Chapter 2

Groups

Definition and Examples of Groups

$G \neq \phi$ ← non empty set دايما الـ

$*: G \times G \to G$ ← اقتران G*G

$*(a,b) \in G \quad , \forall a,b \in G$ ← binary operation

$*(a,b) = a*b$

$a \cdot b = ab$

$*$ is called a binery opperation on G or G is closed under $*$

Binary Operation:

let G be a set, A binary operation on G is a function that assigns each ordered pair of element of G

(1) binary operation on G (Closure)

$\forall a,b \in G \Rightarrow a*b \in G$

(2) Associativity

$\forall a,b,c \in G$

$(a*b)*c = a*(b*c)$ هون مهم الترتيب

له معناها انو بعمل الـ operation لـ a, b بعدين مع ابنا تج بعمل مع c

(1) and (2) $\Rightarrow$ G **Semi group**

(3) Identity

$\exists\, e$ (identity) $\in G$: such that $e * x = x * e = x$

$\forall\, x \in G$

(1) and (2) and (3) $\Rightarrow$ G monoid

(4) Inverse

$\forall\, a \in G$, $\exists\, b$ (inverse for a) $\in G$

such that $a * b = b * a = e$

b inverse a

a is invertable element انو الو inverse

b denoted a^{-1}

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

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

(1), (2), (3) and (4) $\Rightarrow$ G Group

* G Group and $a * b = b * a$, $\forall\, a, b \in G$

$\Rightarrow$ G Commutative group or obelian group

EX: ① Is $(\mathbb{Z}, +)$ a Group?

① binary?

$\forall a, b \in \mathbb{Z}$

$a+b \in \mathbb{Z}$ ✓

② $a, b, c \in \mathbb{Z}$

$(a+b)+c = a+(b+c)$ ✓

③ identity 0

$0+a = a+0 = a \quad \forall a \in \mathbb{Z}$ ✓

④ inverse

$a \in \mathbb{Z}, -a \in \mathbb{Z}$

$a + -a = -a + a = 0$

⑤ $a+b = b+a \quad \forall a \in \mathbb{Z}$

So $(\mathbb{Z}, +)$ a belian group

↳ $\mathbb{Z}$ under addition.

③ $(\mathbb{Z}, -)$

① $a, b \in \mathbb{Z}$

$a-b \in \mathbb{Z}$ ✓

$a-b = a + -b \in \mathbb{Z}$

② $a, b, c \in \mathbb{Z}$

Is $(a-b)-c \overset{??}{=} a-(b-c)$.

نعطي مثال للحل No

Example : $(1-0)-2 \overset{??}{=} 1-(0-2)$ خلص اذا فشلت الثانية

$-1 \neq 3$ خلص داعي اكمل واشوف الباقي

not semi group.

$(\mathbb{Z}, \cdot)$

① $\forall a, b \in \mathbb{Z}$

$a \cdot b \in \mathbb{Z}$ binary ✓

② associativity

$\forall a, b, c$

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

③ Identity

$1 \in \mathbb{Z} : 1 \cdot a = a \cdot 1 , \forall a \in \mathbb{Z}$

$\Rightarrow (\mathbb{Z}, \cdot)$ monoid

commutative monoid

④ Inverse : No

1, -1 inverse لين الواحد والسالب واحد النهر

2 No inverse

$\mathbb{Z}$ under multiplication it is not group.

Ex: $(\mathbb{Q}, +)$, $(R, +)$, $(C, +)$ } a belian groups.

$(R, \cdot)$

① Closure ✓

② Associativity : $(ab)c = a(bc)$ ✓

③ Identity : $1 \in R , 1 \cdot a = a \cdot 1 , \forall a \in R$

④ Inverse : 0 has no invese.

$(R^*, \circ)$ علشان اتخلص من مشكلة الصفر بأخد R^*

(1) closure ✓

(2) Associativity ✓

(3) Identity ✓

(4) Inverse : $\forall a \neq 0, a \in R, \frac{1}{a} \in R$

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$$

$$a^{-1} = \frac{1}{a} \in R^*$$

(5) $ab = ba, \forall a, b \in R^*$

هوالكلام صحيح حتى لو مع الصفر برضه

علشان انا بشتغل على R^*

$(R^*, \circ)$ a belian group

$(Q^*, \circ)$ a belian group → $\frac{a}{b} \in Q^*, a, b \neq 0$

$\frac{b}{a} \in Q^*$ ∘ $(\frac{a}{b})^{-1} = (\frac{b}{a})$

$(C^*, \circ)$ a belian group

complex

* Matrses.

$M_{m \times n}(R) = \{A_{m \times n} : a_{ij} \in R\}$

$M_{m\times n}(R, +)$

(1) $\forall A, B_{m\times n} \Rightarrow (A+B)_{m\times n}$ ✓

(2) $A, B, C_{m\times n}$: $(A+B)+C = A+(B+C)$

(3) Identity $O_{m\times n}$: $A+O = O+A = A$
Zero matrix

(4) $A_{m\times n}, -A_{m\times n}$, $A+-A = -A+A = O$

(5) $A+B = B+A$

$M_{m\times n}(R, +)$ belian group

* $M_{m\times n}(R, \cdot)$

(1) NO $A_{m\times n}, B_{m\times n}$ هون الضرب غير معرف

* $M_{n\times n}(R, \cdot)$
Square matrix لهيك اسمها

(1) $A, B_{n\times n}$: $(AB)_{n\times n}$ define
علشان يصير الضرب معرف

(2) $(AB)C = A(BC)$ ✓

(3) I_n : $I_n A = AI = A$

monoid

not commutative

$AB \neq BA$

(4) Inverse : No

Inverse لها matrix مش كل

$M_{n\times n}(R,\cdot)$ not group

Notation

Invertiable nxn ← بلي

$GL(n,R) = \{A_{n\times n}$ Invertable , $a_{ij} \in R\}$ ← الهم Inverse

(1) $A,B \in GL(n,R) \Rightarrow AB$ invertible

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

(3) $I_n \in GL(n,R)$

(4) $A \in GL(n,R)$, A^{-1} exists

$|A| \neq 0$

$|A^{-1}| = \frac{1}{|A|} \neq 0$

(5) $AB \neq BA$

non abelian

$(\mathbb{Z}_n, \oplus_n)$

$aRb \leftrightarrow n \mid a-b$

Equivalence Relation

$[0], [1], \ldots, [n-1]$

$[x] \oplus_n [y] = [x+y]$

$n = 4$

$[0], [1], [2], [3]$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*Review

(1) binary opperation (closar opperation)

$\forall a, b \in G, a * b \in G$

Def: monoid G with *

[1] * binary: $\forall a, b \in G \Rightarrow a * b \in G$

[2] associative: $\forall a, b, c \in G$,

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

monoid with identity $\Rightarrow$ semi group

* $\exists e \in G$ s.t $e * a = a * e = a$, $\forall a \in G$

Identity

Group: semi group with inverse property

**Inverse: let $a \in G$, then $b \in G$ is called an inverse on a If and only if $a * b = b * a = e$

Group: $G \neq \phi$, with an operation *

① * binary

② * associative

③ Identity element $\boxed{e \in G}$: $e * a = a * e$

$\forall a \in G$

④ $\forall a \in G$, a has inverse denote by a^{-1}

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

$(G, *)$ group
In addition $*$ commutes: $a*b = b*a$, $\forall a,b \in G$

$*$ is called commutative, and $(G,*)$ is called a commutative group or abelian group

Ex) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ abelian group

$(\mathbb{N}_0, +)$ is not a group

$(\mathbb{N}_0, +)$ is a semi group where $\boxed{\mathbb{N} = \mathbb{Z}^+}$

with Zero — No inverse — بدون ال Zero

$M_{m\times n}(\mathbb{R}) = \{A_{m\times n} : a_{ij} \in \mathbb{R}\}$, $+$ is abelian

$M_{n\times n}(\mathbb{R}) = \{A_{n\times n} : a_{ij} \in \mathbb{R}\}$, $\cdot$ not group

inverse مشكلتها في

Def: ① General linear group

$GL(n, \mathbb{R}) = \{A_{n\times n} : a_{ij} \in \mathbb{R}, |A| \neq 0\}$

size — entres

$(GL(n,\mathbb{R}), \cdot)$ is a non abelian group

لانو عملية الضرب غير تبديلية

② Special Linear group

$SL(n,R) = \{A_{n\times n} : |A| = 1, a_{ij} \in R\}$ special ll

group with •

Gererou linear.

