Facts about finite fields

David Mandell Freeman

September 28, 2011

Basic definitions. A *field* is a commutative ring in which all nonzero elements are invertible. We write the additive identity as 0 and the multiplicative identity as 1, and we assume that $0 \neq 1$.

If F is a field, we use F^+ to denote the additive group of F, i.e., the set of all elements of F with the addition operation. We use $F^\times$ or F^* to denote the multiplicative group of F, i.e., the set of all nonzero elements of F with the multiplication operation.

A *finite field* is a field with a finite number of elements; the number of elements is the *order* of the field. For every prime p, the ring of integers modulo p is a finite field of order p and is denoted $\mathbb{Z}_p$ or $\mathbb{F}_p$.[1]

Characteristic and cardinality. The *characteristic* of a field is the smallest positive integer k such that

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

If no such k exists then the field is said to have characteristic 0. The characteristic of any field is either 0 or a prime p.[2] Fields of characteristic 0 are necessarily infinite (and contain the rational numbers $\mathbb{Q}$); fields of prime characteristic may be finite or infinite.

If F is a finite field of characteristic p, then the order of F is a prime power $q = p^r$ for some positive integer r, and we write $F = \mathbb{F}_{p^r}$ or $F = \mathbb{F}_q$. (We will see below how to construct finite fields of non-prime order.) If F and F' are two fields of order q, then F and F' are isomorphic (i.e., there is a bijective ring homomorphism $\phi \colon F \to F'$). Thus we can talk about *the* finite field $\mathbb{F}_q$.

Polynomials. If F is any field, then $F[x]$ denotes the ring of polynomials in the variable x with coefficients in F, i.e., expressions of the form $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ with the $a_i \in F$. The integer d is the *degree* of f. A polynomial f of degree d is *monic* if $a_d = 1$. A polynomial $f(x)$ of degree d is *irreducible* if there is no way to write $f(x) = g(x)h(x)$ with $\deg g < \deg f$ and $\deg h < \deg f$. Any polynomial $f \in F[x]$ can be written uniquely as a product of a scalar $a \in F$ and monic irreducible polynomials $f_1, \ldots, f_\ell \in F[x]$. (In this sense, irreducible polynomials play the role in $F[x]$ that prime numbers do in the integers.)

[1] Proof: it is clear that $\mathbb{F}_p$ is a commutative ring, so we just have to show that every nonzero element is invertible. To see this, observe that if $\gcd(a, p) = 1$ then there are x, y such that $ax + by = 1$, so $x = a^{-1}$ in $\mathbb{F}_p^*$.

[2] Proof: if F has characteristic $mn > 0$ for integers m and n, then $mn = 0$ in F, so one of m or n is not invertible in F^*, and thus either $m = 0$ or $n = 0$ as elements of F. If $m, n > 1$ this contradicts the minimality property of characteristic.

If $f \in F[x]$ is a polynomial, a *root* of f is an element $\alpha \in F$ with $f(\alpha) = 0$. Any polynomial $f \in F[x]$ of degree d has at most d roots in F. When F is finite, this property, combined with the fundamental theorem of abelian groups, can be used to show the following:

Important fact. The multiplicative group of a finite field is cyclic.[3]

Extension fields. Let F be any field, and let $f(x) \in F[x]$ be an irreducible polynomial of degree d with coefficients in the field F. We can create the *quotient ring* $K = F[x]/(f(x))$, which is defined to be the ring of all polynomials with coefficients in F subject to the relation $f(x) = 0$. Concretely, the ring K can be represented as the set of all polynomials with degree less than d and coefficients in F. Addition is carried out as usual for polynomials. When multiplying two polynomials, the relation $f(x) = 0$ is used to reduce terms of degree d or greater.

As an additive group, K is isomorphic to the vector space F^d. Since $f(x)$ is irreducible, every nonzero element of K is invertible,[4] so K is a field. A field constructed in this way is called an *extension field of F*. The *degree* of K is defined to be the degree d of F.

For example, if $F = \mathbb{Q}$ and $f(x) = x^2 + 1$, then $K = \mathbb{Q}[x]/(x^2 + 1)$ consists of all linear (i.e., degree 1) polynomials $ax + b$ with $a, b \in \mathbb{Q}$. We multiply two such polynomials $ax + b, cx + d$ by computing $(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$ and using the relation $x^2 = -1$ to obtain $(ad + bc)x + (bc - ac)$, which is also a linear polynomial. In the field K the element x is a square root of -1. To denote this property we write $K = \mathbb{Q}(\sqrt{-1})$, which is read as "$\mathbb{Q}$ adjoin the square root of -1."

