Finite Fields

Basic Definitions

A ***group*** is a set G with a binary operation • (i.e., a function from G×G into G) such that:

1) The operation is *associative*, $a\bullet(b\bullet c) = (a\bullet b)\bullet c \quad \forall\ a,b,c \in G$.
2) There exists an *identity element* e, $a\bullet e = e\bullet a = a \quad \forall\ a \in G$.
3) Each element a has an *inverse element* a^{-1}; $a\bullet a^{-1} = a^{-1}\bullet a = e$.

A group (G,•) is ***commutative*** (abelian) if $a\bullet b = b\bullet a \quad \forall\ a,b \in G$.

Examples: $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}-\{0\}, \times)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_p-\{0\},\times)$

All these examples are abelian groups.

Basic Definitions

A ***field*** is a set F with two binary operations + and $\times$ such that:

1) (F, +) is a commutative group with identity element 0.
2) (F-{0},$\times$) is a commutative group with identity element 1.
3) The distributive law $a(b+c) = ab + ac$ holds $\forall$ $a,b,c \in F$.

Examples: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$ for p a prime are fields with the usual operations of addition and multiplication.

A ***subfield*** of a field F is a subset of F which is itself a field with the same operations as F.

Examples: $\mathbb{Q}$ is a subfield of $\mathbb{R}$. $\mathbb{R}$ is a subfield of $\mathbb{C}$. $\mathbb{Z}_p$ has no subfields (other than itself).

Characteristic of a Field

Since 1 is in any field and addition is a closed operation (the sum of any two elements is another element of the field) we have that; 1, 1+1, 1+1+1, 1+1+1+1, 1+1+1+1+1, etc. are all elements of the field. Two possibilities exist for this sequence of elements – either some sum of 1's will equal 0 (in which case the sequence cycles through some finite set of values) or not (in which case none of the elements of the sequence are the same and we get an infinite number of elements in the field).

The smallest positive number of 1's whose sum is 0 is called the ***characteristic*** of the field. If no number of 1's sum to 0, we say that the field has ***characteristic zero***.

Prime Subfield

It can be shown (not difficult) that the characteristic of a field is either 0 or a prime number.

If the characteristic of a field is p, then the elements which can be written as sums of 1's form a $\mathbb{Z}_p$ inside the field, i.e., a subfield. This subfield is the smallest subfield that the field can contain.

If the characteristic of the field is 0, then these elements form a copy of the natural numbers inside the field. This set of elements together with their additive and multiplicative inverses create a copy of $\mathbb{Q}$, the rational numbers, inside the field. Again, this must be the smallest subfield contained in the field.

The smallest subfield of a field is called the ***prime subfield*** and it is either a $\mathbb{Z}_p$ or $\mathbb{Q}$.

Extension Fields

If K is a subfield of a field L, then we say that L is an ***extension*** (or extension field) of K. Every field is thus an extension of its prime subfield.

A field may always be viewed as a vector space over any of its subfields. (The field elements are the vectors and the subfield elements are the scalars). If this vector space is finite dimensional, the dimension of the vector space is called the ***degree*** of the field over its subfield. A finite field *must* be a finite dimensional vector space, so all finite fields have degrees.

The number of elements in a finite field is the ***order*** of that field.

The order of a finite field

A finite field, since it cannot contain $\mathbb{Q}$, must have a prime subfield of the form **GF**(p) for some prime p, also:

Theorem - *Any finite field with characteristic p has p^n elements for some positive integer n. (The order of the field is p^n.)*

Proof: Let L be the finite field and K the prime subfield of L. The vector space of L over K is of some finite dimension, say n, and there exists a basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ of L over K. Since every element of L can be expressed uniquely as a linear combination of the α_i over K, i.e., every $a \in L$ can be written as, $a = \sum \beta_i \alpha_i$, with β_i in K, and since K has p elements, L must have p^n elements. ❑

Splitting Fields

The previous result does not prove the existence of finite fields of these sizes. To prove existence we need to talk about polynomials.

Given a polynomial with coefficients in a field K, the smallest extension of K in which the polynomial can be completely factored into linear factors is called a ***splitting field*** for the polynomial.

