1. Introduction to Group Theory

Binary Operations

Like abstract multiplication

Definition

Let A be a set. A binary operation $*$ on A is a function

$$*: A \times A \to A \; ; \; (a,b) \mapsto a * b \in A$$

We do not write $*(a,b)$

Notation:

1) $\mathbb{N}$: Natural Numbers
2) $\mathbb{Z}$: Integers
3) $\mathbb{Q}$: Rational numbers, $\mathbb{Q} = \{p/q, \; p,q \in \mathbb{Z}, \; q \neq 0\}$
4) $\mathbb{R}$: Real Numbers
5) $\mathbb{C}$: Complex Numbers

Examples: Example of binary operations

1) $+$ is a binary operation on $\mathbb{R}, \mathbb{C}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}$
2) $-$ is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, not $\mathbb{N}$
3) $/ : (a,b) \mapsto a/b$ on $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ where $S^* = S \setminus \{0\}$
4) $+$ on $M_n(\mathbb{R})$ (nxn matrices on $\mathbb{R}$)
5) $\times$ on $M_n(\mathbb{R})$

Remarks:

i) $a*b \in A$ is expressed by saying $*$ is closed or A is "closed" under $*$

Notice: '$-$' is closed on $\mathbb{Z}$ but not in $\mathbb{N}$ as

$$\underset{\in \mathbb{N}}{1} - \underset{\in \mathbb{N}}{2} = -1 \notin \mathbb{N}$$

ii) Order matters, in general, $a*b \neq b*a$

Example in $\mathbb{Z}$, $1-2 \neq 2-1$

iii) The fact that $*$ is a function with domain A means

$$\forall (a,b) \in A \times A, \quad a*b \text{ is defined}$$

$$A \times A = \{(a,b);\ a,b \in A\}$$

eg: $/$ on $\mathbb{R}$ where $(a,b) \mapsto a/b$ is not a binary operation as $a/0$ not defined

iv) The fact that $*$ is a function with $A \times A$ means for any $(a,b) \in A \times A$, $a*b$ is uniquely defined

Warning: Not always clear $*$ is well defined

Example: $*$ on $\mathbb{Q}$ given by

$$\frac{a}{b} * \frac{c}{d} = \frac{a+c}{|b|+|d|}$$

$*$ is not a binary operation as it is not well defined.

$$\frac{1}{2} * \frac{2}{3} = \frac{1+2}{2+3} = \frac{3}{5}$$

But $\frac{1}{2} = \frac{2}{4} \implies \frac{2}{4} * \frac{2}{3} = \frac{2+2}{4+3} = \frac{4}{7}$

and $\frac{3}{5} \neq \frac{4}{7} \implies$ not well defined

Definition

A binary operation $*$ is commutative if

$$\forall a,b \in A, \quad a*b = b*a$$

Examples

1) $+$ on $\mathbb{Z}$ is commutative as $a+b = b+a \ \forall a,b \in \mathbb{Z}$

2) $-$ on $\mathbb{Z}$ is not commutative as $1-2 \neq 2-1$

Notation:

Common symbols for binary operations are

1) $a \cdot b$ particularly for commutative operations
2) $a \circ b$ (composition of functions)
3) $a + b$
4) Nothing; ab called juxtaposition

Cayley Tables

$*$ on a finite set G

$*$	$\cdots$	g	$\cdots$	h	$\cdots$
$\vdots$					
g		$g*g$		$g*h$	
$\vdots$					
h		$h*g$		$h*h$	

Note

$*$ is commutative

$\Updownarrow$

table is symmetric around leading diagonal

Example: $\times$ on $\{0, 1, -1\}$ is commutative, has table

$\times$	0	-1	1
0	0	0	0
-1	0	1	-1
1	0	-1	1

But $*$ on $\{0, 1, -1\}$ with table

$*$	0	1	-1
0	0	1	-1
1	0	1	-1
-1	0	1	1

Groups

Definition 1.5 Group

A **group** $(G, *)$ is a set G together with binary operation $*$ such that

(a) **Associativity**

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

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

(b) **Existence of identity**

$\exists\ e \in G$ such that for all $a \in G$

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

(c) **Inverse**

$\forall\ a \in G, \exists\ b \in G$ such that

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

Remark:

i) (a) is called associative property

ii) we often drop '$*$' when it is clear saying 'G' rather than $(G, *)$ and writing ab for $a*b$

iii) being closed is built into definition of binary operation

Definition Order

Let G be a group.

Order of a group is the **cardinality** of the set G

$$|G| = \text{order}$$

$$\boxed{\text{A group is finite/infinite} \iff \text{order is finite/infinite}}$$

Lemma Uniqueness of identity and inverse

Let G be a group. Then

i) The element e such that
$$e * a = a = a * e \quad \forall a \in G$$
is unique

ii) given a, the element b such that
$$a * b = e = b * a$$
is unique

Proof:

i) Suppose $e, f \in G$ and for all $a \in G$
$$(1)\ e * a = a = a * e \quad \text{and} \quad f * a = a = a * f\ (2)$$
Then
$$(1)\ e * f = f \quad \text{and} \quad e * f = e\ (2)$$
$$\Longrightarrow \quad e = f$$

ii) Let $a \in G$ and suppose $b, c \in G$ with
$$b * a = e = a * b \quad \text{and} \quad c * a = e = a * c$$
Then
$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$
(associativity)

