# Finite Fields

Albert Ye

June 8, 2020

In this paper, we discuss properties of finite fields such as the criteria for subfields of finite fields and finite extension fields.

## §1 Definitions and Properties

We refer to the operations $+$ and $\cdot$ as addition and multiplication, respectively, and $+$ and $\cdot$ are implied to be binary operations over the sets named in the definitions below. We use the regular definitions for groups and fields.

A **finite field** is a field with a finite order. We first explore some initial properties of the finite field.

**Definition 1.1.** The **characteristic** of a field $F$ is the smallest number $m$ such that adding 1 $m$ times gives the additive identity. If $m$ doesn't exist (i.e. the field is infinite), then we say $F$ has characteristic 0.

**Proposition 1.2**

The characteristic of a finite field is a prime $p$, and furthermore there does not exist any other primes $q$ such that $\underbrace{1+1+\ldots+1}_{q \text{ ones}} = 0$.

*Proof.* Suppose that $p$ can be expressed as $ab$ with $a, b \in F$. Then $0 = p = ab$, but since the multiplicative group $F \setminus \{0\}$ is closed, $ab$ must be in this group and thus cannot be 0, contradiction, so $p$ is prime. By definition $q$ must be greater than $p$, but this contradicts our assumption that $p = q = 0$. □

**Proposition 1.3**

If $F$ is a finite field with $q$ elements, then $a^q = a$ for all $a \in F$.

*Proof.* This is clearly true for $a = 0$. By definition of a group, all of the nonzero elements of $F$ form an abelian group (which we denote as $F^\times$ and call the **multiplicative group** of $F$) of order $q - 1$. All groups satisfy the property that $a^{|G|} = e_G$. As $|G| = q - 1$, it follows that $a^{q-1} = e_G$ for all $a \in F^\times$. Therefore, $a^q = a$ for all $a \in F^\times$. As we know that this is also true for $a = 0$, we are done. □

## §2 Classification of general finite fields

We introduce a few claims that will help us prove the final theorem.

**Proposition 2.1** (Freshman's dream)

If a finite field $\mathbb{F}$ has a characteristic of $p$, then taking the $p$th power is linear. That is, for any positive integer $n$,

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

over $\mathbb{F}$.

*Proof.* Note that from distributivity in fields, the Binomial Theorem must hold.

We use induction. When we expand $(x+y)^p$, we have by the Binomial Theorem that

$$(x+y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p.$$

Note that $\binom{p}{i}$ will not have have $p$ in the denominator $\forall i \in [0,p]$ since $p$ is prime, so these terms are all divisible by $p$ except $\binom{p}{0}$ and $\binom{p}{p}$ because the rest all have $p$ in the numerator. Hence, all that remains in the expansion is $x^p + y^p$. We can then take the $n$th power to get the desired result. □

**Theorem 2.2** (Order of Finite Fields)

The order of a finite field $\mathbb{F}$ is $p^n$ for some prime $p$ and positive integer $n$.

*Proof.* Suppose that two primes $p$ and $q$ divide the order of $\mathbb{F}$. By Cauchy's Theorem, there must exist elements of order $p, q$ in the additive group $\mathbb{F}$, but this would require that $p = q = 0$, contradiction. □

**Note 2.3.** Let $\mathbb{F}_x$ denote a field with size $x$. Note that $x$ must be a prime power. By the end of the section, we will realize that $\mathbb{F}_x$ is unique – that it is *the* field with size $x$, up to isomorphism.

**Example 2.4**

$\mathbb{Z}/n\mathbb{Z}$ is a finite field if and only if all elements of $\mathbb{Z}/n\mathbb{Z}$ have a multiplicative inverse – in other words, $n$ must be prime.

**Lemma 2.5** (Factorization)

Let $F$ be a finite field and $K$ a subfield of $F$. Then, the polynomial $f(x) = x^q - x$ in $K[x]$ factors in $F[x]$ as

$$f(x) = \prod_{a \in F}(x-a),$$

and $F$ is a splitting field of $f(x)$ over $K$.

*Proof.* Since $f(x)$ is a degree-$q$ polynomial, it must have at most $q$ roots in $F$. From Proposition 1.3, we have that all elements of $F$ are roots of the polynomial as $x^q = x$ for all $x \in F$. Therefore, there must be $q$ roots.

It follows that $f(x)$ splits in $F$, and cannot split in any subfield of $F$, by definition of splitting field. □

**Lemma 2.6** (Multiple Roots)

An element $\alpha \in F$ is a multiple root of $f \in F[x]$ if and only if it is a root of both $f$ and its derivative $f'$.

*Proof.* We let $f(x) = (x - \alpha)g(x)$, where $\alpha$ is an arbitrary root. We just take the derivative: $f'(x) = (x - \alpha)g'(x) + g(x)$.

