An Exploration of Quadratic Residues in Finite Fields

Ian Kessler

May 7, 2014

SIGNATURE PAGE

This thesis for honors recognition has been approved for the

Department of Mathematics, Computer Science, and Engineering

Director — 5/5/2014 (Date)

Reader — 5-5-14 (Date)

Reader — 5/5/14 (Date)

Abstract

If an element in a given field can be expressed as a product of two equivalent elements that are also in the field, then this element is a quadratic residue of that field. For example, the set of quadratic residues of the field of rational numbers are the ratios of perfects squares. In the real numbers, the quadratic residues are the nonnegative numbers, and in the complex field, every number is a quadratic residue. We will explore quadratic residues of finite fields, which are fields with a finite number of elements. Finite fields operate under modular arithmetic. Furthermore, we can construct any finite field using factor rings of polynomial rings. We will explore relationships between finite fields and their quadratic residues, including similarities and differences between finite and the more familiar infinite fields.

Contents

List of Figures

List of Tables

1 Introduction

When two integers are added together, the sum of those integers is also an integer. That is, for all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$. For example, $5, 7 \in \mathbb{Z}$ and $5 + 7 = 12 \in \mathbb{Z}$. This implies the set of integers has closure under addition. Furthermore, when you multiply two integers together, the product of those integers is also an integer. That is, for all $a, b \in \mathbb{Z}$, $ab \in \mathbb{Z}$. This implies the set has closure under multiplication. The same can be said for multiplication and addition over rational numbers, real numbers, and complex numbers. However, notice that division is not closed in the integers, as $\frac{1}{2} \notin \mathbb{Z}$, but division is closed in the rational numbers, real numbers, and complex numbers. For any integer a, $a + 0 = a$ and $a \cdot 1 = a$. Furthermore, for all $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0$. The same is true for the rational numbers, real numbers, and complex numbers. These properties give the integers an algebraic structure that is different than the rational numbers or real numbers. These properties of the integers are taken for granted. However, knowing these properties like those mentioned above helps us to generalize algebraic structures. This notion of algebraic abstraction is important, because with one proof we can make statements that are true about a vast number of systems, such as the integers, polynomials with real coefficients, and real-valued matrices.

The type of algebraic structures that will be the focus of this paper are fields and finite fields. Furthermore, we will look into the idea of quadratic residues in finite fields. A quadratic residue is an abstraction of square root. Given a field element a, is there another field element b such that $b^2 = a$? The nature of quadratic residues is well known in the standard number systems. The quadratic residues of the field of rational numbers are the ratios of perfect squares. The quadratic residues of the field of real numbers are all nonnegative real numbers. We know the quadratic residues of the field of complex numbers is the entire field of complex numbers thanks to the fundamental theorem of algebra. In this work, we will develop the theory of finite

fields, completely characterize finite fields, and explore quadratic residues in finite fields.

2 Preliminaries

A *ring* is an Abelian group under addition that also has associative multiplication that distributes over addition. A *zero-divisor* is a nonzero element a of a commutative ring R, such that there is a nonzero element $b \in R$ with $ab = 0$. An *integral domain* is a commutative ring with unity and no zero-divisors.

Theorem 1 (Cancellation)**.** *Let D be an integral domain. For all $a, b, c \in D$ if $ab = ac$ and $a \neq 0$, then $b = c$.*

Proof. We assume $ab = ac$. Then $ab - ac = 0$, so $a(b - c) = 0$. Since $a \neq 0$, then $(b - c) = 0$, so $b = c$. □

A *field* is a commutative ring with unity in which every nonzero element is a unit. A *finite field* is a field that has a finite number of elements. An *infinite field* is a field that has an infinite number of elements. Examples of infinite fields are $\mathbb{Q}$, the field of rational numbers, $\mathbb{R}$, the field of real numbers, and $\mathbb{C}$, the field of complex numbers. Let $\alpha \in F$ where F is a field. Then α is a quadratic residue of F if there exists $a \in F$, such that $a^2 = \alpha$. In other words, an element in a field is a quadratic residue of the field if the square root of the element is also in the field. The quadratic residues of $\mathbb{Q}$ are the ratios of perfect squares $\frac{p^2}{q^2}$ where $p, q \in \mathbb{Z}$. The quadratic residues of $\mathbb{R}$ are the nonnegative numbers $\{x \in \mathbb{R} : x \geq 0\}$. For all $z \in \mathbb{C}$, by the Fundamental Theorem of Algebra, z is a quadratic residue in $\mathbb{C}$. However, quadratic residues in finite fields are the focus of this paper. In order to explore quadratic residues in finite fields, we first need to develop the theory necessary to classify finite fields and to understand the structure of finite fields. We begin by exploring some examples of finite fields.

Let $\mathbb{Z}_n$ be the set of elements such that for all $a, b \in \mathbb{Z}_n$, if n divides $a - b$ then $a \equiv b \pmod{n}$. Thus $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. For example, $3 \equiv 15 \pmod{12}$ and $5 \equiv -7 \pmod{12}$.

Theorem 2. *Let D be a finite set of elements. Then, D is an integral domain if and only if D is a field.*

Proof. Suppose D is a finite integral domain with unity 1. Let a be any nonzero element D. We must show that a is a unit. If $a = 1$, a is its own inverse, so we may assume $a \neq 1$. Now consider the following sequence of elements of $D : a, a^2, a^3, ...$ Since D is finite, there must me two positive integers i and j, such that $i > j$ and $a^i = a^j$. By Theorem 1, $a^{i-j} = 1$. Since a is not the unity, we know that $i - j > 1$. Thus, $a \cdot a^{i-j-1} = a^{i-j} = 1$, so a^{i-j-1} is the inverse of a. Therefore, D is a field.

Suppose D is a finite field. Let $a, b \in D$ such that $ab = 0$. Since D is a field, then there exists $a^{-1} \in D$. Therefore, $a^{-1}ab = a^{-1}0 = 0$. Thus, $b = 0$. Therefore, D has no zero-divisors, so D is an integral domain. □

Theorem 3 ($\mathbb{Z}_p$ is a Field)**.** *$\mathbb{Z}_p$ is a field if and only if p is prime.*

Proof. For the sake of contrapositive, we assume that p is not prime. Then there exists non-zero elements $a, b < p$ such that $ab = p$. Thus, in $\mathbb{Z}_p$, $ab = 0$. We assume a is a unit of $\mathbb{Z}_p$. Then $a^{-1}ab = a^{-1}0$, so $b = 0$. This contradicts the fact that $b \neq 0$. Thus, not every element is a unit, so $\mathbb{Z}_p$ is not a field.

We assume p is prime. Then, suppose $a, b \in \mathbb{Z}_p$ such that $ab = 0$. Then $ab = pk$ for some integer k. By Euclid's Lemma, $p|a$ or $p|b$. Thus, in $\mathbb{Z}_p$, $a = 0$ or $b = 0$. Thus, $\mathbb{Z}_p$ is an integral domain. By Theorem 2, since $\mathbb{Z}_p$ is a finite integral domain, then it is also a field. □

The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0.

Theorem 4 (Characteristic of a Ring with Unity)**.** *Let R be a ring with unity* 1*. If* 1 *has order n under addition, then the characteristic of R is n.*

Proof. If 1 has additive order n, then $n \cdot 1 = 0$, and n is the least positive integer with this property. So, for any $x \in R$, we have

$$\begin{aligned} n \cdot x &= x + x + \cdots + x \text{ (n summands)} \\ &= (1 + 1 + \cdots + 1)x \text{ (n summands)} \\ &= (n \cdot 1)x = 0x = 0 \end{aligned}$$

□

Since 1 has order p in $\mathbb{Z}_p$, then $\mathbb{Z}_p$ has characteristic p.

We have shown that if p is prime, then $\mathbb{Z}_p$ is a finite field with characteristic p. Although finite fields can be of the form $\mathbb{Z}_p$ where p is prime, they are not the only type of finite fields. However, all finite fields have prime characteristics.

Theorem 5 (Characteristic of a Finite Field)**.** *The characteristic of a finite field is prime.*

Proof. Suppose that 1 has order n and that $n = st$, where $1 \leq s,\ t \leq n$. Then $0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$. By Theorem 2, since finite fields are integral domains, then $(s \cdot 1) = 0$ or $(t \cdot 1) = 0$. Since n is the least positive integer with the property $n \cdot 1 = 0$, we must have $s = n$ or $t = n$. Thus, n is prime. By Theorem 4, the characteristic is n. Thus, every finite field has a prime characteristic. □

Knowing that finite fields have prime characteristics will help us in the classification of all finite fields and help us to understand the structure of finite fields. However, we first need to develop more ring theory and the fundamentals of field theory before we develop finite fields.

3 Fields From Factor Rings

Let R be a commutative ring with unity and let $a \in R$. Then, the set $\langle a \rangle = \{ra : r \in R\}$ is a subring of R called the *principal ideal* generated by a. In general, an ideal A of R is a subring of R such that for all $r \in R$ and for all $a \in A$, both $ra \in A$ and $ar \in A$. The set of cosets of $\langle a \rangle$ in R is $R/\langle a \rangle = \{r + \langle a \rangle : r \in R\}$. In this case, r represents the *coset representative* of each coset.

