Finite field

In mathematics, a **finite field** or **Galois field** (so-named in honor of Évariste Galois) is a field that contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules. The most common examples of finite fields are given by the integers mod p when p is a prime number.

The *order* of a finite field is its number of elements, which is either a prime number or a prime power. For every prime number p and every positive integer k there are fields of order p^k, all of which are isomorphic.

Finite fields are fundamental in a number of areas of mathematics and computer science, including number theory, algebraic geometry, Galois theory, finite geometry, cryptography and coding theory.

Contents

Properties

A finite field is a finite set which is a field; this means that multiplication, addition, subtraction and division (excluding division by zero) are defined and satisfy the rules of arithmetic known as the field axioms.

The number of elements of a finite field is called its *order* or, sometimes, its *size*. A finite field of order q exists if and only if q is a prime power p^k (where p is a prime number and k is a positive integer). In a field of order p^k, adding p copies of any element always results in zero; that is, the characteristic of the field is p.

If $q = p^k$, all fields of order q are isomorphic (see § Existence and uniqueness below).[1] Moreover, a field cannot contain two different finite subfields with the same order. One may therefore identify all finite fields with the same order, and they are unambiguously denoted $\mathbb{F}_q$, $\mathbf{F}_q$ or $\mathrm{GF}(q)$, where the letters GF stand for "Galois field".[2]

In a finite field of order q, the polynomial $X^q - X$ has all q elements of the finite field as roots. The non-zero elements of a finite field form a multiplicative group. This group is cyclic, so all non-zero elements can be expressed as powers of a single element called a primitive element of the field. (In general there will be several primitive elements for a given field.)

The simplest examples of finite fields are the fields of prime order: for each prime number p, the prime field of order p, $\mathbb{F}_p$, may be constructed as the integers modulo p, $\mathbf{Z}/p\mathbf{Z}$.

The elements of the prime field of order p may be represented by integers in the range $0, \ldots, p - 1$. The sum, the difference and the product are the remainder of the division by p of the result of the corresponding integer operation. The multiplicative inverse of an element may be computed by using the extended Euclidean algorithm (see Extended Euclidean algorithm § Modular integers).

Let F be a finite field. For any element x in F and any integer n, denote by $n \cdot x$ the sum of n copies of x. The least positive n such that $n \cdot 1 = 0$ is the characteristic p of the field. This allows defining a multiplication $(k, x) \mapsto k \cdot x$ of an element k of $\mathrm{GF}(p)$ by an element x of F by choosing an integer representative for k. This multiplication makes F into a $\mathrm{GF}(p)$-vector space. It follows that the number of elements of F is p^n for some integer n.

The identity

$$(x + y)^p = x^p + y^p$$

(sometimes called the freshman's dream) is true in a field of characteristic p. This follows from the binomial theorem, as each binomial coefficient of the expansion of $(x + y)^p$, except the first and the last, is a multiple of p.

By Fermat's little theorem, if p is a prime number and x is in the field $\mathrm{GF}(p)$ then $x^p = x$. This implies the equality

$$X^p - X = \prod_{a \in \mathrm{GF}(p)} (X - a)$$

for polynomials over $\mathrm{GF}(p)$. More generally, every element in $\mathrm{GF}(p^n)$ satisfies the polynomial equation $x^{p^n} - x = 0$.

Any finite field extension of a finite field is separable and simple. That is, if E is a finite field and F is a subfield of E, then E is obtained from F by adjoining a single element whose minimal polynomial is separable. To use a jargon, finite fields are perfect.

A more general algebraic structure that satisfies all the other axioms of a field, but whose multiplication is not required to be commutative, is called a division ring (or sometimes *skew field*). By Wedderburn's little theorem, any finite division ring is commutative, and hence is a finite field.

Existence and uniqueness

Let $q = p^n$ be a prime power, and F be the splitting field of the polynomial

$$P = X^q - X$$

over the prime field GF(p). This means that F is a finite field of lowest order, in which P has q distinct roots (the formal derivative of P is $P' = -1$, implying that $\gcd(P, P') = 1$, which in general implies that the splitting field is a separable extension of the original). The above identity shows that the sum and the product of two roots of P are roots of P, as well as the multiplicative inverse of a root of P. In other words, the roots of P form a field of order q, which is equal to F by the minimality of the splitting field.

