Galois fields

1 Fields

A field is an algebraic structure in which the operations of addition, subtraction, multiplication, and division (except by zero) can be performed, and satisfy the usual rules.

More precisely, a *field* is a set F with two binary operations $+$ (addition) and $\cdot$ (multiplication) are defined, in which the following laws hold:

(A1) $a+(b+c)=(a+b)+c$ (associative law for addition)

(A2) $a+b=b+a$ (commutative law for addition)

(A3) There is an element 0 (zero) such that $a+0=a$ for all a.

(A4) For any a, there is an element $-a$ such that $a+(-a)=0$.

(M1) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (associative law for multiplication)

(M2) $a\cdot b=b\cdot a$ (commutative law for multiplication)

(M3) There is an element 1 (not equal to 0) such that $a\cdot 1=a$ for all a.

(M4) For any $a\neq 0$, there is an element a^{-1} such that $a\cdot a^{-1}=1$.

(D) $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ (distributive law)

Using the notion of a group, we can condense these nine axioms into just three:

- The elements of F form an Abelian group with the operation $+$ (called the *additive group* of F).
- The non-zero elements of F form an Abelian group under the operation $\cdot$ (called the *multiplicative group* of F).
- Multiplication by any non-zero element is an automorphism of the additive group.

We usually write $x \cdot y$ simply as xy. Many other familiar arithmetic properties can be proved from the axioms: for example, $0x = 0$ for any x.

Familiar examples of fields are found among the number systems (the rational numbers, the real numbers, and the complex numbers are all fields). There are many others. For example, if p is a prime number, then the *integers mod p* form a field: its elements are the congruence classes of integers mod p, with addition and multiplication induced from the usual integer operations.

For example, here are the addition and multiplication tables for the integers mod 3. (We use $0, 1, 2$ as representatives of the congruence classes.)

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2 Finite fields: existence

Galois (in one of the few papers published in his lifetime) answered completely the question of which finite fields exist.

First, the number of elements in a finite field must be a prime power, say $q = p^r$, where p is prime.

Then, for each prime power $q = p^r$, there exists a field of order q, and it is unique (up to isomorphism).

The construction is as follows. First, let F_0 be the field of integers mod p. Now choose an irreducible polynomial $f(X)$ of degree r over F_0. (It can be shown that such polynomials always exist; indeed, it is possible to count them.) We can assume that the leading coefficient of f is equal to 1; say

$$f(X) = X^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0.$$

We take the elements of F to be all expressions of the form

$$x_0 + x_1a + x_2a^2 + \cdots + x_{r-1}a^{r-1},$$

where a is required to satisfy $f(a) = 0$, and $x_0, \ldots, x_{r-1} \in F_0$. (This is very similar to the construction of the complex numbers as of the form $x + y\mathrm{i}$, where $\mathrm{i}^2 + 1 = 0$, and x and y are real numbers.)

Now the number of expressions of the above form is p^r, since there are p choices for each of the r coefficients $x_0,\ldots,x_{r-1}$. Adding these expressions is straightforward. To multiply them, observe that

$$a^r = -c_{r-1}a^{r-1} - \cdots - c_1 a - c_0,$$

so a^r (and similarly any higher power of a) can be reduced to the required form.

It can be shown, using the irreducibility of the polynomial f, that this construction produces a field. Moreover, even though there are different choices for the irreducible polynomials, the fields constructed are all isomorphic.

For an example, we construct a field of order $9 = 3^2$, using the polynomial $X^2 + 1$, which is irreducible over the field of integers mod 3. The elements of the field are all expressions of the form $x + ya$, where $a^2 = 2$, and $x,y = 0,1,2$. As examples of addition and multiplication, we have

$$\begin{aligned} (2+a)+(2+2a) &= 4+3a = 1, \\ (2+a)(2+2a) &= 4+6a+2a^2 = 4+0+4 = 8 = 2. \end{aligned}$$

3 Finite fields: properties

In this section, we describe some properties of the Galois field $F = \mathrm{GF}(q)$, where $q = p^r$ with p prime. As noted in the last section, the elements $0,1,2,\ldots,p-1$ of F form a subfield F_0 which is isomorphic to the integers mod p; for obvious reasons, it is known as the *prime subfield* of F.

Additive group. The additive group of $\mathrm{GF}(q)$ is an elementary Abelian p-group. This is because

$$x + \cdots + x = (1 + \cdots + 1)x = 0x = 0,$$

where there are p terms in the sum. Thus, it is the direct sum of r cyclic groups of order p.