■

We say e is the identity of G, we can also write e_G, 1, 1_G

b is the inverse of a and write $b = a^{-1}$

We emphasize a^{-1} is the unique element of G such that
$$\boxed{a^{-1} * a = e = a * a^{-1}}$$

Lemma

Let G be a group. Then, $\forall a,b,c \in G$,

1) $(a^{-1})^{-1} = a$
2) $(ab)^{-1} = b^{-1}a^{-1}$
3) $ab = ac \Rightarrow b = c$ left cancellation
4) $ba = ca \Rightarrow b = c$ right cancellation

__Proof__:

1) Follows from the fact that

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

and uniqueness of inverse

2) We have

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

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

$$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$$ by uniqueness of inverses

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

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

$\Rightarrow eb = ec$ inverse

$\Rightarrow b = c$ identity

4) $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1}$

$\Rightarrow be = ce$ associativity

$\Rightarrow be = ce$ inverse

$\Rightarrow b = c$ identity

$\blacksquare$

$\boxed{\text{(3) and (4) called left and right cancellation laws}}$

Corollary

Let G be a group. Then $\forall\, a_1, \dots, a_n \in G$

$$(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$$

Proof Previous Lemma and induction

For $n=2$,

$$(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$$

by previous lemma

Inductive hypothesis: Assume true for $n=k$

$$(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$$

Inductive step: If property true for $n=k \implies$ true for $n=k+1$

$$\begin{aligned}
(a_1 \cdots a_k a_{k+1})^{-1} &= ((a_1 \cdots a_k)\, a_{k+1})^{-1} && \text{associative} \\
&= a_{k+1}^{-1} (a_1 \cdots a_k)^{-1} && \text{base case} \\
&= a_{k+1}^{-1} a_k^{-1} \cdots a_1^{-1} && \text{inductive hypothesis}
\end{aligned}$$

■

Corollary Latin Square Property

Let G be a group of finite order

Then every element of G occurs exactly once in every row and in every column of the table of G

Proof: Consider row R_a labelled by $a \in G$

$$R_a \longrightarrow \begin{array}{c|ccc} & e & & y \\ \hline e & e & & y \\ & & & \vdots \\ a & a & \cdots & ay \end{array}$$

Let $g \in G \Rightarrow a^{-1}g \in G$ closure

$$
\begin{array}{c|ccc}
 & e & & a^{-1}g \\
\hline
e & e & & a^{-1}g \\
 & & & \vdots \\
R_a \rightarrow \quad a & a & \cdots\cdots & a(a^{-1}g)
\end{array}
$$

$$a(a^{-1}g) = (aa^{-1})g = eg = g$$

So that g occurs in row R_a and column of $a^{-1}g$

If g also occurs in column labelled by h, then

$$
\begin{array}{c|cccccc}
 & e & & a^{-1}g & & h \\
\hline
e & e & & a^{-1}g & & \vdots \\
 & & & \vdots & & \vdots \\
a & a & \cdots\cdots & g & \cdots\cdots & g
\end{array}
$$

$g = a(a^{-1}g) = ah$ so by cancellation, $a^{-1}g = h$

So g occurs exactly once in R_a. Similar for columns ■

Example.

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

is the partial table of a group then we can complete it uniquely

↳ Latin square property

In any group with identity f,

$$ff = f$$

$\Rightarrow$ identity must be in leading diagonal

Definition

A group $(G, *)$ is commutative or abelian

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

Notation:

- For $X \subseteq \mathbb{C}$, $X^* = X \setminus \{0\}$
- $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$
- $\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$

Notation: If $(G, +)$ is a group, we write

- 0 for identity
- $-a$ for inverse of a

On occasion, for clarity, we write

- e_G for identity
- 0_G for order of group G under '$+$'

Examples of Groups

Examples:

1) $(\mathbb{R}^*, \times)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}^+, \times)$, $(\mathbb{R}^+, \times)$, $(\mathbb{C}, \times)$ are all commutative infinite groups
2) $(\mathbb{Z}, *)$ not a group, no inverses except $1, -1 \in \mathbb{Z}^*$
3) $T = \{1, -1\}$, $(T, \times)$ is a commutative group

$\times$	1	-1
1	1	-1
-1	-1	1

order$(T) = 2$

4) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all infinite abelian groups

identity: 0

inverse of a: $-a$

Convention:

- $\mathbb{Q}^+$, $\mathbb{R}^+$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ - always groups under $\times$
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ - always groups under $+$

General Linear Group

Definition General Linear Group

Let $GL(n,\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$

Proposition

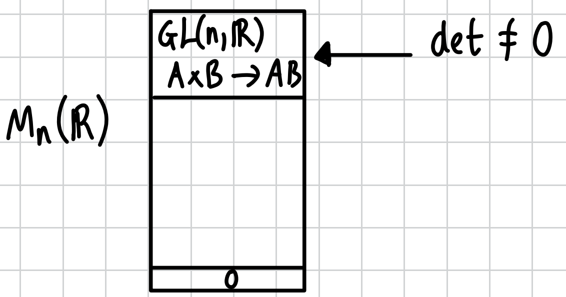
$(GL(n,\mathbb{R}), \times)$ is a group: general linear group of size n over $\mathbb{R}$

Proof:

