WHICH FINITE RINGS HAVE THE MOST OR FEWEST UNITS?

JONATHAN COHEN AND ALAN ROCHE

Abstract. Among finite rings of a fixed order that are not fields, we classify those that have the most units. Our methods also give the finite rings that have the fewest units.

Introduction.

Which finite rings have the most units? Well, it depends. If you ask for the finite ring with the highest proportion of units, the answer is the zero ring: its one member is both a zero element for addition and an identity element for multiplication, and so 100% of its elements are units. Following Rotman, however, we cast this ring into outer darkness ([8, p. 99]): for us, rings always have a multiplicative identity 1 (otherwise, there's no question to answer) and $1 \neq 0$.

Now in a division ring each nonzero element is a unit. Further, a finite division ring is a field (Wedderburn's little theorem). Thus, as the finite rings having the fewest nonunits, a natural answer to our question is *finite fields*. That's too banal, however. So let's put finite fields aside. The precise question we address is the following.

> *For n a positive integer, consider rings of order n other than fields. Which rings in this family have the most units?*

Recall that for each prime power p^e there is a finite field $\mathbb{F}_{p^e}$ of order p^e which is unique up to isomorphism and that there are no other finite fields. Say $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n. A ring R of order n then decomposes as a product of rings R_i of order $p_i^{e_i}$ (for $i = 1, \ldots, r$) and the group of units $R^\times$ splits as the direct product of the groups of units $R_i^\times$ (for $i = 1, \ldots, r$). It follows that if n has two or more prime factors, then among rings of order n the product $\mathbb{F}_{p_1^{e_1}} \times \cdots \times \mathbb{F}_{p_r^{e_r}}$ has the most units.

Our question thus reduces to the case of rings of prime-power order, say p^e. The final answer depends on e.

Theorem. *Consider rings of order p^e other than fields. Among such rings, suppose R has a group of units $R^\times$ of maximum size.*

- *(a) If $e = 2m$ is even, then $|R^\times| = p^{2m} - p^m$. Up to isomorphism, there are $m+1$ such rings.*
- *(b) If $e = 2m+1$ is odd with $m > 1$, so $e > 3$, then $|R^\times| = \left(p^{m+1} - 1\right)(p^m - 1)$ and $R \simeq \mathbb{F}_{p^{m+1}} \times \mathbb{F}_{p^m}$.*
- *(c) If $e = 3$, then $|R^\times| = p^3 - p^2$. The number of such rings (up to isomorphism) is 6 for p odd and 5 for $p = 2$.*

We explicitly describe the rings that can occur in parts (a) and (c) in Section 7. Those in part (a) are local with residue field $\mathbb{F}_{p^m}$. That is, they contain a unique maximal ideal (left, right, or two-sided) with corresponding quotient $\mathbb{F}_{p^m}$. Of the $m+1$ rings, $m-1$ are noncommutative—but in a very mild way. The rings in part (c) are also local, now with residue field $\mathbb{F}_p$, and are all commutative.

The proof of the theorem is in large part an exercise in Wedderburn–Artin theory. The classification of Galois rings is also a key ingredient. We summarize the requisite background in Section 1 (Wedderburn–Artin theory) and Section 7 (Galois rings).

The following is an easy consequence of our analysis (see Section 8).

Corollary. *Let R be a finite ring that is not a field. Then $|R^\times| \leq |R| - \sqrt{|R|}$ with equality if and only if R is one of the rings in part (a) of the theorem. Thus a finite ring R such that $|R^\times| > |R| - \sqrt{|R|}$ is necessarily a field.*

This is not new. Apart from the statement on equality, it was observed by MacHale [6] via a short elementary argument, a slight variant of which we include below. In fact, our article amounts to a quantitative supplement to MacHale's in that we classify the rings R that meet his upper bound on $|R^\times|$ or come as close as possible. MacHale's inequality was also recorded by Sury, recently and independently, by effectively the same method [9].

In the last section, we look at the complementary question *Among finite rings of a fixed order, which have the fewest units?* The analysis in this case is substantially more straightforward. As sketched above, the question reduces again to rings of prime-power order. The final answer: if R has order p^e then $|R^\times| \geq (p-1)^e$ with equality if and only if $R \simeq \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ (e factors).

1. Background.

We give an overview of some aspects of module theory and noncommutative ring theory that are pivotal to our arguments. In particular, we discuss the notion of a composition series of a module and—most crucially—record a version of a central result of Wedderburn and Artin, the pinnacle of what's now often called Wedderburn–Artin theory. By necessity, our presentation is condensed and largely utilitarian. For a careful, well-motivated development that brings out the elegance and essential simplicity of Wedderburn–Artin theory, see [3] or [5].

1.1. **Modules.** Let R be a ring. Recall that a *left R-module M* is an abelian group that admits (scalar) multiplication on the left by elements of R. More precisely, for any $r \in R$ and $m \in M$, there is a product $rm \in M$ subject to the following axioms, for all $r, s \in R$ and $m, n \in M$:

(1) $r(m+n) = rm + rn$;
(2) $(r+s)m = rm + sm$;
(3) $r(sm) = (rs)m$;
(4) $1m = m$.

A *right R-module* M is defined in a parallel manner: it admits multiplication on the right by elements of R so that the right-sided analogues of (1)–(4) hold. In particular, $(mr)s = m(rs)$ for $r, s \in R$ and $m \in M$. More perversely, we could still write our scalars on the left but replace (3) by $r(sm) = (sr)m$ for $r, s \in R$ and $m \in M$. The left-right distinction only arises for noncommutative rings.

We will almost always work on the left and will simply say "module" or "R-module" in place of "left module" or "left R-module." The various notions that we define or review on the left have evident analogues on the right.

A $\mathbb{Z}$-module is just an abelian group. For F a field, an F-module is just an F-vector space.

An *R-submodule* of an R-module M is an abelian subgroup N of M that is closed under scalar multiplication. Note that N is then an R-module in its own right. Further, the quotient M/N is an R-module via $r(m+N) = rm+N$ (for $r \in R$ and $m \in M$). Multiplication in R makes R into an R-module, called the *regular module*. Its submodules are the left ideals in R.

An R-module M is *simple* if it is nontrivial and its only submodules are itself and $\{0\}$. If I is a maximal left ideal in R, then the quotient R/I is a simple R-module. Conversely, every simple R-module arises in this way. The simple $\mathbb{Z}$-modules, for example, are just the various quotients $\mathbb{Z}/p\mathbb{Z}$ for p a prime (the simplest finite simple groups).

