Palestine Journal of Mathematics

Vol. 1(2) (2012) , 76–85

THE FRATTINI SUBSEMIGROUP OF THE MULTIPLICATIVE MONOID OF A FINITE SPECIAL PRINCIPAL IDEAL RING

David E. Dobbs and Brian C. Irick

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 20M99, 13F10; Secondary 13A15, 13M05.

Keywords and phrases: Semigroup, maximal subsemigroup, nongenerator, power-joined partition, special principal ideal ring, finite ring, prime ideal, nilpotent, unit, Frattini subgroup.

Abstract The Frattini subsemigroup of a finite semigroup S is introduced as the intersection of the maximal subsemigroups of S and is characterized, in case S is finite with more than one element, as the set of all the semigroup-theoretic nongenerators of S. As an application, the Frattini subsemigroup of the multiplicative monoid of a finite special principal ideal ring (SPIR) (R, M) which is not a field is computed as the disjoint union of M^2 and the Frattini subgroup of the group of units of R.

1 Introduction

All rings considered below are commutative with identity. All semigroups considered are written multiplicatively, in view of the intended application to the multiplicative monoid of a (commutative) ring. Our starting point is the classical concept of the Frattini subgroup $\Phi_g(G)$ of a group G, defined as the intersection of all the maximal subgroups of G (and taken to be G if G has no maximal subgroups): cf. [6, page 156], [11, page 159]. By analogy, we define the Frattini subsemigroup $\Phi_s(S)$ of a semigroup S to be the intersection of all the maximal subsemigroups of S (and taken to be S if S has no maximal subsemigroups). If G is a finite group, then $\Phi_s(G) = \Phi_g(G)$, since the maximal subsemigroups of G are the same as the maximal subgroups of G. To see this, one need only recall that a finite cancellative semigroup is the same thing as a finite group.

However, if one pursues a semigroup-theoretic analogue of the characterization of the Frattini subgroup of a group as the set of (group-theoretic) nongenerators of G (cf. [11, item 7.3.2, page 159]), matters do not go as smoothly. In fact, the comments just prior to and immediately following Proposition 2.2 explain why the set of semigroup-theoretic non-generators of a finite group G need *not* constitute the Frattini subgroup of G. The underlying reason is, of course, that the definition of "nongenerator" is not the same in the two contexts. As is well known (cf. [6, page 156], [11, page 159]), a *nongenerator (in the group-theoretic sense)* of a group G is any element $x \in G$ such that $T \setminus \{x\}$ is a (group-theoretic) generating set of G whenever T is a (group-theoretic) generating set of G. By analogy, we say that a *nongenerator (in the semigroup-theoretic sense)* of a semigroup S is any element $x \in S$ such that $T \setminus \{x\}$ is a (semigroup-theoretic) generating set of S whenever T is a nonempty (semigroup-theoretic) generating set of S.

The fact that attention was restricted to nonempty sets T in the last definition is both crucial and unavoidable. We say "crucial" because this restriction has the effect that the identity element 1 is (resp., is not) a nongenerator of a trivial group in the group-theoretic (resp., semigroup-theoretic) sense. We say "unavoidable" because, while it is customary to declare that the empty subset of a group G group-theoretically generates the trivial subgroup of G, there is no corresponding way to define the subsemigroup generated by the empty subset of a semigroup S, as S need not have a unique smallest subsemigroup. For this reason, if B is a nonempty subset of a semigroup S, we let $< B >$ denote the subsemigroup of S generated by B, but we give no semigroup-theoretic meaning to the notation $< \emptyset >$.

Despite the above-mentioned differences between the corresponding semigroup- and group-theoretic concepts, we obtain a semigroup-theoretic analogue of [11, item 7.3.2, page 159] in Corollary 2.3, which is the main result of Section 2. This result establishes that if S is a finite semigroup with more than one element, then $\Phi_s(S)$ is the set of all the nongenerators of S (in the semigroup-theoretic sense). For finite semigroups, this result is the best possible analogue, for the above comments yield that if E is a trivial group, then $\Phi_s(E)$ is *not* the set of all the nongenerators of S (in the semigroup-theoretic sense). A noteworthy result is Lemma 2.1: a finite semigroup with no proper subsemigroups must be a trivial group.

Perhaps the most useful semigroup associated to a ring R is the *multiplicative monoid of* R, that is, the structure consisting of the underlying set of R together with its binary operation of multiplication. One sees this topic in the current *renaissance* in factorization theory, but it was already apparent more than 50 years ago, as in Jacobson's approach to unique factorization domains via Gaussian monoids [7, pp. 115–127]. In dealing with the semigroup-ring interface, one must exercise caution, as the semigroup-theoretic ideal theory of S may differ from the ring-theoretic ideal theory of R. Indeed, according to a result of Aubert [1], each (semigroup-theoretic) ideal of S is an (ring-theoretic) ideal of R if and only if any pair of elements of R have the property that at least one of them divides the other in R. One class of rings satisfying this property consists of the special principal ideal rings, or SPIRs; this may be seen as a consequence of a well known factorization result [12, Example, p. 245]. (Recall also from [12, p. 245] that a ring R is called an SPIR in case R is a quasilocal principal ideal ring whose unique maximal ideal is nilpotent.) As Bullington [2] has recently determined the minimal generating sets of submodules of any free module over a finite SPIR, we are motivated to determine $\Phi_s(S)$ in case S is the multiplicative monoid of a finite SPIR. This goal is essentially achieved in Corollary 3.6, the main result of Section 3. When supplemented with Remark 3.7 (a), Corollary 3.6 accomplishes the computation promised by the title of this note. Also noteworthy in Section 3 is the study of power-joined partitions: see especially the connection with prime ideals in Proposition 3.2 (d).

