideal, the same is true of S. Its prime ideal, say N, clearly satisfies $N \cap R = M$.

It is clear that $S \subseteq T$. We claim that this inclusion is proper. If the claim fails, then $y \in S$, so that $y = \lambda + \mu x = \lambda + \mu py$ for some $\lambda, \mu \in R$. Then there exist $g^*, h^* \in R[Y]$ such that $(1 - \mu p)Y - \lambda = (Y^2 - Y)g^*(Y) + p^2Yh^*(Y)$. Then $Y \mapsto 0$ leads to $\lambda = 0$, and so $(1 - \mu p)Y = (Y^2 - Y)g^*(Y) + p^2Yh^*(Y)$. It follows that $1 - \mu p = (Y - 1)g^*(Y) + p^2h^*(Y)$. Then $Y \mapsto 1$ leads to $1 - \mu p = p^2h^*(1)$, whence $1 = \mu p + p^2h^*(1) \in Rp = M$, a contradiction. This proves the claim that $S \subset T$.

In fact, we claim that $S \subset T$ is a decomposed extension (necessarily with crucial maximal ideal N, since N is the only prime ideal of S). We will next use the criteria in [7, Theorem 2.3 (b)] to prove this claim. We have $S \subset T = S[y]$, with $y^2 - y = 0 \in N$. Therefore, to establish the claim, it suffices to prove that $yN \subseteq N$. The above isomorphism $R(+)R/M \to R(+)Rx = R+Rx = S$ must carry the maximal ideal $M(+)R/M$ onto N, and so $N = M+Rx = Rp+Rx$. We have $yp = py = x \in N$ and $yx = py^2 = py = x$, and so $yN \subseteq N$, thus proving the claim that $S \subset T$ is decomposed.

By Theorem 2.2, it will be enough to prove that $(R : T) = M^2$. By the valid part of the proof of [3, Theorem 2.8], $M^2 \subseteq (R : T)$ (it is also easy to check this directly for the present data); and it is clear that $(R : T) \subseteq M$ since $R \subset T$. So, by the standard background about SPIRs that we are assuming (see [20, page 245]), it suffices to prove that $(R : T) \neq M$. This, in turn, follows since $py = x \notin R$. The proof is complete. □

One may ask, in the spirit of Example 2.4, if there was any flexibility in the construction of the R-algebra T in Example 2.5. We next answer that question in the negative in case R is taken from two specific classes of SPIRs. One consequence of Theorem 2.6 is that if (R, M) is an SPIR with $M^2 = 0$, the counter-example to [3, Theorem 2.8] which is given in the Corrigendum to [3] (and is due to the second- and third-named authors) is uniquely determined up to R-algebra isomorphism. In the proofs of Theorem 2.6 and Corollary 2.20 (b), it will be convenient to use the following notation. If I is a ideal of a ring A, then $\mathrm{nil}_A(I)$ denotes the radical of I (as an ideal of A), in the sense of [15, page 17].

Theorem 2.6. Let (R, M) be an SPIR. For $i = 1, 2$, let $R \subset S_i$ be a ramified extension (necessarily with crucial maximal ideal M), let N_i denote the unique prime ideal of S_i (necessarily such that $N_i \cap R = M$), and let $S_i \subset T_i$ be a decomposed extension (necessarily with crucial maximal ideal N_i) such that $|[R, T_i]| = 3$. Assume also that (at least) one of the following two conditions holds: (1) $M^2 = 0$; (2) $R/M \cong \mathbb{F}_2$. Then $T_1 \cong T_2$ and $S_1 \cong S_2$ as R-algebras.

Proof. By Theorem 2.2, $(R : T_1) = M^2 = (R : T_2)$. Therefore M^2 is an ideal of both T_1 and T_2. Fix $p \in R$ such that $M = Rp$. Fix $i \in \{1, 2\}$. By the hypothesis on $R \subset S$, $M \subset N_i$, and with a fixed $x_i \in N_i \setminus M$, we have $S_i = R[x_i]$, $x_i^2 \in M$, $x_iM \subseteq M$, $N_i = M + Rx_i$ and $N_i^2 \subseteq M$ (cf. [7, Theorems 2.2 and 2.3] and the proof of [10, Proposition 2.12]). It also follows that $S_i = R + Rx_i$. Note that $px_i \in N_i^2 \subseteq M = pR$.

Since $S_i \subset T_i$ is decomposed, another appeal to [7] and [10] gives (exactly two) distinct prime ideals Q_1, Q_2 of T_i that lie over N_i and, with a fixed $y_i \in Q_1 \setminus Q_2$, we have $Q_1Q_2 = Q_1 \cap Q_2 = N_i$, $y_i^2 - y_i \in N_i$, $y_iN_i \subseteq N_i$, and $T_i = S_i[y_i]$. Also, $x_iy_i \in N_iQ_1 \subseteq N_i = M + Rx_i$, and so

$$T_i = S_i + S_iy_i = R + Rx_i + Ry_i + Rx_iy_i = R + Rx_i + Ry_i.$$

We claim that $py_i \in N_i \setminus R$ $(= N_i \setminus M)$. It is clear that $py_i \in N_iQ_1 \subseteq N_i$. So, if the claim were to fail, then $py_i \in M$, so that

$$pT_i = p(R + Rx_i + Ry_i) \subseteq pR + Rpx_i + Rpy_i \subseteq M + M + M \subseteq R,$$

and it would follow that $p \in (R : T_i) = M^2$, a contradiction (cf. [20, page 245]). This proves the claim $py_i \in N_i \setminus R$.

We claim that y_i can be (re)chosen so that $p^2y_i = 0$. In any event, we have that $p^2y_i = p(py_i) \in MN_i \subseteq N_i^2 \subseteq M$. Let α be the index of nilpotency of M. Thus $\alpha \geq 2$, $M^\alpha = 0$ and $M^{\alpha-1} \neq 0$. It will be useful to note that if the claim is granted, then it remains the case that $x_iy_i \in N_i$, as we saw earlier. Without loss of generality, $p^2y_i \neq 0$. Then $p^2y_i = p^ku$ for some integer k such that $1 \leq k < \alpha$ and some unit u of R. If $k = 1$, then $p(py_i - u) = 0$; thus, as u is a unit of S_i and py_i is nilpotent, it follows that $u - py_i$ is a unit of S_i, and so $p = (u - py_i)^{-1}(u - py_i)p = (u - py_i)^{-1} \cdot 0 = 0$, a contradiction. Hence $k > 1$. The analysis of the case $k = 2$ will require two further paragraphs (that is where the assumptions (1), (2) will become relevant), and so we will spend the rest of this paragraph dispatching the claim in case $k \geq 3$. Consider $z_i := y_i - p^{k-2}u$. As $z_i - y_i \in M \subseteq N_i = Q_1 \cap Q_2$ and $y_i \in Q_1 \setminus Q_2$, we have $z_i \in Q_1 \setminus Q_2$, $T_i = S_i[z_i]$ and $z_iN_i \subseteq N_i$. In addition,

$$z_i^2 - z_i = (y_i^2 - y_i) + p^{2k-4}u^2 - 2y_ip^{k-2}u + p^{k-2}u.$$

We have $y_i^2 - y_i \in N_i$, $p^{2k-4}u^2 \in M \subseteq N_i$, $2y_ip^{k-2}u \in Q_1N_i \subseteq N_i$, and $p^{k-2}u \in M \subseteq N_i$. Consequently, $z_i^2 - z_i \in N_i$. Most importantly, $p^2z_i = p^2(y_i - p^{k-2}u) = p^2y_i - p^ku = 0$. Thus, we may revisit the earlier choice of y_i and harmlessly replace y_i with z_i. In particular, except in case $k = 2$, we henceforth have $p^2y_i = 0$ (and $x_iy_i \in N_i$), thus proving the above claim if $k \neq 2$.

For $k = 2$, the above claim is evident if assumption (1) holds. Indeed, if (1) holds, then $p^2y_i = 0 \cdot y_i = 0$ and there is no need to change y_i. As above, note that the condition $x_iy_i \in N_i$ remains in force.

In this paragraph, $k = 2$ and we assume (2); that is, $p^2y_i = p^2u$ for some unit u of R and $R/M \cong \mathbb{F}_2$. Without loss of generality, $p^2 \neq 0$. Note that $p^2(y_i - u) = 0$. Thus $y_i - u$ is not a unit of T_i. Hence $y_i - u \in Q_1 \cup Q_2$. But $y_i - u \notin Q_1$ (since $y_i \in Q_1$ and u is a unit), and so $y_i - u \in Q_2 \setminus Q_1$. It now follows from the minimality of $S_i \subset T_i$ that $S_i[y_i - u] = T_i$. Also, $(y_i - u)N_i \subseteq N_i$ since $N_i = (S_i : T_i)$ is an ideal of T_i. Thus, the claim will be proven for the present context (at the harmless cost of interchanging Q_1 and Q_2) if we show that $(y_i - u)^2 - (y_i - u) \in N_i$. Recall that $y_i^2 - y_i \in N_i$. Also, since (2) holds, we have that $2 \in M \subseteq N_i$ and $u + 1 \in M \subseteq N_i$. Therefore

$$(y_i - u)^2 - (y_i - u) = (y_i^2 - y_i) + (-uy_i)2 + u(u + 1) \in N_i + N_i + N_i = N_i,$$

thus proving the above claim for $k = 2$ if assumption (2) holds. As above, the condition $x_iy_i \in N_i$ remains in force. This completes the proof that y_i can be chosen so as to also satisfy $p^2y_i = 0$.

Since idempotents can be lifted modulo any nil ideal (cf. [16, Proposition 1, page 72]), there exists $e_i = e_i^2 \in T_i$ such that $y_i - e_i \in N_i$. We claim that $p^2e_i = 0$. To prove this, we may assume, without loss of generality, that $p^2 \neq 0$. Also, note that $e_i \in Q_1 \setminus Q_2$. (Recall that if assumption (2) applies, we interchanged Q_1 and Q_2 so that the new $y_i \in Q_1 \setminus Q_2$.) Next, consider the ideal $J := (0 :_{T_i} p^2)$ of T_i. As $y_i \in J$, we have $J \not\subseteq Q_2$. On the other hand, $1 \notin J$; that is, J is a proper ideal of T_i. Thus, J is contained in some prime ideal of T_i. Since Q_1 and Q_2 are the only prime ideals of T_i, it follows that $J \subseteq Q_1$ and, in fact, $\mathrm{nil}_{T_i}(J) = Q_1$. Therefore $e_i \in \mathrm{nil}_{T_i}(J)$. Hence there exists a positive integer n such that $e_i^n \in J$. Since $e_i^n = e_i$, it follows that $e_i \in J$. In other words, $p^2e_i = 0$, thus proving the above claim.