Ex: The polynomial $x^2 + 1$ does not factor over $\mathbb{R}$, but over the extension $\mathbb{C}$ of the reals, it does, i.e., $x^2 + 1 = (x + i)(x - i)$. Thus, $\mathbb{C}$ is a splitting field for $x^2 + 1$.

Theorem: If f(x) is an irreducible polynomial with coefficients in the field K, then a splitting field for f(x) exists and any two such are isomorphic.

Finite Fields

Theorem: The splitting field of $f(x) = x^{p^n} - x$ thought of as a polynomial over GF(p) has p^n elements, and is denoted $GF(p^n)$.

Corollary: For each prime p and positive integer n, the field $GF(p^n)$ exists and is unique (two fields of the same order are isomorphic).

By definition, the non-zero elements of a field form a group under multiplication. In particular, $GF(p^n) - \{0\} = GF(p^n)^*$ is a cyclic group under multiplication (all the elements of the group can be represented as powers of a single element, called a ***generator***), and the generators of this group are called ***primitive elements*** of the field.

Constructing Finite Fields

There are several ways to represent the elements of a finite field. The text describes a representation using polynomials. This method is a bit cumbersome for doing calculations. We will give other representations that are more computationally friendly.

Using the fact that a field is a vector space over its prime subfield it is easy to write all the elements as vectors.

Example: GF(4) is a 2-dimensional vector space over GF(2), so its four elements can be written as (0,0), (0,1), (1,0) and (1,1). Adding these elements is done componentwise (in GF(2)). Multiplication however is more complicated and involves a strange rule ... so this is not a great way to represent the field.

Constructing Finite Fields

Another idea that can be used as a basis for a representation is the fact that the non-zero elements of a finite field can all be written as powers of a primitive element.

Example: Let ω be a primitive element of GF(4). The elements of GF(4) are then 0, ω, ω^2, ω^3. Multiplication is easily done in this representation (just add exponents mod 3), but addition is not obvious.

If we can link these two representations together, we will easily be able to do both addition and multiplication.

Example: In GF(4) we have:

$$
\begin{aligned}
0 &\leftrightarrow (0,0) \\
\omega &\leftrightarrow (0,1) \\
\omega^2 = 1 + \omega &\leftrightarrow (1,1) \\
\omega^3 = 1 &\leftrightarrow (1,0)
\end{aligned}
$$

$$a + b\omega \leftrightarrow (a,b)$$

Constructing Finite Fields

The task is thus to locate a primitive element and set up this table of correspondences.

In $GF(p^n)$ with $n > 1$, a primitive element can not be in the prime subfield. Thus, we must seek them amongst the roots of irreducible polynomials over GF(p). In particular, they will be found as roots of irreducible polynomials of degree n, in fact, roots of primitive polynomials of degree n.

While we could determine whether or not an irreducible polynomial is primitive, it is often easier just to look at the roots of irreducible polynomials and see if they are generators. Also, we need only examine ***monic*** (leading coefficient is 1) polynomials since multiplying a polynomial by a non-zero scalar does not change its roots.

Finding Irreducible Polynomials

An irreducible monic polynomial is one which can not be factored. Irreducibility is dependent on the field over which the polynomial is defined, so general procedures for obtaining them are difficult to come by. In small cases (when either the degree or the field is small) there are several ideas which can be used to locate them.

Example: Irreducible quadratics over GF(3).
For this small field we can actually list all the monic polynomials.
x^2, $x^2 + 1$, $x^2 + 2$, $x^2 + x$, $x^2 + x + 1$, $x^2 + x + 2$, $x^2 + 2x$, $x^2 + 2x + 1$, $x^2 + 2x + 2$.
We can find the irreducible ones by eliminating all the reducible polynomials from this list. A sufficient (but not necessary) condition for reducibility is having a root, since this corresponds to a linear factor.

Finding Irreducible Polynomials

Example: Irreducible quadratics over GF(3).

~~x^2~~

$x^2 + 1$

~~$x^2 + 2$~~

~~$x^2 + x$~~

~~$x^2 + x + 1$~~

$x^2 + x + 2$

~~$x^2 + 2x$~~

~~$x^2 + 2x + 1$~~

$x^2 + 2x + 2$

If 0 is a root, there is no constant term, so these are easily recognized.

Now plug in 1. If we obtain a multiple of 3, then 1 will be a root.

