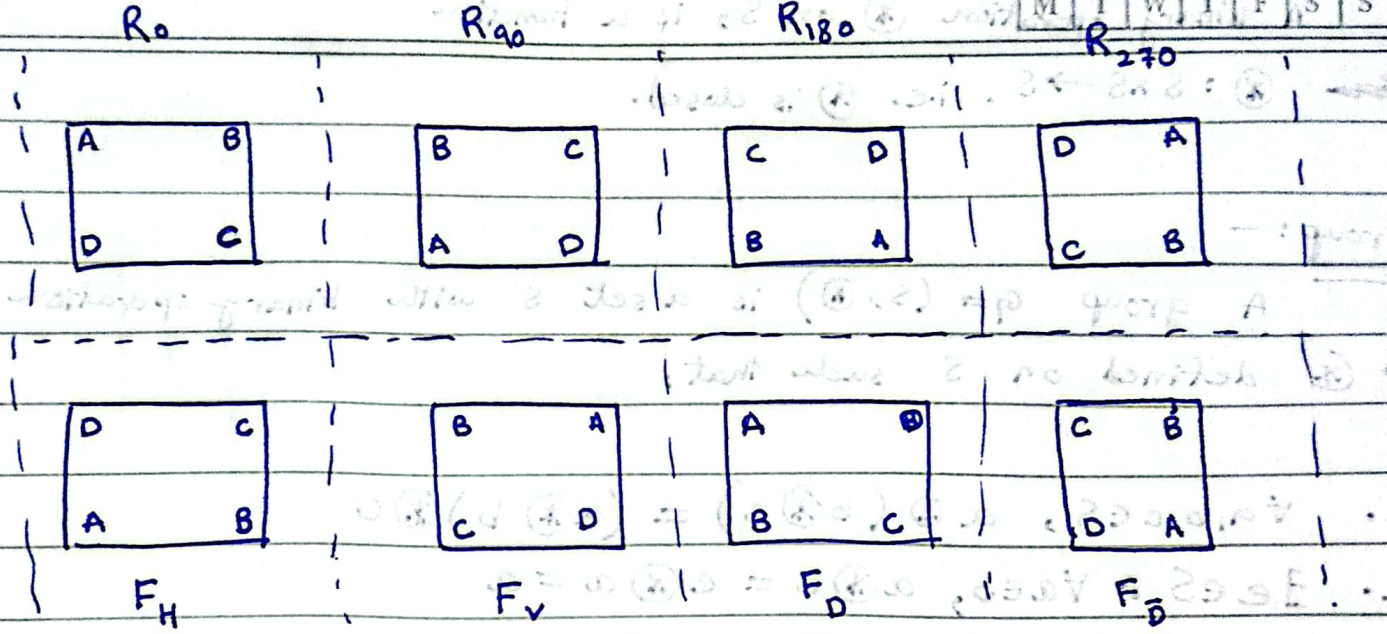
Abstract Algebra

Date 9/01/2024

M	T	W	T	F	S	S



First \ second	R_0	R_{90}	R_{180}	R_{270}	F_H	F_V	F_D	$F_{\bar{D}}$
R_0	R_0	R_{90}	R_{180}	R_{270}	F_H	F_V	F_D	$F_{\bar{D}}$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	F_D	$F_{\bar{D}}$	F_V	F_H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_V	F_H	$F_{\bar{D}}$	F_D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_{\bar{D}}$	F_D	F_H	F_V
F_H	F_H	$F_{\bar{D}}$	F_V	F_D	R_0	R	R	R
F_V	F_V	F_D	F_H	$F_{\bar{D}}$	R	R_0	R	R
F_D	F_D	F_H	$F_{\bar{D}}$	F_V	R	R	R_0	R
$F_{\bar{D}}$	$F_{\bar{D}}$	F_V	F_D	F_H	R	R	R	R_0

$D_{H4} := \{R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, F_{\bar{D}}\}$

Def

Binary operation:—

Date 11/01/2024

A binary operation $\circledast$ on S, is a function $\circledast : S \times S \to S$. i.e. $\circledast$ is closed.

Group:—

A group $G = (S, \circledast)$ is a set S with binary operation $\circledast$ defined on S such that,

1. $\forall a, b, c \in S,\ a \circledast (b \circledast c) = (a \circledast b) \circledast c$
2. $\exists e \in S \ni \forall a \in S,\ a \circledast e = e \circledast a = a$
3. $\forall a \in S, \exists b \in S \Rightarrow a \circledast b = b \circledast a = e$

Abelian Group:—

If in a group G, $a \circledast b = b \circledast a$ then G is called an Abelian Group, otherwise G is a non-Abelian group.

Example:- $G = \{1, -1, i, -i\}$ with usual multiplication.

•	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Example: $\mathbb{Z}_n := \{0, 1, 2, 3, \ldots, n-1\}$ is a group under addition modulo n.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Date
M T W T F S S

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}_n$ is accoslative over addition modulo n.

$$((a+b) \pmod n + c) \pmod n = (a + (b+c) \pmod n) \pmod n$$

$$\binom{n}{n-2} = \binom{n}{2} = \frac{n(n-1)}{2}$$

$$\binom{n}{1} = n$$

2^n

Date
M T W T F S S

Thm 1: In a group G, identity is always a unique element.

Thm 2: In a group, every element has a unique inverse.

Proof 1:– Lets suppose there are two identities $e, e' \in G$. $\forall a \in G, \exists$

$$ae = ea = a$$
$$ae' = e'a = a$$

$$e' = e'e = e$$

since e is identity.

since e' is identity

Proof 2:–

$$ab = e$$

Set of irrationals is not a group under addition, because it is not closed

Date 14/01/2024

M	T	W	T	F	S	S

Groups under addition:-

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_{n\in\mathbb{N}}$, $[\ ]_{n\times n;n\in\mathbb{N}}$

Groups under multiplication,

$\mathbb{Q}^*$, $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$, $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$

$$U(n) = \{x \mid x \pmod n \in \mathbb{Z} \wedge \gcd(x,n) = 1\}$$

$U(6) = \{1,5\}$

$U(10) = \{1,3,7,9\}$

Show that $\forall a,b \in U(n)$, $ab \in U(n)$, i.e. $\gcd(ab,n)=1$ then

Proof:-

Let $\gcd(ab,n) = r \neq 1$ then $r = p_1 p_2 \cdots p_n$, p_i is prime.

i.e.

$$p_i \mid r \Rightarrow p_i \mid n \Rightarrow p_i \mid ab \Rightarrow (p_i \mid a) \vee (p_i \mid b)$$
$$\Rightarrow \gcd(a,p_i) \neq 1 \vee \gcd(b,p_i) \neq 1$$
$$\Rightarrow \gcd(a,n) \neq 1 \vee \gcd(b,n) \neq 1$$

which is a contradiction.

Show that $\forall a \in U(n), \exists\, b \in U(n) \ni ab \pmod n \equiv 1$.

Proof,

$$\gcd(a,n) = 1 \Leftrightarrow \exists\, s,t \ni as + nt = 1 \Rightarrow \gcd(s,n) = 1$$

Let construct s such that,

$$S = \{s + nx \mid s + nx > 0,\ x \in \mathbb{Z}\}$$

b is the least element of S some unit shifted by s.

e - einheit - identitity.
german english

Date
M T W T F S S

Inverse of "a" can be written as a^{-1} (multiplicative group) and "$-a$" (additive group)

Similarly, $n \in \mathbb{Z}$

$a^n = \underbrace{a \cdot a \cdots a}_{n\text{-times}}$; a if $n < 0$, $a^n = (a^{-1})^{|n|}$, $a^0 = e$

$na = \underbrace{a+a+\cdots+a}_{n\text{-times}}$, $0a = e$, if $n<0$, $na = |n|(-a)$

Group of ~~roots of unities~~ roots of unity.

Order of a group:-

18/01/2024

If a group is finite, then order of the group is the number of elements in the group. If or number of elements are infinite, then the order is infinite.

Order of an element g:-

Order of an element g is the smallest positive n such that $g^n = e$.

If there doesn't exist such as n then order of g is infinite.

Order of $g := |g|$

Subgroup of a group:—

Let G be a ~~subs~~ group, let H be a subset of G, that forms a group under the operation of G, then H is called a subgroup of G. we write $H \leq G$.

Date
M T W T F S S

$|H| < |G| \iff H < G$ (Proper sub-group)

$|H| = |G| \iff H \leq G$ (Improper sub-group)

$\forall G$, $\{e\} \leq G$ called the trivial subgroup. ~~All trivial~~

All other subgroup are non-trivial.

sub group tests.