Back to our general setup. If $F = \mathbb{F}_p$ is the finite field of order p and f has degree d, then $K = \mathbb{F}_p[x]/(f(x))$ is a field of order p^d. By our discussion above, there is a unique finite field of order p^d (up to isomorphism), so we can say that K *is* the field $\mathbb{F}_{p^d}$. However, this representation is not unique; for example, the field $\mathbb{F}_{25}$ can be expressed as all of the following:

$$\begin{aligned}
\mathbb{F}_{25} &= \mathbb{F}_5[x]/(x^2 - 2) = \mathbb{F}_5(\sqrt{2}) \\
\mathbb{F}_{25} &= \mathbb{F}_5[y]/(y^2 - 3) = \mathbb{F}_5(\sqrt{3}) \\
\mathbb{F}_{25} &= \mathbb{F}_5[z]/(z^2 + z + 1)
\end{aligned}$$

Isomorphisms between these fields are given by $y = 2x$ and $z = 3x + 2$.

Theoretically, the representation of a finite field makes no difference; however, when doing computations choosing a good "defining polynomial" $f(x)$ can make a huge difference in running time, especially when using fields of large extension degree.

Field containment and algebraic closure. We can construct extensions as above where the base field is any field $\mathbb{F}_q$, not just a prime field $\mathbb{F}_p$. For example, we have the "tower"

$$\mathbb{F}_7 \quad \subset \quad \mathbb{F}_{49} = \mathbb{F}_7(\sqrt{3}) \quad \subset \quad \mathbb{F}_{7^6} = \mathbb{F}_{49}(\sqrt[3]{2}).$$

In general, we have $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if m divides n.

[3] Proof idea: if F^* has order n but is not cyclic, then there is some $m < n$ such that $a^m = 1$ for all n values of $a \in F^*$, contradicting the fact that the polynomial $x^m - 1$ has at most m roots in F.

[4] Proof: since $f(x)$ is irreducible, every polynomial $a(x)$ that is not a multiple of $f(x)$ is relatively prime to f. Thus there are polynomials $g(x)$ and $h(x)$ with $ag + fh = 1$, so $g \bmod f$ is the inverse of $a \bmod f$.

For a fixed $q = p^d$, the union of the finite fields $\mathbb{F}_{q^r}$ for all positive r is the *algebraic closure* of $\mathbb{F}_q$, and is denoted $\overline{\mathbb{F}}_q$. The field $\overline{\mathbb{F}}_q$ has the property that any polynomial $f \in \mathbb{F}_q[x]$ has $\deg f$ roots in $\overline{\mathbb{F}}_q$.

Frobenius. If $F = \mathbb{F}_q$ is a finite field of characteristic p, then for any x and y in F we have $(x+y)^q = x^q + y^q$ (since the coefficients of all cross terms are divisible by p). It follows that the map $\phi(x) = x^q$ is a ring homomorphism from F to itself. The map ϕ is called the *q-power Frobenius map* or *q-power Frobenius automorphism.*

Recall from above that the multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$. Thus every nonzero element of $\mathbb{F}_q$ satisfies $x^{q-1} = 1$. Multiplying by x to capture 0 as well, we see that *every* element of $\mathbb{F}_q$ satisfies $x^q = x$. Conversely, if $x^q = x$ then x is in $\mathbb{F}_q$. Thus an element $x \in \overline{\mathbb{F}}_q$ is in $\mathbb{F}_q$ if and only if $x^q = x$, i.e., x is fixed by the q-power Frobenius automorphism.

Finite fields in SAGE.

To construct a field of prime order p, use the command `GF(p)`:[5]

```
sage: F = GF(7)
sage: F
Finite Field of size 7
```

Use parentheses to coerce an integer or rational number into a finite field. (Make sure that the characteristic doesn't divide the denominator!)

```
sage: GF(7)(3)^6
1
sage: GF(31)(22/7)
12
```

There are several ways to construct fields of non-prime order. The simplest is to use the `GF` constructor directly:

```
sage: K.<a> = GF(25)
sage: K
Finite Field in a of size 5^2
```

Note that you must name the variable that you adjoin to the base field, but if you use this construction you have no control over the relation that the variable satisfies. You can use the `charpoly` command to find the relation:

```
sage: a.charpoly()
x^2 + 4*x + 2
sage: a^2 + 4*a + 2
0
sage: K.random_element()
3*a + 1
```

[5] GF stands for "Galois field."

To specify the relation, use the modulus argument when calling GF. You first have to define a polynomial ring that will contain the defining polynomial.

```
sage: R.<x> = GF(2)[]                        # polynomial ring in x over GF(2)
sage: K.<z> = GF(2^5, modulus=x^5+x^3+1)  # finite field of size 32
sage: z^31
1
```

For more information, look at the help text for the GF() and F.extension() commands (where F is a finite field).