JOURNAL OF COMMUTATIVE ALGEBRA
Volume 5, Number 4, Winter 2013

A CONSTRUCTIVE THEORY OF MINIMAL ZERO-DIMENSIONAL EXTENSIONS

FRED RICHMAN

ABSTRACT. Chiorescu characterized the minimal zero-dimensional extensions of certain one-dimensional rings in terms of families of ideals indexed by prime ideals. In this paper we give a constructive development of these extensions, which, to achieve maximum generality, must necessarily avoid dependence on prime ideals. This forces us to develop a purely arithmetic theory. Along the way we get a characterization, in terms of the lattice of radicals of finitely generated ideals, of when a ring with primary zero-ideal has dimension at most one.

1. Introduction. In this paper we prove a constructive version of Chiorescu's theorem [**3**] that gives a complete set of invariants for minimal zero-dimensional extensions of a commutative ring R which satisfies the three conditions:

1. $\dim R \leq 1$.
2. The zero ideal of R is primary.
3. R has Noetherian spectrum.

Chiorescu's invariants are phrased in terms of the prime ideals of R. One of our goals was to formulate a theorem that would work when $R = k[X]$ for k a (discrete) field. In that setting, we cannot necessarily prove that every polynomial of degree greater than zero is a product of irreducible polynomials, so Chiorescu's theorem cannot be applied. Generally, when doing constructive commutative ring theory, you avoid formulations involving prime ideals because you might not have the tools to construct them. But even, outside the constructive framework, it is of interest to develop purely arithmetic theories when possible.

For our main theorem (Section 8), we don't need the third condition. In order to derive Chiorescu's theorem as she stated it, we will

2010 AMS *Mathematics subject classification.* Primary 13B02, Secondary 03F65.
Received by the editors on August 12, 2011, and in revised form on October 31, 2011.

DOI:10.1216/JCA-2013-5-4-545

use a condition that is equivalent to Noetherian spectrum for finite-dimensional rings, has lots of computational content, and applies, for example, to the ring of integers of a finite-dimensional algebraic number field.

We formulate the second condition as saying that every element of R is either regular or nilpotent. This implies, for a nontrivial ring R (or for a trivial ring R), the purely constructive condition that every element of R is either nilpotent or not. That is, the nilradical of R is detachable–the only nonclassical condition that we impose on R for the general theorem. We don't impose any such conditions on the extension ring.

For the first condition, we follow the constructive treatment of Krull dimension in [**5**]. In the presence of the second condition, the condition $\dim R \leq 1$ takes a particularly simple form.

The invariant for a zero-dimensional extension of R is a family of ideals $I_{\mathfrak{a}}$ of R indexed by the finitely generated regular ideals $\mathfrak{a}$ of R. We require, for all finitely generated regular ideals $\mathfrak{a}, \mathfrak{b}$ of R, that

- $\mathfrak{a} \subset \operatorname{rad} I_{\mathfrak{a}}$,
- $I_{\mathfrak{a}\mathfrak{b}} = I_{\mathfrak{a}} \cap I_{\mathfrak{b}}$,
- if $\mathfrak{a} \subset \mathfrak{b}$, then $I_{\mathfrak{a}} \subset I_{\mathfrak{b}}$.

For the integers $\mathbf{Z}$, this is equivalent to specifying, for each prime p, an ideal I_p, possibly improper, containing a power of p. Given a zero-dimensional extension S of R, or even just a zero-dimensional R-algebra, the ideal $I_{\mathfrak{a}}$ is the R-annihilator of $1 - e_{\mathfrak{a}} \in S$. Equivalently, it is $R \cap Se_{\mathfrak{a}}$. Here $e_{\mathfrak{a}}$ is the unique idempotent of S such that $e_{\mathfrak{a}} \in \mathfrak{a}S$ and $\mathfrak{a}^n(1 - e_{\mathfrak{a}}) = 0$ for some n (see Section 2).

While the ideals $\mathfrak{a}$ are required to be finitely generated, no such condition is imposed on the ideals $I_{\mathfrak{a}}$. We will show how to construct, from any such family of ideals, a minimal zero-dimensional extension of R with that family as its invariant (Theorem 15).

It might be argued that this invariant is too complicated to give any insight into the minimal zero-dimensional extensions of R, but this is already belied by its transparency in the case $R = \mathbf{Z}$. We describe two other situations in which the invariant becomes fairly simple. The first is $R = k[X]$ where k is any algebraic number field, not necessarily finite dimensional. For example, if P is an arbitrary proposition we

could set $k = \mathbf{Q} \cup \{x \in \mathbf{Q}[i] : P\}$. The invariant in this case is uniquely specified by giving an ideal I_p in $k[X]$, containing some power of p, for each monic irreducible polynomial p in $\mathbf{Q}[X]$. More generally, we may replace $\mathbf{Q}$ by any factorial field (a field over which you can write every nonconstant polynomial as a product of irreducible polynomials).

In the second situation, Chiorescu's Noetherian-spectrum hypothesis holds in a constructively strong form. Here the monoid of finitely generated regular ideals of R, modulo the equivalence $\mathfrak{a} \sim \mathfrak{b}$ if $\operatorname{rad} \mathfrak{a} = \operatorname{rad} \mathfrak{b}$, is naturally identified with the set of finite subsets of the nonzero prime ideals M of R that are radicals of finitely generated ideals (Theorem 17), and the invariant can be specified by giving an ideal I_M in R, containing some power of M, for each such ideal M of R. An example of this situation is the ring of algebraic integers in a finite-dimensional extension of $\mathbf{Q}$.

2. Krull dimension zero. The following lemma is a combination of [**3**, Lemma 1], which references [**2**, Lemma 4.1 and Lemma 2.1]. The proofs there are straightforward and constructive.

Lemma 1. *Let x be an element of a commutative ring R and $n \in \mathbf{N}$. Then the following are equivalent*:

1. $x^n \in Rx^{n+1}$,
2. *There is an idempotent $e \in Rx$ such that $x^n(1-e) = 0$.*
3. *There is an idempotent e such that $Re = Rx^n$.*

An idempotent e satisfies condition 2 *for some n if and only if $x(1-e)$ is nilpotent and $x + 1 - e$ is invertible.*

There is at most one idempotent e satisfying 3 *for some n. We denote this idempotent, if it exists, by e_x and denote $1 - e_x$ by f_x.*

We say that R is *zero dimensional* if for all $x \in R$, there exists $n \in \mathbf{N}$ satisfying the conditions of Lemma 1. Possibly we should say that R is *at most* zero dimensional, reserving dimension -1 for the trivial ring as in [**4**], but I don't think that this distinction will be important here. See [**2**, Theorem 2.2] for a proof that this definition is classically equivalent to the usual one.

If R is a ring with exactly two idempotents, then R is zero dimensional if and only if every element of R is either a unit or nilpotent. To see this, note that the idempotents are 0 and 1, and that $0 \neq 1$. The statement then follows from the fact that $e_x = 1$ if and only if x is a unit, and that $e_x = 0$ if and only if x is nilpotent. As a consequence, the ring $\mathbf{R}$ of real number is zero dimensional if and only if it is *discrete*, that is, if each element of $\mathbf{R}$ were either zero or nonzero, which is one of the traditional omniscience principles that admits no constructive proof. That is not to say that there is no good notion of "zero dimensional" such that $\mathbf{R}$ is zero dimensional from a constructive point of view, but this is not such a notion.

Here are a few observations:

• If R is a discrete integral domain, and K is the quotient field of R, then K is a minimal zero-dimensional extension of R. To see that a discrete field K is zero dimensional, take $n = 1$. Then $0 \in K0^2$ and $x \in Kx^2 = K$ if $x \neq 0$. To see that K is minimal, suppose $K' \subset K$ is a zero-dimensional extension R. If r is a nonzero element of R, then r is cancellable, hence invertible in K', so $K' = K$.

