AN OVERVIEW OF FINITE FIELDS

Here is a compendium of "everything you need to know about finite fields" purloined from my Simple Groups course lecture notes last semester. I give references (in brackets) to where these facts are proved in Dummit–Foote. I have also included my recap of an introduction to fields; and I'll give a couple of examples too.

Recall that, in general, a *field* is any set F together with two commutative binary operations, always written as addition and multiplication with respective (distinct) identities 0, 1 such that you can do all the usual arithmetic involving $+, -, \times, \div$ in F (including the distributive laws) (Section 1.4.).

If p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field of p elements, and is denoted by $\mathbb{F}_p$.
[Exercise: If $n > 1$ is not a prime, $\mathbb{Z}/n\mathbb{Z}$ cannot be a field because it contains nonzero elements whose product is 0 (called zero divisors)— check this; and show that this never happens in a field.]

For each $n \in \mathbb{Z}^+$ let n denote $1 + 1 + \cdots + 1$ (n times) in F. If no n is zero in F, we say F has *characteristic 0*; and if some n equals 0 in F, it is easy to see n must be a prime, $n = p$, and we then say F has *characteristic* p. (This follows easily from the preceding exercise — see Section 13.1.) The familiar fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have characteristic 0. It is an easy exercise to see that

every finite field F must have characteristic p, for some prime p.

Moreover, every field F contains a unique smallest subfield, F_0, which is the subfield of F generated by 1. It is easy to see that F_0 is either $\mathbb{Q}$ (when F has characteristic 0) or $\mathbb{F}_p$ (when F has characteristic p); we call F_0 the *prime subfield of* F (Section 13.1).

The usual operations in F make F a vector space over any of its subfields K, and we call the dimension of the K-vector space F the *degree of the extension of F over K*, and denote this by $[F : K]$. For example, $[\mathbb{C} : \mathbb{R}] = 2$, and indeed we talk about $\mathbb{C}$ as being the complex plane (i.e., view $\mathbb{C}$ as a 2-dimensional real vector space). If the degree of F over a subfield K is finite, say $[F : K] = n$, then by basic vector space theory (Section 11.1) F is isomorphic as an K-vector space to $K^n = K \times K \times \cdots \times K$ (n-factors). (Note: this isomorphism is not "multiplicative" in the sense that if you multiply the n-tuples componentwise, then the product of copies of K always contains zero divisors when $n \geq 2$.)

When F is a finite field and $K = F_0 = \mathbb{F}_p$, then $[F : F_0]$ must be finite (why?), and so

every finite field is isomorphic as a vector space over $\mathbb{F}_p$ to $\mathbb{F}_p^n$, for some n.

This is the first result in the following Omnibus Theorem on Finite Fields. The results and proofs are the same, mutatis mutantis, for any finite field, not just $\mathbb{F}_p$, so we state them in generality. References to proofs are given; but most of these can be established by elementary means, independent of the "overhead" in the book.

Date: April 3, 2019.

Theorem 0.1. *Let F be any finite field.*

(1) F has characteristic p for some prime p, and $|\,F\,| = p^n$ for some $n \in \mathbb{Z}^+$, where $n = [F : \mathbb{F}_p]$.

(2) For each prime p and positive integer n there is a unique (up to isomorphism) field of order p^n. (This field is denoted as $\mathbb{F}_{p^n}$.) Henceforth let $q = p^n$. Consequently, for every positive integer m there is a field $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$ of dimension (degree) m over $\mathbb{F}_q$.

(3) $\mathbb{F}_q$ is the set of all roots of the polynomial $X^q - X$ in some algebraic closure of $\mathbb{F}_p$. In particular, $a^q = a$ for all $a \in \mathbb{F}_q$.

(4) As an additive *group, $\mathbb{F}_q$ is elementary abelian, so $\mathbb{F}_q \cong E_{p^n}$.*

(5) As a multiplicative*, the group, $\mathbb{F}_q^\times$, of all nonzero elements of $\mathbb{F}_q$ is cyclic, i.e., $\mathbb{F}_q^\times \cong Z_{q-1}$.*

(6) We have the following containments of fields: $\mathbb{F}_{q^b}$ is (isomorphic to) a subfield of $\mathbb{F}_{q^a}$ if and only if $b \bigm| a$.