The uniqueness up to isomorphism of splitting fields implies thus that all fields of order q are isomorphic. Also, if a field F has a field of order $q = p^k$ as a subfield, its elements are the q roots of $X^q - X$, and F cannot contain another subfield of order q.

In summary, we have the following classification theorem first proved in 1893 by E. H. Moore:[1]

> *The order of a finite field is a prime power. For every prime power q there are fields of order q, and they are all isomorphic. In these fields, every element satisfies*
>
> $$x^q = x,$$
>
> *and the polynomial $X^q - X$ factors as*
>
> $$X^q - X = \prod_{a \in F} (X - a).$$

It follows that GF(p^n) contains a subfield isomorphic to GF(p^m) if and only if m is a divisor of n; in that case, this subfield is unique. In fact, the polynomial $X^{p^m} - X$ divides $X^{p^n} - X$ if and only if m is a divisor of n.

Explicit construction

Non-prime fields

Given a prime power $q = p^n$ with p prime and $n > 1$, the field $\mathrm{GF}(q)$ may be explicitly constructed in the following way. One first chooses an irreducible polynomial P in $\mathrm{GF}(p)[X]$ of degree n (such an irreducible polynomial always exists). Then the quotient ring

$$\mathrm{GF}(q) = \mathrm{GF}(p)[X]/(P)$$

of the polynomial ring $\mathrm{GF}(p)[X]$ by the ideal generated by P is a field of order q.

More explicitly, the elements of $\mathrm{GF}(q)$ are the polynomials over $\mathrm{GF}(p)$ whose degree is strictly less than n. The addition and the subtraction are those of polynomials over $\mathrm{GF}(p)$. The product of two elements is the remainder of the Euclidean division by P of the product in $\mathrm{GF}(p)[X]$. The multiplicative inverse of a non-zero element may be computed with the extended Euclidean algorithm; see Extended Euclidean algorithm § Simple algebraic field extensions.

Except in the construction of $\mathrm{GF}(4)$, there are several possible choices for P, which produce isomorphic results. To simplify the Euclidean division, one commonly chooses for P a polynomial of the form

$$X^n + aX + b,$$

which make the needed Euclidean divisions very efficient. However, for some fields, typically in characteristic 2, irreducible polynomials of the form $X^n + aX + b$ may not exist. In characteristic 2, if the polynomial $X^n + X + 1$ is reducible, it is recommended to choose $X^n + X^k + 1$ with the lowest possible k that makes the polynomial irreducible. If all these trinomials are reducible, one chooses "pentanomials" $X^n + X^a + X^b + X^c + 1$, as polynomials of degree greater than 1, with an even number of terms, are never irreducible in characteristic 2, having 1 as a root.[3]

A possible choice for such a polynomial is given by Conway polynomials. They ensure a certain compatibility between the representation of a field and the representations of its subfields.

In the next sections, we will show how the general construction method outlined above works for small finite fields.

Field with four elements

The smallest non-prime field is the field with four elements, which is commonly denoted $\mathrm{GF}(4)$ or $\mathbb{F}_4$. It consists of the four elements $0, 1, \alpha, 1 + \alpha$ such that $\alpha^2 = 1 + \alpha$, $1 \cdot \alpha = \alpha \cdot 1 = \alpha$, $x + x = 0$, and $x \cdot 0 = 0 \cdot x = 0$, for every $x \in \mathrm{GF}(4)$, the other operation results being easily deduced from the distributive law. See below for the complete operation tables.

This may be deduced as follows from the results of the preceding section.

