An Elementary Construction of Finite Fields

Uthsav Chitra

August 13, 2014

While most proofs of the existence of finite fields involve splitting fields, we present here a construction that uses no math higher than basic abstract algebra. In particular, this means no Galois theory or the theory behind splitting fields will be used.

1 Setting the Stage

Let p be a prime. Consider $\mathbb{F}_p[x]/(\pi(x))$ for some irreducible $\pi(x) \in \mathbb{F}_p[x]$. Because $\mathbb{F}_p[x]$ is a PID, it follows that $(\pi(x))$ is a maximal ideal, so that $\mathbb{F}_p[x]/(\pi(x))$ is a field. Furthermore, if $\deg \pi(x) = n$, then $\mathbb{F}_p[x]/(\pi(x)) = \{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} : a_i \in \mathbb{F}_p\}$ and $\left|\mathbb{F}_p[x]/(\pi(x))\right| = p^n$. Thus, if we can show that for every $n > 0$, there exists an irreducible polynomial of degree n then we're done.

To do this, we'll develop an expression for the number of irreducible polynomials of degree n in $\mathbb{F}_p[x]$ and then show that this expression must be greater than 0 for all primes p.

2 Multiplying Polynomials

Like most constructions of finite fields, we consider the polynomial $f(x) = x^{p^n} - x$, with $f(x) \in \mathbb{F}_p[x]$ (n is fixed of course). The bulk of this article is in the proof of the following:

Theorem 2.1

Let $g_d(x)$ be the product of all degree d monic irreducible polynomials in $\mathbb{F}_p[x]$. Then,

$$f(x) = \prod_{d|n} g_d(x).$$

Proof. We proceed by strong induction on n. For our base case, let $n = 1$. Then, the product of all monic irreducibles of degree 1 is $x \cdot (x-1) \cdot \ldots \cdot (x-(p-1)) = x^p - x$ by Fermat's Little Theorem.

Now suppose the statement holds for all $n' < n$. Let $\pi(x)$ denote a monic irreducible let $\deg \pi = d$ where $d|n$. First we will show that $\pi|f$, which will imply that $\prod_{d|n} g_d \Big| f$.

Consider $F = \mathbb{F}_p[x]/(\pi(x))$. This is a finite field with p^d elements. In particular, $F^\times$ is an abelian group of order $p^d - 1$, so for all $a \in F^\times$, we have $a^{p^d-1} = 1$. Therefore for all $a \in F$, $a^{p^d} = a$ (since $0^{p^d} = 0$).

Taking both sides to the p^d-th power gives $(a^{p^d})^{p^d} = a^{p^d} \Rightarrow a^{p^{2d}} = a$. Repeating this process, we see that for any integer $y > 0$, $a^{p^{(yd)}} = a$. Since $d|n$, if we let $y = \frac{n}{d}$, we get that $a^{p^n} = a \Rightarrow a^{p^n} - a = 0$.

Setting $a = x$ yields $x^{p^n} - x = 0$ in $F = \mathbb{F}_p[x]/(\pi(x))$, which implies that $\pi(x) \Big| x^{p^n} - x$. From our discussion before, this gives $\prod_{d|n} g_d \Big| f$.

We can also easily show that f has no double roots, so that if π is a monic irreducible of degree d such that $\pi|f$ (with $d|n$), then $\pi^2 \nmid f$. To do this, note that $f' = (p^n)(x^{p^{n-1}}) - 1 = -1$ in $\mathbb{F}_p[x]$. Thus, f' shares no roots with f, so f has no double roots.

Now assume for the sake of contradiction that $f(x) \neq \prod_{d|n} g_d(x)$. Since $\prod_{d|n} g_d \Big| f$ and f has no double roots, this means that f has some other factors besides the product of g_d's. Thus we can assume that there exists some monic irreducible π' such that $\pi'|f$ but $\pi' \nmid g_d$ for any $d|n$.

Let the degree of π' be d'. For π' not to divide any of the g_d's, we must have that $d' \nmid n$. So by the inductive hypothesis, $\pi'|f'$, where $f' = x^{p^{d'}} - x$. Since $\pi'|f$ and $\pi'|f'$, we must have that $\pi'|(f', f)$. Using the well-known fact that $(x^n - 1, x^m - 1) = x^{(n,m)} - 1$, we find that:

$$\begin{aligned}
(f', f) &= (x^{p^{d'}} - x, x^{p^n} - x) \\
&= x \cdot (x^{p^{d'}-1} - 1, x^{p^n - 1} - 1) \\
&= x \cdot (x^{(p^{d'}-1, p^n-1)} - 1) \\
&= x \cdot (x^{p^{(d',n)}-1} - 1) \\
&= x^{p^{(d',n)}} - x
\end{aligned}$$

Therefore $\pi'|x^{p^{(d',n)}} - x$. Since $d' \nmid n$, it follows that $(d', n) < d'$, so by the inductive hypothesis we see that $\deg \pi' \leq d' = \deg \pi'$, which is clearly a contradiction.