We have just seen that the "nongenerator" content of Corollary 2.3 combines with the "minimal generating set" content of [2] to motivate the context of Corollary 3.6. We next mention another related ring-theoretic reason to be interested in determining the objects described in the title of this note. If G is a group admitting a set of operators P, the intersection of the maximal P-subgroups of G is denoted by $Fr_P(G)$, the so-called P-Frattini subgroup of G. If P is empty, then $Fr_P(G) = \Phi_g(G)$; and if P is a ring acting on its own additive group G by multiplication, then $Fr_P(G)$ is just the Jacobson radical of P [5, Example 3, p. 97]. Moreover, [5, Proposition 1, page 98] gives a $Fr_P(G)$-theoretic generalization of both Nakayama's Lemma and the result on group-theoretic nongenerators [11, item 7.3.2, page 159] that motivated Corollary 2.3. See also Remark 3.7 (d).

As usual, $\subset$ denotes proper inclusion. As to our other notational conventions, $\mathbb{N}$ denotes the set of positive integers; and, as in [4, page 10], $C(r, m)$ denotes a finite cyclic semigroup of index r and period m. If S is a semigroup, then Max(S) denotes the set of maximal subsemigroups of S. If A is a ring, $\sqrt{I}$ denotes the radical of an ideal I of A; Spec(A) the set of prime ideals of A; Nil(A) the intersection of the prime ideals of A, that is, the set of nilpotent elements of A; and $U(A)$ the group of units of A. Any unexplained material is standard, as in [4], [8], [10], [12].

2 The Frattini Subsemigroup of a Finite Semigroup

We begin an important piece of strategy. Observe that any overring-theoretic study of integral domains must deal with the fact that the valuation domains of Krull dimension at most 1 are the integral domains having only themselves and their quotient fields as overrings (cf. [8, Exercise 29, page 43]). Similarly, any semigroup-theoretic study in terms of subsemigroups must characterize the semigroups having no proper subsemigroups. (Recall that if S is a semigroup, then a *proper subsemigroup of* S is a subsemigroup T of S such that $T \subset S$.) Lemma 2.1 provides this characterization.

Lemma 2.1. The following conditions are equivalent:

(1) S is a finite semigroup with no proper subsemigroups;

(2) S is a trivial group (that is, a group with only one element).

Proof. (2) $\Rightarrow$ (1) trivially. Conversely, suppose (1). Choose $x \in S$. By (1), S must coincide with $< \{x\} >$, which is a finite cyclic semigroup, necessarily (semigroup-isomorphic to) $C(r, m)$, for some $r, m \in \mathbb{N}$. According to [4, Theorem 2.1], this means that $m = k - r$, where $1 \leq r < k, x^r = x^k, S = \{x^i \mid 1 \leq i \leq k-1\}$ has cardinality $k-1$, and $G := \{x^i \mid r \leq i \leq k-1\}$ is a cyclic group of order m. However, by (1), we also have that $S =< \{x^r\} >= \{x^{rj} \mid j \geq 1\} \subseteq G$. It follows that $r = 1$ and S is a group (necessarily equal to G). In particular, S is a group without any proper sub(semi)groups and, hence, a trivial group. This completes the proof. □

As mentioned in the Introduction, Corollary 2.3 is the semigroup-theoretic analogue of a characterization of the Frattini subgroup of a group. The well known proof of that group-theoretic result ([6, Theorem 10.4.1], [11, item 7.3.2, page 159]) depends on both Zorn's Lemma and the fact that the identity element 1 of any group G must be a nongenerator of G in the group-theoretic sense; that is, $1 \in \Phi_g(G)$. In preparing the way for Corollary 2.3, we can avoid the issues associated with Zorn's Lemma by concentrating on finite subsemigroups. However, we must come to grips with the fact that the identity element 1 of a trivial group E *is not* a nongenerator of E in the semigroup-theoretic sense; that is, $1 \notin \Phi_s(E)$. (The crucial point is that the subsemigroup $< B >$ is defined only in case the set B is nonempty.) Thus, while its statement may be ostensibly similar to a familiar characterization of $\Phi_g(G)$, Proposition 2.2 differs fundamentally from that group-theoretic motivation by needing to rely on the semigroup-theoretic notion of "nongenerator". To avoid confusion, the statement of Proposition 2.2 emphasizes the semigroup-theoretic nature of the terms involved; subsequent uses of the term "nongenerator" are tacitly made in only the semigroup-theoretic sense.

