

# Need to Knows about Finite Fields

The purpose of this document is to give a thorough outline of the theory of finite fields as discussed in class. There are two sides to the study of finite fields. First, we take an abstract approach and show that IF finite fields exist, then there is a unique finite field of  $p^n$  elements for any prime  $p$ , and any  $n \geq 1$  and these exhaust the list of possible finite fields. Second, we take the concrete approach to construct these finite fields as elements living in the ring of polynomials  $\mathbb{F}_p[x]$  with coefficients in  $\mathbb{F}_p$ . We will show that the finite fields are polynomials in this ring modulo irreducible polynomials in  $\mathbb{F}_p[x]$ .

## 1. MAIN RESULTS

Most everything important about finite fields can be piled into a single theorem with several parts. We stated this in class, but let me restate it again.

**Theorem 1.** *Let  $p$  be a prime and  $q = p^n$  for  $n \geq 1$ .*

- (1) *There exists a field  $\mathbb{F}_q$  of size  $q$ .*
- (2) *Any two fields of size  $q$  are isomorphic (that is, they have the same structure).*
- (3)  *$\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$  is cyclic.*
- (4) *Elements of  $\mathbb{F}_q$  are distinct roots of  $x^q - x$ .*
- (5) *The irreducible factors of  $x^q - x$  in  $\mathbb{F}_p[x]$  are ALL the monic irreducible polynomials of degree  $d$  dividing  $n$ .*
- (6)  *$\mathbb{F}_{q'} \subset \mathbb{F}_q$  if and only if  $q' = p^k$  where  $k$  divides  $n$ .*

We won't prove all parts of the theorem in this document. But let me suggest where some come from. First, we've implicitly assumed that  $\mathbb{F}_q$  has prime power order. This comes from investigations about the characteristic and the fact that  $\mathbb{F}_q$  can be thought of as a finite dimensional vector space over  $\mathbb{F}_p$  (see Section 3 for these facts). Part 1 we now demonstrate by explicitly constructing such a field. This is the most important single component of the above theorem.

For (1), We consider the set of elements in  $\mathbb{F}_p[x]/(f(x))$  for some monic, irreducible polynomial  $f(x) \in \mathbb{F}_p[x]$ . This notation means that we consider all polynomials in  $\mathbb{F}_p[x]$  mod the irreducible polynomial  $f(x)$ . Since  $\mathbb{F}_p$  is a field, we can do division here. Why does this produce a field? One can see that if  $f(x)$  has degree  $n$ , then there are exactly  $p^n$  polynomials which are inequivalent mod  $f(x)$  (these are all the polynomials in  $\mathbb{F}_p[x]$  with degree less than  $n$ ). Then one can check that these satisfy the field axioms given in the next section. That is, elements can be added and multiplied and remain in the set  $\mathbb{F}_p[x]/(f(x))$  and have additive and multiplicative inverses, etc.

Part (2) is a more detailed algebraic consideration than we want to get into. But it is interesting that a finite field of any size is unique in this sense. So in particular, if we choose

a different irreducible polynomial for our  $f(x)$ , then the resulting structure of the field is the same. The representatives of the field are still the same polynomials of degree less than  $n$  but they may play different roles in the two different fields.

Part (3) is a generalization of the primitive element theorem in  $\mathbb{Z}/p\mathbb{Z}$ . The proof follows in very similar fashion.

Part (4) is a generalization of Fermat's little theorem. It uses Lagrange's theorem in the general case for  $q = p^n$  with  $n > 1$ . For  $n = 1$ , it is Fermat's little theorem.

## 2. DEFINITIONS AND EXAMPLES

**Definition 1.** A **FIELD** is a set  $F$  which is *CLOSED* under two operations  $+$  and  $\times$  (that is, for any  $a, b \in F$ , both  $a + b$  and  $a \times b \in F$ ) and satisfies the following properties:

- (1)  $F$  is a (commutative ( $a + b = b + a$ )) group under  $+$ .
- (2)  $F^\times = F - \{0\}$  is a (commutative ( $a \times b = b \times a$ )) group under multiplication.
- (3) Natural distributive laws hold:

$$a \times (b + c) = a \times b + a \times c, \quad \text{for every } a, b, c \in F$$

### Examples:

- (1)  $\mathbb{Z}/p\mathbb{Z}$ , our notation for the integers mod  $p$  under the usual addition and multiplication mod  $p$ .
- (2)  $\mathbb{R}$ , the real numbers, are also a field under addition and multiplication of real numbers. Note in particular that every non-zero real number  $x$  has a multiplicative inverse, namely  $1/x$ , so  $\mathbb{R}^\times$  is a group under multiplication.
- (3) For similar reasons to the above example,  $\mathbb{Q}$  and  $\mathbb{C}$ , the rational numbers and complex numbers, respectively, are fields.

