FINITE FIELDS

KEITH CONRAD

This handout discusses finite fields: how to construct them, some algebraic properties, and their Galois groups. We write $\mathbf{Z}/(p)$ and $\mathbf{F}_p$ interchangeably for the field of size p.

1. Construction

Theorem 1.1. *For a prime p and a monic irreducible $\pi(x)$ in $\mathbf{F}_p[x]$ of degree n, the ring $\mathbf{F}_p[x]/(\pi(x))$ is a field of order p^n.*

Proof. The cosets mod $\pi(x)$ are represented by remainders

$$c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}, \quad c_i \in \mathbf{F}_p,$$

and there are p^n of these. Since the modulus $\pi(x)$ is irreducible, the ring $\mathbf{F}_p[x]/(\pi(x))$ is a field using the same proof that $\mathbf{Z}/(m)$ is a field when m is prime. □

Example 1.2. Two fields of order 8 are $\mathbf{F}_2[x]/(x^3 + x + 1)$ and $\mathbf{F}_2[x]/(x^3 + x^2 + 1)$.

Example 1.3. Two fields of order 9 are $\mathbf{F}_3[x]/(x^2 + 1)$ and $\mathbf{F}_3[x]/(x^2 + x + 2)$.

Example 1.4. The polynomial $x^3 - 2$ is irreducible in $\mathbf{F}_7[x]$, so $\mathbf{F}_7[x]/(x^3 - 2)$ is a field of order $7^3 = 343$.

The concrete construction of finite fields in the form $\mathbf{F}_p[x]/(\pi(x))$ does not cover all possible constructions. For instance, $\mathbf{Z}[i]/(3)$ is a field of size 9. We will see that every finite field is isomorphic to a field of the form $\mathbf{F}_p[x]/(\pi(x))$, so these polynomial constructions give us working models of any finite field.

Theorem 1.5. *Any finite field has prime power order.*

Proof. For any commutative ring R there is a unique ring homomorphism $\mathbf{Z} \to R$, given by

$$m \mapsto \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}}, & \text{if } m \geq 0, \\ -(\underbrace{1 + 1 + \cdots + 1}_{|m| \text{ times}}), & \text{if } m < 0. \end{cases}$$

We apply this to the case when $R = F$ is a finite field. The kernel of $\mathbf{Z} \to F$ is nonzero since $\mathbf{Z}$ is infinite and F is finite. Write the kernel as $(m) = m\mathbf{Z}$ for an integer $m > 0$, so $\mathbf{Z}/(m)$ embeds as a subring of F. Any subring of a field is a domain, so m has to be a prime number, say $m = p$. Therefore there is an embedding $\mathbf{Z}/(p) \hookrightarrow F$. Treating F as a $\mathbf{Z}/(p)$-vector space, it is finite-dimensional since F is even a finite set. Letting $n = \dim_{\mathbf{Z}/(p)}(F)$, the elements of F can be written in terms of a basis $\{e_1, \ldots, e_n\}$ over $\mathbf{Z}/(p)$ as unique linear combinations

$$c_1 e_1 + \cdots + c_n e_n, \quad c_i \in \mathbf{Z}/(p).$$

The number of these linear combinations is p^n. □

Lemma 1.6. *If F is a finite field, the group $F^\times$ is cyclic.*

Proof. Let N be the largest order of a number in the group $F^\times$. It is a theorem from group theory that in any finite abelian group, all orders of elements divide the maximal order, so every t in $F^\times$ satisfies $t^N = 1$. Therefore all numbers in $F^\times$ are roots of $x^N - 1$.

Let $q = \#F$. The number of roots of a polynomial over a field is at most the degree of the polynomial, and $x^N - 1$ has $q - 1$ roots in F, so $q - 1 \leq N$. Since N is the order of an element in $F^\times$, which is a group with order $q - 1$, $N|(q - 1)$, so $N \leq q - 1$. Therefore $N = q - 1$, so there are elements of $F^\times$ with order $q - 1$, which means $F^\times$ is cyclic. □

Example 1.7. In the field $\mathbf{F}_3[x]/(x^2+1)$, the nonzero numbers are a group of order 8. The powers of x are

$$x, \quad x^2 = -1 = 2, \quad x^3 = 2x, \quad x^4 = 2x^2 = -2 = 1,$$

so x is not a generator. But $x + 1$ is a generator: its successive powers are in the table below.

k	1	2	3	4	5	6	7	8
x^k	$x+1$	$2x$	$2x+1$	2	$2x+2$	x	$x+2$	1

Example 1.8. For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic: there is an $a \not\equiv 0 \bmod p$ such that $\{a, a^2, a^3, \ldots, a^{p-1} \bmod p\} = (\mathbf{Z}/(p))^\times$. The proof of this is not constructive, and in fact there is no simple algorithm for constructing a generator of $(\mathbf{Z}/(p))^\times$.