• The homomorphic image of a zero-dimensional ring is zero dimensional, as is the product of a finite number of zero-dimensional rings and the direct limit of zero-dimensional rings. That's because of the logical form, "for all x there exist n and r such that $r : x^n = rx^{n+1}$." In particular, $\mathbf{Q} \times (\mathbf{Z}_n/I)$ is zero dimensional for any ideal I of $\mathbf{Z}_n$. Note that we cannot necessarily say that $\mathbf{Z}_n/I$ is isomorphic to some $\mathbf{Z}_m$–it need not even be discrete.

• The ring $\mathbf{Q} \times (\mathbf{Z}_n/I)$ is a minimal zero-dimensional extension of $\mathbf{Z}$. Suppose A is a zero-dimensional subring of $\mathbf{Q} \times (\mathbf{Z}_n/I)$. Then $(n, 0) \in A$, so $(1/n, k) \in A$ for some k, so $(1, 0) \in A$ whence $(m, 0) \in A$ for all $m \in \mathbf{Z}$. If $m \neq 0$, then $(m, 0) \in A$ so $(1/m, k) \in A$ for some k, so $(1/m, 0) \in A$. Thus $\mathbf{Q} \times \{0\} \subset A$ whence $A = \mathbf{Q} \times (\mathbf{Z}_n/I)$.

• If R is zero dimensional, then every regular element of R is invertible. That's because if x is regular, and $x^n = rx^{n+1}$, then $1 = rx$.

We need to generalize the notion of e_x to ideals. Let R be a commutative ring and S an R-algebra. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of R. Then

1. There is at most one idempotent $e \in A$ such that $\mathfrak{a}(1 - e)$ is nil

and $e \in \mathfrak{a}S$. This idempotent is denoted $e_{\mathfrak{a}}$ and we set $f_{\mathfrak{a}} = 1 - e_{\mathfrak{a}}$.

2. If $\mathfrak{a} = (x_1, \ldots, x_k)$, and each e_{x_i} exists, then $e_{\mathfrak{a}} = e_{x_1} \vee \cdots \vee e_{x_k} = 1 - f_{x_1} \cdots f_{x_k}$.

3. If $e_{\mathfrak{a}}$ and $e_{\mathfrak{b}}$ exist, then $e_{\mathfrak{a}b} = e_{\mathfrak{a}} e_{\mathfrak{b}}$.

4. If $e_{\mathfrak{a}}$ exists, then $e_{\operatorname{rad}\mathfrak{a}} = e_{\mathfrak{a}}$. If $e_{\operatorname{rad}\mathfrak{a}}$ exists, then $e_{\mathfrak{a}} = e_{\operatorname{rad}\mathfrak{a}}$.

These four statements are proven in [**3**] as Theorem 8 and Lemmas 9–11. The proofs are straightforward computations with no constructive problems.

3. The invariant. We will be interested in families of ideals $I_{\mathfrak{a}}$ of R, indexed by a multiplicative monoid M of finitely generated regular ideals $\mathfrak{a}$ of R, such that for all $\mathfrak{a}$ and $\mathfrak{b}$ in M,

1. $\mathfrak{a} \subset \operatorname{rad} I_{\mathfrak{a}}$,

2. $I_{\mathfrak{a}b} = I_{\mathfrak{a}} \cap I_{\mathfrak{b}}$,

3. if $\mathfrak{a} \subset \mathfrak{b}$, then $I_{\mathfrak{a}} \subset I_{\mathfrak{b}}$.

Call such a family *admissible*. We define $\operatorname{rad} I$ to be

$$\{r \in R : r^n \in I \text{ for some positive integer } n\},$$

whence the term "radical," rather than the intersection of all prime ideals containing I. The admissible families will be the invariants for minimal zero-dimensional extensions of appropriate rings R. If $a \in R$ is regular, we set $I_a = I_{Ra}$.

Here are a couple of easy examples of admissible families: Set $I_{\mathfrak{a}} = R$ for each $\mathfrak{a}$. Set $I_{\mathfrak{a}} = \operatorname{rad}\mathfrak{a}$ for each $\mathfrak{a}$.

We say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R are *comaximal* if $\mathfrak{a} + \mathfrak{b} = R$.

Lemma 2. *Let $I_{\mathfrak{a}}$ be an admissible family of ideals of R. If $\operatorname{rad}\mathfrak{a} = \operatorname{rad}\mathfrak{b}$, then $I_{\mathfrak{a}} = I_{\mathfrak{b}}$. If $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal, then $I_{\mathfrak{a}b} = I_{\mathfrak{a}} I_{\mathfrak{b}}$ and*

$$I_{\mathfrak{a}} = \{r \in R : r\mathfrak{b}^n \subset I_{\mathfrak{a}b} \text{ for some } n\}.$$

Proof. For the first claim, note that property 2 implies that $I_{\mathfrak{a}^n} = I_{\mathfrak{a}}$ so if $\mathfrak{a} \subset \operatorname{rad}\mathfrak{b}$, then $\mathfrak{a}^n \subset \mathfrak{b}$ for some n, so $I_{\mathfrak{a}} = I_{\mathfrak{a}^n} \subset I_{\mathfrak{b}}$ by property 3.

Now suppose $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal. Because $\mathfrak{a} \subset \operatorname{rad} I_{\mathfrak{a}}$ and $\mathfrak{b} \subset \operatorname{rad} I_{\mathfrak{b}}$ and $\mathfrak{a} + \mathfrak{b} = R$, it follows that $I_{\mathfrak{a}} + I_{\mathfrak{b}} = R$, hence $I_{\mathfrak{a}} \cap I_{\mathfrak{b}} = I_{\mathfrak{a}} I_{\mathfrak{b}}$. For the second claim, first suppose $r \in I_{\mathfrak{a}}$. Then $r\mathfrak{b}^n \subset I_{\mathfrak{a}} \cap I_{\mathfrak{b}}$ for some n. Conversely, if $r\mathfrak{b}^n \subset I_{\mathfrak{a}b}$ for some n, then $r\mathfrak{b}^n \subset I_{\mathfrak{a}}$ because $I_{\mathfrak{a}b} \subset I_{\mathfrak{a}}$. But $\mathfrak{b}^n$ and $I_{\mathfrak{a}}$ are comaximal, because $\mathfrak{b}$ and $\mathfrak{a}$ are comaximal, so $r \in I_{\mathfrak{a}}$. □

Because $\operatorname{rad} \mathfrak{a} = \operatorname{rad} \mathfrak{b}$ implies $I_{\mathfrak{a}} = I_{\mathfrak{b}}$, we could take the index set of an admissible family to be ideals that are radicals of finitely generated ideals. The second condition would more naturally be written as $I_{\mathfrak{a}\cap\mathfrak{b}} = I_{\mathfrak{a}} \cap I_{\mathfrak{b}}$. The ideal $\mathfrak{a} \cap \mathfrak{b}$ is of the right kind because if $\mathfrak{a} = \operatorname{rad} \mathfrak{a}'$ and $\mathfrak{b} = \operatorname{rad} \mathfrak{b}'$, then $\mathfrak{a} \cap \mathfrak{b} = \operatorname{rad} \mathfrak{a}'\mathfrak{b}'$. The third condition would then follow from the second. So an admissible family is simply a monoid homomorphism from a monoid of radicals of finitely generated regular ideals to the monoid of all ideals, subject to the condition $\mathfrak{a} \subset \operatorname{rad} I_{\mathfrak{a}}$, the binary operation in each monoid being intersection.

The following lemma shows why we are interested in admissible families.

