GROUP THEORY

Group : $(G, *)$ → any operation

A set under a specified operation is said to be a group if and only if

* it is closed.
* it is associative $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$
* There exists an identity, $a*e = e*a = a \quad \forall a \in G$
* There exists an inverse, $a*a^{-1} = a^{-1}*a = e \quad \forall a, a^{-1} \in G$

Abelian Group is a group that satisfies the commutative property,

i.e $a*b = b*a \quad \forall a,b \in G$.

Properties

* Identity element is unique.

Proof:

Let e_1 & e_2 be identities.

$\therefore$

$$a*e_1 = e_1*a = a$$

Let $a = e_2$,

then $$e_2*e_1 = e_1*e_2 = e_2 \quad \text{—} (1)$$

Similarly,

$$a*e_2 = e_2*a = a$$

Let $a = e_1$

$$e_1*e_2 = e_2*e_1 = e_1 \quad \text{—} (2)$$

By comparing (1) & (2), we can say that both are True if and only if $e_1 = e_2$

Hence, if identity element exists then, it should be unique.

* Inverse is unique:

i.e Inverse of an element is unique.

Proof:

let 'a' has inverses b & c.

By inverse properties,

$$a * b = b * a = e$$

$$a * c = c * a = e$$

consider,

$$(b * a) * c$$

$$\Rightarrow e * c = c \quad \text{---} (1)$$

As it is associative,

$$b * (a * c)$$

$$\Rightarrow b * e$$

$$= b \quad \text{---} (2)$$

As $(b * a) * c = b * (a * c)$.

c should be equal to b.

$\therefore$ Inverse of element a is unique.

* Sub Group.

Let $H \leq G$, if H itself has a group, then H is a subgroup of G. (where G is a Group)

conditions to check.

i) closure property

ii) identity element should be present in H.

iii) inverse should be present.

Simple method,

if $\forall a, b \in H$, then if $a \cdot b^{-1} \in H$ then,

H is said to be a Subgroup.

order of the sub-group should divide the order of the group.

order of an element x is the smallest number n such that $x^n = e$.

↳ identity element.

* order of an element will always divide the group order.

* If H is a subgroup of G then order(H) | order(G). and the converse is not true.

14/06

1. let p and q be distinct primes. let H be proper subset of integers and H is a group under addition that contains exactly 3 elements of the set $\{p, p+q, (q)^p, pq, (p)^q\}$.

Determine which of the elements are in H.

a) pq, p^q, q^p

b) $p+q, pq, q^p$

c) $p, p+q, pq$

d) p, p^q, q^p

e) p, pq, p^q

Let's assume p is present in H,

As H is a group.

pq can be written as, $p+p+p\ldots$ (q times)

and p^q can be written as

$$p^q = (p \cdot p)\ p \cdot p \cdot p \cdot (q \text{ times})$$

$$= (p+p+p\ldots)\ (p+p+p\ldots)$$
$$(p \text{ times})$$

As p^q, pq, can be generated from p using the addition operation.

$\{p, pq, p^q\}$ are present in H.

2. P.T $G = \{5, 15, 25, 35\}$ is a group under multiplication modulo 40.

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

identity element = 25

$5^{-1} = 5$

$15^{-1} = 15$

$25^{-1} = 25$

$35^{-1} = 35$

$ord(G) = 4$

$ord(5) = n$ such that $5^n = e = 25$

$ord(5) = 2$

$ord(15) = ord(25) = ord(35) = 2$

As ord (elements) | ord (G) we can say that G is a Group.

3. $\times_8$ → operation.

$G' = \{1, 3, 5, 7\}$

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

identity = 1.

$3^{-1} = 3$

$5^{-1} = 5$

$7^{-1} = 7$.

$ord(5) = ord(3) = ord(1)$
$= ord(7) = 2$.

if inverse of G1 & G1' are mapped and similarly other elements are mapped and if they form a one-one mapping then G1, G1' are called isomorphic.

$\{ f(a) = f(b) \}$

Isomorphism

An isomorphism f from a Group G to G' is an one-one mapping that preserves the group operations.

$$f(ab) = f(a) \cdot f(b) \quad \forall a, b \in G.$$

15/06

cyclic notation for permutations:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$O(S_5) = 5!$ (permutation group) $= 120$

$\sigma \in S_5$

then $O(\sigma) = ?$

$O(\sigma)$ can be found using composition of itself to get the identity element, which is cumbersome for large permutation groups.

σ can be expressed as product of disjoint cycles/ ~~groups~~.

