Set - collection of well defined objects.

Relation - subset of a cartesian product $A \times B \rightarrow$ co-domain (domain)

Function - relation which each of domain which a unique element in the co-domain.

Binary operation - a function from $A \times A \rightarrow A$.

M_2

Groups : $(G, *)$

Conditions :

(i) Associativity : $a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in G$.

(ii) Identity : $\exists$ an element $e \in G \ni$

$a * e = e * a = a \quad \forall\ a \in G$.

(iii) Inverse : For any $a \in G$, $\exists\ a^{-1} \in G \Rightarrow$

$a * a^{-1} = a^{-1} * a = e$

Example. (i) $G = \{-1, 1\}$ $G \times G \rightarrow G$ by $a.b = ab$

It is a binary operation.

(i) $a.(b.c) = (a.b).c$

(ii) $a * 1 = 1 * a = a \Rightarrow$ 1 is an identity element.

(iii) $a * \frac{1}{a} = \frac{1}{a} * a = 1 \Rightarrow$ Inverse of 1 is 1
Inverse of -1 is -1

It is a group.

(ii) $G = \{1, -1, i, -i\}$ $G \times G \rightarrow G$ by $a.b = ab$.

It is a binary operation. $* \rightarrow \times$.

(i) $a.(b.c) = (a.b).c$

(ii) $a * 1 = 1 * a = a \Rightarrow$ 1 is an identity element.

(iii) $a * \frac{1}{a} = \frac{1}{a} * a = 1$

$a * a^{-1} = e$.

Inverse of 1 is 1
Inverse of -1 is -1
Inverse of i is $-i$
Inverse of $-i$ is i

$i \times -i = 1$.

$-i^2$

$-(-1) = 1$

It is a group.

(iii) $G : Z \quad Z \times Z \to Z \quad a * b = a + b$.

It is a binary operation.

$(1-2)-3$
$-1-3$
$1-(2-2)$
$1-0=1$

(iv) $a + b + ab$. $\quad a * (b * c) = (a * b) * c$.

LHS: $a * (b + c + bc)$

$a * A$.

$a + A + aA$

$a + b + c + bc + a(b + c + bc)$

$a + b + c + bc + ab + ac + abc$.

RHS: $(a + b + ab) * c$

$(a + b + ab) * C$

$B * c$.

$B + c + Bc$

$a + b + ab + c + ac + bc + abc$.

$-c(a+b-ab)$

~~$(a + b - ab) * e =$~~

$a * e = e * a = a$.

$a + e - ae = a$

$e(1 - a) = 0$.

$e = 0$.

$a * a^{-1} = a^{-1} * a = e$.

$a + a^{-1} - aa^{-1} = 0$.

$a + a^{-1}(1 - a) = 0$.

$a^{-1} = \frac{-a}{1-a}$

A group satisfying all the conditions including commutativity is called Abelian group.

commutativity - $a*b = b*a \quad \forall\ a, b \in G$.

Consider G = Set of all 2×2 invertible ($\det \neq 0$) matrices under R

$* : G \times G \to G$ defined by $A * B = AB$.

(i) $(AB)C = A(BC)$

(ii) $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

(iii) $A^{-1} = \frac{1}{|A|} \text{adj} A$.

It is a Group.

Commutative law is false. $(AB \neq BA)$

∴ It is not an Abilian group.

G: Set of all bijective functions $f : R \to R$.

$* : G \times G \to G$ defined by $f * g = f \circ g$

(i) $(f \circ g) \circ h = f \circ (g \circ h)$

(ii) Identity: $e : R \to R$ defined by $e(x) = x \ \forall$

$e * f = e \circ f = e(f(x)) = f(x)$

$f * e = f \circ e = f(e(x)) = f(x)$

(iii) Inverse exists.

It is a group but not an abilian group ($\because fog \neq$

Give an example of a finite non-abliun group.

Examples of group:

$(Z_n, \oplus_n)$, $(Z_p - \{0\}, \odot_p)$, $GL_2(R)$ - General linear group - set of all 2×2 invertible matrices entries in R under multiplication

(p prime)

$(GL_2(R), \bullet)$ - infinite non abelian group.