Proposition 2.2. (a) Let S be a semigroup, and let $x \in S$ be a nongenerator of S (in the semigroup-theoretic sense). Then $x \in \Phi_s(S)$; that is, x is an element of each maximal subsemigroup of S.

(b) Let S be a finite semigroup that does not consist of only one element. Let $x \in S$ such that $x \in \Phi_s(S)$; that is, x is an element of each maximal subsemigroup of S. Then x is a nongenerator of S (in the semigroup-theoretic sense).

Proof. (a) Deny. Then there exists $M \in \text{Max}(S)$ such that $x \notin M$. As $M \subset < M \cup \{x\} >$, it follows from the maximality of M that $< M \cup \{x\} >= S$. Since x is a nongenerator, $S =< (M \cup \{x\}) \setminus \{x\} >=< M >$. However, $< M >= M \neq S$, the desired contradiction.

(b) Deny. Then there exists a subset T of S such that $< T \cup \{x\} >= S$ but T is not a (semigroup-theoretic) generating set of S.

We claim that T is nonempty. If, on the contrary, $T = \emptyset$, then $S = < \{x\} > \subseteq \Phi_s(S)$. It follows from the definition of $\Phi_s(S)$ that $\text{Max}(S) = \emptyset$, a contradiction to Lemma 2.1, since we assumed that S does not consist of only one element. This establishes the above claim. (Note that the claim permits the definition of I and the finding of M in the next paragraph.)

Put $I := < T >$. Recall that $I \neq S$. Since S is finite, we can find $M \in \text{Max}(S)$ such that $I \subseteq M$. By hypothesis, $x \in M$. Therefore,

$$S = < T \cup \{x\} > \subseteq < I \cup \{x\} > \subseteq < M > = M \subset S,$$

the desired contradiction. The proof is complete. □

We pause to underscore the need for the above formulation that distinguished between some semigroup-theoretic notions and their group-theoretic counterparts. Note that the conclusion of Proposition 2.2 (b) fails in case the semigroup S consists of only one element. Indeed, in that case, S is just a trivial group E, and we have seen that the set of nongenerators of E is empty (even though $\Phi_s(E) = E \neq \emptyset$).

We now give the main result of this section.

Corollary 2.3. Let S be a finite semigroup that does not consist of only one element. Then the Frattini subsemigroup $\Phi_s(S)$ of S (namely, the intersection of the maximal subsemigroups of S) coincides with the set of all the nongenerators of S.

Proof. Just as in the proof of the analogous characterization of the Frattini subgroup of a group, the idea of the proof is to combine parts (a) and (b) of Proposition 2.2. (This works once one notices that the proof of Proposition 2.2 (b) dispatches the case that $\Phi_s(S)$ is defined as an empty intersection, that is, the case in which S has no maximal subsemigroups. Alternately, one can get past this point by invoking Proposition 2.1. Each of these approaches makes clear that our proof requires S to consist of more than one element; and, as we have already noted, the conclusion fails in case S *does* consist of only one element.) The proof is complete. □

Remark 2.4. To close the section, we answer a question that may arise because of the relationship between the Jacobson radical and the P-Frattini subgroup that was mentioned in the Introduction. To wit: why was $\Phi_s(S)$ not defined as the intersection of the maximal *ideals* of S? Our explanation is twofold. First, the semigroups that we are interested in usually have only one maximal ideal. More precisely, let S be a monoid with zero such that S has more than one element. (For instance, let S be the multiplicative monoid of a nonzero ring.) Then the set of all the noninvertible elements of S is the unique maximal ideal of S. Second, this set *need not* be $\Phi_s(S)$. For example, if $S = \{0, 1\}$ is the multiplicative monoid of the ring $\mathbb{Z}/2\mathbb{Z}$, then the unique maximal ideal of S is $\{0\}$, while $\Phi_s(S) = \{0\} \cap \{1\} = \emptyset$.

3 The Power-joined Partition of the Multiplicative Monoid of a Ring

In computing the Frattini subsemigroup of the multiplicative monoid of an SPIR, R, we will find that $\text{Nil}(R)$ and $U(R)$ play important roles in the analysis. Although $\text{Nil}(R)$ and $U(R)$ partition any SPIR R, it seems interesting to study the analogous partitions that arise for more general kinds of rings R. Before doing so in Lemma 3.1 and Proposition 3.2, we need to recall the following definition.

If S is a semigroup and $x, y \in S$, we say that x is *power-joined to* y (*in* S), and write $x \sim y$, if there exist positive integers m, n such that $x^m = y^n$. It is easy to verify that $\sim$ is an equivalence relation on S. The decomposition of a semigroup S into its associated $\sim$-equivalence classes is called the *power-joined partition of* S and is a useful technique in the literature on semigroups (cf. [10, item 3.11, page 110; items 4.4 and 4.5, page 114]). Lemma 3.1 contains two interesting facts from that literature; proofs are included for the sake of completeness.

Lemma 3.1. Let S be a finite semigroup. Then:

(a) Each power-joined equivalence class in S contains a unique idempotent element of S.