1. $$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

it can be expressed as $= (1, 3, 4, 2)$

"order of cycle is same as it is length"

As α is expressed as single cycle,

order(α) = order of cycle

$= 4$,

if the group is expressed as product of disjoint cycles, then order of permutation group is lcm of order of individual cycles.

$$\sigma \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$\sigma = (1,3)(2,4)(5).$$

$$o(1,3) = 2$$
$$o(2,4) = 2$$
$$o(5) = 1.$$

$$o(\sigma) = \text{lcm}(2,2,1).$$
$$= 2.$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

= identity element.

Hence, order of σ is 2.

22/06

Ring :

A set with two Binary Operations : addition (denoted a*b) and multiplication (denoted as ab) such that $\forall a, b, c \in R$.

i) $a+b = b+a$
ii) $a+(b+c) = (a+b)+c$
iii) There is an element 0 ; $a+0 = a$
iv) There is an element $-a$; $a-a = 0$

} Abhelion Group under addition

v) $a(bc) = (ab)c$
vi) $a*(b+c) = ab+ac$ And $(b+c)a = ba+ca$.

$\mathbb{Z}_n$, $+_n$, $\times_n$ → always a Rings.

Field :

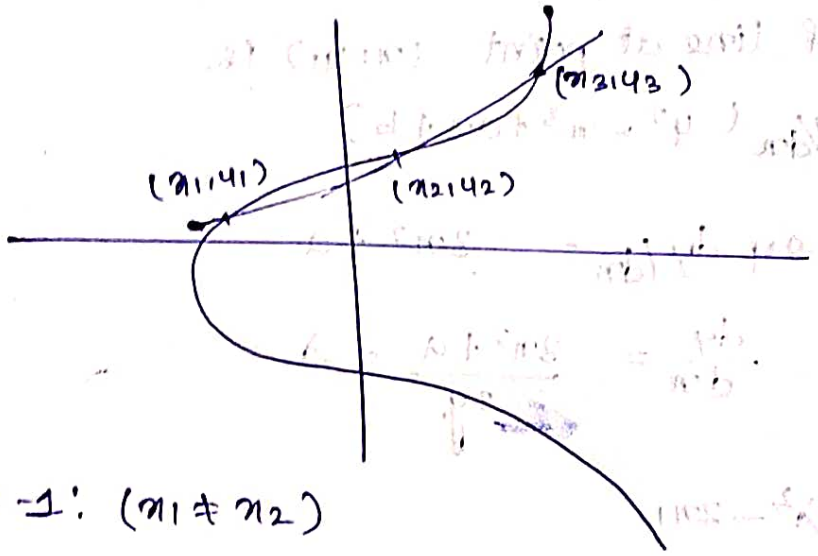
21/06

Elliptic Curves

$y^2 = x^3 + ax + b$ → equation of Elliptic Curves.

condition: $4a^3 + 27b^2 \neq 0$,

'a' 'b' $\in R$ i $4a^3 + 27b^2 \neq 0$, A non-singular elliptic curve is the set E of solutions $(x, y) \in R$ to the equation $y^2 = x^3 + ax + b$, together with a point at ∞, represented as $\mathcal{O}$



case-1: $(x_1 \neq x_2)$

Slope of line: $\frac{y_2 - y_1}{x_2 - x_1} = \lambda$

eqn of line: $y = \lambda x + c$ —①

$$c = y_1 - x_1\lambda = y_2 - \lambda x_2$$

$y^2 = x^3 + ax + b$

$(\lambda x + c)^2 = x^3 + ax + b$

$x^3 - \lambda^2 x^2 - \lambda c x + ax + b - c^2 = 0$.

$x^3 - \lambda^2 x^2 + x(a - c\lambda) + b - c^2 = 0$

~~sum~~ ∞ solutions of eqn x_1, x_2, x_3.

$x_1 + x_2 + x_3 = -(-\lambda^2)/1$ (i.e $x_1 + x_2 + x_3 = -b/a$)

$x_1 + x_2 + x_3 = \lambda^2$

find y_3 using line equation / slope equation

Case-2:

$x_1 = x_2$ i.e lines parallel to y-axis.

$y_1 = -y_2$

$(x_1, x_2) + (y_1, y_2) = \infty \rightarrow$ condition not regular — Addition.

Case-3:

consider point (x_1, y_1);

slope of line at point (x_1, y_1) is.

$dy/dx\ (y^2 = x^3 + ax + b)$

$\therefore \quad 2y\, dy/dx = 3x^2 + a$

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y} = \lambda$$

$x_3 = \lambda^2 - 2x_1$

$y_3 = \lambda(x_1 - x_3) - y_1$

Eg 1:

$y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

$\mathbb{Z}_{11} \times \mathbb{Z}_{11} \rightarrow 121$ points.