$GL_n(F)$ → F - non-empty set
$n \times n$ - mat

$GL_2(R)$ $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$GL_2(Z)$ $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}^{-1} = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1/2 & -1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\notin GL_2(Z)$

$\therefore (GL_2(Z), \odot)$ not a group [but monoid]

$(G, *)$ - only associative law is true ⇒ semi group.

$(G, *)$ - associative + identity ⇒ monoid

Properties of group:

* It satisfies left cancellation & right cancellation.

In a group $(G, *)$ ⇒ $ab = ac \Rightarrow b = c$ [L.C]
$ba = ca \Rightarrow b = c$ [R.C]

Proof. Assume $ab = ac \rightarrow (1)$

Since GL is a group $a^{-1} \in G$.

Multiply (1) by a^{-1} on both sides.

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$ [∵ associative law is true]

$eb = ec$

$\Rightarrow b = c.$

R, C ⇒ Same as L, C.

Take $(N, +)$ it satisfies 1.C law & 2.C law but it is not a group.

$a+b = a+c \Rightarrow b = c$

$b+a = c+a \Rightarrow b = c$

A non-empty set satisfies 1.C law & 2.C law may not be a group.

* Let G be a group and $a, b \in G$. Then

$(ab)^{-1} = b^{-1}a^{-1}$ & $(a^{-1})^{-1} = a$ $\quad aa^{-1} = e$ $\quad a^{-1}a = e$

Proof: $(ab)(b^{-1}a^{-1})$ $\quad (ab)(b^{-1}a^{-1})$

$b^{-1}(a^{-1}a)b$ $\quad a(bb^{-1})a^{-1}$

$b^{-1}eb$ $\quad aea^{-1}$

$b^{-1}b$ $\quad aa^{-1}$

e $\quad e$

$a^{-1}a = aa^{-1} = e$

$\Rightarrow$ inverse of a^{-1} is a. $\Rightarrow (a^{-1})^{-1} = a$.

* Let G be a group and $a \in G$ for any +ve int n

$a^n = a * a * a * \dots * a$ (n times)

Note: $a^{-n} = (a^n)^{-1} = (a^{-1})^n$

* An element is called idempotent when

$a^2 = a \Rightarrow a+a = a$.

$(R, +)$ $\quad a+a = a \Rightarrow 0$ is idempotent.

$(R-\{0\}, \cdot)$ $\quad a.a = a \Rightarrow 1$ is idempotent.

%% Example of an finite group having more than one elements in which idempotent
Example of an infinite group in which every element is ↑
Example of a group in which every element is idempotent

03/03/2022

ASSIGNMENT TUTORIAL

ALGEBRA AND NUMBER THEORY

1) Set of odd integers under addition is not a group.

Because,

* Binary operation is not satisfied.
* And if we add two odd integers, the resultant will be an even number which does not belongs to the group. identity & inverse does not exist

---

2) Let the 2x2 matrices with entries from be

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \quad B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \quad C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

(*) Binary operation is satisfied.

* Associative : $A * (B * C) = (A * B) * C$.

LHS: $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} * \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} * \begin{bmatrix} a_2a_3 - b_2c_3 & a_2b_3 - b_2d_3 \\ a_3c_2 - c_3d_2 & c_2b_3 + d_2d_3 \end{bmatrix}$$

$a_1a_2a_3 - a_1b_2c_3$

Matrix Multiplication satisfied associative property.

Binary:
$\det A = 1$
$\det B = 1$
$\det(AB) = \det A \det B$
$= 1$
$\therefore AB \in GL$.

* Identity : Let E be the identity matrix.

$A * E = E * A = A$.

$\therefore$ The identity matrix is $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

* Inverse : Let A^{-1} be the inverse of A.

$A * A^{-1} = A^{-1} * A = E$.

$\therefore$ Inverse of $A = \frac{1}{|A|}[(adj A)]$

$AA^{-1} = A^{-1}A = I$
$\det(A^{-1}) = \frac{1}{\det A}$
$= 1$

From the above three conditions, the set of all 2×2 matrices with entries R is a group under matrix multiplication. Hence, proved.

---

3) Given : $\{5, 15, 25, 35\}$

(*) binary operation is satisfied.