R_n opperation on $\mathbb{Z}$: $aRb \leftrightarrow n \mid a-b$

R_n is an Equivalence Relation on $\mathbb{Z}$, with Classes

$\bar{0}, \bar{1}, \ldots, \overline{n-1}$ partion of $\mathbb{Z}$

This set of classes is denoted by

$\mathbb{Z}_n = [\bar{0}, \bar{1}, \ldots, \overline{n-1}]$

define $\oplus_n$: $a \oplus_n b = c$, $c + nK = a+b$

Similarly $\otimes_n$

$\mathbb{Z}_4$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

inverse في

0 inverse 0

1 ↔ 3

2 ↔ 2

3 ↔ 1

a belian group

$K \in \mathbb{Z}_n$ Then $K^{-1} = n - K$

$(\mathbb{Z}_4, \otimes_4)$

$\otimes_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

not group

Inverse ليس
Zero ليس 1
2 ليس 1

1 inverse 1

3 inverse 3

or identity 1

$1^{-1}=1$ | 0, 2

$3^{-1}=3$ | has no inverse

$(\mathbb{Z}_4^*, \otimes_4)$

$\otimes_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

→ not closed

$\otimes_4 2 = 0$

Thm. $(\mathbb{Z}_n^*, \otimes_n)$ is a group $\leftrightarrow$ n is prime

$\Rightarrow$ by contrapositive: suppose n is not prime (n composite) $\exists\ r, s \in \mathbb{Z}^+, \otimes$

$1 < r, s < n$

$\Rightarrow$ $r, s \in \mathbb{Z}^+$ and $r \otimes_n s = 0 \notin \mathbb{Z}_n$

$\rightarrow (\mathbb{Z}_n^*, \otimes_n)$ not group

(⇐) let n be prime

① $\otimes_n$ is binary: if not $\exists a,b \in \mathbb{Z}_n^*, 1<a,b<n-1$

$\rightarrow a \otimes_n b = 0 \Rightarrow$ so n is not prime

② associative ✓

③ identity $1 \in \mathbb{Z}_n^*$

④ inverse: let $k \in \mathbb{Z}_n^*$, n prime

$\Rightarrow grd(a,n)=1$

العامل المشترك الأكبر

So $\exists x,y \in \mathbb{Z} \rightarrow ax+yn=1$

$\Rightarrow ax+yn=1$ —— ①

$a \otimes_n x = 1$ (eq ① and def^n $\otimes_n$)

$a^{-1}=\bar{x}$ $\quad a^{-1}=[x]$, $[x]$: class x mod n

Notation: ① $a*b=ab$

② If commutes then $*$ is denoted by $+$

$a*b=a+b$.

identity e denoted by 0

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

$a^n = \underbrace{a*a*\dots*a}_{n \text{ times}}$

In addition $a^n = \underbrace{a+a+a+\dots+a}_{n}$

$= na$

Field

$(F, +, \cdot)$

① $(F, +)$ a belian group

② $(F^*, \cdot)$ a belian group

③ $\cdot$ distribute over $+$: $a(b+c) = (b+c)a = ab+ac$

Ex: $(R, +, \cdot)$ field

$(Q, +, \cdot)$ field

$(C, +, \cdot)$ field

$(Z_p, \oplus, \odot_n)$ field

p: prime

but $(Z, +, \cdot)$ is not a fied عشان مشكلة inverse

Notation

$GL(n, F) = \{A_{n \times n} : a_{ij} \in F, \text{Field}, |A| \neq 0\}$

$SL(n, F) = \{A_{n \times n} : a_{ij} \in F, \text{Field}, |A| = 1\}$

Ex: $G = \{1, i, -1, -i\}$ under $\cdot$ group

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$GL(2, Z_5) = \{ A_{2\times 2} : |A| \neq 0, a_{ij} \in Z_5 \}$

$A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 3 & 1 \\ 2 & 3 \end{bmatrix}$ Is $A \in GL(2, Z_5)$
Is $B \in GL(2, Z_5)$

$|A| = 2\times 4 - 1\times 3 = 5 \bmod 5 = 0$

$\Rightarrow A \notin GL(2, Z_5)$

singular

$|B| = 3\times 3 - 2\times 1 \bmod 5$

$= 7 \bmod 5$

$= 2 \neq 0$

$B \in GL(2, Z_5)$

What is $B^{-1} = \begin{bmatrix} 3 & -1 \\ -2 & 3 \end{bmatrix} \cdot |B|^{-1}$, $2^{-1} \bmod 5 = 3$
$2\times 3 \bmod 5 = 1$

$= 3 \begin{bmatrix} 3 & 4 \\ 3 & 3 \end{bmatrix}$

$= \begin{bmatrix} 4 & 2 \\ 4 & 4 \end{bmatrix}$

علشان نتأكد

$BB^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 4 & 2 \\ 4 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Th. let G be a group, Then

① identity is unique

② inverse is unique

③ $(ab)^{-1} = b^{-1}a^{-1}$

④ $(a^{-1})^{-1} = a$

proof ① let e, e' be two identities of G

$$e = ee' = e'$$

② let a has two

$$\Rightarrow a'a = e \Rightarrow a'(aa'') = ea''$$

$$a'(e) = ea''$$

$$a' = a''$$

③ $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

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

$$= aa^{-1}$$

$$= e$$

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

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

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

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

④ $a^{-1}a = aa^{-1} = e$

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

2nd ④ $(a^{-1})^{-1} = a$

$aa^{-1} = e$ multiply from right by $(a^{-1})^{-1}$

$a\,a^{-1}(a^{-1})^{-1} = e(a^{-1})^{-1}$

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

$a\ e = (a^{-1})^{-1}$

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

ch 2 done

next lectar discassion of ch 2.

⑤ Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, Z_{11})$

$$A = \begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix} \text{ in } GL(2, Z_{11})$$

$$|A| = 2\times5 - 3\times6 \bmod 11$$
$$= -8 \bmod 11$$
$$= 3 \neq 0$$

A non Singular

$$A^{-1} = 3^{-1}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = 4\begin{bmatrix} 5 & 6 \\ 8 & 2 \end{bmatrix} = \begin{bmatrix} 9 & 9 \\ 16 & 8 \end{bmatrix}$$

Cancellation law

* in G group

$a, b, c \in G$

$ab = ac$

$ba = ca$

$\Rightarrow b = c$

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

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

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

$eb = ec$

$b = c$

$ab = ca$

* مرفوض نعمل كانسل لما يكون الـ a مش بنفس الجهة

⑦ Translate each of the following multiplicative expressions into its additive counterpart Assume that the operation is commutative

(a) $a^2b^3 \equiv 2a+3b$

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

(c) $(ab^2)^{-3}c^2 = e \equiv -3(a+2b)+2c = 0$

⑭ let G be a group with the following property whenever a, b, and c belong to G and ab=ca then b=c brove that G is Abelian

$\forall a, b \in G$

$aba = abá$

$\Rightarrow ba = ab$

* كون مسموح اعمل Cancel من اليمين والشمال.

⑮ Let a,b be elements of an abelian group and let n be any integer show that $(ab)^n = a^n b^n$

Ⓘ By induction for $n \in Z^+$

① $n=1$

$(ab)^1 = a^1 b^1$

② assume it is a true for $n=K$

$(ab)^K = a^K b^K$

③ $n = K+1$

$(ab)^{K+1} = (ab)(ab)^K$

$= (ab)(a^K b^K)$

$= aa^K(bb^K) = a^{K+1} b^{K+1}$

(II) $n=0$

$(ab)^0 = e$

$a^0 = e$, $b^0 = e$

$e = ee$

(III) $n \in \mathbb{Z}^-$

let

$m = -n \in \mathbb{Z}^+$

$(ab)^m = a^m b^m$

$(ab)^{-n} = a^{-n} b^{-n}$

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

$(ab)^n = b^n a^n$, we use $(a^n)^{-1} = (a^{-1})^n$

$(ab)^n = a^n b^n$ نحاول نثبتها.

(19) $(a^{-1}ba)^n = a^{-1}b^n a$ prove, ←

For any elemen from a group any integer n

,

$$(a^{-1}ba)^n = \underbrace{a^{-1}baa^{-1}ba \cdots a^{-1}ba}_{n \text{ time}}$$

$$= \underbrace{a^{-1}bebe \cdots ba}_{n \text{ time}}$$

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

(25) Suppose that table below is groub table
Fill in the blank entries

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

* $n \in \mathbb{Z}^+$

ما بفرق اذا دخلالn اولا

$U(n) = \{1 \leq K < n : gcd(n,K) = 1\} \rightarrow \{K : 1 \leq K \leq n : gcd(n,K) = 1\}$

$U(n)$ ⊗ n is a group

$U(1) = \{1\}$

$U(2) = \{1\}$

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

$U(4) = \{1,3\}$

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

* انهم بكون relative prime مع الواحد وعم اقل من n

$1 \longrightarrow n$

$\otimes_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(26) prove that if $(ab)^2 = a^2b^2$ in a group G then $ab = ba$.

$(ab)^2 = a^2b^2$

$abab = aabb$

$\Rightarrow ba = ab$

(27) let a, b and c be element of a group solve the equation $axb = c$ for x solve $a^{-1}xa = c$ for x

$a^{-1}axb = a^{-1}c$

$(exb = a^{-1}c)\ b^{-1}$

$x = a^{-1}cb^{-1}$

H.W (29), (30), (33)

التسليم خلال ربيتاج قبل يوم الاثنين

Chapter 3

Finite groups and Subgroups

Def: A group G is called a finite group if G as a set finite other wise G is infinte

# of elements in G is called the order of G denoted by $|G| = ord(G) = O(G)$

If # of elements of G is n, $|G| = n$

If # is infinite then $|G| = \infty$ فش فرق اذا كان non countable او countable

Ex: $(\mathbb{Z}_5, \oplus_5)$

$\{0, 1, 2, 3, 4\}$

$|\mathbb{Z}_5| = 5$

$|\mathbb{Z}_5^*| = 4$

$|\mathbb{Z}| = \infty$

$|R| = \infty$

$|R^*| = \infty$

$(U(n), \otimes_n)$

$U(5) = \{1, 2, 3, 4\} = \mathbb{Z}_5^*$ $\rightarrow |U_5| = 4$ prime لأن U

n prime $U(n) = \mathbb{Z}_n^*$

$U(8) = \{1, 3, 5, 7\} \rightarrow |U(8)| = 4$

order of an element in a group

Def: let G be a group, $a \in G$, Then order of a denoted by $|a|$ is the smallest positive integer n $a^n = e$

Ex: $|e| = 1$

$G = \mathbb{Z}_6$ $a^m = na$

$|0| = 1$

$|1| = 6$

$|2| = 3$ $(3 \times 2 = 6$

$|4| = 3$

$|3| = 2$

$|5| = 6$

$5^1 = 5$

$5^2 = 2 \times 5 \bmod 6 = 4$

$5^3 = 3 \times 5 = 3$

$5^4 = 20 = 2$

$5^5 = 1$

$5^6 = 0 \rightarrow |5| = 6$

$G = \mathbb{Z}$ جميع الأعداد الصحيحة

$|1| = \infty \rightarrow$ Zero $\nexists n \in \mathbb{Z}^+$. $1^n = n \cdot 1 = n \neq 0$

in $\mathbb{Z}$ all elements extent 0 has infinite orders

$U(6) = \{1, 5\}$ مزدوج

$|1| = 1$

$|5| = 2$ $5^1 = 5$ $5^5 = 25$ $5^2 = 1$

Z_{11}^* , $\langle 2 \rangle_{11}$

$|2| = 10$

$2^2 = 4$
$2^3 = 8$
$2^4 = 5$
$2^5 = 10$
$2^6 = 9$
$2^7 = 7$
$2^8 = 3$
$2^9 = 6$
$\boxed{2^{10} = 1}$