Let $A, B \in GL(n,\mathbb{R})$. Then

$\det(AB) = \det A \det B \neq 0$ as $\det A \neq 0$, $\det B \neq 0$ closure

multiplicative property of determinant



so $AB \in GL(n,\mathbb{R}) \implies \times$ is a binary operation

- Matrix multiplication is associative
- $\det I_n = 1 \neq 0 \implies I_n \in GL(n,\mathbb{R})$ and

$$I_n A = A = A I_n \qquad \forall A \in GL(n,\mathbb{R})$$

(identity)

- $\forall A \in GL(n,\mathbb{R})$, $\det A^{-1} = \dfrac{1}{\det A} \neq 0 \implies A^{-1} \in GL(n,\mathbb{R})$ and

$$AA^{-1} = I_n = A^{-1}A \quad \text{and} \quad A^{-1} \in GL(n,\mathbb{R})$$

so A^{-1} is the inverse of A in $GL(n,\mathbb{R})$

So $GL(n,\mathbb{R})$ is a group ∎

Note $GL(n,\mathbb{R})$ is not commutative

The same holds for $(GL(n,\mathbb{F}), \times)$ is a group where $\mathbb{F}$ is a field

Corollary

As $GL(n,\mathbb{R})$ is a group, inverse of a matrix is unique
Also if $AB \in GL(n,\mathbb{R})$,
$$(A,B)^{-1} = B^{-1}A^{-1}$$

Similarly for any field f, we denote the set of nxn matrices over $\mathbb{F}$ by $M_n(\mathbb{F})$
Put $GL(n,\mathbb{F}) = \{A \in M_n(\mathbb{F}) : \det A \neq 0\}$

$(GL(n,\mathbb{F}), \times)$ is a group with identity I_n and inverse of A being the same as matrix inverse

$\boxed{(GL(n,\mathbb{F})) \text{ is a general linear group}}$

Klein-4 group

Lemma Klein-4 group

Let $K = \{e, a, b, c\}$ and let '$\cdot$' be given by

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Then, $(K, \cdot)$ is a group and is called **Klein-4 group**

Proof: Checking associativity

Consider expressions $(xy)z = x(yz)$. We need to show that for any values of x, y, z from K, we have
$$(xy)z = x(yz)$$

1) If atleast one of x, y, z is e, result is true
2) If $x, y, z \in \{a, b, c\}$ and are distinct, then $(xy)z = zz = e$ and $x(yz) = xx = e$
3) If $x, y, z \in \{a, b, c\}$ and $x = y \neq z$, then $(xy)z = ez = z$
$x(yz) = xt = z$ where $t = yz \neq x$
4) If $x, y, z \in \{a, b, c\}$ and $x = y = z$, then $(xy)z = ez = z$ and $x(yz) = xe = x = z$

The other cases follow similarly using commutativity ∎

Definition Self inverse

If $x^{-1} = x$ for $x \in G$, then x is self inverse

Note: $e^{-1} = e$ as $ee = e \implies e$ always self inverse

In K, every element is self inverse, K is commutative

The groups $(\mathbb{Z}_n, \oplus)$ and $(\mathbb{Z}_p^*, \otimes)$, p prime

Congruence of Integers

This is a relation $\mathbb{Z}$

Definition Congruence modulo n

Let $n \in \mathbb{N}$ and define relation '$\equiv$' such that

$$a \equiv b \pmod{n} \iff a - b = kn \quad \text{for some } k \in \mathbb{Z}$$

The following are equivalent

1) $a \equiv b \pmod{n}$
2) $n \mid (a-b)$
3) $a = b + kn$
4) a and b leave the same remainder when divided by n
5) $a \bmod n = b \bmod n$

Theorem

For any $n \in \mathbb{N}$, we have $\equiv (\bmod\, n)$ congruence modulo n is an equivalence relation on $\mathbb{Z}$

Proof:

Reflexivity: $\forall a \in \mathbb{Z}$, $a - a = 0$ and $n \mid 0 \implies n \mid a - a$

$\implies a \equiv a \pmod{n}$

Symmetry: for any $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n} \implies a - b = kn$

$\implies b - a = (-k)n$

$\implies b \equiv a \pmod{n}$

Transitivity: for any $a,b,c \in \mathbb{Z}$

$$a \equiv b \pmod n \text{ and } b \equiv c \pmod n \implies a-b = kn \text{ and } b-c = \ell n \text{ for some } k,\ell \in \mathbb{Z}$$
$$\implies a-c = (k+\ell)n$$
$$\implies a \equiv c \pmod n$$

■

For $a \in \mathbb{Z}$, we write

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod n\}$$

i.e. equivalence class of A

By the division algorithm, for any $n \in \mathbb{N}$, $b, a \in \mathbb{Z}$,

$$b = kn + a, \quad 0 \leq a < n$$

Therefore there are n-distinct equivalence classes

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

Theorem

If '$\sim$' is an equivalence relation on set A, then $\forall a, b \in A$

$$a \sim b \iff [a] = [b]$$

Proof:

($\implies$): Suppose $a \sim b$ and $x \in [a]$

$$x \in [a] \implies x \sim a \text{ and } a \sim b$$
$$\implies x \sim b \qquad \text{Transitivity}$$
$$\implies x \in [b]$$
$$\implies [a] \subseteq [b]$$