Theorem 1.9. *Every finite field is isomorphic to $\mathbf{F}_p[x]/(\pi(x))$ for some prime p and some monic irreducible $\pi(x)$ in $\mathbf{F}_p[x]$.*

Proof. Let F be a finite field. By Theorem 1.5, F has a prime power order, say p^n, and there is a field embedding $\mathbf{F}_p \hookrightarrow F$. The group $F^\times$ is cyclic by Lemma 1.6. Let γ be a generator of $F^\times$. We get a ring homomorphism $\varphi\colon \mathbf{F}_p[x] \to F$ by evaluating polynomials at γ: $\varphi(f(x)) = f(\gamma)$. Since every number in F is 0 or a power of γ, φ is onto ($0 = \varphi(0)$ and $\gamma^r = \varphi(x^r)$ for any $r \geq 0$). Therefore $\mathbf{F}_p[x]/\ker\varphi \cong F$. The kernel of φ is a maximal ideal in $\mathbf{F}_p[x]$, so it must be $(\pi(x))$ for some monic irreducible $\pi(x)$ in $\mathbf{F}_p[x]$. □

Theorem 1.9 does not assure us fields of all prime power orders exist. It only tells us that *if* a field of order p^n exists then it is isomorphic to some $\mathbf{F}_p[x]/(\pi(x))$. In the next section we will show a field of any prime power order exists.

2. Finite fields as splitting fields

We can describe any finite field as a splitting field of a polynomial depending only on the size of the field.

Lemma 2.1. *A field of prime power order p^n is a splitting field over $\mathbf{F}_p$ of $x^{p^n} - x$.*

Proof. Let F be a field of order p^n. From the proof of Theorem 1.5, F contains a subfield isomorphic to $\mathbf{Z}/(p) = \mathbf{F}_p$. Explicitly, the subring of F generated by 1 is a field of order p.

Every $t \in F$ satisfies $t^{p^n} = t$: if $t \neq 0$ then $t^{p^n-1} = 1$ since $F^\times = F - \{0\}$ is a multiplicative group of order $p^n - 1$, and then multiplying through by t gives us $t^{p^n} = t$, which is also true when $t = 0$. The polynomial $x^{p^n} - x$ has every element of F as a root, so F is a splitting field of $x^{p^n} - x$ over the field $\mathbf{F}_p$. □

Theorem 2.2. *Any two finite fields of the same size are isomorphic.*

Proof. The size of a finite field must be a prime power, say p^n. By Lemma 2.1, any field of order p^n is a splitting field of $x^{p^n} - x$ over $\mathbf{F}_p$.

By field theory, any two splitting fields of a fixed polynomial over $\mathbf{F}_p$ are isomorphic, so any two fields of order p^n are isomorphic. □

The analogous theorem for finite groups and finite rings is false: having the same size does not imply isomorphism. For instance, $\mathbf{Z}/(4)$ and $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ both have order 4 and they are nonisomorphic as additive groups and also as commutative rings.

Using splitting fields, we can now show finite fields of any prime power order exist.

Theorem 2.3. *For any prime power p^n, a field of order p^n exists.*

Proof. Taking our cue from the statement of Lemma 2.1, let F be a field extension of $\mathbf{F}_p$ over which $x^{p^n} - x$ splits completely. General theorems from field theory guarantee there is such a field.

Inside F, the roots of $x^{p^n} - x$ form the set

$$S = \{t \in F : t^{p^n} = t\}.$$

This set has size p^n since the polynomial $x^{p^n} - x$ is separable: $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$ since $p = 0$ in F, so $x^{p^n} - x$ has no roots in common with its derivative. It splits completely over F and has degree p^n, so it has p^n roots in F.

We will show S is a field. It is easily closed under multiplication and (for nonzero solutions) inversion. It remains to show S is an additive group. Since $p = 0$ in F, so $(a+b)^p = a^p + b^p$ for all a and b in F (the intermediate terms in $(a+b)^p$ coming from the binomial theorem have coefficients $\binom{p}{k}$ that are all multiples of p). Therefore $t \mapsto t^p$ on F is additive, so its n-th iterate $t \mapsto t^{p^n}$ is also additive. The fixed points of an additive map are a group under addition, so S is a group under addition. □

Corollary 2.4. *For any prime p and positive integer n, there is a monic irreducible of degree n in $\mathbf{F}_p[x]$.*

Proof. By Theorem 2.3, an abstract field of order p^n exists. By Theorem 1.9, the existence of an abstract field of order p^n implies the existence of a monic irreducible $\pi(x)$ in $\mathbf{F}_p[x]$ of degree n. □

We write $\mathbf{F}_{p^n}$ for a finite field of order p^n. By the proof of Theorem 1.5, $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. All fields of order p^n are isomorphic to each other and they each contain $\mathbf{F}_p$ in only one way (the subfield generated by 1 is isomorphic to $\mathbf{F}_p$).