(b) If S is commutative, then each power-joined equivalence class in S is a subsemigroup of S.

Proof. (a) The "uniqueness" part of the assertion is easy to establish, for if z_1 and z_2 are idempotent elements of S such that $z_1 \sim z_2$, then there exist $p, q \in \mathbb{N}$ such that $z_1 = z_1^p = z_2^q = z_2$. As for the "existence" assertion, fix $x \in S$, and let $\mathcal{C}$ denote the $\sim$-equivalence class in S containing x. Then $T := < \{x\} > = \{x^i \mid i \in \mathbb{N}\} \subseteq \mathcal{C}$, and so it is enough to prove that T contains an idempotent element. As T is (semigroup-isomorphic to) $C(r, m)$ for some positive integers r and m, it follows from [4, Theorem 2.1] (or see the facts recalled in the proof of Lemma 2.1) that $C(r, m)$ contains a canonical group, namely, $G := \{x^j \mid r \leq j \leq r + m - 1\}$. Then the identity element of G is an idempotent element having the asserted property.

(b) Let x, y be power-joined in S. By (a), there is an (unique) idempotent element z in the power-joined equivalence class $\mathcal{C}$ that contains x and y. Since $z^k = z$ for each $k \in \mathbb{N}$, the definition of "power-joined" leads to $i, j \in \mathbb{N}$ such that $x^i = z = y^j$. Then, since S is commutative, we have that $(xy)^{ij} = x^{ij}y^{ij} = z^j z^i = z^{j+i} = z$. Therefore, $xy \sim z$, whence $z \in \mathcal{C}$. Thus, $\mathcal{C}$ is closed under multiplication; that is, $\mathcal{C}$ is a subsemigroup of S, to complete the proof. □

We next focus on the multiplicative monoids of finite rings.

Proposition 3.2. Let R be a finite nonzero ring and let S denote the multiplicative monoid of R. Then:

(a) Nil(R) and $U(R)$ are distinct power-joined equivalence classes in S.

(b) If R is a local ring (for instance, a finite SPIR), then S has exactly two power-joined equivalence classes, namely, Nil(R) and $U(R)$.

(c) Let $u, v \in R$. Then $u \sim v$ if and only if $\sqrt{Ru} = \sqrt{Rv}$.

(d) If R has exactly k prime ideals, then S has exactly 2^k power-joined equivalence classes.

Proof. (a) If $u, v \in$ Nil(R), then there exist $p, q \in \mathbb{N}$ such that $u^p = 0 = v^q$, whence $u\,(\sim 0) \sim v$. Conversely, if $u \sim 0$, then u is nilpotent. Therefore, Nil(R) is the power-joined equivalence class in S that contains 0. Moreover, Nil$(R) \cap U(R) = \emptyset$ since R is a nonzero ring. It remains only to show that $U(R)$ is a power-joined equivalence class in S.

Fix $x \in U(R)$. As R is finite, the elements $x, x^2, x^3, \ldots$ cannot be pairwise-distinct, and so there exist positive integers $r < k$ such that $x^r = x^k$. Multiplying by $(x^{-1})^r$, we find that $x^m = 1$, where $m := k - r \in \mathbb{N}$. In particular, $x \sim 1$. (Alternately, one could argue as in the proof of Lemma 3.1 (a), by using the theory of finite cyclic semigroups, to show that $\{x^i \mid i \in \mathbb{N}\}$ contains an idempotent element, say e. Then $e^2 = e \in U(R) \subseteq R \setminus \{0\}$, whence $e = 1$.) Conversely, if $y \in S$ such that $y \sim 1$, then $y^n = 1$ for some $n \in \mathbb{N}$, whence $y \in U(R)$. Therefore, $U(R)$ is a power-joined equivalence class in S.

(b) As R is a finite ring, it has Krull dimension 0 (cf. [12, Theorem 2, page 203]); that is, $P \not\subset Q$ if P and Q are distinct prime ideals of R. Since R is assumed local, R therefore has a unique prime ideal, say M. Consequently, $M =$ Nil(R) (cf. [12, Note II, page 151], [8, Theorem 25]). It follows that every nonunit of R is nilpotent. Hence, R is the (disjoint) union of Nil(R) and $U(R)$. The assertion now follows from (a).

(c) If $w \in R$, then $w \in U(R)$ if and only if $\sqrt{Rw} = R$. Therefore, as it was shown in (a) that $U(R)$ is a power-joined equivalence class, the assertion follows in case either u or v is a unit of R. Suppose henceforth that u and v are each nonunits of R. If $u \sim v$, then there exist $p, q \in \mathbb{N}$ such that $u^p = v^q$, whence $\sqrt{Ru} = \sqrt{Ru^p} = \sqrt{Rv^q} = \sqrt{Rv}$. It remains only to prove that if u and v are nonunits of R such that $\sqrt{Ru} = \sqrt{Rv}$, then $u \sim v$.

