Defn: A group $(G, \bullet)$ is a set G along with a binary operation $\bullet$ such that the following axioms are satisfied:

1) The binary operation $\bullet$ is associative.
2) There is an element e in G such that $e \bullet x = x \bullet e = x$ for all $x \in G$.
   This element e is an identity element for $\bullet$ on G.
3) For each $x \in G$ there is an element $x' \in G$ with the property that $x' \bullet x = x \bullet x' = e$.
   The element x' is an inverse of x with respect to the operation $\bullet$.

Defn: A group G is abelian if its binary operation $\bullet$ is commutative. That is if $x \bullet y = y \bullet x$ for every $x, y \in G$.

examples:

1) The integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are all abelian groups under addition.

2) $\mathbb{Z}_n = \{ 0, 1, 2, \ldots, n-1 \}$ under addition modulo n is an abelian group.

3) $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ is an abelian group under multiplication modulo p.

Defn: A field $(F, +, \cdot)$ is a set F along with two binary operations + and $\cdot$ (called addtion and multiplication) defined on F such that the following axioms hold:

$(F, +)$ is an abelian group.

a) The binary operation + is associative.
b) There is an identity element for +.
c) Each element in F has an additive inverse.
d) The binary operation + is commutative.

$(F^*, \cdot)$ is an abelian group.

e) The binary operation $\cdot$ is associative.
f) There is an identity element for $\cdot$.
g) Each element in F has a muliplicative inverse.
h) The binary operation $\cdot$ is commutative.

Multiplication distributes over addition:

i) For all $a, b, c \in F$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

and

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

The finite field $\mathbb{Z}_{17}$:

$\mathbb{Z}_{17}$ = { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 } under addition modulo 17 and multiplication modulo 17 is a field. Here is the multiplication table:

·	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
01	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
02	02	04	06	08	10	12	14	16	01	03	05	07	09	11	13	15
03	03	06	09	12	15	01	04	07	10	13	16	02	05	08	11	14
04	04	08	12	16	03	07	11	15	02	06	10	14	01	05	09	13
05	05	10	15	03	08	13	01	06	11	16	04	09	14	02	07	12
06	06	12	01	07	13	02	08	14	03	09	15	04	10	16	05	11
07	07	14	04	11	01	08	15	05	12	02	09	16	06	13	03	10
08	08	16	07	15	06	14	05	13	04	12	03	11	02	10	01	09
09	09	01	10	02	11	03	12	04	13	05	14	06	15	07	16	08
10	10	03	13	06	16	09	02	12	05	15	08	01	11	04	14	07
11	11	05	16	10	04	15	09	03	14	08	02	13	07	01	12	06
12	12	07	02	14	09	04	16	11	06	01	13	08	03	15	10	05
13	13	09	05	01	14	10	06	02	15	11	07	03	16	12	08	04
14	14	11	08	05	02	16	13	10	07	04	01	15	12	09	06	03
15	15	13	11	09	07	05	03	01	16	14	12	10	08	06	04	02
16	16	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01

Notice the table is symmetric since multiplication modulo 17 is a commutative operation.

We can find inverses: e.g. $11^{-1} = 14$.

Notice 3 is a primitive element: $3^1 = 3$, $3^2 = 9$, $3^3 = 10$, $3^4 = 13$, $3^5 = 5$, $3^6 = 15$, $3^7 = 11$, $3^8 = 16$, $3^9 = 14$, $3^{10} = 8$, $3^{11} = 7$, $3^{12} = 4$, $3^{13} = 12$, $3^{14} = 2$, $3^{15} = 6$, $3^{16} = 1$.

Division Algorithm for F[x]: Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

be elements in F[x] such that a_n, b_m are nonzero elements in F and $m>0$. Then, there are unique polynomials $q(x)$, $r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$, with the degree of $r(x)$ less than m.

Defn: A nonconstant polynomial $f(x) \in F[x]$ is call an <u>irreducible polynomial over F</u> if $f(x)$ cannot be expressed as a product of two polynomials in F[x] both having lower degree than the degree of $f(x)$.

Theorem: Let p be a prime. There is a unique finite field of order p^n for every $n \in Z^+$. This field is usually denote $GF(p^n)$ and is called the <u>Galois field of order p^n</u>.

$Z_p[x]$

$p(x)$ irreducible mod p

$\deg(p(x)) = n$

$GF(p^n) \cong Z_p[x] \bmod p(x)$

$GF(4)$ in two ways

$\{0, 1, \omega, \omega^2\}$

$\Updownarrow$ find

$\{0, 1, x, x+1\}$

Construction of a field of order 8:

Consider $\mathbb{Z}_2 = \{ 0, 1\}$ which is a field with just two elements. Form $\mathbb{Z}_2[x]$, the set of all polynomials in the indeterminate x. Define addition and multiplication of polynomials in the usual way. Look at $f(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]$. Any element in $\mathbb{Z}_2[x]$ can be divided by f(x) yielding a remainder of degree 2 or less. These possible remainders are $\{ 0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$. On this set of remainders define addition as usual and define multiplication "modulo f(x)". That is, to multiply two elements together, do so in the usual way and then divide by f(x) and take the remainder.

A miracle occurs! This set, denoted $\mathbb{Z}_2[x]/(x^3 + x + 1)$, is a field with 8 elements.

Associate $a_2x^2 + a_1x + a_0$ with the ordered tuple $a_2a_1a_0$. The multiplication table is:

	001	010	011	100	101	110	111
001	001	010	011	100	101	110	111
010	010	100	110	011	001	111	101
011	011	110	101	111	100	001	010
100	100	011	111	110	010	101	001
101	101	001	100	010	111	011	110
110	110	111	001	101	011	010	100
111	111	101	010	001	110	100	011

$GF(9) = GF(3^2)$

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

$F = \{x + ya : +, *\}$, $a^2 = 2$

Ex: $(2+a) + (2+2a) = 1$

$(2+a) * (2+2a) = 2$

F - vector space of dimension r over F_0 (prime field)

$\exists g \; \forall s \in F \quad s = g^i, \quad 1 \le i \le q-1$

$g^i \cdot g^j = g^{i+j}$

$g = 1 + a$, primitive in F

$F = GF(p^r)$ $\quad q = r \quad$ $F_0 = Z_p$

$f(x) \in F_0[x]$, degree r, irreducible

$f(x) = x^r + c_{r-1}x^{r-1} + \cdots + c_1 x + c_0$

think $a \in F$, $f(a) = 0$

$F = \{ x_0 + x_1 a + \cdots + x_{r-1} a^{r-1} : +, * \bmod f$

Example (over R)

$f(x) = x^2 + 1, \quad a = i \in \mathbb{C}$

$|F| = p^r$

$$a^r = -\sum_{i=0}^{r-1} c_i a^i$$

i	g^i
0	1
1	$a+1$
2	$2a$
3	$2a+1$
4	2
5	$2a+2$
6	a
7	$a+2$
8	1

Galois fields

B

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.

Peter Cameron

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

·	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

$$x = x_1a_1 + \cdots + x_ra_r$$

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* 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 $0 \le i \le q-2$. 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 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 $0 \le i \le r-1$.

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 GF(p^r) has a subfield 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 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 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 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 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.