A *composition series* of an R-module M is a sequence of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_d = \{0\} \tag{C}$$

such that the successive quotients $S_i = M_{i-1}/M_i$ are simple (for $i = 1, \ldots, d$). Equivalently, M_i is a maximal submodule of M_{i-1} (for $i = 1, \ldots, d$). The zero module has the empty composition series. A nonzero module can have many composition series (or none). For example, the $\mathbb{Z}$-module $\mathbb{Z}/12\mathbb{Z}$ admits three:

$$\mathbb{Z}/12\mathbb{Z} \supset 2\mathbb{Z}/12\mathbb{Z} \supset 4\mathbb{Z}/12\mathbb{Z} \supset \{0\}, \tag{C1}$$

$$\mathbb{Z}/12\mathbb{Z} \supset 2\mathbb{Z}/12\mathbb{Z} \supset 6\mathbb{Z}/12\mathbb{Z} \supset \{0\}, \tag{C2}$$

$$\mathbb{Z}/12\mathbb{Z} \supset 3\mathbb{Z}/12\mathbb{Z} \supset 6\mathbb{Z}/12\mathbb{Z} \supset \{0\}. \tag{C3}$$

In each case, the simple quotients are $\mathbb{Z}/2\mathbb{Z}$ (twice) and $\mathbb{Z}/3\mathbb{Z}$ (once), but the order in which these factors occur varies. The three composition series correspond to the three ways of writing 12 as a product of primes:

$$(\mathsf{C1}) \longleftrightarrow 12 = 2 \cdot 2 \cdot 3,$$

$$(\mathsf{C2}) \longleftrightarrow 12 = 2 \cdot 3 \cdot 2,$$

$$(\mathsf{C3}) \longleftrightarrow 12 = 3 \cdot 2 \cdot 2.$$

This is an instance of a general phenomenon. Indeed, the Jordan–Hölder theorem says that, for any composition series (C) of a module M, the (isomorphism class of the) associated graded object $\mathrm{gr}(M) = \bigoplus_{i=1}^{d} S_i$ is an invariant of M. In order words, the multiset of successive simple quotients $\{S_i\}_{i=1,\ldots,d}$ (meaning the set of simple modules $\{S_i\}$, up to isomorphism, and the multiplicities with which they occur) is the same for each composition

series of M. The modules S_i (strictly, their isomorphism classes) are called the *composition factors* of M.

As in our example, the Jordan–Hölder theorem applied to the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ (n a positive integer) says precisely that the prime factorization of n is unique (up to order).

1.2. **Jacobson radical.** For M an R-module, the elements of R that act trivially on M form the annihilator $\operatorname{ann}(M)$ of M, that is,

$$\operatorname{ann}(M) = \{r \in R : rm = 0, \text{ for all } m \in M\}.$$

Note that $\operatorname{ann}(M)$ is a two-sided ideal in R. The *Jacobson radical* J of R is the intersection of the annihilators of the simple R-modules, and so is a two-sided ideal in R. By definition, the elements of J act trivially on each simple R-module. Thus simple R-modules and simple R/J-modules are effectively the same.

Notation. We invariably write J for the Jacobson radical of any ring under consideration. We usually refer to it as just the *radical*.

Elementary arguments show that $r \in J$ if and only if $1 + xry \in R^\times$ for all $x, y \in R$. In particular, $1+J = \{1+r : r \in J\}$ is a subgroup of $R^\times$. Indeed, the set $1+J$ is visibly closed under multiplication. Further, if $r \in J$ and $(1+r)v = 1$ for $v \in R$ then $v = 1 - rv \in 1 + J$, so that $1 + J$ is also closed under taking inverses.

1.3. **Wedderburn–Artin theorem.** We recall a version of Artin's generalization of work of Wedderburn. The result applies to rings R that satisfy the descending chain condition on left ideals: that is, if $\{\mathfrak{a}_i\}_{i=1,2,\dots}$ is a collection of left ideals in R satisfying

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots,$$

then there is an N such that $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$. Such rings are now called *left Artinian*. Artin's original formulation involved stronger chain conditions, later shown to be superfluous.

Before stating the theorem, we need one more definition. A ring is *simple* if its only two-sided ideals are itself and $\{0\}$. Fields—more generally, division rings—are simple. Moreover, if a commutative ring is simple, then it must be a field. That is, the commutative simple rings are just the fields. Are there noncommutative simple rings that are not division rings? Yes—an abundance. The most accessible ones comes from matrices. In fact, if R is simple then the matrix ring $\mathrm{M}_n(R)$ (for any positive integer n) is again simple. Thus, for any divison ring D and any positive integer n, the ring $\mathrm{M}_n(D)$ is simple. The Wedderburn–Artin theorem says, in part, that these are the only simple Artinian rings.

Theorem. *Let R be a left Artinian ring with radical J and set $\overline{R} = R/J$.*

- *(a) The ring $\overline{R}$ splits as $\overline{R} = \overline{R}_1 \times \cdots \times \overline{R}_t$ for simple rings $\overline{R}_i$ (for $i = 1, \dots, t$). These simple factors are unique (as two-sided ideals in $\overline{R}$).*
- *(b) The factors $\overline{R}_i$ are matrix rings over division rings. That is, there exist positive integers n_i and division rings D_i such that $\overline{R}_i \simeq \mathrm{M}_{n_i}(D_i)$ (for $i = 1, \dots, t$). The integer n_i and the isomorphism class of D_i are uniquely determined.*

We also need an addendum. Let S be a simple R-module. Equivalently, S is a simple $\overline{R}$-module. Part (a) implies that there is a unique factor $\overline{R}_i$ of $\overline{R}$ such that S is a simple $\overline{R}_i$-module. Indeed, by part (a), $S = \bigoplus_{j=1}^{t} \overline{R}_j S$. Hence, by simplicity, there is a unique index i such that $S = \overline{R}_i S$ and $\overline{R}_j S = \{0\}$ for $j \neq i$. It follows that S is a simple $\overline{R}_i$-module, as asserted. Conversely, we can view any simple $\overline{R}_i$-module as a simple $\overline{R}$-module by making the factors $\overline{R}_j$ (for $j \neq i$) act trivially. Now the simple ring $\overline{R}_i$ has just one simple module (up to isomorphism): it corresponds under the isomorphism in part (b) to column vectors of size n_i with entries in D_i. In sum, R has t distinct simple modules (up to isomorphism), given by viewing the unique simple modules for the factors $\overline{R}_i$ as R-modules.

It may help to see a concrete example.

Example. For F a field, consider the subring R of $\mathrm{M}_3(F)$ consisting of matrices of the form

$$\begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix}.$$

Standard results and manipulations (which we omit) show that

$$J = \left\{ \begin{bmatrix} 0 & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\}.$$

Then $\overline{R} \simeq F \times \mathrm{M}_2(F)$. It can be realized as the subring of block-diagonal matrices of the form $\begin{bmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{bmatrix}$. There are two simple R-modules or $\overline{R}$-modules S_1 and S_2 (up to isomorphism). We can view them as spaces of column vectors:

$$S_1 = \left\{ \begin{bmatrix} * \\ 0 \\ 0 \end{bmatrix} \right\}, \; S_2 = \left\{ \begin{bmatrix} 0 \\ * \\ * \end{bmatrix} \right\}.$$

Under the isomorphism $\overline{R} \simeq F \times \mathrm{M}_2(F)$, the module S_1 corresponds to the unique simple F-module and S_2 corresponds to the unique simple $\mathrm{M}_2(F)$-module.