Recall that $e_i \in Q_1 \setminus Q_2$. It is also easy to see that $T_i = S_i[e_i] = S_i + S_ie_i$ and $e_iN_i \subseteq N_i$. Thus, it is harmless to replace y_i with e_i, and so we can assume henceforth that $y_i^2 = y_i$ (and the salient earlier properties of y_i, including $p^2y_i = 0$ and $x_iy_i \in N_i$, remain in place).

The above choices of y_i did not depend essentially on x_i. Moreover, with y_i in hand, notice that py_i has all the salient properties that we required of x_i earlier. In other words, $py_i \in N_i \setminus R$; $S = R[py_i]$ (since $R \subset S$ is a minimal ring extension); $(py_i)^2 = y_i(p^2y_i) = y_i \cdot 0 = 0$; and $py_iM = p^2y_iR = \{0\} \subseteq M$. Thus, we may revisit the earlier choice of x_i and harmlessly replace x_i with py_i; that is, $py_i = x_i$ henceforth. It follows that $x_i^2 = 0 = px_i$. In addition, $x_iy_i = py_i^2 = py_i = x_i$.

Considering M as an additive subgroup of R, choose a set $\mathfrak{S}$ of coset representatives of M in R with the property that $\{0, 1\} \subseteq \mathfrak{S}$. Recall that $S_i = R + Rx_i$. We claim that $S_i = R + \mathfrak{S}x_i$. To prove the claim, it suffices to show that if $r \in R$, then there exists $b \in \mathfrak{S}$ such that $rx_i = bx_i$. To that end, let b be the element of $\mathfrak{S}$ such that $m := r - b \in M$. We have $m = dp$ for some

$d \in R$. Then $rx_i = bx_i + mx_i = bx_i + dpx_i = bx_i$, with the last step holding since $px_i = 0$. This proves the above claim.

Next, we claim that an element of S_i can be expressed in the form $a + bx_i$, with $a \in R$ and $b \in \mathfrak{S}$, in only one way. Indeed, suppose that $a_1 + b_1x_i = a_2 + b_2x_i$ with $\{a_1, a_2\} \subseteq R$ and $\{b_1, b_2\} \subseteq \mathfrak{S}$. Then $(b_2 - b_1)x_i = a_1 - a_2 \in Rx_i \cap R \subseteq N_i \cap R = M$. Since $Mx_i = \{0\}$ and $x_i \notin M$, it follows that $b_2 - b_1 \in (M :_R x_i) = M$. As b_1 and b_2 are elements of $\mathfrak{S}$ which are congruent modulo M, we get $b_1 = b_2$. Then $a_1 = a_2$ follows easily, which proves the above claim.

Next, recall that $T_i = S_i + S_iy_i$. We claim that each element of T_i can be expressed in exactly one way as $z + cy_i$ where $z \in S_i$ and $c \in \mathfrak{S}$. To get "at least one way," take r, b, m and d as in the argument two paragraphs ago, and notice that

$$ry_i = my_i + by_i = dpy_i + by_i = dx_i + by_i \in S_i + \mathfrak{S}y_i.$$

To get "at most one way," it is straightforward to adapt the reasoning in the preceding paragraph, bearing in mind that $(S_i :_R y_i) = M$.

By the preceding three paragraphs, each element $\xi \in T_i$ can be uniquely expressed in the "canonical form" $a + bx_i + cy_i$ where $a \in R$ and $\{b, c\} \subseteq \mathfrak{S}$. Define a function $g : T_1 \to T_2$ as follows. If $\xi \in T_1$, express ξ in canonical form as $a + bx_1 + cy_1$; then let

$$g(\xi) = g(a + bx_1 + cy_1) := a + bx_2 + cy_2.$$

It is now clear that g is a bijection and that $g(r) = r$ for all $r \in R$. We will proceed to verify that g preserves addition, multiplication, and scalar multiplication (using scalars from R). These verifications will be somewhat tedious, with a flavor that is reminiscent of (but easier than) some arguments given in [5]. We will outline these verifications, leaving some intermediate steps to the reader.

Let $\xi_1, \xi_2 \in T_1$. For $j = 1, 2$, write ξ_j in canonical form as $a_j + b_jx_1 + c_jy_1$. Also write

$$b_1 + b_2 = kp + \beta_1, \;\; c_1 + c_2 = k^*p + \beta_2, \;\; \beta_1 + k^* = k_*p + \beta_3$$

where $k, k^*, k_* \in R$ and $\beta_1, \beta_2, \beta_3 \in \mathfrak{S}$. Using the facts that $px_2 = 0$ and $py_2 = x_2$, it is straightforward to verify that $g(\xi_1) + g(\xi_2) =$

$$a_1 + a_2 + (kp + \beta_1)x_2 + (k^*p + \beta_2)y_2 = a_1 + a_2 + \beta_3x_2 + \beta_2y_2.$$

On the other hand, $\xi_1 + \xi_2$ can be expressed in canonical form as $a_1 + a_2 + \beta_3x_1 + \beta_2y_1$, and so it is now clear that $g(\xi_1 + \xi_2) = g(\xi_1) + g(\xi_2)$.

Let $\xi_1, \xi_2 \in T_1$, written in canonical form as above. Also write

$$a_1b_2 + b_1a_2 + b_1c_2 + b_2c_1 = hp + \gamma_1, \;\; a_1c_2 + a_2c_1 + c_1c_2 = h^*p + \gamma_2, \;\; \text{and}$$

$\gamma_1 + h^* = h_*p + \gamma_3$, where $h, h^*, h_* \in R$ and $\gamma_1, \gamma_2, \gamma_3 \in \mathfrak{S}$. Using the facts that $x_2^2 = 0 = px_2$, $x_2y_2 = x_2$ and $y_2^2 = y_2$, it is straightforward to verify that $g(\xi_1)g(\xi_2) =$

$$a_1a_2 + (hp + \gamma_1)x_2 + (h^*p + \gamma_2)y_2 = a_1a_2 + \gamma_3x_2 + \gamma_2y_2.$$

On the other hand, $\xi_1\xi_2$ can be expressed in canonical form as $a_1a_2 + \gamma_3x_1 + \gamma_2y_1$, and so it is now clear that $g(\xi_1\xi_2) = g(\xi_1)g(\xi_2)$.

To show that g is an R-algebra isomorphism, it remains only to verify that $g(r\xi) = rg(\xi)$ for all $r \in R$ and $\xi \in T_1$. This, in turn, holds since g preserves multiplication and restricts to the identity map on R.

It remains only to prove that $S_1 \cong R(+)R/M \cong S_2$ as R-algebras. Fix $i \in \{1, 2\}$. It suffices to prove that S_i is R-algebra isomorphic to $R(+)R/M$. Take j to be the unique element of $\{1, 2\} \setminus \{i\}$. Replace T_j with the ring T that was constructed in Example 2.5. Recall from the fourth paragraph of the proof of Example 2.5 that the intermediate ring S_j (for this T) is R-algebra isomorphic to $R(+)R/M$. So, it will be enough to prove that the above R-algebra isomorphism (which is either g or g^{-1}) $h : T_i \to T_j$ carries S_i onto S_j. This, in turn, is a consequence of the injectivity of h. Indeed, since $[R, T_i] = \{R, S_i, T_i\}$ and $[R, T_j] = \{R, S_j, T_j\}$, with $h(R) = R$ and $h(T_i) = T_j$, it must be the case that $h(S_i) = S_j$. The proof is complete. □

Corollary 2.7. Let (R, M) be an SPIR such that either $M^2 = 0$ or $R/M \cong \mathbb{F}_2$. Fix $p \in M$ so that $Rp = M$. Then there exist a ramified extension $R \subset S$ (necessarily with crucial maximal ideal M) and a decomposed extension $S \subset T$ with crucial maximal ideal N such that $N \cap R = M$ and $|[R, T]| = 3$. For any such data, there exist R-algebra isomorphisms

$$T \cong R[Y]/(Y^2 - Y, p^2Y) \quad \text{and} \quad S \cong R(+)R/M,$$

where Y is an indeterminate over R.

Proof. In view of the statements of Theorem 2.6 and Example 2.5, one need only verify that the data in Example 2.5 satisfy $R[x] \cong R(+)R/M$ as R-algebras. For this isomorphism, see the beginning of the fourth paragraph of the proof of Example 2.5. □

We next give the analogue of Theorem 2.2 for the context in which the base ring R is an arbitrary principal ideal domain (PID), but not a field.

Theorem 2.8. Let R be a Dedekind domain (for instance, a PID), but not a field. Let $R \subset S$ be a ramified ring extension, and let M denote the crucial maximal ideal of $R \subset S$. Let $S \subset T$ be a decomposed ring extension. Suppose also that N, the crucial maximal ideal of $S \subset T$, satisfies $N \cap R = M$. Then S is the only ring properly contained between R and T (that is, $|[R, T]| = 3$) if and only if $(R : T) = M^2$.

Proof. Put $C := (R : T)$. Since T is algebra-finite over R, integrality ensures that T is a finitely generated R-module. It follows that $C_M = (R_M : T_M)$. As in the proof of Theorem 2.2, $C \subseteq M$. By the valid part of the "proof" of [3, Theorem 2.8],

$$(MR_M/C_M)^2 \subseteq (M^2R_M + C_M)/C_M = C_M/C_M = 0.$$

If $C_M = 0$, then $M^2R_M = (MR_M)^2 = 0$, a contradiction (because the fact that M is a nonzero ideal of the integral domain R ensures that $0 \subset M^2 \subseteq M^2R_M$). Hence $C_M \neq 0$.

We claim that if M^* is a maximal ideal of R which is distinct from M, then $C_{M^*} = R_{M^*}$. Since M^* is not the crucial maximal ideal of $R \subset S$, there is a unique prime (in fact, maximal) ideal N^* of S such that $N^* \cap R = M^*$ and $S_{M^*} = R_{M^*}$ canonically. Since N^* is not the crucial maximal ideal of $S \subset T$, there is a unique prime (in fact, maximal) ideal Q^* of T such that $Q^* \cap S = N^*$ and $T_{N^*} = S_{N^*}$ canonically. By [7, Lemma 2.4], $S_{M^*} = S_{N^*}$ and $T_{N^*} = T_{Q^*}$ canonically. However, it is also the case that Q^* is the unique prime ideal of T such that $Q^* \cap R = M^*$, and so [7, Lemma 2.4] gives the canonical equality $T_{M^*} = T_{Q^*}$. The upshot is that

$$T_{M^*} = T_{Q^*} = T_{N^*} = S_{N^*} = S_{M^*} = R_{M^*}$$

canonically. Thus, $C_{M^*} = (R : T)_{M^*} \cong (R_{M^*} : T_{M^*}) = (R_{M^*} : R_{M^*}) = R_{M^*}$. (The last equality holds since the "Dedekind" assumption ensures that R_{M^*} is a DVR, hence a Noetherian integrally closed integral domain, hence a completely integrally closed domain.) View this isomorphism as an identification. This proves the above claim.