For example, since $3 \in \mathbb{Z}$, then $\langle 3 \rangle$ is the principal ideal of $\mathbb{Z}$ generated by 3.

The only unique cosets of $\langle 3 \rangle$ in $\mathbb{Z}$ are

$$0 + \langle 3 \rangle = \{0 + 0, 0 + 3, 0 - 3, 0 + 6, 0 - 6, ...\}$$
$$1 + \langle 3 \rangle = \{1 + 0, 1 + 3, 1 - 3, 1 + 6, 1 - 6, ...\}$$
$$2 + \langle 3 \rangle = \{2 + 0, 2 + 3, 2 - 3, 2 + 6, 2 - 6, ...\}$$

Adding 3 to every element in $\langle 3 \rangle$ has the same effect as adding 0 to every element in $\langle 3 \rangle$.

$$3 + \langle 3 \rangle = \{3 + 0, 3 + 3, 3 - 3, 3 + 6, 3 - 6, ...\} = \{3, 6, 0, 9, -3, ...\} = 0 + \langle 3 \rangle$$

We see that the principal ideal "absorbs" multiples of 3. Each of these cosets are distinguished by their coset representative where the coset representatives are under modulo 3. We know that $\mathbb{Z}_3$ also operates under modulo 3. In fact, this set has the same algebraic structure as $\mathbb{Z}_3$.

In general, for $R/\langle a \rangle$, each coset can be recognized as an element that is identified by its coset representative where the set forms a factor ring where coset representatives

are under modulo a and for all $s, t \in R$.

$$(s + \langle a \rangle) + (t + \langle a \rangle) = s + t + \langle a \rangle$$
$$(s + \langle a \rangle)(t + \langle a \rangle) = st + \langle a \rangle$$

A *maximal ideal* A of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$ then $B = A$ or $B = R$. Thus, the only ideal that contains a maximal ideal is the entire ring.

Theorem 6. *Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.*

Proof. We assume R/A is a field and B is an ideal of R that properly contains A. Let $b \in B$ but $b \notin A$. Then $b + A$ is a nonzero element of R/A and, therefore, there exists an element $c + A$ such that $(b + A) \cdot (c + A) = 1 + A$, the multiplicative identity of R/A. Since $b \in B$ and B is an ideal, we have $bc \in B$. Since $bc = 1$, then $1 - bc = 0$, the additive identity, so $(1 - bc) \in A \subset B$. Since B has closure under addition, $(1 - bc) + bc = 1 \in B$. Since B is an ideal, then for all $r \in R$, $1 \cdot r = r \in B$, so $B = R$. Thus, A is maximal.

We assume A is maximal and let $b \in R$ but $b \notin A$. Consider $B = \{br + a : r \in R, a \in A\}$. For all $r \in R$, $r(br + a) = (br + a)r = br^2 + ra$ where $r^2 \in R$ and $ra \in A$. Thus, B is an ideal of R. Since $A = \{br + a : r = 0, a \in A\}$ and $A \bigcap \{br + a : r = 1, a = 0\} = \emptyset$, then B properly contains A. Since A is maximal, we must have $B = R$. Thus, $1 \in B$, so $1 = bc + a'$ where $a' \in A$ and $c \in R$. Then, $1 + A = (bc + a') + A = bc + A = (b + A)(c + A)$. Thus, the multiplicative inverse of b is c. Thus, R/A is a field. □

Let R be a commutative ring. Thus, the *ring of polynomials* over R is defined as

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in R, \text{n is a nonnegative integer}\}$$

Every element in $R[x]$ is a polynomial that has coefficients from R.

Theorem 7 (The Factor Theorem)**.** *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.*

Proof. By the division algorithm, there exists unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = (x - a)q(x) + r(x)$ and $\deg(r(x)) = 0$. We assume a is a zero of $f(x)$. Then, $f(a) = (a - a)q(a) + r(a) = r(a) = 0$. Since $\deg(r(x)) = 0$ then $r(x) = c \in F$. Thus, $r(x) = c = 0$, so $(x - a)$ is a factor of $f(x)$. We assume $(x - a)$ is a factor of $f(x)$. Then, $f(x) = (x - a)q(x)$ for some $q(x) \in F[x]$. Thus, $f(a) = (a - a)q(a) = 0$. Thus, a is a zero of $f(x)$. □

Theorem 8. *A polynomial of degree n over a field has at most n zeros, counting multiplicity.*

Proof. We proceed by strong induction on n. Our base case is $n = 0$. Clearly, a polynomial of degree 0 over a field has no zeros. Let us assume that a polynomial of degree m has at most m zeros where $m < n$. Now suppose that $f(x)$ is a polynomial of degree n over a field and a is a zero of $f(x)$ of multiplicity k. Then, $f(x) = (x-a)^k q(x)$ and $q(a) \neq 0$; and, since $n = \deg(f(x)) = \deg((x-a)^k q(x)) = k + \deg(q(x))$, we have $k \leq n$. If $f(x)$ has no zero other than a, we are done. On the other hand, if $b \neq a$ and b is a zero of $f(x)$, then $0 = f(b) = (b-a)^k q(b)$, so that b is also a zero of $q(x)$. Since $\deg(q(x)) < \deg(f(x))$, then, by strong induction, we assumed that $q(x)$ has at most $\deg(q(x)) = n-k$ zeros, counting multiplicity. Thus, $f(x)$ has at most $k+(n-k) = n$ zeros. Thus, by strong induction, a polynomial of degree n has at most n zeros. □

Theorem 9 (Criterion for $I = \langle g(x) \rangle$)**.** *Let F be a field, I a nonzero ideal in $F[x]$,*

and $g(x)$ an element of $F[x]$. Then $I = \langle g(x) \rangle$ if $g(x)$ is a nonzero polynomial of minimum degree in I.

Proof. Let I be a nonzero ideal in $F[x]$. Let $g(x)$ be a nonzero element of minimum degree in I. Since $g(x) \in I$, we have $\langle g(x) \rangle \subseteq I$. Let $f(x) \in I$. Then, by the division algorithm, we may write $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Since $r(x) = f(x) - g(x)q(x) \in I$, the minimality of $\deg(g(x))$ implies that the latter condition cannot hold. Thus, $r(x) = 0$, so $f(x) = g(x)q(x)$. Thus, $f(x) \in \langle g(x) \rangle$. Therefore, $I \subseteq \langle g(x) \rangle$. Thus, $I = \langle g(x) \rangle$. □

Let F be a field. A nonconstant polynomial $f(x)$ from $F[x]$ is said to be *irreducible* over F if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $F[x]$, then $g(x)$ or $h(x)$ is a constant in $F[x]$. Thus, a nonconstant $f(x) \in F[x]$ is irreducible if $f(x)$ cannot be expressed as a product of two nonconstant polynomials. A nonconstant element in $F[x]$ that is not irreducible over F is called *reducible* over F.

Although there are many reducibility tests, we will only be concerned with one of them.

Theorem 10 (Reducibility Tests for Degrees 2 and 3)**.** *Let F be a field. If $f(x) \in F[x]$ and $degf(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Proof. Suppose that $f(x)$ is reducible over F. Then, $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ belong to $F[x]$ and have degrees less than that of $f(x)$. Since $\deg(f(x)) = \deg(g(x)) + \deg(h(x))$ and $\deg(f(x))$ is 2 or 3, at least one of $g(x)$ and $h(x)$ has degree 1. Say $g(x) = ax + b$. Then, $-a^{-1}b$ is a zero of $g(x)$ and therefore a zero of $f(x)$ as well.

Suppose that $f(a) = 0$, where $a \in F$. Then, by Theorem 7, we know that $(x - a)$ is a factor of $f(x)$ and, therefore, $f(x)$ is reducible over F. □

Combining our theory of principal ideals and polynomials, we will now construct fields in a different way.

Theorem 11. *Let F be a field and let $p(x) \in F[x]$. Then $F[x]/\langle p(x)\rangle$ is a field if and only if $p(x)$ is irreducible over F.*

Proof. Suppose that $F[x]/\langle p(x)\rangle$ is a field. Then, by Theorem 6, $\langle p(x)\rangle$ is a maximal ideal in $F[x]$. Then, $p(x)$ cannot be the zero polynomial because $\{0\}$ is never the maximal ideal. Furthermore, if $p(x)$ was a unit, then for all $f(x) \in F[x]$, $f(x) \in \langle p(x)\rangle$ because $f(x) = p(x)p(x)^{-1}f(x)$, so $\langle p(x)\rangle = F[x]$, which is not a maximal ideal in $F[x]$. Thus, $p(x)$ cannot be a unit, so $p(x)$ cannot be a constant. If $p(x) = g(x)h(x)$ is a factorization of $p(x)$ over F, then $\langle p(x)\rangle \subseteq \langle g(x)\rangle \subseteq F[x]$. Thus, $\langle p(x)\rangle = \langle g(x)\rangle$ or $F[x] = \langle g(x)\rangle$. In the first case, we must have, by Theorem 9, $\deg(p(x)) = \deg(g(x))$. In the second case, it also follows from Theorem 9 that $\deg(g(x)) = 0$ and, consequently, $\deg(h(x)) = \deg(p(x))$. Thus, $p(x)$ cannot be written as a product of two polynomials in $F[x]$ of lower degree. Thus, $p(x)$ is irreducible.