(7) For any positive integer m, the lattice of all subfields of $\mathbb{F}_{q^m}$ that contain $\mathbb{F}_q$ is the same as the lattice of subgroups of the cyclic group Z_m (one subgroup for each divisor of m, with $\langle\, a\,\rangle \le \langle\, b\,\rangle \iff b \bigm| a$). In particular, this describes the lattice of all subfields of $\mathbb{F}_{p^n}$.

(8) The group of all field automorphisms of $\mathbb{F}_{q^m}$ that act as the identity on $\mathbb{F}_q$ is a cyclic group of order m with generator σ, where $\sigma(a) = a^q$ for every $a \in \mathbb{F}_{q^m}$. (This group is called the Galois group *of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and σ is called the* Frobenius automorphism.*)*

(9) Every nonzero element of a finite field is a root of unity. Let $k \in \mathbb{Z}^+$ and write $k = p^\alpha m$ where $(p, m) = 1$. Then $X^k - 1 = (X^m - 1)^{p^\alpha}$ in the polynomial ring $\mathbb{F}_q[X]$. The k^{th} roots of unity (in some algebraic closure) are therefore the same as the m^{th} roots of 1; and 1 is the only p-power root of 1. The smallest field containing $\mathbb{F}_q$ and all k^{th} roots of unity is $\mathbb{F}_{q^t}$ where t is the smallest positive integer such that $m \bigm| (q^t - 1)$, i.e., t is the multiplicative order of q in $(\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. (1) Section 13.1; (2) Section 13.5; (3) is a generalization of Fermat's Little Theorem (use Lagrange); (4) is an exercise; (5) Section 9.5; (6), (7) and (9) are exercises in Section 13.5; (8) Section 14.3. □

Examples

We can explicitly construct the (unique) finite field of order $q = p^n$ by finding an *irreducible* polynomial $f(x)$ in $\mathbb{F}_p[x]$ of degree n (one that does not factor), and then forming the quotient ring $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n}$. The irreducibility of $f(x)$ is essential to ensuring that this quotient ring is a field (has no zero divisors), for the same reasons that $\mathbb{Z}/N\mathbb{Z}$ is a field if and only if N is a prime number. There may be different irreducible polynomials of degree n, but all resulting quotient rings are isomorphic (although a specific isomorphism may not be evident).

Note that although $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, for $n \ge 2$ it is *not* true that $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ — the latter ring is never a field (it has zero divisors). So do not say "mod q" when working in $\mathbb{F}_q$ in general!

For example, $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ because it has no linear factors: it has no roots in $\mathbb{F}_2$ by simply plugging in 0 and 1 to see this! Thus $\mathbb{F}_2[x]/(x^2 + x + 1)$ is the field $\mathbb{F}_4$ of four elements. Let α be the coset of x in this quotient ring. Just like in $\mathbb{Z}/N\mathbb{Z}$ every element in this field has a "least residue" of the form $a + b\alpha$, where $a, b \in \mathbb{F}_2$. Addition is componentwise: add like powers of α and reduce mod 2. Multiplication of polynomials in α is as usual for polynomial (distributive law) multiplication of polynomials, followed by the "reduction rule" that $\alpha^2 = \alpha + 1$ (because $\alpha^2 + \alpha + 1 = 0$ in the quotient ring).

When $p = 3$ we can similarly construct the field of order 9 as $\mathbb{F}_3[x]/(x^2+1) = \mathbb{F}_9$. Again x^2+1 is irreducible because it has no linear factors (no roots) in $\mathbb{F}_3[x]$. With α again denoting the coset of x in the quotient, we see that the elements of $\mathbb{F}_9$ can all be (uniquely) written as $a + b\alpha$ where now the "reduction rule" for multiplication is $\alpha^2 = -1$. Thus $\mathbb{F}_9$ is analogous to constructing the complex numbers, starting from the base field of real numbers!

If one tried to mimic the same "complex numbers" construction starting instead from $\mathbb{F}_5$ one would see that $\mathbb{F}_5[x]/(x^2+1)$ is not a field: it has zero divisors! This is because $x^2+1 = (x+2)(x-2)$ in $\mathbb{F}_5[x]$, that is, $\mathbb{F}_5$ already contains all fourth roots of unity (note: $4 \bigm| (5-1)$).

The general construction and arithmetic of field extensions (using the Euclidean Algorithm to find inverses) is described in Section 13.1 of Dummit–Foote, with many more explicit examples.