One-Step Test:—

~~If~~ If H is a subgroup G such that $\forall a, b \in H$, $ab^{-1} \in H$, then H is a subgroup of G.

$H \leq G \iff \forall a, b \in H,\ ab^{-1} \in H$

Proof:—

Lets ~~proof~~ prove,

$\forall a, b \in H,\ ab^{-1} \in H \implies H \leq G$.

Take, $a = b$, ~~b = a~~,

$ab^{-1} \in H \implies aa^{-1} = e \in H$

Take $a = e$,

$ab^{-1} \in H \implies (e)b^{-1} = b^{-1} \in H$

Take, ~~b = a~~ $a = x$, $b = y^{-1}$.

$ab^{-1} \in H \implies x(y^{-1})^{-1} = xy \in H$

Let G be an Abelian group with identity e, then $H = \{x \mid x^2 = e\}$ is a subgroup of G.

Date

M	T	W	T	F	S	S

$H \neq \emptyset$ since $e = e^2 \in H$. $\forall x, y \in H$, show that $xy^{-1} \in H$.

~~$xy^{-1} \in H$~~

$$\begin{aligned}(xy^{-1})^2 &= xy^{-1}xy^{-1} \\ &= xxy^{-1}y^{-1} \\ &= x^2(y^2)^{-1} \\ &= e(e)^{-1} \\ &= ee \\ &= e \in H\end{aligned}$$

In an abelian group G, $H = \{x^2 \mid x \in G\}$ is a subgroup.

Proof:-

$e^2 = e \in H$

~~Let~~ a.

$\forall a, b \in H$, $\exists x, y \ni a = x^2, b = y^2$.

$$\begin{aligned}ab^{-1} &= x^2(y^2)^{-1} \\ &= x^2(yy)^{-1} \\ &= x^2y^{-1}y^{-1} \\ &= xxy^{-1}y^{-1} \\ &= xy^{-1}xy^{-1} \\ &= (xy^{-1})^2 \in H\end{aligned}$$

2 Step Sub-group test:-

Date 23/01/2024

M	T	W	T	F	S	S

1. if $\forall a, b \in H$,

$$(ab \in H) \wedge (a^{-1} \in H) \iff H \leq G.$$

Eg:- For G Abelian,

$$H = \{a \in G \mid |a| \text{ is finite}\}$$

is a subgroup of G.

Proof:-

H is non-empty because it has element of finite order and identity has finite order.

if $a \in H$,

$$|a| = n$$
$$\Rightarrow a^n = e$$
$$\Rightarrow a^{n-1} = a^{-1}$$
$$\Rightarrow (a^{-1})^n = (a^n)^{-1} = e$$
$$\Rightarrow |a^{-1}| \text{ is finite,}$$
$$\Rightarrow a^{-1} \in H$$

if $a, b \in H$, let $|a| = n$, $|b| = m$,

$$(ab)^{mn} = a^{mn} b^{mn} = (a^n)^m (b^m)^n$$
$$= e^m e^n = e$$

Eg: For G Abelian, $H \leq G$, $K \leq G$,

$$HK = \{ hk \mid h \in H, k \in K \}$$

is a subgroup of G.

Proof:-

$$e \in H, e \in K \Rightarrow ee \in HK \Rightarrow e \in HK$$

$$hk \in HK \iff h \in H \wedge k \in K$$
$$\iff h^{-1} \in H \wedge k^{-1} \in K$$
$$\iff h^{-1}k^{-1} \in HK$$
$$\iff (kh)^{-1} \in HK$$
$$\iff (hk)^{-1} \in HK$$

$$h_1k_1, h_2k_2 \in HK \iff (h_1k_1)(h_2k_2) \in HK$$
$$\iff (h_1h_2)(k_1k_2) \in HK$$

Finite subgroup test:-

If $H \neq \emptyset$, $H \subseteq G$ is finite then if $\forall a, b \in H$, $ab \in H$, then $H \leq G$.

Proof:-

since $H \neq \emptyset$, $\exists a \in H \ni a, a^2, a^3, \ldots \in H$, since H is finite the sequence $a, a^2, a^3, \ldots$ does not contain all distinct elements.

$$\Rightarrow \exists\, i > j \in \mathbb{N} \ni a^i = a^j$$
$$\Rightarrow a^i (a^j)^{-1} \in G$$
$$\Rightarrow a^j (a^j)^{-1} \in G$$
$$\Rightarrow a^{i-j} \in G.$$

For $a \in G$,

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

Date
M T W T F S S

Proof:-

$e = a^0 \in \langle a \rangle$

$a^{-1} \in \langle a \rangle$

$\forall\, i, j,\ a^i, a^j \in \langle a \rangle \iff a^i a^j = a^{i+j} \in G.$

$\langle a \rangle$ is a group.

$\Leftrightarrow$

Def:-

If $\exists\, a \in G \ni G = \langle a \rangle$, the G is called cyclic group and a is called a generator of G.

Thm:-

Every cyclic group is Abelian.

Proof:-

If $G = \langle a \rangle$

$\forall\, i, j \in \mathbb{Z},\ a^i a^j \in \langle a \rangle$

$\Leftrightarrow a^{i+j} \in \langle a \rangle$

$\Leftrightarrow a^{j+i} \in \langle a \rangle$

$\Leftrightarrow a^j a^i \in \langle a \rangle$

D_n: Dihedral group over n regular polygon.

D_n is the group of symmetries of n-gon.

$|D_n| = 2n$

$R = R_{360/n}$ anticlockwise rotation.

$\langle R_{360/n} \rangle$ = subgroup of D_n with all possible rotations.

$R^n = e$, $R^{-1} = R^{n-1}$

Page No. _____ RC Signature _____

Def: If G is a group. $S \subseteq G$.

$\langle S \rangle :=$ the smallest subgroup of G containing S.

Date: M T W T F S S

if $S \subseteq H$ and $H \leq G$, then $\langle S \rangle \leq H$.

In $\mathbb{Z}_{10}$, $\langle 2, 3 \rangle = \mathbb{Z}_{10}$,

$\langle 2, 6 \rangle \neq \mathbb{Z}_{10}$.

In $\mathbb{Z}_{20}$, $\langle 8, 14 \rangle = \langle 2 \rangle$ 25/01/2024

In $\mathbb{Z}$, $\langle 5, 8 \rangle = \mathbb{Z}$

In D_4, $\langle R_{90}, F_V \rangle = \{ R_{90}, R_{180}, R_{270}, R_0, F_V, F_H, F_D, F_{\bar{D}} \} = D_4$

Def: centre of a group G, $Z(G) := \{ x \mid \in x \in G, \forall a \in G, xa = ax \}$

↳ centre → Zentrum (in German).

Proof: $Z(G) \leq G$.

Identity commutes with each element, therefore it is in $Z(G)$.

~~$\forall a \in Z(G), \forall b \in G, ab \in Z(G) \Rightarrow ab \in G$.~~ (closure).

~~$\forall a \in Z(G), \exists a^{-1} \in G, aa^{-1} = e$~~

~~$\forall a \in Z(G), \exists a^{-1} \in G, \ni aa^{-1} = a^{-1}a \Rightarrow a^{-1} \in G \Rightarrow a^{-1} \in Z(G)$~~

$\forall a \in Z(G)$, ~~$ax = xa$~~ $\forall x \in G$, $ax = xa$

$\Leftrightarrow axa^{-1} = xaa^{-1}$

$\Leftrightarrow a^{-1}axa^{-1} = a^{-1}xe$

$\Leftrightarrow exa^{-1} = a^{-1}x$

$\Leftrightarrow xa^{-1} = a^{-1}x$

$\Rightarrow a^{-1} \in Z(G)$

~~$\forall a \in G, \Rightarrow ac$~~

$\forall a, b \in Z(G)$, $\forall c \in G$, $ac = ca$, $bc = cb$,

$(ab)c = abc = a(bc) = a(cb)$

$= acb = (ac)b = (ca)b = cab = c(ab)$

$\Rightarrow ab \in Z(G)$

For D_n, where $n \geq 3$,

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\}, \text{ where } n \text{ is even.} \\ \{R_0\}, \text{ where } n \text{ is odd.} \end{cases}$$

Proof:-

R_0 is identity, it commutes with every element. Let R be a reflection and F be any reflection in D_n. We can argue that

$$R_\alpha R_\beta = R_{\alpha+\beta}$$
$$= R_{\beta+\alpha}$$
$$= R_\beta R_\alpha$$

Now, RF will always give us reflection, because reflection happens at an axis and then rotating the reflection rotates the axis, which makes it a different reflection.