Suppose that $p(x)$ is irreducible over F. Let I be any ideal of $F[x]$ such that $\langle p(x)\rangle \subseteq I \subseteq F[x]$. By Theorem 9, we know that $I = \langle g(x)\rangle$ for some $g(x)$ in $F[x]$. So, $p(x) \in \langle g(x)\rangle$ and, therefore, $p(x) = g(x)h(x)$, where $h(x) \in F[x]$. Since $p(x)$ is irreducible over F, it follows that either $g(x)$ is a constant or $h(x)$ is a constant. In the first case, $g(x)$ is a unit, so $I = F[x]$; in the second case, we have $\deg(p(x)) = \deg(g(x))$, so, by Theorem 9, $\langle p(x)\rangle = \langle g(x)\rangle = I$. Thus, $\langle p(x)\rangle$ is maximal in $F[x]$. Therefore, by Theorem 6, $F[x]/\langle p(x)\rangle$ is a field. □

Theorem 12. *For any field in the form $F[x]/\langle p(x)\rangle$ where $\deg(p(x)) = n$, each element can be uniquely expressed as $\{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 + \langle p(x)\rangle : a_i \in F\}$.*

Proof. Since $\deg(p(x)) = n$, then $p(x) = b_nx^n + ... + b_0$ where $b_i \in F$. Thus, in $F[x]/\langle p(x)\rangle$, $b_nx^n + ... + b_0 + \langle p(x)\rangle \equiv 0 + \langle p(x)\rangle$, so $x^n + \langle p(x)\rangle \equiv -b_n^{-1}b^{n-1}x^{n-1} +$

$... - b_n^{-1}b_0 + \langle p(x)\rangle$. Let $c_j = -b_n^{-1}b_j$. Then $x^n + \langle p(x)\rangle \equiv c_{n-1}x^{n-1} + ... + c_0 + \langle p(x)\rangle$ where $c_i \in F$.

Let $g(x) + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$ where $\deg(g(x)) = k$ such that $k \geq n$. We will proceed by weak induction on k. Our base case is $k = n$. Let $g(x) = d_n x^n + ... + d_0$ where $d_i \in F$. Then $g(x) + \langle p(x)\rangle \equiv d_n x^n + ... + d_0 + \langle p(x)\rangle \equiv d_n(c_{n-1}x^{n-1} + ... + c_0) + ... + d_0 + \langle p(x)\rangle \equiv (d_n c_{n-1} + d_{n-1})x^{n-1} + ... + (d_n c_0 + d_0) + \langle p(x)\rangle$. Let $e_j = d_n c_j + d_j$. Thus, $g(x) + \langle p(x)\rangle \equiv e_{n-1}x^{n-1} + ... + e_0 + \langle p(x)\rangle$ where $e_i \in F$. Thus, the base case is satisfied.

Let us assume if $\deg(g(x)) \equiv k$, then $g(x) + \langle p(x)\rangle \equiv f_{n-1}x^{n-1} + ... + f_0 + \langle p(x)\rangle$ where $f_i \in F$. Let $\deg(g(x)) = k + 1$. Then, $g(x) = h_{k+1}x^{k+1} + ... + h_0$ where $h_i \in F$. Thus, $g(x) + \langle p(x)\rangle \equiv h_{k+1}x^{k+1} + ... + h_0 + \langle p(x)\rangle \equiv x(h_{k+1}x^k + ... + h_1) + h_0 + \langle p(x)\rangle$. By inductive assumption, $g(x) + \langle p(x)\rangle \equiv x(f_{n-1}x^{n-1} + ... + f_0) + h_0 + \langle p(x)\rangle \equiv f_{n-1}x^n + ... + f_0 x + h_0 + \langle p(x)\rangle$. By the base case, $g(x) + \langle p(x)\rangle \equiv e_{n-1}x^{n-1} + ... + e_0 + \langle p(x)\rangle$. Thus, by weak induction, each element in $F[x]/\langle p(x)\rangle$ can be expressed as $\{a_{n-1}x^{n-1} + ... + a_0 + \langle p(x)\rangle : a_i \in F\}$.

To show uniqueness, let $a_{n-1}x^{n-1} + ... + a_0 + \langle p(x)\rangle \equiv b_{n-1}x^{n-1} + ... + b_0 + \langle p(x)\rangle$. Then $(a_{n-1} - b_{n-1})x^{n-1} + ... + (a_0 - b_0) + \langle p(x)\rangle \equiv 0 + \langle p(x)\rangle$. Thus, $(a_{n-1} - b_{n-1})x^{n-1} + ... + (a_0 - b_0) \in \langle p(x)\rangle$, so $(a_{n-1} - b_{n-1})x^{n-1} + ... + (a_0 - b_0) = p(x)q(x)$ where $q(x) \in F[x]$. If $q(x) \neq 0$, then $\deg((a_{n-1} - b_{n-1})x^{n-1} + ... + (a_0 - b_0)) = \deg(p(x)) + \deg(q(x)) \geq n$. Since this is a contradiction, then $q(x) = 0$, so $(a_{n-1} - b_{n-1})x^{n-1} + ... + (a_0 - b_0) = 0$. Thus, $a_k = b_k$ for all $k = 0, 1, ..., n-1$. Thus, each element in $F[x]/\langle p(x)\rangle$ is uniquely expressed as

$$\{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 + \langle p(x)\rangle : a_i \in F\}.$$

□

We will use this method of constructing fields along with the use of $\mathbb{Z}_p$ to construct

finite fields. For any prime p, we can, by Theorem 3, construct a finite field, $\mathbb{Z}_p$. If we can find an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ with degree n, then, by Theorem 11, $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a finite field where each element can be uniquely expressed as $\{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 + \langle f(x)\rangle : a_i \in \mathbb{Z}_p\}$. Since there are p elements in $\mathbb{Z}_p$ and there are n places for our coefficients of $\mathbb{Z}_p$ to be placed, then there are p^n elements within our constructed field $\mathbb{Z}_p[x]/\langle f(x)\rangle$. A natural question is that, if we have a field $\mathbb{Z}_p$, can we always find an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ that has degree n? What is the relationship between two fields that have the same order of p^n? Are these the only type of finite fields? These are questions that we will answer. However, we first have to look at the theory of isomorphisms.

4 Ring Isomorphisms

A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

$$\phi(a+b) = \phi(a) + \phi(b); \quad \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*. An isomorphism is used to show that two rings are algebraically identical.

Theorem 13 (Property of Ring Homomorphisms)**.** *Let ϕ be a ring homomorphism from a ring R to a ring S. Then, ϕ is an isomorphism if and only if ϕ is onto and $Ker\phi = \{r \in R : \phi(r) = 0\} = \{0\}$ ($Ker\phi$ is the kernel of ϕ).*

Proof. Suppose ϕ is an isomorphism. Thus, ϕ is 1-1 and onto. Let $a, b \in R$ and let $\phi(a) = 0$. Thus, $\phi(a) + \phi(b) = \phi(b)$. Since ϕ preserves addition, $\phi(a + b) = \phi(b)$. Since ϕ is 1-1, then $a + b = b$, so $a = 0$. Thus, $\text{Ker}\phi = \{0\}$.

Suppose that $\text{Ker}\phi = \{0\}$ and ϕ is onto. Let $\phi(a) = \phi(b)$. Then $\phi(a) - \phi(b) = 0$.

