MINIMAL SETS IN FINITE RINGS

LEANNE CONAWAY AND KEITH A. KEARNES

Abstract. We describe how to calculate the $\langle \alpha, \beta \rangle$-minimal sets in any finite ring.

1. Introduction

In the mid-1980's, David Hobby and Ralph McKenzie introduced a general localization theory for algebras, called *tame congruence theory*. The theory has proven to be an effective tool for analyzing the structure of finite algebras and locally finite varieties. A preliminary version of the theory appears in [13], the handbook of the theory is [4], and later expositions of the theory can be found in [1, 2, 5, 8, 9, 10].

One of the strengths of tame congruence theory is that its concepts are language-independent. But this feature raises a question about how the theory might make connections with classical algebra. Since the theory studies finite algebras via the structure and distribution of their minimal sets, this question might be phrased more specifically as: "How do you calculate the minimal sets in a finite group, ring, module, semigroup, etc?" One of the problems posed by Hobby and McKenzie is:

Problem 15 of [4]**.** Investigate $\langle 0, \alpha \rangle$-minimal sets for abelian minimal congruences α of finite groups. Do the same for finite rings.

In this paper we solve the second half of Problem 15 by describing all minimal sets in finite rings[1] up to polynomial isomorphism. As part of the solution we find it necessary to describe the minimal sets in finite modules and bimodules. The main results are Theorems 2.9, 3.5, 4.1, and Corollary 4.2.

The part of Problem 15 concerning finite groups seems harder than the part about rings, and it is still open. A partial result in this direction was proved in 1996 by K. Kearnes, E. W. Kiss and C. Szabo: if $\mathbf{G}$ is a finite group, then any p-Sylow subgroup of $\mathbf{G}$ is a "neighborhood". (See the next section for this definition. See [8] for a proof of this statement about groups.) This result solves the part of Problem 15 that concerns nilpotent groups.

1991 *Mathematics Subject Classification.* Primary 08B05, Secondary 16P10.

Key words and phrases. finite ring, minimal set, tame congruence theory.

This material is based upon work supported by the National Science Foundation under Grant No. DMS 9802922.

[1]In this paper, the word "ring" always means "associative ring with unit element".

Since the part of Problem 15 that concerns groups is still mostly open, it goes without saying that the corresponding problems for semigroups and loops have not been solved. However, the E-minimal semigroups and loops have been characterized in [16, 7] respectively. Identifying the E-minimal algebras in a given variety is a special but important subcase of the problem of describing all minimal sets in members of the variety. The classification of E-minimal (nonunital) rings is an unpublished result of S. Seif.

2. Preliminaries

The following definition is a slight specialization of a concept from [8].

Definition 2.1. Let $\mathbf{A} = \langle A; F\rangle$ be an algebra. A *neighborhood of* $\mathbf{A}$ is a subset of A of the form $U = \varepsilon(A)$ where ε is a nonconstant idempotent unary polynomial of $\mathbf{A}$. Neighborhoods U and V are *polynomially isomorphic* if there exist unary polynomials f and g of $\mathbf{A}$ such that $f|_U : U \to V$ and $g|_V : V \to U$ are inverse bijections. The polynomials f and g are called *polynomial isomorphisms*.

Note that if $\mathbf{A}$ is a finite algebra, $U, V \subseteq A$ are neighborhoods, and there exist unary polynomials f and g of $\mathbf{A}$ such that $f|_U : U \to V$ and $g|_V : V \to U$ are injective, then U and V must be polynomially isomorphic. The reason for this is that the finiteness of U and V imply that $f|_U$ and $g|_V$ are bijections. To exhibit a pair of inverse bijections, choose $n > 0$ so that $(f \circ g)^n(x) = x$ on V. Then $f|_U$ and $g \circ (f \circ g)^{2n-1}|_V$ are restrictions of unary polynomials and are inverse bijections between U and V.

Let $\mathbf{A}$ be an algebra, ε be an idempotent polynomial, and $U = \varepsilon(A)$ be the image of ε. Suppose that f and g are unary polynomials of $\mathbf{A}$ such that $g \circ f(x) = x$ on U. Then $f \circ \varepsilon \circ g$ is an idempotent polynomial of $\mathbf{A}$. Moreover, if $V = f \circ \varepsilon \circ g(A)$, then $f|_U : U \to V$ and $g|_V : V \to U$ are inverse polynomial bijections, so V is a neighborhood polynomially isomorphic to U.

Later in this paper we will focus on algebras that have an underlying additive group structure (rings, modules and bimodules). Since the group of additive translations (i.e., the polynomials of the form $\pi(x) = x + a$) acts transitively on any such algebra, the observation of the previous paragraph implies that each neighborhood of a ring, module, or bimodule is polynomially isomorphic to a neighborhood of zero.

Neighborhoods support algebras that locally approximate the polynomial structure of $\mathbf{A}$. These algebras are called "induced algebras".

Definition 2.2. If $\mathbf{A}$ is an algebra and $U \subseteq A$ is a neighborhood, then the *(nonindexed) algebra that* $\mathbf{A}$ *induces on* U is

$$\mathbf{A}|_U = \langle U; \mathrm{Pol}(\mathbf{A})|_U\rangle.$$

(Here $\mathrm{Pol}(\mathbf{A})|_U$ means the clone on U consisting of the restrictions to U of all polynomial operations of $\mathbf{A}$ that can be restricted to U.)

It is not hard to show that if U and V are polynomially isomorphic neighborhoods, then $\mathbf{A}|_U$ and $\mathbf{A}|_V$ are isomorphic nonindexed algebras. (See pages 28 and 29 of [4].)

Lemma 2.3. *Let $\mathbf{A}$ be a finite algebra, let $U \subseteq A$ be a neighborhood, and let $V \subseteq U$ be a subset. Then*

(1) *V is a neighborhood of $\mathbf{A}$ iff it is a neighborhood of $\mathbf{A}|_U$.*
(2) *If the equivalent conditions in (1) hold, then $\mathbf{A}|_V = (\mathbf{A}|_U)|_V$.*

Proof. For (1), if ε is an idempotent unary polynomial of $\mathbf{A}$ whose image is V, then $\varepsilon|_U$ is an idempotent unary polynomial of $\mathbf{A}|_U$ whose range is V. Conversely, if ε is an idempotent polynomial of $\mathbf{A}$ whose image is U, and φ is a polynomial of $\mathbf{A}$ that can be restricted to U for which $\varphi|_U$ is an idempotent polynomial of $\mathbf{A}|_U$ with image V, then $\varphi \circ \varepsilon$ is an idempotent polynomial of $\mathbf{A}$ whose image is V.

Part (2) follows from Exercise 2.5 (2) of [4]. □

The next result explains the connection between neighborhoods and $\langle \alpha, \beta \rangle$-minimal sets for finite algebras with a Maltsev polynomial.

Lemma 2.4. *Let $\mathbf{A}$ be a finite algebra with a Maltsev polynomial. A subset $U \subseteq A$ is an $\langle \alpha, \beta \rangle$-minimal set for some prime quotient $\langle \alpha, \beta \rangle$ of $\mathbf{A}$ if and only if U is minimal under inclusion among neighborhoods of $\mathbf{A}$. If U is minimal under inclusion among neighborhoods, then U is $\langle \alpha, \beta \rangle$-minimal for any $\alpha \prec \beta$ for which $\alpha|_U \neq \beta|_U$.*

Proof. For the forward direction of the first statement, Lemma 4.17 and Theorems 4.31 and 8.5 of [4] imply that if $\mathbf{A}$ has a Maltsev polynomial and U is an $\langle \alpha, \beta \rangle$-minimal set, then the only unary idempotent polynomials of $\mathbf{A}|_U$ are constants and the identity function. It follows that there is no nonconstant idempotent unary polynomial of $\mathbf{A}$ whose image is a proper subset of U. Thus, U is a minimal neighborhood.

Conversely, suppose that U is a minimal neighborhood of $\mathbf{A}$. Let ε be an idempotent unary polynomial for which $\varepsilon(A) = U$. Since $|U| > 1$, there exist congruences $\alpha \prec \beta$ such that $\alpha|_U \neq \beta|_U$. For any such congruences $\varepsilon(\beta|_U) \not\subseteq \alpha$, so by Theorem 2.8 (3) of [4] the set $\varepsilon(U) = U$ contains an $\langle \alpha, \beta \rangle$-minimal set. This minimal set must be U itself, since U is a minimal neighborhood. This proves the backward direction of the first statement, and the second statement of the lemma. □

Based on the observation of this lemma, our procedure for determining $\langle \alpha, \beta \rangle$-minimal sets of abelian type of a finite ring $\mathbf{R}$ will be the following: we will construct some neighborhoods of $\mathbf{R}$, and then test whether the corresponding induced algebras have proper subneighborhoods. If so, then we continue the procedure by constructing subneighborhoods until a minimal one is located. As the next lemma proves, it is much easier to determine minimal sets of nonabelian type (when $\mathbf{A}$ has a Maltsev polynomial).

Lemma 2.5. *Let* $\mathbf{A}$ *be a finite algebra with a Maltsev polynomial. If* $\langle \alpha, \beta \rangle$ *is a nonabelian prime quotient, then there is a least congruence* θ *satisfying* $\theta \leq \beta$ *and* $\theta \not\leq \alpha$*. The* $\langle \alpha, \beta \rangle$*-minimal sets are precisely the sets of the form* $U = \{0, 1\}$ *where* $(0, 1) \in \theta - \alpha$*.*

Proof. If $\langle \alpha, \beta \rangle$ is a nonabelian prime quotient, and $\mathbf{A}$ has a Maltsev polynomial, then $\operatorname{typ}(\alpha, \beta) = \mathbf{3}$ by Theorem 5.7 and Exercise 8.8 (1) of [4]. By Lemma 5.15 (2) of [4] there is a smallest congruence $\theta \leq \beta$ such that $\theta \not\leq \alpha$. Necessarily θ is join-irreducible with lower cover $\theta_* = \theta \cap \alpha$, and $\langle \theta_*, \theta \rangle$ is perspective with $\langle \alpha, \beta \rangle$. By Exercise 2.19 (3) of [4] the two quotients have the same minimal sets. By Lemma 4.17 and Theorem 8.5 of [4], any such minimal set is a two-element set $\{0, 1\}$ where $(0, 1) \in \theta - \theta_* = \theta - \alpha$. This proves that every $\langle \alpha, \beta \rangle$-minimal set has the form claimed.

Now suppose that $\{0, 1\}$ is one $\langle \alpha, \beta \rangle$-minimal set, and that $\{u, v\}$ is another two-element set with $(u, v) \in \theta - \alpha$. By showing that $\{u, v\}$ is a neighborhood we will establish that it is an $\langle \alpha, \beta \rangle$-minimal set, according to Lemma 2.4. Since θ is join-irreducible and $(0, 1), (u, v) \in \theta - \theta_*$ the pairs $(0, 1)$ and (u, v) generate the same congruence. By Theorem 4.70.ii of [14] there exist unary polynomials f and g such that $f(\{0, 1\}) = \{u, v\}$ and $g(\{u, v\}) = \{0, 1\}$; in other words, $\{0, 1\}$ and $\{u, v\}$ are polynomially isomorphic. As observed after Definition 2.1, any set V polynomially isomorphic to a neighborhood U is again a neighborhood. This shows that our set $\{u, v\}$ is a minimal neighborhood polynomially isomorphic to $\{0, 1\}$, and consequently $\{u, v\}$ satisfies the criterion that defines $\langle \alpha, \beta \rangle$-minimal sets. □

Soon we will use this lemma to describe how to locate a representative collection of minimal sets of nonabelian type in a finite ring.

From this point forward we will restrict our attention to rings, modules and bimodules. Congruences on such algebras are determined by ideals, submodules, and subbimodules respectively. If P and Q are the ideals (or submodules or subbimodules) that correspond to the congruences α and β, then we will use P and Q in place of α and β in most situations (example: we use "$\langle P, Q \rangle$-minimal" in place of "$\langle \alpha, \beta \rangle$-minimal"). If we need to refer to the congruence associated to the ideal/submodule/subbimodule P, we will denote it θ_P.

Recall that the Jacobson radical of a ring $\mathbf{R}$ is defined to be the intersection of maximal left ideals of $\mathbf{R}$. The following result summarizes the results we need about the Jacobson radical of a finite ring.