بنفس الطريقة $|3| = 10$
$|4| \neq 10$

Th. let G be a group, $a \in G$, $|a| = n$, and let $K \in Z^+$ $a^K = e$, then $n | K$

proof: By division Algorithm, $\exists\, q, r \in Z^+$

$K = nq + r$, $0 \leq r < n$

$\Rightarrow e = a^K = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q a^r = a^r$

$\Rightarrow a^r = e$, $0 \leq r < n \Rightarrow r = 0 \Rightarrow K = nq \Rightarrow n | K$

علشان لو كان اقل من n يصير اقل من $|a|$

Subgroups

Def: let G be a group, a nonemply subset H of G is called a subgroups of G iff H under the operation of G is a group denoted by $H \leq G$

Ex: $(\mathbb{Z},+) \leq (\mathbb{R},+)$

but $(\mathbb{Z}_5,\oplus_5) \not\leq (\mathbb{Z},+)$, $\mathbb{Z}_5 \not\leq \mathbb{Z}$, $\oplus_5 \neq +$

↳ لانو مش نفس الـ operation

$\mathbb{Z}_n \not\leq \mathbb{Z}$ / $(\mathbb{Z}_4,\oplus_4) \not\leq (\mathbb{Z}_8,\oplus_8)$

Ex $(\mathbb{Z},+)$

$H=\{\text{even integers}\}$, $+$

$H \leq \mathbb{Z}$:

① even + even = even

② associative ✓

③ Identity : 0 even.

④ x even $\Rightarrow -x$ even $\Rightarrow -x \in H$

$x \in H$ ✓

$K=\{odd\}$, $+$

① Not binary

odd + odd = even $\notin K$

* اي جروب هو subgroup بنفسه و

✓ الـ Identity برضو subgroup باي جروب

Ex: $(\mathbb{Z}_4,\oplus_4)$

* Subgroup $\mathbb{Z}_4$, $\{0\}$ trivial

↳ لانو موجودين بكل group لانو نفس الـ group

بكون subgroup وبرضو الـ Identity

RMK: In any group G, $G, \{e\} \leq G$ called the trivial subgroup

Def: let G group, $H \leq G$, $H \neq G$ (H proper subset)

Then H is called a proper subgroup.

Tests for Subgroups:

Two step Test:

Th. let G be a group, $H \overset{\neq \phi}{\subseteq} G$, Then $H \leq G$ iff (1) $\forall x, y \in H \Rightarrow xy \in H$

(2) $\forall x \in H, x^{-1} \in H$

proof: $\Rightarrow$ ✓

* لان واضح هدول بحققو شروط الـ group (الشرط الاول والرابع).

$\Leftarrow$ (1) ✓

(2) associative: $\forall a, b, c \in H \Rightarrow a, b, c \in G$

$(ab)c = a(bc)$

(3) identity: Since $H \neq \phi$, so $\exists x \in H$

$\Rightarrow x^{-1} \in H$ by (2) $\Rightarrow xx^{-1} = e \in H$

RMK: If $H \leq G$, Then $e \in H$

One step Test:

Th. let G be a group, $H \overset{\neq \phi}{\subseteq} G$, then $H \leq G$ iff

$\forall x, y \in H, x^{-1}y \in H$

proof: $\Rightarrow$ ✓ Since if $H \leq G, x, y \in H \Rightarrow x^{-1} \in H \Rightarrow x^{-1}y \in H$

$\Leftarrow$ (1) Since $H \neq \phi \Rightarrow \exists x \in H$, let $y = x \Rightarrow x^{-1}x = e \in H$

(2) let $x \in H, y = e \rightarrow x^{-1}y = x^{-1}e = x^{-1} \in H$

(3) let $x, y \in H, x^{-1} \in H \Rightarrow (x^{-1})^{-1}y = xy \in H$

$\Rightarrow$ by 2-step test $\geq$

$\rightarrow H \leq G$.

Ex: let G abelian group, $H = \{x \in G : x^2 = e\}$, Then $H \leq G$

proof: $H \neq \phi$ since $e \in G$, $e^2 = e \Rightarrow e \in H$ ← اهم خطوة

by two step Test: (abeliane.)

(1) Let $x, y \in H \Rightarrow x^2 = e, y^2 = e \Rightarrow (xy)^2 = x^2y^2 = ee = e$

$\Rightarrow xy \in H$

(2) Let $x \in H \Rightarrow x^2 = e \Rightarrow (x^2)^{-1} = (x^{-1})^2 = e^{-1} = e$

$\Rightarrow x^{-1} \in H \Rightarrow H \leq G$

* one step: ① $H \neq \phi$ since $e \in H$

let $x, y \in H$, Show $x^{-1}y \in H$

$x^2 = y^2 = e \Rightarrow (x^{-1}y)^2 = (x^{-1})^2 y^2$

RMK: In previous if G is not abelian

Then H need not be a subgroup of G

Give an example

لو نروح للمصفوفات اسهل اشي

Def: Center and Centralizer

let G be a group, $g \in G$, then

① The Center of G denoted by

$Z(G) = \{x \in G : xy = yx, \forall y \in G\}$

② Centralizer of g denoted by

$C(g) = \{x \in G : xg = gx\}$

$Z(G) \leq C(g), \forall g \in G$

ال Z و C nonempty لانو في عنا دايما e

بدل مع اي g.

CamScanner المسموحة ضوئيا بـ

Th. Let G be a group, Then ⇒

(1) $Z(G) \leq G$

(2) for any $g \in G$, $C(g) \leq G$

(3) $Z(G) \leq C(g)$, $\forall g \in G$

proof: [1] ① $Z(G) \neq \phi$ Since $e \in Z(G)$

$ex = xe = x$, $\forall x \in G$.

② Let $x, y \in Z(G) \Rightarrow xa = ax$, $\forall a \in G$

$ya = ay$, $\forall a \in G$

$\Rightarrow$ for any $a \in G$, $(xy)a = x(ya) = x(ay)$

$= (xa)y = (ax)y = a(xy)$

$\Rightarrow xy \in Z(G)$

③ Let $x \in Z(G)$

$\Rightarrow xa = ax$ $\forall a \in G$

$\Rightarrow x^{-1}(xa = ax)x^{-1}$

$x^{-1}xax^{-1} = x^{-1}axx^{-1}$

$ax^{-1} = x^{-1}a$

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

[2] let $g \in G$

① $C(g) \neq \phi$ Since $e \in C(g)$: $eg = ge = g$

② Let $x, y \in C(g) \Rightarrow xg = gx$, $yg = gy$

$\Rightarrow (xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$

$\Rightarrow xy \in C(g)$

③ Let $x \in C(g) \Rightarrow xg = gx$

$\Rightarrow x^{-1}g = gx^{-1} \Rightarrow x^{-1} \in C(g)$

$C(g) \leq G$

(3) $Z(G) \subseteq C(g)$, $\forall g \in G$

$\Rightarrow Z(G) \leq C(g)$

(4) $Z(G) = \bigcap_{g \in G} C(g)$

$\subseteq$ ✓ by ③

$\supseteq$ let $x \in \bigcap C(g) \Rightarrow xg = gx$, $\forall g \in G$ — تعريف ال Center

$\Rightarrow x \in Z(G) \Rightarrow \bigcap \subseteq Z(G)$

★ Special Case

Test For Finites subsets H of a group

Th. let G be a group, H finite subset of a group G, Then $H \leq G \Leftrightarrow \forall a, b \in H$, $ab \in H$

proof $\Rightarrow$ ✓

$\Leftarrow$ let $a \in H$, we need to show $a^{-1} \in H$ (use Two step Test)

Case 1: If $a = e$, then $a^{-1} = e^{-1} = e \in H$

Case 2: Let $a \in H$, $a \neq e$

Consider $S = \{a^n : n \in \mathbb{Z}^+\} \subseteq H$

but H is finite

$\Rightarrow$ S finite

$\Rightarrow \exists\, n, m \in \mathbb{Z}^+$, $n \neq m$

and $a^n = a^m$, otherwise a^k are distinct $\forall k \in \mathbb{Z}^+$

$S = \{a^k, k \in \mathbb{Z}^+\}$ infinite subset of H which is finite.

ما بزبط احكي انو في Infinit set من Finite set(H)

$\Rightarrow a^n = a^m$, $n \neq m$, $n, m \in \mathbb{Z}^+$, Say $n < m$

by cancillation Law: $a^n = a^n a^{m-n}$

$e = a^{m-n}$

and $a \neq e \Rightarrow m-n > 1 \Rightarrow e = aa^{m-n-1}$, $m-n-1 \geq 1$

$m-n \geq 2$

$\Rightarrow a^{-1} = a^{m-n-1} \in S \subseteq H$

$\Rightarrow H \subseteq G$

Cayley $G = \mathbb{Z}_6$

$H = \{0, 2, 4\}$, $S = \{0, 2, 3, 4\} \not\subseteq G$

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$H \subseteq G$

$\oplus_6$	0	2	3	4
0	0	2	3	4
2	2	4		
3	3	(5)		
4	4			

$\rightarrow 5 \notin S$.