Inverse of a reflection is the reflection itself.

$$RF = (RF)^{-1}$$
$$RF = F^{-1}R^{-1}$$
$$RF = FR^{-1}$$

$RF = FR \Leftrightarrow FR^{-1} = FR \Leftrightarrow R^{-1} = R$

This only happen in.

$R_{\frac{k360}{n}} \times R_{\frac{(n-k)360}{n}} = R_0$

when $n = 0, 1$.

Def:- Centralizer of $a \in G$,

$$C(a) := \{x \mid x \in G, xa = ax\}$$

Date: M T W T F S S

$a \in C(a)$, $ae = ea \Rightarrow e \in C(a)$.

$\forall x \in G$, $xa = ax \Leftrightarrow a^{-1}x = xa^{-1}$

$\forall a, b \in G$, ~~$abab = baba$~~, $bc \in C(a)$
$ca = ac$ & $ba = ab$ $\Leftrightarrow$

1. ~~$Z(G) \leq C(a)$~~ $\forall a \in G$, $Z(G) \leq C(a)$
2. $\forall a \in G$, $C(a) = G \Leftrightarrow G$ is Abelian.

Thm: 4.1 :- 30/01/2024

Criterion for $a^i = a^j$,

(1) If $|a|$ G is infinite, $a^i = a^j$ iff $i = j$.

(2) If $|a|$ is finite then $a^i = a^j$ iff $i - j$ is divisble by $|a|$.

Proof:-

(1) If $i = j$ then $a^i = a^j$

If $a^i = a^j$ then $a^{i-j} = a^0 = e \Rightarrow i - j = 0$.

(2) If $i - j = nk$ then $i = nk + j$,

$$a^i = a^{nk+j}$$
$$a^i = a^{nk} a^j$$
$$a^i = e a^j$$
$$a^i = a^j$$

Let remainder of $i - j$ divided by n be some r.

$$i - j = nq + r \text{ , where } 0 \leq r < n$$
$$a^{i-j} = a^{nq+r} = a^r.$$

Since, n is the least positive integer such that $a^n = e$ and $r < n$, r must be 0.

Corollary 1:-

$|a| = |\langle a \rangle|$

Let $|a| = n$,

$a^i \neq a^j$ for $i \neq j$, $i, j < n$

$\Rightarrow |\langle a \rangle| = n$.

Let $|\langle a \rangle| = n$, then $\langle a \rangle = \{ e, a, a^2, \cdots, a^{n-1} \}$.

Corollary 2:-

if $a^k = e \Rightarrow |a| \mid k$ (→ divides.)

(↳ finite.)

Corollary 3:-

If $a, b \in G$, where G is finite and $ab = ba$,

$|ab| \mid |a||b|$

Proof:-

Let $|a| = m$ and $|b| = n$,

$(ab)^{mn} = (a^m)^n (b^n)^m$

$= e^n e^m$

$= e$

By Corollary 2,

$|ab| \mid mn = |ab| \mid |a||b|$

Thm. 4.2.

Let $|a| = n$, let $\gcd(k, n) = d$ then $\langle a^k \rangle = \langle a^d \rangle$ and $|a^k| = n/d$.

Proof:-

$\langle a^k \rangle \subseteq \langle a^d \rangle$

k is $\gcd(k, n)$ means, $\exists z \in \mathbb{Z} \ni k = zd$ then,

$a^{ki} \in \langle a^k \rangle \Rightarrow a^{d(iz)} \in \langle a^d \rangle$

$\langle a^d \rangle \subseteq \langle a^k \rangle$,

$\forall\, d_i$, $a^{d_i} \in \langle a^d \rangle$, since $d = \gcd(n,k)$

$\exists s,t,\ s \in \mathbb{Z} \Rightarrow d = ns + kt$

then, $a^d = a^{nst+kt} = a^{ns} a^{kt} = a^{kt} \in \langle a^k \rangle$

Hence, $\langle a^d \rangle = \langle a^k \rangle$.

Now, we will proove,

$$|a^k| = \frac{n}{d}$$

$$\Rightarrow (a^k)^{\frac{n}{d}} = (a^n)^{k/d}$$

$$= e^{k/d}$$

$$= e$$

$k/d \in \mathbb{Z}$ because d is $\gcd(n,k)$.

To show, n/d is smallest & positive integer. Let $i \in \mathbb{Z}^+$, $i < \frac{n}{d}$ we will show that $a^{ki} \neq e$

Since, $\langle a^k \rangle = \langle a^d \rangle$. We show $|\langle a^d \rangle| = \frac{n}{d}$,

$$(a^d)^{\frac{n}{d}} = e$$

Let $i < n/d$ such that $a^{di} = e$, but this means $di < n$ is a positive integer such that $a^{di} = e \Rightarrow n$ is not the order of a.

Corollaries:— 1/02/2024

1. In a finite cyclic group the order of any element divides the order of the group.

Proof:— $G = \langle a \rangle$, where $|a| = n$, $|a^k| = \frac{n}{\gcd(n,k)}$

2. $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(i,n) = \gcd(j,n)$ and $|\langle a^i \rangle| = |\langle a^j \rangle|$ iff $\gcd(i,n) = \gcd(j,n)$.

Date
M T W T F S S

Eg:- $|a| = 30$,

$\langle a^{14} \rangle = \langle a^{\gcd(30,14)} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, \cdots, a^{28}\}$

$\langle a^{27} \rangle = \langle a^{\gcd(27,30)} \rangle = \langle a^3 \rangle = \{e, a^3, a^6, \cdots, a^{27}\}$

$\langle a^{17} \rangle = \langle a^{\gcd(17,30)} \rangle = \langle a \rangle$

Eg:- $|a| = 1000$

$\langle a^{108} \rangle = \langle a^{\gcd(1000,108)} \rangle$

$\gcd(1000, 108) = \gcd(2^3 \times 5^3, 2^2 \times 3^3) = 4$

$\langle a^{108} \rangle = \langle a^4 \rangle$

Corollary 3:-

In a finite cyclic group, $G = \langle a \rangle$, $|a| = n$. All generators of G are a^k where $\gcd(k, n) = 1$.

Corollary 4:-

Generator of $\mathbb{Z}_n$ are k where $\gcd(k,n) = 1$.

Eg, $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

$U(50) = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49\}$

$U(50) = \langle 3 \rangle = \langle 27 \rangle = \langle 37 \rangle = \langle 33 \rangle = \langle 47 \rangle = \langle 23 \rangle = \langle 13 \rangle = \langle 17 \rangle$

FUNDAMENTAL THEOREM OF CYCLIC GROUPS:-

Every subgroup of a cyclic group is cyclic. Moreover if $|a| = n$, then order of any subgroup of $\langle a \rangle$ is a divisor of n, and for each divisor k of n, there is exactly one group of order k namely $\langle a^{n/k} \rangle$.

Proof of fundamental theorem:-

Let G be cyclic, H a subgroup of G.

Date

M	T	W	T	F	S	S

If $H = \langle e \rangle$, then we are done.

Let $b \in H$, $b \neq e$, then $b = a^j$ for some $j > 0$. (since, H is a subgroup, if $b \in H$, then $b^{-1} \in H$.)

There exists some $a^m \in H$ such that $m \in \mathbb{N}$ is the least positive number where $a^m \in H$.

claim : $H = \langle a^m \rangle$

Let $a^t \in H$, by division algorithm,

$$t = mq + r \quad \text{for some } r, q \in \mathbb{N}, \ 0 \leq r < m.$$

since, $a^t \in H$, $a^{mq} \in H$, then $a^{-mq} \in H$ and $a^t \cdot a^{-mq} \in H$

$a^{t-mq} = a^r \in H. \Rightarrow r = 0$ (the least element).

$\Rightarrow H = \langle a^m \rangle$

2nd Part:-

If $G = \langle a \rangle$, $|a| = n$, any subgroup $H \leq \langle a \rangle$ is cyclic and is generated by some a^n, that is $H = \langle a^m \rangle$.

$a^n = e \in H \Rightarrow n = mq$ for some q.

$\Rightarrow \gcd(n, m) = m$ which divides n.

3rd Part:-

Let k be any positive divisor of n. we will show that $\langle a^{n/k} \rangle$ is the only group of order k.