Lemma 3. *Let S be a zero-dimensional extension R. For each finitely generated regular ideal $\mathfrak{a}$ of R, define $I_{\mathfrak{a}} = \operatorname{ann}_R f_{\mathfrak{a}}$. Then the family of ideals $I_{\mathfrak{a}}$ is admissible. Moreover, if $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal, then $f_{\mathfrak{a}}$ and $f_{\mathfrak{b}}$ are orthogonal idempotents.*

Proof. The first property of admissibility follows from the fact that $\mathfrak{a} f_{\mathfrak{a}}$ is nil. For the second property, note that if $r f_{\mathfrak{a}b} = 0$, then $r(1 - e_{\mathfrak{a}} e_{\mathfrak{b}}) = 0$, so $r \in Re_{\mathfrak{a}}$. Therefore $r = re_{\mathfrak{a}}$ whence $rf_{\mathfrak{a}} = 0$. Similarly for $f_{\mathfrak{b}}$, so $I_{\mathfrak{a}b} \subset I_{\mathfrak{a}} \cap I_{\mathfrak{b}}$. Conversely, suppose that $rf_{\mathfrak{a}} = 0 = rf_{\mathfrak{b}}$. Then $r = re_{\mathfrak{a}}$ and $r = re_{\mathfrak{b}} = re_{\mathfrak{a}} e_{\mathfrak{b}} = re_{\mathfrak{a}b}$. For the third property, if $\mathfrak{a} = (x_1, x_2, \dots, x_m)$ and $\mathfrak{b} = (x_1, x_2, \dots, x_n)$, with $m \leq n$, then

$$f_{\mathfrak{a}} = \prod_{i=1}^{m} f_{x_i} \text{ is a factor of } f_{\mathfrak{b}} = \prod_{i=1}^{n} f_{x_i}.$$

For the last claim, we know that $I_{\mathfrak{a}}$ and $I_{\mathfrak{b}}$ are comaximal and are both contained in $\operatorname{ann}_R f_{\mathfrak{a}} f_{\mathfrak{b}}$. It follows that $\operatorname{ann}_R f_{\mathfrak{a}} f_{\mathfrak{b}} = R$ so $f_{\mathfrak{a}} f_{\mathfrak{b}} = 0$. □

For suitable rings, we will show that every admissible family arises from a minimal zero-dimensional extension (Theorem 15), and that this family characterizes those minimal zero-dimensional extensions up to isomorphism (Theorem 16).

4. The lattice $L(R)$. Let R be any commutative ring. We are interested in the lattice of radical ideals. The elements of this lattice are ideals of R and the preorder is given by $\mathfrak{a} \leq \mathfrak{b}$ if $\operatorname{rad}\mathfrak{b} \subset \operatorname{rad}\mathfrak{a}$. Perhaps this preorder seems back-to-front, but I'm motivated partly by the aphorism that "to contain is to divide," and I would also like relatively prime elements to be disjoint in the lattice. This preorder induces an equivalence relation which we will denote by $\mathfrak{a} \sim \mathfrak{b}$ when we don't want it to be confused with equality of sets. Of course we could restrict our attention to radical ideals, but it is often more convenient to consider all ideals together with the equivalence relation.

The lattice operations are given by $\mathfrak{a} \vee \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ and $\mathfrak{a} \wedge \mathfrak{b} = \mathfrak{a} + \mathfrak{b}$. Note that we could as well define $\mathfrak{a} \vee \mathfrak{b}$ to be the equivalent ideal $\mathfrak{a} \cap \mathfrak{b}$, but $\mathfrak{a}\mathfrak{b}$ has the virtue of being finitely generated if $\mathfrak{a}$ and $\mathfrak{b}$ are. Moreover, multiplication of ideals distributes over addition, so this makes it immediately apparent that the lattice is distributive. The bottom element of the lattice is the improper ideal R. The top element is the zero ideal, but we will normally restrict ourselves to regular ideals.

In a distributive lattice with a bottom element 0, the *relative complement* $a \setminus b$ is defined to be that element c, if it exists, such that $c \wedge b = 0$ and $c \vee (b \wedge a) = a$. Note that $c \vee (b \wedge a) = a$ is equivalent to $c \leq a$ and $c \vee b \geq a$. That the relative complement is unique is easily seen by forming the meet of c' with $a = c \vee (b \wedge a)$.

The finitely generated regular ideals of R form a sublattice $L(R)$. A *regular ideal* is one that contains a *regular element*—an element that is cancellable under multiplication. It is this lattice that we will be concerned with. The lattice $L(\mathbf{Z})$ is naturally isomorphic to the lattice of finite subsets of the primes, so is a relatively complemented distributive lattice. That's a good thing for our purposes. This is also true for $L(R)$ when $R = k[X]$ where k is a (discrete) field. Classically the reason is the same as for $L(\mathbf{Z})$, but constructively we cannot assume that every nonconstant polynomial is a product of irreducible polynomials. However, it is still true that every finitely generated

regular ideal is generated by a nonzero polynomial, and if f and g are nonzero polynomials, then, in the lattice $L(R)$, the relative complement $Rf \setminus Rg$ is generated by $f/\gcd(f, g^{\deg f})$.

If $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ are finitely generated regular ideals of R, then $\mathfrak{c} = \mathfrak{a} \setminus \mathfrak{b}$ in the lattice $L(R)$ exactly when $\mathfrak{a} \sim \mathfrak{c}(\mathfrak{a} + \mathfrak{b})$ and $\mathfrak{b} + \mathfrak{c} = R$.

We will focus on commutative rings R with *detachable nilradical*, that is, for each $x \in R$, either x is nilpotent or it is not. We will say that 0 *is a primary ideal* of R if every nonnilpotent element of R is regular. This agrees with the classical definition. The two conditions imply that every element of R is either nilpotent or regular. The converse is true for nontrivial rings (and for trivial ones). In fact, the two conditions are equivalent to the two conditions

(1) every element of R is either nilpotent or regular, and

(2) R is either trivial or nontrivial.

Notice that any discrete integral domain satisfies these two conditions. By "discrete," I mean that each x in R is either zero or nonzero. Actually, I'm not quite sure what an integral domain is in the general constructive context except that it probably should be the same as a subring of a field. But then, I'm not quite sure what a field should be, other than a discrete field.

We are interested in the conditions that $\dim R \leq 1$ and $\dim T(R) = 0$ where $T(R)$ is the total ring of quotients of R.

What do we mean by $\dim R \leq 1$? As in [**5**] we define, for each $x \in R$, the ideal

$$N(x) = Rx + \bigcup_{n \in \mathbf{N}} (0 : x^n)_R .$$

Then $\dim R \leq 1$ exactly when $\dim R/N(x) = 0$ for all $x \in R$. This is equivalent, classically, with the usual definition in terms of prime ideals. If 0 is a primary ideal, and R has a detachable nilradical, then $(0 : x^n) = 0$ unless x is nilpotent, in which case $N(x) = R$. So $\dim R \leq 1$ if and only if $\dim R/Rx = 0$ whenever $x \in R$ is not nilpotent. We might also note that $\dim R = 0$ if and only if $R/N(x) = 0$ for all x in R.

Lemma 4. *If every element of R is either nilpotent or regular, then* $\dim T(R) = 0$.

Proof. Given $x \in R$, we must find $n \in \mathbf{N}$, a regular element $s \in R$ and an element $t \in R$ such that $sx^n = tx^{n+1}$. If x is nilpotent, take n so that $x^n = 0$ and $s = t = 1$. If x is regular, take $s = x$ and $t = 1$. □

The following lemma relates relative complements of finitely generated ideals to relative complements of principal ideals.