Theorem 2.6. *Let* $\mathbf{R}$ *be a finite ring with Jacobson radical* J*.*

(1) $\mathbf{R}/J$ *is a direct product of (nonabelian) simple rings.*
(2) J *is the intersection of the maximal ideals of* $\mathbf{R}$*.*
(3) J *is the largest nilpotent ideal of* $\mathbf{R}$*, and also the largest nil ideal.*
(4) J *is the largest ideal* I *for which* $1 + I$ *consists of units.*

(5) *The prime quotient* $\langle I, K\rangle$ *is nonabelian iff it is perspective with* $\langle I+J, K+J\rangle$. *It is abelian iff it is perspective with* $\langle I \cap J, K \cap J\rangle$.

Proof. Part (1) follows from the Wedderburn-Artin Theorem together with the observation that any nontrivial unital ring is nonabelian (since the multiplication operation witnesses that $\langle 0, 1\rangle$ is a 2-snag — see Theorem 7.2 of [4]).

Part (2) is a translation of (1) into the language of ideals.

Part (3) follows from Lemma 4.11 and Theorem 4.12 of [11].

Part (4) follows from Corollary 4.5 of [11].

For part (5), let $\langle I, K\rangle$ be any prime quotient of $\mathbf{R}$. Since the ideal lattice of $\mathbf{R}$ is modular, one of the quotients $\langle I+J, K+J\rangle$ or $\langle I\cap J, K\cap J\rangle$ is trivial and the other is a prime quotient that is perspective with $\langle I, K\rangle$. Perspectivity preserves abelianness and nonabelianness. Thus (4) follows from the fact that all prime quotients of the form $\langle I \cap J, K \cap J\rangle$ are abelian (since J is nilpotent), and all prime quotients of the form $\langle I + J, K + J\rangle$ are nonabelian (since $\mathbf{R}/J$ is finite product of nonabelian simple algebras). □

We will make frequent use of idempotents in finite rings. The next definition and the succeeding result summarize the properties that we need.

Definition 2.7. Let $\mathbf{R}$ be a ring. An element $e \in R$ is *idempotent* if $e^2 = e$. Idempotents $e, f \in R$ are *orthogonal* if $ef = fe = 0$. A nonzero idempotent $e \in R$ is *primitive* if it whenever $e = f + g$ where f and g are orthogonal idempotents, then $f = 0$ or $g = 0$. If $e, f \in R$, then $e \leq f$ if $ef = fe = e$. A nonzero idempotent f is *minimal* if whenever e is a nonzero idempotent satisfying $e \leq f$, then $e = f$. An idempotent $e \in R$ is *local* if $e\mathbf{R}e$ is a local ring (i.e., a ring whose nonunits form an ideal). If $e, f \in R$ are nonzero idempotents, then e is *isomorphic* to f (written $e \simeq f$) if $\mathbf{R}e \cong \mathbf{R}f$ as left $\mathbf{R}$-modules.

The relation $\leq$ defined above by $e \leq f$ iff $ef = fe = e$ is a partial order on the set of the idempotents of $\mathbf{R}$. It is trivial that this relation is reflexive and antisymmetric. To see that this relation is transitive, suppose that $e, f, g \in R$ are idempotent and $e \leq f \leq g$. Then $eg = (ef)g = e(fg) = ef = e$ and similarly $ge = e$, so $e \leq g$. An idempotent is "minimal" if it is a minimal element of this partial order.

Theorem 2.8. *Let* $\mathbf{R}$ *be a finite ring with radical* J.

(1) *The following are equivalent for an idempotent* $e \in R$*:*
   (i) e *is primitive.*
   (ii) e *is minimal.*
   (iii) e *is local.*

(2) *An ideal* $I \subseteq R$ *contains a primitive idempotent iff* $I \not\subseteq J$.

(3) *If* $e \in R$ *is a primitive idempotent, then the ideal* (e) *generated by* e *is join-irreducible with lower cover equal to* $(e) \cap J$.

(4) *The following are equivalent for idempotents $e, f \in R$:*
  (i) $e \simeq f$.
  (ii) *e and f generate the same ideal.*
  (iii) *There exist $p, q, r, s \in R$ such that $e = pfq$ and $f = res$.*
  (iv) *There exist $c, d \in R$ such that $e = cd$ and $f = dc$.*
  If e and f are primitive, then these conditions are equivalent to:
  (v) $eRf \not\subseteq J$.
  (vi) *There exists a maximal ideal M such that $e \notin M$ and $f \notin M$.*

(5) *A nonzero idempotent $e \in R$ may be represented as $e = e_1 + \cdots + e_k$ where the e_i are pairwise orthogonal primitive idempotents. In any such representations $e_j \leq e$ for all j.*

(6) *If $1 = e_1 + \cdots + e_k$ is a representation of 1 as a sum of pairwise orthogonal primitive idempotents, and f is a primitive idempotent, then $e_j \simeq f$ for some j.*

(7) *If I is a nilpotent ideal of $\mathbf{R}$, and $\bar{e} = \bar{e}_1 + \cdots + \bar{e}_k$ is a representation of an idempotent $\bar{e} \in \mathbf{R}/I$ as a sum of pairwise orthogonal primitive idempotents in $\mathbf{R}/I$, then there exist idempotents $e, e_1, \ldots, e_k \in \mathbf{R}$ such that $\bar{e} = e/I, \bar{e}_i = e_i/I$, and $e = e_1 + \cdots + e_k$ is a representation of e as a sum of pairwise orthogonal primitive idempotents in $\mathbf{R}$.*

(8) *If I is a nilpotent ideal in $\mathbf{R}$, and $e, f \in R$ are idempotents, then e/I is primitive in $\mathbf{R}/I$ iff e is primitive in $\mathbf{R}$. Moreover $e/I \simeq f/I$ in $\mathbf{R}/I$ iff $e \simeq f$ in $\mathbf{R}$.*

Proof. Item (1) follows from Theorems 21.8 of [11] and VII.8 of [12].

If I contains a primitive idempotent e, then $e \in I - J$ since J contains no nonzero idempotents. Conversely, using the facts that (a) J is the largest nilpotent ideal, (b) a nonnilpotent ideal of a finite ring contains a nonzero idempotent (Theorem VII.5 of [12]), and (c) if $e \leq f$ are comparable idempotents, then $(e) \subseteq (f)$, it follows that if $I \not\subseteq J$, then I contains a minimal (hence primitive) idempotent. This proves (2).

If $I = (e)$ is generated by a primitive idempotent e, then $I \not\subseteq J$. Choose any ideal $I' \subset I$. If $I' \not\subseteq J$, then there exists a primitive idempotent $f \in I'$ $(\subseteq I = (e))$ by (iii). But if e and f are primitive idempotents and $f \in (e)$, then $(f) = (e)$ according to Exercise VII.9 of [12]. This can't happen if I' is strictly contained in I, so we conclude that for any ideal $I' \subsetneq I$ properly contained in I we have $I' \subseteq J$. Hence I is join-irreducible with lower cover $I \cap J$. This proves (3)

For part (4), the conditions (i), (ii) and (iv) are shown to be equivalent in Theorem 21.20 of [11] and Exercise VII.9 of [12]. But (iv)⇒(iii) since we can take $(p, q, r, s) = (c, d, d, c)$, and (iii)⇒(ii) since $e = pfq \in (f)$ and $f = res \in (e)$. The equivalence of these conditions with condition (v) when e and f are primitive is part of Exercise VII.9 of [12]. To prove the equivalence of condition (vi) with these properties, assume that e and f are primitive idempotents. Since $e \notin J$ there is a maximal

ideal M not containing e. If we assume that $e \simeq f$, then we get that $(f) = (e) \not\subseteq M$, so $f \notin M$. This proves that (i)⇒(vi). Conversely, assume that there exists a maximal ideal M not containing e or f. Then $R = (e) + M = (f) + M$, so

$$R = ((e) + M)((f) + M) = (e)(f) + M.$$

Now $(e)(f) \subseteq (e)$; if the containment is proper, then according to part (3) we have that $(e)(f) \subseteq J \subseteq M$. But this implies that $R = (e)(f) + M \subseteq M$, which is false. Hence $(e)(f) = (e)$. The same argument shows that $(e)(f) = (f)$, so $(e) = (f)$, which implies that $e \simeq f$. This proves that (vi)⇒(i).

Now, to prove (5), let $e \in R$ be a nonzero idempotent. If e is primitive, then there is nothing to show, so assume otherwise. According to part (1), there exists an idempotent $f \neq e$ such that $f \leq e$. The element $g = e - f$ is an idempotent (since $g^2 = (e-f)^2 = e^2 - ef - fe + f^2 = e - f - f + f = g$) for which $g \leq e$ (since $ge = (e-f)e = e^2 - fe = e - f = g = eg$) and $e = f + g$ is a representation of e as a sum of orthogonal idempotents (since $fg = f(e-f) = fe - f^2 = f - f = 0 = gf$). Proceeding by induction, assume that we have found pairwise orthogonal idempotents f_i for which

$$e = f_1 + \cdots + f_m$$

and all $f_i \leq e$. Assume that one of these, say f_m, is not minimal. Then choose $h \neq f_m$ satisfying $h \leq f_m \leq e$. For $k = f_m - h$ we also get that k is idempotent and $k \leq f_m \leq e$. Since $hk = h(f_m - h) = h - h^2 = 0 = kh$, the idempotents h and k are orthogonal with each other. To see that they are orthogonal with all f_j, $j \neq m$, note that

$$f_j = ef_j = ((\sum_{i=1}^{m-1} f_i) + h + k)f_j = (\sum_{i=1}^{m-1} f_i)f_j + hf_j + kf_j = f_j + hf_j + kf_j,$$

so $hf_j + kf_j = 0$. Multiplying on the left by h yields $hf_j = h(hf_j + kf_j) = 0$. Similarly $f_jh = f_jk = kf_j = 0$. Thus, we can lengthen any representation of e as a sum of orthogonal idempotents if any one of the idempotents is not minimal. This process cannot go on indefinitely, since there are finitely many idempotents and the idempotents in any orthogonal representation must be distinct. This shows that a representation of e as a sum of pairwise orthogonal primitive idempotents exists. The orthogonality of the e_i's and the idempotence of each e_j implies that $ee_j = e_je = e_j$ for each j, so $e_j \leq e$ as claimed. This proves (5).

For part (6), assume that $1 = e_1 + \cdots + e_k$ is a representation of 1 as a sum of pairwise orthogonal primitive idempotents, and that f is a primitive idempotent. The representation $1 = f + (1 - f)$ is a representation of 1 as a sum of orthogonal idempotents with f primitive. Using the procedure described in the proof of part (5) we can refine this to a representation $1 = f_1 + f_2 + \cdots + f_m$ of 1 as a sum of pairwise orthogonal primitive idempotents with $f_1 = f$. By Theorem VII.13 of [12], $k = m$ and there is a unit $u \in R$ and a permutation $\pi \in S_k$ such that $ue_iu^{-1} = f_{\pi(i)}$ for all

i. Thus, there is a unit u and an e_j such that $ue_ju^{-1} = f_1 = f$ and $u^{-1}fu = e_j$. By the equivalence of (4)(i) and (4)(iii) we get that $e_j \simeq f$.

Part (7) follows from Proposition 21.25 of [11].

Part (8) follows from Theorems 21.21 and 21.22 of [11]. □

Note that the arguments for parts (5) and (6) show that if there is a representation of 1 as sum of k primitive idempotents that are pairwise orthogonal, then any representation of 1 as a sum of orthogonal idempotents uses $\leq k$ idempotents, and that a representation uses k idempotents only when all idempotents in the representation are primitive.

Now we can describe the minimal sets of nonabelian type in a finite ring.