From 4.2. $|\langle a^{n/k} \rangle| = \dfrac{n}{\gcd(\frac{n}{k}, n)} = \dfrac{n}{n/k} = k.$

Now H be any subgroup of order k, then $H = \langle a^m \rangle$ where m divides n. $m = \gcd(m, n)$, then $k = |a^m| = |a^{\gcd(m,n)}|$

$= \dfrac{n}{\gcd(m,n)} = \dfrac{n}{m}.$

Page No.

$\Rightarrow k = \frac{n}{m} \Rightarrow m = \frac{n}{k}$.

Date 6/02/2024

M T W T F S S

~~Corollary:-~~

Example:- In $\mathbb{Z}_n$, for each positive divisor k of n $\langle \frac{n}{k} \rangle$ is the unique sub-group of order k.

Theorem:-

For a cyclic group of order n, for a k a divisor of n, number of elements ~~that generate other sub-group~~ of order k are, $|U(k)| = \#\, i$ such that $\gcd(i,k) = 1$.

$$\varphi(k) := \begin{cases} 1 & \text{if } k = 1 \\ |U(k)| & \text{otherwise.} \end{cases}$$

Proof:-

From fundamental theorem ~~of~~ there is a some $a \in G$ such that $|\langle a \rangle| = k$ for divisor of n. For any other element b of order k, $\langle b \rangle = \langle a \rangle$ by fundamental theorem.

For HW:- $\varphi(p^n) = p^n - p^{n-1}$

for. $\forall m, n$, $\gcd(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Theorem:- For a finite group of order n, ~~for a divisor of n~~ number of elements of order k is a multiple of $\varphi(k)$.

Proof:-

There is no element of order k then 0 is a multiple of $\varphi(k)$. we are done.

Otherwise, Let $a \in G$ such that $|a| = |\langle a \rangle| = k$, so $\langle a \rangle$ has $\varphi(k)$ generator. If there exists some $b \in G$ such that $b \notin \langle a \rangle$

with order k. Then $\langle b \rangle$ has $\varphi(k)$ generators.

We have to show that these generators are different.

Let $c \in \langle a \rangle$ and $c \in \langle b \rangle$ such that c is also a generator of $\langle a \rangle$ and $\langle b \rangle$ then, $\langle c \rangle = \langle a \rangle = \langle b \rangle$, which implies $b \in \langle a \rangle$, but we assumed $b \notin \langle a \rangle$; therefore a contradiction.

Date M T W T F S S

13/02/2024

Permutation Group.

Ordered set A, a permutation on element A is a bijective function on set A.

A permutation group of a set A is a group of permutations of A.

Although permutation on infinite sets exists, but we will only consider finite sets.

A permutation on a sets of ~~objects~~ objects can be considered a permutation of set $[n] = \{1, 2, 3, \cdots, n\}$.

~~Representation~~

A permutation is represented as : array,

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

means $1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1$.

composition of permutations,

Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{bmatrix}$, $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{bmatrix}$

RC Signature

$\alpha\beta$ is read right to left,

$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{bmatrix}$$

Date
M T W T F S S

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{bmatrix}$$

Example: S_3 the set of permutations on 3 elements under composition is a permutation

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \quad \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = \varepsilon$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \beta^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \quad \beta^2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = \varepsilon$$

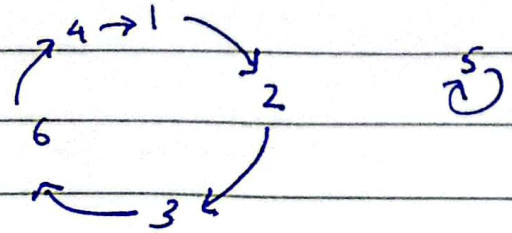
$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad \alpha\beta^2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

$$S_3 = \{ \varepsilon, \alpha, \alpha^2, \beta, \beta^2, \alpha\beta, \alpha\beta^2 \}$$

S_n is called the symmetry group of degree n is the group of all permutations on n element.

cycle notation for permutations: —

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 1 & 5 & 4 \end{bmatrix}$$



$\alpha = (1,2,3,6,4)(5)$

RC $\alpha = (3,6,4,1,2)(5)$

Page No.

Signature

Thm:- Every permutation can be written as a product of disjoint cycles.

Date 15/02/2024

Proof:-

Let $A = \{1, 2, 3, \dots, n\}$, let α be a permutation on A, let $a_1 \in A$,

Let $a_2 = \alpha(a_1)$, $a_3 = \alpha(a_2) = \alpha(\alpha(a_1)) = \alpha^2(a_1)$

$\dots$, $a_k = \alpha^{k-1}(a_1)$.

Claim, there exists m such that $\alpha_{m+1} = \alpha^m(a_1) = a_1$

The sequence $\{\alpha^k(a_1)\}_{k \in \mathbb{N}}$ is infinite, where as the set A is finite,

$\Rightarrow \exists\, i < j \ni \alpha^i(a_1) = \alpha^j(a_1)$

$\Rightarrow \alpha^{-i}(\alpha^i(a_1)) = \alpha^{-i}(\alpha^j(a_1))$

$\Rightarrow a_1 = \alpha^{j-i}(a_1)$

take $m = j - i$. Let m be the least natural number where this happens, then $\alpha = (a_1, a_2, \dots, a_n)$.

If there exist $b_1 \in A$ not in $(a_1, a_2, \dots, a_m)$, then we create a similar cycle using b_1,

$(b_1, \alpha(b_1), \alpha^2(b_1), \dots, \alpha^x(b_1))$

The cycles $(a_1, \alpha(a_1), \alpha^2(a_1), \dots, \alpha^p(a_1))$ and $(b_1, \alpha(b_1), \alpha^2(b_1), \dots, \alpha^q(b_1))$ are disjoint. Otherwise, $\alpha^i(a_1) = \alpha^j(b_1)$

$\Rightarrow \alpha^{i-j}(a_1) = b_1$

$\Rightarrow b_1 \in (a_1, \alpha(a_1), \alpha^2(a_1), \dots, \alpha^p(a_1))$

which is a contradiction. Continue this process till all elements of A are exhausted.

Thm:- Disjoint cycles commutes.

Thm:- If a permutation over finite sets written as a product of disjoint cycles. Then the order of the permutation is the L.C.M of the lengths of cycles.

Proof:-

1. A cycle of length n has order n.
2. Let α, β be disjoint cycles of length n and m respectively.

~~Let k = lcm(n, m)~~

$$(\alpha\beta)^k = \alpha^k \beta^k = \alpha^{\frac{mn}{\gcd(m,n)}} \beta^{\frac{mn}{\gcd(m,n)}}$$

$$= (\alpha^n)^{\frac{m}{\gcd(m,n)}} (\beta^m)^{\frac{n}{\gcd(m,n)}}$$

$$= \alpha^0 \beta^0$$

$$= (\alpha\beta)^0$$

3. Let $t \in \mathbb{N}$ be the order of $\alpha\beta$,

$$\Rightarrow (\alpha\beta)^t = (\alpha\beta)^0 \qquad (\forall z \in A, (\alpha\beta)^t(z) = \varepsilon)$$

$$\Rightarrow t \mid k$$

$$(\alpha\beta)^t = \alpha^t \beta^t = \alpha^0 \beta^0$$

$$= \alpha^t = \beta^{-t}$$

For this to be true,

$$\alpha^t(a_i) = a_{i+t \pmod n}$$

$$\beta^{-t}(a_i) = a_i$$

$$\Rightarrow a_i = a_{i+t \pmod n}$$

$$\Rightarrow n \mid t.$$

Similarly,

$$\alpha^t(b_i) = b_i$$

$$\beta^{-t}(b_i) = b_{i-t \pmod m}$$

$$b_i = b_{i-t \pmod m}$$

$$\Rightarrow m \mid t$$

Since,

~~If~~ $n \mid t$ and $m \mid t \Rightarrow t = \text{lcm}(m, n)$.

A cycle can be written as a product of 2-cycles (transpositions).

Date 20/02/2024

Eg: $(1\ 2\ 3\ 4\ 5)$

$= (1\ 5)(1\ 4)(1\ 3)(1\ 2)$

$= (5\ 4)(5\ 3)(5\ 2)(5\ 1)$

Eg: $(1\ 3\ 5\ 7)(2\ 6\ 4)$

$= (1\ 7)(1\ 5)(1\ 3)(2\ 4)(2\ 6)$

Thm. Every permutation in S_n, $n>1$ can be written as a product of 2-cycles.