* Associative : $a * (b * c) = (a * b) * c$.

Let $5 \times_{40} (15 \times_{40} 25) = (5 \times_{40} 15) \times_{40} 25$

$5 \times_{40} 15 = 35 \times_{40} 25$

$35 = 35$.

$\therefore$ Associative property is true.

* Identity :

$a * e = e * a = a$.

$5 \times_{40} 25 = 5$

$15 \times_{40} 25 = 15$

$25 \times_{40} 25 = 25$

$35 \times_{40} 25 = 35$

~~$\therefore$ Identity element is I which ∈ group~~

$\therefore$ Identity element is 25.

* Inverse :

$a * a^{-1} = a^{-1} * a = e$.

$a * a^{-1} = e$.

$5 \times_{40} 5 = 25$

$15 \times_{40} 15 = 25$

$25 \times_{40} 25 = 25$

$35 \times_{40} 35 = 25$

$\therefore$ Inverse of a is itself.

$\therefore$ The given set is a group.

4) Group with 105 elements.

$G_1 : (Z_{105}, \oplus_{105})$ Integers under modulo addition.

Group with 44 elements.

dihedral group $G_1 : (Z_{44}, \oplus_{44})$ Integers under modulo addition.

~~$G_1 : (Z_{43}, \odot_{43})$ Integers under modulo multiplication~~

---

5) Set of all rational numbers of the form $3^m 6^n$ (*) the binary operation is satisfied.

* Associative : Multiplication satisfies associative property.

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

$\therefore$ It is true.

* Identity : $a * e = e * a = a$.

$a = 3^{m_1} 6^{n_1}$

$b = 3^{m_2} 6^{n_2}$

$ab = 3^{m_1+m_2} 6^{n_1+n_2}$

$\therefore$ The identity element is 1.

* Inverse :

$a * a^{-1} = a^{-1} * a = e.$

$a^{-1} = \frac{1}{a}$

$\therefore$ Inverse of a is $\frac{1}{a}$

$\therefore$ From the above conditions, the set of all rational numbers of the form $3^m 6^n$ is a group.

---

6) Given : $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ Lower triangular matrices

* binary operation is satisfied. Heisenberg group.

* **Associative :**

W.K.T. Matrix Multiplication satisfies associative property. $A * (B * C) = (A * B) * C$.

* **Identity :**

Let E be the identity matrix.

$$A * E = E * A = A.$$

$$= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

$$= A.$$

$\therefore E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is the identity matrix.

* **Inverse :** ~~matrix.~~

Let A^{-1} be the inverse of A.

$$A * A^{-1} = A^{-1} * A = E.$$

$$AA^{-1} = E.$$

$$A^{-1} = \frac{1}{|A|} (\text{adj } A)$$

$$|A| = \begin{vmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{vmatrix}$$

$$= 1(1-0) - a(0-0) + b(0-0)$$

$$= 1$$

$$(\text{adj } A) = \begin{bmatrix} 1 & c & 0 & 1 \\ 0 & 1 & 0 & 0 \\ a & b & 1 & a \\ 1 & c & 0 & 1 \end{bmatrix}^T$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ ac-b & -c & -a \end{bmatrix}^T$$

$$\therefore A^{-1} = \frac{1}{1} \begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ ac-b & -c & -a \end{bmatrix}^T \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & -a \end{bmatrix}$$

∴ From the above conditions, set of all 3×3 matrices with real entries is a group.

---

7) consider a group of set of all whole numbers with the binary operation $a * b = a + b + ab$.

non-abelian group

G : (Real numbers) $G = \{R\}$

Given: $a^{-1} b a \neq b$.

Let $a = 2$, $b = 3$.

Inverse of a is $\frac{-2}{3}$ i.e a^{-1}.

$$\therefore a^{-1} b a = \frac{-2}{3} \times 3 \times 2 = -4\frac{13}{3}$$

$$b = 3.$$

$$-4 \neq 3.$$

∴ The group is set of all real numbers under the condition $a * b = a + b + ab$.