Lemma 5. *Let L be a distributive lattice with least element 0. Let S be a subset of L and M the set of finite meets of elements of S. If any two elements of S have a relative complement in L, then any two elements of M have a relative complement in L.*

Proof. We will show that if $a, b, c \in L$, then

$$(a \wedge b) \setminus c = (a \setminus c) \wedge (b \setminus c)$$
$$c \setminus (a \wedge b) = (c \setminus a) \vee (c \setminus b)$$

in the sense that, if the right side exists, then so does the left. The lemma then follows by induction on the number of meets in the expressions for the two elements of M. We have

$$\begin{aligned}
(a \setminus c) \wedge (b \setminus c) \wedge c &= (a \setminus c) \wedge 0 = 0 \\
((a \setminus c) \wedge (b \setminus c)) \vee c &= (((a \setminus c) \vee c) \wedge ((b \setminus c) \vee c)) \geq a \wedge b \\
((c \setminus a) \vee (c \setminus b)) \wedge (a \wedge b) &= ((c \setminus a) \wedge (a \wedge b)) \vee ((c \setminus b) \wedge (a \wedge b)) \\
&= 0 \\
((c \setminus a) \vee (c \setminus b)) \vee (a \wedge b) &= (((c \setminus a) \vee (c \setminus b)) \vee a) \\
&\quad \wedge (((c \setminus a) \vee (c \setminus b)) \vee b) \\
&\geq c \wedge c = c \qquad \square
\end{aligned}$$

It turns out that the existence of relative complements in $L(R)$ is intimately related to the dimension of R.

Theorem 6. *Let R be a ring in which every element is either regular or nilpotent. Then the following are equivalent:*

1. $\dim R \leq 1$.

2. *For all regular $x, y \in R$ there exist (finitely generated) ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{b}', \mathfrak{c}$ of R such that*

(a) $Rx = \mathfrak{a}\mathfrak{b}$ and $Ry = \mathfrak{b}'\mathfrak{c}$,

(b) $\mathfrak{a} + Ry = R = \mathfrak{c} + Rx$,

(c) $\mathfrak{b} \sim \mathfrak{b}'$.

3. *The lattice $L(R)$ is relatively complemented.*

Proof. Condition 2 implies that principal ideals of R have relative complements in $L(R)$ because $Rx \setminus Ry = \mathfrak{a}$. So 3 holds by Lemma 5. Suppose 3 holds. We will show that if $x \in R$ is regular, then $\dim R/Rx = 0$. That is, we will show that if $y \in R$, then there is a positive integer n, and an element $r \in R$, such that x divides $y^n - ry^{n+1} = y^n(1 - ry)$. If y is nilpotent, that's clear. Otherwise, $Rx = \mathfrak{a}\mathfrak{b}$ and $Ry = \mathfrak{b}'\mathfrak{c}$ as in 2. First note that, because $\mathfrak{a} + Ry = R$, there exists $r \in R$ so that $1 - ry \in \mathfrak{a}$. Then, because $\mathfrak{b} \sim \mathfrak{b}'$, there is a positive integer n such that $y^n \in \mathfrak{b}$. So $y^n(1 - ry)$ is in $\mathfrak{a}\mathfrak{b}$, hence is divisible by x.

Finally suppose $\dim R \leq 1$ and let $x, y \in R$ be regular. There is a positive integer n and elements $r, s \in R$ such that x divides $y^n(1 - ry)$ and y divides $x^n(1 - sx)$. Let $\mathfrak{a} = (x, 1 - ry)$ and $\mathfrak{b} = (x, y^n)$. Note that $(1 - ry, y^n) = R$. Similarly let $\mathfrak{c} = (y, 1 - sx)$ and $\mathfrak{b}' = (y, x^n)$. □

If k is a discrete field, and x is a nonzero element of $R = k[X]$, then $R/(x)$ is a finite dimensional vector space over k, hence zero dimensional. Thus $\dim R \leq 1$, so the lattice $L(R)$ is relatively complemented by Theorem 6. One can compute the relative complements directly by repeatedly taking gcd's and eliminating duplicate factors.

In reference to the equivalence of 1 and 3 of Theorem 6, Joyal showed that $\dim R$ can be read from the Zariski lattice of R, which in this case is essentially $L(R)$, see [**6**].

For convenience, we will call a commutative ring R *suitable* if it has a detachable nilradical and a primary zero-ideal, and $\dim R \leq 1$.

Theorem 7. *Let L be a relatively complemented distributive lattice. If $x_1, \ldots, x_m$ are elements of L, then there exist disjoint elements $a_1, \ldots, a_n$ of L such that each x is the join of some of the a's. If $m = 2$,*

then we can take $n = 3$ *and write* $x_1 = a_1 \vee a_2$, *and* $x_2 = a_2 \vee a_3$ *where* $a_2 = x_1 \wedge x_2$.

Proof. Induction on m. If $m = 1$, take $n = 1$ and $a_1 = m_1$. Suppose $m > 1$ and $a_1, \ldots, a_n$ works for $x_1, \ldots, x_{m-1}$. Replace the a's by $x_m \wedge a_i$ and $a_i \setminus x_m$, for $i = 1, \ldots, n$, and throw in $x_m \setminus \bigvee_{j=1}^n a_j$. These are clearly disjoint, and since $a_i = (x_m \wedge a_i) \vee (a_i \setminus x_m)$, and $x_m = (x_m \setminus \bigvee_{j=1}^n a_j) \vee \bigvee_{j=1}^n a_j \wedge x_m$, each x is the join of some of them. Note that for $m = 2$, we replace x_1 by $x_2 \wedge x_1$ and $x_1 \setminus x_2$, and throw in $x_2 \setminus x_1$, which gives us the last claim. □

Take L to be $L(R)$ and look at the idempotents $f_{\mathfrak{a}_1}, \ldots, f_{\mathfrak{a}_m}$ in some minimal zero-dimensional extension. It follows from the theorem that we can construct finitely generated regular ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ that are pairwise comaximal so that each $f_{\mathfrak{a}_i}$ is a sum of some of the $f_{\mathfrak{b}_i}$.

Corollary 8. *If* R *is a suitable ring, then for any finitely generated regular ideals* $\mathfrak{s}$ *and* $\mathfrak{t}$ *of* R, *there exist pairwise comaximal finitely generated regular ideals* $\mathfrak{a}$, $\mathfrak{b}$, *and* $\mathfrak{c}$, *such that* $\mathfrak{s} \sim \mathfrak{ab}$ *and* $\mathfrak{t} \sim \mathfrak{bc}$.

Corollary 9. *If* R *is a suitable ring, then, for a fixed positive integer* n, *the family* $I_{\mathfrak{a}} = (\operatorname{rad} \mathfrak{a})^n$ *is admissible.*

Proof. The only problem is showing that $(\operatorname{rad} \mathfrak{s}t)^n = (\operatorname{rad} \mathfrak{s})^n \cap (\operatorname{rad} \mathfrak{t})^n$. This is always true for $n = 1$. If $\mathfrak{s}$ and $\mathfrak{t}$ are comaximal, then $(\operatorname{rad} \mathfrak{st})^n = (\operatorname{rad} \mathfrak{s} \cdot \operatorname{rad} \mathfrak{t})^n = (\operatorname{rad} \mathfrak{s})^n (\operatorname{rad} \mathfrak{t})^n = (\operatorname{rad} \mathfrak{s})^n \cap (\operatorname{rad} \mathfrak{t})^n$. For the general case, write $\mathfrak{s} \sim \mathfrak{ab}$ and $\mathfrak{t} \sim \mathfrak{bc}$ as in the previous corollary. Then $(\operatorname{rad} \mathfrak{s})^n = (\operatorname{rad} \mathfrak{a})^n \cap (\operatorname{rad} \mathfrak{b})^n$ and $(\operatorname{rad} \mathfrak{t})^n = (\operatorname{rad} \mathfrak{b})^n \cap (\operatorname{rad} \mathfrak{c})^n$, while $\operatorname{rad} \mathfrak{st} = \operatorname{rad} \mathfrak{a} \cap \operatorname{rad} \mathfrak{b} \cap \operatorname{rad} \mathfrak{c} = \operatorname{rad} \mathfrak{a} \cdot \operatorname{rad} \mathfrak{b} \cdot \operatorname{rad} \mathfrak{c}$, so

$$\begin{aligned}(\operatorname{rad} \mathfrak{st})^n &= (\operatorname{rad} \mathfrak{a})^n (\operatorname{rad} \mathfrak{b})^n (\operatorname{rad} \mathfrak{c})^n \\ &= (\operatorname{rad} \mathfrak{a})^n \cap (\operatorname{rad} \mathfrak{b})^n \cap (\operatorname{rad} \mathfrak{c})^n \\ &= ((\operatorname{rad} \mathfrak{a})^n \cap (\operatorname{rad} \mathfrak{b})^n) \cap ((\operatorname{rad} \mathfrak{b})^n \cap (\operatorname{rad} \mathfrak{c})^n) \\ &= (\operatorname{rad} \mathfrak{s})^n \cap (\operatorname{rad} \mathfrak{t})^n . \qquad \square\end{aligned}$$