Thus, $\phi(a-b)=0$. Since the Ker$\phi=\{0\}$, $a-b=0$, so $a=b$. Thus, ϕ is 1-1. Therefore, ϕ is an isomorphism. □

Theorem 14. *Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker$\phi=\{r\in R:\phi(r)=0\}$ is an ideal of R.*

Proof. Let $r\in R$ and $a\in$ Kerϕ. Then, $\phi(ar)=\phi(a)\phi(r)=0\cdot\phi(r)=0$. Thus, $ar\in$ Kerϕ. Furthermore, $\phi(ra)=\phi(r)\phi(a)=\phi(r)\cdot 0=0$. Thus, $ra\in$ Kerϕ. Therefore, Kerϕ is an ideal of R. □

Theorem 15 (First Isomorphism Theorem for Rings)**.** *Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/Ker\phi$ to $\phi(R)$, given by $r+Ker\phi\to\phi(r)$ is an isomorphism. In symbols, $R/Ker\phi\approx\phi(R)$.*

Proof. Let $\alpha: R/\text{Ker}\phi\to\phi(R)$ such that $\alpha(r+\text{Ker}\phi)=\phi(r)$. Let $r_1,r_2\in R$. Then,

$$\alpha(r_1+\text{Ker}\phi)+\alpha(r_2+\text{Ker}\phi)=\phi(r_1)+\phi(r_2)=\phi(r_1+r_2)=\alpha(r_1+r_2+\text{Ker}\phi)$$
$$\alpha(r_1+\text{Ker}\phi)\alpha(r_2+\text{Ker}\phi)=\phi(r_1)\phi(r_2)=\phi(r_1r_2)=\alpha(r_1r_2+\text{Ker}\phi)$$

Thus, α preserves addition and multiplication, so α is a homomorphism. For all $\phi(r)$, there exists $r\in R$ such that $\alpha(r+\text{Ker}\phi)=\phi(r)$. Thus, α is onto. Let $\alpha(r+\text{Ker}\phi)=0$. Then $\phi(r)=0$, so $r\in$ Kerϕ. Thus, $r+\text{Ker}\phi=0+\text{Ker}\phi$, so Ker$\alpha=\{0+\text{Ker}\phi\}$. By Theorem 13, α is an isomorphism. Therefore, $R/\text{Ker}\phi\approx\phi(R)$. □

Theorem 16 (Finite Fields Contain $\mathbb{Z}_p$)**.** *If F is a finite field of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$.*

Proof. Let F be a field. Since $1\in F$ and F has closure under addition, then we can let $S=\{k\cdot 1:k\in\mathbb{Z}\}\subseteq F$. It can be shown that the mapping $\phi:\mathbb{Z}\to S$ is an isomorphism, and by Theorem 15, $\mathbb{Z}/\text{Ker}\phi\approx\phi(\mathbb{Z})\approx S$. Furthermore, Ker$\phi=\langle n\rangle$,

where n is the additive order of 1, which is also, by Theorem 4, the characteristic of F. If the characteristic of F is p, then $S \approx \mathbb{Z}/\langle p\rangle \approx \mathbb{Z}_p$. □

Although not every finite field is in the form $\mathbb{Z}_p$, we have proven that every finite field contains $\mathbb{Z}_p$. This also helps us to characterize finite fields. Now that we have covered ring isomorphisms, we now have enough theory to develop field extensions.

5 Field Extensions

Since x^2+1 is an irreducible polynomial over $\mathbb{R}$, then $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field. Furthermore, notice that $x^2+1+\langle x^2+1\rangle = 0+\langle x^2+1\rangle$ because the ideal "absorbs" multiples of x^2+1. Thus, $x^2 \equiv -1 \mod (x^2+1)$. According to Theorem 12, each element in $\mathbb{R}/\langle x^2+1\rangle$ can be uniquely expressed as $\{ax+b+\langle x^2+1\rangle : a,b \in \mathbb{R}\}$. Furthermore, notice that every element in the field of complex numbers can be uniquely expressed as $\{ai+b : a,b \in \mathbb{R}\}$ and $i^2 \equiv -1$ in $\mathbb{C}$. If we define a mapping $\phi : \mathbb{R}[x]/\langle x^2+1\rangle \to \mathbb{C}$ such that $\phi(ax+b+\langle x^2+1\rangle) = ai+b$, then ϕ is an isomorphism. Thus, $\mathbb{R}[x]/\langle x^2+1\rangle \approx \mathbb{C}$. These two fields are algebraically identical.

A field E is an *extension field* of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F. If E is an extension field of F, then we may call F a *base field* of E. The field of complex numbers $\mathbb{C}$ contains the field of real numbers $\mathbb{R}$ and also contains a zero of x^2+1, which is i. Therefore, $\mathbb{R}[x]/\langle x^2+1\rangle$ is an extension field of $\mathbb{R}$ that contains a zero of x^2+1. This leads us to an amazing general result.

Theorem 17 (Fundamental Theorem of Field Theory)**.** *Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.*

Proof. Let $f(x)$ be a nonconstant polynomial in $F[x]$. Then, $f(x)$ has an irreducible factor, which we will call $p(x)$. We will construct an extension field E of F in which

$p(x)$ has a zero. Let $E = F[x]/\langle p(x)\rangle$. Since $p(x)$ is irreducible, then by Theorem 11, E is a field. Since the mapping $\phi : F \to E$ given by $\phi(a) = a + \langle p(x)\rangle$ is one-to-one and preserves both operations, E has a subfield isomorphic to F, so $F \subseteq E$. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. In E, $x + \langle p(x)\rangle$ is a zero of $p(x)$ because

$$\begin{aligned} p(x + \langle p(x)\rangle) &= a_n(x + \langle p(x)\rangle)^n + a_{n-1}(x + \langle p(x)\rangle)^{n-1} + \cdots + a_0 \\ &= a_n(x^n + \langle p(x)\rangle) + a_{n-1}(x^{n-1} + \langle p(x)\rangle) + \cdots + a_0 \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle \end{aligned}$$

Since $0 + \langle p(x)\rangle$ maps to 0 in F, $x + \langle p(x)\rangle$ is a zero for $f(x)$. □

Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ *splits* in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a *splitting field* for $f(x)$ over F if $f(x)$ splits in E but in no proper subfield of E. In other words, a splitting field of $f(x)$ over F is the smallest extension field of F that contains all of the zeros of $f(x)$.

The following notation is convenient. Let F be a field and let $a_1, a_2, ..., a_n$ be elements of some extension E of F. We use $F(a_1, a_2, ..., a_n)$ to denote the smallest subfield of E that contains F and the set $\{a_1, a_2, ..., a_n\}$. Notice that if $f(x) \in F[x]$ and $f(x)$ factors as $b(x - a_1)(x - a_2)\cdots(x - a_n)$ over some extension E of F where $b \in F$, then $F(a_1, a_2, ..., a_n)$ is a splitting field for $f(x)$ over F in E.

Theorem 18. *Let F be a field and let $f(x)$ be a nonconstant element of $F[x]$. Then there exists a splitting field E for $f(x)$ over F.*

Proof. We proceed by strong induction on the $\deg(f(x))$. If $\deg(f(x)) = 1$, then $f(x)$ is linear, so our base case is satisfied. Now suppose that the statement is true for all fields and all polynomials of degree less than that of $f(x)$. By Theorem 17, there is an

extension E of F in which $f(x)$ has a zero, which we will call a_1. By Theorem 7, we may write $f(x) = (x - a_1)g(x)$, where $g(x) \in E[x]$. Since $\deg(g(x)) < \deg(f(x))$, by inductive assumption, there is a field K that contains E and all of the zeros of $g(x)$, say $a_2, ..., a_n$. Thus, a splitting field for $f(x)$ over F is $F(a_1, a_2, ..., a_n)$. Therefore, by strong induction, there exists a splitting field for all nonconstant elements $f(x)$ over F. □

Although we have found a way to construct extension fields using factor rings, it would be convenient if we could construct them in a more convenient way that did not require using x as both a placeholder for polynomials and as a coset representative. The following theorem shows us that we can.

Theorem 19 ($F(a) \approx F[x]/\langle p(x)\rangle$)**.** *Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)$ is isomorphic to $F[x]/\langle p(x)\rangle$. Furthermore, if deg$(p(x)) = n$, then every member of $F(a)$ can be uniquely expressed in the form $c_{n-1}a^{n-1}+c_{n-2}a^{n-2}+\cdots+c_1a+c_0$ where $c_0, c_1, ..., c_{n-1} \in F$.*

Proof. Consider the function ϕ from $F[x]$ to $F(a)$ given by $\phi(f(x)) = f(a)$, so $\phi(F[x]) \subseteq F(a)$. It can be shown that ϕ is a ring homomorphism. Since a is a zero of $p(x)$ then $p(a) = 0$, so $\langle p(x)\rangle \subseteq \text{Ker}\phi$. Since $p(x)$ is irreducible, then by the proof of Theorem 11, $\langle p(x)\rangle$ is a maximal ideal in $F[x]$. Since Kerϕ does not contain the constant polynomial $f(x) = 1$, we know Ker$\phi \neq F[x]$. Thus, Ker$\phi = \langle p(x)\rangle$. Thus, by Theorem 15, since $F[x]/\text{Ker}\phi \approx \phi(F[x])$, then $F[x]/\langle p(x)\rangle \approx \phi(F[x])$ by the mapping $\alpha(f(x) + \langle p(x)\rangle) = \phi(f(x))$. Since $F[x]$ contains F and x, then $\phi(F[x])$ contains both F and a. Since $F(a)$ is the smallest field containing both F and a, then $F(a) \subseteq \phi(F[x])$, so $\phi(F[x]) = F(a)$. Therefore, $F[x]/\langle p(x)\rangle \approx F(a)$. The final part of the theorem follows from the fact that, by Theorem 12, every element in $F[x]/\langle p(x)\rangle$ can be expressed uniquely in the form $c_{n-1}x^{n-1}+\cdots+c_0+\langle p(x)\rangle$, where $c_0, ..., c_{n-1} \in F$.

By the way α carries elements from $F[x]/\langle p(x)\rangle$ to $F(a)$, it follows that every element in $F(a)$ can be uniquely expressed in the form $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_0$. $\square$

We will now lead up to showing that splitting fields are unique. This will help prove the uniqueness of finite fields.