Proof:-

A permutation in S_n is a product of disjoint cycles, say,

$(a_1\ a_2 \cdots a_r)(b_1\ b_2 \cdots b_s)(c_1\ c_2 \cdots c_t)$

Then the 2-cycles are;

$(a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1 a_2)\ (b_1\ b_s)(b_1\ b_{s-1}) \cdots (b_1\ b_2)\ (c_1\ c_t)$

$(c_1\ c_{t-1}) \cdots (c_1\ c_2)$

Lemma:- The identity permutation ε is always a product of even number of 2-cycles. i.e. if $\varepsilon = \beta_1 \beta_2 \cdots \beta_r$ where β_i is a 2-cycles then r is even.

Proof:-

- $\varepsilon \neq \beta_1$ for any β_1, since β_1 is a transposition, it swap places of two elements.
- ε can be written as a product of two 2-cycles, $\varepsilon = (ab)(a\ b)$
- Suppose $\varepsilon = \beta_1 \beta_2 \cdots \beta_r$ Let $\beta_r = (a\ b)$

Then, $\beta_{r-1}\beta_r$,

Case 1: $(a\ b)(a\ b) = (ab)(a\ b)$

Case 2: $(a\ c)(a\ b) = (a\ b)(c\ b)$

ease 3: $(b\ c)(a\ b) = (a\ c)(b\ c)$

Case 4: $(c\ d)(ab) = (a\ b)(c\ d)$

Signature

If case 1, then.
$\varepsilon = \beta_1 \beta_2 \cdots \beta_{r-2}$
where $r-2$ is even by hypothesis.

Date
M T W T F S S

Hypothesis; §

$\forall k < r$, $\varepsilon = \beta_1 \beta_2 \cdots \beta_k \Rightarrow k$ is even.

Induction step:

~~Case 1:~~

If case 1 than $\varepsilon = \beta_1 \beta_2 \cdots \beta_{r-2}$, where $r-2$ is even by hypothesis, that implies r is even.

In all case other than case 1, where $\beta_r = (a\ b)$, $\beta_{r-1}\beta_r$ ca be written in the form such that "a" appears only in β_{r-1} (2^{nd} right transposition).

Now we work with $\beta_{r-2}\beta_{r-1}$ we either have $\beta_{r-2}\beta_{r-1} = (a\ x)($ in which case $\varepsilon = \beta_1 \beta_2 \cdots \beta_{r-3}\beta_r$ is a product of 2-cycles wi less than r transpositions, which implies even # number of transpositions.

Or only β_{r-2} contains "a" in $\beta_{r-2}\beta_{r-1}$. we keep on going like this. Until we have that "a" only appear in β_1 but the ε is identitiy. §

RC

Signature

Theorem:- If α a permutation can be written as a product of even (odd) 2-cycles, then every representation of α as a product of 2-cycles has even (odd) transposition.

Date | M | T | W | T | F | S | S |

i.e. $\alpha = \beta_1 \beta_2 \cdots \beta_r$

$\beta = \gamma_1 \gamma_2 \cdots \gamma_s$

where β_i, γ_j transpositions then r and s have same parity.

Proof:-

$$\beta_1 \beta_2 \cdots \beta_r = \gamma_1 \gamma_2 \cdots \gamma_s$$

$$\varepsilon = \beta_1 \beta_2 \cdots \beta_r \cdot \gamma_s^{-1} \gamma_{s-1}^{-1} \cdots \gamma_1^{-1}$$

$$= \beta_1 \beta_2 \cdots \beta_r \cdot \gamma_s \gamma_{s-1} \cdots \gamma_1$$

By lemma s+r is even $\Rightarrow$ either s and r are even or odd.

Thm:- set of all even permutations form a group. 22/02/2024 (under composition).

Proof:-

1. Composition is associative.
2. Identity exists.
3. If $\alpha = \beta_1 \beta_2 \cdots \beta_r$, where β_i is a 2-cycles.

$$\alpha^{-1} = \beta_r^{-1} \beta_{r-1}^{-1} \cdots \beta_1^{-1}$$

$$\alpha^{-1} = \beta_r \beta_{r-1} \cdots \beta_1.$$

4. If α, γ are even then $\alpha\gamma$ ~~xxx~~ is even.

A_n: The alternating group over n symbols. The group of all even permutations over n-symbols.

Thm:- The number of even permutation = number of odd permutation over n symbols.

Proof:-

In any group G,

$\forall x \in G, xa = xb \Rightarrow a = b$

$\Leftrightarrow \quad a \neq b \Rightarrow xa \neq xb$

If α and β are two odd ~~eqates~~ permutations such that $\alpha \neq \beta$ then $(1\ 2)\alpha \neq (1\ 2)\beta$. are ~~non~~ even permutations, i.e. there are atleast as many even cycles as odd cycles.

Given α, β even $\neq$, $\alpha \neq \beta$, $(1\ 2)\alpha \neq (1\ 2)\beta$ and bothe $(1\ 2)\alpha$ and $(1\ 2)\beta$ are odd $\Rightarrow$ there are atleast as many odd cycles as even cycles.

Together we have the result.

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

A symmetric Polynomial over n variables is a polymial which doesn't change when any two variables are ~~same~~ swapped (transposed).

Example. $x_1, x_2 x_3$

$x^2 + 2xy + y^2$

An alternating polynomial is one where swapping any two variables gives the negative of the ~~original~~ original polynomial.

Example:- $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$

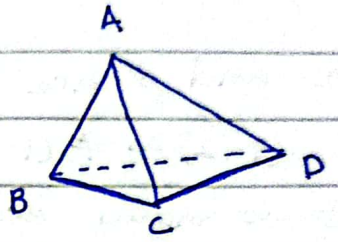
Symmetric polynomials invariant under elements of S_n.

Alternating polynomials are invariant under elements of A_n.

Date

M	T	W	T	F	S	S

Rotatations of Tetrahedron.



$\varepsilon = (A\ B)(A\ B)$

$(B\ C\ D) = (B\ D)(B\ C)$

$(B\ D\ C) = (B\ C)(B\ D)$

$(A\ C\ D) = (A\ D)(A\ C)$

$(A\ D\ C) = (A\ C)(A\ D)$

$(A\ B\ D) = (A\ B)(A\ B)$

$(A\ B\ B) = (A\ B)(A\ D)$

$(A\ B\ C) = (A\ C)(A\ B)$

~~$(A\ B\ C)$~~

$(A\ C\ B) = (A\ B)(A\ C)$

$(A\ B)(C\ D) =$ ~~A~~

$(A\ C)(B\ D)$

$(A\ D)(C\ B)$

Isomorphism:—

Given $G, \bar{G}$ groups an isomorphism is a bijective function $\varphi: G \to \bar{G}$ such that it preserves the structure of the group.

$$\varphi(ab) = \varphi(a)\,\varphi(b)$$

If such a function exists then we say G and $\bar{G}$ are isomorphic and write $G \approx \bar{G}$.

How to prove $G \approx \bar{G}$

1. A candidate function $\varphi: G \to \bar{G}$

Date 29/02/2024

M	T	W	T	F	S	S

2. Show φ is one-to-one (injective).

$\forall a, b \in G, \varphi(a) = \varphi(b) \iff a = b$

3. Show φ is onto,

$\forall \bar{g} \in \bar{G}, \exists g \in G \ni \varphi(g) = \bar{g}$

4. Show operation preserving.

$\forall a, b \in G, \varphi(ab) = \varphi(a)\,\varphi(b)$

Example:—

$(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ are isomorphic by $\varphi(x) = 2^x$

$$\varphi(a+b) = \varphi(a)\,\varphi(b)$$
$$2^{a+b} = 2^a 2^b$$
$$2^{a+b} = 2^{a+b}.$$

Example:—

Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$, by $\varphi(x^n) = n$.

~~$\forall a, b \in \langle x \rangle, \varphi(a^m) = \varphi(b^n) \iff a^m = b^n \iff a = b$~~

$\forall x^m, x^n \in \langle x \rangle, \varphi(x^m) = \varphi(x^n) \iff x^m = x^n$

$\forall n \in \mathbb{Z}, \exists x^n \in \langle x \rangle \ni \varphi(x^n) = n.$

$$\varphi(x^n x^m) = \varphi(x^{n+m}) = n + m = \varphi(x^n) + \varphi(x^m)$$

Example:- Any finite cyclic group of order n is $\langle x \rangle \ni |\langle x \rangle| = n$ is isomorphic to $\mathbb{Z}_n$, under $\varphi(x^k) = k \pmod n$

Example:

$(\mathbb{Q}, +)$ and $(\mathbb{Q} - \{0\}, \times)$ are not isomorphic.

