finite field

Canonical name	FiniteField
Date of creation	2013-03-22 12:37:50
Last modified on	2013-03-22 12:37:50
Owner	yark (2760)
Last modified by	yark (2760)
Numerical id	16
Author	yark (2760)
Entry type	Definition
Classification	msc 12E20
Classification	msc 11T99
Synonym	Galois field
Related topic	AlgebraicClosureOfAFiniteField
Related topic	IrreduciblePolynomialsOverFiniteField

A *finite field* (also called a *Galois field*) is a field that has finitely many elements. The number of elements in a finite field is sometimes called the *order* of the field. We will present some basic facts about finite fields.

1 Size of a finite field

Theorem 1.1. *A finite field F has positive characteristic $p > 0$ for some prime p. The cardinality of F is p^n where $n := [F : \mathbb{F}_p]$ and $\mathbb{F}_p$ denotes the prime subfield of F.*

Proof. The characteristic of F is positive because otherwise the additive subgroup generated by 1 would be an infinite subset of F. Accordingly, the prime subfield $\mathbb{F}_p$ of F is isomorphic to the field $\mathbb{Z}/p\mathbb{Z}$ of integers mod p. The integer p is prime since otherwise $\mathbb{Z}/p\mathbb{Z}$ would have zero divisors. Since the field F is an n–dimensional vector space over $\mathbb{F}_p$ for some finite n, it is set–isomorphic to $\mathbb{F}_p^n$ and thus has cardinality p^n. $\square$

2 Existence of finite fields

Now that we know every finite field has p^n elements, it is natural to ask which of these actually arise as cardinalities of finite fields. It turns out that for each prime p and each natural number n, there is essentially exactly one finite field of size p^n.

Lemma 2.1. *In any field F with m elements, the equation $x^m = x$ is satisfied by all elements x of F.*

Proof. The result is clearly true if $x = 0$. We may therefore assume x is not zero. By definition of field, the set $F^\times$ of nonzero elements of F forms a group under multiplication. This set has $m - 1$ elements, and by Lagrange's theorem $x^{m-1} = 1$ for any $x \in F^\times$, so $x^m = x$ follows. $\square$

Theorem 2.2. *For each prime $p > 0$ and each natural number $n \in \mathbb{N}$, there exists a finite field of cardinality p^n, and any two such are isomorphic.*

Proof. For $n = 1$, the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ has p elements, and any two such are isomorphic by the map sending 1 to 1.

In general, the polynomial $f(X) := X^{p^n} - X \in \mathbb{F}_p[X]$ has derivative -1 and thus is separable over $\mathbb{F}_p$. We claim that the splitting field F of this polynomial is a finite field of size p^n. The field F certainly contains the set S of roots of $f(X)$. However, the set S is closed under the field operations, so S is itself a field. Since splitting fields are minimal by definition, the containment $S \subset F$ means that $S = F$. Finally, S has p^n elements since $f(X)$ is separable, so F is a field of size p^n.

For the uniqueness part, any other field F' of size p^n contains a subfield isomorphic to $\mathbb{F}_p$. Moreover, F' equals the splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$, since by Lemma **??** every element of F' is a root of this polynomial, and all p^n possible roots of the polynomial are accounted for in this way. By the uniqueness of splitting fields up to isomorphism, the two fields F and F' are isomorphic. □

Note: The proof of Theorem **??** given here, while standard because of its efficiency, relies on more abstract algebra than is strictly necessary. The reader may find a more concrete presentation of this and many other results about finite fields in [**?**, Ch. 7].

Corollary 2.3. *Every finite field F is a normal extension of its prime subfield $\mathbb{F}_p$.*

Proof. This follows from the fact that field extensions obtained from splitting fields are normal extensions. □

3 Units in a finite field

Henceforth, in light of Theorem **??**, we will write $\mathbb{F}_q$ for the unique (up to isomorphism) finite field of cardinality $q = p^n$. A fundamental step in the investigation of finite fields is the observation that their multiplicative groups are cyclic:

Theorem 3.1. *The multiplicative group $\mathbb{F}_q^*$ consisting of nonzero elements of the finite field $\mathbb{F}_q$ is a cyclic group.*

Proof. We begin with the formula

$$\sum_{d|k} \phi(d) = k, \tag{1}$$

where ϕ denotes the Euler totient function. It is proved as follows. For every divisor d of k, the cyclic group C_k of size k has exactly one cyclic subgroup

C_d of size d. Let G_d be the subset of C_d consisting of elements of C_d which have the maximum possible `http://planetmath.org/OrderGroup`order of d. Since every element of C_k has maximal order in the subgroup of C_k that it generates, we see that the sets G_d partition the set C_k, so that

$$\sum_{d|k} |G_d| = |C_k| = k.$$

The identity (**??**) then follows from the observation that the cyclic subgroup C_d has exactly $\phi(d)$ elements of maximal order d.