Let $P_1, \ldots, P_k$ denote the (pairwise distinct) prime ideals of R. Relabel these ideals so that $P_1, \ldots, P_i$ are the prime ideals of R that contain u (resp., v); that is, so that $\sqrt{Ru} = P_1 \cap \ldots \cap P_i = \sqrt{Rv}$. If $i = k$, then u and v are nilpotent (cf. [12, Note II, page 151], [8, Theorem 25]), whence (a) ensures that $u \sim v$, as desired. Thus, without loss of generality, $i < k$.

Consider any index j such that $1 \leq j \leq i$. As $A_j := R_{P_j}$ is an Artinian local ring, its unique prime ideal is nilpotent, say of nilpotency index e_j [12, Lemma 4, page 207]. Put $e := e_1 \cdot \cdots \cdot e_i$. Since u and v are in each P_j, the canonical images of u^e and v^e in $\prod_{j=1}^{i} A_j$ agree (each of these images being 0). The same is then true for the canonical images of u^{fe} and v^{fe}, for any $f \in \mathbb{N}$.

Next, consider any index j such that $i+1 \leq j \leq k$. Put $A_j := R_{P_j}$. As the labeling of the primes ensures that the canonical images of u and v are in $U(A_j)$, it follows from (a) that these images are power-joined in the multiplicative monoid of A_j. In fact, it follows from Lagrange's Theorem that if f_j is the order of the finite group $U(A_j)$, then the canonical images of u^{f_j} and v^{f_j} in A_j agree (each of these images being 1). Put $f := f_{i+1} \cdot \cdots \cdot f_k$. It follows that the canonical images of u^f and v^f in $\prod_{j=i+1}^{k} A_j$ agree. The same is then true for the canonical images of u^{fe} and v^{fe} in $\prod_{j=i+1}^{k} A_j$. In conjunction with the result of the preceding paragraph, this shows that the canonical images of u^{fe} and v^{fe} in $\prod_{j=1}^{k} A_j$ agree. By globalization, the kernel of the canonical map $R \to \prod_{j=1}^{k} A_j$ is 0, whence $u^{fe} = v^{fe}$ and $u \sim v$, as desired.

(d) Once again, let $P_1, \ldots, P_k$ denote the prime ideals of R. As noted above, $P_i \not\subset P_j$ if i and j are distinct indexes. It follows that if I_1 and I_2 are distinct nonempty subsets of $\{P_1, \ldots, P_k\}$, then $\bigcap\{P_i \mid i \in I_1\}$ and $\bigcap\{P_i \mid i \in I_2\}$ are distinct. If u is any nonunit of R, then $\sqrt{Ru}$ is such an intersection (cf. [8, Theorem 26]). Moreover, given such an intersection $\bigcap\{P_i \mid i \in I_1\}$, we claim that it is of the form $\sqrt{Ru}$, where u may be chosen to be any element of $(\bigcap\{P_i \mid P_i \in I_1\}) \setminus (\bigcup\{P_i \mid P_i \notin I_1\})$. Indeed, if I_1 consists of all the prime ideals of R, this set-theoretic difference is nonempty since it is $\mathrm{Nil}(R)$; in the remaining case, this set-theoretic difference is nonempty as a consequence of the Prime Avoidance Lemma [8, Theorem 81]. This proves the above claim. Therefore, by (c), the number of equivalence classes induced by $\sim$ on $R \setminus U(R)$ is the number of nonempty subsets of $\{P_1, \ldots, P_k\}$, namely, $2^k - 1$. As we saw in (a) that $U(R)$ is a power-joined equivalence class, the total number of power-joined equivalence classes on S is $(2^k - 1) + 1 = 2^k$, as asserted.

We next offer an alternate proof of (d). By Artinian structure theory [12, Theorem 3, page 205], R can be expresed as an internal direct product of finitely many, say d, finite local (nonzero) rings (R_j, J_j). It is well known that the prime ideals of R are the sets of the form $R_1 \times \cdots \times R_{j-1} \times J_j \times R_{j+1} \times \cdots \times R_d$, where $1 \leq j \leq d$. Therefore, $d = k$. As each local ring has exactly 2 idempotent elements, R has exactly 2^k idempotent elements. Since Lemma 3.1 (a) yields a bijection between the set of power-joined equivalence classes in S and the set of idempotent elements of S, the second proof of (d) is complete. □

Remark 3.3. (a) The above methods give a sharper understanding of the power-joined relation on a finite semigroup S: if $u, v \in S$, then $u \sim v$ (if and) only if there exists $n \in \mathbb{N}$ such that $u^n = v^n$. (If S is the multiplicative monoid S of a nonzero finite ring R, this was shown in the proof of Proposition 3.2 (c) in case u and v are nonunits of R. That proof also reduces us to the case $u, v \in U(R)$. Then, by Lagrange's Theorem, it suffices to take n to be the order of the finite group $U(R)$.) This can be seen in general by using Lemma 3.1 (a). Indeed, if z is the (unique) idempotent element in the $\sim$-equivalence class containing u and v, then $u^p = z = v^q$ for some $p, q \in \mathbb{N}$, whence $u^{pq} = z^q = z = z^p = v^{pq}$.

(b) The use of Artinian structure theory in the proof of the "if" assertion in Lemma 3.2 (c) was unavoidable. Indeed, that assertion fails if R is infinite, as is shown by the example $R := \mathbb{Z}, u := 12, v := 18$.