Over $\mathrm{GF}(2)$, there is only one irreducible polynomial of degree 2:

$$X^2 + X + 1$$

Therefore, for $\mathrm{GF}(4)$ the construction of the preceding section must involve this polynomial, and

$$\mathrm{GF}(4) = \mathrm{GF}(2)[X]/(X^2 + X + 1).$$

Let α denote a root of this polynomial in GF(4). This implies that

$$\alpha^2 = 1 + \alpha,$$

and that α and $1 + \alpha$ are the elements of GF(4) that are not in GF(2). The tables of the operations in GF(4) result from this, and are as follows:

Addition $x+y$

x \ y	**0**	**1**	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Multiplication $x \cdot y$

x \ y	**0**	**1**	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Division x/y

x \ y	**1**	α	$1+\alpha$
0	0	0	0
1	1	$1+\alpha$	α
α	α	1	$1+\alpha$
$1+\alpha$	$1+\alpha$	α	1

A table for subtraction is not given, because subtraction is identical to addition, as is the case for every field of characteristic 2. In the third table, for the division of x by y, the values of x must be read in the left column, and the values of y in the top row. (Because $0 \cdot z = 0$ for every z in every ring the division by 0 has to remain undefined.)

The map

$$\varphi : x \mapsto x^2$$

is the non-trivial field automorphism, called Frobenius automorphism, which sends α into the second root $1 + \alpha$ of the above mentioned irreducible polynomial $X^2 + X + 1$.

GF(p^2) for an odd prime p

For applying the above general construction of finite fields in the case of GF(p^2), one has to find an irreducible polynomial of degree 2. For $p = 2$, this has been done in the preceding section. If p is an odd prime, there are always irreducible polynomials of the form $X^2 - r$, with r in GF(p).

More precisely, the polynomial $X^2 - r$ is irreducible over GF(p) if and only if r is a quadratic non-residue modulo p (this is almost the definition of a quadratic non-residue). There are $\frac{p-1}{2}$ quadratic non-residues modulo p. For example, 2 is a quadratic non-residue for $p = 3, 5, 11, 13, \ldots$, and 3 is a quadratic non-residue for $p = 5, 7, 17, \ldots$. If $p \equiv 3 \bmod 4$, that is $p = 3, 7, 11, 19, \ldots$, one may choose $-1 \equiv p - 1$ as a quadratic non-residue, which allows us to have a very simple irreducible polynomial $X^2 + 1$.

Having chosen a quadratic non-residue r, let α be a symbolic square root of r, that is a symbol which has the property $\alpha^2 = r$, in the same way as the complex number i is a symbolic square root of -1. Then, the elements of GF(p^2) are all the linear expressions

$$a + b\alpha,$$

with a and b in GF(p). The operations on GF(p^2) are defined as follows (the operations between elements of GF(p) represented by Latin letters are the operations in GF(p)):

$$\begin{aligned} -(a+b\alpha) &= -a+(-b)\alpha \\ (a+b\alpha)+(c+d\alpha) &= (a+c)+(b+d)\alpha \\ (a+b\alpha)(c+d\alpha) &= (ac+rbd)+(ad+bc)\alpha \\ (a+b\alpha)^{-1} &= a(a^2-rb^2)^{-1}+(-b)(a^2-rb^2)^{-1}\alpha \end{aligned}$$

GF(8) and GF(27)

The polynomial

$$X^3 - X - 1$$

is irreducible over GF(2) and GF(3), that is, it is irreducible modulo 2 and 3 (to show this, it suffices to show that it has no root in GF(2) nor in GF(3)). It follows that the elements of GF(8) and GF(27) may be represented by expressions

$$a + b\alpha + c\alpha^2,$$

where a, b, c are elements of GF(2) or GF(3) (respectively), and α is a symbol such that

$$\alpha^3 = \alpha + 1.$$

The addition, additive inverse and multiplication on GF(8) and GF(27) may thus be defined as follows; in following formulas, the operations between elements of GF(2) or GF(3), represented by Latin letters, are the operations in GF(2) or GF(3), respectively:

$$\begin{aligned} -(a+b\alpha+c\alpha^2) &= -a+(-b)\alpha+(-c)\alpha^2 \qquad \text{(for GF(8), this operation is t} \\ (a+b\alpha+c\alpha^2)+(d+e\alpha+f\alpha^2) &= (a+d)+(b+e)\alpha+(c+f)\alpha^2 \\ (a+b\alpha+c\alpha^2)(d+e\alpha+f\alpha^2) &= (ad+bf+ce)+(ae+bd+bf+ce+cf)\alpha+(af+be+ \end{aligned}$$