Date
M T W T F S S

Cayley's Theorem (1854):

Every group is isomorphic to some permutation group.

Proof:—

Let G be any group, let $g \in G$ then $T_g : G \to G$

$T_g(x) = gx$. T_g is a permutation on G.

T_g is injective,

$$T_g(x) = T_g(y) \iff gx = gy$$
$$\iff x = y$$

$\forall y \in G$,

$$T_g(g^{-1}y) = y$$

Let $\bar{G} = \{ T_g \mid g \in G \}$ under function composition is a group.

$$\phi : G \to \bar{G}$$
$$\phi(g) = T_g$$

There is identity,

$$T_e T_g := T_e T_g(x) = T_g(T_g(x)) = T_e(gx) = egx$$
$$= gx = T_g(x)$$

There is a closure,

$$\forall T_g, T_h \in \bar{G}, \quad T_g T_h \in \bar{G}$$
$$T_g T_h(x) = T_g(T_h(x)) = T_g(hx) = ghx = T_{gh}(x)$$

Inverse also exists,

$\forall T_g \in \bar{G}$, $T_g^{-1} \in \bar{G}$ $\Rightarrow$ $T_g T_g^{-1} = e$.

Date 05/03/2024

It is also associative, because function composition is associative.

claim: $\varphi : G \to \bar{G}$ $\ni$ $\varphi(g) = T_g$ is isomorphism.

Proof:-

$$T_g = T_h \iff \forall x \in G,\ T_g(x) = T_h(x)$$
$$\iff gx = hx$$
$$\iff g = h$$

φ is injective and by construction it is surjective. φ is also operation preserving.

$$\varphi(gh) = \varphi(g)\varphi(h)$$
$$\Rightarrow T_{gh} = T_g(T_h)$$
$$T_{gh} = T_{gh}.$$

φ is an isomorphism. ▨

$U(12) = \{1, 5, 7, 11\}$

$\overline{U(12)} = \{T_1 = (5),\ T_5 = (1\ 5)(7\ 11),\ T_7 = (1\ 7)(5\ 11),\ T_{11} = (1\ 11)(5$

$U(12)$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\overline{U(12)}$	T_1	T_5	T_7	T_{11}
T_1	T_1	T_5	T_7	T_{11}
T_5	T_5	T_1	T_{11}	T_7
T_7	T_7	T_{11}	T_1	T_5
T_{11}	T_{11}	T_7	T_5	T_1

$\overline{U(12)}$ is called the regular left representation of $U(12)$.

Properties of Isomorphism acting on elements:—

If $\varphi: G \to \bar{G}$ is an isomorphism, then,

Date M T W T F S S

1. $\varphi(e) = \bar{e}$

$$\varphi(ee) = \varphi(e)\varphi(e) = \varphi(e)$$

$$[\varphi(e)]^{-1}\varphi(e)\varphi(e) = [\varphi(e)]^{-1}\varphi(e)$$

$$\varphi(e) = \bar{e}$$

2. $\forall n \in \mathbb{Z}$, $\varphi(a^n) = [\varphi(a)]^n$,

For $n \in \mathbb{Z}^+$, $\varphi(a^n) = \underbrace{\varphi(a)\varphi(a)\cdots\varphi(a)}_{n} = [\varphi(a)]^n$

For $n \in \mathbb{Z}^-$, $\varphi(a^{n-n}) = \varphi(e) = \bar{e}$

$$\varphi(a^n)\varphi(a^{-n}) = \bar{e}$$

$$\varphi(a^n)[\varphi(a)]^{-n} = \bar{e}$$

$$\varphi(a^n) = \bar{e}[\varphi(a)]^n$$

$$\varphi(a^n) = [\varphi(a)]^n$$

3. $\forall a, b \in G$, $ab = ba \iff \varphi(a)\varphi(b) = \varphi(b)\varphi(a)$.

$$ab = ba \Rightarrow \varphi(ab) = \varphi(ab)$$

$$= \varphi(ba)$$

$$\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$$

$$\varphi(a)\varphi(b) = \varphi(b)\varphi(a) \Leftrightarrow \varphi(a)\varphi(b)$$

$$\Rightarrow \varphi(ab) = \varphi(ba)$$

$$\Rightarrow ab = ba$$

This means abelian groups are only mapped to abelian groups.

4. $G = \langle a \rangle \iff \bar{G} = \langle \varphi(a) \rangle$

5. $\forall a \in G$, $|a| = |\varphi(a)|$

6. For any $b \in G$, $n \in \mathbb{Z}$, $x^n = b$ has the same numbers of solutions in G as $x^n = \varphi(b)$ in $\bar{G}$.

Date 4/03/2024

Proof:-

$\forall y \in G$, y is a solution of $x^n = b$, then $y^n = b$, $\varphi(y^n) = \varphi(b)$,

$[\varphi(y)]^n = \varphi(b)$.

7. If G is finite, then G and $\bar{G}$ have exactly same number of elements of any given order.

Thm 6.3: Properties of Isomorphism acting on groups:-

If $\varphi: G \to \bar{G}$ is an isomorphism, then

1. $\varphi^{-1}: \bar{G} \to G$ is an isomorphism.

Proof:-

φ is bijective then φ^{-1} is also bijective. Let $\forall \bar{a}, \bar{b} \in \bar{G}$ and, $\exists a, b \in G$ such that,

$$\varphi(a) = \bar{a} \iff a = \varphi^{-1}(\bar{a})$$

$$\varphi(b) = \bar{b} \iff b = \varphi^{-1}(\bar{b})$$

For operation preserving,

~~$\varphi(ab) = \varphi(a)\varphi(b)$~~

$$\varphi^{-1}(\bar{a})\varphi^{-1}(\bar{b}) = ab$$

$$\iff = \varphi^{-1}(\varphi(a)\varphi(b))$$

$$\iff \varphi^{-1}(a)\varphi^{-1}(\bar{b}) = \varphi^{-1}(\bar{a}\bar{b})$$

2. G is Abelian iff $\bar{G}$ is Abelian.
3. G is cyclic iff $\bar{G}$ is cyclic
4. Subgroup map to subgroups.

$K \leq G \Rightarrow \varphi(K) := \{\varphi(k) \mid k \in K\} \leq \bar{G}$

5. $\bar{K} \leq \bar{G} \Rightarrow \varphi^{-1}(K) \leq G$.

6. $\varphi(Z(G)) = Z(G)$

~~Example:~~

Date
M T W T F S S

Automorphism:-

12/03/2024

An isomorphism from a group to itself is called an automorphism.

$\varphi : (\mathbb{C}, +) \longrightarrow (\mathbb{C}, +)$

$\varphi(z) = \bar{z}$

$\varphi^* : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{C}^*, \times)$

$\varphi^*(z) = \bar{z}$

$\varphi : \mathbb{R}^2 \to \mathbb{R}^2 \qquad (a,b)+(c,d) = (a+c, b+d)$

$\varphi(a,b) = (b,a)$

Rotations centered around origin are all automorphisms of plane.

Inner Automorphism:-

Inner Automorphism induced by $a \in G$, for group G,

Inner Automorphism, $\varphi_a : G \to G$.

$$\varphi_a(x) = axa^{-1}$$

Injective, $\varphi_a(x) = \varphi_a(y) \iff x = y$ (trivial)

Surjective, ~~$\varphi_a(a^{-1}ya) = y$~~ $\forall y \in G$, $\varphi_a(y^{-1}ay) = y$

Operation preserving, $\varphi_a(xy) = \varphi_a(x)\,\varphi_a(y)$

Aut(G) = set of all automorphisms of G.

Inn(G) = set of all inner automorphisms of G.

Date
M T W T F S S

Thm:— Aut(G) and Inn(G) are groups under function composition.

Proof:—

Determining Inn(G) is ...