Suppose R is the ring $\mathbf{Z}$ of integers in Corollary 9. The minimal zero-dimensional extension of $\mathbf{Z}$ corresponding to this family can be thought

of as follows. It is the subring of the product of $\mathbf{Z}/p^n\mathbf{Z}$ over all primes p consisting of those sequences that are eventually constant as rational numbers. The idempotent f_p is the binary sequence whose unique 1 is at p.

5. Extending admissible families. We will refer to the following extension theorem in two different contexts.

Theorem 10. *Let R be a suitable ring. Let V be a join subsemilattice of $L(R)$ such that for all $\mathfrak{a} \in L(R)$ there exists $\mathfrak{u} \in V$ such that $\mathfrak{a} \leq \mathfrak{u}$. Let $(I_\mathfrak{u})_{\mathfrak{u}\in V}$ be an admissible family on V such that if $\mathfrak{v}, \mathfrak{v}' \in V$, and $\mathfrak{v}' = \mathfrak{v} \vee \mathfrak{c}$ and $\mathfrak{v} \wedge \mathfrak{c} = 0$, then*

$$I_\mathfrak{v} = \{r \in R : r\mathfrak{c}^n \subset I_{\mathfrak{v}'} \quad \text{for some } n\}.$$

Then $(I_\mathfrak{u})_{\mathfrak{u}\in V}$ can be extended uniquely to an admissible family on $L(R)$.

Proof. For $\mathfrak{a} \in L(R)$, choose $\mathfrak{v} \in V$ such that $\mathfrak{a} \leq \mathfrak{v}$. As $L(R)$ is relatively complemented, there exists $\mathfrak{b} \in L(R)$ such that $\mathfrak{v} = \mathfrak{a} \vee \mathfrak{b}$, and $\mathfrak{a} \wedge \mathfrak{b} = 0$. Set

$$I_\mathfrak{a} = \{r \in R : r\mathfrak{b}^n \subset I_\mathfrak{v} \text{ for some positive integer } n\}.$$

From Lemma 2 there is no other way to define $I_\mathfrak{a}$, so it's unique. It remains to show that this is a well-defined admissible family. Note that the definition of $I_\mathfrak{a}$ depends only on the equivalence class of $\mathfrak{b}$ in $L(R)$.

To show that $I_\mathfrak{a}$ well defined, we need to show we get the same result for $I_\mathfrak{a}$ if we take $\mathfrak{v}' \geq \mathfrak{a}$. Since V is a join subsemilattice, we may assume $\mathfrak{v}' \geq \mathfrak{v}$. Write $\mathfrak{v}' = \mathfrak{v} \vee \mathfrak{c}$ with $\mathfrak{v} \wedge \mathfrak{c} = 0$. Then $\mathfrak{v}' = \mathfrak{a} \vee \mathfrak{b} \vee \mathfrak{c}$ and the definition of $I_\mathfrak{a}$ using $\mathfrak{v}'$ is

$$I'_\mathfrak{a} = \{r \in R : r\mathfrak{b}^n\mathfrak{c}^n \subset I_{\mathfrak{v}'} \text{ for some positive integer } n\}.$$

To see that $I'_\mathfrak{a} \subset I_\mathfrak{a}$, note that if $r\mathfrak{b}^n\mathfrak{c}^n \subset I_{\mathfrak{v}'}$, then $r\mathfrak{b}^n \subset I_\mathfrak{v}$ because $I_{\mathfrak{v}'} \subset I_\mathfrak{v}$, so $r\mathfrak{b}^n\mathfrak{c}^n \subset I_\mathfrak{v}$ and $\mathfrak{c}^n + I_\mathfrak{v} = R$. To show that $I_\mathfrak{a} \subset I'_\mathfrak{a}$ we need to use the displayed hypothesis of the theorem. Suppose $r \in I_\mathfrak{v}$ so

$$r\mathfrak{b}^n \subset I_\mathfrak{v} = \{r \in R : r\mathfrak{c}^m \subset I_{\mathfrak{v}'} \text{ for some } m\}.$$

Thus $r\mathfrak{b}^n\mathfrak{c}^m \subset I_{\mathfrak{v}'}$. We may assume $m = n$, whence $r \in I'_{\mathfrak{a}}$.

Finally, we must show that this defines an admissible family. Suppose we are given $\mathfrak{s}, \mathfrak{t} \in L(R)$. Choose $\mathfrak{v} \in V$ such that $\mathfrak{s} \vee \mathfrak{t} \leq \mathfrak{v}$. Write $\mathfrak{v} = \mathfrak{s} \vee \mathfrak{a} = \mathfrak{t} \vee \mathfrak{b}$ where $\mathfrak{s} \wedge \mathfrak{a} = \mathfrak{t} \wedge \mathfrak{b} = 0$. It follows that $\mathfrak{v} = \mathfrak{s} \vee \mathfrak{t} \vee (\mathfrak{a} \wedge \mathfrak{b})$ and $(\mathfrak{s} \vee \mathfrak{t}) \wedge (\mathfrak{a} \wedge \mathfrak{b}) = 0$. So

$$\begin{aligned} I_{\mathfrak{st}} &= \{r \in R : r\,(\mathfrak{a} + \mathfrak{b})^n \subset I_{\mathfrak{v}} \text{ for some positive integer } n\} \\ I_{\mathfrak{s}} &= \{r \in R : r\mathfrak{a}^n \subset I_{\mathfrak{v}} \text{ for some positive integer } n\} \\ I_{\mathfrak{t}} &= \{r \in R : r\mathfrak{b}^n \subset I_{\mathfrak{v}} \text{ for some positive integer } n\}\,. \end{aligned}$$

Clearly $I_{\mathfrak{st}} = I_{\mathfrak{s}} \cap I_{\mathfrak{t}}$ (we might have to take the n bigger in $I_{\mathfrak{st}}$). □

Note that if there is an extension of $(I_{\mathfrak{u}})_{\mathfrak{u} \in V}$ from V to $L(R)$, then the displayed hypothesis of the theorem must hold because of Lemma 2.

6. Algebraic extensions of factorial fields. Lemma 2 enables us to give a pleasing description of the admissible families when $R = F[X]$ for F a field of algebraic numbers. In fact, we can do this for any field that is algebraic over a factorial field. By a *factorial field*, we mean a field over which every polynomial of degree greater than zero is a product of irreducible polynomials (see [**7**, VII.1]). Kronecker showed that $\mathbf{Q}$ is a factorial field although Knuth says that Schubert did it a hundred years earlier.