Similarly $[b] \subseteq [a]$. Therefore by mutual containment

$$[a] = [b]$$

($\impliedby$): Suppose $[a] = [b]$

$$x \in [a] \text{ and } x \in [b] \implies x \sim a \text{ and } x \sim b \overset{\text{symmetry}}{\implies} a \sim x \text{ and } x \sim b \overset{\text{transitivity}}{\implies} a \sim b$$

■

Theorem

If '$\sim$' is an equivalence relation on set A, then

$$\Pi = \{[a] : a \in A\} \text{ partitions } A$$

Proof:

Since '$\sim$' is an equivalence relation, it is reflexive

So $\forall a \in A$, $a \sim a \implies a \in [a]$, hence $[a] \neq \emptyset$

Take any $x \in [x]$ (since $\sim$ reflexive) so x belongs to atleast one equivalence class

Suppose $x \in [a]$ and $x \in [b]$ ($[a] \cap [b] \neq \emptyset$)

$$\begin{aligned} &\implies x \sim a \text{ and } x \sim b \\ &\implies a \sim x \text{ and } x \sim b \\ &\implies a \sim b \\ &\implies [a] = [b] \end{aligned}$$

Therefore x belongs to a unique equivalence class since if $[a]$ and $[b]$ are distinct equivalence classes,

$$\begin{aligned} [a] \neq [b] &\implies [a] \cap [b] \neq \emptyset \\ &\implies \text{mutually disjoint} \end{aligned}$$

Further $[a] \subseteq A$ for any $a \in A \implies \bigcup_{a \in A} [a] \subseteq A$

By reflexivity, if $a \in A$, then $a \in [a]$ ($a \sim a$) $\implies A \subseteq \bigcup_{a \in A} [a]$

$$\left.\begin{aligned} &\bigcup_{a \in A} [a] \subseteq A \\ &A \subseteq \bigcup_{a \in A} [a] \end{aligned}\right\} \implies \bigcup_{a \in A} [a] = A$$

$\blacksquare$

Definition Integers modulo n

Set $\mathbb{Z}_n$ is integers modulo n defined by

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$$

By the above theorem, $\mathbb{Z}_n$ partition $\mathbb{Z}$

$$\boxed{\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]}$$

Operations on $\mathbb{Z}_n$

Define operations $\oplus$ and $\otimes$ as follows

$$\boxed{\begin{array}{l} \cdot\ \oplus :\ [a] \oplus [b] = [a+b] \\ \cdot\ \otimes :\ [a] \otimes [b] = [a \times b] \end{array}}$$

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

Lemma

$\oplus$ is a well defined associative, commutative binary operation on $\mathbb{Z}_n$

- $[0]$ is the identity for $\oplus$

Proof Showing $\oplus$ is well defined

We want to show that $[a] \oplus [b]$ is uniquely valued.

Suppose $[a] = [a']$ and $[b] = [b']$

$\Rightarrow$ $a \equiv a' \pmod n$ and $b \equiv b' \pmod n$

$\Rightarrow$ $n \mid (a - a')$ and $n \mid (b - b')$

$\Rightarrow$ $n \mid ((a-a') + (b-b'))$ (distributivity)

$\Rightarrow$ $n \mid (a+b) - (a'+b')$ $\Rightarrow$ $a+b \equiv a' + b' \pmod n$

$\Rightarrow$ $[a+b] = [a'+b']$

$\Rightarrow$ $([a] \oplus [b]) = [a'] \oplus [b']$

Showing $\oplus$ is associative: $\forall\, [a], [b], [c] \in \mathbb{Z}_n$

$$\begin{aligned} ([a] \oplus [b]) \oplus [c] &= [a+b] \oplus [c] \\ &= [(a+b)+c] \\ &= [a+(b+c)] \\ &= [a] \oplus [b+c] \\ &= [a] \oplus ([b] \oplus [c]) \end{aligned}$$

Showing $\oplus$ is commutative: $\forall\, [a], [b] \in \mathbb{Z}_n$,

$$[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]$$

Showing $[0]$ is the identity: $\forall\, [a] \in \mathbb{Z}_n$, $[a] \oplus [0] = [a+0] = [a] = [0+a] = [0] \oplus [a]$ ■

Lemma

$\otimes$ is a well defined associative, commutative binary operation on $\mathbb{Z}_n$

· $[1]$ is the identity for $\otimes$

Proof Showing $\otimes$ is well defined

We want to show that $[a] \otimes [b]$ is uniquely valued.

Suppose $[a] = [a']$ and $[b] = [b']$

$\Rightarrow$ $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$

$\Rightarrow$ $a - a' = kn$ and $b - b' = nl$ for some $k, l \in \mathbb{Z}$

$\Rightarrow$ $a = kn + a'$ and $b = nl + b'$

$\Rightarrow$ $ab = (kn + a')(nl + b') \Rightarrow ab = a'b' + (a'l + b'k + kln)n$

$\Rightarrow ab \equiv a'b \pmod{n}$

$\Rightarrow [ab] = [a'b']$

$\Rightarrow [a] \otimes [b] = [a'] \otimes [b']$

Showing $\otimes$ is associative: $\forall [a], [b], [c] \in \mathbb{Z}_n$

$$\begin{aligned}([a] \otimes [b]) \otimes [c] &= [a \cdot b] \otimes [c] \\ &= [(a \cdot b) \cdot c] \\ &= [a \cdot (b \cdot c)] \\ &= [a] \otimes [b \cdot c] \\ &= [a] \otimes ([b] \otimes [c])\end{aligned}$$