If $C_M = R_M$, then by globalization, $C = R$, which is a contradiction since $R \subset T$. Thus $C_M \neq R_M$. Consequently, $C_M \subseteq MR_M$. The (valid) third paragraph of the "proof" of [3, Theorem 2.8]) can be tweaked to show that $M^2 \subseteq C$. (In detail, if v is any element of T, then, using the notation from [3], the argument given in [3] for the unit u can be adjusted so as to apply to v since $vN \subseteq N$.) Hence, $(MR_M)^2 = M^2R_M \subseteq C_M \ (\subseteq MR_M)$. Since R_M is a DVR, it follows that C_M is either MR_M or M^2R_M.

Suppose once again that M^* is a maximal ideal of R which is distinct from M. As $1 \in MR_{M^*}$, we have $(M^2)_{M^*} = R_{M^*}$. Thus, by the above claim,

$$(C/M^2)_{M^*} \cong C_{M^*}/((M^2)_{M^*}) = R_{M^*}/R_{M^*} = 0.$$

Therefore (regardless of whether R is quasi-local), it follows, via globalization and the above claim, that $C = M^2 \Leftrightarrow C/M^2 = 0 \Leftrightarrow$

$$(C/M^2)_M = 0 \Leftrightarrow C_M/(M^2R_M) = 0 \Leftrightarrow C_M \subseteq M^2R_M.$$

By the (valid) initial part of the "proof" of [3, Theorem 2.8],

$$|[R,T]| = |[R_M,T_M]| = |[R_M/C_M,T_M/C_M]| = |[R_M/C_M,(T/C)_M]|.$$

So, if $C_M = MR_M$ ($\neq M^2R_M$), then R_M/C_M is a field, and so it follows from Proposition 2.1 (ultimately, from the valid part of the proof of [3, Theorem 2.8]) that $|[R,T]| > 3$. Thus, to prove the asserted equivalence, we may suppose, without loss of generality, that $C_M \neq MR_M$. Then $C_M = M^2R_M$. Hence, R_M/C_M is an SPIR (with nonzero maximal ideal MR_M/C_M; moreover, by the above globalization argument, $C = M^2$). It now suffices to prove that $|[R_M/C_M,T_M/C_M]| = 3$.

Applying Theorem 2.2 to the SPIR R_M/C_M gives that

$$|[R_M/C_M,T_M/C_M]| = 3 \Leftrightarrow (R_M/C_M : T_M/C_M) = (MR_M/C_M)^2.$$

But $(R_M/C_M : T_M/C_M) = (R_M : T_M)/C_M = C_M/C_M = 0$, and so

$$|[R_M/C_M,T_M/C_M]| = 3 \Leftrightarrow (MR_M/C_M)^2 = 0 \Leftrightarrow M^2R_M \subseteq C_M.$$

We reduced above to a case where $C_M = M^2R_M$. Thus, by the last display, $|[R_M/C_M,T_M/C_M]| = 3$, and so the proof is complete. □

The next several results dig more deeply into the context where the base ring is a PID (but not a field). They are in the spirit of the SPIR-theoretic behavior studied in Examples 2.3 - 2.5. In particular, Example 2.9 presents a PID-theoretic analogue of Example 2.3, by showing that the necessary and sufficient condition in Theorem 2.8 is not automatically satisfied.

Example 2.9. Let R be a PID, but not a field, and let $M \in \mathrm{Max}(R)$. Then there exist a ramified ring extension $R \subset S$ with crucial maximal ideal M and a decomposed ring extension $S \subset T$ such that N, the crucial maximal ideal of $S \subset T$, satisfies $N \cap R = M$ and $|[R,T]| > 3$. One way to construct such data is the following. Take $S := R(+)R/M$ and denote the maximal ideal of S that lies over M by N ($= M(+)R/M$, noting also that the canonical map $R/M \to S/N$ is an isomorphism which will be viewed henceforth as an identification); then take $T := S \times S/N$ ($= S \times R/M$, where S is viewed as a subring of T via the injective R-algebra homomorphism $S \to T$ that is given by the universal mapping property of the direct product T in conjunction with the identity map $S \to S$ and the canonical projection map $S \to S/N$).

Proof. The construction is an analogue of that in Example 2.3. We can begin the proof by slightly modifying three sentences from the first paragraph of the proof of Example 2.3, as follows. (Unedited sentences from the first paragraph of the earlier proof should be inserted in this paragraph without additional changes.) Although R may not be quasi-local, the crucial maximal ideal of $R \subset S$ is M [10, Corollary 2.5]. A standard fact about idealizations shows that N is the unique prime ideal of S that lies over M. It also follows from the proof of [10, Corollary 2.5] that $S \subset T$ is a decomposed (minimal ring) extension with crucial maximal ideal N.

By Theorem 2.8, it remains only to verify that the above construction satisfies $(R : T) \neq M^2$. We know that $M \neq M^2$ (by the "determinant trick," as in the proof of [20, Lemma, page 255], or by, what is effectively the same here, Nakayama's Lemma). So it will suffice to prove that $M \subseteq (R : T)$. Since $T = S + R/M$ additively, $MT = MS + M(R/M)$. As $M = (R : S)$ by [12, Théorème 2.2 (ii)], $MS = M \subseteq R$. As $M(R/M) = \{0\} \subseteq R$, the proof is complete. □

Remark 2.10. By using [7, Lemma 2.4] and [8, Proposition 7.6 (a)], one can show that the data in Example 2.9 satisfy $|[R,T]| = 4$. We leave the details to the reader.

As counterpoint to Example 2.9, we next present an example of data, with R an arbitrary PID, but not a field, satisfying the hypotheses of Theorem 2.8 and $|[R,T]| = 3$. The construction in Example 2.11 is evidently motivated by the construction in Example 2.5.

Example 2.11. Let R be a PID, but not a field, and let $M \in \mathrm{Max}(R)$. Then there exist a ramified ring extension $R \subset S$ with crucial maximal ideal M and a decomposed ring extension $S \subset T$ such that N, the crucial maximal ideal of $S \subset T$, satisfies $N \cap R = M$ and $|[R,T]| = 3$. One way to construct such data is the following. Fix $p \in M$ such that $M = Rp$. Put $T := R[Y]/(Y^2 - Y, p^2Y)$, with Y an indeterminate over R, and $y := Y + (Y^2 - Y, p^2Y) \in T$. Also put $x := py \in T$ and $S := R[x]$, with N denoting the prime ideal of S that lies over M.

Proof. The first paragraph of the proof of Example 2.5 can be repeated *verbatim* here. That explains how we can view R as a subring of T. Later parts of the proof of Example 2.5 can also be repeated in order to show that $R \subset S \subset T$. Note that $T = R + Ry$. Put $C := (R : T)$ and $I := M^2$ $(= Rp^2)$. Then $I \subseteq C$ since $p^2 \in R$ and $p^2y = 0 \in R$. We have $I \neq 0$ since $M \neq 0$ and R is an integral domain. Also, $I \subseteq M$ and, by the usual "determinant trick," $I \neq M$. (Notice that the preceding step also used that M is a finitely generated nonzero proper ideal of the integral domain R.) Hence, by [20, Example, page 245], $\mathcal{R} := R/I$ is an SPIR, with unique prime ideal $\mathcal{M} := M/I$. Since I is an ideal of T, we can define the ring $\mathcal{T} := T/I$, and $\mathcal{R}$ is a subring of $\mathcal{T}$.

Note that $\pi := p + I$ generates $\mathcal{M}$ as an ideal of $\mathcal{R}$. Consider the elements $\eta := y + I \in \mathcal{T}$ and $\xi := \pi\eta \in \mathcal{T}$. Note that $\xi = x + I$. Since I is an ideal of S, we can define the ring $\mathcal{S} := S/I$, and we have the chain $\mathcal{R} \subseteq \mathcal{S} \subseteq \mathcal{T}$. In fact, since $R \subset S \subset T$, we have $\mathcal{R} \subset \mathcal{S} \subset \mathcal{T}$.

Next, we wish to confirm that when one applies the construction in Example 2.5 to the base ring $\mathcal{R}$, the resulting extension ring is $\mathcal{T}$ (up to canonical isomorphism). Harmlessly abusing notation, let Y denote an indeterminate over both R and $\mathcal{R}$. Then, using the canonical identification $\mathcal{R}[Y] = R[Y]/IR[Y]$, we find that the construction produces $(R/I)[Y]/(Y^2 - Y, \pi^2 Y) =$

$$(R[Y]/IR[Y])/((R[Y](Y^2 - Y) + R[Y]p^2Y + IR[Y])/IR[Y]),$$

which is canonically isomorphic to $R[Y]/(Y^2 - Y, I) \cong$

$$\cong (R[Y]/(Y^2 - Y, p^2Y))/((Y^2 - Y, I)/(Y^2 - Y, p^2Y)),$$

which is naturally $T/I = \mathcal{T}$, as desired. We will proceed to verify that the chain $\mathcal{R} \subset \mathcal{S} \subset \mathcal{T}$ satisfies the hypotheses of Example 2.5.

We have $\mathcal{R} \subset \mathcal{S} = \mathcal{R}[\xi]$, with $\xi^2 = \pi^2\eta^2 = (p^2y)y + I = 0 \in \mathcal{M}$ and $\xi\mathcal{M} \subseteq \mathcal{M}$ (since $\xi\pi = p^2y + I = 0 \in \mathcal{M}$). So, by the criterion in [10, Proposition 2.12], $\mathcal{R} \subset \mathcal{S}$ is a ramified extension with crucial maximal ideal $\mathcal{M}$. This implies that there is a unique maximal ideal (in fact, the only prime ideal) $\mathcal{N}$ of $\mathcal{S}$ which lies above $\mathcal{M}$ and is given by $\mathcal{N} = \mathcal{M} + \mathcal{R}\xi = \mathcal{R}\pi + \mathcal{R}\xi$. Then $N := M + Rx = Rp + Rx$ is a prime ideal of S that contains I, and it also satisfies $N/I = \mathcal{N}$, $N \cap R = M$ and $S/N \cong \mathcal{S}/\mathcal{N}$.