We further sharpen the focus to the main context of this section. First, recall from [12, page 245] that if (R, M) is an SPIR where M has index of nilpotency $e \geq 1$ and $M = R\pi$, then each nonzero element $r \in R$ can be expressed in the form $r = u\pi^i$, where $u \in U(R)$ and i is a uniquely determined integer, $0 \leq i \leq e-1$. A consequence that we use in the proofs of Lemma 3.4 and Theorem 3.5 is that if R, M, π are as above and $x \in M \setminus M^2$, then $U(R)x := \{y \in R \mid$ there exists $u \in U(R)$ such that $y = ux\} = M \setminus M^2$.

Lemma 3.4. Let (R, M) be a local ring and let S denote the multiplicative monoid of R. Then:

(a) If $H \in \text{Max}(U(R))$, then $M \cup H \in \text{Max}(S)$.

(b) If R is also finite and H is a maximal subgroup of $U(R)$, then $M \cup H \in \text{Max}(S)$.

(c) If R is an SPIR that is not a field, then $M^2 \cup U(R) \in \text{Max}(S)$.

Proof. (a) It is easy to see that $K := M \cup H$ is a subsemigroup of S. Also, if $s \in U(R) \setminus H$, then $s \notin K$. Therefore, K is a proper subsemigroup of S. To show that K is maximal, consider any element $x \in S \setminus K$. Then $x \in U(R) \setminus H$. As $H \in \text{Max}(U(R))$, it follows that $< H \cup \{x\} >= U(R)$. Hence,

$$S \supseteq < K \cup \{x\} > \supseteq < H \cup \{x\} > \cup M = U(R) \cup M = R = S.$$

Therefore, K is a maximal subsemigroup of S.

(b) Since $U(R)$ is a finite group, a maximal subgroup of $U(R)$ is the same as a maximal subsemigroup of $U(R)$. Accordingly, the assertion follows from (a).

(c) Note that $L := M^2 \cup U(R)$ is a subsemigroup of S (since M^2 is an ideal of R). Also, $M^2 \neq M$ (since there exists $e \in \mathbb{N}$ such that $M^e = 0 \neq M$). As any element of $M \setminus M^2$ is in $S \setminus L$, it follows that L is a proper subsemigroup of S. To show that L is maximal, consider any element $x \in S \setminus L$. Then $x \in M \setminus M^2$. By the above remarks, $U(R)x = M \setminus M^2$. Hence,

$$S \supseteq < L \cup \{x\} > \supseteq U(R) \cup U(R)x \cup M^2 = U(R) \cup (M \setminus M^2) \cup M^2 = U(R) \cup M = R = S.$$

Therefore, L is a maximal subsemigroup of S, to complete the proof. □

Note that the conclusion of Lemma 3.4 (c) fails in case R is a field, for then $M^2 \cup U(R) = S$ (which is not a maximal – or even a proper – subsemigroup of S).

Theorem 3.5. Let (R, M) be an SPIR which is not a field, and let S denote the multiplicative monoid of R. Let $K \in \text{Max}(S)$. Then:

(a) If $U(R) \subseteq K$, then $K = M^2 \cup U(R)$.

(b) If R is also finite and $U(R) \nsubseteq K$, then there exists $H \in \text{Max}(U(R))$ such that $K = M \cup H$.

Proof. (a) By Lemma 3.4 (c), $M^2 \cup U(R) \in \text{Max}(S)$. Therefore, by the maximality of K, we may assume, without loss of generality, that there exists $x \in K \setminus (M^2 \cup U(R)) \subseteq K \cap (M \setminus M^2)$. As noted above, the hypothesis ensures that $U(R)x = M \setminus M^2$. Moreover, since M is nilpotent, the factorization fact about SPIRs that was recalled above from [12] ensures that $< M \setminus M^2 >= M$. Hence, since $U(R) \subseteq K$, we have

$$S \supset K \supseteq < U(R)x \cup U(R) > \supseteq M \cup U(R) = R = S.$$

This contradiction completes the proof of (a).

(b) Since R is a nonzero ring, we see from the coset decomposition of the additive group of R via cosets of M that $U(R) = R \setminus M$ is the union of a nonempty family of pairwise disjoint sets each of which is in bijection with M. It follows that $|U(R)| \geq |M| \geq 2$ (where, as usual, $|T|$ denotes the cardinality of a set T; and $|M| \geq 2$ since R is not a field). Thus, $U(R) \supset \{1\}$. As $U(R)$ is a finite group, it follows that $U(R)$ does have at least one maximal sub(semi)group.

Next, put $L := K \cap U(R)$. We claim that L is nonempty. If the claim fails, then choose a maximal subgroup G of $U(R)$ and observe that $K \subseteq M \subset M \cup G \subset S$, the last step holding by virtue of Lemma 3.4 (b). As this contradicts the maximality of K, the claim has been established.