Another way of saying this is that F is a vector space of dimension r over F_1; that is, there is a *basis* $(a_1,\ldots,a_r)$ such that every element x of F can be written uniquely in the form

$$x = x_1 a_1 + \cdots + x_r a_r$$

for some $a_1,\ldots,x_r \in F_0 = \{0,1,\ldots,p-1\}$.

Multiplicative group. The most important result is that *the multiplicative group of* $\mathrm{GF}(q)$ *is cyclic*; that is, there exists an element g called a *primitive root*) such that every non-zero element of F can be written uniquely in the form g^i for some i with $0 \leq i \leq q-2$. Moreover, we have $g^{q-1} = g^0 = 1$.

Squares. Suppose that q is odd. Then the cyclic group of order $q-1$ has the property that exactly half its elements are squares (those which are even posers of a primitive element). The squares are sometimes called *quadratic residues*, and the non-squares are *quadratic non-residues*. (These terms are used especially in the case where q is prime, so that $\mathrm{GF}(q)$ is the field of integers mod q.

Automorphism group. An automorphism of F is a one-to-one mapping $x \mapsto x^\pi$ from F onto F, such that

$$(x+y)^\pi = x^\pi + y^\pi, \qquad (xy)^\pi = x^\pi y^\pi$$

for all x,y.

The map $\sigma : x \mapsto x^p$ is an automorphism of F, known as the *Frobenius automorphism*. The elements of F fixed by the Frobenius automorphism are precisely those lying in the prime subfield F_0. Moreover, the group of automorphisms of F is cyclic of order r, generated by σ. (This means that every automorphism has the form $x \mapsto x^{p^i}$ for some value of i with $0 \leq i \leq r-1$.

Special bases. We saw that F has bases of size r as a vector space over F_0. These bases can be chosen to have various additional properties.

The easiest type of basis to find is one of the form $\{1, a, a^2, \ldots, a^{r-1}\}$, where a is the root of an irreducible polynomial of degree r over F_0. The existence of such basis is guaranteed by the construction.

A basis of the form $\{a, a^\sigma, a^{\sigma^2}, \ldots, a^{\sigma^{r-1}}\}$, where σ is the Frobenius automorphism, is called a *normal basis*. Such a basis always exists. Note that the automorphism group of F has a particularly simple form relative to a normal basis, since the basis elements are just permuted cyclically by the automorphisms.

Subfields. If the field $\mathrm{GF}(p^r)$ has a subfield $\mathrm{GF}(p_1^s)$, where p and p_1 are primes, then $p = p_1$ and s divides r. Conversely, if s divides r then $\mathrm{GF}(p^r)$ has a unique subfield of order p^s. The necessity of the condition is proved by applying Lagrange's Theorem to the additive and multiplicative groups. The sufficiency is proved by observing that, if σ is the Frobenius automorphism of $\mathrm{GF}(p^r)$, and s divides r, then the fixed elements of the automorphism σ^s (that is, the elements a satisfying $a^{p^s} = a$) form the unique subfield of order p^s.

Calculation in finite fields. Addition in $\mathrm{GF}(q)$ is easy if we have chosen a basis: we have

$$(x_1a_a + \cdots + x_ra_r) + (y_1a_1 + \cdots + y_ra_r) = (x_1 + y_1)a_1 + \cdots + (x_r + y_r)a_r,$$

in other words, we add "coordinate-wise".

On the other hand, multiplication is easy if we have chosen a primitive root g: we have

$$(g^i) \cdot (g^j) = g^{i+j},$$

where the exponent is reduced mod $q - 1$ if necessary.

In order to be able to perform both operations, we need a table telling us how to translate between the two representations. This is essentially a table of logarithms (for those who remember such things), since if $g^i = x$, we can think of i as the "logarithm" of x.

For the field $\mathrm{GF}(9)$ which we constructed earlier, using an element a satisfying $a^2 = 2$ (over the integers mod 3), we find that $g = 1 + a$ is a primitive element, and the table of logarithms is as follows:

g^0	1
g^1	$a+1$
g^2	$2a$
g^3	$2a+1$
g^4	2
g^5	$2a+2$
g^6	a
g^7	$a+2$

For example, $(a+2)(2a+2) = g^7 \cdot g^5 = g^{12} = g^4 = 2$.

References

[1] R. Lidl and H. Niederreiter, *Finite Fields,* Cambridge University Press, Cambridge, 1996.

Peter J. Cameron
May 30, 2003