Instead of recapitulating further the reasoning from the proof of Example 2.5, let us recall its conclusions: $\mathcal{R} \subset \mathcal{S}$ is a ramified extension (necessarily with crucial maximal ideal $\mathcal{M}$) and $\mathcal{S} \subset \mathcal{T}$ is a decomposed extension with crucial maximal ideal $\mathcal{N}$ such that ($\mathcal{N} \cap \mathcal{R} = \mathcal{M}$ and) $|[\mathcal{R}, \mathcal{T}]| = 3$. To conclude that $R \subset S$ is a ramified extension with crucial maximal ideal M and $S \subset T$ is a decomposed ring extension (such that N, the crucial maximal ideal of $S \subset T$, satisfies $N \cap R = M$), observe the canonical isomorphisms

$$R/M \cong \mathcal{R}/\mathcal{M},\ S/M \cong \mathcal{S}/\mathcal{M},\ S/N \cong \mathcal{S}/\mathcal{N},$$

and $T/N \cong \mathcal{T}/\mathcal{N}$, and apply the criteria in [6, Corollary II.2] (cf. also [10, Corollary 2.5]). The reader may also be interested in a direct verification that $(S : T) = N$. This follows since

$$(S : T)/I = (S/I : T/I) = (\mathcal{S} : \mathcal{T}) = \mathcal{N} = N/I.$$

Finally, to conclude that $|[R, T]| = 3$, one need only use a standard homomorphism theorem to observe that the assignment $A \mapsto A/I$ determines a bijection $[R, T] \to [\mathcal{R}, \mathcal{T}]$. The proof is complete. □

The reader may have noticed that it would be possible to prove Example 2.11 by aping the steps in the proof of Example 2.5. That may be shorter than the alternate proof given above. (Of course, one would need to verify that the data satisfy the criterion "$(R : T) = M^2$" from Theorem 2.8.) The proof given above does have the virtue of illustrating the theme that certain results about PIDs can be reduced to the corresponding results about SPIRs. That method of proof also leads to the next result. Corollary 2.12 is the closest to a PID-theoretic analogue of Corollary 2.7 that we know of at this time.

Corollary 2.12. Let R be a PID, but not a field. Let $M \in \mathrm{Max}(R)$ and fix $p \in M$ such that $M = Rp$. Let $R \subset S$ be a ramified ring extension with crucial maximal ideal M and let $S \subset T$ be a decomposed ring extension whose crucial maximal ideal N satisfies $N \cap R = M$. Suppose

also that $|[R,T]| = 3$. Then one has an isomorphism of (R/M^2)-algebras (equivalently, of R-algebras)

$$T/M^2 \cong R[Y]/(Y^2 - Y, p^2),$$

where Y is an indeterminate over R.

Proof. By Theorem 2.8, $I := M^2 = (R : T)$. Put $\mathcal{R} := R/I$, $\mathcal{M} := M/I$, $\mathcal{S} := S/I$, $\mathcal{N} := N/I$, and $\mathcal{T} := T/I$. By tweaking the reasoning in the proof of Example 2.11, one can show that $(\mathcal{R}, \mathcal{M})$ is an SPIR, $\mathcal{R} \subset \mathcal{S}$ is a ramified extension (necessarily with crucial maximal ideal $\mathcal{M}$), $\mathcal{S} \subset \mathcal{T}$ is a decomposed ring extension whose crucial maximal ideal $\mathcal{N}$ satisfies $\mathcal{N} \cap \mathcal{R} = \mathcal{M}$, and $|[\mathcal{R}, \mathcal{T}]| = 3$. In addition, $\mathcal{M}^2 = 0$. Therefore, by Corollary 2.7, there is an (R/M^2)-algebra isomorphism (hence, an R-algebra isomorphism)

$$T/M^2 = T/I \cong \mathcal{R}[Y]/(Y^2 - Y, (p+I)^2 Y) \cong$$

$$(R[Y]/M^2R[Y])/((Y^2 - Y, p^2)/M^2R[Y]) \cong R[Y]/(Y^2 - Y, p^2). \qquad \square$$

Next, it will be convenient to introduce some notation and terminology that will be useful in the next four results. For the moment, fix a prime number p. Put $M = p\mathbb{Z}$, $K := \mathbb{Z}/p\mathbb{Z}$, $B_1 := \mathbb{Z}(+)K$, $\delta := (0, 1 + p\mathbb{Z}) \in B_1$, $N = M(+)K$, $\mathcal{S} := \{0, \ldots, p-1\}$ and $\mathcal{S}^* := \mathcal{S} \setminus \{0\}$. Note that $B_1 = \mathbb{Z}(+)\mathbb{Z}\delta$. In fact, we see, by reasoning as above and in [5], that each element of B_1 can be expressed uniquely in the form $n + \sigma\delta$ for some $n \in \mathbb{Z}$ and $\sigma \in \mathcal{S}$. In short, $B_1 = \mathbb{Z} + \mathcal{S}\delta$; similarly, $N = M + \mathcal{S}\delta$. Also, recall that $\mathbb{Z} \subset B_1$ is a ramified extension with crucial maximal ideal M [9] (see also [10, Corollary 2.5]). We next begin to assemble some machinery to develop a theory that will be reminiscent of the approach that led to [5, Theorem 2.20]. If $(a, b) \in \mathcal{S} \times \mathcal{S}^*$, we will say that a ring R is an (a, b)-*model* and that $y \in R$ is an (a, b)-*element* (*of* R) if $B_1 \subset R = B_1[y]$, $y^2 - y = a\delta$ and $py = b\delta$.

Next, Theorem 2.13 gives, for each prime number p, an upper bound on the number of isomorphism classes of data satisfying the equivalent conditions in Theorem 2.8 in case the base ring R is $\mathbb{Z}$.

Theorem 2.13. Let p be a fixed prime number, with $M, K, B_1, \delta, N, \mathcal{S}$ and $\mathcal{S}^*$ as above. Then:

(a) Let R be an (a, b)-model and y an (a, b)-element of R. Then $\delta y = \delta$.

(b) If $(a, b) \in \mathcal{S} \times \mathcal{S}^*$, then any two (a, b)-models are isomorphic.

(c) If $(a, b) \in \mathcal{S} \times \mathcal{S}^*$ and R is an (a, b)-model, then $B_1 \subset R$ is a decomposed extension with crucial maximal ideal N, $N \cap \mathbb{Z} = M$, and $|[\mathbb{Z}, R]| = 3$.

(d) Let R be a ring for which there exist a ramified extension $\mathbb{Z} \subset B$ with crucial maximal ideal M and a decomposed extension $B \subset R$ with crucial maximal ideal $\mathcal{N}$ such that $\mathcal{N} \cap \mathbb{Z} = M$ and $|[\mathbb{Z}, R]| = 3$. Then there exists $(a, b) \in \mathcal{S} \times \mathcal{S}^*$ such that R is isomorphic to an (a, b)-model.

(e) Let n_p denote the cardinal number of isomorphism classes of rings R for which there exist a ramified extension $\mathbb{Z} \subset B$ with crucial maximal ideal M and a decomposed extension $B \subset R$ with crucial maximal ideal $\mathcal{N}$ such that $\mathcal{N} \cap \mathbb{Z} = M$ and $|[\mathbb{Z}, R]| = 3$. Then $1 \leq n_p \leq p(p-1)$.

Proof. (a) We have $py = b\delta$. As $b \in \mathcal{S}^*$, there exists $\beta \in \mathcal{S}^*$ such that $b\beta - 1 \in M$. Thus $\beta py = \beta b\delta = \delta$, since $M\delta = 0$. Hence

$$\delta y = (\beta py)y = \beta py^2 = \beta p(y + a\delta) = \beta py + 0 = \beta py = \delta.$$

(b) By reasoning as above, if R is an (a, b)-model and y is an (a, b)-element of R, then every element of R can be expressed uniquely in the form $n + \sigma\delta + \tau y$ for some $n \in \mathbb{Z}$ and $\sigma, \tau \in \mathcal{S}$. When we combine (a) with the definition of an (a, b)-model and the basic facts that $p\delta = 0 = \delta^2$, it follows that the algebraic structure of R is determined by the equations $y^2 = a\delta + y$, $py = b\delta$, and $\delta y = \delta$. With these comments in place, we leave the proof of (b) to the reader. (That verification follows the lines of the proof for case (2) of Theorem 2.6.)

(c) Since $y^2 - y \in N$ and $yN = y(\mathbb{Z}p + \mathbb{Z}\delta) \subseteq \mathbb{Z}\delta \subseteq N$, [10, Corollary 2.5] ensures that $B_1 \subset R$ is a decomposed extension with crucial maximal ideal N. Also, it is clear (and well known) that $N \cap \mathbb{Z} = M$. In view of the above comments and Theorem 2.8, it now suffices to show that $(\mathbb{Z} : R) = M^2$. One inclusion is clear, as $p^2\delta = p \cdot 0 = 0$ and $p^2 y = p(py) = b(p\delta) = 0$. Then $M^2 \subseteq (\mathbb{Z} : R) \subseteq (\mathbb{Z} : B_1) = M$, and so $(\mathbb{Z} : R)$ is either M^2 or M. But $(\mathbb{Z} : R) \neq M$ since the fact that $b \in \mathcal{S}^*$ ensures that $py = b\delta \notin \mathbb{Z}$.