Showing $\otimes$ is commutative: $\forall [a], [b] \in \mathbb{Z}_n$,

$$[a] \otimes [b] = [a \cdot b] = [b \cdot a] = [b] \otimes [a]$$

Showing $[1]$ is the identity: $\forall [a] \in \mathbb{Z}_n$, $[a] \otimes [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \otimes [a]$ ■

Theorem

$(\mathbb{Z}_n, \oplus)$ is a commutative group of order n

Proof: From previous lemma, $\oplus$ is a binary operation, commutative, associative with identity $[0]$

$$\forall [a] \in \mathbb{Z}_n, \ [a] \oplus [0] = [a+0] = [a] = [0+a] = [0] \oplus [a]$$

We just need to show the existence of inverses

$$\forall [a] \in \mathbb{Z}_n, \ \exists [-a] \in \mathbb{Z}_n \text{ and } [a] \oplus [-a] = [a-a] = [0]$$
$$= [-a] \oplus [a]$$

Hence $(\mathbb{Z}_n, \oplus)$ is a commutative group, with identity $[0]$ and inverse $[-a]$

■

Convention

i) $\mathbb{Z}_n$ always means $\mathbb{Z}_n$ under $\oplus$

ii) We may drop $\circ$ from $\oplus$ and $[\ ]$ from $[a]$ where the context is clear.

eg: in $\mathbb{Z}_4$

$$7 = 3, \quad -15 = 1, \quad 7 + (-15) = -8 = 0 = 3+1 = 4$$

Table for $(\mathbb{Z}_2, \oplus)$

+	0	1
0	0	1
1	1	0

This is the "same as" $(T, \times)$ where $T = \{1, -1\}$

Note: We write $[a][b]$ for $[a] \otimes [b]$

Dropping the $[\ ]$, we have

$(\mathbb{Z}_3, \otimes)$

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

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

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

Neither of these the table of a group as $[0]$ is not invertible, and it disobeys latin square property (0 appears more than once)

Notation: In $\mathbb{Z}_n$, sometimes we write

$$[a] = \bar{a} \quad \text{and} \quad \mathbb{Z}_n = \{\bar{0}, \dots, \overline{n-1}\}$$

Definition

For $n \in \mathbb{N}$,

$$\mathbb{Z}_n^* = \{[1], [2], \dots, [n-1]\} = \mathbb{Z}_n \setminus \{0\}$$

Note: $[x] \in \mathbb{Z}_n^* \iff [x] \neq [0] \iff n \nmid x$

Theorem

Let p be prime. Then $(\mathbb{Z}_p^*, \otimes)$ is a commutative group, order $p-1$

Proof Lemma above: $\otimes$ well-defined on $\mathbb{Z}_p$.

$\otimes$ is associative, commutative; identity $[1]$, $[1] \in \mathbb{Z}_p^*$

Closure: Need to show $\mathbb{Z}_p^*$ is closed under $\otimes$

Let $[a], [b] \in \mathbb{Z}_p^* \implies p \nmid a$ and $p \nmid b$

contrapositive $\implies p \nmid ab$

$\implies ab \not\equiv 0 \pmod{p}$

$\implies [ab] \neq [0]$

$\implies [a] \otimes [b] = [ab] \in \mathbb{Z}_p^*$

Note: p prime

$p \mid ab \implies p \mid a$ or $p \mid b$

Hence $\times$ is a binary operation on $\mathbb{Z}_p^*$

Inverses: Need to show existence of inverses. $[a][a^{-1}] = [1]$

Since $p \nmid a$, we have $\gcd(a,p) = 1$ * ($p \nmid a$ and prime $\implies \gcd(a,p) = 1$)

So $\exists\, s, t \in \mathbb{Z}$ s.t $1 = sa + tp$. Hence

$[1] = [sa + tp] \implies sa + tp \equiv 1 \pmod{p}$

$\implies sa + tp - 1 = pk$ for some $k \in \mathbb{Z}$

$\implies sa - 1 = p(k - t)$

$\implies sa \equiv 1 \pmod{p}$

$\implies [sa] = 1 \implies [a][s] = 1$

So we have

$$[1] = [sa + tp] = [sa] = [s][a] \quad (\text{and also } [s] \in \mathbb{Z}_p^*)$$

Hence inverse exists

* Note: p prime

Only integers that divide p is 1 and p

■

Table for $(\mathbb{Z}_7^*, \otimes)$

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Note: $(\mathbb{Z}_n^*, \otimes)$ is NOT a group if n composite

$\mathbb{Z}_n^* = \{[1], \ldots\ldots, [n-1]\}$

For n composite, $\exists [a] \in \mathbb{Z}_n^*$ such that $a \mid n$

$$a \mid n \implies n = al \quad \text{for some } l \in \mathbb{Z}$$

$$\implies [n] = [a][l]$$

$$\implies [0] = [a][l]$$

Further $0 < l < n \implies [l] \in \mathbb{Z}_n^*$

Hence not closed under $\otimes$ $\implies$ NOT a group

2. Orders of Elements, Subgroups and Cyclic Subgroups

General Associative Law

The general associative law: leave out brackets

For group $(G,*)$, by associative law

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

But for 4 elements;

$$a*b*c*d$$

many ways to bracket. For example

$$(a*b)*(c*d)$$

$$a*(b*(c*d))$$

etc.