Theorem 2.9. *Let* $\mathbf{R}$ *be a finite ring. If* $I \prec K$ *are ideals of* $\mathbf{R}$ *and* e *is a primitive idempotent in* $K - I$*, then* $\{0, e\}$ *is a* $\langle I, K\rangle$*-minimal set of nonabelian type. If* e *and* f *are primitive idempotents, then* $U = \{0, e\}$ *is polynomially isomorphic to* $V = \{0, f\}$ *iff* $e \simeq f$*. If* $1 = e_1 + \cdots + e_k$ *is a representation of* 1 *as a sum of pairwise orthogonal primitive idempotents, then the sets* $U_i = \{0, e_i\}$*,* $1 \leq i \leq k$*, represent all minimal sets of nonabelian type up to polynomial isomorphism.*

Proof. It follows from Lemma 2.5 and Theorem 2.8 (3) that $\{0, e\}$ is a $\langle (e) \cap J, (e)\rangle$-minimal set. Since $(0, e) \in \theta_K - \theta_I$, it is also a $\langle I, K\rangle$-minimal set according to Lemmas 2.4 and 2.5 The type is nonabelian since multiplication in $\mathbf{R}$ is a polynomial operation witnessing that $\langle 0, e\rangle$ is a 2-snag. This proves the first statement.

If $g : U \to V$ is a polynomial isomorphism, then composing g with the polynomial $h(x) = f - x$ if necessary we may assume that $g(0) = 0$ and $g(e) = f$. This implies that $f \in (e)$, and similar reasoning shows that $e \in (f)$, hence $e \simeq f$ by Theorem 2.8 (4). Conversely, if $e \simeq f$, then (in the notation of Theorem 2.8 (4)(iii)) the functions $h(x) = pxq$ and $k(x) = rxs$ are polynomial isomorphisms between U and V. This proves the second statement.

Suppose that $I \prec K$ are ideals and that $\langle I, K\rangle$ is a nonabelian prime quotient. By the remarks at the end of Chapter 1 of [3], the fact that $\langle I, K\rangle$ is nonabelian means that $K^2 \not\subseteq I$. Thus, the minimal ideal K/I of $\mathbf{R}/I$ satisfies

$$(K/I)^2 = (K^2 + I)/I = K/I = (K/I)^n \quad \text{for all } n.$$

Hence K/I is not contained in the radical of $\mathbf{R}/I$, according to Theorem 2.6 (3). Part (3) of Theorem 2.6 therefore implies that K/I is not nil, so there is an element $r \in K$ such that r/I is not nilpotent in $\mathbf{R}/I$. This implies that no power r^k belongs to I. Since $\mathbf{R}$ is finite there is a k such that $e = r^k$ is an idempotent, and for this idempotent we have arranged that $e \in K - I$. By Theorem 2.8 (5) it is possible to represent e as a sum $e = f_1 + \cdots + f_m$ or pairwise orthogonal primitive idempotents all $\leq e$. Each f_i belongs to K, since $f_i = f_ie \in f_iK \subseteq K$, but not all belong to I since $e \notin I$. If $f_j \notin I$, then the first statement of this theorem shows that $V = \{0, f_j\}$ is a $\langle I, K\rangle$-minimal set. According to Theorem 2.8 (6), $f_j \simeq e_i$ for some i, and by

the second statement of this theorem that means that V is polynomially isomorphic to U_i. This proves the final statement. □

The previous theorem does not produce an idempotent polynomial whose image is $U = \{0, e\}$, where $e \in R$ is a primitive idempotent, but it is not hard to construct one. If k is an integer for which $\mathbf{R} \models x^k = x^{2k}$, then the polynomial $\varepsilon(x) = (exe)^k$ has range equal to the set of idempotents in $e\mathbf{R}e$. By Theorem 2.8 (1) this ring is a local ring with identity e, so this set of idempotents is $U = \{0, e\}$. Since $\varepsilon(x) = x$ on U, it is the desired polynomial.

We conclude this section by recording the definitions of "module" and "bimodule".

Definition 2.10. A *left* $\mathbf{R}$*-module* is an algebra

$$\mathbf{M} = \langle M; +, -, 0, \{\lambda_r(x) \mid r \in R\}\rangle$$

where $\langle M; +, -, 0\rangle$ is an abelian group, each $\lambda_r(x)$ is an abelian group endomorphism, and the assignment $r \mapsto \lambda_r$ is a ring homomorphism from $\mathbf{R}$ to the ring $\mathrm{End}(\mathbf{M})$. If $r \in R$ and $m \in M$, then we will write rm to mean $\lambda_r(m)$. A *right* $\mathbf{S}$*-module* is an algebra $\mathbf{M} = \langle M; +, -, 0, \{\rho_s(x) \mid s \in S\}\rangle$ where $\langle M; +, -, 0\rangle$ is an abelian group, each $\rho_s(x)$ is an abelian group endomorphism, and the assignment $s \mapsto \rho_s$ is a ring homomorphism from the opposite ring $\mathbf{S}^{op}$ to the ring $\mathrm{End}(\mathbf{M})$. We write ms to mean $\rho_s(m)$.

Since $\mathbf{M}$ is a right $\mathbf{S}$-module if and only if it is a left module over the opposite ring, $\mathbf{S}^{op}$, the task of computing minimal sets in modules reduces to computing minimal sets in left modules. Therefore, when we do not specify left or right we will mean left modules.

Definition 2.11. An $(\mathbf{R}, \mathbf{S})$*-bimodule* is an algebra

$$\mathbf{M} = \langle M; +, -, 0, \{\lambda_r(x) \mid r \in R\} \cup \{\rho_s(x) \mid s \in S\}\rangle$$

such that $\langle M; +, -, 0, \{\lambda_r(x) \mid r \in R\}\rangle$ is a left $\mathbf{R}$-module, $\langle M; +, -, 0, \{\rho_s(x) \mid s \in S\}\rangle$ is a right $\mathbf{S}$-module, and the equation

$$(rx)s = r(xs)$$

holds for all $r \in R, s \in S, x \in M$.

Thus, a bimodule is an abelian group together with specified homomorphisms $\mathcal{L} : \mathbf{R} \to \mathrm{End}(\mathbf{M})$ and $\mathcal{R} : \mathbf{S}^{op} \to \mathrm{End}(\mathbf{M})$ such that $\mathcal{L}(r) \circ \mathcal{R}(s) = \mathcal{R}(s) \circ \mathcal{L}(r)$ for all $r \in R$ and $s \in S$.

3. Reduction to the Radical

In this section we reduce the problem of determining the minimal sets of abelian type of a finite ring $\mathbf{R}$ to the problem of determining the minimal sets of $\mathbf{R}|_J$, where J is the Jacobson radical of $\mathbf{R}$.

Theorem 3.1. *The Jacobson radical of a finite ring is a neighborhood.*

Proof. Let $\mathbf{R}$ be a finite ring with radical J. Fix an integer $k > 0$ such that $\mathbf{R}$ satisfies the equation $x^k = x^{2k}$. For each subset $S \subseteq R \times R$ define a unary polynomial

$$P_S(x) = \left(1 + \sum_{(a,b)\in S} axb\right)^k.$$

The theorem is a consequence of the following claim.

Claim 3.2. *Any polynomial of the form* $\varepsilon(x) = x\left(\prod_{S\subseteq R\times R} P_S(x)\right)$, *where the product is over all subsets* $S \subseteq R \times R$ *in some fixed order, is an idempotent unary polynomial of* $\mathbf{R}$ *whose image is* J.

We need to show that $\varepsilon(R) \subseteq J$ and that $\varepsilon(x) = x$ on J. To show the latter, assume that $s \in J$. Then for any $S \subseteq R \times R$ the element $\left(\sum_{(a,b)\in S} asb\right) \in J$, so any element of the form $(1 + \sum asb)$ is a unit in $\mathbf{R}$ according to Theorem 2.6 (4). The element $P_S(s) = (1 + \sum asb)^k$ is an idempotent unit, since $\mathbf{R} \models x^k = x^{2k}$, so $P_S(s) = 1$ for any $S \subseteq R \times R$ and any $s \in J$. Thus $\varepsilon(s) = s\,(\prod 1) = s$ when $s \in J$.

To show that $\varepsilon(R) \subseteq J$, choose an arbitrary $r \in R$. By Theorem 2.6 (2), J is the intersection of the maximal ideals of $\mathbf{R}$. Thus it will suffice to show that $\varepsilon(r) \in M$ where M is an arbitrarily chosen maximal ideal. For this we can work in the quotient ring $\overline{\mathbf{R}} = \mathbf{R}/M$, which is simple. In this ring we must show that for an arbitrary $\bar{r} \in \overline{\mathbf{R}}$ it is the case that

$$\bar{\varepsilon}(\bar{r}) = \bar{r}\left(\prod_{S\subseteq R\times R} \overline{P_S}(\bar{r})\right) = \bar{0}.$$

If $\bar{r} = \bar{0}$, then the leading $\bar{r}$ in this expression gives the desired conclusion. If $\bar{r} \neq \bar{0}$, then the ideal generated by $\bar{r}$ is $\overline{\mathbf{R}}$, therefore

$$-\bar{1} = \sum_{(a,b)\in S} \bar{a}\bar{r}\bar{b}$$

for some $S \subseteq R \times R$. This shows that $\overline{P_S}(\bar{r}) = \bar{0}$ for this choice of S, so $\bar{\varepsilon}(\bar{r}) = \bar{0}$. Hence $\varepsilon(r) \in M$ for each $r \in R$ and each maximal ideal M, which proves that $\varepsilon(R) \subseteq J$. The claim is proved. □

Corollary 3.3. *Let* $\mathbf{R}$ *be a finite ring with Jacobson radical* J. *If* $I \prec K$ *are ideals of* $\mathbf{R}$, *and* U *is an* $\langle I, K\rangle$*-minimal set of abelian type, then* U *is polynomially isomorphic to a minimal set contained in* J.

Proof. By Theorem 2.6 (5), the prime quotient $\langle I, K\rangle$ is perspective with $\langle I\cap J, K\cap J\rangle$, so the two quotients have the same minimal sets according to Exercise 2.19 (3) of [4]. Thus we lose no generality if we assume that $I \prec K \leq J$. Now let ε be an idempotent unary polynomial of $\mathbf{R}$ such that $\varepsilon(R) = J$. Since $I, K \subseteq J$ we have $\varepsilon(K) = K \not\subseteq I = \varepsilon(I)$. By Theorem 2.8 (6) of [4], this implies that the set $\varepsilon(R) = J$ contains an $\langle I, K\rangle$-minimal set V. But all $\langle I, K\rangle$-minimal sets are polynomially isomorphic, so V is a minimal set in J that is polynomially isomorphic to U. □

This corollary shows that if $\langle I, K\rangle$ is an abelian prime quotient of the finite ring $\mathbf{R}$, then there is an $\langle I, K\rangle$-minimal set $U \subseteq J$. By Lemmas 2.3 and 2.4, the minimal sets of $\mathbf{R}$ contained in J are exactly the minimal sets of $\mathbf{R}|_J$. Indeed, the minimal set U is characterized up to polynomial isomorphism by the fact that it is a minimal neighborhood of the algebra $\mathbf{R}|_J$ for which $\theta_I|_U \neq \theta_K|_U$. Thus, our job now is to determine the minimal sets of $\mathbf{R}|_J$.

The polynomials of $\mathbf{R}|_J$ are the precisely the restrictions to J of polynomials $\varphi(x_1, \ldots, x_n)$ of $\mathbf{R}$ satisfying $\varphi(J, \ldots, J) \subseteq J$. Since $0 \in J$ this condition implies that $\varphi(0, \ldots, 0) \in J$. Conversely, since J is an ideal, any polynomial of $\mathbf{R}$ for which $\varphi(0, \ldots, 0) \in J$ also satisfies $\varphi(J^n) \subseteq J$. Hence the polynomials of $\mathbf{R}|_J$ are precisely (the restrictions of) the polynomials of $\mathbf{R}$ that satisfy $\varphi(0, \ldots, 0) \in J$. As usual for rings, we call a polynomial a *monomial* if it is a product of constants and variables, and note that any polynomial of the ring $\mathbf{R}$ is a sum of monomials. A typical monomial has the form $\mu(x) = r_0 x r_1 x \cdots x r_m$ for some $m \geq 0$ (which will be referred to as the *degree* of the monomial). For any polynomial φ, $\varphi(0, \ldots, 0)$ is the sum of monomials of degree 0, which may be replaced with a single monomial of degree 0 that we call the *constant term* of φ. Thus the polynomials of $\mathbf{R}|_J$ are the restrictions of the polynomials of $\mathbf{R}$ whose constant term belongs to J.