(d) Suppose that $\mathbb{Z} \subset B \subset R$ satisfies the hypotheses. By [9, Theorem 2.7] (see also [10, Corollary 2.5]), there is, up to isomorphism, only one ramified extension B of $\mathbb{Z}$ having crucial maximal ideal $p\mathbb{Z}$, namely, $B_1 = \mathbb{Z}(+)\mathbb{Z}/p\mathbb{Z}$. As R can be changed up to isomorphism, there is no harm in taking $B = B_1$ henceforth. Then the crucial maximal ideal of $B \subset R$ is $N = M(+)\mathbb{Z}/p\mathbb{Z}$. By [7, Theorems 2.2 and 2.3], there are exactly two distinct prime (in fact, maximal) ideals, say Q_1 and Q_2, of R that lie over N, they satisfy $Q_1Q_2 = Q_1 \cap Q_2 = N$, and $R = B[y]$ for some $y \in Q_1 \setminus Q_2$ such that $y^2 - y \in N$ and $yN \subseteq N$. Note that $\delta y \in NQ_1 \subseteq N \subseteq B$, and it follows that $R = B[y] = \mathbb{Z} + \mathbb{Z}\delta + \mathbb{Z}y$. By reasoning as above and in [5], we see that each element of R can be expressed uniquely in the form $n + \sigma\delta + \tau y$ with $n \in \mathbb{Z}$ and $\sigma, \tau \in \mathcal{S}$. In addition, Theorem 2.8 gives that $(\mathbb{Z} : R) = M^2 \subset M$, and so $p \notin (\mathbb{Z} : R)$. Since p and $p\delta = 0$ are elements of $\mathbb{Z}$, it follows that $py \notin \mathbb{Z}$. In particular, $py \neq 0$. This seemingly innocuous fact will have significant consequences. As a final preparatory piece, note that the above argument that $\delta y \in N$ can be tweaked to show that $y^2, y^3, py \in N$.

Consider $J := 0(+)K$ $(= \mathcal{S}\delta \subset B)$. The proof of [5, Proposition 2.12 (a)] can be easily adapted to show that J is an ideal of R. Observe via [10, Corollary 2.5] that $R/N \cong B/N \times B/N \cong \mathbb{Z}/M \times \mathbb{Z}/M = K \times K$ as algebras over $K \times K$. Then $\mathbb{Z} \cong B/J \subset R/J$ is a decomposed extension with crucial maximal ideal N/J by [10, Corollary 2.5], since $(R/J)/(N/J) \cong R/N \cong K \times K$ and $(B/J)/(N/J) \cong B/N \cong K$. Also, since $N = M(+)K$ and $J = 0(+)K$, we have a canonical isomorphism $N/J \cong M$. By yet another application of [10, Corollary 2.5], we have $R/J \cong \mathbb{Z} \times (B/J)/(N/J) \cong \mathbb{Z} \times B/N \cong \mathbb{Z} \times K$. Choose $y^* \in R \setminus J$ such that the isomorphism $R/J \to \mathbb{Z} \times K$ carries $y^* + J$ to $(0,1) \in \mathbb{Z} \times K$. That isomorphism carries $(y^*)^2 + J = (y^* + J)^2$ to $(0,1)^2 = (0,1)$, and so $(y^*)^2 + J = y^* + J$; that is $(y^*)^2 - y^* \in J$. Next, note that y^* is a nonunit of R since the isomorphism $R/J \to \mathbb{Z} \times K$ carries $y^* + J$ to a nonunit of $\mathbb{Z} \times K$. On the other hand, that isomorphism clearly carries $1 - y^* + J$ to $(1,0)$. Thus, $y^*(1 - y^*) \in J \subset N = Q_1 \cap Q_2$. Relabeling the Q_i if necessary, we have $y^* \in Q_1$. Then $y^* \notin Q_2$, since $y^* \notin N$. Indeed, $y^* \notin B$, since the only idempotent elements of (the integral domain $\mathbb{Z} \cong$) B/J are $0 + J$ and $1 + J$ and neither of these elements equals $y^* + J$ (since $(0,1)$ is neither $(0,0)$ nor $(1,1)$). It follows from the minimality of $B \subset R$ that $R[y^*] = B$. We claim that $y^*N \subseteq N$. As $N = Rp + R\delta$, it will suffice to show that $y^*p \in N$ and $y^*\delta \in N$. As y^*p is the sum of p copies of y^*, the isomorphism $R/J \to \mathbb{Z} \times K$ carries $y^*p + J$ to the sum of p copies of $(0,1)$, that is, to $(0, p + p\mathbb{Z}) = 0 \in \mathbb{Z} \times K$. Hence $y^*p + J = 0 \in R/J$; that is, $y^*p \in J \subseteq N$. Finally, since $\delta + J = 0 \in R/J$, the isomorphism $R/J \to \mathbb{Z} \times K$ carries $y^*\delta + J = (y^* + J)(\delta + J)$ to 0, whence $y^*\delta + J = 0$ and $y^*\delta \in J$. By *abus de langage*, we replace y with y^*. Henceforth, we have $R = B[y]$ with $y \in Q_1 \setminus Q_2$, $yN \subseteq N$ and $\{y^2 - y, py, \delta y\} \subseteq J$. Recall from the first paragraph of this proof of (d) that $py \neq 0$. Hence, there exist $a \in \mathcal{S}$ and $b \in \mathcal{S}^*$ such that $y^2 - y = a\delta$ and $py = b\delta$. Thus R is (isomorphic to) an (a,b)-model having y as an (a,b)-element.

(e) We have $1 \leq n_p$ by Example 2.11. In view of parts (d) and (b), $n_p \leq |\mathcal{S}| \cdot |\mathcal{S}^*| = p(p-1)$. This completes the proof. □

Proposition 2.14. Let p be a prime number, with $\mathcal{S} := \{0, \ldots, p-1\}$ and $\mathcal{S}^* := \mathcal{S} \setminus \{0\}$. Then:

(a) For each $(a,b) \in \mathcal{S} \times \mathcal{S}^*$, there exists an (a,b)-model.

(b) Let $(a_1,b_1), (a_2,b_2) \in \mathcal{S} \times \mathcal{S}^*$. Let R_1 be an (a_1,b_1)-model and let R_2 be an (a_2,b_2)-model. Then R_1 is isomorphic to R_2.

Proof. (a) As above, take $B_1 := \mathbb{Z}(+)\mathbb{Z}/p\mathbb{Z}$ and $\delta := (0, 1 + p\mathbb{Z}) \in B_1$. Let Y be an indeterminate over B_1. We will show that

$$R := B_1[Y]/(Y^2 - a\delta - Y, pY - b\delta, \delta Y - \delta)$$

is an (a,b)-model. To do so, we will prove that the canonical B_1-algebra homomorphism $B_1 \to R$ is injective (thus allowing us to view $B_1 \subseteq R$); and that $y := Y + (Y^2 - a\delta - Y, pY - b\delta, \delta Y - \delta) \notin B_1$ (so that $B_1 \subset B_1[y] = R$). Since $y^2 - y = a\delta$ and $py = b\delta$, that will complete the proof of (a).

Suppose that $\xi \in B_1$ is sent to 0 by the above map $B_1 \to R$. Write $\xi = n + \lambda\delta$ for some $n \in \mathbb{Z}$ and $\lambda \in \mathcal{S}$. Then

$$\xi = n + \lambda\delta = (Y^2 - a\delta - Y)f(Y) + (pY - b\delta)g(Y) + (\delta Y - \delta)h(Y)$$

for some $f, g, h \in B_1[Y]$. Write $f(Y) = \sum_i f_i Y^i$, with $f_i = f_{i0} + f_{i1}\delta$ for some $f_{i0} \in \mathbb{Z}$ and $f_{i1} \in \mathcal{S}$. Express $g(Y) = \sum_i (g_{i0} + g_{i1}\delta)Y^i$ and $h(Y) = \sum_i (h_{i0} + h_{i1}\delta)Y^i$ similarly. Equating constant terms gives

$$n + \lambda\delta = -a\delta f_{00} - b\delta g_{00} - \delta h_{00}.$$

It follows that $n = 0$, and so $\xi = \lambda\delta$. Without loss of generality, $\xi \neq 0$ (and we seek a contradiction). Thus $\lambda \neq 0$; that is, $\lambda \in \mathcal{S}^*$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, there exists $\lambda^* \in \mathcal{S}^*$ such that $\lambda^*\lambda - 1 \in M$, and so $\lambda^*\lambda\delta = \delta$. Then $\lambda^*\xi = \delta$. Notice that the canonical map $B_1 \to R$ sends $\lambda^*\xi$ to 0. Moreover $\lambda^*\xi \neq 0$, since $\lambda(\lambda^*\xi) = \xi \neq 0$. Thus, by replacing ξ with $\lambda^*\xi$, we can assume that $\xi = \delta$ (and $\lambda = 1$).

Next, equating coefficients of Y in the displayed expression for ξ leads to

$$0 = -a\delta f_{10} - f_{00} - f_{01}\delta + pg_{00} - b\delta g_{10} + \delta h_{00} - \delta h_{10}.$$

It follows that $f_{00} = pg_{00} \in M$. Since $\xi = \delta$, the displayed expression for ξ also gives

$$0 = p\delta = p\xi = p(Y^2 - Y)f(Y) + p^2 Y g(Y).$$

By applying the B_1-algebra endomorphism of $B_1[Y]$ determined by $Y \mapsto 1$ to the last display, we get $p^2 g(1) = 0$. Since $g(1) \in B_1$, it follows that $g(1) \in \mathcal{S}\delta$. Therefore, applying $Y \mapsto 1$ to the displayed expression for ξ leads to

$$\delta = \xi = -a\delta f(1) + (p - b\delta)g(1) = -a\delta f(1) + 0 = -a\delta f(1).$$

Consider $0 = \delta^2 = \xi^2 =$

$$((Y^2 - a\delta - Y)f(Y) + (pY - b\delta)g(Y) + (\delta Y - \delta)h(Y))^2.$$

After some algebraic simplification and dividing through by Y, one finds that $Y(Y-1)^2 f(Y)^2 \in NB_1[Y]$, where as usual, $N := M + \mathcal{S}\delta$. As $B_1[Y]/NB_1[Y] \cong (B_1/N)[Y]$ is an integral domain, $NB_1[Y]$ is a prime ideal of $B_1[Y]$. Since neither Y nor $Y-1$ is an element of $NB_1[Y]$, we get that $f(Y) \in NB_1[Y]$. Consequently $f(1) \in N$, so that $\delta = -a\delta f(1) = 0$, the desired contradiction. This proves that we can view $B_1 \subseteq R$.

It remains only to prove that $y \notin B_1$. Suppose the assertion fails. Then $y = c + \tau\delta$ for some $c \in \mathbb{Z}$ and $\tau \in \mathcal{S}$. Hence

$$0 \neq b\delta = py = p(c + \tau\delta) = pc + 0 = pc \in \mathbb{Z} \cap \mathbb{Z}\delta = \{0\},$$

the desired contradiction.