### NON-Examples:

- (1)  $\mathbb{Z}/n\mathbb{Z}$ , the integers mod  $n$ , for a composite number  $n$  is not a field. Any divisor  $d$  of  $n$  does not have a multiplicative inverse since the  $\gcd(d, n) > 1$ . Hence  $(\mathbb{Z}/n\mathbb{Z}) - \{0\}$  is not a group under multiplication. (Of course, we can make a group called  $(\mathbb{Z}/n\mathbb{Z})^\times$  but we have to exclude many more elements than just 0, so  $\mathbb{Z}/n\mathbb{Z}$  is not a field.
- (2)  $\mathbb{Z}$ , the integers, are not a field. There is no multiplicative inverse for any elements other than  $\pm 1$ . That is, there is no element  $y$  for which  $2y = 1$  in the integers.

## 3. ABSTRACT RESULTS ABOUT FINITE FIELDS

Let  $G$  be a finite group of  $k$  elements. Lagrange's theorem tells us that under the operation  $*$ ,

$$\underbrace{a * a * \cdots * a}_{k \text{ times}} = e, \quad \text{for any } a \in G, \text{ where } e \text{ is the identity in } G.$$

A field  $F$  is a group under addition with additive identity called 0. If  $F$  is a finite field of  $k$  elements, this means that for any  $a \in F$ ,

$$\underbrace{a + a + \cdots + a}_{k \text{ times}} = 0$$

so there is always an integer  $N$  for which any element of the field added to itself  $N$  times is 0. Let the smallest such integer be called the “characteristic of  $F$ ”, denoted  $\text{char}(F)$ . Clearly if  $F$  has  $k$  elements, the above shows that  $\text{char}(F) < k$ .

**Proposition 1.** *Given a finite field  $F$ , the characteristic,  $\text{char}(F)$ , is always a prime number  $p$ .*

*Proof.* The characteristic exists by the above arguments. Suppose the characteristic was  $N = mk$  for some composite  $N$ . Then since  $N$  is the characteristic,

$$\underbrace{1 + 1 + \cdots + 1}_{N \text{ times}} = 0$$

But  $N = mk$ , so using the distributive axiom, we may rewrite the above as

$$\left( \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} \right) \times \left( \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} \right) = 0$$

We claim that this implies at least one of the above sums is 0. If both are 0, then done. If not, then take one of the non-zero sums (say the sum of  $m$  1’s, without loss of generality). It is an element of the field, by closure of addition, so it has a multiplicative inverse. And multiplying by the inverse on both sides of the above equality leaves

$$\left( \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} \right) = 0$$

so one sum is always 0. But then for any  $a \in F$ ,

$$\underbrace{a + a + \cdots + a}_{k \text{ times}} = \underbrace{a \times 1 + a \times 1 + \cdots + a \times 1}_{k \text{ times}} = a \times \left( \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} \right) = a \times 0 = 0$$

contradicting the fact that  $N$  was the characteristic. Hence  $N$  can’t be composite. (Note that we were very careful in this proof not to use anything but the axioms for the field using 0 and 1 only as additive and multiplicative identities. You could call  $1 + 1 = 2$  in the field, but you shouldn’t assume this 2 behaves like 2 in the integers without explaining why using the axioms.)  $\square$

**Proposition 2.** *If the characteristic of  $F$  is the prime  $p$ , then  $F$  contains a copy of the finite field  $\mathbb{F}_p$  (a set of  $p$  elements that behaves like  $\mathbb{Z}/p\mathbb{Z}$ ).*

*Proof.* We know that every field contains an additive identity (call it 0) and multiplicative identity (call it 1). Since the characteristic of  $F$  is  $p$ , then we could form the set of  $p$  elements

$$\left\{ 0, 1, 1 + 1, 1 + 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{p-1 \text{ times}} \right\}$$

and the sums of 1's will all be non-zero. It remains to check that these behave like  $\mathbb{F}_p$ .

(In group theory speak, we would say that we require an isomorphism between the two sets, but we haven't discussed these in class. What you can check is that adding and multiplying any two of these elements produces a result which remains in the set, since the characteristic is  $p$ , so sums of more than  $p$  1's reduce to smaller sums. Then check inverses, etc. We leave this to the interested reader.)  $\square$

To be added:

vector spaces as field extensions.

elements of the field correspond to roots of polynomial  $x^q - x$ .