Finite fields

Students, you might have come across several abstract algebraic structures, particularly groups, ring, fields and polynomials.

Group → $(G, \cdot)$ is a nonempty set G together with a binary operation.

Group is a set of elements, [for ex, set of rational numbers, ~~matrix~~ ~~polynomial~~ real numbers, integers - -]. We are performing on this set of elements following binary operation $(\cdot)$ such that conds hold.

a) Closure — for all $a, b \in G$ $a+b \in G$

b) Inverse — $a + (-a) = 0$

c) Associativity $a+(b+c) = (a+b)+c$

d) Identity → $a + 0 = a$

$a + 0 = a$

Set of integers $(\mathbb{Z})$ is satisfying all axioms.

so $(\mathbb{Z}, +)$ is a group. | abelian group

$(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$ are groups.

$(\mathbb{N},+)$ is not a group.

does not satisfy Inverse in $\mathbb{N}$

N - Natural no's = $\{1, 2, 3 \ldots\}$

W = whole no's = $\{0, 1, 2, 3 \ldots\}$

Z = Integers = $\{-1, -2, -3, 0, 1, 2, 3 \ldots\}$

Q - Rational numbers = $\{p/q ; p$ & q are integers$\}$

I - Irrational " = {non-Rational no}

R - Real numbers -

C - complex " $\{a+bi, \ldots\}$.

<u>Ring</u> - It consists of a set equipped with 2 binary oprs that generalize the arithmetic oprs of addition & multiplication

$+$ & $\cdot$

<u>Addition</u>	Multiplication
<u>closure</u>.	→ Associative. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
<u>Inverse</u>	
<u>Associativity</u>	
Identity.	

$$\boxed{\begin{array}{l} \text{Distributive properties.} \\ a \cdot (b+c) = a \cdot b + a \cdot c \text{ and } \\ (a+b) \cdot c = a \cdot c + b \cdot c \end{array}}$$

Z, R, C are examples for rings with identity.

eld

Field is an extension of group.
A field is a set of elements on which addition, substraction, multiplication & division are defined.

- Addition
- Additive Inverse
- Multiplication
- Multiplicative Inverse for every non zero element.

Example of field.

Set of rational no's (a/b)
Where a & b are integers and b is not equal to 0.

- They are commutative with addition.
- " " " with multiplica
- All elements have Multiplicative Inverse.

{Q; + - x ÷} Here set of rational no's satisfies all properties. So it is a field i.e. but it is a infinite field.

Note Set of Integers do not form a field
Set of 2x2 matrices do not " "

CamScanner

Finite field →

Field with finite no. of elements.

In cryptography, we are looking for finite no. of fields, satisfying all properties.

→ The no. of elements in a finite field is also called Galois field. is always a prime or power of prime.

$GF(2) = GF(2^1) = \{0, 1\}$.

$GF(5) = GF(5^1) = \{0, 1, 2, 3, 4\}$.

This no. should be a prime no.

$GF(81) = GF(3^4)$ ----.

$GF(256) = GF(2^8)$ --.

↳ finite field of 256 elements. used in cryptography for AES.

× GF (12) is not a finite field

prime field & Extension field

$GF(2^1)$ Here $m = 1$ → it is a prime field

ie $GF(p^m) = GF(2^1)$

where $m = 1$

& $p = \{0, 1\}$ ----

$GF(p^m)$ Here if $m > 1$ it is extension field.

Extension fields.
for ex:-
$GF(2^8)$ Here $m = 8$.
$p = 2$.

For AES-$GF(2^8)$ is used.

Here the elements in the set are polynomials not integers.

Polynomial — many terms attached together

ex:- $x^3 + x^2 + 1$

$3x^3 + 4x^2 + 1$

A polynomial can have any no. of terms but it cannot be infinite.

$GF(2^8) = GF(256)$
↳ elements

Finite field Arithmetic

$GF(2^3) = GF(8) = \{0, 1, 2 \longrightarrow 7\}$

$GF(2) = \{0, 1\}$.

Set of polynomial.

$GF(2^3) = \{$ it takes up the form

polynomials

000	$ax^2 + ax + 1 = 0$
001	$0 \quad 0 \cdot 1 = 1$
010	$0 \quad 1 \quad 0 =$
011	$0 + \cancel{x} + 0 = x$
100	$0 + x^1 + 1 = x + 1$
101	$a \times 1 + 0 + 0 = ax^2 = x^2$
110	$x^2 + 0 + 1 = x^2 + 1$
111	$x^2 + x + 0 = x^2 + x + 0$
$x^2\, x^1\, x^0$	$x^2 + x + 1$

When addition, Multiplication, additive inverse →.

polynomial —

$\{$ polynomial

AES — GF(256) — GF(2^8)

Here there are 256 elements and can be represented as:

$$\underline{x^7 + x^6 + x^5 +}\ x^4 + \underline{x^3 + x^2 + x^1 +}\ x^0$$

00000000 — 0
00000001 → 1
00000010 → x
00000011 → $x+1$
00000100
⋮
11111111

Ex:-

{02} = 0000 0010
{87} = 1000 0111

$x^7\ x^6\ x^5\ x^4\ x^3\ x^2\ x^1\ x^0$
0 0 0 0 0 0 1 0 → x
1 0 0 0 0 1 1 1 → $x^7 + x^2 + x^1 + x^0$.

$$x * (x^7 + x^2 + x^1 + x^0)$$

$$\underline{x^8 + x^3 + x^2 + x}$$

So consider irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$

So divide $(x^8 + x^3 + x^2 + x)/p(x)$