By the hypothesis of (b), $L \subset U(R)$. Also, L is evidently a subsemigroup of $U(R)$ (in view of the above claim and the fact that K is a subsemigroup of S). Next, since $U(R)$ is finite, we can find $H \in \text{Max}(U(R))$ such that $L \subseteq H$. As $K \subseteq M \cup L \subseteq M \cup H$, Lemma 3.4 (a) and the maximality of K yield that $K = M \cup H$, to complete the proof. □

We next take the main step in computing the object described in the title of this note.

Corollary 3.6. Let (R, M) be a finite SPIR which is not a field, and let S denote the multiplicative monoid of R. Then the Frattini subsemigroup $\Phi_s(S)$ of S coincides with the disjoint union $M^2 \cup \Phi_g(U(R))$.

Proof. By Lemma 3.4 and Theorem 3.5, Max(S) is the union of $\{M \cup H \mid H \in \text{Max}(U(R))\}$ and $\{M^2 \cup U(R)\}$. Notice that the first of these “unionands" is nonempty, as it was shown in the proof of Theorem 3.5 (b) that Max$(U(R))$ is nonempty. Therefore, by the definition of the Frattini subsemigroup,

$$\Phi_s(S) = M^2 \cup \bigcap\{H \mid H \in Max(U(R))\} = M^2 \cup \Phi_s(U(R)) = M^2 \cup \Phi_g(U(R)),$$

the last step holding since, as noted in the first paragraph of the Introduction, $\Phi_s(G) = \Phi_g(G)$ for any finite group G. The proof is complete. □

Remark 3.7. (a) We now take the final step in computing the titular object. If R is a finite field and S is the multiplicative monoid of R, then

$$\Phi_s(S) = \begin{cases} \emptyset & \text{if } |R| = 2 \\ \Phi_g(R \setminus \{0\}) = \Phi_g(U(R)) & \text{if } |R| \geq 3. \end{cases}$$

Notice that, as might be expected from the comment preceding the statement of Theorem 3.5, neither case in the above display coincides with the formula in Corollary 3.6 (which dealt with finite SPIRs that are not fields). Indeed, since R is a finite field, $M^2 \cup \Phi_g(U(R)) = \{0\} \cup \Phi_g(U(R))$, a set that properly contains the above-stated value(s) of $\Phi_s(S)$.

For a proof, note that the final comment in Section 2 takes care of the case $|R| = 2$. Assume henceforth that $|R| \geq 3$. It is straightforward to verify that if $H \subseteq U(R)$, then $H \in \text{Max}(U(R))$ if and only if the disjoint union

$H \cup \{0\} \in \text{Max}(S)$. Moreover, $U(R) \in \text{Max}(S)$. Therefore, by the definition of the Frattini subsemigroup, $\Phi_s(S) = U(R) \cap \bigcap\{H \cup \{0\} \mid H \in \text{Max}(U(R))\} = \bigcap\{H \mid H \in \text{Max}(U(R))\} = \Phi_s(U(R)) = \Phi_g(U(R))$, to complete the proof.

(b) Despite the disparity between (a) and Corollary 3.6, all finite SPIRs (R, M) *do* behave in a uniform way that captures the M^2 part of the formula in Corollary 3.6, if one considers the Frattini subsemigroup of the multiplicative semigroup M. Indeed, $\Phi_s(M) = M^2$ in all cases (regardless of whether R is a field).

The assertion is evident if R is a field, for then $M = 0$, $\text{Max}(M) = \emptyset$, and by definition, $\Phi_s(M) = M = \{0\} = M^2$. Assume next that the finite SPIR (R, M) is not a field. Recall from the proof of Theorem 3.5 (a) that $< M \setminus M^2 >= M$. Therefore, it is straightforward to check that $\text{Max}(M) = \{M^2 \cup H \mid H$ is a maximal proper subset of $M \setminus M^2\}$. In the spirit of the proof of Theorem 3.5 (b), consider the decomposition of the additive group of M via cosets of M^2. The upshot is that $|M \setminus M^2| \geq |M^2|$. Thus, if $|M \setminus M^2| \geq 2$, it easily follows from the definition of the Frattini subsemigroup that $\Phi_s(M) = M^2$. In the remaining case, $|M \setminus M^2| = 1$. Then $M^2 = 0$ and $M = \{0, \pi\}$ with $\pi \neq 0 = \pi^2$, whence $\{0\}$ is the only maximal subsemigroup of M and $\Phi_s(M) = 0 = M^2$. The proof is complete.

(c) In the spirit of Remark 2.4, we next reinterpret the arguments given in (b). If (R, M) is any finite SPIR, then M^2 is the intersection of the set of all the maximal ideals of the multiplicative semigroup M. Indeed, as in (b), the assertion is trivial if R is a field. Assume then that R is not a field. Observe that if H is a proper subset of $M \setminus M^2$, then $M^2 \cup H$ is a proper (semigroup-theoretic) ideal of M. Moreover, since M is finite, each proper (semigroup-theoretic) ideal of M is a subset of some maximal subsemigroup of M. Hence, by the proof in (b), $\text{Max}(M)$ coincides with the set of all the maximal ideals of M. As it was shown in (b) that the intersection of this set is M^2, the proof is complete.