Thus, $f = \prod_{d|n} g_d$, and we are done. ◻

3 Counting Polynomials

Theorem 3.1

For all natural numbers n, there is an irreducible polynomial of degree n.

Proof. Let $p(n)$ be the number of monic irreducible polynomials of degree n. Degree comparison of Theorem 2.1 yields:

$$p^n = \sum_{d|n} d \cdot p(d) \Rightarrow p^n = \sum_{d|n} h(d),$$

where $h(x) = x \cdot p(x)$. Mobius inversion yields

$$h(n) = \sum_{d|n} \mu(d) \cdot p^{\frac{n}{d}} \Rightarrow p(n) = \frac{1}{n}\left(\sum_{d|n} \mu(d) \cdot p^{\frac{n}{d}}\right) \tag{1}$$

We will show that $p(n) > 0$ for all $n > 0$. It is sufficient for us to show that $h(n) > 0$. This is equivalent to

$$h(n) > 0 \iff p^n + \sum_{d|n} \epsilon_d \cdot p^d > 0 \iff p^n > \sum_{d|n} -\epsilon_d \cdot p^d,$$

fi where ϵ_d is either $+1$, 0, or -1 depending on the value of d. Since $1 \geq -\epsilon_d$,

$$\sum_{d|n} p^d \geq \sum_{d|n} -\epsilon_d \cdot p^d.$$

Furthermore, letting q be the smallest prime factor of n, we get the loose bound

$$\sum_{i=1}^{n/q} p^i \geq \sum_{d|n} p^d.$$

Thus, if we can show that $p^n > \sum_{i=1}^{n/q} p^i$, we'll be done.

Noting that the RHS of the above equation is a geometric series, we get:

$$p^n > \sum_{i=1}^{\frac{n}{q}} p^i \iff p^n(p-1) > p^{\frac{n}{q}+1} - 1.$$

Since $p^n(p-1) > p^n > p^n - 1$, it is sufficient to show that

$$p^n > p^{\frac{n}{q}+1}.$$

Looking at exponents:

$$\begin{aligned} n > \frac{n}{q} + 1 \\ &\iff n\left(1 - \frac{1}{q}\right) > 1 \\ &\iff n > \frac{q}{q-1} \geq 2, \end{aligned}$$

since the smallest possible value of q is 2.

Therefore, $h(n) > 0$ for $n > 2$. $n = 1$ and $n = 2$ can be handled easily by examination. $n = 1$ is clear, since any monic polynomial of degree 1 is irreducible. For $n = 2$, let s be a quadratic nonresidue mod p and look $x^2 - s$. □

By Theorem 3.1, a monic irreducible polynomial of degree n exists for all $n > 0$, and so we can construct a finite field of order p^n for any prime p and integer n.

4 Other Facts About Finite Fields

Now that we've constructed finite fields, we want to prove two other things about finite fields to finish up our discussion:

- All finite fields have size p^n.
- If two finite fields have the same size, they must be isomorphic.

Let's start with the first one.

Claim 4.1. If F is a finite field, it must have size p^n for some prime p and positive integer n.

Proof. Let F be a finite field. Since F is finite, it cannot have characteristic 0. Therefore, let F have characteristic p for some prime p. Consider $S = \{1, 1+1, 1+1+1, \ldots, 1+1+1+\ldots+1\}$, a subset of F, where the last element is the sum of $p-1$ 1's. Note that $S \cong \mathbb{F}_p$, so there exists an embedding of $\mathbb{F}_p$ inside F.

Now, the key insight in the proof is to realize that we can make F a vector space over this copy of $\mathbb{F}_p$ (why not over another field? Because F has characteristic p). So, as a vector space, suppose F has a basis of n elements given by $\{e_1, e_2, \ldots, e_n\}$. Then, $F = \{c_1 e_1 + \ldots + c_n e_n : c_i \in \mathbb{F}_p\}$, so it follows that $|F| = p^n$ for some n. □

For the second item… I'm not sure of a good way to prove it without using splitting fields or the ideas underlying them. There are certainly ways to do it without directly using a splitting field, but the methods I've come across use concepts from the proofs of splitting fields, so it feels like it's cheating to cite those as elementary.