Def: Let G be a group, $a \in G$

Then $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G

Called the subgroup of generated by a.

proof: $\langle a \rangle \neq \emptyset$ Since $a^1 = a \in \langle a \rangle$

By one Step Test, let $x, y \in \langle a \rangle$, So $\exists n, m \in \mathbb{Z}$

$\rightarrow x = a^n$, $y = a^m$

$\Rightarrow x^{-1}y = a^{-n}a^m = a^{m-n} \in \langle a \rangle$

Since $m-n \in \mathbb{Z}$

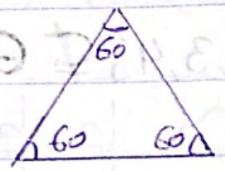
So $\langle a \rangle$ is a Subgroup of G

* Back to ch1

Dyhedral groups or Symmetric group

let $n \geq 3$, $n \in \mathbb{Z}^+$, an n-gon is an n-sided legular polygon with equal sides and outer equal angles $\frac{360}{n}$

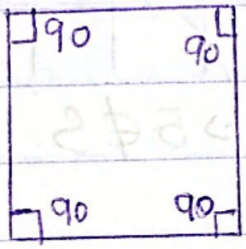
* equilaterial Triangle



$n = 3$

$\frac{360}{3} = 120$ ← الزوايا الخارجية

* Square



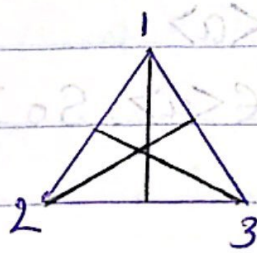
$n = 4$

$\frac{360}{4} = 90$

الزوايا الخارجية 90

~ الداخلية 90

n-gon Symmetry



Symmetries

Reflection R_1, R_2, R_3

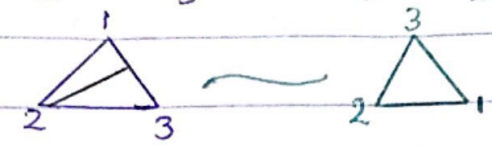
Rotation $P_0 = P_{360}, P_1 = P_{120}, P_2 = P_{240}$

* we have 6 Symmetric

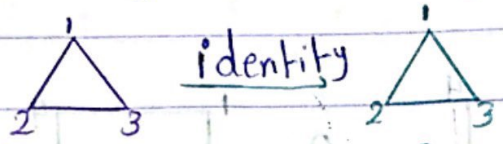
* = Composition of maps

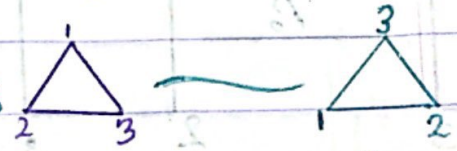
opperation ← تركيب الاقترانات

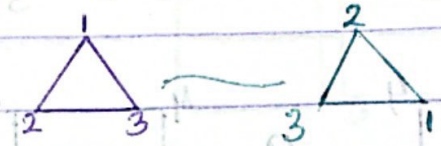
R_1 : 

R_2 : 

R_3 : 

P_0 : 

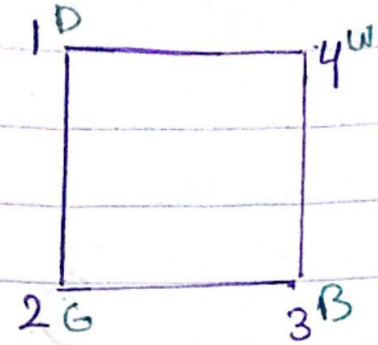
$P_1 = P_{120}$: 

$P_2 = P_{240}$: 

*	R_1	R_2	R_3	P_0	P_1	P_2
R_1	P_0	P_1	P_2	R_1	R_3	R_2
R_2	P_1	P_0	P_1	R_2	R_1	R_3
R_3	P_2	P_1	P_0	R_3	R_2	R_1
P_0	R_1	R_2	R_3	P_0	P_1	P_2
P_1	R_3	R_1	R_2	P_1	P_2	P_0
P_2	R_2	R_3	R_1	P_2	P_0	P_1

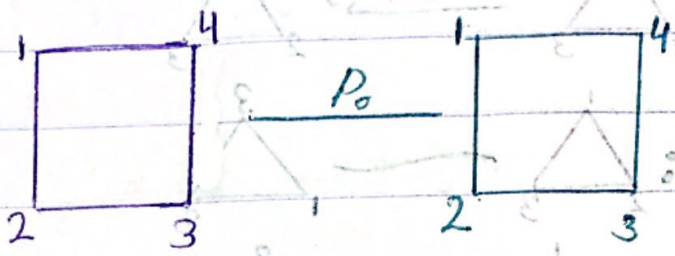
* نستوي بالباقي.

* Square

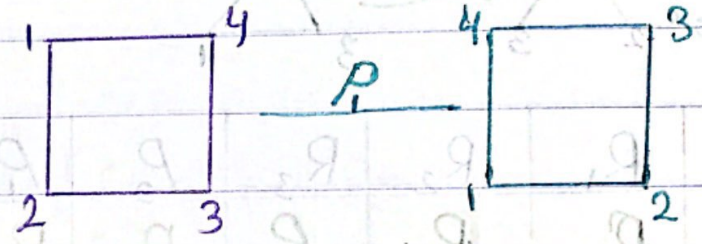


Rotation

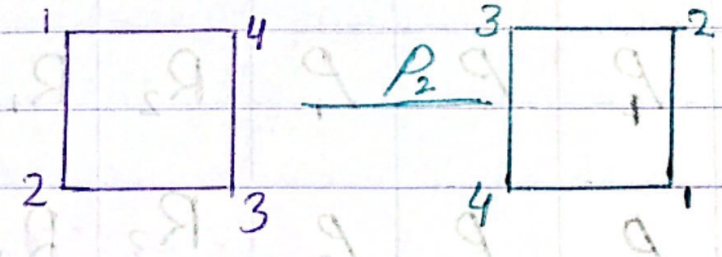
$P_0 = R_0 = R_{360}$



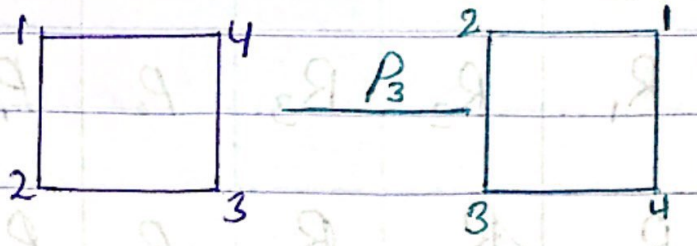
$P_1 = R_{90}$



$P_2 = R_{180}$

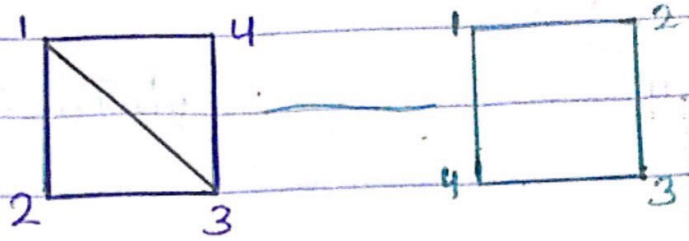


$P_3 = R_{270}$

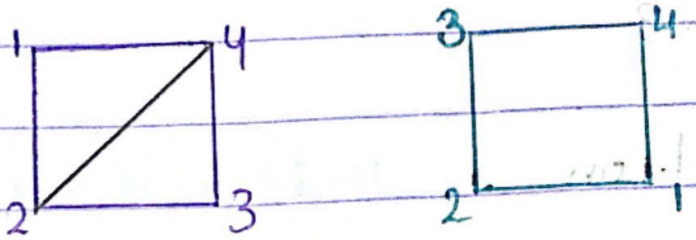


Reflection

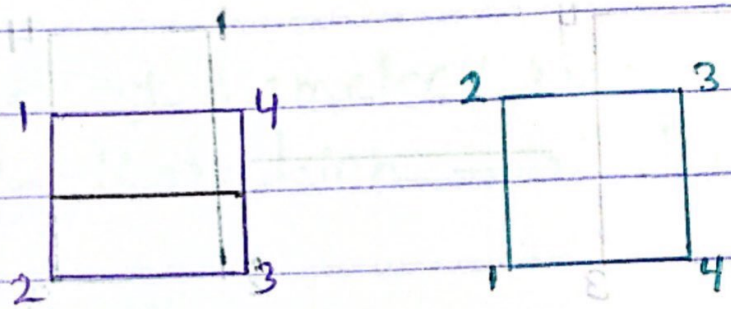
$D = P_{13}$:



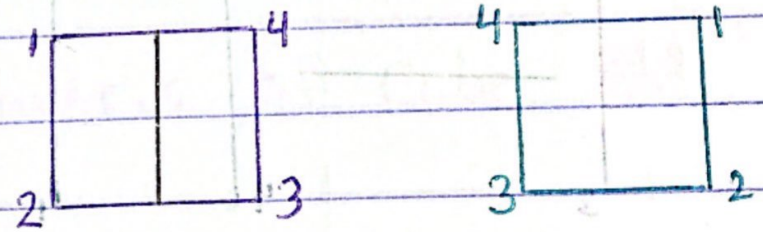
$D' = P_{24}$:



H Horizontal :



V Vertical :



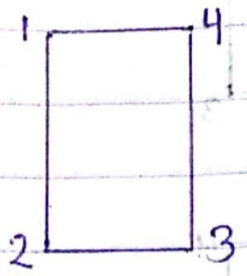
* page (31)

موجودة في الـ table كلها
اذا حبا يدو يطلع عليها

symmetrices.

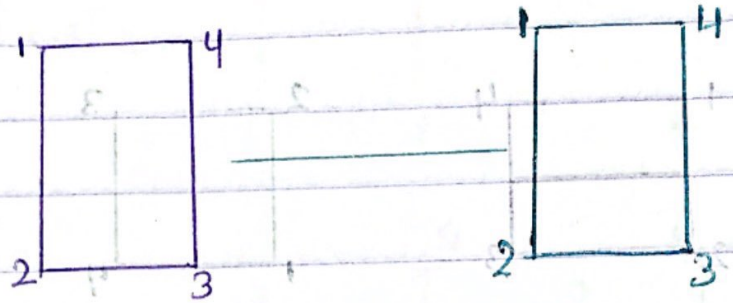
*Rectangle

*نلتزم بالتسمية من البداية.