GF(16)

The polynomial

$$X^4 + X + 1$$

is irreducible over GF(2), that is, it is irreducible modulo 2. It follows that the elements of GF(16) may be represented by expressions

$$a + b\alpha + c\alpha^2 + d\alpha^3,$$

where a, b, c, d are either 0 or 1 (elements of GF(2)), and α is a symbol such that

$$\alpha^4 = \alpha + 1$$

(that is, α is defined as a root of the given irreducible polynomial). As the characteristic of GF(2) is 2, each element is its additive inverse in GF(16). The addition and multiplication on GF(16) may be defined as follows; in following formulas, the operations between elements of GF(2), represented by

Latin letters are the operations in GF(2).

$$(a+b\alpha+c\alpha^2+d\alpha^3)+(e+f\alpha+g\alpha^2+h\alpha^3)=(a+e)+(b+f)\alpha+(c+g)\alpha^2+(d+h)\alpha^3$$
$$(a+b\alpha+c\alpha^2+d\alpha^3)(e+f\alpha+g\alpha^2+h\alpha^3)=(ae+bh+cg+df)+(af+be+bh+cg+$$
$$(ag+bf+ce+ch+dg+dh)\alpha^2+(ah+b$$

The field GF(16) has eight primitive elements (the elements that have all nonzero elements of GF(16) as integer powers). These elements are the four roots of X^4+X+1 and their multiplicative inverses. In particular, α is a primitive element, and the primitive elements are α^m with m less than and coprime with 15 (that is, 1, 2, 4, 7, 8, 11, 13, 14).

Multiplicative structure

The set of non-zero elements in GF(q) is an abelian group under the multiplication, of order $q-1$. By Lagrange's theorem, there exists a divisor k of $q-1$ such that $x^k=1$ for every non-zero x in GF(q). As the equation $x^k=1$ has at most k solutions in any field, $q-1$ is the highest possible value for k. The structure theorem of finite abelian groups implies that this multiplicative group is cyclic, that is, all non-zero elements are powers of a single element. In summary:

> *The multiplicative group of the non-zero elements in* GF(q) *is cyclic, and there exists an element* a*, such that the* $q-1$ *non-zero elements of* GF(q) *are* $a, a^2, \ldots, a^{q-2}, a^{q-1}=1$.

Such an element a is called a primitive element. Unless $q=2, 3$, the primitive element is not unique. The number of primitive elements is $\varphi(q-1)$ where φ is Euler's totient function.

The result above implies that $x^q=x$ for every x in GF(q). The particular case where q is prime is Fermat's little theorem.

Discrete logarithm

If a is a primitive element in GF(q), then for any non-zero element x in F, there is a unique integer n with $0\le n\le q-2$ such that

$$x=a^n.$$

This integer n is called the discrete logarithm of x to the base a.

While a^n can be computed very quickly, for example using exponentiation by squaring, there is no known efficient algorithm for computing the inverse operation, the discrete logarithm. This has been used in various cryptographic protocols, see Discrete logarithm for details.

When the nonzero elements of GF(q) are represented by their discrete logarithms, multiplication and division are easy, as they reduce to addition and subtraction modulo $q-1$. However, addition amounts to computing the discrete logarithm of a^m+a^n. The identity

$$a^m+a^n=a^n(a^{m-n}+1)$$

allows one to solve this problem by constructing the table of the discrete logarithms of a^n+1, called Zech's logarithms, for $n=0, \ldots, q-2$ (it is convenient to define the discrete logarithm of zero as being $-\infty$).

Zech's logarithms are useful for large computations, such as linear algebra over medium-sized fields, that is, fields that are sufficiently large for making natural algorithms inefficient, but not too large, as one has to pre-compute a table of the same size as the order of the field.