If $\alpha$ is a root of $f'(x)$, $x - \alpha$ must divide $(x - \alpha)g'(x) + g(x)$. As the first term of $(x-\alpha)g'(x)$ has an $x-\alpha$ term, this implies that $\alpha$ must also be a root of $g(x)$, and hence a double root of $f(x)$.

Conversely, if $\alpha$ is a double root of $f(x)$, $x - \alpha$ must divide $g(x)$. Therefore, $x - \alpha$ must divide $(x - \alpha)g'(x) + g(x)$, so $x - \alpha | f'(x)$, which completes the proof. □

**Theorem 2.7** (Existence and Uniqueness)

For every prime $p$ and positive integer $n$, there exists a finite field with $p^n$ elements. Any finite field of the same order is isomorphic.

*Proof.* We prove each claim separately.

- Let $q = p^n$, and let $F$ be the splitting field of $f(x) = x^q - x$ over $\mathbb{F}_p[x]$. Since the derivative of $f$ is $qx^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$, we know from Lemma 2.5 that $f(x)$ must not have any multiple roots.

  Let's make a set $S = \{a \in F | a^q - a = 0\}$. Note that $S$ must be a subfield of $F$, as $S$ contains 0, Freshman's Dream on $F$ leads to $(a - b)^q = a^q - b^q = a - b$, and for $a, b \in S$ we have $(ab^{-1})^q = a^q b^{-q} = ab^{-1} \in S$. Also, $x^q - x$ must split in $S$ because $S$ contains all of its roots, so $F$ must be a subfield of $S$. Hence, $F = S$, and since $S$ has $q$ elements, $F$ must be the finite field with $q$ elements.

- We know that because $F$ has order $p^n$ that $F$ has characteristic $p$, and therefore $\mathbb{F}_p$ must be a subfield of $F$. (We already know $\mathbb{F}_p$ is a field.) From Lemma 2.4, we know that $x^q - x$ must factor into $\Pi_{a \in \mathbb{F}_p}(x - a)$. This implies that $F$ must be a splitting field of $\mathbb{F}_p$. As all splitting fields of any generic field $G$ must be unique up to isomorphism, all $F \cong \mathbb{F}_p$.

□

We know from uniqueness that all finite fields with the same order are isomorphic. Therefore, we can refer to $\mathbb{F}_p$ as *the* field with cardinality of $p$.

**Example 2.8**

We know know that $\mathbb{F}_3$ is *the* unique field of cardinality 3.

We construct a field $K = \mathbb{F}_3(\eta)$, where $\eta$ is a root of $f(x) = x^2 + 2x + 5$ in $F_3[x]$. $K$ must be *the* finite field with 9 elements, or $\mathbb{F}_9$.

# §3 Subfield Criteria

In this section, we find criteria for the sub

We first introduce a lemma that gives a basic criterion for subfields.

**Lemma 3.1**

Let $F$ be a finite field containing a subfield $K$ with order $q$. Then $F$ has $q^m$ elements, where $m = [F : K]$.

*Proof.* By definition of degree, we can set $F$ as a vector space over $K$. Obviously, the dimension of $F$ must be finite. Therefore, every basis of $F$ over $K$ must have exactly $m = [F : K]$ elements.

By definition of vector space, every element of $F$ can be expressed as $k_1b_1 + \cdots + k_mb_m$ for $k_i \in K$ for all $i \in \{1, 2, \ldots, m\}$.

Each of the $k_i$ can take exactly $q$ values, so as there are $m$ such $k_i$ there exist $q^m$ elements in $F$. □

We use Lemma 3.1 to find a stronger criterion for finding subfields.

**Theorem 3.2** (Subfield Criterion)

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order $p^m$, where $m$ is a positive divisor of $n$. Conversely, if $m|n$, then there is exactly one subfield of $\mathbb{F}_q$ with $p^m$ elements.

Before we begin, we first prove the following lemma.

**Lemma 3.3**

If $m|n$, then $p^m - 1|p^n - 1$.

*Proof.* Let $n = qm$. This implies that $p^n - 1 = p^{qm} - 1$, which in turn is equal to $(p^m)^q - 1 = (p^m)^q - (1)^q$. The expression is well-known to factor into $(p^m - 1)((p^m)^{q-1} + (p^m)^{q-2} + \cdots + p^m + 1)$. □

*Proof.* We know that the cardinality of a finite field must be a prime power, and from Lemma 3.1, we have that if $G$ is a subfield of $F$, then $|F|$ is a power of $|G|$. Therefore, the cardinality of all subfields of $\mathbb{F}_q$ must be equal to $p^m$ for some $m$ such that $(p^m)^k = p^n$ for positive integer $k$. This implies that $m|n$.