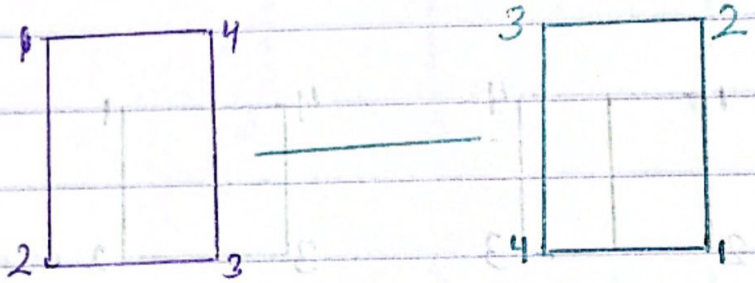


*Rotation

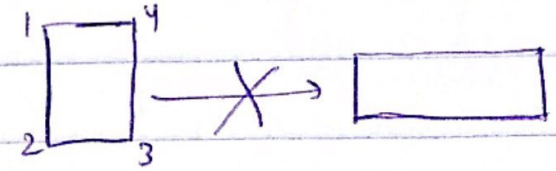
P_0 :



P_{180}



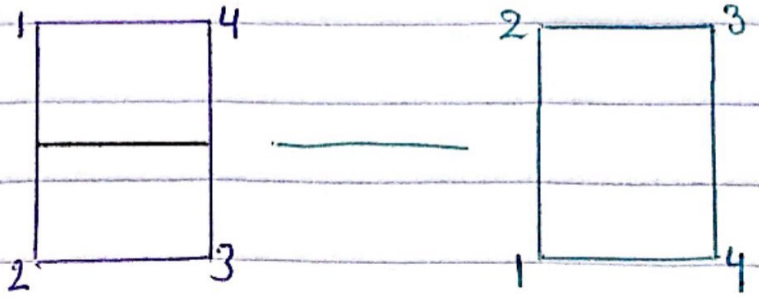
P_{90}



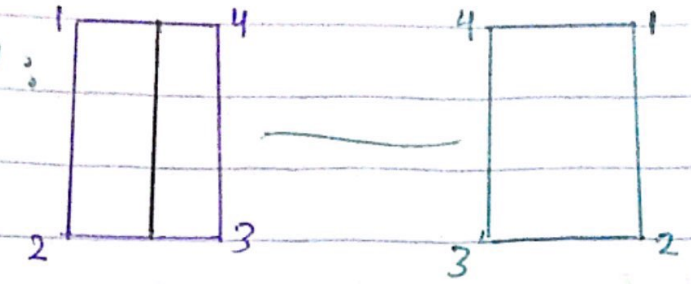
P_{90} مايناظرهو في ماعنا P_{270} أو

*Reflection

H:



V:



* Circle

*Reflection اي قطر يربط

* any diameter (قطر) → infinite

Rotation (عند اي زاوية يربط) → infinite

*Symmetric infinite

H.W) Symmatric of Cube 

* n-gon , $n \geq 3$ للشكل المنتظم

# of Symmetrices is $2n$: n Reflections + n Rotations

The set of all Symmetrics of n-gon is anonabelian groub called the group of symmetrics or the Dihedral group denoted by D_n

$|D_n| = 2n$, $|D_3| = 6$, $|D_4| = 8$

* الحصة الجاية نكمل ch 3

Chapter 4

Cyclic groups

G group, $a \in G$, $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$
$\langle a \rangle \leq G$, a is called a generator of $\langle a \rangle$

Def: let G be a group, if $\exists\, g \in G$ $\langle g \rangle = G$, Then G is called a cyclic group, and g is called a generator of G

Ex: $(\mathbb{Z}, +)$ is cyclic: 1 generator $\in \langle 1 \rangle$
Since $n \in G$, $n = \underbrace{1+1+1+1+\cdots+1}_{n \text{ times}} = 1^n = n(1)$

-1 is also a generator
Since $n \in \mathbb{Z} = n = (-1)^{-n} = -n(-1) = n$
$\{-1, 1\}$ are only generators of $\mathbb{Z}$
Since if $K \neq \pm 1$, $K \in \mathbb{Z}$
$\langle K \rangle = \{K^i = iK, i \in \mathbb{Z}\}$

EX: $\mathbb{Q}, +$: Is $\mathbb{Q}$ Cyclic
No: $a \in \mathbb{Q}$, $a = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$
$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$
Take $\frac{1}{2}$ $a \in \mathbb{Q}$
Is $\frac{1}{2}a$ can be written as $a^i = ia$, $i \in \mathbb{Z}$
$\frac{1}{2}a \notin \langle a \rangle$
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ not cyclic

Ex: $\mathbb{Z}_n, \oplus_n$, Is it cyclic yes

1 generator

$k \in \mathbb{Z}_n$, $K(1) = 1^k \in \langle 1 \rangle$

$(\mathbb{Z}_p^*, \otimes_p)$ is cyclic

$(\mathbb{Z}_4, \oplus_4)$

Cyclic : $\langle 1 \rangle = \mathbb{Z}_4$

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

$\langle 1 \rangle = \mathbb{Z}_4$

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

$\langle 3 \rangle = \{3, 2, 1, 0\} = \mathbb{Z}_4$

Two generator 1, 3

$\mathbb{Z}^* : 1, -1$

$-1 = 1^{-1}$ inverse

$3 = 1^{-1} = 4 - 1$

Remark: If G is Cyclic generated by g

Then g^{-1} is another generated.

Since if $x \in G = \langle g \rangle$

$\exists k \in \mathbb{Z}$ s.t $x = g^k$

$= (g^{-1})^{-k}$, $-k \in \mathbb{Z}$

$G < g^{-1} >$

Th. If $g \in G$, $|g| = n$ and $g^k = e$
Then $n \mid |k|$ $(n \mid k)$

← ما بتفرق كتير اذا حطيت العلاقة المطلقة

DA: If $m, n \in \mathbb{Z}$, Then $\exists\ q, r \in \mathbb{Z}$
s.t $m = nq + r$: $0 \leq r < |n|$

$\begin{cases} n, k \in \mathbb{Z} \\ n \mid k \leftrightarrow \exists q \in \mathbb{Z} \\ k = nq \end{cases}$

$4 \overline{)-15}$ -3, ± 12, -3 ← لازم رقم سالب موجب

$4 \overline{)-15}$ -4, ± 16, 1

Th. let G be a group, $a \in G$, Then
① $|a| = \infty \leftrightarrow \forall i \neq j \in \mathbb{Z} \Rightarrow a^i \neq a^j$
② $|a| = n$ Then $a^i = a^j \leftrightarrow n \mid i-j$

proof:
(1) $|a| = \infty$ $(\Rightarrow)$ $\forall n \in \mathbb{Z}^+$
$a^n \neq e$ So $i \neq j \Rightarrow a^i \neq a^j$
Otherwise if $i \neq j$, $a^i = a^j = e^{i-j} = e$
(finite تناقض) $|a| < |i-j|$ contradiction
$\Leftarrow$ $|a| = n$, let $i = n$, $j = 0$
$(\Rightarrow)$ $i \neq j$ but $a^i = a^j$

(2) $(\Rightarrow)$ let $|a| = n$
and $a^i = a^j \Rightarrow a^{i-j} = e$
$\Rightarrow n \mid i-j$

$(\Leftarrow)$

$n \mid i-j = i-j = nK \Rightarrow a^{i-j} = a^{nK} = (a^n)^K = e$

$\Rightarrow a^{i-j} = e \Rightarrow a^i = a^j$

Th. let G a group ; $a \in G$, $|a| = n$ and $d \mid n, d > 0$

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

proof: Since $(a^d)^{\frac{n}{d}} = a^{d \cdot \frac{n}{d}} = a^n = e$

$\Longrightarrow |a^d| \leq \frac{n}{d}$, suppose $|a^d| < s < \frac{n}{d}$

$(a^d)^s = e \Rightarrow a^{ds} = e \Rightarrow ds < d \cdot \frac{n}{d} = n$

$|a| \leq ds < n$ X لانو المعروف انو n هو اصغر ... مرفوض وهو المطلوب

Ex: Z_5^+ : generators

* معنى انو ال operation هو +

$1, 4, 2, 3$

$\langle 2 \rangle = \{2, 4, 1, 3, 0\} = Z_5$

$\langle 3 \rangle = \{2, 4, 1, 3, 0\}$

$3 = 2^{-1}$ $= \langle 2 \rangle$

Z_8

$1, 7$

$\langle 2 \rangle = \{2, 4, 6, 0\}$

$\langle 3 \rangle = \{3, 6, 1, \ldots\} = Z_8$

ما بكمل لانو اعطاني ال generater فالواحد بيعطي الباقي ..