(b) For $i = 1, 2$, pick some $y_i \in R_i$ that is an (a_i, b_i)-element (of R_i). Then $y_i^2 = a_i\delta + y_i$, $py_i = b_i\delta$ and $\delta y_i = \delta$. Choose c to be the unique element of $\mathcal{S}^*$ such that $c + M = (b_2 + M)(b_1 + M)^{-1}$ in the multiplicative group of nonzero elements of the field $\mathbb{Z}/p\mathbb{Z}$. It will be convenient to let λ denote the unique element of $\mathcal{S}$ such that $\lambda - (a_1 c - a_2) \in M$. With c and λ in hand, define a function (which will be shown to be an isomorphism) $f : R_1 \to R_2$ as follows. Let $\xi \in R_1$. Then ξ can be uniquely expressed in the "canonical form" $n + \sigma\delta + \tau y_1$ where $n \in \mathbb{Z}$ and $\{\sigma, \tau\} \subseteq \mathcal{S}$. Let

$$f(\xi) = f(n + \sigma\delta + \tau y_1) := n + (\sigma c + \tau\lambda)\delta + \tau y_2.$$

In particular, $f(n) = n$ for all $n \in \mathbb{Z}$, $f(\delta) = c\delta$ and $f(y_1) = \lambda\delta + y_2$. We next proceed to verify that f preserves addition and multiplication. As those verifications will involve some lengthy but straightforward calculations, we will leave some intermediate steps to the reader. Lastly, we will show that f is a bijection.

Let $\xi_1, \xi_2 \in R_1$. For $j = 1, 2$, write ξ_j in canonical form as $n_j + \sigma_j\delta + \tau_j y_1$. Also write

$$\sigma_1 + \sigma_2 = \sigma_3 + pe_1, \;\; \tau_1 + \tau_2 = \sigma_4 + pe_2, \;\; \text{and} \;\; \sigma_3 + e_2 b_1 = \sigma_5 + pe_3,$$

where $\sigma_3, \sigma_4, \sigma_5 \in \mathcal{S}$ and $e_1, e_2, e_3 \in \mathbb{Z}$. One checks easily that $\xi_1 + \xi_2 = n_1 + n_2 + (\sigma_5 + pe_3)\delta + \sigma_4 y_1 = n_1 + n_2 + \sigma_5\delta + \sigma_4 y_1$. Therefore

$$f(\xi_1 + \xi_2) = n_1 + n_2 + (\sigma_5 c + \sigma_4\lambda)\delta + \sigma_4 y_2.$$

On the other hand, one checks easily that

$$f(\xi_1) + f(\xi_2) = n_1 + n_2 + [(\sigma_3 + pe_1)c + (\sigma_4 + pe_2)\lambda]\delta + (\sigma_4 + pe_2)y_2 =$$

$n_1 + n_2 + [\sigma_3 c + \sigma_4\lambda + e_2b_2]\delta + \sigma_4 y_2$. Thus, checking that $f(\xi_1 + \xi_2) = f(\xi_1) + f(\xi_2)$ (for all ξ_1 and ξ_2) comes down to verifying that

$$\sigma_5 c\delta = (\sigma_3 c + e_2b_2)\delta,$$

that is, that $c(\sigma_3 + e_2b_1)\delta = (\sigma_3 c + e_2b_2)\delta$; or, equivalently, that $e_2b_2\delta = ce_2b_1\delta$. This, in turn, holds because the above choice of c ensures that $e_2(b_2 - cb_1) \in e_2M \subseteq M$. This completes the proof that f preserves addition.

Let $\xi_1, \xi_2 \in R_1$, written in canonical form as above. Also write

$$n_1\sigma_2 + n_2\sigma_1 + \sigma_1\tau_2 + \sigma_2\tau_1 + \tau_1\tau_2 a_1 = \sigma_6 + pe_4,$$

$n_1\tau_2 + n_2\tau_1 + \tau_1\tau_2 = \sigma_7 + pe_5$, and $\sigma_6 + e_5b_1 = \sigma_8 + pe_6$ for some $\sigma_6, \sigma_7, \sigma_8 \in \mathcal{S}$ and $e_4, e_5, e_6 \in \mathbb{Z}$. It is straightforward to check that $\xi_1\xi_2$ simplifies to the canonical form $n_1n_2 + \sigma_8\delta + \sigma_7 y_1$, and so

$$f(\xi_1\xi_2) = n_1n_2 + [\sigma_8 c + \sigma_7\lambda]\delta + \sigma_7 y_2.$$

We next indicate how to show that $f(\xi_1)f(\xi_2)$ simplifies to the same thing.

Using the fact that $\lambda - (a_1c - a_2) \in M$, one can show that $f(\xi_1)f(\xi_2) = n_1n_2 + \mu\delta + (\sigma_7 + pe_5)y_2$, for a complicated expression μ that can be simplified to

$$\mu = c(\sigma_6 + pe_4) + (\sigma_7 + pe_5)\lambda.$$

Thus $f(\xi_1)f(\xi_2) = n_1n_2 + (\mu + e_5b_2)\delta + \sigma_7 y_2$. Hence, checking that $f(\xi_1\xi_2) = f(\xi_1)f(\xi_2)$ (for all ξ_1 and ξ_2) comes down to verifying that

$$[\sigma_8 c + \sigma_7\lambda] - [\mu + e_5b_2] \in M,$$

that is, that $[\sigma_8 c + \sigma_7\lambda] - [c\sigma_6 + \sigma_7\lambda + e_5b_2] \in M$; or, equivalently, that

$$(\sigma_6 c + e_5b_1c) - (c\sigma_6 + e_5b_2) \in M.$$

This, in turn, holds since the above choice of c ensures that

$$e_5b_1c - e_5b_2 = e_5(b_1c - b_2) \in e_5M \subseteq M.$$

This completes the proof that f preserves multiplication.

We verify next that f is an injection. Since f preserves addition, it suffices to show that if $f(\xi) = 0$, then $\xi = 0$. Write $\xi = n + \sigma\delta + \tau y_1$ for some (uniquely determined) $n \in \mathbb{Z}$ and $\sigma, \tau \in \mathcal{S}$. Then $0 = f(\xi) = n + (\sigma c + \tau\lambda)\delta + \tau y_2$. Hence $n = 0$, $\sigma c + \tau\lambda \in M$ and $\tau = 0$. It will suffice to prove that $\sigma = 0$. As $\sigma c \in M$ and there exists $c^* \in \mathcal{S}^*$ such that $m := cc^* - 1 \in M$, we have $\sigma = \sigma(cc^* - m) = (\sigma c)c^* - \sigma m \in M + M = M$. Then $\sigma \in M \cap \mathcal{S} = \{0\}$, so that $\sigma = 0$, as desired.

It remains only to prove that f is surjective. Of course, the image of f contains $\mathbb{Z}$. With $c^* \in \mathcal{S}^*$ as above, we have $f(c^*\delta) = c^*f(\delta) = c^*c\delta = \delta$. As f preserves addition and $R_2 = \mathbb{Z} + \mathbb{Z}\delta + \mathbb{Z}y_2$, it suffices to prove that y_2 is in the image of f. In fact,

$$f(-c^*\lambda\delta + y_1) = (-c^*\lambda c + \lambda)\delta + y_2 = \lambda(-c^*c + 1)\delta + y_2 = \lambda \cdot 0 + y_2 = y_2.$$

The proof is complete. □

We can now improve the estimate of n_p given in Theorem 2.13 (e).

Corollary 2.15. Let p be a fixed prime number, with $M = \mathbb{Z}p$. Let B_1, δ, $\mathcal{S}$ and $\mathcal{S}^*$ be as above. Then a unique isomorphism class is formed by the rings R for which there exist a ramified extension $\mathbb{Z} \subset B$ with crucial maximal ideal M and a decomposed extension $B \subset R$ with crucial maximal ideal $\mathcal{N}$ such that $\mathcal{N} \cap \mathbb{Z} = M$ and $|[\mathbb{Z}, R]| = 3$. (In the terminology of Theorem 2.13, $n_p = 1$.) Some members of this isomorphism class are $\mathbb{Z}[Y]/(Y^2 - Y, p^2Y)$, where Y is an indeterminate over $\mathbb{Z}$, and the rings of the form

$$B_1[X]/(X^2 - i\delta - X, pX - j\delta, \delta X - \delta),$$

where X denotes an indeterminate over B_1, $i \in \mathcal{S}$, and $j \in \mathcal{S}^*$.

Proof. The first assertion follows by combining parts (c) and (d) of Theorem 2.13 with both parts of Proposition 2.14. As for the validity of the asserted members of the isomorphism class, see Example 2.11, Proposition 2.14 (a) and Theorem 2.13 (c). □

Remark 2.16. (a) It seems natural to ask how one could discover the formulas for $f(y_1)$ and $f(\delta)$ that were used in the proof of Proposition 2.14 (b). We next explain why no other formulas for f could possibly have worked. Suppose, then, in the context of Proposition 2.14 (b), that $F : R_1 \to R_2$ is an isomorphism. Since $|[\mathbb{Z}, R_i]| = 3$ and the injectivity of F force $F(B_1) = B_2$ and $F(\delta) \notin \mathbb{Z}$, we get $F(\delta) = n^* + c\delta$ for some $n^* \in \mathbb{Z}$ and $c \in \mathcal{S}^*$. As $0 = F(p\delta) = pF(\delta) = pn^*$ and $\mathbb{Z}$ is an integral domain with $p \neq 0$, we get $n^* = 0$, so that $F(\delta) = c\delta$. Next, since the injectivity of F forces $F(y_1) \notin B_1$, we can write $F(y_1) = n + \lambda\delta + \tau y_2$ for some $n \in \mathbb{Z}$, $\lambda \in \mathcal{S}$ and $\tau \in \mathcal{S}^*$. Applying F to the identity $py_1 = b_1\delta$ leads to $p(n + \lambda\delta + \tau y_2) = b_1F(\delta) = b_1c\delta$, whence $pn = b_1c\delta - \tau b_2\delta \in \mathbb{Z} \cap \mathbb{Z}\delta = \{0\}$. Invoking the integrity of $\mathbb{Z}$ once again, we get $n = 0$. In addition, $\tau b_2 - b_1c \in (0 :_{\mathbb{Z}} \delta) = M$. Next, applying F to the identity $y_1^2 = a_1\delta + y_1$ leads, after simplification, to

$$(\tau^2 a_2 + 2\lambda\tau - a_1c - \lambda)\delta + (\tau^2 - \tau)y_2 = 0.$$

Hence, $\tau(\tau - 1) = \tau^2 - \tau \in (B_1 :_{\mathbb{Z}} y_2) = M$. As $\tau \notin M$ and M is a prime ideal of $\mathbb{Z}$, we get $\tau - 1 \in M$. Since τ and 1 are each elements of $\mathcal{S}$, it follows that $\tau = 1$. Consequently, $b_1c\delta - b_2\delta = b_1c\delta - \tau b_2\delta = 0$, whence $b_1c - b_2 \in M$. This determines $c + M$ as $(b_2 + M)(b_1 + M)^{-1}$ in the field $\mathbb{Z}/p\mathbb{Z}$, and so the formula for c in the proof of Proposition 2.14 (b) has been justified/explained. It remains only to explain why λ had to be chosen in that proof to be $a_1c - a_2$ (modulo M) . In fact, since $(a_2 + \lambda - a_1c)\delta =$

$$(a_2 + 2\lambda - a_1c - \lambda)\delta = (\tau^2 a_2 + 2\lambda\tau - a_1c - \lambda)\delta = -(\tau^2 - \tau)y_2 = 0,$$

we get $a_2 + \lambda - a_1c \in M$, so that $\lambda + M = a_1c - a_2 + M$, as desired.

