Finite Fields

Albert Zhu

June 5, 2020

In this paper, we give a brief overview of finite fields. We first discuss the properties of a polynomial intimately related with finite fields. We then provide an abstract construction of finite fields, addressing their existence and uniqueness, and finally present a more useful characterization. Most of the material in this paper was adapted from [Con], with help from [For07] and [Dub15] as well. The LaTeX package used for this paper was taken from Evan Chen, with minor edits by the author.

§1 Definitions and preliminary results

In any field F, we refer to its multiplicative group $F \setminus \{0\}$ as $F^\times$. We also assume that any irreducible polynomial is monic unless otherwise stated, and use the notation $\mathbb{F}$ for a finite field.

Definition 1.1. The **characteristic** of a field F is the smallest natural number m such that adding 1 m times gives the additive identity 0. 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 $\mathbb{F}$ 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 $a, b \in \mathbb{F}$. Then $0 = p = ab$, but since the multiplicative group $\mathbb{F}^\times$ 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 $p = q = 0$. □

Theorem 1.3 (Unique Factorization)

Over a field F, any monic polynomial $f(x)$ can uniquely be expressed in the form

$$f(x) = \prod_{i=1}^{k} d_i(x)$$

up to the order of the factors, where $d_1, d_2, \ldots, d_k$ are irreducible polynomials.

Proof. We use strong induction on the degree of the polynomial. Clearly all monic polynomials with degree 0 and 1 are irreducible, so suppose that all monic polynomials with a degree that is a positive integer less than some positive integer n have unique factorizations. If a monic polynomial f with degree n is irreducible, we're done, but otherwise f must be able to be split into two monic polynomials g, h of smaller degree such that $f(x) = g(x) \cdot h(x)$. But by the induction hypothesis g and h both have unique factorizations, so f does too. □

Theorem 1.4 (Classification of finite fields of prime order)

For a prime p, any field $\mathbb{F}$ of size p is isomorphic to the field $\mathbb{Z}/p\mathbb{Z}$.

Proof. First we'll show that $\mathbb{Z}/p\mathbb{Z}$ is a field. We'll only check that all elements have multiplicative inverses since the other field axioms follow from the fact that $\mathbb{Z}$ is a ring. By Bézout's Identity, for any element $a \in \mathbb{Z}/p\mathbb{Z}$, there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$, so taking modulo p on both sides implies that the remainder of x upon division by p is the multiplicative inverse of a. Now we'll show the isomorphism. It suffices to show that the additive group $\mathbb{F}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, but this follows from Lagrange since the order of any non-identity element of $\mathbb{F}$ must divide p and thus generates it. □

From here on out we let $\mathbb{F}_p$ denote *the* field with p elements, since there is only one up to isomorphism.

Theorem 1.5 (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. □

Definition 1.6. A **primitive element**, or a **multiplicative generator**, of a finite field $\mathbb{F}$ of size p^n is an element with multiplicative order $p^n - 1$.

Lemma 1.7

Let $\mathbb{F}$ be a finite field with order p^n for prime p and positive integral n. Then $\mathbb{F}^\times$ is cyclic, or in other words, there always exists a primitive element.

Proof. Let $S \leq \mathbb{F}$ be the cyclic subgroup of a given order d, which we know must be unique because there are at most d solutions to the equation $x^d - 1 = 0$ by the Fundamental Theorem of Algebra. Suppose that S is generated by $a \in S$, so all of its elements are of the form a^i for some $0 \leq i < d$. Then a^i has order d if and only if $\gcd(i, d) = 1$, because otherwise we would have $(a^i)^{\frac{d}{\gcd(d,i)}} = 1$, and clearly $\frac{d}{\gcd(d,i)}$ is strictly less than d. Thus, if ϕ is the Euler Totient Function, there are $\phi(d)$ elements in S with order d, and d always divides $p^n - 1 = |\,\mathbb{F}\,|$ by Lagrange's Theorem, but it's a well-known result in number theory that $p^n - 1 = \sum_{d | p^n - 1} \phi(d)$, so no d can be left out[1]. Thus, there exists

[1] Another way to see that the function $\sigma(d)$ counting the number of elements with order d must be the same as $\phi(d)$ is through the Möbius Inversion Formula, as outlined in [Dub15].

exactly $\phi(p^n-1)$ elements of order p^n-1, but $\phi(p^n-1)\geq 1$, since ϕ always counts 1, so it follows that there must be at least one primitive element. □

§2 The polynomial $x^{p^n}-x$

We first look at the factorization of a very special polynomial that will be instrumental in both of our characterizations.

Theorem 2.1 (Factorization of $x^{p^n}-x$)

If $\mathbb{F}$ is a finite field with size p^n, $x^{p^n}-x$ can be represented as the product of all minimal polynomials of elements in $\mathbb{F}$ over $\mathbb{F}_p$.