CamScanner الممسوحة ضوئيا بـ

ماكانش
راي احسب
5
لانها
$5 = 3^{-1}$

$\langle 4 \rangle = \{4, 0\}$

$\langle 5 \rangle = \{5, 2, 7, 4, 1, \ldots\} = \mathbb{Z}_8$

$\langle 6 \rangle = \langle 2 \rangle$ — لانها 2^{-1}

2^{-1}

وال هو Generation — generaters 1, 7, 3, 5

(انو هون القوى هي ارقام) $1, 1^3, 1^5, 1^7$

$1^3 = 3$, $1^5 = 5$, $1^7 = 7$

1, 3, 5, 7 relatively prime 8

$\mathbb{Z}_5$: 1, 2, 3, 4 relatively prime 5

$\mathbb{Z}_6$: 1, 5 — بدون ما احسب

$\mathbb{Z}_9$: 1, 2, 4, 5, 7, 8 — generaters — بس نشيل مضاعفات ال 3

Th. let G be a group, $a \in G$, Then
$|a| = |\langle a \rangle|$

proof: If $|a| = \infty$, then $a^n = e \iff n = 0$

$\Rightarrow \langle a \rangle = \{a^k, k \in \mathbb{Z}\}$, $a^i \neq a^j$, $\forall\, i \neq j$

$\Rightarrow |\langle a \rangle| = \infty$

also, $|a| = n \Rightarrow \langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$

$|\langle a \rangle| = n$

CamScanner الممسوحة ضوئيا بـ

Th. let G be a group. $a \in G$, $|a| = n$ and $K \in \mathbb{Z}^+$
Then $\langle a^K \rangle = \langle a^{\gcd(n,K)} \rangle$ and $|a^K| = \frac{n}{\gcd(n,K)}$

proof: For simplicity let $d = \gcd(n,K) \Rightarrow d|n, d|K$ ($K = ds$)
we show $\langle a^K \rangle = \langle a^d \rangle$
$\langle a^K \rangle \subseteq \langle a^d \rangle$ — ① since $x \in \langle a^K \rangle$
$\Rightarrow \exists e \in \mathbb{Z} \rightarrow x = |a^K|^e = a^{Ke} = a^{dse} =$
$= (a^d)^{se} \in \langle a^d \rangle$

Now, we show $\langle a^d \rangle \subseteq \langle a^K \rangle$, show $a^d \in \langle a^K \rangle$
$d = s_1 n + tK$

$a^d = a^{s_1 n + tK} = \underbrace{(a^n)^{s_1}}_{e} \cdot (a^K)^t = (a^K)^t \in \langle a^K \rangle$

$\Rightarrow \langle a^d \rangle \subseteq \langle a^K \rangle$ — ②

Number theory
$d = \gcd(n,K)$
$s_1, t \in \mathbb{Z}$
$d = s_1 n + tK$

①, ② $\Rightarrow \langle a^K \rangle = \langle a^d \rangle$

$\Rightarrow$ by pervious Th.
$|a^K| = |\langle a^K \rangle| = |\langle a^{\gcd(n,K)} \rangle| = |a^{\gcd(n,K)}|$
$= \frac{n}{\gcd(n,K)}$ ($\gcd(n,K)|n$)

($|a| = n$, $d|n \Rightarrow |a^d| = \frac{n}{d}$)

Cordy ① If G is a group, $a \in G$, $|a| = n$

$k, m \in \mathbb{Z}^+$

Then $|a^k| = |a^m| \iff \gcd(n,k) = \gcd(n,m)$

proof: $|a^k| = |a^m| \iff \frac{n}{\gcd(n,k)} = \frac{n}{\gcd(n,m)} \iff \gcd(n,k) = \gcd(n,m)$

Corrly ② let G be agroup, $|G| = n$, a generator of G, $G = \langle a \rangle$, $|G| = |a| = n$, Then a^k is a generator of G

iff: $|a^k| = n = \frac{n}{\gcd(n,k)} \iff \gcd(n,k) = 1$

Example: $\mathbb{Z}_{12}$, Find ① all generators of $\mathbb{Z}_{12}$

② Find all elements in $\mathbb{Z}_{12}$ with order 4

③ $|a| = 3$

Sdw ① 1 generators, all generaters of $\mathbb{Z}_{12}$ are of the form 1^k, $\langle k, 12 \rangle = 1$

$\Rightarrow 1, 5, 7, 11$

$1^1 = 1$, $1^5 = 5$, $1^7 = 7$, $1^{11} = 11$

② $1^3 = 3 \Rightarrow |3| = \frac{12}{3} = 4$

1^k, $\gcd(12,k) = 3$

$k = 3, 9$

③ $1^4 = 4$, 1^k $\gcd(12,k) = 4$

$k = 4, 8$

Ex: $(\mathbb{Z}_{11}^*, \otimes_{11})$, $|\mathbb{Z}_{11}^*| = 10$, $\mathbb{Z}_{11}^* = \{1, 2, \dots, 10\}$

Is $\mathbb{Z}_{11}^*$ cyclic, if so Find all generators of $\mathbb{Z}_{11}^*$

$2: 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,\ 2^6 = 9$

$2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 12$

$|2| = 10 = |\mathbb{Z}_{11}^*| \Rightarrow \mathbb{Z}_{11}^*$ is Cyclic

all generators 2^K, $\gcd(10, K) = 1$

relatively prime to 10

$K = 1, 3, 7, 9$

generator $2^1, 2^3, 2^7, 2^9$ → $2, 8, 7, 6$

Corly ③ let G be cyclic with $|G| = n$

Then for any $g \in G$, $|g| \mid |G|$

Since $G = \langle a \rangle$, $|a| = n$ and $g \in G$

$\Rightarrow g = a^K$, $|g| = |a^K| = \frac{n}{\gcd(n, K)}$

with divides $n = |G|$

RMK: ① In $G = \mathbb{Z}_n$, all generators of $\mathbb{Z}_n$ are 1^K, $\gcd(n, K) = 1$

$k(1) = k$

② let G cyclic, $G = \langle a \rangle$, $|a| = n$

Then all generators of G are a^K

$\gcd(n, k) = 1$

Ex: $G=\langle a\rangle$, $|G|=|a|=30$, Find ① generators.

a^K, $\gcd(30,K)=1$ ② $|a^{12}|$

$K=1,7,11,13,17,19,23,29$

$|a^{12}|=\frac{30}{\gcd(30,12)}=\frac{30}{6}=5$

Fundamental Th. of cyclic groups (FTCG)

أهم نظرية

Th. A subgroup of cyclic is cyclic and if G is finite cyclic with $|G|=n$ Then for $K|n$, $\exists!$ subgroup $H\leq G$ $\rightarrow |H|=K$

[! → unique]

proof: let G be cyclic, and $H\leq G$,

Say $G=\langle a\rangle$, $a\in G$

Case 1: if $H=\{e\}$, then H is cyclic and $H=\langle e\rangle$

So Case 2: let $H\neq\{e\}$, since $H\leq G$, So $\exists x\in H$

$x\neq e$, $x\in G=\langle a\rangle$ ($\{e\}\neq$)

So $\exists K\in\mathbb{Z}\rightarrow x=a^K \Rightarrow x^{-1}=a^{-K}\in H$

So $\exists K\in\mathbb{Z}^+\rightarrow a^K\in H$

Consider $S=\{i\in\mathbb{Z}^+, a^i\in H\}\neq\phi$

Since $i=K$ ($x=a^K$) or $-K$ ($x^{-1}=a^{-K}$)

By well-ordering principle

S has a least element m

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

Number Th.

well ordering princip

Any nonempty Subset

$\mathbb{Z}^+=\mathbb{N}$

has aleast elemat

RHS $\subseteq H$ by closure property since $a^m \in H$ — ①

we show $H \subseteq \langle a^m \rangle$

let $y \in H \leq G = \langle a \rangle$, so $y = a^\ell$, $\ell \in \mathbb{Z}$,

by D.A: $\exists\, q, r \in \mathbb{Z} \Rightarrow \ell = mq + r$, $0 \leq r < m$

$a^\ell = a^{mq+r} \in H$, $a^{mq} \in H \Rightarrow a^r = a^{\ell - mq} \in H$, $0 \leq r < m$

$r = 0 \Rightarrow 0 = mq \Rightarrow y = a^\ell \in \langle a^m \rangle$

$\Rightarrow H \subseteq \langle a^m \rangle$ — ②

①, ② $\Rightarrow H = \langle a^m \rangle$

Secand part, let G finite cyclic $|G| = n$, $G = \langle a \rangle$

$k \mid n$, show $\exists!\, H \leq G$, $|H| = k$

let $H = \langle a^{\frac{n}{k}} \rangle \Rightarrow |H| = |a^{\frac{n}{k}}| = \frac{n}{\frac{n}{k}} = k$

uniquenses, let $K \leq G$, $|K| = k$

K is cyclic $K = \langle a^m \rangle$, m smallest +ve integer

$a^m \in K$, $m \mid n \Rightarrow |K| = |a^m| = \frac{n}{m} = \frac{n}{\frac{n}{k}}$

$\rightarrow \quad m = \frac{n}{k} \Rightarrow K = H = \langle a^{\frac{n}{k}} \rangle$

Th. let G be cyclic with $|G|=n$, then the # of generators of G is $\phi(n)$ where $\phi(n) = |U(n)|$

proof: let $G = \langle a \rangle$, $|a|$. then the generators of G are a^k, $\gcd(k,n)=1$, $1 \le k < n$
number of such k is $|U(n)| = \phi(n)$

Ex: $G = Z_{12}$
generators $1^k = k$, $\gcd(k,12)=1$
$k = 1, 5, 7, 11$

Th: let G be finite and $n \mid |G|$, Then The number of elements in G which has order n is a multiple of $\phi(n)$

proof: let $n \in Z^+$, $n \mid |G|$, If G has no element of order n, Then # of elements in G of order n is Zero and Zero is a multiple of $\phi(n)$
(any $k \in Z^+$, $k|0$) so we are done

So Suppose G has an element $a_1 \in G$ s.t. $|a_1| = n \Rightarrow |\langle a_1 \rangle| = n \Rightarrow \langle a_1 \rangle$ has $\phi(n)$ elements of order n if all element in G of order n are in $\langle a_1 \rangle$ Then G has $\phi(n)$ element of order n

Otherwise G has an element a_2, $|a_2| = n$ but $a_2 \in \langle a_1 \rangle$ so $\langle a_1 \rangle$ has $\phi(n)$ element of order n and $\langle a_2 \rangle$ has $\phi(n)$ element of order $\phi(n)$, so if any element in G of order n is either in $\langle a_1 \rangle$ or in $\langle a_2 \rangle$, Then G has $2\phi(n)$ elements of order n, otherwise $\exists\, a_3 \in G \setminus (\langle a_1 \rangle \cup \langle a_2 \rangle)$, $|a_3| = n$

$\langle a_1 \rangle \longrightarrow \phi(n)$ elements
$\langle a_2 \rangle \longrightarrow \sim \quad \sim$
$\langle a_3 \rangle \longrightarrow \sim \quad \sim$
$\vdots$
$\langle a_k \rangle \longrightarrow \sim \quad \sim$

$\Rightarrow G$ has $k\phi(n)$ element of order n

Chapter 5:

permutation group (symmetric group)

Def: let X be a non empty set, a permutation α on X is bijective (1-1 onto) from X onto X

$\alpha : X \longrightarrow X$; α 1-1, onto

Ex: $X = \mathcal{N} = \mathbb{Z}^+$, $\alpha : X \longrightarrow X$, 1-1 not onto

$\alpha(n) = 2n$ is α a permutation.

