Taylor & Francis
Taylor & Francis Group

The American Mathematical Monthly

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

The Fundamental Theorem of Finite Fields: A Proof from First Principles

Anastasia Chavez & Christopher O'Neill

To cite this article: Anastasia Chavez & Christopher O'Neill (2022) The Fundamental Theorem of Finite Fields: A Proof from First Principles, The American Mathematical Monthly, 129:3, 268-275, DOI: 10.1080/00029890.2022.2011567

To link to this article: https://doi.org/10.1080/00029890.2022.2011567

The Fundamental Theorem of Finite Fields: A Proof from First Principles

Anastasia Chavez and Christopher O'Neill

Abstract. A mathematics student's first introduction to the fundamental theorem of finite fields (FTFF) often occurs in an advanced abstract algebra course and invokes the power of Galois theory to prove it. Yet, the combinatorial and algebraic coding theory applications of finite fields can show up early on for students in STEM. To make the FTFF more accessible to students lacking exposure to Galois theory, we provide a proof from algebraic "first principles."

1. INTRODUCTION. A student's first introduction to finite fields and the magic they invoke often occurs in an advanced undergraduate or graduate abstract algebra course. In particular, the fundamental theorem of finite fields (FTFF) is most commonly proved via Galois theory. Finite fields have many exciting combinatorial applications, one of which is algebraic coding theory. Error-correcting codes, t-designs, and Hamming codes are common topics for computer science majors with minimal abstract algebra training. For curious undergraduates with just one year of abstract algebra, such applied combinatorics is both enriching and inspiring. Yet, the Galois theory approach to finite fields leaves these students at a disadvantage. To fill an apparent gap in the accessibility of the FTFF, we provide a proof of this great theorem from "first principles," i.e., without appealing to Galois groups or splitting fields.

The Fundamental Theorem of Finite Fields.

1. *There is a field with exactly q elements if and only if $q = p^r$ for p prime, $r \geq 1$.*
2. *Any two finite fields of the same cardinality are isomorphic.*
3. *For any finite field $\mathbb{F}$ with $|\mathbb{F}| = p^r$ for p prime,*
   (a) *the additive group $(\mathbb{F}, +) \cong ((\mathbb{Z}_p)^r, +)$, and*
   (b) *the multiplicative group $(\mathbb{F} \setminus \{0\}, \cdot)$ is cyclic.*

The proof we provide here is built from several different sources, many of which either briefly mention or wave their hands at Galois theory for one or more parts of the argument [**1**–**4**]. This approach of introducing finite fields to those with little abstract algebra exposure has been successfully implemented in several iterations of the applied combinatorics course at our former home institution.

We provide this manuscript as a resource for those in need of a proof of the fundamental theorem that does not utilize the heavy machinery of Galois theory.

This article is organized as follows. In Section 2, we survey the assumed abstract algebra background, and in Section 3, we review quotient rings and outline a general method for explicitly constructing finite fields. Sections 4 and 5 together contain the proof of the FTFF, with the former section providing a key lemma that has some consequences of its own.

doi.org/10.1080/00029890.2022.2011567
MSC: Primary 11T06

2. PREREQUISITE BACKGROUND. In this section, we survey the minimal prerequisite definitions and results that are needed for this article. We assume the reader is familiar with undergraduate-level linear algebra (including vector space dimension) and ring theory (including cosets and quotient rings). Please see Dummit and Foote [2] and Hungerford [3] for more details. Note that all rings are assumed to be commutative and to have a multiplicative identity.

There are two main families of rings appearing in this article. The first is the ring $\mathbb{Z}_n$ of integers modulo $n \geq 2$. Note that $\mathbb{Z}_n$ is a field whenever n is prime, and contains zero-divisors whenever n is composite. The second is the polynomial ring $F[x]$ whose coefficient ring F is a field, as well as quotients $F[x]/I$ by an ideal I. Several times throughout this article, we will use the fact that the polynomial ring $F[x]$ is:

1. a *principal ideal domain (PID)*, meaning every ideal $I \subset F[x]$ can be written as $I = \langle f(x) \rangle$ for some $f(x) \in I$, and the quotient ring $F[x]/I$ is a field if and only if $f(x)$ is irreducible; and
2. a *unique factorization domain (UFD)*, meaning that every monic, nonconstant polynomial in $F[x]$ can be written uniquely (up to reordering) as a product of monic irreducible polynomials in $F[x]$.