Similarly, plug in 2.

Whatever remains on the list is irreducible in this case.

Finding Irreducible Polynomials

Example: Irreducible quadratics over GF(3).

~~x^2~~

$x^2 + 1$

~~$x^2 + 2$~~

~~$x^2 + x$~~

~~$x^2 + x + 1$~~

$x^2 + x + 2$

~~$x^2 + 2x$~~

~~$x^2 + 2x + 1$~~

$x^2 + 2x + 2$

Alternatively, we can take the product of all linear factors to find the reducible quadratics.

$(x + 1)(x + 1) = x^2 + 2x + 1$

$(x + 1)(x + 2) = x^2 + 2$

$(x + 2)(x + 2) = x^2 + x + 1$

and remove them from the list.

Constructing GF(9)

Since $9 = 3^2$, we consider monic irreducible polynomials of degree 2 over GF(3) : $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$.

For example, letting α be a root of $x^2 + 1$, i.e., $\alpha^2 + 1 = 0$, so $\alpha^2 = 2$, we can write out the powers of α.

$$\alpha^1 = \alpha,$$
$$\alpha^2 = 2,$$
$$\alpha^3 = 2\alpha,$$
$$\alpha^4 = 2\alpha(\alpha) = 2\alpha^2 = 2(2) = 1$$

and so α has order 4 and does not generate the cyclic group of order 8, i.e., α is **not** a primitive element.

Constructing GF(9)

On the other hand, consider λ a root of the polynomial $x^2 + x + 2$, so that $\lambda^2 + \lambda + 2 = 0$ or $\lambda^2 = 2\lambda + 1$. Now the powers of λ give us:

$$\lambda^1 = \lambda$$
$$\lambda^2 = \mathbf{2\lambda + 1}$$
$$\lambda^3 = \lambda(2\lambda + 1) = 2\lambda^2 + \lambda = 2(2\lambda + 1) + \lambda = \mathbf{2\lambda + 2}$$
$$\lambda^4 = 2\lambda^2 + 2\lambda = \lambda + 2 + 2\lambda = \mathbf{2}$$
$$\lambda^5 = \mathbf{2\lambda}$$
$$\lambda^6 = 2\lambda^2 = \mathbf{\lambda + 2}$$
$$\lambda^7 = \lambda^2 + 2\lambda = 2\lambda + 1 + 2\lambda = \mathbf{\lambda + 1}$$
$$\lambda^8 = \lambda^2 + \lambda = 2\lambda + 1 + \lambda = \mathbf{1}$$

So λ is a primitive element and we have represented the elements of **GF**(9) as the 8 powers of λ together with 0. Notice also that the bolded terms on the right are all the possible terms that can be written as linear combinations of the basis $\{1,\lambda\}$ over **GF**(3).

Constructing GF(8)

Since $8 = 2^3$, the prime field is **GF**(2) and we need a monic irreducible cubic polynomial over that field. These are just $x^3 + x + 1$ and $x^3 + x^2 + 1$. Now the multiplicative group of this field is a cyclic group of order 7 and so every nonidentity element is a generator. Letting λ be a root of the first polynomial, we have $\lambda^3 + \lambda + 1 = 0$, or $\lambda^3 = \lambda + 1$, so the powers of λ are:

$$\lambda^1 = \lambda$$
$$\lambda^2 = \lambda^2$$
$$\lambda^3 = \lambda + 1$$
$$\lambda^4 = \lambda^2 + \lambda$$
$$\lambda^5 = \lambda^2 + \lambda + 1$$
$$\lambda^6 = \lambda^2 + 1$$
$$\lambda^7 = 1$$

Constructing GF(8)

Now suppose we had chosen a root of the second polynomial, say , α. We would then have $\alpha^3 = \alpha^2 + 1$ and the representation would be given by

$$\alpha^1 = \alpha$$
$$\alpha^2 = \alpha^2$$
$$\alpha^3 = \alpha^2 + 1$$
$$\alpha^4 = \alpha^2 + \alpha + 1$$
$$\alpha^5 = \alpha + 1$$
$$\alpha^6 = \alpha^2 + \alpha$$
$$\alpha^7 = 1$$

We know that these two representations must be isomorphic, show that the isomorphism is induced by $\lambda \rightarrow \alpha^6$.