Range $R_\alpha = 2\mathbb{Z}^+ \equiv$ even, α is not a permutation

EX If X is finite

$X = \{1, \dots, n\}$, and $\alpha : X \longrightarrow X$, Then

α is 1-1 $\iff$ α is onto

Th. let X be nonempty set then the set of all permutations on X denoted by S_X is a group under The Composition of maps (If $\alpha, \beta \in S_X$, then $\alpha\beta = \alpha \circ \beta$)

(الغا بم بيتا)

proof: ① binary: let $\alpha, \beta \in S_X \Rightarrow \alpha, \beta$ bijective on X

$\Rightarrow \alpha\beta = \alpha \circ \beta : X \longrightarrow X$ bijective

$X \xrightarrow{\alpha} X \xrightarrow{\beta} X$

$f : A \xrightarrow{\text{bij}} B \xrightarrow{\text{bij}} C$

$gof : A \longrightarrow C$ is bijective

$\alpha\beta = \alpha \circ \beta : X \longrightarrow X$ bijective

② associative True for all functions.

③ Identity: $I(x) = x$, $\forall x \in X$ denoted by ϵ

④ Inverse: let $\alpha \in S_X$

If $\alpha : X \longrightarrow X$ bijective

$\alpha^{-1} : X \longrightarrow X$ is defined.

$\Rightarrow \alpha^{-1} \in S_X$

Notation: if X finite $|X| = n$, then we consider X as $\{1, 2, \ldots, n\}$, and S_X is denoted by S_n

RMK: S_X non abielian if $|X| \geq 3$

rotation: If $\alpha \in S_n$, then we can represent α by a 2 row matrix α: $\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$

EX: list elements of S_1, S_2, S_3

$S_1 = |\epsilon|$ $\quad 1 \longrightarrow 1$

identity

$S_2 : \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $\alpha : \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

$S_2 = |\epsilon, \alpha|$

$S_3 : \overset{\epsilon}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}$

$\alpha_1 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\alpha_2 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\alpha_3 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\alpha_4 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \longrightarrow$ shift 1

$\alpha_5 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \longrightarrow$ shift 2.

$|S_3| = 6$

$|S_n| = n!$

1. # of choices $\rightarrow n$
2. # of choices $\rightarrow n-1$
3. $\sim \quad \sim \quad \sim \rightarrow n-2$

n # of choices $\rightarrow 1$

* D_n # of Symmetries of n-gon

$\alpha \in D_n : \alpha : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$

α 1-1 on to

$\alpha \in S_n$

$D_n \leq S_n$

$|D_n| = 2n, \quad |S_n| = n!$

$n = 3, \ 2n = 6 \neq 3!$

$D_3 = S_3 \rightarrow$ لأن ترتيباتهما

$3 = n$ لما

$n > 3 \ldots, D_n \not\leq S_n$

D_n not abelian $\Longrightarrow$ S_n not abelian

$n \geq 3$ $\qquad$ $n \geq 3$

Ex: $\alpha, \beta \in S_4$, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ Find $\alpha\beta$, $\beta\alpha$

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

لـ اذا تكرر اي رقم بكون الحل غلط

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

مثال — يا انو طلع عنا $\alpha\beta = \beta\alpha$ وهاي مابكون متساويا.

Ex: $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

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

$\alpha\beta$: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\beta\alpha$: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\alpha\beta \neq \beta\alpha$

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

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

$$\alpha\gamma \neq \gamma\alpha$$

Cycle: $\alpha = (x_1\ x_2 \text{ --- } x_k)$ is called a Cycle with all elements not in the cycle are fixed.

$x_1 \to x_2$

$x_2 \to x_3$

$\vdots$

$x_i \to x_{i+1}$

$\vdots$

$x_k \to x_1$

Ex: $n = 4$ $\quad (1\ 2)$ $\quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$

انو الموجودة بال cycle هي ال 2 و 1 وهذا مريح الموجودة في ال cycle وإذا هي 4 و 3 بتكون Fixed

$\epsilon = (1) \equiv \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$

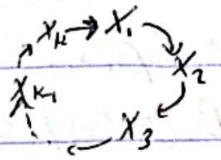
$(2) \equiv$

بقدر امثل identity بس اني احط عنصر واحد بالcycle

Def: A subgroup of S_X is called a permutation group.

Def: A cycle of the form $\alpha = (x_1, \dots, x_k)$, The length of α is k

طول الدائرة



والي مابتونو جوى الدائرة

fixed point بتونو

Def: The transposition is a cycle of length 2 which is (xy)

Def: Two cycles α, β are called disjoint cycle $\leftrightarrow$ α, β no elements or numbers is common

Ex: $\alpha = (1\ 3\ 5\ 7)$, $\beta = (2\ 4\ 8)$, $\gamma = (3\ 2\ 6)$

α, β disjoints ما في شي مشترك بينهم

but α, γ and β, γ not disjoints

length α is 4, length β is 3, length γ is 3

$(1\ 3)$ Transposition.

Th. Disjoint cycles commute

proof: let $\alpha, \beta \in S_n$, α, β Disjoint and let $x \in \{1, 2, \ldots, n\}$ show $\alpha\beta(x) = \beta\alpha(x)$

$x \notin \alpha$, $x \notin \beta$ or $x \in \alpha$, $x \notin \beta$, or $x \in \alpha$, $x \in \beta$

Case 1: $x \notin \alpha$, $x \notin \beta \Rightarrow \alpha(x) = x$, $\beta(x) = x$

$\Rightarrow (\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$

and $(\beta\alpha)(x) = \beta(\alpha(x)) = \beta(x) = x$

$\Rightarrow \alpha\beta(x) = \beta\alpha(x)$

Case 2: $x \in \alpha$, $x \notin \beta$, Say $\alpha(x) = y$

$\Rightarrow \alpha\beta(x) = \alpha(\beta(x)) = \alpha(x) = y$

$\Rightarrow \beta\alpha(x) = \beta(\alpha(x)) = \beta(y) = y$ Since both $x, y \notin \beta$

$\Rightarrow \alpha\beta(x) = \beta\alpha(x)$

Case 3: Similar, $x \in \beta$, $x \notin \alpha \Rightarrow \alpha(x) = x$ and Say, $\beta(x) = z$

$\Rightarrow \beta\alpha(x) = \beta(x) = z$

$\Rightarrow (\alpha\beta)(x) = \alpha(z) = z$

$\Rightarrow \alpha\beta(x) = \beta\alpha(x)$

$\Rightarrow \alpha\beta(x) = \beta\alpha(x), \forall x \in (1, \ldots, n)$

$\Rightarrow \alpha\beta = \beta\alpha$

Th. Any permutation $\alpha \in S_n$ can be written as a product of disjoint cycles

proof: let $\alpha \in S_n$ if α is a cycle then done

So let $\alpha \in S_n$, α not a cycle

So let $x_1 \in (1, \ldots, n)$ be any element which is not fixed under α

let $A_1 = (X_1\ X_2\ X_3 \cdots X_{K_1}) \neq A$

So $\exists\ y_1 \in A$, $A(y_1) \neq y_1$

$y_1 \notin (X_1 \text{ — } X_{K_1})$

let $A_2 = (y_1\ y_2 \cdots y_{K_2})$

if $A = A_1 A_2$

otherwise $\exists\ Z_1 \in (1 \text{ — } n)$ s.t $A(Z_1) \neq Z_1$

$Z_1 \notin A_1$, $Z_1 \notin A_2$

let $A_3 = (Z_1\ Z_2 \text{ —— } Z_{K_3})$; if $A = A_1 A_2 A_3$ then done

Otherwise $A = A_1 A_2 A_3 A_4$ or

$$A = A_1 A_2 A_3 \cdots A_K, \quad K \leq \frac{n}{2}$$

Ex: $A \in S_8$, $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 4 & 6 & 5 & 8 & 7 \end{pmatrix}$

write A as a product disjoint cycles

$A = (132)(56)(78)$

هون الترتيب مش مهم

$(87)(321)(65)$

نفس الشي

"الطريقة مش وحيدة" unique

Th. Any cycle (or any permutation) in S_n Can be written as a product of transposition

proof: let $A = (X_1 \text{ — } X_K) \in S_n$

Then $A = \underbrace{(X_1 X_K)(X_1 X_{K-1})(X_1 X_{K-2}) \cdots (X_1 X_2)}_{\#\ K-1}$

Ex: $(1\ 3\ 7) = (1\ 7)(1\ 3)$

$1 \to 3$

$7 \leftarrow 1$ و $1 \to 3$ لأن

$7 \leftarrow 3$ لأن

Ex: $(1\ 3\ 5\ 7) = (1\ 7)(1\ 5)(1\ 3) \to 3$

$(1\ 7)(1\ 5)$ لأن fixed 3 و $(3 \leftarrow 1)$

$(5 \leftarrow 3) \leftarrow 5 \leftarrow 1 \leftarrow 3$

$(7 \leftarrow 5)\ 7 \leftarrow 1 \leftarrow 5$

$1 \leftarrow 7$

نفس عدد Transposition ③

نغير cycle

$(5\ 7\ 1\ 3) = (5\ 3)(5\ 1)(5\ 7) \to 3$

$=$

$(3\ 5\ 7\ 1) = (3\ 1)(3\ 7)(3\ 5) \to 3$

$(1\ 3\ 5\ 7) = (1\ 3\ 5\ 7) \in$ identity

$= (1\ 7)(1\ 5)(1\ 3)\ \underbrace{(1\ 2)(1\ 2)}_{\in}(1\ 2)(1\ 2)(5\ 7)(5\ 7) \to 9$

$\to 5 \quad \to 7$

ضرب بالـ identity كمرات

المشترك بين هذول الأعداد (9, 7, 5, 3) أنهم أعداد فردية.