The following operations are polynomials operations of $\mathbf{R}|_J$: constants from J, $\lambda_r(x) = rx$ for each $r \in R$, $\rho_s(x) = xs$ for each $s \in R$, addition $+(x, y) = x + y$, and multiplication $\cdot(x, y) = xy$. These operations generate all other polynomials of $\mathbf{R}|_J$ since

(1) a monomial $\mu(x) = r_0 x_{i_1} r_1 x_{i_2} \cdots x_{i_m} r_m$ can be generated by composing $\lambda_{r_0}(x)$ with the product $\rho_{r_1}(x_{i_1}) \cdot \rho_{r_2}(x_{i_2}) \cdots \rho_{r_m}(x_{i_m})$, and
(2) sums of monomials can be generated with $+$.

Thus $\mathbf{R}|_J$ is polynomially equivalent to the $(\mathbf{R}, \mathbf{R})$-bimodule

$$\langle J; +, -, 0, \{\lambda_r(x) \mid r \in R\} \cup \{\rho_s(x) \mid s \in R\}\rangle$$

endowed with an associative, bilinear multiplication. Following R. Pierce we call any $(\mathbf{R}, \mathbf{R})$-bimodule endowed with an associative, bilinear multiplication a *multiplicative* $(\mathbf{R}, \mathbf{R})$-*bimodule* (Definition 11.7 of [15]). Since J is a nilpotent ideal of $\mathbf{R}$, the multiplication operation of $\mathbf{R}|_J$ satisfies the condition that there exists an integer

n such that all n-fold products are zero. If the multiplication of some multiplicative $(\mathbf{R}, \mathbf{R})$-bimodule satisfies this condition we will call it a *nilpotent* multiplicative $(\mathbf{R}, \mathbf{R})$-bimodule.

The remarks above establish the following theorem.

Theorem 3.4. *Let* $\mathbf{R}$ *be a finite ring with Jacobson radical* J*. The algebra* $\mathbf{R}|_J$ *is polynomially equivalent to a nilpotent multiplicative* $(\mathbf{R}, \mathbf{R})$*-bimodule.*

Our next goal is to prove that we need to consider only the linear structure on J when computing neighborhoods. Namely, we will show that if $\mathbf{J}^\circ$ is a nilpotent multiplicative $(\mathbf{R}, \mathbf{R})$-bimodule, and $\mathbf{J}$ is the $(\mathbf{R}, \mathbf{R})$-bimodule reduct of $\mathbf{J}^\circ$, then every neighborhood of $\mathbf{J}$ is a neighborhood of $\mathbf{J}^\circ$ (since $\mathbf{J}$ is a reduct of $\mathbf{J}^\circ$), and conversely any neighborhhood U of $\mathbf{J}^\circ$ is polynomially isomorphic in $\mathbf{J}^\circ$ to a set V that is simultaneously a neighborhood of $\mathbf{J}$ and of $\mathbf{J}^\circ$. Thus, up to polynomial isomorphism in $\mathbf{J}^\circ$ the neighborhoods in $\mathbf{J}$ and $\mathbf{J}^\circ$ are the same. The rest of this section will be devoted to proving this statement in the following form:

Theorem 3.5. *Let* $\mathbf{R}$ *be a finite ring, and let* $\mathbf{J}^\circ$ *be a nilpotent multiplicative* $(\mathbf{R}, \mathbf{R})$*-bimodule. Every neighborhood of* $\mathbf{J}^\circ$ *is polynomially isomorphic to a neighborhood of the underlying bimodule.*

The additive and multiplicative structure of $\mathbf{J}^\circ$ are those of a nilpotent (nonunital) ring. The ring-theoretic ideals of $\mathbf{J}^\circ$ that are $(\mathbf{R}, \mathbf{R})$-subbimodules will be called *ideals*. The congruences of $\mathbf{J}^\circ$ are determined by its ideals in the usual way. Ideals are closed under the ring-theoretic product because the multiplication is bilinear. The ideal J^k consists of elements of J that are sums of k-fold products of elements of J. Since there is an $n > 1$ such that all n-fold products in J are zero, we must have

$$J \supset J^2 \supset \cdots \supset J^n = \{0\}.$$

We will say that a unary polynomial ν of $\mathbf{J}^\circ$ is *nilpotent* if $a \equiv b \pmod{J^m}$ implies that $\nu(a) \equiv \nu(b) \pmod{J^{m+1}}$ for each m.

Lemma 3.6. *Assume that* $\mathbf{R}$ *is a finite ring and* $\mathbf{J}^\circ$ *is a nilpotent multiplicative* $(\mathbf{R}, \mathbf{R})$*-bimodule. If* φ *is a unary polynomial of* $\mathbf{J}^\circ$ *that fixes* 0*, then* $\varphi = \lambda + \nu$ *where* λ *is a unary* $(\mathbf{R}, \mathbf{R})$*-bimodule polynomial that fixes* 0 *and* ν *is a nilpotent polynomial that fixes* 0*.*

Proof. As is true for rings, the associativity and bilinearity of multiplication implies that any unary polynomial φ is expressible as a sum $\sum_{i=1}^{s} \mu_i$ of monomials, where a typical monomial of degree m has the form $\mu(x) = r_0 x r_1 x \cdots x r_m$. Fix such an expression for φ. Since $\varphi(0) = 0$, we may assume that all monomials in this expression have degree at least 1. Let λ equal the sum of the monomials of degree 1, and let ν equal the sum of the monomials of degree > 1. Both fix 0. Since λ has the form

$$\lambda(x) = a_1 x b_1 + \cdots + a_t x b_t$$

for some t, it is a bimodule polynomial. To show that ν is nilpotent it suffices to check that monomials of degree > 1 are nilpotent, since it is clear from the definition that sums of nilpotent polynomials are nilpotent.

To see that $\mu(x) = r_0 x r_1 x \cdots x r_m, m > 1$, is nilpotent, assume that $a \equiv b \pmod{J^k}$. Then $a - b = c \in J^k$, so $\mu(a) - \mu(b) = \mu(b + c) - \mu(b)$. The expression $\mu(b + c) = r_0(b + c)r_1(b + c) \cdots (b + c)r_m$ can be expanded into the sum of all terms of the form $r_0 z_1 r_1 z_2 \cdots z_m r_m$ with $(z_1, \ldots, z_m) \in \{b, c\}^m$. Exactly one term in this string equals $\mu(b) = r_0 b r_1 b \cdots b r_m$, and since $m > 1$ all other terms have at least one occurrence of c ($\in J^k$) and at least one other occurrence of either b or c ($\in J$). Thus each term in the sum for $\mu(b + c)$ except the term equal to $\mu(b)$ is in J^{k+1}. Hence $\mu(b + c) - \mu(b) \in J^{k+1}$, proving that $\nu(x)$ is nilpotent. □

Lemma 3.7. *Assume that* $\mathbf{R}$ *is a ring and* $\mathbf{J}^\circ$ *is a finite nilpotent multiplicative* $(\mathbf{R}, \mathbf{R})$*-bimodule. If* ε *is an idempotent unary polynomial of* $\mathbf{J}^\circ$ *that fixes* 0*, then* $\varepsilon = \lambda + \nu$ *where* λ *is an idempotent unary* $(\mathbf{R}, \mathbf{R})$*-bimodule polynomial that fixes* 0 *and* ν *is a nilpotent polynomial that fixes* 0*.*

Proof. Let $\mathcal{L}$ be the set of all unary polynomials λ of $\mathbf{J}^\circ$ such that

(*i*) λ is an $(\mathbf{R}, \mathbf{R})$-bimodule polynomial that fixes 0, and
(*ii*) there exists a nilpotent unary polynomial ν of $\mathbf{J}^\circ$ that fixes 0 such that $\varepsilon = \lambda + \nu$.

According to Lemma 3.6, $\mathcal{L}$ is not empty.

Claim 3.8. $\mathcal{L}$ *is closed under composition.*

If $\lambda, \lambda' \in \mathcal{L}$, then there exist nilpotent polynomials ν and ν' such that $\varepsilon = \lambda + \nu = \lambda' + \nu'$. Thus,

$$\begin{aligned} \varepsilon &= \varepsilon \circ \varepsilon = (\lambda + \nu) \circ (\lambda' + \nu') \\ &= \lambda \circ (\lambda' + \nu') + \nu \circ (\lambda' + \nu') \\ &= \lambda \circ \lambda' + \lambda \circ \nu' + \nu \circ (\lambda' + \nu') \\ &= \lambda \circ \lambda' + (\lambda \circ \nu' + \nu \circ \varepsilon) \end{aligned}$$

where the second to last line follows from the fact that $\lambda(a + b) = \lambda(a) + \lambda(b)$ for any bimodule polynomial that fixes 0. Since bimodule polynomials are closed under composition, $\lambda \circ \lambda'$ satisfies condition (*i*) of the definition of $\mathcal{L}$. To finish the proof of the claim we have to verify (*ii*), which we will do by showing that $\lambda \circ \nu' + \nu \circ \varepsilon$ is nilpotent.

Assume that $a \equiv b \pmod{J^k}$ for some k. Then $\nu'(a) \equiv \nu'(b) \pmod{J^{k+1}}$ since ν' is nilpotent, and $\varepsilon(a) \equiv \varepsilon(b) \pmod{J^k}$ since polynomials preserve congruences. Furthermore $\lambda(\nu'(a)) \equiv \lambda(\nu'(b)) \pmod{J^{k+1}}$ since polynomials preserve congruences, and $\nu(\varepsilon(a)) \equiv \nu(\varepsilon(b)) \pmod{J^{k+1}}$ since ν is nilpotent. This shows that $\lambda \circ \nu'$ and $\nu \circ \varepsilon$ are each nilpotent, so the sum $\lambda \circ \nu' + \nu \circ \varepsilon$ is nilpotent.

$\mathcal{L}$ is nonempty, finite, and closed under composition, so $\mathcal{L}$ contains an idempotent. (Any nonempty finite semigroup contains an idempotent.) This finishes the proof. □

Now we are in position to prove Theorem 3.5.

Proof. Assume that U is a neighborhood of $\mathbf{J}^\circ$. As observed after Definition 2.1, U is polynomially isomorphic to a neighborhood of 0, so no generality is lost in assuming that $0 \in U$. Any idempotent unary polynomial ε of $\mathbf{J}^\circ$ for which $\varepsilon(J) = U$ must fix 0. From Lemma 3.7 we know that ε is expressible as $\varepsilon = \lambda + \nu$ where λ is an idempotent unary bimodule polynomial, ν is a unary nilpotent polynomial, and both fix 0. The set $V = \lambda(J)$ is a neighborhood of $\mathbf{J}^\circ$ and of the underlying bimodule. We argue now that U and V are polynomially isomorphic in $\mathbf{J}^\circ$.

Claim 3.9. *The polynomial functions $\lambda|_U : U \to V$ and $\varepsilon|_V : V \to U$ are bijections.*

Since U and V are finite, it is enough to show that the functions are injective. Suppose instead that a and b are distinct elements of U such that $\lambda(a) = \lambda(b)$. Let p be the largest integer such that $a \equiv b \pmod{J^p}$. Since $a, b \in U = \varepsilon(U)$ we have

$$a = \varepsilon(a) = \lambda(a) + \nu(a) = \lambda(b) + \nu(a) \equiv \lambda(b) + \nu(b) = \varepsilon(b) = b \pmod{J^{p+1}},$$

contradicting the choice of p. Similarly, if c and d are distinct elements of $V = \lambda(V)$ such that $\varepsilon(c) = \varepsilon(d)$, then we can choose q to be the largest integer such that $c \equiv d \pmod{J^q}$. As before, we have

$$c = \lambda(c) = \varepsilon(c) - \nu(c) = \varepsilon(d) - \nu(c) \equiv \varepsilon(d) - \nu(d) = \lambda(d) = d \pmod{J^{q+1}}$$

This proves the claim.

Since there are polynomial bijections between U and V, they are polynomially isomorphic. □

4. Minimal Sets in Modules and Bimodules

We have reduced the problem of describing a representative collection of minimal sets in a finite ring $\mathbf{R}$ with radical J to the problem of describing the minimal sets of J considered as an $(\mathbf{R}, \mathbf{R})$-bimodule. In this section we solve the reduced problem.