Lemma General Associative Law

For any group G and any $a_1,\dots,a_n \in G$, the product

$$a_1 * a_2 * \cdots * a_n$$

is unambiguous

<u>Proof</u>: We show that no matter how

Powers in groups

For $g \in G$, we write

$$g^2 = gg$$

and

$$g^3 = ggg$$

So for example, $(ab)^2 = (ab)(ab)$

Note: If $ab = ba$, i.e. a and b commute then, in this case

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

However

$$\boxed{\text{In general } (ab)^2 \neq a^2b^2}$$

Definition

For $n \in \mathbb{N}$ and $g \in G$

$$g^n = (\underbrace{g \cdots\cdots g}_{n \text{ factors}})$$

By convention

$$\boxed{\begin{aligned} &g^0 = e \\ &g^{-n} = (g^{-1} \cdots\cdots g^{-1}) = (g^{-1})^n \end{aligned}}$$

Proposition Index Laws

Let G be a group. For any $g \in G$ and $z_1, z_2 \in \mathbb{Z}$, we have

1) $g^{z_1} g^{z_2} = g^{z_1 + z_2}$
2) $(g^{z_1})^{z_2} = g^{z_1 z_2}$

Note: We deduce

$$g^{z_1} g^{z_2} = g^{z_1 + z_2} = g^{z_2} g^{z_1}$$

so that powers of g commute with each other.

Notation:

	Multiplicative	Additive
$x * y$	xy	$x+y$
identity	e or 1 or e_G or 1_G	0 or 0_G
inverse	x^{-1}	$-x$
power	x^z	zx
index laws	$(g^{z_1})^{z_1} = g^{z_1 z_2}$	$z_1(z_2 g) = (z z_1) g$
	$g^{z_1} g^{z_2} = g^{z_1+z_2}$	$z_1 g + z_2 g = (z_1+z_2) g$

Orders of elements

Let G be a group. For $a \in G$, $n \in \mathbb{N}$, we have

$$a^0 = e, \quad a^n = a \cdots\cdots a \quad \text{(n terms)}$$

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

Also $ee = e \Longrightarrow e^{-1} = e$, we have

$$e^0 = e \quad ; \quad e^n = \underbrace{e \cdots\cdots e}_{n \text{ terms}} = e$$

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

i.e. $\boxed{e^z = e \quad \forall z \in \mathbb{Z}}$

Consider the list $a \in G$

$$a \; (= a^1), a^2, a^3, \ldots$$

So either atleast one $a^i = e$ or no $a^i = e$

Definition order of element $a \in G$

Let G be a group. For any $a \in G$

The **order** of a written, $o(a)$ is the **least** $n \in \mathbb{N}$ such that

$$a^n = e \quad \text{if such } n \in \mathbb{N} \text{ exists}$$

If no such n exists, then $o(a) = \infty$

Caution! $o(a)$ does **NOT** have the same meaning as the order of G

For any $a \in G$, we have

$$o(a)=1 \iff a^1 = e \iff a=e$$

So

$$\boxed{e \text{ is the ONLY element of order } 1}$$

For any $a \in G$, we have

$$o(a)=2 \iff a=a^1 \neq e \text{ and } a^2=e$$

$$\iff a \neq e \text{ and } a^{-1}=a$$

$$\boxed{o(a)=1 \text{ or } 2 \iff a \text{ is self-inverse}}$$

Examples:

1) $(\mathbb{R}^*, \times)$

- 1 has order 1 (identity)
- -1 has order 2 ; $x^2=1 \Rightarrow x=-1$
- For $x \in \mathbb{R}^* \setminus \{-1,1\}$, $x^n \neq 1 \ \forall n \in \mathbb{N} \Rightarrow o(x)=\infty$

2) $(\mathbb{C}^*, \times)$

- i has order 4 since

$$i^1=i,\ i^2=-1\neq 1,\ i^3=-i \neq 1,\ i^4=1$$

- Infact $\mathbb{C}^*$ contains elements of every order.

To see this, consider $z \in \mathbb{C}^*$

$$z=re^{i\theta}$$

Want to find smallest integer such that $z^n=1$

$$z^n=r^n e^{in\theta}=1 \Rightarrow r^n=1 \text{ and } e^{in\theta}=1 \Rightarrow n\theta=2k\pi \quad (e^{i2\pi k}=1)$$

$$r=1 \Rightarrow r^n=1 \ \forall n \in \mathbb{N} \text{ and then } n\theta=2k\pi \Rightarrow \theta=\frac{2k\pi}{n}$$

$\Rightarrow \theta$ can take any value

$r \neq 1 \Rightarrow n=0$

3) $(\mathbb{R},+)$

- $o(0)=1$ (identity)
- $x \neq 0$, $o(x)=\infty$ as $x+\cdots+x$ (n times) $\neq 0 \quad \forall n \in \mathbb{N}$

4) $(GL(2,\mathbb{R}), \times)$

- The matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ has order 2

Theorem

Let G be a finite group and let $a \in G$. Then

$$o(a) \text{ is finite}$$

proof: (counting argument):