In a key argument in Section 3, we work with the composition factors of the radical of a finite ring. In the present example, how is the radical J assembled from the two distinct (isomorphism classes of) simple R-modules? The matrix identity

$$\begin{bmatrix} \alpha & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix} \begin{bmatrix} 0 & x & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \alpha x & \alpha y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

says that the R-module J is the direct sum of two copies of S_1. Thus S_1 occurs with multiplicity 2 in J and S_2 with multiplicity 0.

Finite rings are certainly left Artinian. In Section 3, we apply the Wedderburn–Artin theorem and its addendum to reduce our question about unit groups of maximum size to

two cases: local rings and products of fields. Local rings are precisely the rings R such that $\overline{R} = R/J$ is a division ring. An equivalent requirement: R has a unique maximal ideal (left, right, or two-sided), necessarily equal to J ([5, Theorem 19.1]).

Convention. To simplify some statements, we adopt the convention that $J \neq \{0\}$ in a local ring. In other words, we do not view division rings as local rings.

2. First Reduction.

It's well known that a finite ring is (canonically) a direct product of rings of prime-power order. Our question thus reduces to the prime-power case. For completeness, we write out this first reduction step.

Let R be a finite ring and say $p_1, \ldots, p_r$ are the distinct prime divisors of $|R|$. We set

$$R_i = \{x \in R : p_i^k x = 0, \text{ for some positive integer } k = k_x\}$$

(for $i = 1, \ldots, r$). As an abelian group, R splits as

$$R = R_1 \oplus \cdots \oplus R_r. \tag{1}$$

By construction, each R_i is a two-sided ideal in R. Thus $R_i R_j \subseteq R_i \cap R_j$, and so

$$R_i R_j = \{0\}, \quad \text{for } i \neq j. \tag{2}$$

It follows that the factors R_i are rings with identity and that (1) is a splitting of rings. Indeed, if we write

$$1 = e_1 + \cdots + e_r$$

with $e_i \in R_i$ (for all i), then a quick check using (1) and (2) shows that R_i has identity element e_i (for all i). Moreover, (2) implies that the decomposition (1) is respected by the multiplication law in R. Accordingly, the unit group $R^\times$ splits as

$$R^\times = R_1^\times \times \cdots \times R_r^\times.$$

Assume now that $|R|$ has two or more prime divisors and write $|R| = p_1^{e_1} \cdots p_r^{e_r}$ for positive integers $e_1, \ldots, e_r$. In particular, $|R_i| = p_i^{e_i}$ (for $i = 1, \ldots, r$). Among rings of the same order as R, it follows that the product of fields $\mathbb{F}_{p_1^{e_1}} \times \cdots \times \mathbb{F}_{p_1^{e_r}}$ has the largest unit group.

3. Main Reduction.

The elementary argument of the preceding section reduces us to looking at rings of prime-power order. In this section, we reduce further to local rings or products of fields. As above, and for the remainder of the article, we write $R^\times$ for the group of units or unit group of a ring R.

First, a preliminary observation.

Lemma 1. *For any ring R, the canonical quotient map from R to $\overline{R} = R/J$ induces an isomorphism of groups $R^\times/(1+J) \simeq \overline{R}^\times$. In particular, if R is finite then*

$$|R^\times| = |J||\overline{R}^\times|.$$

Proof. The homomorphism of groups

$$r \mapsto r + J : R^\times \to \overline{R}^\times \tag{3}$$

has kernel $1 + J$. We need to show that the map is surjective. To this end, let $r \in R$ with $r + J \in \overline{R}^\times$. Thus there is an $s \in R$ with

$$(r + J)(s + J) = 1 + J = (s + J)(r + J),$$

so that $rs = 1 + x$ and $sr = 1 + y$ for $x, y \in J$. Since $1 + x, 1 + y \in R^\times$, it follows that r admits left and right inverses, whence $r \in R^\times$. This proves surjectivity of (3). □

Our main reduction step is the following.

Proposition 1. *Let R be a ring of prime-power order, say p^e, with nontrivial radical J. If R is not local (that is, if R/J is not a field), then there is a product of fields $\mathbb{K}_1 \times \mathbb{K}_2$ of order p^e with $|R^\times| < |\mathbb{K}_1^\times \times \mathbb{K}_2^\times|$.*

Thus a ring of order p^e with a group of units of maximum size among nonfields of order p^e is either local or a product of two fields.

Proof. The result follows from some simple estimates. First, we need some notation. By part (a) of the Wedderburn–Artin theorem,

$$R/J = \overline{R}_1 \times \cdots \times \overline{R}_t \tag{4}$$

with $\overline{R}_i$ a simple ring for $i = 1, \ldots, t$. By part (b), there exist p-powers q_i such that

$$\overline{R}_i \simeq \mathrm{M}_{n_i}(\mathbb{F}_{q_i}) \qquad (i = 1, \ldots, t). \tag{5}$$

For each i, we fix a representative S_i for the unique isomorphism class of simple $\overline{R}_i$-modules. Under the isomorphism (5), S_i corresponds to column vectors of size n_i with entries in $\mathbb{F}_{q_i}$, so that

$$|S_i| = q_i^{n_i} \qquad (i = 1, \ldots, t).$$

Via (4), we view each S_i as an R-module. As we observed after the statement of the Wedderburn–Artin theorem, the family $\{S_1, \ldots, S_t\}$ is a complete set of representatives for the collection of isomorphism classes of simple R-modules.

Consider J as an R-module and set

$$m_i \;=\; \text{multiplicity of } S_i \text{ as a composition factor of } J. \qquad (i = 1, \ldots, t)$$

Then

$$|J| = |S_1|^{m_1} \cdots |S_t|^{m_t} = q_1^{n_1 m_1} \cdots q_t^{n_t m_t}. \tag{6}$$

Hence, using Lemma 1 and (5),

$$|R^\times| = \prod_{i=1}^{t} q_i^{n_i m_i} |\mathrm{GL}_{n_i}(\mathbb{F}_{q_i})|. \tag{7}$$

For each i, we call $q_i^{n_i m_i} |\mathrm{GL}_{n_i}(\mathbb{F}_{q_i})|$ the ith *contribution* to $|R^\times|$.

Our estimates vary according to the following three cases.

Case 1. $n_i = 1$. The ith contribution to $|R^\times|$ is $q_i^{m_i}(q_i - 1)$. We have

$$q_i^{m_i}\,(q_i - 1) \,\le\, q_i^{m_i+1} - 1 \,=\, |\mathbb{F}^\times_{q_i^{m_i+1}}|,$$

with equality if and only if $m_i = 0$.