(b) It is interesting to reassess the construction in Example 2.11 from the point of view of (a, b)-models. Specializing that construction to the situation where the PID base ring is $\mathbb{Z}$, we obtain, for any fixed prime number p, the ring (let us denote it here by) $R := \mathbb{Z}[Y]/(Y^2 - Y, p^2Y) = \mathbb{Z}[y]$, with Y an indeterminate over $\mathbb{Z}$, and $y := Y + (Y^2 - Y, p^2Y) \in R$. Thus $y^2 = y$ and $p^2y = 0$. Recall that $x := py \in R$ and $S := \mathbb{Z}[x] = \mathbb{Z} + \mathbb{Z}x$ are such that $\mathbb{Z} \subset S$ is a ramified extension with crucial maximal ideal $M = p\mathbb{Z}$, $S \subset R$ is a decomposed extension with crucial maximal ideal $\mathcal{N} := M + \mathcal{S}x$, $\mathcal{N} \cap \mathbb{Z} = M$ and $|[\mathbb{Z}, R]| = 3$. We next give a "hands-on" proof, and then a more sophisticated proof, that R is isomorphic to a $(0, 1)$-model.

Since $x^2 = 0 = px$, we have $S = \mathbb{Z}(+)\mathbb{Z}x \cong \mathbb{Z}(+)\mathbb{Z}/(0 :_{\mathbb{Z}} x) = \mathbb{Z}(+)\mathbb{Z}/p\mathbb{Z} = B_1$. In fact, a specific isomorphism $f : S \to B_1$ can be given by $n_1 + n_2x \mapsto n_1 + n_2\delta$ for all $n_1, n_2 \in \mathbb{Z}$. The "hands-on" proof is as follows. Access the list of elements in R and change the name "x" to "δ". Next, access the addition table and the multiplication table for (the elements of) R and change every occurrence of "x" in those tables to "δ." These hands-on actions have produced a mathematical structure that is patently isomorphic to R. It is also a $(0, 1)$-model, since $y^2 - y = 0$ and $py = (x =)\ \delta$.

The above argument can be given a presentation that is more in keeping with today's norms. Use the above isomorphism $f : S \to B_1$ to view B_1 as an S-algebra. Then f induces an isomorphism $g : R \to \mathcal{T} := R \otimes_S B_1$ (given by $r \mapsto r \otimes 1$ for each $r \in R$). When g is restricted to S, the result is an injective homomorphism $h : S \to \mathcal{T}$. Then $j := h \circ f^{-1} : B_1 \to \mathcal{T}$ is an injective homomorphism which can be identified with the inclusion map $S \hookrightarrow R$. Given what we know about $S \subset R$, it follows that $j(B_1) \subset \mathcal{T}$ is a decomposed extension whose crucial maximal ideal, $jf(\mathcal{N}) = g(\mathcal{N})$, clearly lies over M and $|[\mathbb{Z}, \mathcal{T}]| = |[\mathbb{Z}, R]| = 3$. If we use j to view $B_1 \hookrightarrow \mathcal{T}$, then $\mathcal{T}$ is a $(0, 1)$-model having $g(y) = y \otimes 1$ as a $(0, 1)$-element. The assertion follows since R is isomorphic to $\mathcal{T}$ via g.

As mentioned in the Introduction, when one combines the results in this note with (the valid part of) [3], [4] and [5], the result is a characterization of the (commutative unital) rings with exactly two proper (unital) subrings. Corollaries 2.17 and 2.18, respectively, state that characterization for rings of positive characteristic and for rings of characteristic 0. We wish to stress that the major work in producing these conclusions was not done in the present work, as our main interest here has been to correct the known relevant errors in the literature that were caused by the erroneous statement of [3, Theorem 2.8].

Corollary 2.17. 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 [4, 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) $\alpha \geq 2$, 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 $(A : E) = M^2$.

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). In addition, for each prime number p and each integer $\alpha \geq 2$, there exist at least one, but only finitely many, isomorphism classes of rings R that form part of a set of data satisfying the above condition (f); if either $\alpha = 2$ or $p = 2$, that number of isomorphism classes is 1 and a representative of that isomorphism class is $E = (\mathbb{Z}/p^\alpha\mathbb{Z})[Y]/(Y^2 - Y, p^2Y)$, where Y is an indeterminate.

Proof. The statement has edited [5, Corollary 3.6] by adding condition (f) and the "In addition" assertion. Note that [5, Corollary 3.6] was a refinement of [4, Theorem 2.15], with the main contribution of [5, Corollary 3.6] being the above formulation of condition (e) and the "Furthermore" assertion. Unfortunately, [4, Theorem 2.15] had been based, in part, on the erroneous [3, Theorem 2.8]. In view of the supporting FIP-theoretic work in [11, Theorem 4.1], this situation has required the addition of a condition (f); and Theorems 2.2 and 2.6 combine with Corollary 2.7 to show that the above formulation of (f) fills the gap that existed in the earlier works. Finally, we turn to the "In addition" assertion. Its "existence" part follows from Example 2.5. Its "but only finitely many" part follows because any R of interest in (f) has cardinality $p^{\alpha+2}$ (and of course, there are, up to isomorphism, only finitely many faithful commutative A-algebras of cardinality $p^{\alpha+2}$). Its statements concerning $\alpha = 2$ (resp., $p = 2$) come from using condition (1) (resp., condition (2)) in Theorem 2.6 in conjunction with Corollary 2.7. □

Corollary 2.18. The rings R of characteristic 0 that have exactly two proper subrings can be classified, up to isomorphism, as the rings satisfying (exactly) one of the following three conditions:

(a) $R := \mathbb{Z} \times \mathbb{F}_{p^q}$, where p and q are (possibly equal) prime numbers (which are uniquely determined by R);

(b) If one takes $A = \mathbb{Z}$, then for some (uniquely determined) prime number p, R is (isomorphic to exactly) one of the rings R_1, R_2, R_3 in [5, Examples 2.3-2.4];

(c) $R := \mathbb{Z}[Y]/(Y^2 - Y, p^2Y)$, where Y is an indeterminate over $\mathbb{Z}$ and p is a prime number (which is uniquely determined by R).

Also, for each prime number p, the cardinal number of the collection of isomorphism classes of the rings R satisfying the above condition (a) (resp., (b); resp., (c)) is $\aleph_0$ (resp., 3; resp., 1).

Proof. The statement has edited [5, Corollary 2.21] by adding condition (c) and the "Also" assertion for (c). Note that [5, Corollary 2.21] was a refinement of [4, Theorem 2.6 (1)], with the main contribution of [5, Corollary 2.21] being the above formulation of condition (b) and the "Also" assertions concerning (a) and (b). Unfortunately, [4, Theorem 2.6 (1)] had been based, in part, on the erroneous [3, Theorem 2.8]. In view of the supporting FIP-theoretic work in [11, Theorem 4.1], this situation has required the addition of a condition (c). Theorem 2.8, Example

2.11 and Corollary 2.15 combine to show that the above formulation of (c) fills the gap that existed in the earlier works and also to establish the "Also" assertion concerning (c). □

Corollary 2.20 will generalize Theorem 2.2 and the PID case of Theorem 2.8 to the context where the base ring R is an arbitrary (nonzero) principal ideal ring (PIR). Lemma 2.19 will focus on some relevant preparatory material. The relevance of Lemma 2.19 to PIRs derives from the well known structure theorem (cf. [20, Theorem 33, pages 245-246]) that a ring R is a PIR if and only if R is isomorphic to a finite direct product $\prod_{k=1}^{n} R_k$ such that for each index k, R_k is either a field, a PID which is not a field, or an SPIR. In the next two results, we use the convention that if a factor in a finite direct product of rings is itself a direct product that is indexed by the empty set, then we ignore that factor.

Lemma 2.19. For some positive integer n, let $A_k \subseteq B_k$ be a ring extension for each $k = 1, \ldots, n$. Put $A := \prod_{k=1}^{n} A_k$ and $B = \prod_{k=1}^{n} B_k$. Then:

(a) $(A : B) = \prod_{k=1}^{n} (A_i : B_i)$.

(b) Let $A \subset B$ be a minimal ring extension with crucial maximal ideal M. Then there exist a unique index i and a unique $M_i \in \mathrm{Max}(A_i)$ such that $A_i \subset B_i$ is a minimal ring extension with crucial maximal ideal M_i and $A_k = B_k$ for each index $k \neq i$. Moreover,

$$M = \prod_{1 \leq k < i} A_k \times M_i \times \prod_{i < k \leq n} A_k.$$

Furthermore, $A \subset B$ is a ramified (resp., decomposed) extension if and only if $A_i \subset B_i$ is a ramified (resp., decomposed) extension.