Proof. Suppose that a is a nonzero element of $\mathbb{F}$. By Lagrange's Theorem, the order of a must divide p^n-1 since the cyclic group generated by a under multiplication is a subgroup of $\mathbb{F}^\times$. Thus, $a^{p^n}=a$ for all $a\in\mathbb{F}$ and as a result the polynomial $x^{p^n}-x$ factors as

$$x^{p^n}-x=\prod_{a\in\mathbb{F}}(x-a).$$

However, $x^{p^n}-x$ is also a polynomial with coefficients in $\mathbb{F}_p$, a field, so $x^{p^n}-x$ factorizes uniquely into a product of polynomials irreducible over $\mathbb{F}_p[x]$ as well. But these irreducible polynomials are contained in $\mathbb{F}[x]$, so by unique factorization applied again they must all be reducible into a product of degree 1 monic polynomials in order to match the earlier factorization of $x^{p^n}-x$ we gave, meaning that these are exactly the minimal polynomials of $\mathbb{F}$ over $\mathbb{F}_p$. as desired. □

Corollary 2.2

Any irreducible polynomial $\pi(x)$ in $\mathbb{F}_p[x]$ divides $x^{p^n}-x$ if and only if its degree divides n.

Proof. As we saw in theorem 1.5, $\mathbb{F}$ is an extension of $\mathbb{F}_p$ by Cauchy's Theorem. Treating $\mathbb{F}$ as a vector space over $\mathbb{F}_p$, note that for any basis $\{e_1,e_2,\dots,e_k\}$ of $\mathbb{F}$, all elements of $\mathbb{F}$ by definition can be written uniquely as an expression of the form

$$e_1f_1+e_2f_2+\cdots+e_kf_k, f_i\in\mathbb{F}_p\,.$$

There are p choices for each f_i, so it follows that $\mathbb{F}$ must have p^k elements, and therefore $k=n=\dim_{\mathbb{F}_p}(\mathbb{F})=[\mathbb{F}:\mathbb{F}_p]$. By theorem 2.1, if $\pi(x)$ divides $x^{p^n}-x$, then it must be the minimal polynomial of some element $\alpha\in\mathbb{F}$ over $\mathbb{F}_p$. By the Tower Law, $n=[\mathbb{F}:\mathbb{F}(\alpha)][\mathbb{F}(\alpha):\mathbb{F}_p]$, which implies the "if" direction. For the "only if" direction, let d be the degree of π, and let $n=dk$ for some $k\in\mathbb{Z}$. Any element a in the field $\mathbb{F}_p[x]/(\pi(x))$ is a power of a primitive element, so we must have $a^{p^d}=a$. In particular, x is an element of $\mathbb{F}_p[x]/(\pi(x))$, and we have

$$x\equiv x^{p^d}\equiv x^{p^{2d}}\equiv x^{p^{3d}}\equiv\cdots\equiv x^{p^{kd}}\pmod{\pi(x)}$$

by continuously raising both sides to the p^dth power, whence $\pi(x)\mid x^{p^n}-x$ as desired. □

§3 Finite fields as splitting fields

We present our first characterization of arbitrary finite fields, which turns out to suffice for classification , though is not very useful in practice.

Theorem 3.1 (Splitting Field Construction)

For any prime p and positive integer n, there exists a finite field with p^n elements.

Proof. Let $\mathbb{F}$ be a field extension of $\mathbb{F}_p$ over which $x^{p^n} - x$ splits completely (i.e. $\mathbb{F}$ contains all of $x^{p^n} - x$'s roots, but is not necessarily a splitting field). Since $p \equiv 0 \pmod{p}$, we find that $(x^{p^n} - x)' = p^n x^{p^n-1} - 1 = -1$, so $x^{p^n} - x$ has no double roots over $\mathbb{F}$. In light of this, we will show that the subset S of $\mathbb{F}$ containing the p^n distinct roots of $x^{p^n} - x$ over $\mathbb{F}$ is a field, which will be our construction. Consider the map $\phi : \mathbb{F} \to \mathbb{F}$ given by $\phi(x) = x^{p^n}$: by the Binomial Theorem,

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 \cdots + \binom{p}{p}b^p = a^p + b^p$$

since p never appears in the denominators of any of the terms, meaning that the pth-power map is a homomorphism. Composing this map n times then implies that ϕ is a homomorphism as well, and its fixed points are just the elements of S, so S is a group under addition modulo p. The other field axioms are easy to check, so we're done. □

Theorem 3.2 (Uniqueness)

For any prime p and positive integer n, there only exists one finite field with p^n elements up to isomorphism.