Theorem 20 (Splitting Fields Are Unique (Part I))**.** *Let F be a field, let $p(x) \in F[x]$ be irreducible over F, and let a be a zero $p(x)$ in some extension of F. If ϕ is a field isomorphism from F to F' and b is a zero of $\bar{\phi}(p(x))$ in some extension of F', then there is an isomorphism from $F(a)$ to $F'(b)$ that agrees with ϕ on F and carries a to b (see Figure 1).*

Proof. Let $\bar{\phi} : F[x] \to F'[x]$ be a ring isomorphism that agrees with ϕ on F and $\bar{\phi}(x) = x$. Thus, $\bar{\phi}(p(x))$ is irreducible over F'. Thus, by Theorem 11, the mapping $\bar{\bar{\phi}} : F[x]/\langle p(x)\rangle \to F'[x]/\left\langle \bar{\phi}(p(x)\right\rangle$ that is defined by $\bar{\bar{\phi}}(f(x) + \langle p(x)\rangle) = \bar{\phi}(f(x)) + \left\langle \bar{\phi}(p(x)\right\rangle$ is a field isomorphism that agrees with ϕ on F. From the proof of Theorem 19, we know there is an isomorphism $\alpha : F(a) \to F[x]/\langle p(x)\rangle$ that is the identity on F and carries a to $x + \langle p(x)\rangle$. Also, $\bar{\bar{\phi}}$ carries $x + \langle p(x)\rangle$ to $\bar{\phi}(x) + \left\langle \bar{\phi}(p(x))\right\rangle = x + \left\langle \bar{\phi}(p(x))\right\rangle$. Similarly, there is an isomorphism $\beta : F'[x]/\left\langle \bar{\phi}(p(x))\right\rangle \to F'(b)$ that is the identity on F' and carries $x + \left\langle \bar{\phi}(p(x))\right\rangle$ to b. Thus, $\beta\bar{\bar{\phi}}\alpha : F(a) \to F'(b)$ is an isomorphism that agrees with ϕ on F and carries a to b. $\square$

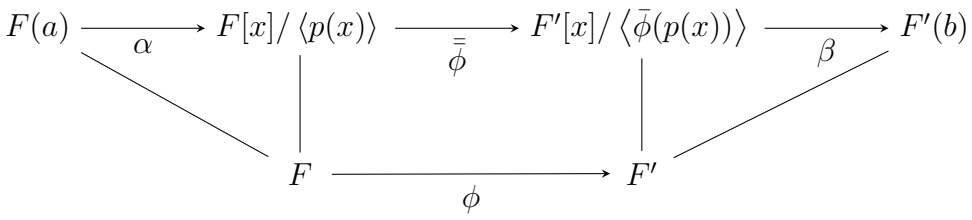

Figure 1: $\beta\bar{\bar{\phi}}\alpha$ carries a to b

Theorem 21 (Splitting Fields Are Unique (Part II))**.** *Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\bar{\phi}(f(x))$ over F', then there is an isomorphism from E to E' that agrees with ϕ on F (see Figure 2).*

Proof. We proceed by strong induction on $\deg(f(x))$. If $\deg(f(x)) = 1$, then $E = F$ and $E' = F'$, so that ϕ itself is the desired mapping. Thus, our base case is satisfied. Let us assume our hypothesis is true for polynomials with a degree less than that of $f(x)$. If $\deg(f(x)) > 1$, let $p(x)$ be an irreducible factor of $f(x)$, let a be a zero of $p(x)$ in E, and let b be a zero of $\bar{\phi}(p(x))$ in E'. By Theorem 20, there is an isomorphism $\alpha : F(a) \to F'(b)$ that agrees with ϕ on F and carries a to b. Now write $f(x) = (x - a)g(x)$, where $g(x) \in F(a)[x]$. Then, E is a splitting field for $g(x)$ over $F(a)$. Furthermore, let $\bar{\alpha} : F(a)[x] \to F'(b)[x]$ be a ring isomorphism that agrees with α on $F(a)$ and $\bar{\alpha}(x) = x$. Then, $\bar{\phi}(f(x)) = \bar{\alpha}(f(x)) = \bar{\alpha}((x - a)g(x)) = \bar{\alpha}(x - a)\bar{\alpha}(g(x)) = (\bar{\alpha}(x) - \bar{\alpha}(a))\bar{\alpha}(g(x)) = (x - b)\bar{\alpha}(g(x))$, where $\bar{\alpha}(g(x)) \in F'(b)[x]$. Thus, E' is a splitting field for $\bar{\alpha}(g(x))$ over $F'(b)$. Since $\deg(g(x)) < \deg(f(x))$ then, by our inductive assumption, there is an isomorphism $\beta : E \to E'$ that agrees with α on $F(a)$ and, therefore, with ϕ on F. □

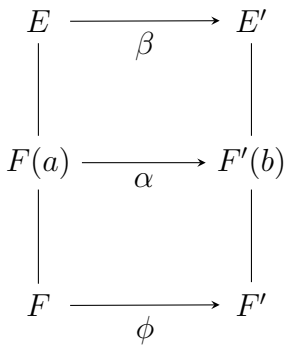

Figure 2: Function Extensions

Theorem 22 (Splitting Fields Are Unique (Part III)). *Let F be a field and let $f(x) \in F[x]$. Then any two splitting fields of $f(x)$ over F are isomorphic.*

Proof. Suppose that E and E' are splitting fields of $f(x)$ over F. Since $F \approx F$, then, by Theorem 21, $E \approx E'$. □

We will now look at a criterion for multiple zeros. This will help us determine the size of splitting fields, which will, in turn, help us to determine the size of finite fields.

Theorem 23 (Criterion for Multiple Zeros). *A polynomial $f(x)$ over a field F has a multiple zero in some extension E only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.*

Proof. If a is a multiple zero of $f(x)$ in some extension of E, then there is a $g(x) \in E[x]$ such that $f(x) = (x-a)^2 g(x)$. Since $f'(x) = (x-a)^2 g'(x) + 2(x-a)g(x)$, we see that $f'(a) = 0$. Thus, by Theorem 7, $(x-a)$ is a factor of both $f(x)$ and $f'(x)$ in the extension E of F. Now if $f(x)$ and $f'(x)$ have no common divisor of positive degree in $F[x]$, there are polynomials $h(x)$ and $k(x)$ in $F[x]$ such that $f(x)h(x) + f'(x)k(x) = 1$. Viewing $f(x)h(x) + f'(x)k(x)$ as an element of $E[x]$, we see that $(x-a)^2 g(x)h(x) + ((x-a)^2 g'(x) + 2(x-a)g(x))k(x) = 1$, so $(x-a)$ is a factor of 1. Since this is a contradiction, $f(x)$ and $f'(x)$ must have a common divisor of positive degree in $F[x]$. □

6 Classification of Finite Fields

Developing the theory behind splitting fields, characteristics of fields, polynomials, and isomorphisms is necessary to classify finite fields.

Theorem 24 (Classification of Finite Fields). *For each prime p and each positive integer n, there is, up to isomorphism, a unique finite field of order p^n.*

Proof. Let $f(x)$ be a polynomial over $\mathbb{Z}_p$ such that $f(x) = x^{p^n} - x$. By Theorem 18, there exists a splitting field E for $f(x)$ over $\mathbb{Z}_p$. Since $f(x)$ splits in E, we know, by Theorem 8, $f(x)$ has exactly p^n zeros in E, counting multiplicity. Since $f'(x) = p^n x^{p^n-1} - 1 = -1$, we see that $f(x)$ and $f'(x)$ have no common factors. Thus, by Theorem 23, $f(x)$ has no multiple zeros, so every zero of $f(x)$ has multiplicity 1. Thus, $f(x)$ has p^n distinct zeros in E. Let $a, b \in E$ such that $f(a) = f(b) = 0$. Then $f(a+b) = (a+b)^{p^n} - (a+b) = a^{p^n} + \binom{p^n}{1} a^{p^n-1}b + ... + \binom{p^n}{p^n-1} ab^{p^n-1} + b^{p^n} - (a+b)$. Since each $\binom{p^n}{i}$ is divisible by p^n and the characteristic of $\mathbb{Z}_p$, by Theorem 4, is p, then $f(a+b) = (a^{p^n} - a) + (b^{p^n} - b) = f(a) + f(b) = 0$. Furthermore, $f(a-b) = (a-b)^{p^n} - (a-b) = a^{p^n} + (-b)^{p^n} - a + b = (-b)^{p^n} + b$. If p is odd, then $f(a-b) = -b^{p^n} + b = -(b^{p^n} - b) = 0$. If $p = 2$, then the characteristic of $\mathbb{Z}_p$ is 2 and $f(a-b) = b^{p^n} + b$. If b is odd, then b^{p^n} is odd, so $b^{p^n} + b$ is even. If b is even, then b^{p^n} is even, so $b + b^{p^n}$ is even. Thus, $f(a-b) = 0$. If a or b is zero, but not both, then $f(ab) = 0$ and $f(\frac{a}{b}) = 0$ or $f(\frac{b}{a}) = 0$. We assume $a, b \neq 0$. Then, since $a^{p^n} - a = 0$, then, by Theorem 1, $a^{p^n-1} - 1 = 0$, so $a^{p^n-1} = 1$. Thus, $f(ab) = (ab)^{p^n} - (ab) = a(a^{p^n-1}b^{p^n} - b) = a(b^{p^n} - b) = a(0) = 0$. Furthermore, $f\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)^{p^n} - \left(\frac{a}{b}\right) = \frac{1}{b}(\frac{a^{p^n}}{b^{p^n-1}} - \frac{a}{1}) = \frac{1}{b}(a^{p^n} - a) = \frac{1}{b}(0) = 0$. Without loss of generality, $f(\frac{b}{a}) = 0$. Thus, the set of zeros of $f(x)$ in E is closed under addition, subtraction, multiplication, and division (by nonzero elements). Furthermore, since $f(1) = 0$ and the set of zeros has closure under addition, then the set of zeros of $f(x)$ contains $\mathbb{Z}_p$. Thus, the set of zeros of $f(x)$ is E and, therefore, $|E| = p^n$.