Theorem 4.1. *Let $\mathbf{R}$ be a finite ring, and let $\mathbf{M}$ be an $\mathbf{R}$-module. The following hold.*

1. *Suppose that $U \subseteq M$ and $|U| > 1$. Then U is a neighborhood of zero if and only if $U = eM$ for some idempotent element $e \in R$.*
2. *If $U = eM$ is a neighborhood of zero, then the induced algebra $\mathbf{M}|_U$ is polynomially equivalent to $e\mathbf{M}$ considered as a module over the ring $e\mathbf{R}e$.*
3. *The neighborhood U is minimal if and only if $U = eM$ for some primitive idempotent e of $\mathbf{R}$.*
4. *Let U be a minimal neighborhood, and let e be a primitive idempotent such that $U = eM$. If $P \prec Q$ are submodules of $\mathbf{M}$, then U is a $\langle P, Q\rangle$-minimal set if and only if $eQ \not\subseteq P$.*

(5) *Suppose that $e, f \in R$ are idempotents, and that $U = eM$ and $V = fM$ are neighborhoods of zero.*
   (i) *If $e \simeq f$, then U is polynomially isomorphic to V.*
   (ii) *If U is polynomially isomorphic to V, and either $\mathbf{M}$ is a faithful $\mathbf{R}$-module or both e and f are primitive, then $e \simeq f$.*

Proof. Any polynomial of $\mathbf{M}$ may be written as

$$p(x_1, \ldots, x_n) = r_1x_1 + \cdots + r_nx_n + a$$

with $r_i \in R$ and $a \in M$. An idempotent unary polynomial of $\mathbf{M}$ whose image contains 0 has this form with $n = 1$ and $a = 0$. If $\varepsilon(x) = rx$ is an idempotent unary polynomial, then the fact that $\varepsilon(\varepsilon(x)) = \varepsilon(x)$ implies that $r^2 - r$ annihilates $\mathbf{M}$. If k is chosen so that $r^k = r^{2k}$, then for $e = r^k$ we have that e is idempotent and $\varepsilon(x) = \varepsilon^k(x) = ex$. This shows that the idempotent unary polynomials that fix 0 have the form $\varepsilon(x) = ex$ for some idempotent $e \in R$. Therefore the neighborhoods of $\mathbf{M}$ containing zero are precisely the sets $U = \varepsilon(M) = eM$ for which $|U| > 1$.

The neighborhood defined by $\varepsilon(x) = ex$ is $U = eM$, and this set is an additive subgroup of $\mathbf{M}$. The polynomial operations of $\mathbf{M}$ that can be restricted to eM are those polynomials $p(x_1, \ldots, x_n) = r_1x_1 + \cdots + r_nx_n + a$ for which $p((eM)^n) \subseteq eM$. Such a polynomial agrees with

$$\varepsilon p(\varepsilon(x_1), \ldots, \varepsilon(x_n)) = (er_1e)x_1 + \cdots + (er_ne)x_n + ea$$

on eM. This is a polynomial of $e\mathbf{M}$ considered as an $e\mathbf{R}e$-module. Conversely, every polynomial of $e\mathbf{M}$ as an $e\mathbf{R}e$-module has this form. Thus $\mathbf{M}|_U$ is polynomially equivalent to $e\mathbf{M}$ considered as an $e\mathbf{R}e$-module.

To prove (3), assume that $U = eM$ is a minimal neighborhood of zero. From Theorem 2.8 (5) we know that we can express e as a sum of pairwise orthogonal primitive idempotents: $e = e_1 + \cdots + e_k$. Since $eM \neq \{0\}$ there is a j such that $e_jM \neq \{0\}$. All idempotents in this orthogonal decomposition of e must be $\leq e$, so we have $\{0\} \subsetneq e_jM = ee_jM \subseteq eM = U$. The minimality of U implies that $U = e_jM$. This proves the forward direction of (3). Conversely, assume that $U = eM$ where e is a primitive idempotent of $\mathbf{R}$. Then $\mathbf{M}|_U$ is polynomially equivalent to a module over the local ring $e\mathbf{R}e$. Since the subneighborhoods of U in $\mathbf{M}$ are exactly the neighborhoods of $\mathbf{M}|_U$, it suffices to cite the remarks preceding Definition 13.7 of [4] (which say that a module over a local ring is E-minimal) to conclude that U is a minimal neighborhood of $\mathbf{M}$.

For (4), assume that $U = eM$ is a $\langle P, Q\rangle$-minimal set. Then there must exist a pair $(a, b) \in \theta_Q|_U - \theta_P$, and since U is an additive subgroup we also have $(a - b, 0) \in \theta_Q|_U - \theta_P$. Hence $a - b \in Q \cap U - P$. Thus $a - b = e(a - b) \in eQ - P$, proving the forward direction of (4). Conversely, if $eQ \not\subseteq P$, then for any $u \in eQ - P$ we have that $(u, 0) \in \theta_Q|_U - \theta_P$. According to Lemma 2.4 this shows that U is $\langle P, Q\rangle$-minimal.

For part (i) of (5), assume that $U = eM, V = fM$ and $e \simeq f$. By Theorem 2.8 (4)(iv) there exist $c, d \in R$ such that $e = cd$ and $f = dc$. The polynomials $f(x) = dx$ and $g(x) = cx$ restrict to inverse bijections $f|_U : U \to V$ and $g|_V : V \to U$, proving that U and V are polynomially isomorphic. For part (ii), assume that $g|_U : U \to V$ and $h|_U : V \to U$ are inverse bijections. If $g(x) = rx + a$ and $h(x) = sx + b$, then $a = g(0) \in V = fM$ (so $fa = a$) and $b = h(0) \in U = eM$ (so $eb = b$). Since $b = eb \in eM = U$, and U is an additive subgroup of M, the polynomial $h'(x) = x - b$ is a polynomial permutation of U. We can compose $h(x) = sx + b$ with $eh'(x) = e(x - b)$ to get a polynomial $eh' \circ h(x) = h''(x) = esx$ that fixes zero and is a bijection $h''|_V : V \to U$. Similarly $g''(x) = frx$ fixes zero and is a bijection from U to V. As argued after Definition 2.1, there is an integer n for which the polynomials g'' and $h'' \circ (g'' \circ h'')^{2n-1}$ are inverse bijections between U and V. Therefore we may start the argument over assuming that $g(x) = erx$ and $h(x) = fsx$ are inverse bijections between U and V. Now, for any $m \in M$ we have $em \in U$, so $em = g(h(em)) = erfsem$. Similarly, for any $m \in M$ we have $fm = fserfm$. If $\mathbf{M}$ is a faithful $\mathbf{R}$-module, then these facts imply that $e = erfse$ and $f = fserf$. It follows from the equivalence of (i) and (ii) (or (iii)) of Theorem 2.8 (4) that $e \simeq f$ in the case when $\mathbf{M}$ is a faithful module. In the case that e and f are primitive and not isomorphic, then $eRf \subseteq J$ by Theorem 2.8 (4)(v). Hence, for integers k exceeding the nilpotence degree of J we get $em = erfsem = (erfs)^k em \in J^k M = \{0\}$ for all $m \in M$. This is impossible since $eM = U \neq \{0\}$. Hence we must have $e \simeq f$ when e and f are primitive. □

If $P \subseteq Q$ are submodules of $\mathbf{M}$, then the set $(P : Q)_{\mathbf{R}} = \{r \in R \mid rQ \subseteq P\}$ is a 2-sided ideal in $\mathbf{R}$ called *the annihilator of* $\langle P, Q\rangle$. We drop the subscript when it is clear which ring is involved. The ring $\mathbf{R}/(P : Q)$ acts faithfully on the quotient module Q/P. If $P \prec Q$, then Q/P is simple, so $\mathbf{R}/(P : Q)$ is a finite primitive ring. Such rings are simple by the Jacobson Density Theorem. This shows that $(P : Q)$ is a maximal ideal whenever $\mathbf{R}$ is finite and $P \prec Q$. Part (4) of the previous theorem shows that a $\langle P, Q\rangle$-minimal set of the module $\mathbf{M}$ is $U = eM$ for some primitive idempotent $e \in R - (P : Q)$. According to Theorem 2.8 (4)(vi) and part (5) of the previous theorem, if f is any other primitive idempotent in $R - (P : Q)$, then $e \simeq f$ and fM is also a $\langle P, Q\rangle$-minimal set. Therefore, if we fix a representation $1 = e_1 + \cdots + e_k$ of 1 as a sum of pairwise orthogonal primitive idempotents, then each $e_i M$ is either $\{0\}$ or a minimal set, and every minimal set of $\mathbf{M}$ is polynomially isomorphic to a set on the list: $e_1 M, \ldots, e_k M$. (Here we are using Theorem 2.8 (6), that every primitive idempotent is isomorphic to one of the e_i's, and Theorem 4.1 (5), that isomorphic primitive idempotents determine polynomially isomorphic neighborhoods.) Therefore, the previous theorem explains everything one needs to know in order to determine a representative set of minimal sets in any

module over a finite ring. We now explain how to use this theorem to determine the minimal sets in any $(\mathbf{R}, \mathbf{S})$-bimodule, when $\mathbf{R}$ and $\mathbf{S}$ are finite rings.

Recall from Definition 2.11 that a bimodule is an abelian group together with specified homomorphisms $\mathcal{L} : \mathbf{R} \to \mathrm{End}(\mathbf{M})$ and $\mathcal{R} : \mathbf{S}^{op} \to \mathrm{End}(\mathbf{M})$ such that $\mathcal{L}(r) \circ \mathcal{R}(s) = \mathcal{R}(s) \circ \mathcal{L}(r)$ for all $r \in R$ and $s \in S$. By the universal property of tensor products (cf. [6], pages 143-144),[2] the pair of homomorphisms $(\mathcal{L}, \mathcal{R})$ factors uniquely through a ring homomorphism

$$\mathcal{L} \otimes \mathcal{R} : \mathbf{R} \otimes \mathbf{S}^{op} \to \mathrm{End}(\mathbf{M})$$

defined on basic tensors by $\mathcal{L} \otimes \mathcal{R}(r \otimes s)(x) = rxs$. Such a homomorphism uniquely determines a left $\mathbf{R} \otimes \mathbf{S}^{op}$-module structure on $\mathbf{M}$. Conversely, a left $\mathbf{R} \otimes \mathbf{S}^{op}$-module structure on $\mathbf{M}$ is determined by a homomorphism $\mathcal{H} : \mathbf{R} \otimes \mathbf{S}^{op} \to \mathrm{End}(\mathbf{M})$. Composing such a homomorphism $\mathcal{H}$ with the natural homomorphisms

$$\mathcal{T}_1 : \mathbf{R} \to \mathbf{R} \otimes \mathbf{S}^{op} : r \mapsto r \otimes 1$$

and

$$\mathcal{T}_2 : \mathbf{S}^{op} \to \mathbf{R} \otimes \mathbf{S}^{op} : s \mapsto 1 \otimes s$$

produces homomorphisms $\mathcal{L} = \mathcal{H} \circ \mathcal{T}_1 : \mathbf{R} \to \mathrm{End}(\mathbf{M})$ and $\mathcal{R} = \mathcal{H} \circ \mathcal{T}_2 : \mathbf{S}^{op} \to \mathrm{End}(\mathbf{M})$, whose images commute. Hence a left $\mathbf{R} \otimes \mathbf{S}^{op}$-module structure on $\mathbf{M}$ induces a natural $(\mathbf{R}, \mathbf{S})$-bimodule structure on $\mathbf{M}$. By examining this correspondence, it is not hard to prove that the algebra that is $\mathbf{M}$ considered as an $(\mathbf{R}, \mathbf{S})$-bimodule is definitionally equivalent[3] to the algebra that is $\mathbf{M}$ considered as an $\mathbf{R} \otimes \mathbf{S}^{op}$-module. Concretely, the unary module polynomial $(r_1 \otimes s_1 + \cdots + r_k \otimes s_k)x + t$ corresponds to the unary bimodule polynomial $r_1 x s_1 + \cdots + r_k x s_k + t$.

Using the correspondence just described we can reduce the problem of computing minimal sets in $(\mathbf{R}, \mathbf{S})$-bimodules to the problem solved in Theorem 4.1.