Case 2. $n_i > 1$ and $m_i = 0$. The ith contribution to $|R^\times|$ is now

$$|\mathrm{GL}_{n_i}(\mathbb{F}_{q_i})| \,<\, q_i^{n_i^2} - 1 \,=\, |\mathbb{F}^\times_{q_i^{n_i^2}}|.$$

Case 3. $n_i > 1$ and $m_i > 0$. The ith contribution to $|R^\times|$ is $q_i^{n_i m_i}|\mathrm{GL}_{n_i}(\mathbb{F}_{q_i})|$. To simplify the notation, we temporarily write

$$q = q_i,\ m = m_i,\ N = n_i.$$

We claim that

$$q^{Nm}\,|\mathrm{GL}_N(\mathbb{F}_q)| \,<\, \left(q^{Nm} - 1\right)\left(q^{N^2} - 1\right) = |\mathbb{F}^\times_{q^{Nm}} \times \mathbb{F}^\times_{q^{N^2}}|. \tag{8}$$

Using $|\mathrm{GL}_N(\mathbb{F}_q)| = \prod_{j=0}^{N-1}\left(q^N - q^j\right)$, we can write (8) as

$$q^{Nm}\left(q^N - 1\right)\left(q^N - q\right)\cdots\left(q^N - q^{N-1}\right) \,<\, \left(q^{Nm} - 1\right)\left(q^{N^2} - 1\right).$$

Dividing each side by q^{Nm} then gives the equivalent inequality

$$\left(q^N - 1\right)\left(q^N - q\right)\cdots\left(q^N - q^{N-1}\right) \,<\, \left(1 - q^{-Nm}\right)\left(q^{N^2} - 1\right). \tag{9}$$

Observe now that as $m \ge 1$, we have $1 - q^{-N} \le 1 - q^{-Nm}$, so it suffices to prove (9) in the case $m = 1$, that is,

$$\left(q^N - 1\right)\left(q^N - q\right)\cdots\left(q^N - q^{N-1}\right) \,<\, \left(1 - q^{-N}\right)\left(q^{N^2} - 1\right).$$

Next, we rewrite as

$$\frac{\left(q^N - 1\right)}{q^N}\frac{\left(q^N - q\right)}{q^N}\cdots\frac{\left(q^N - q^{N-1}\right)}{q^N} \,<\, \frac{\left(1 - q^{-N}\right)\left(q^{N^2} - 1\right)}{q^{N^2}},$$

or

$$\left(1 - q^{-N}\right)\left(1 - q^{1-N}\right)\cdots\left(1 - q^{-1}\right) \,<\, \left(1 - q^{-N}\right)\left(1 - q^{-N^2}\right).$$

Canceling $1 - q^{-N}$ from each side, we're reduced to

$$\left(1 - q^{1-N}\right)\left(1 - q^{2-N}\right)\cdots\left(1 - q^{-1}\right) \,<\, 1 - q^{-N^2}. \tag{10}$$

Since $N > 1$, we have $1 - q^{-1} < 1 - q^{-N^2}$. Thus (10) certainly holds and we've established the original inequality (8).

Putting the cases together, we obtain

$$|R^\times| \,<\, \prod_{n_i=1} |\mathbb{F}^\times_{q_i^{m_i+1}}| \quad\cdot \prod_{n_j>1,\, m_j=0} |\mathbb{F}^\times_{q_j^{n_j^2}}| \quad\cdot \prod_{n_k>1,\, m_k>0} |\mathbb{F}^\times_{q_k^{n_k m_k}} \times \mathbb{F}^\times_{q_k^{n_k^2}}|.$$

The three terms in the product correspond to the three cases.

By construction, the product of fields

$$\prod_{n_i=1} \mathbb{F}_{q_i^{m_i+1}} \;\times \prod_{n_j>1,\, m_j=0} \mathbb{F}_{q_j^{n_j^2}} \;\times \prod_{n_k>1,\, m_k>0} \mathbb{F}_{q_k^{n_k m_k}} \times \mathbb{F}_{q_k^{n_k^2}}$$

has order p^e. Further, as $J \neq \{0\}$, at least one of the multiplicities m_i or m_k must be nonzero. That is, either the first or third term in the product is nonempty.

Suppose now that R/J is not a field. In this case, we observe that at least two fields must appear in the overall product. Indeed, this is evident if some $m_k > 0$. Assume then that the third term is empty, so that the first term must be nonempty. If the middle term is also nonempty, then again the whole product contains at least two fields. Thus we're left with the case in which only the first term is nonempty, that is, $n_i = 1$ for all indices i, or R/J is a product of fields. By hypothesis, R/J is not itself a field, so again the product contains at least two factors.

We've proved that if R is not local, then there exist fields $\mathbb{E}_1, \ldots, \mathbb{E}_w$ with $w \geq 2$ such that

$$|R| = |\mathbb{E}_1 \times \cdots \times \mathbb{E}_w| \text{ and } |R^\times| < |\mathbb{E}_1^\times \times \cdots \times \mathbb{E}_w^\times|.$$

Finally, we set $\mathbb{K}_1 = \mathbb{E}_1$ and write $\mathbb{K}_2$ for the field of order $|\mathbb{E}_2 \times \cdots \times \mathbb{E}_w|$, so that

$$|R^\times| < |\mathbb{E}_1^\times \times \cdots \times \mathbb{E}_w^\times| \leq |\mathbb{K}_1^\times \times \mathbb{K}_2^\times|.$$

This completes the proof. □

4. Local Rings.

By Proposition 1, the contest for the largest unit group among nonfields of order p^e is a duel between local rings and products of fields. In this section, we decide the winner among local rings. In the next, the winner among products of fields will emerge. The winners of these preliminary contests will face each other in Section 6.

Assume that R is a local ring of order p^e, so that $R/J \simeq \mathbb{F}_{p^f}$ for some integer f with $1 \leq f < e$. Note first that f must divide e. Indeed, $\mathbb{F}_{p^f}$ is the unique simple R-module (up to isomorphism). Hence, if we write m for the multiplicity of $\mathbb{F}_{p^f}$ as a composition factor of R, then $|R| = |\mathbb{F}_{p^f}|^m$, and so $e = fm$. Now

$$|R^\times| = |R| - |J| = |R| - \frac{|R|}{|\mathbb{F}_{p^f}|}.$$

To maximize $|R^\times|$, we need to choose f as large as possible. That is, we want f to be the largest divisor of e that is less than e. Thus $f = \dfrac{e}{l}$ for l the smallest prime divisor of e.

We've proved the following.

Lemma 2. *Let p be a prime and e be a positive integer, and write l for the least prime divisor of e. Among local rings R of order p^e, the maximum possible value of $|R^\times|$ is given by*

$$|R^\times| = p^e - p^{e-e/l}.$$

In particular, for $e = 2m$ even, the maximum possible value is

$$|R^\times| = p^{2m} - p^m.$$

The maximum is attained by the local ring $\mathbb{F}_{p^f}[\mathrm{X}]/\left(\mathrm{X}^l\right)$.

