Finite Fields

Sam Auyeung

October 30, 2019

The goal of this note is to classify all finite fields. For each prime p and $n \in \mathbb{Z}^+$, there exists a unique field up to isomorphism with p^n elements. These are in fact, all of them. So for example, there is no field with 10 elements. We'll also talk about the Galois group of $GF(p^n)$ over $\mathbb{F}_p$ and other extensions.

1 The Characteristic of a Finite Field is Prime

Suppose that we have a field F. If it has characteristic zero, then there is a field embedding $\mathbb{Q} \to F$ and so F cannot be finite. Thus, let F be a finite field. It must have positive characteristic, say k. Consider the set $S = \{0, 1, 1+1, ..., 1+1+...+1\}$ where the last sum is 1 added to itself $k-1$ times. It's clear that S is closed under addition as a sum of 1's with another sum of 1's is still a sum of 1's. The cyclic nature here ensures we stay in S. It is also closed under multiplication. If we have $(1+...+1)(1+...+1)$ where the first sum consists of a copies of 1 and the second has b copies, then the product is ab copies of 1. Thus, S is in fact a subring isomorphic to $\mathbb{Z}_k$. But F has no zero divisors so in fact, we need $p := k$ to be prime.

2 Some Basic Definitions and Lemmas

Recall that a **splitting field** E of a polynomial $f(x) \in F[x]$ is the minimal field in which $f(x)$ splits into linear terms. That is, there are no proper subfields in which f splits. Splitting fields must contain the base field and it's an interesting question to ask what are the automorphisms on E that fix the base field F. We give some useful theorems and lemmas but we don't always give proofs.

Theorem 2.1. *The splitting field of a polynomial $f(x) \in F[x]$ exists and is unique up to isomorphism.*

Lemma 2.2. *A polynomial $f(x) \in F[x]$ has multiplicity of zeros in its splitting field E if and only if $f(x)$ and $f'(x)$, its formal derivative, share common factors of positive degree.*

Example 2.3. A trivial example is that of $p(x) = (x+1)^2$ over $\mathbb{Q}$; $p'(x) = 2(x+1)$ and so they share a common factor.

Lemma 2.4. *In a field F of characteristic p, if $x, y \in F$, then $(x+y)^p = x^p + y^p$.*

Proof. Using the binomial theorem, we can expand to get

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

We just need to show that $\binom{p}{k}$ for $1 < k < p$ is divisible by p. Then the characteristic of F being p ensures those terms vanish. Now,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \implies p! = k!(p-k)!\binom{p}{k}.$$

Clearly, p divides the LHS and p does not divide $k!$ and does not divide $(p-k)!$. But one of the defining properties of a prime is that if $p|ab$, then $p|a$ or $p|b$. The contrapositive tells us that p cannot divide the product $k!(p-k)!$. Thus, p divides $\binom{p}{k}$. $\square$

3 Classification of Finite Fields

We first show that for every prime p and $n \in \mathbb{Z}^+$, we have a unique field of order p^n (up to isomorphism). Then we show that there can be no other orders for finite fields.

Let us fix p and n and let $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. This polynomial is clearly reducible. We'll let E be the splitting field of f over $\mathbb{F}_p$. Thus, it contains all the roots of f. We first show that the roots of f are all distinct and hence, there are p^n distinct roots of f.

This is simply an application of the multiplicity lemma above. $f'(x) = p^n x^{p^n-1} - 1 = -1$ as p^n vanishes. Thus, $f'(x)$ has zero degree and thus, there can't be multiplicity of roots. Thus, E has at least p^n elements.

Now consider $K \subset E$ be the set containing all the roots of f. We will show that K is in fact closed under $+, -, \times, \div$ and also contains 0 and 1. Hence, it is a subfield. So suppose $\alpha, \beta \in K$.

1. $+$: We have that $f(\alpha+\beta) = (\alpha+\beta)^{p^n} - (\alpha+\beta)$. By the lemma above, $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$. Thus, $f(\alpha+\beta) = f(\alpha) + f(\beta) = 0$.

2. $-$: We need only show that $f(-\alpha) = 0$. If p is an odd prime, then $(-1)^{p^n} = -1$ and so $f(-\alpha) = -f(\alpha)$. If $p = 2$, then $-1 = +1$ and so the result also holds.