Lemma 11. *Let k be a commutative ring, F an integral extension of k, and h a monic polynomial in $F[X]$. Then h divides a monic polynomial in $k[X]$.*

Proof. For an indeterminate Y, consider the ring $R = F[Y]/(h(Y))$ which is an integral extension of F which, in turn, is an integral extension of k. So R is an integral extension of k [**7**, VI Corollary 1.5]. Thus the image of Y in R satisfies a monic polynomial over k. By the construction of R, this polynomial must be divisible by h. □

Theorem 12. *Let k be a discrete field and F an algebraic extension of k. Suppose for each nonzero polynomial $q \in k[X]$ we are given an ideal I_q of $F[X]$ so that the family $(I_q)_{q \in k[X] \setminus \{0\}}$ is admissible. Then*

this family can be extended uniquely to a family $(I_p)_{p\in F[X]\setminus\{0\}}$ *that is admissible.*

Proof. We prove this by appealing to Theorem 10. First we need to show that every monic polynomial in $F[X]$ divides a monic polynomial in $k[X]$, but this follows from Lemma 11. Next suppose x and y are in $k[X]$ and c is monic in $F[X]$. If $y = x \vee c$ and $x \wedge c = 0$, we will show that c is equivalent in $L(F[X])$ to an element of $k[X]$. The discussion following Theorem 6 shows that both $L(k[X])$ and $L(F[X])$ are relatively complemented, so x has a complement c' in y that lies in $L(k[X])$. By uniqueness of the relative complement, c' is equivalent to c in $L(F[X])$. Lemma 2 now says that the hypothesis of Theorem 10 is satisfied. □

The point here is that admissible families of ideals in $F[X]$, indexed by the ring $k[X]$, are specified by giving an ideal I_p in $F[X]$, containing some power of p, for each monic irreducible polynomial $p \in k[X]$. So it is fairly transparent what the admissible families $(I_p)_{p\in F[X]\setminus\{0\}}$ of ideals in $F[X]$ are.

A related question concerns whether for an arbitrary suitable ring, it suffices to look at admissible families indexed by the principal regular ideals. The question is whether these admissible families can be extended, and the answer to that question depends on whether such families automatically satisfy the hypothesis of Theorem 10. Note that this is a question with nontrivial classical content. I would guess that the answer is "no," but I don't have a counterexample.

7. Arapović's theorem. By *the total quotient ring of* $R[E]$ *within* S we mean the set of elements of the form $t/s \in S$ where $s, t \in R[E]$ and s is invertible in S. The following is [**3**, Theorem 4]:

Theorem 13. *Let* S *be an* R*-algebra such that* e_x *is defined in* S *for every* $x \in R$*. Let* $E = \{e_x \in S : x \in R\}$*. Then* e_x *is defined in* S*, and is in* $R[E]$*, for every* $x \in R[E]$*, and every regular element of* $R[E]$ *is invertible in* S*. It follows that the total quotient ring of* $R[E]$ *within* S *is the same as the total quotient ring* $T(R[E])$ *of* $R[E]$*.*

Proof. I'll sketch the proof from [**3**], which is constructive as it stands, but not completely straightforward. Each element of $R[E]$ can be written as $x = \sum r_i g_i$ where $r_i \in R$ and the g_i are orthogonal idempotents in the Boolean algebra generated by E (which is contained in $R[E]$). Note that from a constructive point of view we may not be able to tell whether or not a given g_i is zero, and several of them might be. Then we form $e = \sum e_{r_i} g_i \in R[E]$ and show that it satisfies the defining conditions for e_x. The key observation is that

$$x\,(1-e) = \sum r_i\,(1-e_{r_i})\,g_i$$

is nilpotent because $r_i(1-e_{r_i})$ is nilpotent and the g_i are orthogonal, and that $e_{r_i} g_i \in S r_i g_i$ so $e \in Sx$. If x is regular in $R[E]$, then, because $x(1-e)$ is nilpotent, we get $e = 1$ so $1 \in Sx$, that is, x is invertible in S. □

Arapović's theorem [**1**, Theorem 7], characterizing minimal zero-dimensional R-algebras, as stated in [**3**, Theorem 6], is:

Theorem 14 (Arapović). *Let R be a ring and S an R-algebra such that e_x is defined in S for each $x \in R$. Let $E = \{e_x \in S : x \in R\}$. Then the total quotient ring T' of $R[E]$ within S is the minimal zero-dimensional R-algebra within S.*

Proof. The proof of Arapović's theorem in [**3**, Theorem 6] goes as follows. Theorem 13 says that the regular elements of $R[E]$ are invertible in S. Then we observe that T' is contained in any zero-dimensional R-subalgebra of S because such a ring must be a total quotient ring and must contain $R[E]$ because of the uniqueness of the idempotents e_x. If $x \in T'$, then $x = a/b$ where $a, b \in R[E]$ and b is regular in $R[E]$. Theorem 13 says that e_a is defined in S and is in $R[E] \subset T'$. To see that e_a is defined in T', we note that since e_a is defined in S, Lemma 1 says that $a(1-e_a)$ is nilpotent and $a + 1 - e_a \in R[E]$ is invertible in S, hence in T'. Since b is regular in $R[E]$, it is invertible in T', so $e_b = 1$. Thus $e_x = e_{a/b} = e_a$ is defined in T' for every $x \in T'$, so T' is zero dimensional. □

8. The main theorem for suitable rings. Let L be a relatively complemented lattice. Consider the set D of finitely enumerable subsets

of L consisting of pairwise disjoint elements. If α and β are such subsets, set $\alpha \le \beta$ if each element of α is a join of some elements of β. This gives a partial preorder on D that is directed upwards. Note that if $\{a_1, \dots, a_n\} \in D$, and $\bigvee_{i\in I} a_i = \bigvee_{j\in J} a_j$ for some finite subsets I and J of $\{1, \dots, n\}$, then $a_k = 0$ for each $k \in (I \setminus J) \cup (J \setminus I)$. It follows that if $\alpha \le \beta$ and $\beta \le \alpha$, then $\alpha = \beta$.

Following Jacobson, by an *rng* we mean a ring that doesn't necessarily have an identity element. Note that a rng-homomorphism of rings need not take the identity to the identity. A key element of the construction of a minimal zero-dimensional extension of R is the formation of the ring U^* from a rng U by adjoining an identity. Actually, the rng U will have a compatible R-module structure, and the ring U^* is formed from the R-module $R \oplus U$ by setting $(r, u)(r', u') = (rr', ru' + r'u + uu')$.

If U is a ring, that is, if U has an identity, then U^* is naturally isomorphic to $R \times U$ under the map taking $(r, u) \in U^*$ to $(r, u + r \cdot 1) \in R \times U$. So if U is a ring of dimension zero, then $(r, u) \in U^*$ is regular if and only if r is regular and $u + r \cdot 1$ is invertible in U. Let U and V be rings with $\dim U = 0$. Then any rng map $U \to V$ induces a ring map $U^* \to V^*$ that takes regular elements to regular elements, thus inducing a map $T(U^*) \to T(V^*)$.

We have set the stage for the *main construction*. Given a suitable ring R and an admissible family $(I_{\mathfrak{a}})_{\mathfrak{a}\in L(R)}$ of ideals of R, we will construct a ring $S = \mathcal{F}((I_{\mathfrak{a}})_{\mathfrak{a}\in L(R)})$. Let D be the set of finitely enumerable subsets of $L(R)$ consisting of pairwise disjoint elements. For $\alpha = (\mathfrak{a}_1, \dots, \mathfrak{a}_m) \in D$, let U_α be the ring $\bigoplus_{i=1}^m R/I_{\mathfrak{a}_i}$. If $\alpha \le \beta = (\mathfrak{b}_1, \dots, \mathfrak{b}_n)$, then each $\mathfrak{a}_i$ is a join of elements of β, so $\mathfrak{a}_i \sim \prod_{j\in K_i} \mathfrak{b}_j$ whence $I_{\mathfrak{a}_i} = \bigcap_{j\in K_i} I_{\mathfrak{b}_j}$ so $R/I_{\mathfrak{a}_i}$ is naturally isomorphic to $\bigoplus_{j\in K_i} R/I_{\mathfrak{b}_i}$. If $j \in K_i \cap K_{i'}$, and $i \ne i'$, then $I_{\mathfrak{b}_j} = R$, so we may assume that the sets K_i are disjoint. We define a map from U_α to U_β by taking $R/I_{\mathfrak{a}_i}$ to $\bigoplus_{j\in K_i} R/I_{\mathfrak{b}_j}$ via the natural isomorphism. Because the K_i are disjoint, this map is one-to-one. We then set U equal to the direct limit of $(U_\alpha)_{\alpha\in D}$, and set $S = T(U^*)$. Note that U^* is the direct limit of $(U_\alpha^*)_{a\in D}$ and S is the direct limit of $(T(U_\alpha^*))_{\alpha\in D}$.