5. Products of Fields.

Next we consider products of fields $\mathbb{F}_{p^f} \times \mathbb{F}_{p^{e-f}}$ for $f = 1, \ldots, e-1$. By symmetry, it suffices to take $f = 1, \ldots, \left\lfloor \frac{e}{2} \right\rfloor$.

The unit group $\mathbb{F}_{p^f}^{\times} \times \mathbb{F}_{p^{e-f}}^{\times}$ has size

$$\left(p^f - 1\right)\left(p^{e-f} - 1\right) = p^e - p^{e-f} - p^f + 1,$$

which attains a maximum when $p^{e-f} + p^f$ is at a minimum. Further, the minimum value of $p^{e-f} + p^f$ occurs at $f = \left\lfloor \frac{e}{2} \right\rfloor$ (when f and $e - f$ are as close as possible). One way to verify this last statement is to set

$$G(x) = \frac{p^e}{x} + x,$$

so that $G(p^f) = p^{e-f} + p^f$. By computing the derivative of G or by a direct calculation, we see that G is decreasing on the interval $\left(0, p^{e/2}\right]$. In particular, the minimum value of $G(p^f)$ for $f = 1, \ldots, \left\lfloor \frac{e}{2} \right\rfloor$ indeed occurs at $\left\lfloor \frac{e}{2} \right\rfloor$.

We sum up as follows.

Lemma 3. *Among the products $\mathbb{F}_{p^f} \times \mathbb{F}_{p^{e-f}}$ for $1 \leq f < e$, the unit group of maximum size occurs at $f = \left\lfloor \frac{e}{2} \right\rfloor$. In other words:*

(a) for $e = 2m$ even, the largest unit group has size

$$\left(p^m - 1\right)^2 = p^{2m} - 2p^m + 1;$$

(b) for $e = 2m + 1$ odd, the largest unit group has size

$$\left(p^m - 1\right)\left(p^{m+1} - 1\right) = p^{2m+1} - p^{m+1} - p^m + 1.$$

6. Local Rings versus Products of Fields.

We've reached the final round in our contest for the largest unit group (among rings of order p^e other than fields). To decide the ultimate winner, we just have to determine the relative sizes of the expressions in Lemmas 2 and 3. The comparison splits into cases.

Case 1. $e = 2m$ even. The answer here is immediate. For local rings, the maximum is $p^{2m} - p^m$; for a product of fields, it's

$$p^{2m} - 2p^m + 1 = p^{2m} - (2p^m - 1).$$

Since $p^m < 2p^m - 1$ for $m \geq 1$, the winner is local rings.

Case 2. $e = 2m + 1$ odd with $m > 1$. For local rings the maximum is $p^e - p^{e-e/l}$ for l the least prime divisor of e; for a product of fields, it's

$$p^{2m+1} - p^{m+1} - p^m + 1 = p^{2m+1} - (p^{m+1} + p^m - 1).$$

Thus we need to compare

$$(\alpha)\ p^{e-e/l} = p^{2m+1-(2m+1)/l} \text{ and } (\beta)\ p^{m+1} + p^m - 1.$$

Whichever is smaller gives the winner.

Since $l \geq 3$, we have

$$e - \frac{e}{l} \geq \frac{2}{3}\, e,$$

so that

$$p^{e-e/l} \geq p^{2e/3} = p^{(4m+2)/3}.$$

Hence $(\alpha) > (\beta)$ whenever

$$p^{(4m+2)/3} \geq p^{m+1} + p^m. \tag{11}$$

This will hold for p sufficiently large as long as $(4m+2)/3 > m+1$, equivalently $m > 1$.

To obtain a more precise statement, we assume $m > 1$ and set

$$f(x) = x^{(4m+2)/3} - x^{m+1} - x^m = x^m \left(x^{(m+2)/3} - x - 1 \right).$$

The inequality (11) then says $f(p) \geq 0$. By calculus, f is increasing on $(1, \infty)$, so

$$f(p) \geq f(2) = 2^m \left(2^{(m+2)/3} - 3 \right).$$

A quick check shows that $f(2) \geq 0$ if and only if $m \geq 3$, equivalently $e \geq 7$. Therefore (11) holds for all primes p and all $m \geq 3$ (or $e \geq 7$), and so in this range the winner is products of fields.

What happens for $m = 2$? Then (11) becomes

$$p^4 \geq p^3 + p^2$$

which holds for all p (as $p^4 \geq 2p^3 > p^3 + p^2$). Hence products of fields win once more in the case $m = 2$ (or $e = 5$) for all primes p.

Case 3. $e = 3$. We need to compare (α) and (β) for $m = 1$. Here (α) is p^2 and (β) is $p^2 + p - 1$. Thus (α) is smaller, so local rings win in this final case. Hurray for local rings!

7. Classification.

Our object now is to list the local rings that can occur in Cases 1 and 3 of the preceding section (up to isomorphism).

To begin, let's look at Case 1, so $e = 2m$ is even. Thus R is a local ring of order p^{2m} with $|R^\times| = p^{2m} - p^m$, equivalently $R/J \simeq \mathbb{F}_{p^m}$.

First, we describe a family of examples. We'll see eventually that the family accounts for all but one of the possibilities for R.

Notation. For simplicity, we set $\mathbb{F} = \mathbb{F}_{p^m}$.

Example. For σ a field automorphism of $\mathbb{F}$, we write $\mathbb{F}[\mathrm{X}; \sigma]$ for the skew-polynomial ring consisting of polynomials with coefficients in $\mathbb{F}$ where scalar multiplication is "twisted" by σ. This means that, for all $\lambda \in \mathbb{F}$,

$$\mathrm{X} \cdot \lambda = {}^{\sigma}\lambda \cdot \mathrm{X},$$

and so monomials in $\mathbb{F}[\mathrm{X}; \sigma]$ multiply according to

$$\lambda_1 \mathrm{X}^{n_1} \cdot \lambda_2 \mathrm{X}^{n_2} = \lambda_1 \, {}^{\sigma^{n_1}}\lambda_2 \, \mathrm{X}^{n_1+n_2}.$$

It follows that, for any positive integer k, the left and right ideals generated by X^k coincide; we write $\left(\mathrm{X}^k\right)$ for this two-sided ideal.

Now consider the quotient ring $R = \mathbb{F}[\mathrm{X};\sigma]/\left(\mathrm{X}^2\right)$. The field $\mathbb{F}$ embeds in R via $\lambda \mapsto \lambda \cdot 1 : \mathbb{F} \to R$ and we identify $\mathbb{F}$ with its image under this embedding. With $\epsilon = \mathrm{X} + \left(\mathrm{X}^2\right)$, we have $R = \mathbb{F} \oplus \mathbb{F}\epsilon$ as an $\mathbb{F}$-vector space. Multiplication in R is then determined by the identities

$$\epsilon^2 = 0 \text{ and } \epsilon \cdot \lambda = {}^{\sigma}\lambda \cdot \epsilon, \text{ for all } \lambda \in \mathbb{F}.$$

We write $R = \mathbb{F}[\epsilon;\sigma]$. We have $J = \mathbb{F}\,\epsilon$, so $R/J \simeq \mathbb{F}$.