Proof. By theorem 3.1, any finite field with p^n elements is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, but all splitting fields of a fixed polynomial over $\mathbb{F}_p$ are isomorphic, so we're done. □

Corollary 3.3

For every $d|n$, there exists exactly one subfield $\mathbb{F}_d \subseteq \mathbb{F}$ with p^d elements.

Proof. By the Fundamental Theorem of Algebra, $x^{p^d} - x$ can have at most p^d roots in $\mathbb{F}_p$, which means that there can only be at most one $\mathbb{F}_d$. However, also observe that

$$d \mid n \implies p^d - 1 \mid p^n - 1 \implies x^{p^d-1} - 1 \mid x^{p^n-1} - 1 \implies x^{p^d} - x \mid x^{p^n} - x,$$

so $x^{p^d} - x$ must have p^d distinct roots in $\mathbb{F}$ since $x^{p^n} - x$ does too, so there also exists at least one $\mathbb{F}_d$ as desired. □

§4 Finite fields as quotient rings

We first prove a counting lemma due to Gauss in order to make this construction standalone from the previous one.

Lemma 4.1 (Gauss)
The number of monic irreducible polynomials of degree n over a field $\mathbb{F}$ of size q is

$$\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d,$$

where μ is the Möbius function. In particular, this number is always positive when q is prime, but can also be zero otherwise.

Proof 1 (Möbius Inversion Formula). Suppose that there are $\sigma(n)$ irreducible polynomials of degree n. First of all, observe that there are q^n nth degree polynomials in $\mathbb{F}[x]$, so associating every such polynomial to the term x^n, we get the generating function

$$\sum_{n=0}^{\infty} q^n x^n = \frac{1}{1-qx}.$$

On the other hand, by unique factorization, we know that each polynomial $f(x)$ can be factored as

$$f(x) = f_1(x)^{e_1}\cdots f_r(x)^{e_r}$$

for some r, where each of the f_i are irreducible in $\mathbb{F}[x]$. This means that f is associated with the term $x^{\deg(f_1)e_1+\cdots+\deg(f_r)e_r}$, so

$$\begin{aligned}\frac{1}{1-qx} &= \prod_{\text{irreducible } f(x)}(1+x^{\deg(f)}+x^{2\deg(f)}+\cdots)\\ &= \prod_{\text{irreducible } f(x)}\frac{1}{1-x^{\deg(f)}}\\ &= \prod_{i=1}^{\infty}(1-x^i)^{-\sigma(i)}.\end{aligned}$$

Logarithmically differentiating, this becomes

$$\frac{q}{1-qx} = \sum_{i=1}^{\infty}\frac{i\sigma(i)x^{i-1}}{1-x^i} = \sum_{i=1}^{\infty}\sum_{d|i} d\sigma(d)x^{i-1},$$

which means that $q^n = \sum_{d|n} d\sigma(d)$. Applying the Möbius Inversion Formula then gives the desired result. □

Proof 2 (Principle of Inclusion-Exclusion, largely adapted from [CM11]). This proof assumes the results of the previous construction, but is too beautiful not to include. Again let $\sigma(n)$ count the number of irreducible polynomials of degree n in $\mathbb{F}$, and let $\sum_{sym}$ denote the symmetric sum going through all permutations of the dummy variable (for example, for three variables a, b, c, $\sum_{sym} ab = 2ab + 2bc + 2ca$). In the case $n = 1$, there are clearly just q monic polynomials in $\mathbb{F}[x]$ of degree 1, which matches our formula, so suppose now that $n > 1$'s prime decomposition is $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$. By theorem 2.1 and corollary 2.2, the roots of all irreducible polynomials of degree n in $\mathbb{F}_p[x]$ must be contained in $\mathbb{F}$, cannot be shared, and furthermore all have multiplicity 1. Therefore, there are n roots for each irreducible polynomial, meaning that it suffices to find the number of roots across all irreducible polynomials of degree n. The set $\mathcal{R}_n$ consisting of these roots can be defined as

$$\begin{aligned}\mathcal{R}_n &= \{\alpha \in \mathbb{F} \mid [\mathbb{F}(\alpha) : \mathbb{F}_p] = n\} \\ &= \{\alpha \in \mathbb{F} \mid \alpha \text{ is not contained in any proper subfield of } \mathbb{F}\} \\ &= \{\alpha \in \mathbb{F} \mid \alpha \text{ is not contained in any maximal proper subfield of } \mathbb{F}\} \\ &= \left(\mathbb{F}_{p^{n/p_1}} \cup \mathbb{F}_{p^{n/p_2}} \cup \cdots \cup \mathbb{F}_{p^{n/p_r}}\right)^C,\end{aligned}$$

so PIE implies that

$$\sigma(n) = \frac{1}{n}|R_n| = \frac{1}{n}\left(p^n - \sum_{sym} p^{\frac{n}{p_1}} + \sum_{sym} p^{\frac{n}{p_1p_2}} - \sum_{sym} p^{\frac{n}{p_1p_2p_3}} + \cdots + (-1)^r p^{\frac{n}{p_1p_2\cdots p_r}}\right),$$

which becomes the desired result once we translate everything into the language of the Möbius Function. □

> **Remark 4.2.** Of course, we can extend this result to count all irreducible polynomials, not just monic ones, by multiplying our formula by $q-1$ since any non-monic irreducible polynomial can be expressed as $ar(x)$ for some monic irreducible polynomial $r(x)$ of the same degree and nonzero a.