8) Given : $(ab)^{-1} = a^{-1}b^{-1}$ (1)

W.K.T. $(ab)^{-1} = b^{-1}a^{-1}$ (2)

From (1) & (2)

$a^{-1}b^{-1} = b^{-1}a^{-1}$

Taking inverses,

$(a^{-1}b^{-1})^{-1} = (b^{-1}a^{-1})^{-1}$

$(b^{-1})^{-1}(a^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1}$

$ba = ab$

Commutative property is true.

∴ The group G1 is an Abelian group.

---

9) $G1 = \{0, 1, 2\}$

$a * b = |a - b|$

$*$ is binary operation satisfied.

* Associative :

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

$a * (b * c) = a * |b - c|$

$= |a - |b - c||$

$(a * b) * c = ||a - b| - c|$

not associative.

$a = 2, b = 1, c = 1.$

not a group.

∴ Associative property is satisfied.

* Identity :

$a * e = e * a = a$

$|a - e| = a$

$a - e = a$

$-e = 0$

$e = 0$

$|a - e| = a$

$-(a - e) = a$

$-a + e = a$

$e = 2a \Rightarrow$ does not exist

∵ e value depends on a.

∴ Identity element is 0.

* Inverse :

$a * a^{-1} = e.$

$|a - a^{-1}| = 0$

Inverse of a is the element itself.

∴ The given G1 is group, Hence, proved.

Let $(H, \cdot)$ and $(K, *)$ be two groups

Let $(R, +)$ & $(R - \{0\}, \cdot)$

$(R \times R - \{0\}, \square)$

$(a_1, b_1) \square (a_2, b_2) = (a_1 + a_2, b_1 b_2)$

0 is the identity in I

1 is the identity in II.

$\therefore (0, 1)$ is the identity of $(R \times R - \{0\}, \square)$

Inverse: $(-a, \frac{1}{b})$

$(a, b) \square (c, d) = (a \oplus_2 c, b \oplus_2 d)$

$(Z_2 \times Z_2, \square)$ $Z_2 = \{0, 1\}$ Binary operation: $\oplus_2$

(Idempotent) $(a^2 = a)$

$Z_2 \times Z_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

Group: Klean's - 4 - group. (Self - inverse)

finite abelian group. $(a^2 = e)$

Subgroup:

$(Z, +)$ is a subgroup of $(R, +)$ & $(C, +)$

Example of a group which has infinite no. of sub groups

* $(Z, +)$ has infinite no. of sub groups of the form $(nZ, +)$ where $n \in Z$.
* Every finite group has a finite number of sub groups.
* $(e, *)$ is a trivial sub group of G.
* G itself is a sub group of $(G, *)$
* A group $H \subseteq G$ is called a proper sub group of G, $H \neq \{e\}, G$.

Necessary and Sufficient condition for a non empty sub set

6m · A nonempty subset H of a group G is a group if and only if $ab^{-1} \in H$ for all $a, b \in H$.

G - group, $H \neq \phi$ and $H \in G$, H is a subset $\Leftrightarrow ab^{-1} \in H$. $\forall a, b \in H$

1) G = Set of all 2×2 matrices entries in R under addition $M_2(R)$

H : Set of all 2×2 matrices entries in R having trace $= 0$.

Trace of A : sum of the diagonal entries.

Prove that H is a sub group of G.

Let $A, B \in H$. Then trace of $A = 0$ and trace of $B = 0$.

To prove: $A + B^{-1} \in H$. i.e trace of $A + B^{-1} = 0$.

W.K.T' Trace $(A+B)$ = trace (A) + trace (B)

$\Rightarrow$ Trace $(A+B^{-1})$ = trace of A + trace of B^{-1}

$= 0 + 0$.

$= 0$.

trace of B^{-1} = trace of B

$\therefore$ H is a sub group of G.

2) Prove that H is a sub group of G.

$G = GL_2(R) = GL(R, 2)$

$H = \{A \in GL_2(R) : A = A^T\}$

= collection of all symmetric matrices.

To prove: $AB^{-1} \in H \ \forall \ A, B \in H$.

i.e. $AB^{-1} = (AB^{-1})^T$

Let $A, B \in H$. Then $A = A^T$, $B = B^T$, $B^{-1} = (B^T)^{-1} = (B^{-1})^T$

Then $(AB^{-1})^T = (B^{-1})^T A^T = B^{-1} A$.