We close this section with the following theorems, all of which are usually covered in an introductory course in rings, and which will be used in the proof of the Key Lemma given in Section 4.

The Root Theorem. *Fix a field F. For any $f \in F[x]$, we have $f(a) = 0$ if and only if $f(x) = (x - a)g(x)$ for some $g \in F[x]$.*

The Freshman's Dream. *Fix a prime p, and let R be a ring with characteristic p (that is, $p \cdot 1 = 0$ in R). If $a, b \in R$, then $(a + b)^p = a^p + b^p$.*

The First Isomorphism Theorem. *If R, S are rings and $\sigma : R \to S$ is a ring homomorphism, then $\mathrm{Im}(\sigma) \subset S$ is a subring, $\ker(\sigma) \subset R$ is an ideal, and $R/\ker\sigma \cong \mathrm{Im}(\sigma)$.*

3. CONSTRUCTING FINITE FIELDS. When constructing small finite fields from first principles, a common approach is to use the addition and multiplication tables (or "$+/\cdot$ tables") to help guide the behavior of the field's elements. For example, suppose we wish to discover all possible finite fields with 3 elements. We know there must be two distinguished elements 0 and 1, so denoting the only remaining element a, we can consider all possible ways of completing the $+/\cdot$ tables of $0, 1, a$ in such a way that all of the field axioms are satisfied. It is a fun exercise (with a lot of similarities to playing Sudoku) to show that the only possible configurations are those given in the left-hand side of Figure 1. In fact, one can easily check that these tables match those for the well-known field $\mathbb{Z}_3$. In general, this approach works for any prime value p to produce the finite field $\mathbb{Z}_p$.

When constructing finite fields of nonprime cardinality, such as 4 (a prime power), we can use the same approach. Let us consider elements $\{0, 1, a, b\}$. After checking all the ways to fill out the $+/\cdot$ tables, we see there is again a unique solution, depicted in Figure 1. As there is only one way to complete the tables, we once again obtain a unique finite field of this size, which we denote by $\mathbb{F}_4$. Note that $\mathbb{F}_4$ has characteristic 2 (i.e., $1 + 1 = 0$), so $\mathbb{F}_4$ is **not** simply $\mathbb{Z}_4$ (which is, in particular, not a field).

+	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

•	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

•	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Figure 1. Unique operation tables for $\mathbb{F}_3$ (left) and $\mathbb{F}_4$ (right).

It would be nice to identify $\mathbb{F}_4$ as a more "familiar" ring, as we did with $\mathbb{F}_3 \cong \mathbb{Z}_3$. One way to do this is to view the elements $0, 1, a, b \in \mathbb{F}_4$ as the elements $\overline{0}, \overline{1}, \overline{z}, \overline{z+1}$ in the quotient ring $\mathbb{Z}_2[z]/\langle z^2+z+1\rangle$. In particular, $\overline{z^2+z+1} = \overline{0}$ in this quotient ring, meaning $\overline{z^2} = \overline{-z-1}$. As such, each element can be represented by a polynomial in z with coefficients in $\mathbb{Z}_2$, and terms of degree 2 and higher can be eliminated via the substitution $\overline{z^2} = \overline{z+1}$, e.g.,

$$(\overline{z+1})(\overline{z+1}) = \overline{z^2+2z+1} = \overline{(z+1)+2z+1} = \overline{3z+2} = \overline{z},$$

or equivalently using division by z^2+z+1, e.g.,

$$(\overline{z+1})(\overline{z+1}) = \overline{z^2+2z+1} = \overline{1}(\overline{z^2+z+1}) + \overline{z} = \overline{z}.$$

Using this collection of elements, the $+/\cdot$ tables are then obtained by performing polynomial addition and multiplication, reducing coefficients modulo 2, and then performing polynomial long division by z^2+z+1; see Figure 2. Note that in order for this quotient ring to be a field, it is imperative that z^2+z+1 is irreducible. (In fact, it is the only degree-2 irreducible polynomial in $\mathbb{Z}_2[z]$.) To verify z^2+z+1 is indeed irreducible, note that any reducible degree 2 polynomial has a degree-1 factor, and therefore has a root by the Root Theorem. However, neither element of $\mathbb{Z}_2$ is a root of z^2+z+1, so it must be irreducible.