The next construction we provide is much more useful than theorem 3.1, and is the one that is most commonly used.

Theorem 4.3 (Quotient Ring Construction)
For any prime p and positive integer n, there exists a finite field with p^n elements.

Proof. Let $\pi(x)$ be an irreducible polynomial with degree n in $\mathbb{F}_p[x]$. Note that elements of the quotient ring $\mathbb{F}_p[x]/(\pi(x))$ are of the form $a_{n-1}x^{n-1} + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_{n-1}, a_{n-2}, \ldots, a_0 \in \mathbb{F}_p[x]$, so there are clearly p^n of them since we have p choices for each coefficient a_i, of which there are a total of n. Thus, we now just need to check that multiplicative inverses exist, since the rest of the field axioms are all given to us by the ring axioms and aren't hard to check either. We follow a very similar process to the one we did in theorem 1.4. Let $a(x)$ be an element of $\mathbb{F}_p[x]/(\pi(x))$. By Bézout's Identity, there exists polynomials $u(x), v(x) \in \mathbb{Q}[x]$ such that $a(x)u(x) + \pi(x)v(x) = 1$. If $k \in \mathbb{Z}$ is the largest common multiple of all the denominators of coefficients of u and v, then multiplying by k on both sides results in $a(x)u'(x) + \pi(x)v'(x) = k$ for $u'(x), v'(x) \in \mathbb{Z}[x]$, and taking modulo $\pi(x)$ on both sides gives

$$a(x)u'(x) = k',$$

where k' is the remainder of k upon dividing by p. But k' has a multiplicative inverse modulo p, so $k'^{-1}u'(x)$ is the multiplicative inverse of $a(x)$. □

Lemma 4.4
For any prime p and positive integer n, any field of size p^n must be isomorphic to one of the form $\mathbb{F}_p[x]/(\pi(x))$, where $\pi(x)$ is an irreducible polynomial over $\mathbb{F}_p[x]$.

Proof 1. Let $\mathbb{F}$ and $\mathbb{F}'$ be fields with p^n elements and γ be a primitive element generating $\mathbb{F}^\times$. Then if $\pi(x)$ is the minimal polynomial of γ over $\mathbb{F}_p$, by theorem 2.1 there must also exist a root γ' of $\pi(x)$ in $\mathbb{F}'$ and furthermore γ' is a primitive element generating $\mathbb{F}'^\times$. This means that both $\mathbb{F}$ and $\mathbb{F}'^\times$ are isomorphic to $\mathbb{F}_p[x]/(\pi(x))$. □

Proof 2 (First Isomorphism Theorem). Again, let $\mathbb{F}$ be a field with p^n elements and γ be a primitive element generating $\mathbb{F}^\times$. Consider the ring homomorphism $\phi : \mathbb{F}_p[x] \to \mathbb{F}$ given by $\phi(f(x)) = f(\gamma)$: since $\mathbb{F} = \mathbb{F}_p(\gamma)$, it follows that the map is surjective, so $\mathbb{F}_p[x]/\ker(\phi) \cong \operatorname{im}(\phi) = \mathbb{F}$. This implies that $\ker(\phi)$ is a maximal ideal in $\mathbb{F}_p[x]$, so it must be an ideal generated by an nth degree monic irreducible polynomial in $\mathbb{F}_p[x]$, and we're done. □

> **Remark 4.5.** If we assume theorem 3.1, then this proves that irreducible polynomials in $\mathbb{F}_p[x]$ of arbitrary degree always exist, which guarantees that theorem 4.3 always works without needing the very strong lemma 4.1.

References

[CM11] Sunil K. Chebolu and Ján Mináč. *Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle*. 2011. URL: https://www.maa.org/sites/default/files/Chebolu11739.pdf.

[Con] Keith Conrad. *Finite Fields*. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf.

[Dub15] Trinity College Dublin. *Finite fields*. 2015. URL: https://www.maths.tcd.ie/pub/Maths/Courseware/NumberTheory/ch07.pdf.

[For07] G. David Forney. *Introduction to finite fields*. 2007. URL: https://web.stanford.edu/class/ee392d/Chap7.pdf.