$\neq AB^{-1}$.

$\therefore$ H is not a sub group of G.

3) $G = M_2 R$ under addition.

$H = \{A \in M_2(R) : A = A^T\}$

Prove that H is a sub group of G.

To prove: $AB^{-1} \in H$ i.e $A + B^{-1} \in H$. i.e $A - B \in H$.

$(A-B)^T = A - B$.

$(A-B)^T = A^T - B^T = A - B$.

$\therefore$ It is a sub group.

4) $G = GL_2(R)$

$H = \{A \in GL_2(R) : \det(A) = 1\}$

Prove that H is a sub group of G.

T.P. $AB^{-1} \in H$.

i.e $\det(AB^{-1}) \in H$.

Let $A, B \in H$. $\det A = 1$, $\det B = 1$, $\det B^{-1} = \frac{1}{\det B} = 1$.

$\det(AB^{-1}) = \det(A) \cdot \det(B^{-1})$

$= 1 \cdot 1$

$= 1$. It is a sub group.

5) $G = GL_2(R)$ [multiplication]

$H = \{A \in GL_2(R) \mid A = -A^T\}$

= collection of all asymmetric matrices.

Verify H is a sub group or not?

T.P. $AB^T \in H$. $\forall$ $A, B \in H$.

$A = -A^T$, $B = -B^T$, $B^{-1} = (-B^T)^{-1} = (-B^{-1})^T$

$= -(B^{-1})^T$

$AB^{-1} = (-AB^{-1})^T$

$= (B^{-1})^T(-A^T)$

$= B^{-1}A$.

$\neq AB^{-1}$

$A + B^{-1} = -(A + B^{-1})^T$

$= -(A - B)^T$

$= -A^T + B^T$

$= +A - B$.

6) $G = (Z, +)$

H = Set of all even integers.

It is a sub group.

7) $G = (Z, +)$

H = Set of all multiples of three.

It is a sub group.

Union of two sub groups need not be a sub group

$G = (Z, +)$

$H = 2Z \cup 3Z$

↓ Union

It is not a sub group. $\because ab^{-1} \notin H$

Intersection of two sub groups is a sub group.

Proof:

Let H_1 & H_2 be two sub groups.

To prove: $H_1 \cap H_2$ is a sub group.

Let $a, b \in H_1 \cap H_2$ then $a, b \in H_1$ and $a, b \in H_2$

claim: $ab^{-1} \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1$ & $ab^{-1} \in H_2$

$Z(G) \rightarrow$ centre of G.

$Z(G) = \{a \in G : ax = xa, \forall x \in G\}$

$G = (GL_2(R), 2)$ $\quad Z(G) = \left\{\begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} k \in R\right\}$

↳ Prove that $Z(G)$ is a sub group.

To prove: $ab^{-1} \in Z(G)$

Let $a, b \in Z(G)$

$\Rightarrow ax = xa$

$bx = xb$.

Multiply b^{-1}

$b^{-1}bx = b^{-1}xb$.

$x = b^{-1}xb$

$xb^{-1} = b^{-1}xbb^{-1}$

$xb^{-1} = b^{-1}x$

To prove:

$(ab^{-1})x = x(ab^{-1})$

$(ab^{-1})x = a(b^{-1}x)$

$(ab^{-1})x = a(xb^{-1})$

$(ab^{-1})x = (ab^{-1})x$

$\therefore$ It is a sub group

Find $Z(G)$ for the following groups.

1) Klean's 4 group. $Z(G)$ is G itself for both groups. ∵ they are abelian groups.
2) $(Z_5, \oplus)$

Let A, B be two subsets of a group G we define

$$AB = \{ab : a \in A \text{ and } b \in B\}$$

※ Theorem : Let A and B be 2 subgroups of a group G. Then AB is a subgroup of G if and only if $AB = BA$.

Let G be a group and $a \in G$, then

$N(a) = \{x : x \in G \text{ and } ax = xa\}$ is called the normaliser of a in G.

Prove $N(a)$ is a sub group.