(d) The motivation alluded to in the penultimate paragraph of the Introduction helps to cast yet another point of view on the calculations in (b) and (c). Here only, let us consider (commutative, for the sake of simplicity)"rings possibly without identity". Consider such an object A. In [3], Fuchs introduced the (right) Frattini subring of A, showing essentially that it could be viewed as the intersection of the maximal ideals of A and also as the set of (right) "nongenerators" of A. There is an extensive literature on the Frattini subring and such "nongenerators": cf. [9, Theorem 4.1.1]. However, the notion of "nongenerator" used in that "ring possibly without identity"-theoretic literature is essentially group-theoretic, not semigroup-theoretic, in the sense of the second and third paragraphs of the Introduction. In particular, the literature in question countenances the possibility of empty generating sets by viewing the symbol $< \emptyset >$ as $\{0\}$, while our semigroup-theoretic approach to nongenerators accords no meaning to the symbol $< \emptyset >$.

Nevertheless, if one follows the approach of the literature in question by defining the "Frattini subalgebra" of an (not necessarily unital) "algebra" B to be the intersection of the maximal right ideals of B, as in [9, page 53], we reach a point of contact with the above parts (b) and (c). Indeed, if (R, M) is a finite SPIR, then the multiplicative semigroup M is certainly a nilpotent (nonunital) "algebra" in the sense of [9]. If one applies the observation by Kruse-Price [9, page 53] that the Frattini subalgebra of a nilpotent ($\mathbb{Z}$-) algebra B is B^2 to the case $B := M$, one obtains the result that the intersection of the maximal "ring without identity"-theoretic ideals of (the "ring without identity)" M is M^2. This assertion should be compared to the fact established in (c) that M^2 is the intersection of the maximal semigroup-theoretic ideals of M.

Despite this coincidence, one cannot conclude that the maximal semigroup-theoretic ideals of M are the same as the maximal "ring without identity"-theoretic ideals of M. For example, consider the finite SPIR $(R, M) := \mathbb{F}_3[X]/(X^3) = \mathbb{F}_3 + \mathbb{F}_3 x + \mathbb{F}_3 x^2$, where $\mathbb{F}_3 = \{0, 1, 2\}$ is a field of order 3 and $x := X + (X^3)$. It is easy to verify that M consists of 9 elements and that $M \setminus M^2 = \{x, 2x, x + x^2, 2x + x^2, x + 2x^2, 2x + 2x^2\}$. By (b), $M \setminus \{x\}$ is a maximal subsemigroup of M; and by (c), $M \setminus \{x\}$ is also a maximal semigroup-theoretic ideal of M. However, $M \setminus \{x\}$ is *not* a (maximal) "ring without identity"-theoretic ideal of M. Indeed, it is not even closed under addition, for $2x + 2x = x$. This example contrasts with the fact, noted in the Introduction as a consequence of a result of Aubert [1], that each semigroup-theoretic ideal of an SPIR, A, is a ring-theoretic ideal of A. In distinguishing the behavior of M from that of R, our discussion thus serves to highlight an important role of the units of a ring.

In closing, we indicate two possible directions for future work. It would be of interest to replace the restriction on finite semigroups in Section 2 by considering semigroups that satisfy suitable chain conditions. Also, it would be interesting to enlarge the class of rings considered in Corollary 3.6 beyond the realm of finite SPIRs.

References

[1] K. E. Aubert, On the ideal theory of commutative semi-groups, *Math. Scand.* **1**, 39–54 (1953).

[2] G. D. Bullington, On the expected number of generators of a submodule of a free module over a finite special principal ideal ring, *Rend. Circ. Mat. Palermo* **51**, 5–50 (2002).

[3] L. Fuchs, A remark on the Jacobson radical, *Acta Sci. Math. (Szeged)* **14**, 167–168 (1952).

[4] R. Gilmer, *Commutative Semigroup Rings*, Chicago Lectures in Math., Univ. Chicago Press, Chicago (1984).

[5] K. W. Gruenberg, *Cohomological Topics in Group Theory*, Lecture Notes in Math. **143**, Springer-Verlag, Berlin (1970).

[6] M. Hall, Jr., *The Theory of Groups*, Macmillan, New York (1959).

[7] N. Jacobson, *Lectures in Abstract Algebra*, volume I, Van Nostrand, Princeton (1951).

[8] I. Kaplansky, *Commutative Rings* (Revised Edn), Univ. Chicago Press, Chicago (1974).

[9] R. L. Kruse and D. T. Price, *Nilpotent Rings*, Gordon and Breach, New York (1969).

[10] E. S. Ljapin, *Semigroups*, Translations Math. Monographs **3**, Amer. Math. Soc., Providence (1974).

[11] W. R. Scott, *Group Theory*, Prentice-Hall, Englewood Cliffs (1964).

[12] O. Zariski and P. Samuel, *Commutative Algebra*, volume I, Van Nostrand, Princeton (1958).

Author information

David E. Dobbs and Brian C. Irick, Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1320, U. S. A..
E-mail: `dobbs@math.utk.edu`

Received: December 3, 2011

Accepted: March 25, 2012