The list

$$a, a^2, a^3, \dots \text{ is an infinite sequence of a finite set}$$

sequence must contain repeats, say

$$a^i = a^j \text{ where } i \neq j \Rightarrow a^{-i}a^i = a^{-i}a^j$$
$$\Rightarrow a^0 = a^{j-i}$$
$$\Rightarrow e = a^{j-i} \text{ and } j-i \in \mathbb{N}$$

as $j-i \in \mathbb{N}$, we have $o(a)$ is finite and $o(a) \leq j-i < \infty$ ■

Examples:

If $o(a)=4$, then $aa^3 = a^4 = e = a^2a^2$

So
- a, a^3 are mutually inverse
- a^2 is self inverse

$$a^5 = aa^4 = ae,$$
$$a^6 = a^2a^4 = a^2e = a^2$$
$$a^7 = aa^6 = aa^2 = a^3$$
$$a^8 = (a^4)^2 = e^2 = e$$

Also in the direction

$$a^{-1} = a^3, \quad a^{-2} = a^2, \quad a^{-4} = (a^4)^{-1} = e^{-1} = e$$

... so rewrite the first line to the second

$$a^{-5}, a^{-4}, a^{-3}, a^{-2}, a^{-1}, \overset{a^0}{e}, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, \ldots$$
$$a^3, e, a, a^2, a^3, e, a, a^2, a^3, e, a, a^2, a^3, e, a \ldots$$

For example, $\quad a^7 = a^4 a^3 = e a^3 = a^3$

Lemma Remainder Lemma

Let $a \in G$ with $o(a) = n < \infty$. Let $z, z' \in \mathbb{Z}$ with $z = nq + r$ where $q, r \in \mathbb{Z}$, $0 \leq r < n$

Then,

(1) $a^z = a^r$

(2) $0 \leq s < t < n \implies a^s \neq a^t$

(3) $a^z = e \iff n \mid z \iff z \equiv 0 \pmod n$

(4) $a^z = a^{z'} \iff z \equiv z' \pmod n$

Proof:

(1) We have
$$\begin{aligned} a^z = a^{nq} a^r &= (a^n)^q a^r \\ &= e^q a^r \\ &= a^r \qquad \text{using index laws} \end{aligned}$$

(2) if $0 \leq s < t < n$ notice that $0 < t - s < n$ so if

$$a^s = a^t \implies a^{t-s} = e \implies o(a) = t - s < n \quad \# \text{ contradiction as } o(a) = n$$

So $a^s \neq a^t$

(3) $a^z = e \iff a^r = e$

if $0 < r < n$, $\implies$ contradicts $o(a) = n$. Therefore

$$r = 0 \implies n \mid z \qquad (\text{remember } 0 \leq r \leq n)$$

since $a^i \neq e$ for any i with $0 < i < n$ and $0 \leq r < n$

(4) $a^z = a^{z'} \iff a^{z-z'} = e \iff n \mid (z-z') \iff z = z' \equiv (\text{mod } n)$

using (3) ■

Consequently if $o(a) = n < \infty$, then

$$e, a, a^2, \dots, a^{n-1}$$

is a complete list of the distinct powers of a

Example

1) Let $o(a) = 3$. Then the remainders are 0, 1, 2 and

$$\{a^z, z \in \mathbb{Z}\} = \{a^0, a^1, a^2\} = \{e, a, a^2\} \text{ and } |\{e, a, a^2\}| = 3$$

Also

$$a^{22} = a^{7 \cdot 3 + 1} = a \quad (a^1)$$

Subgroups

Definition Subgroups

Let G be a group. Let $H \subseteq G$.

Then, H is a subgroup of G denoted $H \leq G$ if

(i) $a, b \in H \Rightarrow ab \in H$ closure

(ii) $a \in H \Rightarrow a^{-1} \in H$ closure under inverse

(iii) $e \in H$ contains identity $\Rightarrow H \neq \emptyset$

Note: $H \leq G \iff$ H is a group under the restriction of the binary operation in G to H

The converse is also true, that is

$$\boxed{\forall\, H \subseteq G,\ H \leq G \iff (H, \circ) \text{ is a group, '}\circ\text{' is the restriction of binary operation of } G \text{ to } H \times H}$$

proof: H is a group under same binary operation $\Longrightarrow$ H is closed under this operation.

Since H is a group, it contains an identity say $f \in H \Longrightarrow f^2 = f \in G$ and $e^2 = e$ in G

$\Longrightarrow e = f$ and $e \in H$

Let $a \in H$. Inverse of 'a' in H is an element b such that

$$ab = f = ba \qquad (*)$$

But by above $e = f \Rightarrow a^{-1} \in G$ is unique satisfying (*). Hence $b = a^{-1} \in H$. ■

Examples:

1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

2) $\mathbb{Q}^* \leq \mathbb{R}^*$ BUT $(\mathbb{R}^*, \times)$ is NOT a subgroup of $(\mathbb{R}, +)$

3) For $n \in \mathbb{N}$, $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ (eg $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$)

Then $n\mathbb{Z} \leq \mathbb{Z}$

4) $SL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$ Then $SL(n,\mathbb{R}) \leq GL(n,\mathbb{R})$

proof:

As $\det A = 1 \neq 0 \quad \forall A \in SL(n,\mathbb{R}) \Rightarrow A \in GL(n,\mathbb{R})$