Date
M T W T F S S

$Inn(D_4) = \{ \varphi_{R_0}, \varphi_{R_{90}}, \varphi_{R_{180}}, \varphi_{R_{270}}, \varphi_{F_H}, \varphi_{F_V}, \varphi_{F_D}, \varphi_{F_{\bar{D}}} \}$

$= \{ \varphi_{R_0}, \varphi_{R_{90}}, \varphi_{F_H}, \varphi_{F_D} \}$

$\varphi_{R_0} = \varphi_{R_{180}}$

$\varphi_{R_{90}} = \varphi_{R_{270}}$

$\varphi_{F_H} = \varphi_{F_V}$

$\varphi_{F_D} = \varphi_{F_{\bar{D}}}$

~~$H = R_{180} V$~~ $F_H = R_{180} F_V$

$F_{\bar{D}} = R_{180} F_D$

$Aut(\mathbb{Z}_{10}) = \{ \varphi_1, \varphi_3, \varphi_7, \varphi_9 \}$

$\varphi_1(1) = 1$

$\varphi_3(1) = 3$

$\varphi_{57}(1) = 57$

$\varphi_9(1) = 9$

	φ_1	φ_3	φ_7	φ_9
φ_1	φ_1	φ_3	φ_7	φ_9
φ_3	φ_3	φ_7	φ_9	φ_1
φ_7	φ_7	φ_9	φ_1	φ_3
φ_9	φ_9	φ_1	φ_3	φ_7

	φ_1	φ_3	φ_7	φ_9
φ_1	φ_1	φ_3	φ_7	φ_9
φ_3	φ_3	φ_9	φ_1	φ_7
φ_7	φ_7	φ_1	φ_9	φ_3
φ_9	φ_9	φ_7	φ_3	φ_1

$\cong U(10)$

Theorem:- $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$

Proof:-

For $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, $\alpha(1) \in U(n)$

Date M T W T F S S

$T: \mathrm{Aut}(\mathbb{Z}_n) \longrightarrow U(n)$

$T(\alpha) = \alpha(1)$

Injective : $T(\alpha) = T(\beta) \Leftrightarrow \alpha(1) = \beta(1)$

and we know that,

$\forall k \in \mathbb{Z}_n,\ \alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$

$\Rightarrow \quad \alpha = \beta$

Surjective: For $r \in U(n)$, consider $\alpha: \mathbb{Z}_n \to \mathbb{Z}_n$,

$\alpha(s) = sr \pmod n$

α is an automorphism, $\alpha(1) = r \Rightarrow T(\alpha) = r$

$$T(\alpha\beta) = \alpha\beta(1) = \alpha(\underbrace{\beta(1)}_{\text{number}}) = \alpha(1)\beta(1) = T(\alpha)T(\beta)$$

~~EOE~~

14/03/2024

~~COSET~~ COSET & LANGRANGE THEOREM

Def:-

Given group G, subset H of G for $g \in G$,

$gH := \{gh \mid h \in H\}$

If $H \leq G$, $\exists\, a \in G \Rightarrow aH$ is called the left coset of H containing a. Similarly, Ha is the right coset containing a. The element a is called the ~~representation~~ coset representative of aH or Ha.

Page No. _____ RC Signature _____

Example:— $G = S_3$, $H = \{(1), (1\ 3)\}$

Left coset repre of G,

Date
M T W T F S S

~~(1) $S_3 = S_3$~~

(1) $H = H$

$(1\ 2)H = \{(1\ 2), (1\ 3\ 2)\}$

$(1\ 3)H = \{(1\ 3), (1)\}$

$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$

$(3\ 2\ 1)H = \{(3\ 2\ 1), (1\ 2)\}$

$(3\ 1\ 2)H = \{(3\ 1\ 2), (3\ 2)\}$

(1)
(1 2)
(1 3)
(3 2 1)
(3 1 2)
(2 3)

Example:— $H = \{R_0, R_{180}\}$, $G = D_4$

(3 2 1)(1 3)

~~(1 2)~~

(3 1 2)(1 3)

$R_0 H = H$

$R_{90} H = \{R_{90}, R_{270}\}$

$R_{180} H = H$

$R_{270} H = \{R_{270}, R_{90}\}$

$F_H H = \{F_V, F_H\}$

$F_V H = \{F_V, F_H\}$

$F_D H = \{F_D, F_{\bar{D}}\}$

$F_{\bar{D}} H = \{F_{\bar{D}}, F_D\}$

Example:— $G = \mathbb{Z}_9$, $H = \{0, 3, 6\}$

$0 + H = H = 3 + H = 6 + H$

$1 + H = \{1, 4, 7\} = 4 + H = 7 + H$

$2 + H = \{2, 5, 8\} = 5 + H = 8 + H$

~~$3 + H = H$~~

~~$4 + H = 2$~~

Go to previous section for further notes.

Signature

Abstract Algebra notes continued from here.

Date

M	T	W	T	F	S	S

Lemma:- Properties of cosets.

$H \leq G$, $a, b \in G$,

1. $a \in aH$
2. $aH = H \iff a \in H$

$a \notin H \Rightarrow aH \neq H$ $\because a \in aH$.

$aH = H \Rightarrow a \in H$

$a \in H \Rightarrow aH = H$

~~$aH \neq H \Rightarrow a \notin H$.~~ ~~because $a \in aH$, so $a \in H$~~

~~$aH \subseteq H$ because $a \in H$~~

$a \in H \Rightarrow a^{-1} \in H$.

$\forall y \in H$, $y = aa^{-1}y \in H \Rightarrow a^{-1}y \in H$, by closure, $\Rightarrow a \in H$.

$H \subseteq aH$.

~~$aH \subseteq H$~~

$a \in H \iff aH = H$.

3. $(ab)H = a(bH)$ or $H(ab) = (Ha)b$

$(ab)H = \{abh \mid h \in H\}$

$bH = \{bh \mid h \in H\}$

$a(bH) = \{abh \mid h \in H\}$

$(ab)H = a(bH)$

4. $aH = bH \iff a \in bH$

$aH = bH \Rightarrow a \in bH$ (~~from 1~~ $a \in aH = bH \Rightarrow a \in bH$.

$a \in bH$, $\exists h \in H \ni a = bh \Rightarrow b = ah^{-1}$.

$bH = \{bh^* \mid h^* \in H\}$

$= \{a(h^{-1}h^*) \mid h^* \in H\}$

$bH = \{ah' \mid h' \in H\}$

$bH \subseteq aH$.

Date

M	T	W	T	F	S	S

5. $(aH = bH) \Leftrightarrow (aH \cap bH = \emptyset)$

$\exists\, c \in aH \cap bH \Rightarrow (c \in aH) \wedge (c \in bH)$

$\Rightarrow (cH = aH) \wedge (cH = bH)$ by 4.

$\Rightarrow cH = aH = bH$

$\Rightarrow aH = bH$.

6. $aH = bH \iff b^{-1}a \in H$.

$aH = bH \Rightarrow \forall\, ah_1 \in aH, \exists\, h_2 \in H \ni ah_1 = bh_2$.

$\Rightarrow h_2 = b^{-1}ah_1 \in H$

$\Rightarrow b^{-1}a \in H \quad \because h_1 \in H.$

$aH = bH \iff b^{-1}(aH) = b^{-1}(bH)$

$\iff (b^{-1}a)H = (b^{-1}b)H$ by 3.

$\iff (b^{-1}a)H = eH$ $\because e \in H$ and 2.

$\iff b^{-1}a \in H$ by 2.

7. $|aH| = |bH|$

$\forall\, h \in H$, let $\varphi : aH \to bH \ni \varphi(ah) = bh$, φ is bijection.

8. $aH = Ha \iff H = aHa^{-1} := \{aha^{-1} \mid h \in \in H\}$

9. $aH \leq G \iff a \in H$

$a \in H \Rightarrow aH = H \leq G$.

Date
M T W T F S S

$a \notin H \Rightarrow \nexists\, h \in H \ni ah = e$ ∵ because $h = a^{-1}$ but $a \notin H$ therefor $a^{-1} \notin H$.

Langrange's Theorem:—

If G is a finite group, $H \leq G$, then $|H| \mid |G|$, and there are $\frac{|G|}{|H|}$ left and right cosets of H.

Proof:—

$\forall a \in G, \exists i \ni a \in a_i H$, where $a_i H$ are the unique cosets of H for $1 \leq i \leq r$. This means,

$$G = \bigcup_{i=1}^{r} a_i H$$

$$|G| = \sum_{i=1}^{r} |a_i H|$$

$$|G| = \sum_{i=1}^{r} |H| \qquad \text{by 2.}$$

$$|G| = r|H|$$

∎

Corollary 1:—

Number of left cosets of H, is called index of H, and written as $|G:H| = \frac{|G|}{|H|}$

Corollary 2:—

$a \in G \Rightarrow |a| = |G|$

Date
M T W T F S S

Corollary 3:—

Groups of prime order are cyclic.