Roots of unity

Every nonzero element of a finite field is a root of unity, as $x^{q-1} = 1$ for every nonzero element of GF(q).

If n is a positive integer, an n-th **primitive root of unity** is a solution of the equation $x^n = 1$ that is not a solution of the equation $x^m = 1$ for any positive integer $m < n$. If a is a nth primitive root of unity in a field F, then F contains all the n roots of unity, which are $1, a, a^2, \ldots, a^{n-1}$.

The field GF(q) contains a nth primitive root of unity if and only if n is a divisor of $q - 1$; if n is a divisor of $q - 1$, then the number of primitive nth roots of unity in GF(q) is $\varphi(n)$ (Euler's totient function). The number of nth roots of unity in GF(q) is $\gcd(n, q - 1)$.

In a field of characteristic p, every (np)th root of unity is also a nth root of unity. It follows that primitive (np)th roots of unity never exist in a field of characteristic p.

On the other hand, if n is coprime to p, the roots of the nth cyclotomic polynomial are distinct in every field of characteristic p, as this polynomial is a divisor of $X^n - 1$, whose discriminant $\boldsymbol{n^n}$ is nonzero modulo p. It follows that the nth cyclotomic polynomial factors over GF(p) into distinct irreducible polynomials that have all the same degree, say d, and that GF(p^d) is the smallest field of characteristic p that contains the nth primitive roots of unity.

Example: GF(64)

The field GF(64) has several interesting properties that smaller fields do not share: it has two subfields such that neither is contained in the other; not all generators (elements with minimal polynomial of degree 6 over GF(2)) are primitive elements; and the primitive elements are not all conjugate under the Galois group.

The order of this field being 2^6, and the divisors of 6 being 1, 2, 3, 6, the subfields of GF(64) are GF(2), GF(2^2) = GF(4), GF(2^3) = GF(8), and GF(64) itself. As 2 and 3 are coprime, the intersection of GF(4) and GF(8) in GF(64) is the prime field GF(2).

The union of GF(4) and GF(8) has thus 10 elements. The remaining 54 elements of GF(64) generate GF(64) in the sense that no other subfield contains any of them. It follows that they are roots of irreducible polynomials of degree 6 over GF(2). This implies that, over GF(2), there are exactly $9 = \frac{54}{6}$ irreducible monic polynomials of degree 6. This may be verified by factoring $X^{64} - X$ over GF(2).

The elements of GF(64) are primitive nth roots of unity for some n dividing 63. As the 3rd and the 7th roots of unity belong to GF(4) and GF(8), respectively, the 54 generators are primitive nth roots of unity for some n in {9, 21, 63}. Euler's totient function shows that there are 6 primitive 9th roots of unity, 12 primitive 21st roots of unity, and 36 primitive 63rd roots of unity. Summing these numbers, one finds again 54 elements.

By factoring the cyclotomic polynomials over GF(2), one finds that:

- The six primitive 9th roots of unity are roots of

$$X^6 + X^3 + 1,$$

and are all conjugate under the action of the Galois group.

- The twelve primitive 21st roots of unity are roots of

$$(X^6 + X^4 + X^2 + X + 1)(X^6 + X^5 + X^4 + X^2 + 1).$$

They form two orbits under the action of the Galois group. As the two factors are reciprocal to each other, a root and its (multiplicative) inverse do not belong to the same orbit.

- The 36 primitive elements of $\mathrm{GF}(64)$ are the roots of

$$(X^6 + X^4 + X^3 + X + 1)(X^6 + X + 1)(X^6 + X^5 + 1)(X^6 + X^5 + X^3 + X^2 + 1)(X^6 + X$$

They split into six orbits of six elements each under the action of the Galois group.

This shows that the best choice to construct $\mathrm{GF}(64)$ is to define it as $\mathrm{GF}(2)[X] / (X^6 + X + 1)$. In fact, this generator is a primitive element, and this polynomial is the irreducible polynomial that produces the easiest Euclidean division.

Frobenius automorphism and Galois theory

In this section, p is a prime number, and $q = p^n$ is a power of p.