+	$\overline{0}$	$\overline{1}$	$\overline{z}$	$\overline{z+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{z}$	$\overline{z+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{z+1}$	$\overline{z}$
$\overline{z}$	$\overline{z}$	$\overline{z+1}$	$\overline{0}$	$\overline{1}$
$\overline{z+1}$	$\overline{z+1}$	$\overline{z}$	$\overline{1}$	$\overline{0}$

	$\overline{0}$	$\overline{1}$	$\overline{z}$	$\overline{z+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{z}$	$\overline{z+1}$
$\overline{z}$	$\overline{0}$	$\overline{z}$	$\overline{z+1}$	$\overline{1}$
$\overline{z+1}$	$\overline{0}$	$\overline{z+1}$	$\overline{1}$	$\overline{z}$

Figure 2. Operation tables for $\mathbb{Z}_2[z]/\langle z^2+z+1\rangle$.

As a final example, we construct the finite field of 8 elements, $\mathbb{F}_8$ (a similar illustration of the construction of $\mathbb{F}_9$ can be found in [1]).

Proceeding as above, we wish to use polynomial quotient rings to write $\mathbb{F}_8$ in the form $\mathbb{Z}_2[z]/\langle f(z)\rangle$, where f is an irreducible polynomial of degree 3. By the Root Theorem, any reducible degree-3 polynomial has a root, so by inspection of all $2^3 = 8$ polynomials of degree 3 in $\mathbb{Z}_2[z]$, we see that only two, namely z^3+z+1 and z^3+z^2+1, are irreducible. Let

$$\mathbb{F}_8 = \mathbb{Z}_2[z]/\langle z^3+z+1\rangle \qquad \text{and} \qquad \mathbb{F}_8' = \mathbb{Z}_2[w]/\langle w^3+w^2+1\rangle.$$

Although the two quotient rings above are both fields with 8 elements, their multiplication "rules" appear different, in that in $\mathbb{F}_8$ we reduce terms of degree 3 and higher

using the equality $\overline{z^3+z+1}=\overline{0}$, while in $\mathbb{F}_8'$ we reduce using $\overline{w^3+w^2+1}=\overline{0}$. For example, despite the visual similarity, the left-hand-side products

$$\mathbb{F}_8 : (\overline{z^2+1})(\overline{z+1}) \bmod (\overline{z^3+z+1}) = \overline{z^2}, \tag{1}$$

$$\mathbb{F}_8' : (\overline{w^2+1})(\overline{w+1}) \bmod (\overline{w^3+w^2+1}) = \overline{w} \tag{2}$$

yield visually distinct results. That said, $\mathbb{F}_8$ and $\mathbb{F}_8'$ are isomorphic by the FTFF, and we give an explicit isomorphism in Section 5.

4. THE KEY LEMMA: FACTORING OVER FINITE FIELDS. For a finite field $\mathbb{F}_q$ with $q=p^r$, the key to the FTFF turns out to be factoring the polynomial x^q-x, both over $\mathbb{F}_q$ itself and over $\mathbb{Z}_p$. The Key Lemma, stated below and followed immediately by several examples, identifies precisely how x^q-x factors as a product of irreducible polynomials over both fields.

The Key Lemma. *Suppose $q=p^r$ for p prime and $r\in\mathbb{Z}_{\geq 1}$.*

1. *If $\mathbb{K}$ is any finite field with $|\mathbb{K}|=q$, then the polynomial x^q-x factors over $\mathbb{K}$ as a product of distinct linear factors.*
2. *The polynomial x^q-x factors over $\mathbb{Z}_p$ as the product of all irreducible polynomials over $\mathbb{Z}_p$ with degree dividing r.*