Corollary 4:—

$a^{|a|} = e$

Corollary 5:— Fermat's little theorem:—

$\forall a \in \mathbb{Z},\ a^p = a \pmod p$

Thm 7.2:—

If $H, K \leq G$,

$\# HK := \{ hk \mid h \in H, k \in K \} \subseteq G$

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Thm 7.3:— 26/03/2024

Classification of all groups of order $2p$, $p > 2$ prime.

Every group of order $2p$ is isomorphic to either $\mathbb{Z}_{2p}$ or D_p

Proof:—

Assume G is a non-cyclic group of order $2p$. Let $e \neq a \in G$, then $|a| = 2$ or $|a| = p$.

Claim 1: There is are some elements $a \in G$, with $|a| = p$. If that is not that case, then $\forall a, b \in G$, $|a| = |b| = 2$.

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

then G is abelian and $H = \{e, a, b, ab\} \leq G$, which is not possible because $4 \nmid 2p$. This is a contradiction to Langrange's Theorem.

i.e. $\exists\, a \in G \ni |a| = p$. Now, let $b \in G \ni b \notin \langle a \rangle$.

Claim 2: $|b| = 2$

consider $\langle b \rangle$, since $b \notin \langle a \rangle$, $\langle b \rangle \neq \langle a \rangle$

$$|\langle a \rangle \cap \langle b \rangle| = 1$$

$$|\langle a \rangle \langle b \rangle| = \frac{|\langle a \rangle| |\langle b \rangle|}{|\langle a \rangle \cap \langle b \rangle|}$$

$$= \frac{|a||b|}{1}$$

$$|\langle a \rangle \langle b \rangle| = p|b|$$

$\Rightarrow |b| = 2$, otherwise, $p^2 > 2p$, which is a contradiction.

consider element ab,

$ab \notin \langle a \rangle$, then $|ab| = 2$

~~$\Rightarrow |ab| = 2 (ab)$~~

$\Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$:

This completly determines the multiplication table of G. D_p is ~~one~~ one such non-cyclic group of order $2p$. so it has the same multiplication table as rest of them.

i.e. all of them are isomorphic to it.

An Application of Cosets to Permutation Groups:-

Date 28/03/2024

M T W T F S S

Def:-

stabilizer of an element i in S. Let G be a permutation group over S, then for $i \in S$, ~~$stab_G(i)$ =~~

$$stab_G(i) := \{ \varphi \in G \mid \varphi(i) = i \}$$

Note:- ~~sta~~ $\forall i \in S$, $stab_G(i) \leq G$.

Def:-

Orbit of $i \in S$, $orb_G(i) := \{ j \in S \mid \varphi(i) = j \text{ for some } \varphi \in G \} \subseteq S$ under G.

Orbit - Stabilizer Theorem :-

For any finite permutation group G over S, and $i \in S$,

$$|G| = |stab_G(i)| \, |orb_G(i)|$$

Proof:-

Since, $stab_G(i) \leq G$, $|stab_G(i)| \mid |G|$. We will show that, $\frac{|G|}{|stab_G(i)|}$ correspondence between cosets of $stab_G(i)$ and elements of $orbit_G(i)$

Let, T: coset of $stab_G(i) \longrightarrow orb_G(i)$. show T is well defined

~~If~~ $\alpha \, stab_G(i) = \beta \, stab_G(i) \iff \alpha^{-1}\beta \in stab_G(i)$

$\iff \alpha^{-1}\beta(i) = i$

$\iff \beta(i) = \alpha(i)$

Let $j \in orb_G(i) \Rightarrow \exists \varphi \in G \ni \varphi(i) = j$

$\Rightarrow \varphi \, stab_G(i)$ is our desired coset that maps under T to j.

Date
M T W T F S S

External Direct Product.

Def:- If $G_1, G_2, \cdots, G_n$ is a finite set of groups, then the direct external product of G_i is defined as,

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n := \{(g_1, g_2, \cdots, g_n) \mid g_i \in G_i\}$$

where product of two elements

$$(g_1, g_2, \cdots, g_n)(h_1, h_2, \cdots, h_n) = (g_1 h_1, g_2 h_2, \cdots, g_n h_n)$$

where $g_i h_i$ is the corresponding operation in G_i. See that external direct product is a group. If $|G_i|$ is finite for each i, then

$$\left| \bigoplus_{i=1}^{n} G_i \right| = \prod_{i=1}^{n} |G_i|$$

Example:-

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$$

RC

Signature

Thm 8.1 :- If g_i are finite

$$|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$$

Date 2/04/2024

M T W T F S S

Proof :-

Lets donate the identity of g_i with e_i, Let,

$s = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$

$t = |(g_1, g_2, \dots, g_n)|$

$$(g_1, g_2, \dots, g_n)^s = (g_1^s, g_2^s, \dots, g_n^s) = (e_1, e_2, \dots, e_n)$$

$\Rightarrow t \mid s$

$$(e_1, e_2, \dots, e_n) = (g_1, g_2, \dots, g_n)^t = (g_1^t, g_2^t, \dots, g_n^t)$$

$\Rightarrow s \mid t$

$\therefore s = t$

Example:-

$\mathbb{Z}_{100}$, ~~$\mathbb{Z}_{50} \oplus \mathbb{Z}_2$~~, $\mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4$, $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $D_{10} \oplus \mathbb{Z}_5$, $D_5 \oplus \mathbb{Z}_{10}$, $D_5 \oplus D_5$, they are not isomorphic to each other.

04/04/2024

Example:- $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$, find # of elements of order 5.

$(a, b) \in$, $|a| = 5$, $|b| = \{1\} \longrightarrow 4$

$|a| = 1$, $|b| = 5 \longrightarrow 4$

$|a| = 5$, $|b| = 5 \longrightarrow 16$

24

Example:- $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$, find the number of cyclic subgroups of order 10.

Date 4/09/2024

M	T	W	T	F	S	S

(a,b), $|a| = 10$, $|b| = 1$ $\rightarrow$ 4

~~$|a| = 5$, $|b| = 2$ $\rightarrow$ 10~~

$|a| = 2$, $|b| = 5$ $\rightarrow$ 4

~~$|a| = 1$, $|b| = 10$~~

$|a| = 10$, $|b| = 5$ $\rightarrow$ 16

Example:- For each divisor r of m and s of n. There is a sub-group isomorphic to $\mathbb{Z}_r \oplus \mathbb{Z}_s$ in $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

In $\mathbb{Z}_{30} \oplus \mathbb{Z}_{14}$ sub-group isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_2$

$\langle 5 \rangle \oplus \langle 7 \rangle \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$

$\varphi((5i, 7j)) = (i, j)$

Thm 8.2:- If G and H are finite cyclic groups, then $G \oplus H$ is cyclic iff $|G|, |H|$ are co-prime. $\gcd(|G|, |H|) = 1$.

Proof:-

Let $|G| = m$ and $|H| = n$ and assume $G \oplus H$ is cyclic. Let $\gcd(|G|, |H|) = d$. For any $(g,h) \in G \oplus H$

$$(g,h)^{mn/d} = \left((g^m)^{n/d}, (h^n)^{m/d}\right) = (e_G, e_H)$$

$\Rightarrow$ (g,h) is the generator of $G \oplus H$ then (g,h) has order mn.

$\Rightarrow$ $mn \leq \frac{mn}{d}$ $\Rightarrow$ $d = 1$.

Conversly, if $\gcd(m,n) = 1$, then let $\langle g \rangle = G$ and $\langle h \rangle = H$

$|(g,h)| = \text{lcm}(m,n) = mn$.

$\Rightarrow$ $G \oplus H$ is cyclic generated by $\langle (g,h) \rangle$.

Corr 1: Let $G_1, G_2, \ldots, G_n$ be finite cyclic groups, then,

Date 9/04/2024

M	T	W	T	F	S	S

$\bigoplus_{i=1}^{n} G_i$ is cyclic if $\forall\, 1 \le i, j \le n,\ i \neq j$

$\gcd(|G_i|, |G_j|) = 1$.

Corr 2:

Let $m = n_1 \cdot n_2 \cdots n_k$, then

$$\mathbb{Z}_m \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{n_i}$$

iff $\forall\, 1 \le i, j \le k,\ i \neq j,\ \gcd(n_i, n_j) = 1$.

Example:-

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_{45} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$$

FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS.

Every finite Abelian ~~Product~~ Group is isomorphic to a direct product of $\mathbb{Z}_{i_s}$.