In $\mathrm{GF}(q)$, the identity $(x + y)^p = x^p + y^p$ implies that the map

$$\varphi : x \mapsto x^p$$

is a $\mathrm{GF}(p)$-linear endomorphism and a field automorphism of $\mathrm{GF}(q)$, which fixes every element of the subfield $\mathrm{GF}(p)$. It is called the Frobenius automorphism, after Ferdinand Georg Frobenius.

Denoting by φ^k the composition of φ with itself k times, we have

$$\varphi^k : x \mapsto x^{p^k}.$$

It has been shown in the preceding section that φ^n is the identity. For $0 < k < n$, the automorphism φ^k is not the identity, as, otherwise, the polynomial

$$X^{p^k} - X$$

would have more than p^k roots.

There are no other $\mathrm{GF}(p)$-automorphisms of $\mathrm{GF}(q)$. In other words, $\mathrm{GF}(p^n)$ has exactly n $\mathrm{GF}(p)$-automorphisms, which are

$$\mathrm{Id} = \varphi^0, \varphi, \varphi^2, \ldots, \varphi^{n-1}.$$

In terms of Galois theory, this means that $\mathrm{GF}(p^n)$ is a Galois extension of $\mathrm{GF}(p)$, which has a cyclic Galois group.

The fact that the Frobenius map is surjective implies that every finite field is perfect.

Polynomial factorization

If F is a finite field, a non-constant monic polynomial with coefficients in F is irreducible over F, if it is not the product of two non-constant monic polynomials, with coefficients in F.

As every polynomial ring over a field is a unique factorization domain, every monic polynomial over a finite field may be factored in a unique way (up to the order of the factors) into a product of irreducible monic polynomials.

There are efficient algorithms for testing polynomial irreducibility and factoring polynomials over finite field. They are a key step for factoring polynomials over the integers or the rational numbers. At least for this reason, every computer algebra system has functions for factoring polynomials over finite fields, or, at least, over finite prime fields.

Irreducible polynomials of a given degree

The polynomial

$$X^q - X$$

factors into linear factors over a field of order q. More precisely, this polynomial is the product of all monic polynomials of degree one over a field of order q.

This implies that, if $q = p^n$ then $X^q - X$ is the product of all monic irreducible polynomials over $\mathrm{GF}(p)$, whose degree divides n. In fact, if P is an irreducible factor over $\mathrm{GF}(p)$ of $X^q - X$, its degree divides n, as its splitting field is contained in $\mathrm{GF}(p^n)$. Conversely, if P is an irreducible monic polynomial over $\mathrm{GF}(p)$ of degree d dividing n, it defines a field extension of degree d, which is contained in $\mathrm{GF}(p^n)$, and all roots of P belong to $\mathrm{GF}(p^n)$, and are roots of $X^q - X$; thus P divides $X^q - X$. As $X^q - X$ does not have any multiple factor, it is thus the product of all the irreducible monic polynomials that divide it.

This property is used to compute the product of the irreducible factors of each degree of polynomials over $\mathrm{GF}(p)$; see Distinct degree factorization.

Number of monic irreducible polynomials of a given degree over a finite field

The number $N(q, n)$ of monic irreducible polynomials of degree n over $\mathrm{GF}(q)$ is given by[4]

$$N(q,n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d},$$

where μ is the Möbius function. This formula is almost a direct consequence of above property of $X^q - X$.

By the above formula, the number of irreducible (not necessarily monic) polynomials of degree n over $\mathrm{GF}(q)$ is $(q-1)N(q, n)$.

A (slightly simpler) lower bound for $N(q, n)$ is

$$N(q,n) \geq \frac{1}{n}\left(q^n - \sum_{p|n,\ p \text{ prime}} q^{n/p}\right).$$

One may easily deduce that, for every q and every n, there is at least one irreducible polynomial of degree n over GF(q). This lower bound is sharp for $q = n = 2$.

Applications

In cryptography, the difficulty of the discrete logarithm problem in finite fields or in elliptic curves is the basis of several widely used protocols, such as the Diffie–Hellman protocol. For example, in 2014, a secure internet connection to Wikipedia involved the elliptic curve Diffie–Hellman protocol (ECDHE) over a large finite field.[5] In coding theory, many codes are constructed as subspaces of vector spaces over finite fields.