Theorems 1.9 and 2.3 tell us there is a monic irreducible $\pi(x)$ such that $x \bmod \pi(x)$ is a generator of the nonzero numbers in $\mathbf{F}_p[x]/(\pi(x))$. For instance, fields of size 9 that are of the form $\mathbf{F}_p[x]/(\pi(x))$ need $p = 3$ and $\deg \pi(x) = 2$. The monic irreducible quadratics in $\mathbf{F}_3[x]$ are $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$. In the fields

$$\mathbf{F}_3[x]/(x^2+1), \quad \mathbf{F}_3[x]/(x^2+x+2), \quad \mathbf{F}_3[x]/(x^2+2x+2),$$

x is not a generator of the nonzero numbers in the first field but is a generator of the nonzero numbers in the second and third fields. So although the field $\mathbf{F}_3[x]/(x^2+1)$ is the simplest choice among these three examples, it's not the one that would come out of the proof of Theorem 1.9 when we look for a "polynomial model" of fields of order 9.

Theorem 2.5. *The subfields of $\mathbf{F}_{p^n}$ have order p^d where $d|n$, and there is one such field for each d.*

Proof. Let F be a field with $\mathbf{F}_p \subset F \subset \mathbf{F}_{p^n}$. Set $d = [F : \mathbf{F}_p]$, so $\#F = p^d$ and d divides $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. We will describe F in a way that only depends on $\#F$, so F is the only subfield of its size in $\mathbf{F}_{p^n}$.

Since $F^\times$ has order $p^d - 1$, for any $t \in F^\times$ we have $t^{p^d-1} = 1$, so $t^{p^d} = t$, and that holds even for $t = 0$. The polynomial $x^{p^d} - x$ has at most p^d roots in $\mathbf{F}_{p^n}$, and since F is a set of p^d different roots,

$$F = \{t \in \mathbf{F}_{p^n} : t^{p^d} = t\}.$$

This shows F is unique, since the right side depends on F only through its size.

To prove for each $d|n$ there is a subfield of $\mathbf{F}_{p^n}$ with order p^d, the set

$$\{t \in \mathbf{F}_{p^n} : t^{p^d} = t\}$$

is a field by the same proof that S is a field in the proof of Theorem 2.3. To show its size is p^d we find $p^d - 1$ nonzero numbers in $\mathbf{F}_{p^n}$ satisfying the condition $t^{p^d-1} = 1$. Let γ be a generator of $\mathbf{F}_{p^n}^\times$, so γ has multiplicative order $p^n - 1$. Since $d|n$, $(p^d - 1)|(p^n - 1)$, so $\alpha := \gamma^{(p^n-1)/(p^d-1)}$ has order $p^d - 1$. The powers α^k $(0 \le k \le p^d - 2)$ all satisfy $t^{p^d-1} = 1$. $\square$

In the diagram below we list all the subfields of $\mathbf{F}_{p^{12}}$. It resembles the lattice of divisors of 12.

$$\begin{tikzcd}
 & \mathbf{F}_{p^{12}} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & & \\
\mathbf{F}_{p^4} \arrow[dr, dash, "2"'] & & \mathbf{F}_{p^6} \arrow[dl, dash, "3"] \arrow[dr, dash, "2"] & \\
 & \mathbf{F}_{p^2} \arrow[dr, dash, "2"'] & & \mathbf{F}_{p^3} \arrow[dl, dash, "3"] \\
 & & \mathbf{F}_p &
\end{tikzcd}$$

3. Galois groups

The numbers in $\mathbf{F}_{p^n}$ are a full set of roots of $x^{p^n} - x$, so $\mathbf{F}_{p^n}$ is the splitting field over $\mathbf{F}_p$ of this separable polynomial. Therefore $\mathbf{F}_{p^n}/\mathbf{F}_p$ is a Galois extension. It is a fundamental feature of finite fields that the Galois group is cyclic, with a canonical generator.

Theorem 3.1. *The Galois group* $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ *is cyclic and a generator is the p-th power map* $\varphi_p \colon t \mapsto t^p$.

Proof. Any $a \in \mathbf{F}_p$ satisfies $a^p = a$, so the function $\varphi_p \colon \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ fixes $\mathbf{F}_p$ pointwise. Also φ_p is a field homomorphism and it is injective (all field homomorphisms are injective), so φ_p is surjective since $\mathbf{F}_{p^n}$ is finite. Therefore $\varphi_p \in \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$.