To show that there is a unique field for each prime-power, suppose that K is any field of order p^n. As a group under addition, the additive order of every element must divide the order of the group. Thus, 1 must have an additive order j that divides p^n. By Theorem 4, the characteristic of K is j. Since, by Theorem 5, the characteristic

of K is prime, j can only be p. Thus, by Theorem 16, K has a subfield isomorphic to $\mathbb{Z}_p$. Since the nonzero elements of K form a multiplicative group of order $p^n - 1$, every nonzero element of K has a multiplicative order that divides $p^n - 1$. Thus, if $a \in K$ and $a \neq 0$, then $f(a) = a^{p^n} - a = a(a^{p^n-1} - 1) = a(1 - 1) = 0$. Furthermore, if $a = 0$, then, $f(a) = 0 - 0 = 0$. Thus, every element of K is a zero of $f(x) = x^{p^n} - x$. So, K must be the splitting field for $f(x)$ over $\mathbb{Z}_p$. By Theorem 22, there is only one such field up to isomorphism. Thus, finite fields of order p^n are unique. □

This shows that for any finite field in the form of $\mathbb{Z}_p$ and for any positive integer n, we can always find an n^{th}-degree irreducible polynomial, $f(x)$, in $\mathbb{Z}_p$ so that we can construct the finite field $\mathbb{Z}_p[x]/\langle f(x)\rangle$ that has the order of p^n. Furthermore, since $x^2 + 2$ and $x^2 + 3$ are both irreducible polynomials over $\mathbb{Z}_5$, then $\mathbb{Z}_5[x]/\langle x^2 + 2\rangle \approx \mathbb{Z}_5[x]/\langle x^2 + 3\rangle$. Because there is only one field for each prime-power p^n, we may unambiguously denote it by $GF(p^n)$, in honor of Éveriste Galois, a founding father of abstract algebra, and call it the *Galois field of order* p^n.

7 The Fundamental Theorem of Finite Abelian Groups And Its Consequences

We see that for every prime p and every positive integer n, there is a unique finite field of order p^n. The natural question to ask is: are these the only types of finite fields? A finite field is an Abelian group under addition and the nonzero elements of a finite field form an Abelian group under multiplication. Thus, understanding more group theory will help us understand how finite fields are structured, which, in turn, will help us answer our question. Since a finite field is a finite Abelian group under addition, we can make use of the Fundamental Theorem of Finite Abelian Groups.

Theorem 25. *Every finite Abelian group is a direct product of cyclic groups of prime-*

power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

(This is the only theorem in this paper that will not be proven. Due to the length of the proof, it is not included. The theorem is proven in Joseph Gallian's *Contemporary Abstract Algebra* textbook in Chapter 11.)

Since a cyclic group of order n is isomorphic to $\mathbb{Z}_n$, Theorem 25 shows that every finite Abelian group G, where $|G| = p_1^{n_1}p_2^{n_2}...p_k^{n_k}$ where each p_i is distinct, is isomorphic to a group of the form $\mathbb{Z}_{p_1^{r_{11}}} \oplus ... \oplus \mathbb{Z}_{p_1^{r_{1t_1}}} \oplus ... \oplus \mathbb{Z}_{p_k^{r_{k1}}} \oplus ... \oplus \mathbb{Z}_{p_k^{r_{kt_k}}}$ where each n_i has the partition $n_i = r_{i1} + ... + r_{it_i}$ where each $r_{ij} > 0$ and $1 \leq i \leq k$, $1 \leq j \leq t_i$.

Let us look at groups whose orders have the form p^n, where p is prime and $n \leq 3$. In general, there is one group of order p^n for each set of positive integers whose sum is n (such a set is called a *partition of* n); that is, if n can be written as $n = r_1 + r_2 + \cdots + r_t$ where each r_i is a positive integer, then $\mathbb{Z}_{p^{r_1}} \oplus \mathbb{Z}_{p^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_t}}$ is an Abelian group of order p^n.

Order of G	Partitions of n	Possible direct products for G
p	1	$\mathbb{Z}_p$
p^2	2	$\mathbb{Z}_{p^2}$
p^2	$1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	$\mathbb{Z}_{p^3}$
p^3	$2+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
p^3	$1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

Table 1: Groups of Order p^n

From Table 1, we can see all of the different isomorphism classes of groups of order p^n where $n \leq 3$. The uniqueness portion of Theorem 25 guarantees that distinct partitions of n yield distinct isomorphism classes. Thus, $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_3 \oplus Z_3 \oplus Z_3$.

The following are some important consequences of Theorem 25.

Theorem 26 (Existence of Subgroups of Abelian Groups)**.** *If m divides the order of a finite Abelian group, then G has a subgroup of order m.*

Proof. Let $|G| = n$. If $n = 1$, then the only subgroup G could have is itself. Let $n > 1$. Then, by the Fundamental Theorem of Arithmetic, $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ where each p_i is a distinct prime and each n_i is a positive integer. Thus, by Theorem 25, $G \approx \mathbb{Z}_{p_1^{r_{11}}} \oplus ... \oplus \mathbb{Z}_{p_1^{r_{1t_1}}} \oplus ... \oplus \mathbb{Z}_{p_k^{r_{k1}}} \oplus ... \oplus \mathbb{Z}_{p_k^{r_{kt_k}}}$ where each n_i has a partition $n_i = r_{i1} + ... + r_{it_i}$ where each $r_{ij} > 0$ and $1 \leq i \leq k$, $1 \leq j \leq t_i$. Since each component of the external direct product, $\mathbb{Z}_{p_i^{r_{ij}}}$ is cyclic, then, by the Fundamental Theorem of Cyclic Groups, $\mathbb{Z}_{p_i^{r_{ij}}}$ contains subgroups of order $p_i^{s_{ij}}$, for each s_{ij} where $0 \leq s_{ij} \leq r_{ij}$. Thus, the order of all of the subgroups of G are $p_1^{s_{11}+...+s_{1t_1}} p_2^{s_{21}+...+s_{2t_2}} ... p_k^{s_{k1}+...+s_{kt_k}}$ where $0 \leq s_{i1} + s_{i2} + ... + s_{it_i} \leq r_{i1} + r_{i2} + ... + r_{it_i} = n_i$. If m divides the order of G, then $m = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$ where, for each i, $0 \leq m_i \leq n_i$. Thus, G has a subgroup of order m. □

Theorem 27 (Finite Fields Have Prime-Powered Order)**.** *Any finite field has order p^n, where p is a prime.*

Proof. Let F be a finite field. Suppose $|F| = p^n q^m r$ where p and q are distinct primes and $n, m \geq 1$. As a finite Abelian group under addition, by Theorem 26, there exists a subgroup G such that $|G| = p$ and a subgroup H such that $|H| = q$. Since $p, q > 1$, then there exists a nonzero element $a \in G$ and a nonzero element $b \in H$. Since $|a|$ divides p and $|b|$ divides q, then $|a| = p$ and $|b| = q$. Thus, $ap = 0$ and $bq = 0$. Since p and q are relatively prime, then there exist integers, s, t such that $sp + tq = 1$. Therefore, $ab(sp + tq) = ab$, so $bs(ap) + at(bq) = 0 + 0 = 0 = ab$. Thus, $a = 0$ or $b = 0$, which contradicts the fact that a and b are nonzero. Thus, any finite field has a prime-powered order. □

We have shown that the only type of finite fields that exist are ones that have a prime-powered order. If a finite field has order p^n, we know that it is a field extension

of the finite field $\mathbb{Z}_p$. What type of extension? Answering this question will help us to further understand the structure of finite fields.

8 Structure of Finite Fields

If E is an extension field of F, we may view E as a vector space over F (that is, the elements of E are the vectors and the elements of F are the scalars). We are then able to use such notions as dimension and basis in our discussion. In fact, we say that E has *degree n over F* and write $[E : F] = n$ if E has dimension n as a vector space over F. If $[E : F]$ is finite, E is called a *finite extension* of F; otherwise, we say that E is an *infinite extension* of F. Figure 3 gives visual representations of finite extensions.