Remark. When σ is the identity, R is often called the *ring of dual numbers over* $\mathbb{F}$. It was introduced by Clifford when the ground field is the real numbers—William Kingdon Clifford (of Clifford algebras), that is, not Alfred Hoblitzelle Clifford (of Clifford theory). For σ nontrivial, we could call R a *ring of twisted dual numbers over* $\mathbb{F}$ but will not need the terminology.

The group $\mathrm{Aut}(\mathbb{F})$ of field automorphisms of $\mathbb{F} = \mathbb{F}_{p^m}$ is cyclic of order m. We claim that distinct elements σ of $\mathrm{Aut}(\mathbb{F})$ give nonisomorphic rings $\mathbb{F}[\epsilon;\sigma]$. Indeed, suppose $\sigma_i \in \mathrm{Aut}(\mathbb{F})$ for $i = 1, 2$ and $f : \mathbb{F}[\epsilon_1;\sigma_1] \to \mathbb{F}[\epsilon_2;\sigma_2]$ is an isomorphism of rings. Then there is a $\tau \in \mathrm{Aut}(\mathbb{F})$ and a nonzero $\mu \in \mathbb{F}$ such that

$$f(\lambda) = {}^{\tau}\lambda \text{ (for all } \lambda \in \mathbb{F}) \text{ and } f(\epsilon_1) = \mu\epsilon_2.$$

Applying f to the identity $\epsilon_1 \cdot \lambda = {}^{\sigma_1}\lambda \cdot \epsilon_1$ in $\mathbb{F}[\epsilon_1;\sigma_1]$, we obtain

$$\mu\epsilon_2 \cdot {}^{\tau}\lambda = {}^{\tau\sigma_1}\lambda \cdot \mu\epsilon_2, \text{ for all } \lambda \in \mathbb{F},$$

so that

$${}^{\sigma_2\tau}(\lambda)\,\mu\,\epsilon_2 = {}^{\tau\sigma_1}(\lambda)\,\mu\,\epsilon_2, \text{ for all } \lambda \in \mathbb{F}.$$

Thus $\sigma_2\tau = \tau\sigma_1$ and $\sigma_1 = \sigma_2$ (since $\mathrm{Aut}(\mathbb{F})$ is abelian).

The family $\{\mathbb{F}[\epsilon;\sigma]\}_{\sigma \in \mathrm{Aut}(\mathbb{F})}$ therefore gives rise to m distinct isomorphism classes of rings. There is one commutative ring in the family, given by the identity automorphism of $\mathbb{F}$.

Next, we collect some general observations.

Lemma 4. *Let $\mathcal{R}$ be a local ring with unique maximal ideal $\mathcal{J}$.*

(a) If $\mathcal{R}^\times$ is abelian, then $\mathcal{R}$ is commutative (and conversely).

(b) For $\mathcal{R}$ finite, the normal subgroup $1 + \mathcal{J}$ of $\mathcal{R}^\times$ admits a complement. That is, $\mathcal{R}^\times$ contains a copy S of $(\mathcal{R}/\mathcal{J})^\times$ and splits as the semidirect product

$$\mathcal{R}^\times = (1 + \mathcal{J}) \rtimes S.$$

(c) If $\mathcal{R}$ has order p^{2m} with $\mathcal{R}/\mathcal{J} = \mathbb{F}$ (our situation), then $\mathcal{J} \simeq \mathbb{F}$ as $\mathcal{R}$-modules, equivalently as $\mathbb{F}$-vector spaces, and $\mathcal{J}^2 = \{0\}$.

Proof. For part (a), note that $\mathcal{R}$ is generated as a ring by $\mathcal{R}^\times$. Indeed, if $x \in \mathcal{R}$ is a nonunit then $x = (1 + x) - 1$ is a sum of units. Hence if $\mathcal{R}^\times$ is an abelian group, then $\mathcal{R}$ is a commutative ring. The converse is obvious.

For part (b), we temporarily write $\mathcal{R}/\mathcal{J} = \mathbb{E}$. By Lemma 1, $\mathcal{R}^\times/(1 + \mathcal{J}) \simeq \mathbb{E}^\times$. Now $|1 + \mathcal{J}| = |\mathcal{J}|$ is a power of $|\mathbb{E}|$: indeed, $|\mathcal{J}| = |\mathbb{E}|^m$ where m is the multiplicity of the unique

simple $\mathcal{R}$-module $\mathbb{E}$ as a composition factor of $\mathcal{J}$. In particular, $|1+\mathcal{J}|$ is relatively prime to $|\mathbb{E}^\times|$. The Schur–Zassenhaus theorem ([4, Section 3B]) then tells us that $\mathcal{R}^\times$ contains a copy S of $\mathbb{E}^\times$ (which is unique up to conjugacy) and splits as $\mathcal{R}^\times = (1+\mathcal{J}) \rtimes S$. We've proved part (b).

For part (c), $|\mathcal{J}| = |\mathcal{R}/\mathcal{J}|$ implies that $\mathcal{J} \simeq \mathbb{F}$ as $\mathcal{R}$-modules. Thus $\mathcal{J}$ acts trivially on the $\mathcal{R}$-module $\mathcal{J}$, so $\mathcal{J}^2 = \{0\}$. □

We can now begin our classification of the local rings R such that $R/J \simeq \mathbb{F}$. The taxonomy varies according as p is or is not 0 in R.

Case a. $p = 0$ in R. In this case, R is an algebra over the field $\mathbb{F}_p$. This means we can apply a well-known result of Wedderburn, often called the Wedderburn principal theorem. It says that R contains a subring S that is isomorphic to $\mathbb{F}$ and splits as $S \oplus J$ as an S-module (see, for example, [2, Section 72]). Less formally, we simply write

$$R = \mathbb{F} \oplus J. \tag{12}$$

For any nonzero $\epsilon \in J$, part (c) of Lemma 4 implies that

$$J = \{\lambda \cdot \epsilon : \lambda \in \mathbb{F}\} \text{ and } \epsilon^2 = 0.$$

We fix such an element ϵ. Now J is also a simple right R/J-module. Hence, for each $\lambda \in \mathbb{F}$,

$$\epsilon \cdot \lambda = \mu \cdot \epsilon,$$

for a unique $\mu \in \mathbb{F}$. In other words, $\mu = {}^\sigma\lambda$ for a bijection $\sigma : \mathbb{F} \to \mathbb{F}$. The module axioms imply that σ is a field automorphism of $\mathbb{F}$. Using the decomposition (12), we conclude that $R \simeq \mathbb{F}[\epsilon; \sigma]$.