Let us work through a few examples. We start with $q=4$, which we constructed as

$$\mathbb{F}_4=\mathbb{Z}_2[z]/\langle z^2+z+1\rangle=\{\overline{0},\overline{1},\overline{z},\overline{z+1}\}$$

in Section 3. Since $0,1\in\mathbb{Z}_2$ are both roots of x^4-x, the Root Theorem tells us x and $x-1$ are both factors. The Key Lemma implies all remaining factors are of degree 2. Since polynomial long division by $x-1$ yields

$$x^4-x=x(x-1)(x^2+x+1),$$

the Key Lemma implies x^2+x+1 is the **only** irreducible polynomial of degree 2 over $\mathbb{Z}_2$, a fact we also observed in Section 3. Now, since $\mathbb{Z}_2\subsetneq\mathbb{F}_4$, the "extra" two elements of $\mathbb{F}_4$ provide more coefficients at our disposal when factoring, so some irreducible polynomials over $\mathbb{Z}_2$, like x^2+x+1 in this case, may be factored further over $\mathbb{F}_4$. Indeed, we obtain four distinct linear factors, one for each element of $\mathbb{F}_4$, i.e.,

$$\begin{aligned} x^4-x &= x(x-1)(x^2+x+1)\\ &= x(x-\overline{1})(x-\overline{z})(x-\overline{z+1}), \end{aligned}$$

wherein $\overline{z}$ and $\overline{z+1}$ are the roots of x^2+x+1 in $\mathbb{F}_4$. Remember that the polynomials in the above expression live in $\mathbb{F}_4[x]$, so in the second line $\overline{z}$ and $\overline{z+1}$ are **coefficients** that live in $\mathbb{F}_4$.

For $q=8$, after factoring x and $x+1$ out of x^8-x, we obtain a degree-6 polynomial that, by the Key Lemma, must factor into (exactly 2) distinct degree-3 irreducible factors over $\mathbb{Z}_3$. As both irreducible polynomials were identified in Section 3, this yields

$$\begin{aligned} x^8-x &= x(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)\\ &= x(x+1)(x^3+x+1)(x^3+x^2+1) \end{aligned}$$

as the factorization over $\mathbb{Z}_3$. It is in this way that we can use the Key Lemma to locate **all** possible choices of an irreducible polynomial when constructing a finite field of a particular size. Next, to factor further over $\mathbb{F}_8$, we will choose the representation $\mathbb{F}_8 = \mathbb{Z}_2[z]/\langle z^3 + z + 1\rangle$ and obtain

$$x^3 + x + 1 = (x - \overline{z})(x - \overline{z^2})(x - \overline{z^2 + z}),$$
$$x^3 + x^2 + 1 = (x - \overline{z + 1})(x - \overline{z^2 + 1})(x - \overline{z^2 + z + 1}),$$

Had we instead chosen the representation $\mathbb{F}'_8 = \mathbb{Z}_2[w]/\langle w^3 + w^2 + 1\rangle$, we would have obtained

$$x^3 + x + 1 = (x - \overline{w + 1})(x - \overline{w^2 + 1})(x - \overline{w^2 + w}),$$
$$x^3 + x^2 + 1 = (x - \overline{w})(x - \overline{w^2})(x - \overline{w^2 + w + 1}),$$

as the remaining linear factors of $x^8 - x$.

We give one final example before proving the Key Lemma. Applying a similar process as above for $q = 9$, we obtain

$$x^9 - x = x(x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$$

over $\mathbb{Z}_3$, and factoring further over $\mathbb{F}_9 = \mathbb{Z}_3[z]/\langle z^2 + 1\rangle$ (this time there were 3 possible representations to choose from) yields

$$x^2 + 1 = (x - \overline{z})(x - \overline{2z}),$$
$$x^2 + x + 2 = (x - \overline{z + 1})(x - \overline{2z + 1}),$$
$$x^2 + 2x + 2 = (x - \overline{z + 2})(x - \overline{2z + 2}),$$

which we encourage the reader to verify as an exercise.

Proof of the Key Lemma. Suppose $q = p^r$ for p prime and $r \geq 1$, and suppose $\mathbb{K}$ is a field with $|\mathbb{K}| = q$. Since $\mathbb{K}$ is a field, $(\mathbb{K} \setminus \{0\}, \cdot)$ is a group of order $q - 1$, meaning that every element has order dividing $q - 1$. As such, $a^{q-1} - 1 = 0$ for every nonzero $a \in \mathbb{K}$, and thus each is a root of $x^q - x$. By the Root Theorem, this produces q distinct linear factors and $x^q - x$ has degree q, so this must be precisely the list of factors, proving part 1.