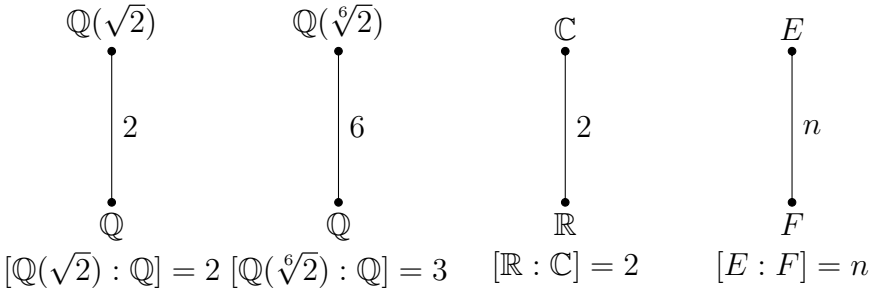

Figure 3: Finite Extensions

If a is the zero of some irreducible polynomial $p(x) \in F[x]$ and $\deg(p(x)) = n$, then, by Theorem 19, we know that $\{1, a, ..., a^{n-1}\}$ is a basis for $F(a)$ over F. In this case, we say that a has degree n over F.

Theorem 28. *Let K be a finite extension field of the field E and let E be a finite extension field of the field F. Then K is a finite extension field of F and $[K : F] = [K : E][E : F]$.*

Proof. Let $X = \{x_1, x_2, ..., x_n\}$ be a basis for K over E, and let $Y = \{y_1, y_2, ..., y_m\}$

be a basis for E over F. It suffices to prove that

$$YX = \{y_j x_i : 1 \leq j \leq m, 1 \leq i \leq n\}$$

is a basis for K over F. To do this, let $a \in K$. Then, since X spans K over E, there are elements $b_1, b_2, ..., b_n \in E$ such that

$$a = b_1 x_1 + b_2 x_2 + \cdots + b_n x_n.$$

And, for each $i = 1, ..., n$, since Y spans E over F, there are elements $c_{i1}, c_{i2}, ..., c_{im} \in F$ such that

$$b_i = c_{i1} y_1 + c_{i2} y_2 + \cdots + c_{im} y_m.$$

Thus,

$$a = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} c_{ij} y_j \right) x_i = \sum_{i,j} c_{ij} (y_j x_i).$$

This proves that YX spans K over F. Now suppose there are elements c_{ij} in F such that

$$0 = \sum_{i,j} c_{ij} (y_j x_i) = \sum_{i} \left(\sum_{j} (c_{ij} y_j) \right) x_i.$$

Then, since each $\sum c_{ij} y_j \in E$ and X is a basis for K over E, we have

$$\sum_{j} c_{ij} y_j = 0$$

for each i. But each $c_{ij} \in F$ and Y is a basis for E over F, so each $c_{ij} = 0$. This proves that the set YX is linearly independent over F. Thus, YX is a basis for K over F where $|YX| = NM$. Thus, $[K : F] = [K : E][E : F]$. □

Now, we can describe the structure of finite fields.

Theorem 29 (Structure of Finite Fields)**.** $[GF(p^n) : GF(p)] = n$.

Proof. As a group under addition, we know, from the proof of Theorem 24, that $GF(p^n)$ has characteristic p. Thus, every element in $GF(p^n)$ has an additive order of, at most p. As a finite Abelian group under addition and by Theorem 25, $GF(p^n) \approx \mathbb{Z}_{p^{r_1}} \oplus \mathbb{Z}_{p^{r_2}} \oplus ... \oplus \mathbb{Z}_{p^{r_t}}$ where the partition of n is $n = r_1 + r_2 + ... + r_t$ where each $r_j > 0$ and $1 \leq j \leq t$. If there exists $r_j \geq 2$, then, by the Fundamental Theorem of Cyclic Groups, there exists an element $a \in GF(p^n)$ such that $|a| = p^2$ which is a contradiction. Thus, each $r_j = 1$, so $GF(p^n) \approx \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus ... \oplus \mathbb{Z}_p}_{\text{n factors}}$. Let $\phi : \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus ... \oplus \mathbb{Z}_p \to a_1v_1 + a_2v_2 + ... + a_nv_n$ where each $a_i \in \mathbb{Z}_p \approx GF(p)$, each $v_i \in GF(p^n)$, and $\phi((c_1, c_2, ..., c_n)) = c_1v_1 + c_2v_2 + ... + c_nv_n$. Then, ϕ is an isomorphism. Thus, $GF(p^n)$ is a vector space over $G(p)$ where $[GF(p^n) : GF(p)] = n$. □

Thus, finite fields of order p^n are degree n field extensions over $\mathbb{Z}_p$. In other words, if $f(x)$ is an irreducible polynomial over $\mathbb{Z}_p$, where the degree of $f(x)$ is n, then the finite field $\mathbb{Z}_p[x]/\langle f(x)\rangle$ has degree n over $\mathbb{Z}_p$. In general, using Theorems 28 and 29, if $f(x)$ and $g(x)$ are irreducible polynomials over $\mathbb{Z}_p$ where $\deg(f(x)) = mn$ and $\deg(g(x)) = n$, then $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a degree m field extension over $\mathbb{Z}_p[x]/\langle g(x)\rangle$ (see Figure 4).

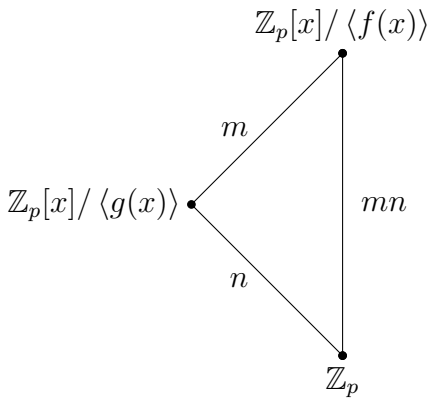

Figure 4: Field Extensions of Finite Fields

9 Exploring Quadratic Residues Using Cayley Tables

As discussed before, a quadratic residue, α, of a field, F, is an element $\alpha \in F$ such that there exists $a \in F$ such that $a^2 = \alpha$. We know that there exists quadratic residues in infinite fields. Are there any quadratic residues in finite fields? Yes, there are. We know that for all fields, 0 and 1, the additive identity and the multiplicative identity, respectively, are in every field. Furthermore, $0^2 = 0$ and $1^2 = 1$. Thus, 0 and 1 are quadratic residues of every finite field. Are there more quadratic residues in finite fields? How can we tell?

One way we can find out is by using a Cayley Table. A *Cayley Table* describes the structure of a finite field by arranging all the possible products of all the field's elements in a table. We can discover what are the quadratic residues of a finite field by looking at the numbers in the cells of the main diagonal of the table. Let us look at Cayley Tables of $\mathbb{Z}_5$ and $\mathbb{Z}_7$, which we know, by Theorem 3, are finite fields.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 2: Z_5

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 3: $\mathbb{Z}_7$

For Tables 2 and 3, the quadratic residues of the fields are the numbers that are in the shaded cells because each of them is expressed as a product of two equivalent elements in the field $\mathbb{Z}_p$. Each of these numbers in the tables are in $\mathbb{Z}_p$ because $\mathbb{Z}_p$ has closure under multiplication. If we look at the nonzero quadratic residues, a^2 of $\mathbb{Z}_5$ in an increasing order of a, we see that the list $\{1, 4, 2, 2, 4, 1\}$ is symmetric. We can see that this is also true for $\mathbb{Z}_7$. In fact, this is true for all $\mathbb{Z}_p$ where p is an odd prime. In the case of where $p = 2$, the quadratic residues of $\mathbb{Z}_p$ are $\{0, 1\}$, so there are two quadratic residues in $\mathbb{Z}_2$, so there is no symmetric pattern. (For the remainder of the paper, we will assume p is an odd prime, so $p \neq 2$.)

In the case where p is an odd prime, we can show that the nonzero quadratic residues are listed in a symmetric way. In other words, for all $a \in \mathbb{Z}_p$, $a^2 \equiv (p - a)^2$ (mod p). This is because the characteristic of $\mathbb{Z}_p$ is p. Thus,

$$(p - a)^2 \equiv p^2 + a^2 - 2pa \equiv a^2 \text{ mod p}$$

Thus, there is, at most, $\frac{p-1}{2}$ nonzero distinct quadratic residues in $\mathbb{Z}_p$. Since the nonzero quadratic residues are listed in a symmetric way, then the only distinct nonzero quadratic residues in $\mathbb{Z}_p$ we could have are $Q^*_{\mathbb{Z}_p} = \{a^2 : 0 < a \leq \frac{p-1}{2}\}$. This leads us to an interesting general result.