For the converse, we again use splitting fields. Note that by our previously stated lemma, if $m|n$, then $p^m - 1|p^n - 1$. Therefore, $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$ in $\mathbb{F}_p[x]$. Thus, every root of $x^{p^m} - x$ must also be a root of $x^{p^n} - x = x^q - x$ (note that we multiplied $x$ to both sides), and is thus an element of $\mathbb{F}_q$. It follows that the splitting field $K$ of $x^{p^m} - x$ over $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$. We know from our proof of existence in Section 2 that $K$ must have a cardinality of $p^m$.

As $x^{p^m} - x$ has only $p^m$ roots, there is only one possible splitting field $K$. From Theorem 2.5, it follows that there is exactly one subfield of $\mathbb{F}_q$ with $p^m$ elements. □

# §4 Finite Extension Fields

In this section, we explore the field extensions of finite fields.

We start with the following proposition.

**Theorem 4.1**

For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^\times$ is cyclic.

*Proof.* We know from Theorem 2.2 that the order of $\mathbb{F}_q^\times$ is $p^n - 1$ for some prime $p$ and integer $n$. Then, there must be $n$ roots of $p^n - 1$ – in other words, $n$ elements whose order divides $n$.

All non-cyclic finite abelian groups have subgroups of the form $(\mathbb{Z}//\mathbb{Z}p\mathbb{Z}/)\mathbb{Z}^2$ for some integer $p$, or in other words it has $p^2$ elements of order $x|p$. Therefore, the multiplicative group $\mathbb{F}_q^\times$ is cyclic. □

To proceed, we need the following definition.

**Definition 4.2.** A **primitive element** $a$ of a finite field $F$ of size $p^n$ for prime $p$ and positive integer $n$ is an element such that $a^n$ has order $p^n - 1$.

In other words, a primitive element $a$ of a finite field $\mathbb{F}_q$ of size $p^n$ is the generator of a the cyclic group $\mathbb{F}_q^\times$. Therefore, we know that $\mathbb{F}_q$ must have $\phi(q)$ primitive elements, as all elements $a \in \mathbb{F}_q$ relatively prime to $q$ can generate such a multiplicative group.

We're now ready to prove an important result.

**Theorem 4.3** (Finite Extension Fields)

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_r$ a finite extension field. Then

- $\mathbb{F}_r$ is a simple extension of $\mathbb{F}_q$, i.e. $\mathbb{F}_r = \mathbb{F}_q(\beta)$ for some $\beta \in \mathbb{F}_r$.
- every primitive element of $\mathbb{F}_r$ can serve as a defining element $\beta$ of $\mathbb{F}_r$ over $\mathbb{F}_q$.

*Proof.* Let $\alpha$ be the primitive element of $\mathbb{F}_r$. Because $\mathbb{F}_q(\alpha)$ contains both 0 and all powers of $\alpha$, it follows that it contains all elements of $\alpha$. It is also clear that $\mathbb{F}_q(\alpha)$ doesn't contain any more elements than $\mathbb{F}_r$ as by definition, $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. Therefore, $\mathbb{F}_r$ is a simple extension, and all primitive elements can serve as defining elements of $\mathbb{F}_r$ over $\mathbb{F}_q$. □

We can thus express any finite field $K$ with subfield $F$ by adjoining any root $\beta$ of some irreducible polynomial of degree $[K : F]$. We finally explore a corollary to the above theorem.

**Corollary 4.4**

For every finite field $\mathbb{F}_q$ and positive integer $n$, there exists some irreducible polynomial in $\mathbb{F}_q[x]$ of degree $n$.

*Proof.* Let $\mathbb{F}_r$ be the extension field of $\mathbb{F}_q$ with order $q^n$ such that the degree of $\mathbb{F}_r \,/\, \mathbb{F}_q$ is $n$. From the above theorem, $\mathbb{F}_r = \mathbb{F}_q(\beta)$ for some $\beta \in \mathbb{F}_r$.

As the degree of such an extension must be finite, $\beta$ is an algebraic extension. Therefore, $\beta$ must have a minimal polynomial $m_\beta(x)$ of degree $n$, and by definition of minimal

polynomial $m_\beta(x)$ is irreducible and all coefficients must be in $\mathbb{F}_q$. Thus, there must exist some irreducible polynomial in $\mathbb{F}_q[x]$ of degree $n$. $\square$

In this paper, we discussed the existence and uniqueness of finite fields, criteria for subfields, and the relation of primitive elements with finite extension fields. We finally proved the existence of irreducible polynomials in all finite polynomial fields $\mathbb{F}_q[x]$. Irreducible polynomials inspire even more discussion not included here.