Corollary 4.2. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite rings, and let $\mathbf{M}$ be an $(\mathbf{R}, \mathbf{S})$-bimodule. If $P \prec Q$ are subbimodules of $\mathbf{M}$, then $P \prec Q$ in the $(\mathbf{R} \otimes \mathbf{S}^{op})$-submodule lattice. If $e \in \mathbf{R} \otimes \mathbf{S}^{op}$ is a primitive idempotent, and $e \notin (P : Q)$, then $U = eM$ is a $\langle P, Q \rangle$-minimal set of $\mathbf{M}$ (considered as a module or a bimodule). The induced algebra $\mathbf{M}|_U$ is polynomially equivalent to $e\mathbf{M}$ considered as a module over the local ring $e(\mathbf{R} \otimes \mathbf{S}^{op})e$.*

This corollary may be slightly unsatisfying because it reduces the calculation of minimal sets of an $(\mathbf{R}, \mathbf{S})$-bimodule $\mathbf{M}$ to the calculation of primitive idempotents of the ring $\mathbf{R} \otimes \mathbf{S}^{op}$ rather than to calculations in $\mathbf{R}$ and $\mathbf{S}$ individually. So, let us spend a few paragraphs describing how to locate a representative set of primitive idempotents of $\mathbf{R} \otimes \mathbf{S}^{op}$, and how to calculate the corresponding minimal sets in $\mathbf{M}$.

[2] In this paper all tensor products are over $\mathbb{Z}$.

[3] Algebras $\mathbf{A}$ and $\mathbf{B}$ are *definitionally equivalent* if they have the same universe and the same clone of term operations.

We start with an algebra $\mathbf{M}$ considered simultaneously as an $(\mathbf{R}, \mathbf{S})$-bimodule and an $\mathbf{R} \otimes \mathbf{S}^{op}$-module. Our goal is to describe how to locate at least one $\langle P, Q\rangle$-minimal set for each covering pair $P \prec Q$ of sub(bi)modules of $\mathbf{M}$. Let $1 = e_1 + \cdots + e_m$ be a representation of $1_{\mathbf{R}}$ as a sum of primitive, orthogonal idempotents in $\mathbf{R}$, and let $1 = f_1 + \cdots + f_n$ be a representation of $1_{\mathbf{S}}$ as a sum of primitive, orthogonal idempotents in $\mathbf{S}$. Then

$$1_{\mathbf{R}\otimes\mathbf{S}^{op}} = 1_{\mathbf{R}} \otimes 1_{\mathbf{S}^{op}} = (e_1 + \cdots + e_m) \otimes (f_1 + \cdots + f_n) = \sum_{i,j} e_i \otimes f_j$$

expresses 1 as a sum of orthogonal idempotents of the form $E_{ij} = e_i \otimes f_j$. Usually these idempotents are not primitive, so to find all minimal sets the decomposition $1 = \sum E_{ij}$ must be refined. This can be done one idempotent at a time. If we are interested in $\langle P, Q\rangle$-minimal sets for a fixed prime quotient $\langle P, Q\rangle$ only, we need to determine which of the E_{ij}'s we need to refine.

Since $P \prec Q$, we get that Q/P is simple as an $\mathbf{R} \otimes \mathbf{S}^{op}$-module. Let N be an $\mathbf{R}$-submodule of $\mathbf{M}$ such that $P \prec N \leq Q$ as $\mathbf{R}$-modules. For each $s \in S$ we get that $(N/P)s$ is trivial or is isomorphic to the $\mathbf{R}$-submodule N/P of Q/P. The sum $\sum_{s\in S}(N/P)s$ is a nontrivial $(\mathbf{R}, \mathbf{S})$-subbimodule of the simple bimodule Q/P, hence it equals Q/P. This shows that Q/P is a sum of isomorphic copies of the simple $\mathbf{R}$-module N/P. It follows from this that, considering $\mathbf{M}$ as an $\mathbf{R}$-module only, $(P : Q)_{\mathbf{R}} = (P : N)_{\mathbf{R}}$ is a maximal ideal of $\mathbf{R}$. Similarly, considering $\mathbf{M}$ as an $\mathbf{S}^{op}$-module only, $(P : Q)_{\mathbf{S}^{op}}$ is a maximal ideal in $\mathbf{S}^{op}$. If an idempotent $E_{ij} = e_i \otimes f_j$ (as described in the previous paragraph) satisfies $E_{ij}Q = e_iQf_j \not\subseteq P$, then it must satisfy $e_iQ \not\subseteq P$ (or $e_i \notin (P : Q)_{\mathbf{R}}$) and $Qf_j \not\subseteq P$ (or $f_j \notin (P : Q)_{\mathbf{S}^{op}}$). Any other idempotent $E_{uv} = e_u \otimes f_v$ satisfying $e_u \notin (P : Q)_{\mathbf{R}}$ and $f_v \notin (P : Q)_{\mathbf{S}^{op}}$, must be isomorphic to E_{ij} for the following reasons: e_i and e_u are primitive, $(P : Q)_{\mathbf{R}}$ is a maximal ideal of $\mathbf{R}$, and $e_i, e_u \notin (P : Q)$, so by Theorem 2.8 (4) there exist p, q, r and s such that $e_i = pe_uq$ and $e_u = re_is$; similarly there exist p', q', r' and s' such that $f_j = p'f_vq'$ and $f_v = r'f_js'$. Hence

$$E_{ij} = (p \otimes p')E_{uv}(q \otimes q') \text{ and } E_{uv} = (r \otimes r')E_{ij}(s \otimes s'),$$

which shows that $E_{ij} \simeq E_{uv}$. In particular, $e_i \otimes f_j \notin (P : Q)_{\mathbf{R}\otimes\mathbf{S}^{op}}$ iff $e_i \notin (P : Q)_{\mathbf{R}}$ and $f_j \notin (P : Q)_{\mathbf{S}^{op}}$.

We now have that there is only one $E_{ij} \in R\otimes S^{op} - (P : Q)_{\mathbf{R}\otimes\mathbf{S}^{op}}$ up to isomorphism. For any such idempotent $E_{ij}Q \not\subseteq P$, so the function $\varepsilon(x) = E_{ij}x = e_ixf_j$ does not collapse Q into P. Thus $U = \varepsilon(M) = e_iMf_j$ contains a $\langle P, Q\rangle$-minimal set. The induced algebra $\mathbf{M}|_U$ is polynomially equivalent to a module over the ring

$$E_{ij}(\mathbf{R} \otimes \mathbf{S}^{op})E_{ij} = (e_i \otimes f_j)(\mathbf{R} \otimes \mathbf{S}^{op})(e_i \otimes f_j) = (e_i\mathbf{R}e_i) \otimes (f_j\mathbf{S}f_j)^{op}.$$

Since U is a neighborhood and $E_{ij}Q \not\subseteq P$ we get that $P|_U \prec Q|_U$. By Lemma 2.4, any $\langle P|_U, Q|_U\rangle$-minimal set V of $\mathbf{M}|_U$ will be a $\langle P, Q\rangle$-minimal set of $\mathbf{M}$. To locate such a minimal set V we need to locate the primitive idempotents of $(e_i\mathbf{R}e_i) \otimes (f_j\mathbf{S}f_j)^{op}$.

Since e_i and f_j are primitive idempotents in $\mathbf{R}$ and $\mathbf{S}$, Theorem 2.8 (1) proves that the rings $\widehat{\mathbf{R}} = e_i\mathbf{R}e_i$ and $\widehat{\mathbf{S}} = f_j\mathbf{S}f_j$ are local. To summarize: for some idempotent $E_{ij} = e_i \otimes f_j$, which is unique up to isomorphism, the neighborhood $U = E_{ij}M = e_iMf_j$ contains a $\langle P, Q\rangle$-minimal set V. The set V equals $\varepsilon(U)$ where $\varepsilon(x) = ex$ for some primitive idempotent $e \in \widehat{\mathbf{R}} \otimes \widehat{\mathbf{S}}^{op}$. Here the rings $\widehat{\mathbf{R}}$ and $\widehat{\mathbf{S}}$ are local. Thus, we have reduced the general problem of finding minimal sets in modules over a finite ring of the form $\mathbf{R} \otimes \mathbf{S}^{op}$ to the case when $\mathbf{R}$ and $\mathbf{S}$ are local.

We now focus on the problem of computing primitive idempotents in a tensor product of two local rings $\mathbf{R}$ and $\mathbf{S}$. Tensor products of local rings are easier to understand when the rings are commutative, so we explain how to reduce to that case. Our strategy will be to choose subrings $\mathbf{R}' \leq \mathbf{R}$ and $\mathbf{S}' \leq \mathbf{S}$ which are small enough that they are commutative, but large enough so that the subring $\mathbf{R}' \otimes \mathbf{S}'$ of $\mathbf{R} \otimes \mathbf{S}$ contains a complete orthogonal decomposition of 1 as a sum of idempotents that are primitive in $\mathbf{R} \otimes \mathbf{S}$. For this purpose, it will be useful to recall the definition of a Galois ring.

Definition 4.3. A *Galois ring* is any ring $\mathrm{GR}(p^n, d)$ isomorphic to a ring of the form $\mathbb{Z}_{p^n}[x]/(m(x))$, where $m(x)$ is a monic integer polynomial of degree d that is irreducible modulo p.

By Theorem XVII.1 of [12], any finite local ring $\mathbf{R}$ contains a unique Galois subring $\mathbf{R}'$ which has the same residue field as $\mathbf{R}$. That is, if $\nu : \mathbf{R} \to \mathbf{R}/J$ is the natural homomorphism, then $\mathbf{R}$ contains a unique Galois subring $\mathbf{R}'$ such that $\nu|_{R'} : \mathbf{R}' \to \mathbf{R}/J$ is surjective. This uniqueness, together with Lemma XV.1 of [12], implies that the ring $\mathbb{Z}_{p^n}[x]/(m(x))$ is isomorphic to $\mathbb{Z}_{p^n}[x]/(n(x))$ if both $m(x)$ and $n(x)$ are monic integer polynomials of degree d that are irreducible modulo p. So, (as the notation suggests) a Galois ring $\mathrm{GR}(p^n, d)$ is determined by its characteristic p^n and the isomorphism type of its residue field (a finite field of size p^d).

Assume that the Galois subring of $\mathbf{R}$ that has the same residue field is $\mathrm{GR}(p^i, a)$ and the Galois subring of $\mathbf{S}$ that has the same residue field is $\mathrm{GR}(p^j, b)$. (There is no loss of generality in assuming that the charactistics are powers of the same prime, since it is easy to show that the tensor product of two finite rings $\mathbf{R}$ and $\mathbf{S}$ is zero if their characteristics are relatively prime. This situation could never arise if there exists a nonzero $(\mathbf{R}, \mathbf{S})$-bimodule, as we are assuming.) We claim that the subring $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$ of the ring $\mathbf{R} \otimes \mathbf{S}$ has the same idempotent structure as the full ring. To see this, observe that if J is the radical of $\mathbf{R}$ and K is the radical of $\mathbf{S}$, then $I = J \otimes S + R \otimes K$ is a nilpotent ideal of $\mathbf{R} \otimes \mathbf{S}$, and the quotient modulo this ideal is $\mathbf{R}/J \otimes \mathbf{S}/K$. The subrings $\mathrm{GR}(p^i, a) \leq \mathbf{R}$ and $\mathrm{GR}(p^j, b) \leq \mathbf{S}$ have the same residue fields $\mathbf{R}/J$ and $\mathbf{S}/K$, so the restriction of I to $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$ is a nilpotent ideal whose quotient is $\mathbf{R}/J \otimes \mathbf{S}/K$. The idempotent structure of a ring is not changed by forming the quotient modulo a nilpotent ideal since, if $1 = e_1 + \cdots + e_k$ is a representation of 1 as a sum of orthogonal idempotents that are

primitive in $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$, then modulo I the representation $\bar{1} = \bar{e}_1 + \cdots + \bar{e}_k$ expresses $\bar{1}$ as a sum of orthogonal idempotents that are primitive in $\mathbf{R}/J \otimes \mathbf{S}/K$ (see Theorem 2.8 (8)). This representation can be pulled back to a representation $f = f_1 + \cdots + f_k$ in $\mathbf{R} \otimes \mathbf{S}$ of an idempotent $f \in 1 + I$ as a sum of orthogonal primitive idempotents (see Theorem 2.8 (7)). The set $1 + I$ consists of units (Theorem 2.6 (3) and (4)), so the idempotent unit f must equal 1. This shows that a representation of 1 as a sum of orthogonal primitive idempotents in $\mathbf{R} \otimes \mathbf{S}$ uses the same number of idempotents as a representation in the subring $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$. By the remarks following the proof of Theorem 2.8, it follows that idempotents primitive in $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$ are primitive in $\mathbf{R} \otimes \mathbf{S}$.