$xy^{-1} \in N(a) \quad \forall\ x, y \in N(a)$

Let $x, y \in N(a)$ Then $xa = ax$

$ya = ay$

$a = y^{-1}ay$

$ay^{-1} = y^{-1}a.$

$(xy^{-1})a = a(xy^{-1})$

LHS : $x(y^{-1}a)$

$x(ay^{-1})$

$(xa)y^{-1}$

$(ax)y^{-1}$

$a(xy^{-1})$

RHS.

G - Group

$a \in G$, $\langle a \rangle$ - sub group generated by a

$\langle a \rangle = \{ a^n \mid n \in Z \}$

$= \{ a^0 = e, a, a^2, \ldots, a^{-1}, a^{-2}, a^{-3} \} \subseteq G$

$G = (Z, +)$

$\langle 1 \rangle = \{0, 1, 2, \ldots -1, -2, \ldots\} = (Z, +)$

$\langle n \rangle = (nZ, +)$

Prove $\langle a \rangle$ is a sub group.

Let $H = \langle a \rangle$

Proof: $e \in \langle a \rangle$, $\langle a \rangle \neq \phi$ ⇒ $\langle a \rangle$ is a non-empty set.

$\because a^0 = e.$

Let $x = a^r$ and $y = a^s$

$xy^{-1} = a^r (a^s)^{-1} = a^r a^{-s} = a^{r-s} \in \langle a \rangle$

$\therefore xy^{-1} \in H.$

$\therefore \langle a \rangle$ is a sub group of G.

Cyclic sub group.

$\langle a \rangle$ - cyclic sub group.

G is cyclic group ⇔ $\langle a \rangle = G$

Ex.

$(Z, +)$ is cyclic group, $\langle 1 \rangle = \langle -1 \rangle$ are cyclic subgroups

Ex.

$(Z_4, \oplus_4) = \{0, 1, 2, 3\}$ → cyclic

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0, 1, 2, 3\} = (Z_4, \oplus_4)$

$\langle 2 \rangle = \{0, 2\}$

$\langle 3 \rangle = \{0, 1, 2, 3\} = (Z_4, \oplus_4)$

X. Any elements which is less than relatively prime by n.

Cyclic sub groups:

$(Z_4, \oplus_4)$ - cyclic generators = 1, 3.

$(Z, +)$ - cyclic generators = 1, -1

$(Z_n, \oplus_n)$ - cyclic generators = 1

$(Z_{12}, \oplus_{12})$ - cyclic generators = 1, 5, 7, 11

What are the generators of $(Z_n, \oplus_n)$?

Set of all elements less than n and relatively prime to n.

$(Z_p, \oplus_p)$ have $p-1$ generators. : $\{1, 2, \ldots p-1\}$

p- prime

$(Z_n, \oplus_n)$ (phi)

No. of generators of $(Z_n, \oplus_n) = \phi(n)$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$$

$(Z_{1000}, \oplus_{1000})$ $n = 1000$.

$1000 = 2^3 \cdot 5^3$

$\phi(1000) = (2^3 - 2^2)(5^3 - 5^2)$

$= (8-4)(125-25)$

$= 400$

$\therefore$ 400 generators are there in $(Z_{1000}, \oplus_{1000})$

$(Z_{720}, \oplus_{720})$ $n = 720$.

$720 = 2^4 3^2 5$.

$\phi(720) = (2^4 - 2^3)(3^2 - 3)(5-1)$

$= (16-8)(9-3)(4)$

$= 8 \times 6 \times 4$

$= 192$

720
2 360
2 180
2 90
5 45
3 9
3 3
1

8 x 6
48 x 4
192

Klean's 4 group is not a cyclic group.

$(Z_2 \times Z_2, \square)$

$(a,b) \square (c,d) = (a \oplus_2 c, b \oplus_2 d)$

$(Z_2 \times Z_2) = \{(0,0), (0,1), (1,0), (1,1)\}$

$\langle (0,0) \rangle = \{(0,0)\}$

$\langle (1,0) \rangle = \{(0,0), (1,0)\}$

$\langle (0,1) \rangle = \{(0,0), (0,1)\}$

$\langle (1,1) \rangle = \{(0,0), (1,1)\}$

Order of G1 $O(G)$:

Order of G is the no. of elements in G.