Theorem 30 (Number of Quadratic Residues in $\mathbb{Z}_p$)**.** *For all finite fields of the form $\mathbb{Z}_p$, where $p \neq 2$, the number of quadratic residues in $\mathbb{Z}_p$ is $1 + \frac{p-1}{2}$.*

Proof. We know, in every field, 0 is always a quadratic residue because 0 is the additive identity of every field and $0^2 = 0$. Furthermore, if $a^2 = 0$, we know that $a = 0$ because $\mathbb{Z}_p$ is an integral domain by Theorem 2. Thus, the only nonzero quadratic residues of $\mathbb{Z}_p$ are $\{a^2 : 0 < a \leq \frac{p-1}{2}\}$. Let a^2 (mod p)$\equiv b^2$ (mod p) such that $0 < a, b \leq \frac{p-1}{2}$. Then, $a \equiv b$ (mod p) or $a \equiv -b$ (mod p). Let us assume that $a \equiv -b$ (mod p). Then, by the rules of modular arithmetic, $a + b = np$ where $n \in \mathbb{Z}$. Since $0 < a, b \leq \frac{p-1}{2}$,

then $0 < a + b \leq p - 1$. Thus, n has to be positive. However, if $n \geq 1$, then $a + b \geq p$ which is a contradiction. Thus, $a \equiv b$ (mod p). Therefore, by contrapositive, for every distinct nonzero, $a < \frac{p-1}{2}$, there is a distinct nonzero quadratic residue, α such that $\alpha = a^2$. Thus, there are $\frac{p-1}{2}$ nonzero quadratic residues in $\mathbb{Z}_p$, so there are $1 + \frac{p-1}{2}$ quadratic residues in $\mathbb{Z}_p$. □

Theorem 30 shows us that not every element in $\mathbb{Z}_p$ is a quadratic residue. Thus, the set of quadratic residues of $\mathbb{Z}_p$, which we will call $Q_{\mathbb{Z}_p}$, does not equal $\mathbb{Z}_p$. However, if we look at degree 2 extensions of finite fields, we can observe an interesting result.

Let us look at the Cayley Table of $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$. Since $x^2 + 1$ is irreducible over $\mathbb{Z}_3$, which we can check by using Theorem 10, then $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ is a degree 2 extension of $\mathbb{Z}_3$. (Note: Each element in the Cayley Table is the coset representative of the element. Since each element in $\mathbb{Z}_3[x]\langle x^2 + 1\rangle$ is only distinguished by the coset representative, we have decided, for simplicity, to only include the coset representative in each cell.)

	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Table 4: $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$

Looking at Table 4, we can see, as expected from Theorem 30, that $2 \notin Q_{\mathbb{Z}_3}$. However, $2 \in Q_{\mathbb{Z}_3[x]/\langle x^2+1\rangle}$. In fact, $\mathbb{Z}_3 \subseteq Q_{\mathbb{Z}_3[x]/\langle x^2+1\rangle}$. This leads us to an amazing general result.

Theorem 31 ($GF(p^n) \subseteq Q_{GF(p^{2n})}$)**.** *The set of quadratic residues of the degree* 2 *extension field of any finite field contains the base field.*

Proof. Let $\alpha \in GF(p^n)$ for some finite field $GF(p^n)$. Let $f(x) \in GF(p^n)[x]$ such that $f(x) = x^2 - \alpha$. If $f(x)$ is irreducible over $GF(p^n)$, then, by Theorem 11, $GF(p^n)[x]/\langle f(x)\rangle$ is a field. By the proof of Theorem 17, we know that $GF(p^n)[x]/\langle f(x)\rangle$ has a zero for $f(x)$ and $GF(p^n) \subseteq GF(p^n)[x]/\langle f(x)\rangle$. Thus, there exists an $a \in GF(p^n)[x]/\langle f(x)\rangle$ such that $f(a) = a^2 - \alpha = 0$, so $a^2 = \alpha$. Thus, $\alpha \in Q_{GF(p^n)[x]/\langle f(x)\rangle}$. Furthermore, since $GF(p^n)[x]/\langle f(x)\rangle$ has p^{2n} elements, then, by Theorem 24, $GF(p^n)[x]/\langle f(x)\rangle \approx GF(p^{2n})$, so $\alpha \in Q_{GF(p^{2n})}$. In general, by Theorem 29, $[GF(p^{mn}) : GF(p)] = mn$ and $[GF(p^n) : GF(p)] = n$. By Theorem 28, $[GF(p^{mn}) : GF(p)] = [GF(p^{mn}) : GF(p^n)][GF(p^n) : GF(p)] = [GF(p^{mn}) : GF(p^n)]n = mn$. Thus, $[GF(p^{mn}) : GF(p^n)] = m$, so $GF(p^{2n})$ is the degree 2 extension field of $GF(p^n)$. If $f(x)$ is reducible over $GF(p^n)$, then, by Theorem 10, there exists an $a \in GF(p^n)$ such that $f(a) = a^2 - \alpha = 0$, so $a^2 = \alpha$. Thus, $\alpha \in Q_{GF(p^n)} \subseteq Q_{GF(p^{2n})}$. Therefore, $GF(p^n) \subseteq Q_{GF(p^{2n})}$. □

For infinite fields, we do not get the same result.

Theorem 32. *It is not the case that the set of quadratic residues of any degree 2 extension field of any infinite field contains the base field.*

Proof. We will prove the negation by finding a counterexample.

We know that $\sqrt{2}$ is a zero of x^2-2 which is an irreducible polynomial over $\mathbb{Q}$. Furthermore, we know that $\sqrt{3}$ is a zero of x^2-3 which is an irreducible polynomial over $\mathbb{Q}$. Thus, by Theorem 19, $\mathbb{Q}(\sqrt{2}) \approx \mathbb{Q}[x]/\langle x^2-2\rangle$ and $\mathbb{Q}(\sqrt{3}) \approx \mathbb{Q}[x]/\langle x^2-3\rangle$. Moreover, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are degree 2 extension fields over $\mathbb{Q}$. We assume $\mathbb{Q}(\sqrt{2}) \approx \mathbb{Q}(\sqrt{3})$. Then, $\mathbb{Q}[x]/\langle x^2-2\rangle \approx \mathbb{Q}[x]/\langle x^2-3\rangle$. Thus, $\phi : \mathbb{Q}[x]/\langle x^2-2\rangle \to \mathbb{Q}[x]/\langle x^2-3\rangle$ such that $\phi(f(x)+\langle x^2-2\rangle) = f(x)+\langle x^2-3\rangle$ is an isomorphism. Since $x^2-2+\langle x^2-2\rangle$ is a zero of $\mathbb{Q}[x]/\langle x^2-2\rangle$, then, by Theorem 13, $x^2-2+\langle x^2-3\rangle$ is a zero of $\mathbb{Q}[x]/\langle x^2-3\rangle$, so $x^2+\langle x^2-3\rangle \equiv 2+\langle x^2-3\rangle$. Furthermore, $x^2-3+\langle x^2-3\rangle$ is also a zero of $\mathbb{Q}[x]\langle x^2-3\rangle$, so $x^2+\langle x^2-3\rangle \equiv 3+\langle x^2-3\rangle$. Since $2 \neq 3$, then this

is a contradiction, so $\mathbb{Q}(\sqrt{2}) \not\approx \mathbb{Q}(\sqrt{3})$.

Now, let us suppose $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then, $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})$. Also, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$. Thus, by Theorem 28, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 1 \cdot 2 = 2$. Therefore, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$. Thus, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 1 over $\mathbb{Q}(\sqrt{3})$, so $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. This implies that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{3})$, so $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$ which is a contradiction. Thus, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so $3 \notin Q_{\mathbb{Q}(\sqrt{2})}$. This shows that $\mathbb{Q} \not\subseteq Q_{\mathbb{Q}(\sqrt{2})}$. □

These results show us that finite fields have a certain algebraic structure that the infinite fields do not have.

10 Conclusion

We have shown that finite fields exist. From the Fundamental Theorem of Finite Abelian Groups, these finite fields can only be prime-powered. Furthermore, for each prime p and each positive integer n, there is a unique finite field of order p^n which we call the Galois field of order p^n. Understanding the structure of finite fields helps us to know the structure of quadratic residues in finite fields. Only until we knew the structure of finite fields could we discover that the number of quadratic residues in $\mathbb{Z}_p$ or the quadratic residues in the degree 2 extension field of a finite field include all of the elements from the base field. Theory builds on theory. However, before we ever develop theory, there is usually a motivation for proving such theory. That motivation is derived from observation of patterns. According to David Niven, "What is the common denominator of intellectual accomplishment in math, science, economics, history, or any other subject, the answer is the same: great thinkers notice patterns" [1, p.273].

One question we may ask: why do we study finite fields and quadratic residues? Finite fields have been applied in computer science, coding theory, information the-

ory, and cryptography. Quadratic residues have also been applied to cryptography. Another question we may ask: does it matter if theory is turned into application? Studying the theory behind mathematical structures is fun and rewarding. It is important to be able to step back from all of this complicated mathematics and say, "This is simply beautiful." Otherwise, what is the point?

References

[1] Joseph Gallian, *Contemporary Abstract Algebra*, seventh edition, Cengage Learning (2009).