We now prove the theorem. Let $k = q - 1$, and for each divisor d of k, let $\psi(d)$ be the number of elements of $\mathbb{F}_q^*$ of order d. We claim that $\psi(d)$ is either zero or $\phi(d)$. Indeed, if it is nonzero, then let $x \in \mathbb{F}_q^*$ be an element of order d, and let G_x be the subgroup of $\mathbb{F}_q^*$ generated by x. Then G_x has size d and every element of G_x is a root of the polynomial $x^d - 1$. But this polynomial cannot have more than d roots in a field, so every root of $x^d - 1$ must be an element of G_x. In particular, every element of order d must be in G_x already, and we see that G_x only has $\phi(d)$ elements of order d.

We have proved that $\psi(d) \leq \phi(d)$ for all $d \mid q-1$. If $\psi(q-1)$ were 0, then we would have

$$\sum_{d|q-1} \psi(d) < \sum_{d|q-1} \phi(d) = q - 1,$$

which is impossible since the first sum must equal $q-1$ (because every element of $\mathbb{F}_q^*$ has order equal to some divisor d of $q-1$). $\square$

A more constructive proof of Theorem **??**, which actually exhibits a generator for the cyclic group, may be found in [**?**, Ch. 16].

Corollary 3.2. *Every extension of finite fields is a primitive extension.*

Proof. By Theorem **??**, the multiplicative group of the extension field is cyclic. Any generator of the multiplicative group of the extension field also algebraically generates the extension field over the base field. $\square$

4 Automorphisms of a finite field

Observe that, since a splitting field for $X^{q^m} - X$ over $\mathbb{F}_p$ contains all the roots of $X^q - X$, it follows that the field $\mathbb{F}_{q^m}$ contains a subfield isomorphic to $\mathbb{F}_q$.

We will show later (Theorem **??**) that this is the only way that extensions of finite fields can arise. For now we will construct the Galois group of the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$, which is normal by Corollary **??**.

Theorem 4.1. *The Galois group of the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is a cyclic group of size m generated by the q^{th} power Frobenius map* Frob_q.

Proof. The fact that Frob_q is an element of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, and that $(\mathrm{Frob}_q)^m = \mathrm{Frob}_{q^m}$ is the identity on $\mathbb{F}_{q^m}$, is obvious. Since the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is normal and of degree m, the group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ must have size m, and we will be done if we can show that $(\mathrm{Frob}_q)^k$, for $k = 0, 1, \ldots, m-1$, are distinct elements of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

It is enough to show that none of $(\mathrm{Frob}_q)^k$, for $k = 1, 2, \ldots, m-1$, is the identity map on $\mathbb{F}_{q^m}$, for then we will have shown that Frob_q is of order exactly equal to m. But, if any such $(\mathrm{Frob}_q)^k$ were the identity map, then the polynomial $X^{q^k} - X$ would have q^m distinct roots in $\mathbb{F}_{q^m}$, which is impossible in a field since $q^k < q^m$. □

We can now use the Galois correspondence between subgroups of the Galois group and intermediate fields of a field extension to immediately classify all the intermediate fields in the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Theorem 4.2. *The field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ contains exactly one intermediate field isomorphic to $\mathbb{F}_{q^d}$, for each divisor d of m, and no others. In particular, the subfields of $\mathbb{F}_{p^n}$ are precisely the fields $\mathbb{F}_{p^d}$ for $d \mid n$.*

Proof. By the fundamental theorem of Galois theory, each intermediate field of $\mathbb{F}_{q^m}/\mathbb{F}_q$ corresponds to a subgroup of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. The latter is a cyclic group of order m, so its subgroups are exactly the cyclic groups generated by $(\mathrm{Frob}_q)^d$, one for each $d \mid m$. The fixed field of $(\mathrm{Frob}_q)^d$ is the set of roots of $X^{q^d} - X$, which forms a subfield of $\mathbb{F}_{q^m}$ isomorphic to $\mathbb{F}_{q^d}$, so the result follows.

The subfields of $\mathbb{F}_{p^n}$ can be obtained by applying the above considerations to the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. □

References

[1] Kenneth Ireland & Michael Rosen, *A Classical Introduction to Modern Number Theory, Second Edition*, Springer–Verlag, 1990 (GTM **84**).

[2] Ian Stewart, *Galois Theory, Second Edition*, Chapman & Hall, 1989.