Order of an element $O(a)$:

$\boxed{a^n = e}$, $n \rightarrow$ least +ve integer.

$(Z_4, \oplus_4) = \{0, 1, 2, 3\}$

$0^1 = 0$ order = 1

$1^4 = 0$ order = 4

$2^2 = 0$ order = 2

$3^4 = 0$ order = 4

$0 \oplus_4 0 = 0$.

$1 \oplus_4 3 = 0$

$2 \oplus_4 2 = 0$.

$3 \oplus_4 1 = 0$.

Inverses.

$1 \oplus_4 3 = 0$

$4 \oplus_4 2 = 2$

$3 \oplus_4 1 = 3$

01/3/2022

ASSIGNMENT TUTORIAL - II

ALGEBRA AND NUMBER THEORY.

8) State and prove Necessary and Sufficient condition for a non-empty set to be a sub group.

Statement: A non-empty subset H of the group G is a sub group if and only if $ab^{-1} \in H$ such that for all $a, b \in H$.

Proof:

A non-empty set H consists of a and b.

Conversely, we assume that $ab^{-1} \in H \ \forall \ a, b \in H$.

This implies, let $a \in H$.

$$a a^{-1} = e \in H.$$

and hence, $e a^{-1} = a^{-1} \in H$.

If a and $a^{-1} \in H$ then $a, b^{-1} \in H$.

But our assumption is,

$$a (b^{-1})^{-1} = ab \in H.$$

$$\Rightarrow H \subseteq G.$$

$\therefore$ H is a sub-group of G if and only if $ab^{-1} \in H \ \forall \ a, b \in H$.

1) Given:

$G : (\mathbb{Z}, +)$

To find:

H which contains 18, 30 and 40.

$H : (2\mathbb{Z}, +)$ which contains 18, 30 and 40.

To find:

finite sub groups of R^*.

$ab^{-1} \in H$.

$a^2 + b^2 = 1$

$R^* : (R - \{0\})$

$a^2 + (b^2)^{-1}$

(i) $\{1, -1\}$

$a^2 + b^{-2}$

(ii) $\{1\}$

$ab^{-1} \in H$

Given:

$G : GL_2(R)$

$H = \{A \in GL_2(R) \mid \det A \text{ is an integer power of } 2\}$

$H = \{A \in GL_2(R) \mid |A| = 2^n\}$

Let $A, B \in H$. $|A| = 2^{n_1}$, $|B| = 2^{n_2}$

To prove: $AB^{-1} \in H$.

$|AB^{-1}| = 2^r$

$|AB^{-1}| = |A||B^{-1}|$

$= |A| \frac{1}{|B|}$

$= \frac{|A|}{|B|}$

$= \frac{2^{n_1}}{2^{n_2}}$

$= 2^{n_1 - n_2} \in H$.

$\therefore$ H is a sub group of G.

3) Given:

$G : C^*$

$H = \{a+bi \mid a, b \in R, a^2+b^2 = 1\}$

$a^2 + b^2 = 1$

$\Rightarrow |Z| = 1.$

Let $Z_1, Z_2 \in H$ then $|Z_1| = |Z_2| = 1$

To prove: $Z_1 Z_2^{-1} \in H.$

$$\frac{Z_1}{Z_2} \in H.$$

$$\left|\frac{Z_1}{Z_2}\right| = \frac{|Z_1|}{|Z_2|} = \frac{1}{1} = 1$$

$\therefore Z_1 Z_2^{-1} \in H.$

$\therefore$ H is a sub group of G.

Elements: complex numbers on the unit circle.

5) Given:

$G : \{M_2(Z), +\}$

$$H = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a+b+c+d = 0\right\}$$

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in H.$

Then $a_1 + b_1 + c_1 + d_1 = 0$ and $a_2 + b_2 + c_2 + d_2 = 0.$

To prove: $AB^{-1} \in H. \Rightarrow A - B \in H.$

$$A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ c_1 - c_2 & d_1 - d_2 \end{bmatrix} \in H.$$

Then $a_1 - a_2 + b_1 - b_2 + c_1 - c_2 + d_1 - d_2$

$$a_1 + b_1 + c_1 + d_1 - (a_2 + b_2 + c_2 + d_2)$$

$$0 - 0 = 0.$$

$\therefore$ H is a sub group of G.