3. $\times$: Consider $f(\alpha\beta) = \alpha^{p^n}\beta^{p^n} - \alpha\beta$ (by commutativity). Since $f(\alpha) = 0$, this means $\alpha^{p^n} = \alpha$. Thus, $f(\alpha\beta) = \alpha f(\beta) = 0$.

4. $\div$: We only need to check
$$f(1/\alpha) = \frac{1}{\alpha^{p^n}} - \frac{1}{\alpha}.$$
Multiplying on both sides by α^{p^n+1}, we get $\alpha^{p^n+1} f(1/\alpha) = \alpha - \alpha^{p^n} = -f(\alpha) = 0$. Since there are no zero divisors in a field and α^{p^n+1} is not zero, then $f(1/\alpha) = 0$.

Lastly, it is clear that $f(0) = f(1) = 0$. Thus, K is a subfield but also contains all the roots of f. So in fact, $E = K$ because K is the splitting field and it is unique up to isomorphism.

Next, we show that there can be no fields of any other type of order. Recall that there is a classification theorem for finitely generated abelian groups. In particular, if G is finite and abelian, then

$$G \cong \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{a_k}}$$

where p_i are primes, not necessarily distinct. It is a finite field of characteristic p is, under addition, a finite abelian group. It's clear that it should be isomorphic to some number of copies of $\mathbb{Z}_p$ because any other combination will give elements with additive order other than p. Thus, we've given a full classification of finite fields.

Thus, the way to construct a field of order p^n is to take a properly chosen irreducible part of $f(x)$, call it $p(x)$, and consider $\mathbb{F}_p[x]/\langle p(x)\rangle$. One may wonder whether it depends on the choice of irreducible part. We address this below.

In honor of Galois, the finite field of order p^n is often denoted by $GF(p^n)$. We also denote this by $\mathbb{F}_{p^n}$.

4 Roots of $f(x)$

We see that $f(x) = x^{p^n} - x = x(x-1)(x^{p^n-2} + x^{p^n-3} + ... + x + 1)$. The last part may be further reducible. Thus, we should choose a irreducible piece $p(x)$ which does not split over $\mathbb{F}_p$ and form a quotient of the polynomial ring in this fashion.

Above, we showed that roots form a field themselves. Of course, if $k \in \mathbb{F}_p$, then $k^{p-1} = 1$ by Lagrange's theorem. Thus, $k^p = k$. And thus, $k^{p^n} = k$. We've shown that elements of the base field are roots of $f(x)$. In fact, we have the following result: Let α be any root of $f(x)$. Then for any $k \in \mathbb{F}_p$, $k\alpha$ is also a root because $f(k\alpha) = kf(\alpha)$.

However, we'll like to see that the group of units $\mathbb{F}_{p^n}^\times$ is cyclic (and hence $\mathbb{Z}_{p^n-1}$).

Proof. Let $G = \mathbb{F}_{p^n}^\times$; it is finite and abelian and so we can apply the structure theorem for finite abelian groups. We use the other version:

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus ... \oplus \mathbb{Z}_{n_k}$$

where each n_{i+1} divides n_i. Let $a = (a_1, ..., a_k)$ be an element. Then $a^{n_1} = (n_1 a_1, ..., n_1 a_k) = 0$; here 0 is the additive identity of the direct sum of cyclic groups but it corresponds to the element $1 \in G$. Thus, the polynomial $x^{n-1} - 1$ has $p^n - 1$ roots in $\mathbb{F}_{p^n}$. The number of zeros cannot exceed the degree of the polynomial so $p^n - 1 \leq n_1$. On the other hand, G has a subgroup isomorphic to $\mathbb{Z}_{n_1}$. Thus $n_1 \leq p^n - 1$ and so they equal. Thus, $\mathbb{F}_{p^n}^\times \cong \mathbb{Z}_{p^n-1}$. $\square$

Thus, we see that we can find some root which generates all the other roots. Say we have such a generating root α. We also have that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and so α is algebraic over $\mathbb{F}_p$ of degree n because $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^n}$. This means, the minimal polynomial of α is degree n. We just need to look for an irreducible piece $p(x)$ of $f(x)$ of degree n. Such a polynomial $p(x)$ might not be unique as seen in the following example.