Case b. $p \neq 0$ in R. As $p = 0$ in $\mathbb{F}$ but not in R, we see that p is a nonzero element of J. We show first that R must be commutative.

We have $J = Rp$ (since J is a simple R-module). Moreover, for any $x \in R$, the products px and xp only depend on $x + J$ (since $J^2 = \{0\}$). It follows that J lies in the center of R: in detail, for any $r, s \in R$,

$$\begin{aligned} r(sp) = (rs)p &= p(rs) \\ &= p(sr) \quad (\text{as } rs + J = sr + J) \\ &= (ps)r \\ &= (sp)r. \end{aligned}$$

Thus $1 + J$ is a central subgroup of $R^\times$. Invoking part (b) of Lemma 4, we see that $R^\times$ is abelian, whence R is commutative by part (a).

Observe next that the set of zero divisors in the finite commutative ring R (plus 0) is the principal ideal (p). This is exactly the definition of a Galois ring (for the prime p). Rings with this property, whose study was initiated by Krull, form a natural generalization of finite fields. Indeed, finite fields of p-power order are precisely the Galois rings of characteristic p. A fundamental result (generalizing the classification of finite fields) says that a Galois ring is determined by its characteristic and cardinality (up to isomorphism)—see, for example, [10,

Theorem 14.6]). Following standard practice, we write $\mathrm{GR}(p^s, p^{st})$ for the unique Galois ring of characteristic p^s and cardinality p^{st} (up to isomorphism). It can be realized as follows. Let $f(\mathrm{X})$ be any monic polynomial of degree t in $\mathbb{Z}_{p^s}[\mathrm{X}]$ whose reduction $\bmod p$ is irreducible in $\mathbb{Z}_p[\mathrm{X}]$ (in particular, $f(\mathrm{X})$ is itself irreducible). Then $\mathrm{GR}(p^s, p^{st}) \simeq \mathbb{Z}_{p^s}[\mathrm{X}]/\left(f(\mathrm{X})\right)$ (again, see [10, Theorem 14.6]).

We have $p^2 \in J^2$, so $p^2 = 0$. Thus R is a Galois ring of characteristic p^2 and cardinality p^{2m}, that is, $R = \mathrm{GR}(p^2, p^{2m})$.

We've completed the classification in the case $e = 2m$. Let's record its two strands in one place.

Proposition 2. *Let R be a local ring of order p^{2m} with $R/J \simeq \mathbb{F}_{p^m}$. There are $m+1$ possibilities for R (up to isomorphism) given as follows.*

(a) If R has characteristic p, then $R \simeq \mathbb{F}_{p^m}[\epsilon;\sigma]$ for a unique $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^m})$.

(b) If R does not have characteristic p, then $R \simeq \mathrm{GR}(p^2, p^{2m})$.

We're left with Case 3 in Section 6. That is, we want to enumerate the possible local rings of order p^3 (up to isomorphism). The residue field must be $\mathbb{F}_p$.

Raghavendran has classified *all* rings of order p^3 [7]. Recall that for us rings always have an identity. More generally, Antipkin and Elizarov give a full list of rings of order p^3 with or without identity in [1]. The novel aspect of their work, however, concerns rings without identity: for rings with identity, they appeal to [7]. From either reference, we can read off that there are

(i) 6 isomorphism classes of local rings of order p^3 for p odd,
(ii) 5 isomorphism classes of local rings of order 2^3,

given explicitly by the following list. The entries (1)–(5) apply for all p, (6) only for p odd.

(1) $\mathbb{Z}_{p^3} = \mathrm{GR}(p^3, p^3)$,
(2) $\mathbb{F}_p[\mathrm{X}]/\left(\mathrm{X}^3\right)$,
(3) $\mathbb{F}_p[\mathrm{X},\mathrm{Y}]/\left(\mathrm{X}^2, \mathrm{XY}, \mathrm{Y}^2\right)$,
(4) $\mathbb{Z}_{p^2}[\mathrm{X}]/\left(p\mathrm{X}, \mathrm{X}^2\right)$,
(5) $\mathbb{Z}_{p^2}[\mathrm{X}]/\left(p\mathrm{X}, \mathrm{X}^2 - p\right)$,
(6) $\mathbb{Z}_{p^2}[\mathrm{X}]/\left(p\mathrm{X}, \mathrm{X}^2 - kp\right)$ with k a nonsquare $\bmod p$.

8. MacHale's Theorem.

MacHale observed the following [6].

MacHale's Theorem. *If a finite ring R is not a field, then $|R^\times| \leq |R| - \sqrt{|R|}$. Equivalently, a finite ring R such that $|R^\times| > |R| - \sqrt{|R|}$ is necessarily a field.*

As noted in the introduction, Sury has also proved the inequality, in effectively the same way [9]. We give a small variant of MacHale's and Sury's argument below. First, we note that the result is an immediate consequence of our various bounds which, for ease of reference, we collect and restate.

Bounds on $R^\times$. *Let R be a ring of order n that is not a field. Write $n = p_1^{e_1} \cdots p_r^{e_r}$ for the prime factorization of n; if $r = 1$, we just write $n = p^e$. We have the following bounds (best possible in each case):*

(a) if $r > 1$, then $|R^\times| \le (p_1^{e_1} - 1) \cdots (p_r^{e_r} - 1)$;

(b) if $r = 1$ and $e = 2m$, then $|R^\times| \le p^{2m} - p^m$;

(c) if $r = 1$ and $e = 2m + 1 > 3$, then $|R^\times| \le p^{2m+1} - p^{m+1} - p^m + 1$;

(d) if $r = 1$ and $e = 3$, then $|R^\times| \le p^3 - p^2$.

It's a simple matter to check that in all cases $|R^\times| \le |R| - \sqrt{|R|}$ with equality only in Case (b). For Case (a), for example, suppose we have real numbers $a_1, \ldots, a_r$ with $a_i > 1$ (for $i = 1, \ldots, r$) and $r \ge 2$. We claim that

$$(a_1 - 1)(a_2 - 1) \cdots (a_r - 1) < a_1 a_2 \cdots a_r - \sqrt{a_1 a_2 \cdots a_r}. \tag{13}$$

To verify the claim, note first that

$$(a_1 - 1)(a_2 - 1) \cdots (a_r - 1) \le (a_1 - 1)(a_2 \cdots a_r - 1).$$

Thus we only need to check (13) when $r = 2$. That is, given $a > 1$ and $b > 1$, we want

$$(a - 1)(b - 1) < ab - \sqrt{ab},$$

or equivalently

$$a + b - 1 > \sqrt{ab}. \tag{14}$$

This is essentially the inequality of the arithmetic and geometric means of a and b. Indeed, from $(\sqrt{a} - \sqrt{b})^2 \ge 0$, we have

$$a + b \ge 2\sqrt{ab} = \sqrt{ab} + \sqrt{ab} > 1 + \sqrt{ab}$$

which gives (14) and hence also (13).