If we replace 0 for 1, it is not a sub group.

G: $R \to R^*$

H: $\{ f \in G \mid f(2) = 1 \}$

Let $a, b \in H$.

$\therefore a(2) = 1 \quad , b(2) = 1.$

To prove: $ab^{-1} \in H$.

$$a(2)(b(2))^{-1} = \frac{a(2)}{b(2)} = \frac{1}{1} = 1$$

$\therefore ab^{-1} \in H.$

$\therefore$ H is a sub group of G.

Yes, 2 can be replaced with any real-number.

G: C

H: $\{ a+bi \mid a, b \in R, ab \geq 0 \}$

Let $x = a + bi \in H.$

Let $x = 1 + 0i \in H$

$(1)(0) \geq 0$

Let $y = 0 - 1i \in H$

$(0)(-1) \geq 0$ It is not equal.

$x + y = 1 - 1i \notin H$

as $1(-1)$ which is less than 0.

$\therefore$ H is not a sub group.

Fundamental theorem of cyclic groups:

Statement:

Every sub group of a cyclic group is cyclic.

Proof:

Let G be a cyclic group and let H be a sub group of G.

Then there exists an element $a \in G$ such that $\exists$

$\langle a \rangle = G.$ $\{a^0, a^1, a^2, \ldots$

$a^{-1}, a^{-2}, \ldots \}$

To prove: H is cyclic.

Suppose $H = \{e\}$, then H is cyclic.

Suppose $H \neq \{e\}$

Then there exists $b \neq e$ which $\in H \Rightarrow b \in G$.

$\Rightarrow b = a^t$ $\because \langle a \rangle = G$.
for some t.

Suppose t is negative, then $a^{-t} \in H$.

$\therefore$ H contains elements of the form a^t where t is +ve

Let a^m be the least such element $\in H$

Eg $5 = 2(2)+1$

Claim: $\langle a^m \rangle = H$.

Let $x \in H$, then $x \in G$.

$x = a^k$ for some k.

Let $k = mq + r$ remainder

Divisor, Quotient

$0 \leq r \leq m-1$

where $q, r \in N$.

$a^k = a^{mq+r}$

$a^k = a^{mq} \cdot a^r$

$\Rightarrow a^r = a^k a^{-mq}$

$a^r = x (a^m)^{-q} \in H$.

$\in H$

If $r = 0$,

$a^k = a^{mq}$.

$x = a^k = (a^m)^q$,

$\Rightarrow x = a^k = (a^m)^q$

$\therefore H$ is a cyclic.

$H = \{a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, a^4, a^5, a^{-5}, a^7, a^{-7}, \ldots\}$

2m

* Every cyclic group is abelian. But every abelian group is not a cyclic group. Ex Klean's - 4 group.

Proof:

Let G be a cyclic group. $\Rightarrow \langle a \rangle = G$, $a \in G$.

Claim:

G is abelian. i.e $xy = yx \ \forall \ x, y \in G$.

Let $x = a^m$ & $y = a^n$ for some m & n.

$xy = a^m a^n$ $\qquad yx = a^n . a^m$

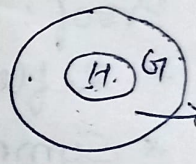
$xy = a^{m+n}$ $\qquad yx = a^{m+n}$

$\Rightarrow xy = yx$

$\therefore$ G is abelian.

Lagrange's theorem:

Definition: Right Coset



$a \in G$.

G - group, H - sub group

$H_a = \{ ha \mid h \in H \}$ $\qquad$ h*a

*Total no. of elements in H_a = $\forall a \in$

i.e $O(H) = O(Ha)$

Ex. $G = (\mathbb{Z}, +)$

$H = (3\mathbb{Z}, +)$

Let $a = 2$.

$H + 2 = \{ h + 2 \mid h \in H \}$

$3\mathbb{Z} + 2 = \{ 2, 5, -1, 8, -4 \ldots \}$

* $H = Ha \Leftrightarrow a \in H$.

if & only if