$(xy)(xy) = \in$

$(1\ 2\ 3) = (1\ 3)(1\ 2) \to 2$

$(2\ 3\ 1) = (2\ 1)(2\ 3) \to 2$

$(1\ 2\ 3)\in = (1\ 3)(1\ 2)(1\ 2)(1\ 2) \to 4$

identity

Def: A permutation is called even (odd) permutation if σ is written as product of an even (odd) number of Transpositions

$(1\ 2\ 3) = \underbrace{(1\,3)(1\,2)}_{\text{even}}$ even

$(1\ 2\ 3\ 4)$

$(1\,4)(1\,3)(1\,2) \rightarrow$ odd.

RMK: if $\sigma = (x_1 \dots x_k)$ k even.

$= \underbrace{(x_1 x_k) \dots (x_1 x_2)}_{k-1}$

$\Rightarrow \sigma$ odd.

if k odd $\Rightarrow \sigma$ even

Ex) Is $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 1 & 2 & 7 & 5 & 6 & 8 & 9 \end{pmatrix}$

Is σ even or odd.

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

$= \underbrace{(1\,3)(1\,2)(1\,4)}_{3} \underbrace{(5\,6)(5\,7)}_{2} \quad = 5$

σ odd

RMK: ① let α, β be even, Then $\alpha\beta$ is even (even+even = even)
② α even, β odd $\rightarrow \alpha\beta$ is odd (even+odd = odd)
③ α, β odd $\rightarrow \beta\beta$ even (odd + odd = even).

Def: ϵ is even

$$\epsilon = \frac{(xy)(xy)}{2}, \quad x \neq y$$

Th. A permutation is always either even or always odd

Def: The set of all even parmutation in S_n is denoted by A_n

Th. For any $n \geq 2$, $A_n \leq S_n$

proof: $A_n \neq \phi$ since $\underset{\text{identity}}{\epsilon} \in A_n$

So let $\alpha, \beta \in A_n \Rightarrow \alpha, \beta$ even $\Rightarrow \alpha^{-1}, \beta^{-1}$ even
$\Rightarrow \alpha\beta^{-1}$ is even $\Rightarrow \alpha\beta^{-1} \in A_n \Rightarrow A_n \leq S_n$

A_n is called the alternating subgroub of S_n

Th. For any $n \geq 2$

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

proof: HW

let odd permutations by B_n → not subgroup since $\epsilon \notin B_n$

Show $|A_n| = |B_n|$

$\phi : A_n \to B_n$ 1-1 onto

ϕ 1-1 onto

or show $|A_n| \leq |B_n|$ and $|B_n| \leq |A_n|$

$\Rightarrow |A_n| = |B_n| = \frac{n!}{2}$

H.W: Ch 3: 6, 8, 12, 13, 14, 18, 24, 26, 33, 43, 45, 60

Ch 4: 8, 10, 13, 14, 15, 20, 22, 30, 32, 40, 41, 54

التسليم لغاية يوم الاربعاء 21/10

Th. let α, β disjoint cycles in S_n, Then

$|\alpha\beta| = Lcm(|\alpha|, |\beta|)$

proof: Let $\alpha, \beta \in S_n$, $|\alpha| = n$, $|\beta| = m$

$|\alpha\beta| = k$

$\alpha^n = \epsilon$, $\beta^n = \epsilon$, $(\alpha\beta)^k = \epsilon$

we show $k = Lcm(m,n)$

① we show $k \leq Lcm(m,n)$

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

$= (\alpha^m)^{e_1} (\beta^n)^{d_2}$

$= \epsilon \epsilon = \epsilon$

$|\alpha\beta| = k \leq Lcm(|\alpha|, |\beta|)$ — ①

$\alpha\beta = \beta\alpha$

$Lcm(m,n) = m\ell_1 = n\ell_2$

Lcm: least common multiple

RMK: $a, b \in G$

$ab = ba$, Then

① If $|a|, |b|$ relatively prime, Then $|ab| = |a||b| = Lcm(|a|, |b|)$

② $|ab| \neq Lcm(|a|, |b|)$ بشكل عام غير صحيح

EX: G group, $a \in G$

$b = a^{-1}$

$|a| = n$, Then $|ab| = |e| = 1 \neq Lcm$

$= Lcm(|a|, |a^{-1}|)$

$= n$

② Now we show $Lcm(m,n) \leq K$

$(\alpha\beta)^K = \epsilon \Rightarrow \alpha^K \beta^K = \epsilon \Rightarrow \alpha^K, \beta^{-K}$

[but α, β disjoint α^K, β^K disjount unless $\alpha^K = \beta^K = \epsilon$
$\Rightarrow \alpha, \beta^{-1}$ disjoint

$\Rightarrow \alpha^K = (\beta^{-1})^K = \epsilon \Rightarrow \alpha^K = \epsilon$ and $\beta^{-1} = \epsilon$

$\Rightarrow \beta^K = \epsilon$

$\Rightarrow m \mid K,\ n \mid K \Rightarrow Lcm(m,n) \leq K$ — ②

from ① and ② $K = Lcm(m,n)$

* Ch 5 Done.

Back to ch 4: Lattic Diagrame or Cayle diagram.

let G be finite cyclic say, $|G| = n$, then for any $d \in \mathbb{Z}^+$, $d \mid n$, $\exists!$ Subgroup H of G of order d.

$G = \langle a \rangle$, $|a| = n$, $d \mid n$, Then $H = \langle a^{\frac{n}{d}} \rangle$

The Sub groups of G can be represented by a diagram. Such that $|e|$ in the bottom G on the Top

Ex: $G = Z_{12} = \langle 1 \rangle$, lattice diagram.

divisors of 12 is 1, 2, 3, 4, 6, 12

$|H_1| = 1 \Rightarrow H_1 = \langle 0 \rangle$

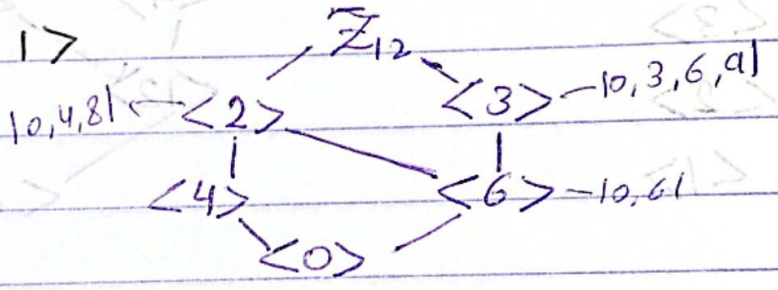
$|H_2| = 2 \Rightarrow H_2 = \langle 6 \rangle$

$H_3 = \langle 4 \rangle$

$H_4 = \langle 3 \rangle$

$H_6 = \langle 2 \rangle$

$H_{12} = Z_{12} = \langle 1 \rangle$



Ex: Lattice diagram $Z_{32} = \langle 1 \rangle$ بنمشي لنشوف العدد بجدين

divisors of 32 is 1, 2, 4, 8, 16 مش ضروري نكمل

$H_1 = \langle 0 \rangle$

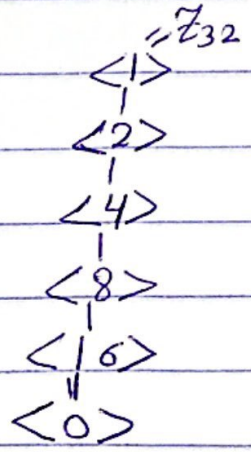
$H_2 = \langle 16 \rangle$

$H_4 = \langle 8 \rangle$

$H_8 = \langle 4 \rangle$

$H_{16} = \langle 2 \rangle$

$H_{32} = \langle 1 \rangle = Z_{32}$



Ex: Z_{36}

divisors: 1, 2, 3, 4, 6, 9, 12, 18

$H_1 = \langle 0 \rangle$

$H_2 = \langle 18 \rangle$

$H_3 = \langle 12 \rangle$

$H_4 = \langle 9 \rangle$

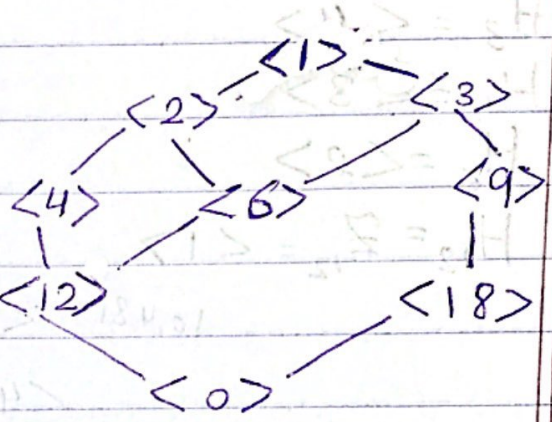
$H_6 = \langle 6 \rangle$

$H_9 = \langle 4 \rangle$

$H_{12} = \langle 3 \rangle$

$H_{18} = \langle 2 \rangle$

$H_{36} = \langle 1 \rangle$



First Exam : CH 2, 3, 4, 5, 6

28/10 Wedensday بوقت المحاضرة