We can think of U as the free R-module on the symbols $1_{\mathfrak{a}}$, for $\mathfrak{a} \in L(R)$, modulo the conditions

- $\operatorname{ann}_R 1_{\mathfrak{a}} = I_{\mathfrak{a}}$
- $1_{\mathfrak{a}} 1_{\mathfrak{b}} = 1_{\mathfrak{a}\wedge\mathfrak{b}}$

- $1_{\mathfrak{a}} = 1_{\mathfrak{b}} + 1_{\mathfrak{c}}$ if $\mathfrak{a} = \mathfrak{b} \vee \mathfrak{c}$ and $\mathfrak{b} \wedge \mathfrak{c} = 0$.

Recall that $0 \in L(R)$ is represented by the ideal R, and that $I_R = R$, so $1_0 = 0$. The third condition gives a test for equality in U (which doesn't mean that U is discrete). Together with Theorem 7 it says that we can write any two elements u and v of U as $u = \sum r_i 1_{\mathfrak{a}_i}$ and $v = \sum s_i 1_{\mathfrak{a}_i}$ where the $\mathfrak{a}_i$ is pairwise disjoint, so $u = v$ exactly when $r_i - s_i \in I_{\mathfrak{a}_i}$ for each i. Of course we have to check that this test (or *definition* of equality, if you will) does not depend on the choice of the $\mathfrak{a}_i$.

Theorem 15. *If R is a suitable ring, and $(I_{\mathfrak{a}})_{\mathfrak{a} \in L(R)}$ is an admissible system of ideals of R, then $S = \mathcal{F}((I_{\mathfrak{a}})_{\mathfrak{a} \in L(R)})$ is a minimal zero-dimensional extension of R such that $I_{\mathfrak{a}} = \operatorname{ann}_R f_{\mathfrak{a}}$ for each $\mathfrak{a} \in L(R)$.*

Proof. Because S is a direct limit of zero-dimensional rings $T(U^*_\alpha)$, it is zero dimensional. We will show that the idempotent $f_{\mathfrak{a}}$ of S is equal to $1_{\mathfrak{a}}$, the identity in $R/I_{\mathfrak{a}}$, so $\operatorname{ann}_R f_{\mathfrak{a}} = I_{\mathfrak{a}}$. Clearly $\mathfrak{a}1_{\mathfrak{a}}$ is nil. We must show that $1 - 1_{\mathfrak{a}} \in \mathfrak{a}S = \mathfrak{a}T(U^*)$. It suffices to show that $1 - 1_{\mathfrak{a}} \in \mathfrak{a}T(U^*_{\{\mathfrak{a}\}})$. But $T(U^*_{\{\mathfrak{a}\}}) = T(R) \times U_{\{\mathfrak{a}\}}$ and $\mathfrak{a}T(R) = T(R)$ because $\mathfrak{a}$ is regular, so $\mathfrak{a}^n(T(R) \times U_{\{\mathfrak{a}\}}) = T(R)$ for some n. But $1 - 1_{\mathfrak{a}} \in T(R)$.

Finally, we need to show that S is a *minimal* zero dimensional extension of R. Let $E = \{e_x \in S : x \in R\}$. Arapović's theorem says that the total quotient ring of $R[E]$ within S is a minimal zero-dimensional extension of R. But $e_x = 1 - 1_x$, if x is regular, so $U^* = R[E]$. Thus S itself is a minimal zero-dimensional extension of R. □

That's the existence theorem. The uniqueness theorem is the following.

Theorem 16. *If S and S' are minimal zero-dimensional extensions of a suitable ring R, and $\operatorname{ann}_R f_{\mathfrak{a}} = \operatorname{ann}_R f'_{\mathfrak{a}}$ for all $\mathfrak{a} \in L(R)$, then S is isomorphic to S'.*

Proof. Let D be the set of finitely enumerable subsets of $L(R)$ consisting of pairwise disjoint elements. For $\alpha \in D$ we let $f_\alpha = \{f_{\mathfrak{a}} \in S : \mathfrak{a} \in \alpha\}$. Three observations: First, we cannot necessarily say, for

$\mathfrak{a} \in \alpha$, that $f_\mathfrak{a} = 0$ or $f_\mathfrak{a} \neq 0$. Second, the elements of f_α are mutually orthogonal idempotents. Third, if $\alpha \leq \beta$, then every element of f_α is a sum of elements of f_β (with distinct indices).

Let $E = \{e_x \in S : x \in R\}$ as in Arapović's theorem. For each $\mathfrak{a} \in L(R)$ we have $f_\mathfrak{a} \in R[E]$. So the union U over $\alpha \in D$ of $R[f_\alpha]$ is contained in $R[E]$. There is a natural isomorphism φ_α of the rings $R[f_\alpha]$ and $R[f'_\alpha]$ that takes $f_\mathfrak{a}$ to $f'_\mathfrak{a}$ because $\operatorname{ann}_R f_\mathfrak{a} = \operatorname{ann}_R f'_\mathfrak{a}$ for all $\mathfrak{a} \in L(R)$. Moreover, if $\alpha \leq \beta$, then the restriction of φ_β to $R[f_\alpha]$ is φ_β. Thus we get a rng-isomorphism $\varphi : U \to U'$. It follows that U^* and U'^* are isomorphic rings.

We want to show that $R[E] = U^*$, that is, that each element of $R[E]$ can be written uniquely as $r + u$ where $r \in R$ and $u \in U$. To show existence, note that $x \in R$ is either nilpotent or regular, so either $e_x = 0$ or $Rx \in L(R)$ whence $e_x = 1 - f_x$. For uniqueness, it suffices to show that if $r + u = 0$, then $r = 0$. There is a regular element $x \in R$ such that $xu = 0$. So $xr = 0$, which implies $r = 0$. Thus $R[E]$ and $R[E']$ are isomorphic rings. As S and S' are *minimal* zero-dimensional extensions, $S = T(R[E])$ and $S' = T(R[E'])$ by Arapović's theorem, so S and S' are isomorphic. □

9. Noetherian spectrum. It is a classical result [**8**, Proposition 2.1] that a commutative ring has Noetherian spectrum exactly when every prime ideal is the radical of a finitely generated ideal. It's also true that a finite-dimensional ring has Noetherian spectrum exactly when the radical of any finitely generated ideal is the intersection of finitely many prime ideals. That's because another classical characterization of Noetherian spectrum [**8**, Proposition 2.1] is that the ring has the ascending chain condition on prime ideals and every finitely generated ideal has only finitely many minimal prime ideals.

We will put those two conditions together and define a ring of dimension at most one (the only case we are interested in) to have *Noetherian spectrum* if the radical of any finitely generated ideal is the intersection of finitely many prime ideals, each of which is the radical of a finitely generated ideal. Notice that this condition allows us to get our hands on prime ideals.

Under this definition, a Noetherian ring need not have Noetherian spectrum from a constructive point of view. Indeed, whatever your

definition of "Noetherian," the ring $F[X]$, where F is a (discrete) field, better satisfy it. However, for $F[X]$ to have Noetherian spectrum, you have to be able to write each nonconstant polynomial in $F[X]$ that is relatively prime to its derivative, and thus generates a radical ideal, as a product of a finite number of irreducible polynomials, which you can't do even when $\mathbf{Q} \subset F \subset \mathbf{Q}[i]$ (consider the polynomial $X^2 + 1$).