Finite fields are used by many error correction codes, such as Reed–Solomon error correction code or BCH code. The finite field almost always has characteristic of 2, since computer data is stored in binary. For example, a byte of data can be interpreted as an element of $GF(2^8)$. One exception is PDF417 bar code, which is $GF(929)$. Some CPUs have special instructions that can be useful for finite fields of characteristic 2, generally variations of carry-less product.

Finite fields are widely used in number theory, as many problems over the integers may be solved by reducing them modulo one or several prime numbers. For example, the fastest known algorithms for polynomial factorization and linear algebra over the field of rational numbers proceed by reduction modulo one or several primes, and then reconstruction of the solution by using Chinese remainder theorem, Hensel lifting or the LLL algorithm.

Similarly many theoretical problems in number theory can be solved by considering their reductions modulo some or all prime numbers. See, for example, Hasse principle. Many recent developments of algebraic geometry were motivated by the need to enlarge the power of these modular methods. Wiles' proof of Fermat's Last Theorem is an example of a deep result involving many mathematical tools, including finite fields.

The Weil conjectures concern the number of points on algebraic varieties over finite fields and the theory has many applications including exponential and character sum estimates.

Finite fields have widespread application in combinatorics, two well known examples being the definition of Paley Graphs and the related construction for Hadamard Matrices. In arithmetic combinatorics finite fields[6] and finite field models[7][8] are used extensively, such as in Szemerédi's theorem on arithmetic progressions.

Extensions

Algebraic closure

A finite field F is not algebraically closed: the polynomial

$$f(T) = 1 + \prod_{\alpha \in F} (T - \alpha),$$

has no roots in F, since $f(\alpha) = 1$ for all α in F.

Fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. The map $\varphi_q\colon \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ sending each x to x^q is called the qth power Frobenius automorphism. The subfield of $\overline{\mathbb{F}}_q$ fixed by the nth iterate of φ_q is the set of zeros of the polynomial $x^{q^n} - x$, which has distinct roots since its derivative in $\mathbb{F}_q[x]$ is -1, which is never zero. Therefore that subfield has q^n elements, so it is the unique copy of $\mathbb{F}_{q^n}$ in $\overline{\mathbb{F}}_q$. Every finite extension of $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$ is this $\mathbb{F}_{q^n}$ for some n, so

$$\overline{\mathbb{F}}_q = \bigcup_{n \geq 1} \mathbb{F}_{q^n}.$$

The absolute Galois group of $\mathbb{F}_q$ is the profinite group

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \varprojlim_n \mathrm{Gal}(\overline{\mathbb{F}}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_n (\mathbf{Z}/n\mathbf{Z}) = \widehat{\mathbf{Z}}.$$

Like any infinite Galois group, $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ may be equipped with the Krull topology, and then the isomorphisms just given are isomorphisms of topological groups. The image of φ_q in the group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^n}/\mathbb{F}_q) \simeq \mathbf{Z}/n\mathbf{Z}$ is the generator 1, so φ_q corresponds to $\mathbf{1} \in \widehat{\mathbf{Z}}$. It follows that φ_q has infinite order and generates a dense subgroup of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, not the whole group, because the element $\mathbf{1} \in \widehat{\mathbf{Z}}$ has infinite order and generates the dense subgroup $\mathbf{Z} \subsetneq \widehat{\mathbf{Z}}$. One says that φ_q is a topological generator of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Quasi-algebraic closure

Although finite fields are not algebraically closed, they are quasi-algebraically closed, which means that every homogeneous polynomial over a finite field has a non-trivial zero whose components are in the field if the number of its variables is more than its degree. This was a conjecture of Artin and Dickson proved by Chevalley (see Chevalley–Warning theorem).