The following theorem is a useful tool for computing primitive idempotents in $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$.

Theorem 4.4. (Theorem XVI.8 of [12]) *If a, b, i and j are positive integers, and p is a prime, then $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b) \cong \big(\mathrm{GR}(p^k, c)\big)^d$ where $c = \mathrm{lcm}(a, b)$, $d = \gcd(a, b)$ and $k = \min(i, j)$.*

In the proof of Theorem 2.8 (6) it is noted that any two representations of 1 as a sum of pairwise orthogonal primitive idempotents are conjugate. Therefore in a commutative ring any complete orthogonal representation of 1 is unique; the representation is uniquely determined by the direct factorization of the ring into indecomposable rings. The previous theorem shows that $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b) \cong \big(\mathrm{GR}(p^k, c)\big)^d$ is a d-th power of a local (hence indecomposable) ring, so the number of primitive idempotents in the complete orthogonal representation of 1 must be d. It would not be very hard to explain how to calculate those idempotents right now, but we prefer to introduce one more simplification first.

By Lemma XVI.7 of [12], every subring of $\mathrm{GR}(p^m, n)$ has the form $\mathrm{GR}(p^m, d)$ for some divisor d of n. Moreover, there is exactly one such subring for each d dividing n: it is $\pi^{-1}(H)$ where $\pi : \mathrm{GR}(p^m, n) \to \mathrm{GR}(p, n)$ is reduction modulo the radical, (p), and H is the unique subfield of $\mathrm{GR}(p, n)$ of degree d over the prime subfield. Thus, for $d = \gcd(a, b)$, our ring $\mathrm{GR}(p^i, a)$ has a unique subring isomorphic to $\mathrm{GR}(p^i, d)$, while $\mathrm{GR}(p^j, b)$ has a unique subring isomorphic to $\mathrm{GR}(p^j, d)$. By symmetry, no generality is lost by assuming that $i \leq j$, so we make that assumption. Applying Theorem 4.4 to the subring $\mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d)$ of $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$, we find that it is also isomorphic to a direct product of d local rings:

$$\mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d) \cong \big(\mathrm{GR}(p^i, d)\big)^d.$$

It follows that the unique representation of 1 as a sum of pairwise orthogonal primitive idempotents in $\mathrm{GR}(p^i, a) \otimes \mathrm{GR}(p^j, b)$ consists of idempotents lying in the subring $\mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d)$.

A list of d orthogonal idempotents that sum to 1 in $\mathrm{GR}(p^i, d)^d$ is $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0), \ldots, e_d = (0, 0, \ldots, 1)$. Since this is the right number for a complete

decomposition in a product of d local rings, $1 = e_1 + \cdots + e_d$ is the unique representation of 1 as a sum of pairwise orthogonal primitive idempotents in this ring. The isomorphism

$$\big(\mathrm{GR}(p^i, d)\big)^d \cong \mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d)$$

may be used to transfer this information about idempotents from the ring on the left to the one on the right.

The transfer of information will be mediated by two homomorphisms φ and ψ. To define the first, let $m(x)$ be a monic integer polynomial of degree d that is irreducible modulo p. By Hensel's Lemma (Theorem XIII.4 of [12]), $m(x) = 0$ has exactly d roots in each of $\mathrm{GR}(p^i, d)$ and $\mathrm{GR}(p^j, d)$, and these roots in either ring are inequivalent modulo the radical of the ring. Let $\alpha_1, \ldots, \alpha_d$ be the roots in $\mathrm{GR}(p^i, d)$, and let β be a root in $\mathrm{GR}(p^j, d)$. Let φ be the homomorphism

$$\varphi : \mathrm{GR}(p^i, d)[x] \to \mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d)$$

determined by $\varphi(c) = c \otimes 1$ if $c \in \mathrm{GR}(p^i, d)$ and $\varphi(x) = 1 \otimes \beta$. The element β generates $\mathrm{GR}(p^j, d)$ (since the subring generated β has the same characteristic and residue field as the full ring), therefore the image of φ contains each of the subrings $\mathrm{GR}(p^i, d) \otimes 1$ and $1 \otimes \mathrm{GR}(p^j, d)$. It follows that φ maps onto $\mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d)$. The kernel of φ contains the ideal $(m(x))$, so the induced homomorphism

$$\overline{\varphi} : \mathrm{GR}(p^i, d)[x]/(m(x)) \to \mathrm{GR}(p^i, d) \otimes \mathrm{GR}(p^j, d)$$

exists, and is surjective. But since m is monic of degree d,

$$|\mathrm{GR}(p^i, d)[x]/(m(x))| = |\mathrm{GR}(p^i, d)|^d,$$

which is the cardinality of the image of $\overline{\varphi}$. It follows that $(m(x))$ is the kernel of φ (and therefore that $\overline{\varphi}$ is an isomorphism).

Next we define ψ. The polynomial $m(x)$ factors completely as $m(x) = (x - \alpha_1) \cdots (x - \alpha_d)$ over $\mathrm{GR}(p^i, d)$. Since the roots are inequivalent modulo the radical, different factors $(x - \alpha_j)$ and $(x - \alpha_k)$ are relatively prime. By the Chinese Remainder Theorem, the function

$$\psi : \mathrm{GR}(p^i, d)[x] \to \mathrm{GR}(p^i, d)^d : f(x) \mapsto (f(\alpha_1), \ldots, f(\alpha_d))$$

is a surjective homomorphism with kernel $(m(x))$. We let $\overline{\psi}$ name the induced isomorphism: $\overline{\psi} : \mathrm{GR}(p^i, d)[x]/(m(x)) \to \mathrm{GR}(p^i, d)^d$.

We now have the following diagram:

$$\begin{array}{ccccc} & & \mathrm{GR}(p^i,d)[x] & & \\ & \overset{\psi}{\swarrow} & \downarrow & \overset{\varphi}{\searrow} & \\ \mathrm{GR}(p^i,d)^d & \overset{\overline{\psi}}{\leftarrow} & \mathrm{GR}(p^i,d)[x]/(m(x)) & \overset{\overline{\varphi}}{\rightarrow} & \mathrm{GR}(p^i,d)\otimes \mathrm{GR}(p^j,d) \end{array}$$

where the vertical homomorphism is the natural one. We will use the isomorphism $\overline{\varphi}\circ\overline{\psi}^{-1} = \varphi\circ\psi^{-1}$ to transfer the information about idempotents from the leftmost ring to the rightmost.

For $j = 1,\dots,d$, let $m_j(x) = \prod_{k\neq j}(x-\alpha_k) = m(x)/(x-\alpha_j)$. Since no two roots α_j and α_k are equivalent modulo the radical of $\mathrm{GR}(p^i,d)$, the element $m_j(\alpha_j) = \prod_{k\neq j}(\alpha_j-\alpha_k)$ is a product of units. Hence $m_j(\alpha_j)$ is a unit in $\mathrm{GR}(p^i,d)$ for each j. We claim that for $j = 1,\dots,d$ the polynomials $E_j(x) = m_j(x)m_j^{-1}(\alpha_j) \in \mathrm{GR}(p^i,d)[x]$ satisfy $\psi(E_j(x)) = e_j$. To prove that

$$\psi(E_j(x)) = \psi(m_j(x)m_j^{-1}(\alpha_j)) = e_j = (0,\dots,\underbrace{1}_{j\text{-th}},\dots,0)$$

we check coordinatewise: the j-th coordinate of $\psi(m_j(x)m_j^{-1}(\alpha_j))$ is $m_j(\alpha_j)m_j^{-1}(\alpha_j) = 1$. The k-th coordinate for $k\neq j$ is $m_j(\alpha_k)m_j^{-1}(\alpha_j) = 0$ since $m_j(\alpha_k) = 0$. Thus, indeed, $\psi(E_j(x)) = \psi(m_j(x)m_j^{-1}(\alpha_j)) = e_j$.

If we set $\varepsilon_j = \varphi(E_j(x)) = \overline{\varphi}\circ\overline{\psi}^{-1}(e_j)$, then we have shown that $\varepsilon_1,\dots,\varepsilon_d$ are the idempotents in $\mathrm{GR}(p^i,d)\otimes\mathrm{GR}(p^j,d)$ that correspond to $e_1,\dots,e_d$ under the isomorphism $\overline{\varphi}\circ\overline{\psi}^{-1}$. These idempotents have been calculated explicitly from a factorization of $m(x)$.

To calculate the minimal sets in an $(\mathbf{R},\mathbf{S})$-bimodule $\mathbf{M}$, when $\mathbf{R}$ and $\mathbf{S}$ are local rings, we would first apply the procedure just described to compute the primitive idempotents $\varepsilon_1,\dots,\varepsilon_d$ of $\mathbf{R}\otimes\mathbf{S}^{op}$. A complete list of minimal sets up to polynomial isomorphism can be found among the sets $\varepsilon_1 M,\dots,\varepsilon_d M$.

Example. The purpose of this example is to illustrate all details of the calculation of minimal sets in a finite ring.

Let $\mathbb{E},\mathbb{F}$ and $\mathbb{G}$ be Galois rings of the form $\mathbb{E} = \mathrm{GR}(4,8)$, $\mathbb{F} = \mathrm{GR}(4,12)$ and $\mathbb{G} = \mathrm{GR}(4,4)$, with $\mathbb{G}$ a common subring of $\mathbb{E}$ and $\mathbb{F}$. Let $\mathbf{M}$ be a faithful $(\mathbb{E},\mathbb{F})$-bimodule. All nontrivial details of the calculation of minimal sets in a finite ring are

illustrated by the calculation of the minimal sets in the triangular ring

$$\mathbf{R} = \left\{ \left[\begin{array}{cc} g & m \\ 0 & h \end{array} \right] \;\middle|\; g \in \mathbb{E}, h \in \mathbb{F}, m \in M \right\}.$$

(The ring operations are the ordinary matrix ring operations.) It is not hard to see that

$$J = \left\{ \left[\begin{array}{cc} g & m \\ 0 & h \end{array} \right] \;\middle|\; g \in 2\mathbb{E}, h \in 2\mathbb{F}, m \in M \right\}$$

is an ideal satisfying $J^3 = 0$. Since $\mathbf{R}/J \cong (\mathbb{E}/2\mathbb{E}) \times (\mathbb{F}/2\mathbb{F})$ is a product of two finite fields it is a semisimple ring; consequently J is the radical of $\mathbf{R}$. Since $1 \in \mathbf{R}/J \cong \mathbb{E}/2\mathbb{E} \times \mathbb{F}/2\mathbb{F}$ is expressible as a sum of two orthogonal primitive idempotents in this ring, any representation of $1 \in \mathbf{R}$ as a sum of two nonzero orthogonal idempotents involves only primitive idempotents. It must be that for

$$I = \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right], \quad E = \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right], \quad F = \left[\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array} \right]$$

the expression $I = E + F$ is a representation of $I = 1_{\mathbf{R}}$ as a sum of orthogonal primitive idempotents. From Theorem 2.9, the sets $\{0, E\}$ and $\{0, F\}$ represent all minimal sets of nonabelian type in $\mathbf{R}$ up to polynomial isomorphism.

From the remarks following Corollary 4.2, we know that each minimal set of abelian type is polynomially isomorphic to a minimal set in J considered as an $(\mathbf{R}, \mathbf{R})$-bimodule. In fact, as we explained there, the decomposition

$$1_{\mathbf{R} \otimes \mathbf{R}^{op}} = I \otimes I = E \otimes E + E \otimes F + F \otimes E + F \otimes F$$

allows us to limit our search to the neighborhoods EJE, EJF, FJE and FJF. Every minimal set of abelian type is polynomially isomorphic to a minimal set of

(1) the $(E\mathbf{R}E, E\mathbf{R}E)$-bimodule EJE,
(2) the $(E\mathbf{R}E, F\mathbf{R}F)$-bimodule EJF,
(3) the $(F\mathbf{R}F, E\mathbf{R}E)$-bimodule FJE, or
(4) the $(F\mathbf{R}F, F\mathbf{R}F)$-bimodule FJF.