Proof. We leave to the reader the easy calculation that proves (a). As for (b), its first assertion follows from [6, Proposition III.4 (b)]. Next, by [12, Théorème 2.2 (ii)], $M = (A : B)$ and $M_i = (A_i : B_i)$. Hence, by (a),

$$M = (A : B) = \prod_{k=1}^{n} (A_k : B_k) = \prod_{1 \leq k < i} A_k \times (A_i : B_i) \times \prod_{i < k \leq n} A_k.$$

It remains only to prove the "Furthermore" assertion. Consider the field $F := A/M$. By a standard homomorphism theorem, $F \cong$

$$\{0\} \times A_i/M_i \times \{0\} \cong A_i/M_i \text{ and } B/M \cong \{0\} \times B_i/M_i \times \{0\} \cong B_i/M_i.$$

It is harmless to view these isomorphism as identifications. Then (cf. the proof of [6, Corollary II.2]) $A \subset B$ is ramified $\Leftrightarrow$ $B/M \cong F[X]/(X^2)$ as an F-algebra $\Leftrightarrow$ $A_i \subset B_i$ is ramified; and $A \subset B$ is decomposed $\Leftrightarrow$ $B/M \cong F \times F$ as an F-algebra $\Leftrightarrow$ $A_i \subset B_i$ is decomposed. □

Corollary 2.20. Let R be a PIR. Let $R \subset S$ be a ramified ring extension and let M denote the crucial maximal ideal of $R \subset S$. Let $S \subset T$ be a decomposed ring extension. Fix a ring isomorphism α from R onto a finite direct product $R^* = \prod_{k=1}^{n} R_k$ such that for each index k, R_k is either a field, a PID which is not a field, or an SPIR. Then there exist a unique index i and a unique $M_i \in \mathrm{Max}(R_i)$ such that

$$\alpha(M) = \prod_{1 \leq k < i} R_k \times M_i \times \prod_{i < k \leq n} R_k.$$

By using the canonical map $S \to S \otimes_R R^*$ induced by α, we get an R-algebra isomorphism β from S onto a finite direct product $S^* = \prod_{k=1}^{n} S_k$ such that for each index k, S_k is a ring such that $R_k \subseteq S_k$. Then there exists a unique index j such that $R_j \subset S_j$ is a minimal ring extension and $R_k = S_k$ for all $k \neq j$. In fact, $j = i$ and $(R_i : S_i) = M_i$ is the crucial maximal ideal of $R_i \subset S_i$. By using the canonical map $T \to T \otimes_S S^*$ induced by β, we get an S-algebra isomorphism (hence R-algebra isomorphism) γ from T onto a finite direct product $T^* = \prod_{k=1}^{n} T_k$ such that for each index k, T_k is a ring such that $S_k \subseteq T_k$. Then there exists a unique index ν such that $S_\nu \subset T_\nu$ is a minimal ring extension and $S_k = T_k$ for all $k \neq \nu$. Let N denote the crucial maximal ideal of $S \subset T$. In fact,

$$\beta(N) = \prod_{1 \leq k < \nu} S_k \times N_\nu \times \prod_{\nu < k \leq n} S_k,$$

where $N_\nu = (S_\nu : T_\nu)$ is the crucial maximal ideal of $S_\nu \subset T_\nu$. Then:
(a) $(R : T) = M^2 \Leftrightarrow i = \nu$ and $(R_i : T_i) = M_i^2$.
(b) $N \cap R = M \Leftrightarrow i = \nu$ and $N_\nu \cap R_\nu = M_i$.
(c) The following three conditions are equivalent:
(1) $|[R, T]| = 3$;
(2) $i = \nu$, R_i is not a field, and $(R_i : T_i) = M_i^2$;
(3) R_i is not a field and $(R : T) = M^2$.

Proof. Since $\alpha(M) \in \mathrm{Max}(R^*)$, the existence and uniqueness of i and M_i follow from the well known description of the prime spectrum of a finite direct product of rings. Next, observe that since $R \subset S$ (resp., $S \subset T$) is a minimal ring extension, so is $R^* \subset S^*$ (resp., $S^* \subset T^*$). Then the existence and uniqueness of j (resp., of ν) follow by combining Lemma III.3 (d) and Proposition III.4 (b) of [6].

We next establish the "In fact" assertions. Recall from [12, Théorème 2.2 (ii)] that the crucial maximal ideal of $R \subset S$ is $(R : S) = M$. Similarly, the crucial maximal ideal of $R_j \subset S_j$ is $(R_j : S_j)$. An easy diagram chase shows that $\beta((R : S)) = (R^* : S^*)$, and so

$$\alpha(M) = \beta(M) = \beta((R : S)) = \prod_{1 \le k < j} R_k \times (R_j : S_j) \times \prod_{j < k \le n} R_k,$$

where the final equality in the preceding display is due to Lemma 2.19 (a). By comparing the preceding display with the first display in the statement of this result, we see that $j = i$ and so $(R_i : S_i) = M_i$. The second "In fact" assertion is proved similarly.

(a) If $\nu < i$, then $\gamma((R : T)) = (R^* : T^*) =$

$$\prod_{1 \le k < \nu} R_k \times (S_\nu : T_\nu) \times \prod_{\nu < k \le i} R_k \times (R_i : S_i) \times \prod_{i < k \le n} R_k.$$

A similar situation holds if $i < \nu$. In addition,

$$\gamma(M^2) = \alpha(M^2) = \prod_{1 \le k < i} R_k \times M_i^2 \times \prod_{i < k \le n} R_k.$$

By the last two displays, if $i \neq \nu$, then $\gamma((R : T)) \neq \gamma(M^2)$, and so $(R : T) \neq M^2$. Equivalently, if $(R : T) = M^2$, then $i = \nu$.

Suppose next that $i = \nu$. Then

$$\gamma((R : T)) = (R^* : T^*) = \prod_{1 \le k < i} R_k \times (R_i : T_i) \times \prod_{i < k \le n} R_k.$$

Hence, $(R : T) = M^2 \Leftrightarrow \gamma((R : T)) = \gamma(M)^2 \Leftrightarrow \gamma((R : T)) = \alpha(M)^2 \Leftrightarrow (R_i : T_i) = M_i^2$. This completes the proof of (a).

(b) $\beta(N \cap R) = \beta(N) \cap \alpha(R) = \beta(N) \cap R^* =$

$$\prod_{1 \le k < \nu} R_k \times \ (S_\nu : T_\nu) \cap R_\nu \ \times \prod_{\nu < k \le n} R_k.$$

On the other hand, $\beta(M) = \alpha(M)$. It follows that $N \cap R = M \Leftrightarrow \beta(N \cap R) = \beta(M) \Leftrightarrow i = \nu$ and $(S_\nu : T_\nu) \cap R_\nu = M_i \Leftrightarrow i = \nu$ and $N_\nu \cap R_\nu = M_i$.

(c) (2) $\Leftrightarrow$ (3): Apply (a).

(1) $\Rightarrow$ (2): Assume (1). Then by [11, Proposition 3.1 (d)], $N \cap R = M$. Hence by (b), $i = \nu$ and $N_\nu \cap R_i = M_i$. (We can also see that $i = \nu$ directly by reasoning as in the first four sentences in the proof of [4, Theorem 15].) Consider the following common ideal of R and T:

$$I := \prod_{1 \le k < i} R_k \times \{0\} \times \prod_{i < k \le n} R_k.$$

The canonical isomorphism $T/I \to T_i$ restricts to an isomorphism $R/I \to R_i$. Thus, a standard homomorphism theorem ensures that $|[R, T]| = |[R_i, T_i]|$, and so $|[R_i, T_i]| = 3$. Next, Lemma

2.19 (b) yields that $R_i \subset S_i$ is ramified and $S_i \subset T_i$ is decomposed. Also, we have seen that the crucial maximal ideal of $S_i \subset T_i$ (namely, N_ν) lies over the crucial maximal ideal of $R_i \subset S_i$ (namely, M_i). Hence, by Proposition 2.1 (or the valid part of the "proof" of [3, Theorem 2.8]), R_i is not a field. Therefore, since R_i is either an SPIR or a PID (which is not a field), we may apply either Theorem 2.2 or Theorem 2.8 to conclude that $(R_i : T_i) = M_i^2$.

(2) $\Rightarrow$ (1): Assume (2). As $i = \nu$, we can then see, as in the proof that (1) $\Rightarrow$ (2), that $|[R, T]| = |[R_i, T_i]|$, and so it suffices to prove that $|[R_i, T_i]| = 3$. We have, as above via Lemma 2.19 (b), that $R_i \subset S_i$ is ramified (with crucial maximal ideal M_i) and $S_i \subset T_i$ is decomposed (with crucial maximal ideal $N_\nu = (S_i : T_i)$). Also, since R_i is not a field, R_i is either an SPIR or a PID (which is not a field). Thus, if we could prove that the hypotheses and (equivalent) conditions in either Theorem 2.2 or Theorem 2.8 are satisfied, the proof would be complete. Therefore, it remains only to show that $N_\nu \cap R_i = M_i$. It will therefore suffice to show that $M_i \subseteq N_\nu$. Now, since $(R_i : T_i) = M_i^2$, we have $\mathrm{nil}_{R_i}((R_i : T_i)) = M_i$. Thus

$$M_i \subseteq \mathrm{nil}_{S_i}((S_i : T_i)) = \mathrm{nil}_{S_i}(N_\nu) = N_\nu.$$

The proof is complete. □

In closing, we record an important special case.

Corollary 2.21. Let R be an (Artinian) semisimple ring, that is, a ring that is (isomorphic to) a finite direct product of fields. Let $R \subset S$ be a ramified ring extension and let $S \subset T$ be a decomposed ring extension. Then $|[R, T]| > 3$.

Proof. Since any (Artinian) semisimple ring is a von Neumann regular ring, the assertion is an immediate consequence of Proposition 2.1. For an alternate (and perhaps more amusing) proof, note first that, since each field is a PIR, it follows from [20, Theorem 33, page 245] that R is a PIR. Then an application of Corollary 2.20 completes the alternate proof. □

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, Every commutative ring has a minimal ring extension, Comm. Algebra **34** (2006), 3875–3881.

[3] 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.

[4] 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.

[5] D. E. Dobbs, Certain towers of ramified minimal ring extensions of commutative rings, Communications in Algebra, DOI:10.1080/00927872.2017.1412446.

[6] D. E. Dobbs, B. Mullins, G. Picavet, and M. Picavet-L'Hermitte, On the FIP property for extensions of commutative rings, Comm. Algebra **33** (2005), 3091–3119.

[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, M. Picavet-L'Hermitte and J. Shapiro, On intersections and composites of minimal ring extensions, JP J. Algebra, Number Theory, Appl. **26** (2012), 103–158.

[9] D. E. Dobbs and J. Shapiro, A classification of the minimal ring extensions of an integral domain, J. Algebra **305** (1) (2006), 185–193.

[10] D. E. Dobbs and J. Shapiro, A classification of the minimal ring extensions of certain commutative rings, J. Algebra **308** (2007), 800–821.

[11] 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.

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

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

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

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

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

[17] G. Picavet and M. Picavet-L'Hermitte, Modules with finitely many submodules, Internat. Electron. J. Algebra **19** (2016), 119–131.

[18] G. Picavet and M. Picavet-L'Hermitte, Personal communication, August 23, 2017.

[19] R. G. Swan, On seminormality, J. Algebra **67** (1980), 210–229.

[20] 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@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: September 20, 2017.

Accepted: December 27, 2017.