Next, fix an irreducible polynomial $f \in \mathbb{Z}_p[x]$, and let $d = \deg f$. We wish to show $f(x) \mid x^q - x$ if and only if $d \mid r$, as this implies that the irreducible factors of $f(x)$ over $\mathbb{Z}_p$ claimed in part (b) are precisely those that appear. Since f is irreducible, as stated in Section 2, the quotient ring $K = \mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field. To more clearly distinguish K from the field $\mathbb{F}_q$ constructed elsewhere in this article, we will denote the elements of K using the "bracket" notation $[h(x)]$ for $h \in \mathbb{Z}_p[x]$ rather than with the "overline" notation. Since $|K| = p^d$, we can list the elements of K as

$$K = \left\{[h_1(x)], \ldots, [h_{p^d}(x)]\right\},$$

with $h_1(x) = 0$. If f is linear, then the claim follows from part 1, so assume $d \geq 2$.

First, suppose $d \mid r$. Since K is a field, multiplication is cancellative, so multiplying by $[x]$ permutes the set of nonzero elements. In particular, the list

$$[x][h_2(x)], \quad [x][h_3(x)], \quad \ldots, \quad [x][h_{p^d}(x)]$$

contains every nonzero element of K exactly once. As such, the product of all elements in this list can be simplified in two ways to obtain

$$\begin{aligned}[x][h_2(x)]\cdots[x][h_{p^d}(x)] &= [h_2(x)][h_3(x)]\cdots[h_{p^d}(x)] \\ &= [x^{p^d-1}][h_2(x)]\cdots[h_{p^d}(x)],\end{aligned}$$

in K, where the expressions on either side of the first equality consist of the product of the same $p^d - 1$ elements of K (albeit in a different order). Subtracting and factoring yields

$$[x^{p^d-1} - 1][h_2(x)][h_3(x)]\cdots[h_{p^d}(x)] = [0] \in K,$$

which implies $[x^{p^d-1} - 1] = [0]$ since K has no zero-divisors. This means we have $x^{p^d-1} - 1 \in \langle f(x)\rangle \subseteq \mathbb{Z}_p[x]$ and thus $f(x) \mid x^{p^d-1} - 1$. Since $d \mid r$, say $r = dk$ for some $k \in \mathbb{Z}$,

$$p^r - 1 = (p^d - 1)(p^{d(k-1)} + p^{d(k-2)} + \cdots + p^d + 1),$$

meaning $p^d - 1 \mid p^r - 1$. Analogously, fixing $t \in \mathbb{Z}_{\geq 0}$ so that $p^r - 1 = t(p^d - 1)$, we have

$$x^{q-1} - 1 = x^{t(p^d-1)} - 1 = (x^{p^d-1} - 1)(x^{(p^d-1)(t-1)} + x^{(p^d-1)(t-2)} + \cdots + 1).$$

Putting all of this together, we conclude $f(x) \mid x^{p^d-1} - 1 \mid x^q - x$.

Conversely, suppose $f(x) \mid x^q - x$. Writing $r = ad + b$ for $a, b \in \mathbb{Z}$ with $0 \leq b < d$ via the division algorithm, we wish to show $b = 0$. By way of contradiction, suppose that b is positive. Since $|K| = p^d$, similar reasoning as in the first paragraph of this proof implies $[x]^{p^d} = [x]$ in K, and by assumption $[x^q - x] = [0]$ in K, so

$$[x] = [x^q] = [x^{p^{ad+b}}] = [(\cdots((\underbrace{x^{p^d})^{p^d})\cdots)^{p^d}}_{a \text{ times}})^{p^b}] = [x^{p^b}].$$

By the Freshman's Dream, for any $g(x) = g_0 + g_1x + g_2x^2 + \cdots \in \mathbb{Z}_p[x]$, we have

$$\begin{aligned}[g(x)]^{p^b} &= [(g_0)^{p^b} + (g_1)^{p^b}(x^{p^b}) + (g_2)^{p^b}(x^{p^b})^2 + \cdots] \\ &= [g_0 + g_1x + g_2x^2 + \cdots] \\ &= [g(x)],\end{aligned}$$

meaning every element of K is a root of $x^{p^b} - x$. However, this is impossible by the Root Theorem since K has $p^d > p^b$ elements, so we conclude $b = 0$. This completes the proof that $f(x) \mid x^q - x$ if and only if $d \mid r$.