Since $FJE = \{0\}$, there are no minimal sets Case (3). Cases (1) and (4) are handled in the same way, so we discuss only Cases (1) and (2).

The ring $E\mathbf{R}E$ is

$$E\mathbf{R}E = \left\{ \left[\begin{array}{cc} g & 0 \\ 0 & 0 \end{array} \right] \;\middle|\; g \in \mathbb{E} \right\},$$

and projection onto the $1,1$-position is an isomorphism onto $\mathbb{E}$. We leave it to the reader to verify that the $(E\mathbf{R}E, E\mathbf{R}E)$-bimodule EJE is definitionally equivalent to the ideal $2\mathbb{E}$ considered as a $(\mathbb{E}, \mathbb{E})$-bimodule. But since $\mathbb{E}$ is a commutative ring the left action agrees with the right action, and so this algebra is definitionally equivalent

to $2\mathbb{E}$ as an $\mathbb{E}$-module. Since $\mathbb{E}$ is local, Theorem 4.1 (1) implies that $2\mathbb{E}$ is the only minimal set contained in $2\mathbb{E}$. Thus, in Case (1) we get that EJE itself is a minimal set. (In Case (4), FJF is a minimal set.)

Now we discuss Case (2). We leave it to the reader to verify that the $(E\mathbf{R}E, F\mathbf{R}F)$-bimodule EJF is definitionally equivalent to $\mathbf{M}$ as an $(\mathbb{E}, \mathbb{F})$-bimodule. The problem of computing a representative list of (ring) minimal sets contained in EJF is equivalent to the problem of computing the minimal sets of $\mathbf{M}$ considered as an $(\mathbb{E}, \mathbb{F})$-bimodule, and this reduces to the problem of computing the primitive idempotents in $\mathbb{E} \otimes \mathbb{F}^{op} = \mathbb{E} \otimes \mathbb{F}$. As explained after Theorem 4.4, all primitive idempotents of the tensor product of two commutative local rings lie in the tensor product of Galois subrings with common residue field. In particular, the primitive idempotents of $\mathbb{E} \otimes \mathbb{F}$ lie in $\mathbb{G} \otimes \mathbb{G}$. Since $\mathbb{G} = \mathrm{GR}(4, 4)$, the prime ring of $\mathbb{G}$ is $\mathbb{Z}_4$. Since $m(x) = x^4 + x + 1$ is irreducible modulo 4, the left copy of $\mathbb{G}$ in $\mathbb{G} \otimes \mathbb{G}$ may be represented as $\mathbb{Z}_4[\alpha]$ where α is a root of $m(x) = 0$ in $\mathbb{G}$. The right copy of $\mathbb{G}$ may be represented as $\mathbb{Z}_4[\beta]$ where β is also a root of $m(x) = 0$ in $\mathbb{G}$.

Using MAPLE, we found that if $\alpha_1 = \alpha$ is a root of $m(x) = 0$ in $\mathbb{G}$, then the other three roots are $\alpha_2 = 3\alpha^2 + 2\alpha + 2$, $\alpha_3 = 2\alpha^2 + \alpha + 3$, and $\alpha_4 = 3\alpha^2 + 3$. Following the discussion immediately preceding this example, we define

$$\begin{aligned}
m_1(x) &= m(x)/(x - \alpha_1) = \; x^3 + \alpha x^2 + \alpha^2 x + \alpha^3 + 1 \\
m_2(x) &= m(x)/(x - \alpha_2) = \; x^3 + (3\alpha^2 + 2\alpha + 2)x^2 + (3\alpha + 3)x \\
&\qquad\qquad\quad +(\alpha^3 + 3\alpha^2 + 3) \\
m_3(x) &= m(x)/(x - \alpha_3) = \; x^3 + (2\alpha^2 + \alpha + 3)x^2 + (\alpha^2 + 2\alpha + 1)x \\
&\qquad\qquad\quad +(\alpha^3 + 3\alpha^2 + \alpha + 2) \\
m_4(x) &= m(x)/(x - \alpha_4) = \; x^3 + (3\alpha^2 + 3)x^2 + (2\alpha^2 + 3\alpha)x \\
&\qquad\qquad\quad +(\alpha^3 + 2\alpha^2 + 3\alpha + 3).
\end{aligned}$$

By our earlier arguments, the primitive idempotents of $\mathbb{G}[x]/(m(x))$ ($\cong \mathbb{G} \otimes \mathbb{G}$) are the elements $E_j(x) = m_j(x)m_j^{-1}(\alpha_j)$. This is easier to calculate than it appears, since $m_j(\alpha_j) = m'(\alpha_j)$ where $m'(x) = 4x^3 + 1 = 1$ is the derivative of $m(x)$ in $\mathbb{Z}_4$. Thus, $E_j(x) = m_j(x)m_j^{-1}(\alpha_j) = m_j(x)$. The primitive idempotents in $\mathbb{G} \otimes \mathbb{G}$ are just $\varepsilon_1, \ldots, \varepsilon_4$, where $\varepsilon_i = \varphi(E_i(x))$ and φ is the function that modifies a polynomial $E_i(x)$ by replacing each coefficient c with $c \otimes 1$ and each x with $1 \otimes \beta$. Thus, the 4 primitive idempotents in $\mathbb{G} \otimes \mathbb{G}$ are:

$$\begin{aligned}
\varepsilon_1 &= \; 1 \otimes \beta^3 + \alpha \otimes \beta^2 + \alpha^2 \otimes \beta + (\alpha^3 + 1) \otimes 1 \\
\varepsilon_2 &= \; 1 \otimes \beta^3 + (3\alpha^2 + 2\alpha + 2) \otimes \beta^2 + (3\alpha + 3) \otimes \beta + (\alpha^3 + 3\alpha^2 + 3) \otimes 1 \\
\varepsilon_3 &= \; 1 \otimes \beta^3 + (2\alpha^2 + \alpha + 3) \otimes \beta^2 + (\alpha^2 + 2\alpha + 1) \otimes \beta + (\alpha^3 + 3\alpha^2 + \alpha + 2) \otimes 1 \\
\varepsilon_4 &= \; 1 \otimes \beta^3 + (3\alpha^2 + 3) \otimes \beta^2 + (2\alpha^2 + 3\alpha) \otimes \beta + (\alpha^3 + 2\alpha^2 + 3\alpha + 3) \otimes 1.
\end{aligned}$$

Each idempotent $\varepsilon_i \in \mathbb{G} \otimes \mathbb{G} \leq \mathbb{E} \otimes \mathbb{F}$ determines a set $U_i = \varepsilon_i M$ which, since $\mathbf{M}$ is a faithful $(\mathbb{E}, \mathbb{F})$-bimodule, is not just $\{0\}$. Thus, each U_i is a minimal set of $\mathbf{M}$ considered as an $(\mathbb{E}, \mathbb{F})$-bimodule. Up to polynomial isomorphism, the neighborhoods

U_1, U_2, U_3 and U_4 represent all minimal sets of the ring $\mathbf{R}$ that are contained in EJF (Case 2).

The idempotent element $\varepsilon_3 = 1 \otimes \beta^3 + (2\alpha^2 + \alpha + 3) \otimes \beta^2 + (\alpha^2 + 2\alpha + 1) \otimes \beta + (\alpha^3 + 3\alpha^2 + \alpha + 2) \otimes 1 \in \mathbb{E} \otimes \mathbb{F}$ determines a polynomial $\varepsilon(X) = \varepsilon_3 \cdot X$ of the $\mathbb{E} \otimes \mathbb{F}$-module $\mathbf{M}$ whose image is U_3. The corresponding $(\mathbb{E}, \mathbb{F})$-bimodule polynomial whose image is U_3 is easy to write down: replace each basic tensor $\alpha^i \otimes \beta^k$ in the expression for ε_3 with a unary polynomial

$$B^{ik}(X) = B^{ik}\left(\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}\right) = \begin{bmatrix} \alpha & 0 \\ 0 & 0 \end{bmatrix}^i \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & \beta \end{bmatrix}^k = \begin{bmatrix} 0 & \alpha^i y \beta^k \\ 0 & 0 \end{bmatrix}.$$

Hence, $\varepsilon(X) = B^{03}(X) + 2B^{22}(X) + B^{12}(X) + 3B^{10}(X) + B^{21}(X) + 2B^{11}(X) + B^{01}(X) + B^{30}(X) + 3B^{20}(X) + B^{10}(X) + 2B^{00}(X)$ is an idempotent bimodule polynomial which maps J onto U_3. To construct a polynomial of the ring $\mathbf{R}$ whose image is U_3, one typically has to compose an idempotent polynomial with image J with a polynomial of this form; however in this case $\varepsilon(X)$ already has range in J, so $\varepsilon(X)$ is itself an idempotent unary ring polynomial with image U_3.

Remark. It is simpler to find the the minimal sets in a ring if it is commutative. First, the identity element of a commutative ring $\mathbf{R}$ has a unique representation $1 = e_1 + \cdots + e_n$ as a sum of orthogonal primitive idempotents. If $K = (e_i)$, and $I \prec K$, then the $\langle I, K \rangle$-minimal sets are precisely the 2-element subsets $\{u, v\} \subseteq K$ where $u - v \notin I$. All minimal sets of nonabelian type in $\mathbf{R}$ have this form.

By restricting the arguments of this paper to the commutative case, one can show that a subset $U \subseteq R$ is a minimal set of abelian type if and only if it is a coset of an ideal of the form $e_i J$, where J is the radical. Such ideals are the minimal direct factors of J. If $U = e_i J$, then the polynomials of the induced algebra $\mathbf{R}|_U$ are generated by the $e_i\mathbf{R}$-module polynomials and the ring multiplication. Thus, $\mathbf{R}|_U$ is polynomially equivalent to a module over the commutative local ring $e_i\mathbf{R}$ endowed with a commutative, associative, nilpotent, bilinear multiplication.

References

[1] J. Berman and S. Seif, *An approach to tame congruence theory via subtraces*, Algebra Universalis, **15** (1982), 359–384.

[2] K. Denecke, *Tame congruence theory*, East-West J. Math. **1** (1998), 1–42.

[3] R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series, **125**, Cambridge University Press, Cambridge-New York, 1987.

[4] D. Hobby and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics, **76**, American Mathematical Society, 1988.

[5] T. Ihringer, *Allgemeine Algebra*, Teubner Studienbücher Mathematik, B. G. Teubner, Stuttgart, 1988.

[6] N. Jacobson, *Basic Algebra II*, W. H. Freeman, 1980.

[7] P. Johnson and S. Seif, *Core simplicity, E-minimality and nilpotence*, manuscript (1994).

[8] K. A. Kearnes, *Local methods in universal algebra*, manuscript (1996).
[9] E. W. Kiss, *An easy way to minimal algebras*, Internat. J. Algebra Comput. **7** (1997), 55–75.
[10] E. W. Kiss, *An introduction to tame congruence theory*, in *Algebraic model theory* (Toronto, ON, 1996), 119–143, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **496**, Kluwer Acad. Publ., Dordrecht, 1997.
[11] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, **131**, Springer-Verlag, New York, 1991.
[12] B. R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, **28**, Marcel Dekker, New York, 1974.
[13] R. McKenzie, *Finite forbidden lattices*, in *Universal Algebra and Lattice Theory* (Puebla, 1982), 176–205, Lecture Notes in Math., **1004**, Springer, Berlin-New York, 1983.
[14] R. McKenzie, G. McNulty, and W. Taylor, *Algebras, Lattices and Varieties, Vol. I*, The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, Calif., 1987.
[15] R. S. Pierce, *Associative Algebras*, Graduate Texts in Mathematics, **88**, Springer-Verlag, New York, 1982.
[16] S. Seif, *E-minimal semigroups*, Semigroup Forum **50** (1995), 117–119.

(LeAnne Conaway) Department of Mathematics, University of Louisville, Louisville, KY 40292, USA
E-mail address: l_conaway@hotmail.com

(Keith Kearnes) Department of Mathematics, University of Colorado, Boulder, CO 80309, USA
E-mail address: kearnes@euclid.colorado.edu