We need to clarify what we will mean by a prime ideal. Of course, this is pretty much the same question as what an integral domain is. I'm going to assume that an integral domain is a discrete commutative ring such that if $rs = 0$, then $r = 0$ or $s = 0$. You might also want $0 \neq 1$ because this is normally required of a field, but that seems counterproductive here. So we will say that an ideal P is a *prime ideal* if it is detachable and if $rs \in P$, then $r \in P$ or $s \in P$. Actually, this, minus the detachability condition, is the definition of "prime ideal" given in [**7**], although the definition of "integral domain" there requires $0 \neq 1$.

We could, with considerably less justification, say that an arbitrary ring (not necessarily finite dimensional) has Noetherian spectrum if it satisfies the conditions above. Possibly this is an interesting class of rings, but I wouldn't bet on it.

Note that the nilradical of a ring with Noetherian spectrum is detachable because it is the radical of the zero ideal so is an intersection of finitely many detachable ideals. In fact the radical of any finitely generated ideal is detachable for the same reason. Note also that a finitely generated ideal is either proper or equal to R because an ideal is equal to R if and only if 1 is in its radical.

Theorem 17. *Let R be a commutative ring. If P and Q are prime ideals of R, and P is the radical of a finitely generated ideal, then either P is contained in Q or there is an element of P that is not in Q. In particular, the set of prime ideals that are radicals of finitely generated ideals is discrete. If R has Noetherian spectrum, then the radical of any finitely generated ideal is uniquely a finite intersection of incomparable prime ideals that are radicals of finitely generated ideals.*

Proof. Suppose P is the radical of the finitely generated ideal I. If $P \subset Q$, then clearly $I \subset Q$. Conversely, if $I \subset Q$, and $r \in P$, then

$r^n \in I \subset Q$ for some n, so $r \in Q$ because Q is prime. Because Q is detachable, and I is finitely generated, either $I \subset Q$ or there exists $r \in I$ such that $r \notin Q$.

Now suppose I is finitely generated and $\operatorname{rad} I = P_1 \cap \cdots \cap P_m$ where the P_i are prime ideals that are radicals of finitely generated ideals. Since we can compare the prime ideals P_i, we may throw out the ones that are not minimal, and we are left with incomparable prime ideals. Suppose now that $\operatorname{rad} I = Q_1 \cap \cdots \cap Q_n$ where the Q_i are incomparable prime ideals that are radicals of finitely generated ideals. For each i and j, either $P_i \subset Q_j$ or there is an element of P_i that is not in Q_j. As Q_j is prime and contains $P_1 \cdots P_m$, it must contain some P_i. Similarly each P_i must contain some Q_j. Because of the incomparability conditions, each P_i must equal some Q_j and vice versa. □

So if R has Noetherian spectrum, then $L(R)$ is discrete, and each element is a finite join of atoms (the prime ideals). It follows that if R is a suitable ring with Noetherian spectrum, then the minimal zero-dimensional extensions of R are determined by specifying, for each prime ideal $\mathfrak{a} \in L(R)$, an ideal $I_{\mathfrak{a}}$ in R that contains a power of $\mathfrak{a}$. This is essentially the main result of [**3**].

Examples of one-dimensional integral domains with Noetherian spectrum are finitely generated subrings R of the ring of algebraic integers in a finite-dimensional extension K of $\mathbf{Q}$. For example, $\mathbf{Z}[2i]$. We know that $\dim R \leq 1$ from [**4**, Corollary 2.4]. Now the ring of integers in K is a finite-rank free abelian group, so any finitely generated subring R is also a finite-rank free abelian group. Here *finitely generated* can be taken to mean as a ring because each element of R satisfies a monic polynomial with coefficients in $\mathbf{Z}$, so $\mathbf{Z}[x_1, \ldots, x_n]$ is finitely generated as an abelian group for $x_1, \ldots, x_n \in R$. Multiplication by nonzero $r \in R$ is one-to-one on R, so R/Rr is finite. So every nonzero finitely generated ideal I of R is detachable and, if proper, is contained in a finitely generated maximal ideal of R. Moreover $\operatorname{rad} I$ is finitely generated.

10. A one-dimensional Bezout domain. The ring $k[X]$, where k is an arbitrary discrete field, is a one-dimensional Bezout domain which need not have Noetherian spectrum in the constructive sense that we

defined the term. Nonetheless, it does have Noetherian spectrum in the classical sense. However, there are one-dimensional Bezout domains that do not have Noetherian spectrum in any sense, and the main theorem in this paper applies to them even though the theorem in [**3**] does not. I will leave it to the reader to evaluate how perspicuous the theorem is in this case.

Let R be the ring of polynomials with rational coefficients and nonnegative rational exponents. This ring is the direct limit of the principal ideal domains $\mathbf{Q}[X]$ where the connecting maps $g_n : \mathbf{Q}[X] \to \mathbf{Q}[X]$ take X to X^n. It has dimension one because it is a direct limit of rings of dimension one. It does not have Noetherian spectrum: The ideals generated by $X-1$, $X^{1/2}-1$, $X^{1/4}-1$, $X^{1/8}-1, \ldots$ are each radical because $X^m - 1$ is square free in $\mathbf{Q}[X]$. They are properly increasing because the only units are nonzero rational numbers. The polynomials $X^q - 1$ where q ranges over all rational numbers generate a proper ideal because $X^{s/n}-1$ and $X^{t/n}-1$ are divisible by $X^{1/n}-1$. This ideal is the kernel of the evaluation map into $\mathbf{Q}$ that takes X to 1. So it's the augmentation ideal. Every $X^q - 1$ generates a radical ideal because it is square free.

Note that if $p(X)$ is an Eisenstein polynomial, then so is $p(X^n)$, so these polynomials are prime in the limit ring.

What's an interesting example of a minimal zero-dimensional extension of this ring? There are the rings $K \times R/I$ where I is any nonzero ideal of R and K is the quotient field of R. More interesting are the universal examples, see Corollary 9, achieved by setting $I_{\mathfrak{a}} = (\operatorname{rad} \mathfrak{a})^n$ for a fixed positive integer n. Is there an example more tailored to this specific ring?

REFERENCES

1. Miroslav Arapović, *The minimal* 0*-dimensional overrings of commutative rings*, Glas. Mat. **18** (1983), 47–52.

2. James W. Brewer and Fred Richman, *Subrings of zero-dimensional rings*, in *Multiplicative ideal theory in commutative algebra*, Springer, New York, 2006, 73–88.

3. Marcela Chiorescu, *Minimal zero-dimensional extensions*, J. Alg. **322** (2009), 259–269.

4. Thierry Coquand, Lionel Ducos, Henri Lombardi and Claude Quitté, *Constructive Krull dimension* I: *Integral extensions*, J. Alg. Appl. **8** (2009), 129–138.

5. Thierry Coquand, Henri Lombardi and Marie-Françoise Roy, *An elementary characterization of Krull dimension*, *From sets and types to topology and analysis*, Oxford Logic Guides **48** (2005), 239–244.

6. Lionel Ducos, Henri Lombardi, Claude Quitté and Maimouna Salou, *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind*, J. Alg. **281** (2004), 604–650.

7. Ray Mines, Fred Richman and Wim Ruitenburg, *A course in constructive algebra*, Springer, New York, 1988.

8. Jack Ohm and Robert Pendleton, *Rings with Noetherian spectrum*, Duke Math. J. **35** (1968), 631–640.

Florida Atlantic University, Department of Mathematics, Boca Raton, FL 33431
Email address: fred@math.fau.edu