There remains one final claim to prove: that each irreducible polynomial $f(x)$ in the factorization of $x^q - x$ over $\mathbb{Z}_p$ appears only once. Indeed, by part 1, the roots of $x^q - x$ in K are all distinct, so $x^q - x$ cannot have repeated factors over $\mathbb{Z}_p$ as this would yield repeated roots in K. This completes the proof. ■

5. THE FUNDAMENTAL THEOREM. In this section, we use the Key Lemma to prove the FTFF in its entirety. Before diving into the proof, let's briefly explore some of its implications in the context of $\mathbb{F}_8$ and $\mathbb{F}_8'$ from Section 3.

First, the set $\mathbb{F}_8 \setminus \{\overline{0}\}$ is ensured to be a cyclic group under multiplication, meaning there is some element $a \in \mathbb{F}_8$ such that the list $a, a^2, a^3, \ldots$ includes every nonzero element of $\mathbb{F}_8$. One such element is $\overline{z+1}$, and we can readily check that every nonzero element of $\mathbb{F}_8$ can be written as $(\overline{z+1})^n$ for some n. In fact, it turns out that any nonzero element we choose for a will do the trick (except $a = \overline{1}$, of course). This is not true in general: in $\mathbb{F}_7$ (which is isomorphic to $\mathbb{Z}_7$), only 2 nonzero elements generate $\{1, 2, 3, 4, 5, 6\}$ as a group under multiplication modulo 7 (one such element is $3 \in \mathbb{Z}_7$, and we encourage the reader to locate the other).

Second, the FTFF implies that $\mathbb{F}_8$ and $\mathbb{F}_8'$ are isomorphic, but it is not hard to show that the map $\mathbb{F}_8 \to \mathbb{F}_8'$ given by $\overline{az^2+bz+c} \mapsto \overline{aw^2+bw+c}$ is **not** an isomorphism (compare, for instance, the right-hand sides of (1) and (2) in Section 3). One possible isomorphism $\sigma : \mathbb{F}_8 \to \mathbb{F}_8'$ turns out to be

$$\begin{aligned} \sigma(\overline{0}) &= \overline{0}, & \sigma(\overline{z}) &= \overline{w+1}, & \sigma(\overline{z^2+z}) &= \overline{w^2+w}, \\ \sigma(\overline{1}) &= \overline{1}, & \sigma(\overline{z^2}) &= \overline{w^2+1}, & \sigma(\overline{z^2+z+1}) &= \overline{w^2+w+1}, \\ \sigma(\overline{z+1}) &= \overline{w}, & \sigma(\overline{z^2+1}) &= \overline{w^2}, \end{aligned}$$

which happens to map a generator to another generator. In general, locating an explicit isomorphism between finite fields of equal size need not be easy, as mapping a generator to a generator does not always yield an isomorphism. This map sends the element $\overline{z+1} \in \mathbb{F}_8$ to the element $\overline{w} \in \mathbb{F}_8'$, and the remaining nonzero elements, necessarily of the form $(\overline{z+1})^n$ for some $n \geq 2$ by the previous paragraph, is sent to $(\overline{w})^n$. This guarantees multiplication is preserved by σ. Verifying that addition is preserved can be done manually, or by observing that every element $a \in \mathbb{F}_8$ can be written uniquely as a sum involving $\overline{1}$, $\overline{z}$, and $\overline{z^2}$, and that for each such a, $\sigma(a)$ equals precisely the image of this sum (for example, $\sigma(\overline{z^2+1}) = \sigma(\overline{z^2}) + \sigma(\overline{1}) = \overline{w^2}$).

Proof of the FTFF. Consider the subring $R \subset \mathbb{F}_q$ consisting of $0, 1, 1+1, \ldots \in \mathbb{F}_q$, and let $p = |R|$ (the *characteristic* of $\mathbb{F}_q$). We see that $R \cong \mathbb{Z}_p$, and so p must be prime, as otherwise $\mathbb{Z}_p$ (and thus $\mathbb{F}_q$) would contain zero-divisors. This makes $\mathbb{F}_q$ a vector space over the field $\mathbb{Z}_p$, necessarily finite-dimensional since $\mathbb{F}_q$ is finite, so the fundamental theorem of linear algebra tells us that $(\mathbb{F}_q, +) \cong (\mathbb{Z}_p)^r$ for some $r \geq 1$. This proves part 3(a) and the forward direction of part 1.