Example 4.1. We consider $p = 3, n = 2$. Then, because we're taking mod 3,

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

The quadratic formula shows us that the six roots we get from the irreducible pieces are $\pm\sqrt{-1}, 2(\pm 1 \pm \sqrt{-1})$. Adjoining $\sqrt{-1}$ is enough to generate all the other roots with addition and multiplication. However, if we wish to generate all the roots multiplicatively, we can't choose $\pm\sqrt{-1}$ as it will generate only 4 things. However, adjoining any of the other 4 will give us roots that multiplicatively, generate all the nonzero roots (and we expect this because the Euler-Totient $\phi(3^2 - 1) = \phi(8) = 4$). So we could adjoin, say $2 + 2\sqrt{-1}$ which should have multiplicative order 8. This example shows that though $\sqrt{-1}$ has a minimal polynomial of degree 2, adjoining it may not give us all the roots through **multiplicative generation**, though certainly it will generate everything if we allow for all four operations. Also, note that since $2 \equiv -1 \pmod 3$, $\sqrt{-1} = \sqrt{2}$.

5 Subfields of Finite Fields

The subfields of $\mathbb{F}_{p^n}$ are quite easy to consider. They are precisely the $\mathbb{F}_{p^m}$ where m divides n.

Example 5.1. Consider $\mathbb{F}_{2^{24}}$. The divisors of 24 are 1, 2, 3, 4, 6, 8, and 12. So we have the following subfield chains: $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16} \subset \mathbb{F}_{512} \subset \mathbb{F}_{2^{24}}$ and also $\mathbb{F}_2 \subset \mathbb{F}_8 \subset \mathbb{F}_{64} \subset \mathbb{F}_{2^{12}} \subset \mathbb{F}_{2^{24}}$. Note that $\mathbb{F}_4$ is not contained in $\mathbb{F}_8$.

6 More Examples

Example 6.1. Consider the polynomial $p(x) = (x^2-2)(x^2-3)$ over $\mathbb{F}_5$. Note that the elements of $\mathbb{F}_5$ square to 0,1, or 4. Thus, nothing squares to 2 or 3. What is the splitting field of this quartic?

We see that if we adjoin $\sqrt{2}$ and $\sqrt{3}$, $p(x)$ splits. But also, $2\sqrt{2}$ squares to $8 \equiv 3 \pmod 5$. Thus, the splitting field is $\mathbb{F}_5(\sqrt{2}) \cong \mathbb{F}_{25}$.

7 The Fröbenius Automorphism and Galois Group

Let G be the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Let $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the automorphism sending $x \mapsto x^p$. This clearly permutes the roots because, from above, we say that if β is a root, then so is β^p. Moreover, φ fixes the base field $\mathbb{F}_p$.

This field automorphism φ is quite important and is called the Fröbenius automorphism. It is quite easy to show that $\varphi^n = \text{id}$. Moreover, suppose α generates $\mathbb{F}_{p^n}^\times$. We can completely define element of the Galois group (an automorphism) by determining where α is sent. It's clear that since the base field is fixed, α can only be sent to powers of α of the form p^k. This means that in fact, the Fröbenius automorphism generates our Galois group G and proves that $G \cong \mathbb{Z}_n$.

With some standard Galois theory, we can now also see what the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^m}$ is when m divides n. They are subgroups of $\mathbb{Z}_n$ and should be $\mathbb{Z}_{n/m}$.

8 Algebraic Closure of $\mathbb{F}_p$

The algebraic closure of any field is simply the union of all the finite extensions. For any two elements $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, their product $ab \in \mathbb{F}_{p^{nm}}$. Thus, letting $\overline{\mathbb{F}}_p$ denote the algebraic closure of $\mathbb{F}_p$,

$$\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n}.$$

It may be interesting to apply the Fröbenius automorphism φ to $\overline{\mathbb{F}}_p$. Since the algebraic closure is this union, then we see that applying φ will move the elements of $\mathbb{F}_{p^n}$ only within itself. In other words, if $\alpha \in \mathbb{F}_{p^n}$, its orbit is contained in $\mathbb{F}_{p^n}$. However, φ does not have finite order now because every $n \in \mathbb{Z}^+$ is represented.

The Galois group $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is something called the profinite completion of the integers (inverse limit):

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}_n.$$

We take this limit of the $\mathbb{Z}_n$ as those are the Galois groups of the finite extensions over $\mathbb{F}_p$. Thus, an interesting fact is that $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \widehat{\mathbb{Z}}$ does not depend on p. The Galois group is the same for every p.