Wedderburn's little theorem

A division ring is a generalization of field. Division rings are not assumed to be commutative. There are no non-commutative finite division rings: Wedderburn's little theorem states that all finite division rings are commutative, and hence are finite fields. This result holds even if we relax the associativity axiom to alternativity, that is, all finite alternative division rings are finite fields, by the Artin–Zorn theorem.[9]

See also

- Quasi-finite field
- Field with one element
- Finite field arithmetic
- Finite ring
- Finite group

- Elementary abelian group
- Hamming space

Notes

1. Moore, E. H. (1896), "A doubly-infinite system of simple groups", in E. H. Moore; et al. (eds.), *Mathematical Papers Read at the International Mathematics Congress Held in Connection with the World's Columbian Exposition*, Macmillan & Co., pp. 208–242
2. This latter notation was introduced by E. H. Moore in an address given in 1893 at the International Mathematical Congress held in Chicago Mullen & Panario 2013, p. 10.
3. *Recommended Elliptic Curves for Government Use* (http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf) (PDF), National Institute of Standards and Technology, July 1999, p. 3
4. Jacobson 2009, §4.13
5. This can be verified by looking at the information on the page provided by the browser.
6. Shparlinski, Igor E. (2013), "Additive Combinatorics over Finite Fields: New Results and Applications", *Finite Fields and Their Applications*, DE GRUYTER, pp. 233–272, doi:10.1515/9783110283600.233 (https://doi.org/10.1515%2F9783110283600.233), ISBN 9783110283600
7. Green, Ben (2005), "Finite field models in additive combinatorics", *Surveys in Combinatorics 2005*, Cambridge University Press, pp. 1–28, arXiv:math/0409420 (https://arxiv.org/abs/math/0409420), doi:10.1017/cbo9780511734885.002 (https://doi.org/10.1017%2Fcbo9780511734885.002), ISBN 9780511734885, S2CID 28297089 (https://api.semanticscholar.org/CorpusID:28297089)
8. Wolf, J. (March 2015). "Finite field models in arithmetic combinatorics – ten years on" (https://doi.org/10.1016%2Fj.ffa.2014.11.003). *Finite Fields and Their Applications*. **32**: 233–274. doi:10.1016/j.ffa.2014.11.003 (https://doi.org/10.1016%2Fj.ffa.2014.11.003). ISSN 1071-5797 (https://www.worldcat.org/issn/1071-5797).
9. Shult, Ernest E. (2011). *Points and lines. Characterizing the classical geometries*. Universitext. Berlin: Springer-Verlag. p. 123. ISBN 978-3-642-15626-7. Zbl 1213.51001 (https://zbmath.org/?format=complete&q=an:1213.51001).

References

- W. H. Bussey (1905) "Galois field tables for $p^n \leq 169$", Bulletin of the American Mathematical Society 12(1): 22–38, doi:10.1090/S0002-9904-1905-01284-2 (https://doi.org/10.1090%2FS0002-9904-1905-01284-2)
- W. H. Bussey (1910) "Tables of Galois fields of order < 1000", *Bulletin of the American Mathematical Society* 16(4): 188–206, doi:10.1090/S0002-9904-1910-01888-7 (https://doi.org/10.1090%2FS0002-9904-1910-01888-7)
- Jacobson, Nathan (2009) [1985], *Basic algebra I* (Second ed.), Dover Publications, ISBN 978-0-486-47189-1
- Mullen, Gary L.; Mummert, Carl (2007), *Finite Fields and Applications I*, Student Mathematical Library (AMS), ISBN 978-0-8218-4418-2
- Mullen, Gary L.; Panario, Daniel (2013), *Handbook of Finite Fields*, CRC Press, ISBN 978-1-4398-7378-6
- Lidl, Rudolf; Niederreiter, Harald (1997), *Finite Fields* (https://archive.org/details/finitefields0000lidl_a8r3) (2nd ed.), Cambridge University Press, ISBN 0-521-39231-4
- Skopin, A. I. (2001) [1994], "Galois field" (https://www.encyclopediaofmath.org/index.php?title=Galois_field), *Encyclopedia of Mathematics*, EMS Press

External links

- Finite Fields (http://mathworld.wolfram.com/FiniteField.html) at Wolfram research.