For the backwards direction of part 1, we must prove $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field with exactly p^r elements. Thus, it is enough to show there exists at least one irreducible polynomial in $\mathbb{Z}_p[x]$ of each degree r. The Key Lemma implies that the sum of the degrees of all irreducible polynomials in $\mathbb{Z}_p[x]$ whose degree divides r is p^r. If we sum only those degrees strictly dividing r, we obtain

$$\sum_{d|r,\, d\neq r} p^d \leq \sum_{d<r} p^d = \frac{p^r-1}{p-1} < p^r.$$

As such, there is an irreducible polynomial $f \in \mathbb{Z}_p[x]$ with $\deg f = r$, as desired.

Next, we prove part 3(b). Let N denote the maximum order of any element of the group $(\mathbb{F}_q \setminus \{0\}, \cdot)$. We claim every element has order dividing N. Indeed, if $|a| = N$ and $|b| = m \nmid N$, then there exists some prime power t such that $t \mid m$ and $t \nmid N$. However, $|ab^{m/t}| = \operatorname{lcm}(N, t) > N$ contradicts the maximality of N. This proves the claim. Now, this means every nonzero element of $\mathbb{F}_q$ is a root of $x^N - 1$, which is only

possible if $\deg(x^N - 1) \geq q - 1 = |\mathbb{F}_q \setminus \{0\}|$. As such, $N = q - 1$, and any element of order N generates $(\mathbb{F}_q \setminus \{0\}, \cdot)$, thereby proving part 3(b).

Finally, we prove part 2. Fix any irreducible polynomial $f \in \mathbb{Z}_p[x]$ of degree r. We claim $\mathbb{F}_q \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$. Since $f(x)$ divides $x^q - x$ by the Key Lemma, some element $a \in \mathbb{F}_q$ is a root of f. Consider the homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}_p[x] &\longrightarrow \mathbb{F}_q \\ g(x) &\longmapsto g(a), \end{aligned}$$

which has kernel

$$\ker(\varphi) = \{g(x) : g(a) = 0\} = \langle f(x)\rangle$$

by the Root Theorem, since f is irreducible over $\mathbb{Z}_p$ and has a as a root. As such, the First Isomorphism Theorem implies $\mathbb{Z}_p[x]/\langle f(x)\rangle \cong \mathrm{Im}(\varphi)$, and φ must be surjective since $\mathbb{F}_q$ and $\mathrm{Im}(\varphi)$ both have q elements, so the claimed isomorphism is shown. ■

ACKNOWLEDGEMENTS. The authors would like to thank Scott Chapman, Lily Silverstein, and Wencin Poh for numerous helpful conversations. We are grateful to Jesús A. De Loera for sharing his lecture notes from the course that inspired this manuscript. We also wish to thank the referees for their insightful comments.

ORCID
Christopher O'Neill http://orcid.org/0000-0001-7505-8184

REFERENCES

[1] Biggs, N. L. (1989). *Discrete Mathematics*, 2nd ed. New York: Oxford Science Publications, The Clarendon Press, Oxford Univ. Press.
[2] Dummit, D. S., Foote, R. (2004). *Abstract Algebra*, 3rd ed. Hoboken, NJ: John Wiley & Sons, Inc.
[3] Hungerford, T. W. (1980). *Algebra*. Graduate Texts in Mathematics, Vol. 73. New York: Springer-Verlag.
[4] Lang, S. (2002). *Algebra*, Graduate Texts in Mathematics, Vol. 211, 3rd ed. New York: Springer-Verlag.

ANASTASIA CHAVEZ received her Ph.D. in mathematics from the University of California, Berkeley. She held a visiting position at the University of California, Davis before joining Saint Mary's College of California.
Department of Mathematics and Computer Science, Saint Mary's College of California, Moraga, CA 94575 USA
amr59@stmarys-ca.edu

CHRISTOPHER O'NEILL is an Associate Professor at San Diego State University. He received his Ph.D, from Duke University and held visting positions at Texas A&M University and University of California Davis.
Department of Mathematics and Statistics, San Diego State University, San Diego, CA 92182, USA
cdoneill@sdsu.edu