Our slight reworking of the proof of MacHale's theorem makes use of the following.

Lemma 5. *Let R be a finite ring. If $x \in R$ has a left or right inverse, then $x \in R^\times$, that is, x has a two-sided inverse.*

Proof. Suppose $wx = 1$ for $w, x \in R$. We'll show that $xw = 1$. Now if $xr = xr'$ for $r, r' \in R$, then $wxr = wxr'$, and so $r = r'$. That is, the map

$$r \mapsto xr : R \to R$$

is injective. Since R is finite, the map is also surjective. Hence $xy = 1$ for some $y \in R$. Standard manipulations then give $y = w$: in fact, we only have to combine the identity $(wx)y = w(xy)$ with $wx = 1$ and $xy = 1$. Therefore $xw = 1$, as required. □

We can now prove the theorem.

Proof of MacHale's theorem. Suppose a finite ring R contains nonzero nonunits, that is, R is not division ring, hence not a field (by Wedderburn's little theorem). For x a nonzero nonunit in R, consider the surjective homomorphism of abelian groups (or R-modules)

$$r \mapsto rx : R \to Rx.$$

Its kernel is $\operatorname{ann} x = \{r \in R : rx = 0\}$ (the (left) annihilator of x). Thus there is an isomorphism of abelian groups (or R-modules) $R/\operatorname{ann} x \simeq Rx$. In particular,

$$|R| = |\operatorname{ann} x||Rx|.$$

Writing R_0 for the set of nonunits in R, we have $\operatorname{ann} x \subseteq R_0$ and $Rx \subseteq R_0$. Indeed, no element of $\operatorname{ann} x$ or Rx can admit a left inverse, so each set consists of nonunits by Lemma 5. Hence $|R| \leq |R_0|^2$, equivalently $\sqrt{|R|} \leq |R_0|$. As R is the disjoint union of $R^\times$ and R_0, it follows that

$$|R| = |R^\times| + |R_0| \geq |R^\times| + \sqrt{|R|},$$

which proves the result. □

9. Which finite rings have the fewest units?

The precise question: among finite rings of a fixed order, which have the fewest units? Our methods yield a quick answer. As noted in Section 2, a finite ring is a product of rings of prime-power order. The problem therefore reduces once more to the case of rings R of order p^e (for p a prime, e a positive integer).

For any such ring, we have $R/J \simeq \mathrm{M}_{n_1}(\mathbb{F}_{q_1}) \times \cdots \times \mathrm{M}_{n_t}(\mathbb{F}_{q_t})$ for positive integers n_i and p-powers q_i (for $i = 1, \ldots, t$). As in Section 3, we write m_i for the multiplicity of the unique simple $\mathrm{M}_{n_i}(\mathbb{F}_{q_i})$-module as a composition factor of J (for $i = 1, \ldots, t$). Equation (6) then says $|J| = \prod_{i=1}^t q_i^{n_i m_i}$, and so

$$p^e = |R| = \prod_{i=1}^t q_i^{n_i m_i + n_i^2}. \tag{15}$$

Our argument hinges on equation (7) which, for convenience, we restate:

$$|R^\times| = \prod_{i=1}^t q_i^{n_i m_i} |\mathrm{GL}_{n_i}(\mathbb{F}_{q_i})|. \tag{7}$$

Recall that, for any positive integer n and prime power q,

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{j=0}^{n-1} \left(q^n - q^j\right).$$

Since $q^n - q^j \geq (q-1)^n$ (for $j = 0, \ldots, n-1$) with equality if and only if $n = 1$, it follows that

$$\begin{aligned} |\mathrm{GL}_n(\mathbb{F}_q)| &\geq (q-1)^n \cdots (q-1)^n \quad (n \text{ factors}) \\ &= (q-1)^{n^2}, \end{aligned}$$

with equality if and only if $n = 1$. Writing $q_i = p^{f_i}$ (for $i = 1, \ldots, t$), we obtain

$$|\operatorname{GL}_{n_i}(\mathbb{F}_{q_i})| \geq \left(p^{f_i} - 1\right)^{n_i^2} \geq (p-1)^{f_i n_i^2},$$

with equality if and only if $f_i = n_i = 1$. Using (7), we deduce that

$$|R^\times| \geq \prod_{i=1}^{t} p^{f_i n_i m_i} (p-1)^{f_i n_i^2} \geq \prod_{i=1}^{t} (p-1)^{f_i n_i m_i + f_i n_i^2}.$$

By (15), this last expression is just $(p-1)^e$. Moreover, equality holds if and only if $f_i = n_i = 1$ and $m_i = 0$, for $i = 1, \ldots, t$, which says precisely that

$$R \simeq \mathbb{F}_p \times \cdots \times \mathbb{F}_p \ (e \text{ factors}).$$

That is, among rings of order p^e, the product $\mathbb{F}_p \times \cdots \times \mathbb{F}_p$ (e factors) has the fewest units.

Putting the lower and upper bounds together, we see that a ring R of order p^e that is not a field (so that $e \geq 2$) satisfies

$$(p-1)^e \leq |R^\times| \leq p^e - p^{e/2}.$$

Acknowledgements. We are grateful to two anonymous reviewers for comments and recommendations which have made for a more readable article. Our presentation has also benefited from Susan Colley's eagle editorial eye.

References

[1] Antipkin, V. G., Elizarov, V. P. (1982). Rings of order p^3. *Siberian Math. J.* 23(4): 457–464.
[2] Curtis, C. W., and Reiner, I. (2006). *Representation Theory of Finite Groups and Associative Algebras.* Reprint of the 1962 original. Providence, RI: AMS Chelsea Publishing.
[3] Dennis, R. K., Farb, B. (1993). *Noncommutative Algebra.* Graduate Texts in Math., 144. New York, NY: Springer-Verlag.
[4] Isaacs, I. M. (2008). *Finite Group Theory.* Graduate Studies in Math., 92. Providence, RI: American Mathematical Society.
[5] Lam, T. Y. (2001). *A First Course in Noncommutative Rings,* 2nd ed. Graduate Texts in Math., 131. New York, NY: Springer-Verlag.
[6] MacHale, D. (1986). Wedderburn's theorem revisited. *Bull. Irish Math. Soc.* 17: 44–46.
[7] Raghavendran, R. (1969). Finite associative rings. *Compositio Math.* 21(2): 195–220.
[8] Rotman, J. (1979). *An Introduction to Homological Algebra.* San Diego, CA: Academic Press.
[9] Sury, B. (2019). A ring-theoretic approach to bound the totient function. *Amer. Math. Monthly.* 126(2): 167.
[10] Wan, Z-X. (2003). *Lectures on Finite Fields and Galois Rings.* Singapore: World Scientific.

Dept. of Mathematics, University of North Texas, Denton, TX 76203.
E-mail address: Jonathan.Cohen@unt.edu

Dept. of Mathematics, University of Oklahoma, Norman, OK 73019.
E-mail address: aroche@ou.edu