The size of the group $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ is $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. We will show φ_p has order n, so it generates the Galois group.

For $r \ge 0$, $\varphi_p^r(t) = t^{p^r}$. So if φ_p^r is the identity then $t^{p^r} = t$ for all $t \in \mathbf{F}_{p^n}$. The polynomial $x^{p^r} - x$ has at most p^r roots in a field, so $p^n \le p^r$, so $n \le r$. Thus φ_p has order at least n in $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$. Since the Galois group has order n, the order of φ_p in the Galois group has to be n. $\square$

Corollary 3.2. *If $\pi(x) \in \mathbf{F}_p[x]$ is irreducible with degree d and it has a root α in some extension field of $\mathbf{F}_p$ then its full set of roots is $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$.*

Proof. We have seen already that any finite field of p-power order is Galois over $\mathbf{F}_p$. The field $\mathbf{F}_p(\alpha)$ is finite, so it is Galois over $\mathbf{F}_p$ and the roots of $\pi(x)$ can be obtained from α by applying $\mathrm{Gal}(\mathbf{F}_p(\alpha)/\mathbf{F}_p)$ to this root. Since the Galois group is generated by the p-th power map, the roots of $\pi(x)$ are $\alpha, \alpha^p, \alpha^{p^2}, \ldots$. Once we reach α^{p^d} we have cycled back to the start: $\alpha^{p^d} = \alpha$ since $\mathbf{F}_p(\alpha) \cong \mathbf{F}_p[x]/(\pi(x))$ has order p^d. The polynomial $\pi(x)$ is separable because its roots lie in a Galois extension $\mathbf{F}_p(\alpha)$ of $\mathbf{F}_p$. Since its degree is d, its different roots must be $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$. □

Example 3.3. The polynomial $T^3 + T^2 + 1$ is irreducible in $\mathbf{F}_2[T]$. In the field $F = \mathbf{F}_2[x]/(x^3 + x^2 + 1)$, one root of $T^3 + T^2 + 1$ is x. The other two roots are x^2 and x^4.

Since $x^3 + x^2 + 1 = 0$ in F, we get $x^3 = x^2 + 1$ (since $-1 = 1$), so $x^4 = x^3 + x = (x^2 + 1) + x = x^2 + x + 1$. Therefore, the roots of $T^3 + T^2 + 1$ in F can be written as x, x^2, and $x^2 + x + 1$.

In F, $x + 1$ is a root of $T^3 + T + 1$. The other two roots of this polynomial are $(x + 1)^2 = x^2 + 1$ and $(x + 1)^4 = (x^2 + 1)^2 = x^4 + 1 = (x^2 + x + 1) + 1 = x^2 + x$.

Example 3.4. In the field $\mathbf{F}_7[x]/(x^3 - 2)$, $x^2 + x + 2$ has minimal polynomial $T^3 + T^2 + 6T + 5$ over $\mathbf{F}_7$. The other roots of this polynomial are $(x^2 + x + 2)^7$ and $(x^2 + x + 2)^{49}$. Using the relation $x^3 = 2$, those powers can be simplified: $(x^2 + x + 2)^7 = 2x^2 + 4x + 2$ and $(x^2 + x + 2)^{49} = 4x^2 + 2x + 2$.

4. General finite base fields

Let's replace the base field $\mathbf{F}_p$ with a general finite field $\mathbf{F}_q$ of size q. The number q is a prime power. Since every $a \in \mathbf{F}_q$ satisfies $a^q = a$, the role of the p-th power map on finite extensions of $\mathbf{F}_p$ is taken over by the q-th power map on finite extensions of $\mathbf{F}_q$. Here are analogues over $\mathbf{F}_q$ of some results over $\mathbf{F}_p$. Proofs are left to the reader.

Theorem 4.1. *For any positive integer n, there is a monic irreducible of degree n in $\mathbf{F}_q[x]$.*

Theorem 4.2. *Between $\mathbf{F}_q$ and $\mathbf{F}_{q^n}$ there is one field of each order q^d where $d|n$. The field of order q^d inside $\mathbf{F}_{q^n}$ can be described as $\{t \in \mathbf{F}_{q^n} : t^{q^d} = t\}$.*

Theorem 4.3. *For any integer $n \geq 1$, $\mathbf{F}_{q^n}/\mathbf{F}_q$ is a Galois extension and the Galois group $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$ is cyclic with generator the q-th power map $\varphi_q \colon t \mapsto t^q$.*

Theorem 4.4. *If $\pi(x) \in \mathbf{F}_q[x]$ is irreducible with degree d and it has a root α in some extension field of $\mathbf{F}_q$ then its full set of roots is $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$.*