Subfields

Recall that a subfield of a field is a field constructed from a subset of the original elements of the larger field. If the larger field is $GF(p^e)$, then any subfield must also have characteristic p since it will contain the 1 of the larger field. We can say more about what subfields exist in the finite field context. We first state two lemmas.

Lemma 1: $GF(p^s) \subseteq GF(p^r)$ iff $x^{p^s-1} - 1$ divides $x^{p^r-1} - 1$.

Pf: Every element of $GF(p^t)$ satisfies the equation $x^{p^t} = x$ since this is the splitting field of $x^{p^t} - x$. The non-zero elements therefore all satisfy $x^{p^t-1} = 1$. The polynomial $x^{p^t-1} - 1$ has no factors other than the linear ones corresponding to the elements of $GF(p^t)$. The lemma now follows immediately. ❑

Subfields

Lemma 2: If x is a variable or an integer, $x^m - 1$ divides $x^n - 1$ iff m divides n.

Pf: By the division algorithm,

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + x^{n-3m} + \ldots + x^{n-km}) + (x^{n-km} - 1),$$

where km is the largest multiple of m which is less than or equal to n. $x^m - 1$ divides $x^n - 1$ iff $x^{n-km} - 1 = 0$ iff $n - km = 0$ iff m divides n. ❑

Subfields

Theorem 40: $GF(p^s) \subseteq GF(p^r)$ iff s divides r and an element α in $GF(p^r)$ is in $GF(p^s)$ iff $\alpha^{p^s} = \alpha$.

Pf: By Lemma 1, $GF(p^s) \subseteq GF(p^r)$ iff $x^{p^s-1} - 1$ divides $x^{p^r-1} - 1$, which by Lemma 2 is valid iff p^s-1 divides p^r-1. Another application of Lemma 2 says that this is valid iff s divides r. The second statement holds since the elements of $GF(p^s)$ are precisely the roots of the equation $x^{p^s} = x$. ❑

Subfields

By this theorem we know that, for instance, the field GF(2^6) has subfields isomorphic to GF(2), GF(4) and GF(8), but not GF(16) or GF(32), since only 1, 2 and 3 divide 6.

GF(32) only has the prime subfield GF(2) since 5 is prime, while GF(16) has subfields GF(2) and GF(4).

GF(3^8) has the proper subfields, GF(3), GF(3^2), and GF(3^4).

Automorphisms of Fields

Two fields are said to be ***isomorphic*** if there exists a bijection from one to the other which preserves both binary operations. If E and K are isomorphic fields then there exists a bijection $f: E \to K$ such that

$$f(x + y) = f(x) + f(y) \text{ and}$$
$$f(xy) = f(x)f(y)$$

for all x and y in E. Note that in the above the operations on the left are those of the field E while the operations on the right are those of the field K. The map f is called an ***isomorphism***.

An isomorphism from a field to itself is called an ***automorphism***.

The identity map from a field to itself is an automorphism, sometimes called the ***trivial*** automorphism.

Examples

Field automorphisms may not be very familiar to you since the only automorphism of $\mathbb{R}$ is the identity and the only non-trivial automorphism of $\mathbb{C}$ is conjugation, i.e., $x + \mathbf{i}y \rightarrow x - \mathbf{i}y$. Thus, the following result is interesting:

Theorem 37: If ***F*** is a finite field of characteristic p, then the mapping φ defined by $\varphi(a) = a^p$ is an automorphism of ***F***.
Proof: $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$, so φ preserves multiplication. $\varphi(a + b) = (a + b)^p = a^p + b^p = \varphi(a) + \varphi(b)$ and addition is preserved. The middle step follows from the binomial theorem and the fact that p is a prime, so all the intermediate coefficients have a factor of p and are therefore 0. That φ is a bijection follows from the fact that $\varphi(a) = 0$ implies $a = 0$. ❑

Examples

It is easy to see that the composition of automorphisms of a field is an automorphism of the field. Thus, raising an element to any power of the characteristic is an automorphism of the field. Moreover,

Theorem: All the automorphisms of $GF(p^e)$ form a cyclic group (under composition) of order e, which has $x \rightarrow x^p$ as a generator.

The automorphism $x \rightarrow x^p$ is called the ***Frobenius automorphism***.