$\Rightarrow SL(n,\mathbb{R}) \subseteq GL(n,\mathbb{R})$

(iii) $\det I_n = 1 \Rightarrow I_n = e \in SL(n,\mathbb{R})$

i) Let $A, B \in SL(n,\mathbb{R})$

$$\det(AB) = \det A \det B = 1\,1 = 1 \Longrightarrow AB \in SL(n,\mathbb{R})$$

ii) $\det A^{-1} = \dfrac{1}{\det A} = \dfrac{1}{1} = 1 \Rightarrow A^{-1} \in SL(n,\mathbb{R})$

Hence $SL(n,\mathbb{R}) \leq GL(n,\mathbb{R})$

5) For any group G, $\{e\} \leq G$, $G \leq G$

Definition Special Linear Group

$$SL(n,\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$$

Cyclic Subgroups

Definition

Let G be a group, $a \in G$. We define

$$\langle a \rangle = \{a^z : z \in \mathbb{Z}\}$$

In '+' notation

$$\boxed{\langle a \rangle = \{za : z \in \mathbb{Z}\}}$$

If $o(a)=\infty$ then $a^i = a^j \implies i=j$

If $o(a)=\infty$ then if $i<j$ and $a^i = a^j \implies a^{j-i}=e$ contradiction ※

So $\dots a^{-2}, a^{-1}, e, a, a^2 \dots$ are all distinct $\implies |\langle a\rangle| = \infty$

Since $a^i = a^j \implies a^{j-i} = e$, so if $j-i \neq 0$, we would say $o(a) \leq |j-i|$

Hence if $\boxed{o(a)=\infty, \ |\langle a\rangle| = \infty}$

If $o(a)=n\in\mathbb{N}$, then from remainder lemma, $\langle a\rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $e, a, a^2, \dots, a^{n-1}$ are distinct

$$\boxed{\text{if } o(a)=n, \ |\langle a\rangle| = n \ \text{ and } \langle a\rangle = \{e, a^1, \dots, a^{n-1}\}}$$

Lemma

For any $a\in G$, we have $\langle a\rangle$ is a commutative subgroup of G and

$$|\langle a\rangle| = o(a)$$

Proof

We have shown $|\langle a\rangle| = o(a)$

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

if $a^h, a^k \in \langle a\rangle$, then $a^h a^k = a^{h+k} \in \langle a\rangle$

$(a^h)^{-1} = a^{-h} \in \langle a\rangle$, hence $\langle a\rangle \leq G$

$a^h a^k = a^{h+k} = a^k a^h$ hence $\langle a\rangle$ is commutative

■

Remark:

If $o(a)=n$, then $a^{-1} = a^{n-1}$

$a^{-2} = a^{n-2}$ etc

If n is even $o(a^{n/2})^{-1} = a^{n/2}$

Definition Cyclic Subgroup

i) $\langle a\rangle$ is the cyclic subgroup generated by a

(ii) a group is cyclic if $G=\langle a\rangle$ for some $a\in G$. Then we say a generates G

Proposition

Let G be a group with $|G| = n < \infty$ finite

Then G is cyclic $\iff \exists\, a \in G$ with $o(a) = n$

Proof:

For any $a \in G$, $\langle a \rangle \leq G$

$$G = \langle a \rangle \iff |\langle a \rangle| = |G|$$

$$\iff |G| = o(a)$$

$$\iff o(a) = n \qquad \blacksquare$$

Examples

i) $\mathbb{Z}$ is cyclic as $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

ii) $\mathbb{Q}$ is not cyclic as if $\mathbb{Q} = \langle a \rangle$ then $a \neq 0$ and $\mathbb{Q} = \{\cdots, -2a, a, 0, a, 2a, \cdots\}$

But $\frac{a}{2} \in \mathbb{Q}$ but $\frac{a}{2} \notin \langle a \rangle$

iii) In $\mathbb{Z}_n$, $o([1]) = n$ as

$$[1] \oplus [1] \oplus \cdots \oplus [1] = [n] = [n]$$

So $\mathbb{Z}_n$ is cyclic and $\mathbb{Z}_n = \langle [1] \rangle$

iv) In K, we have $K = \{e, a, b, c\}$ and $o(e) = 1$, $o(a) = o(b) = o(c) = 2$

Hence K not cyclic

$$\langle e \rangle = \{e\},\ \langle a \rangle = \{e, a\},\ \langle b \rangle = \{e, b\},\ \langle c \rangle = \{e, c\}$$

Theorem

(1) Let $G = \langle a \rangle$ be cyclic of order $n = uv$. Then G has a subgroup of order v

(2) Any subgroup of a cyclic group is cyclic

Proof:

(1) $o(a) = n = uv \Rightarrow o(a^u) = v$ (Exercises)

$\Rightarrow a^u$ generates cyclic subgroups of order v

$\Rightarrow \langle a^u \rangle = \{e, a^u, a^{2u}, \cdots, a^{(v-1)u}\} \leq G$ with $|\langle a^u \rangle| = v$

(2) Let $H \leq G$ where $G = \langle a \rangle$ is cyclic

Suppose $H = \{e\}$, then $H = \langle e \rangle \implies H$ is cyclic

Assume $H \neq \{e\}$. So $\exists\, a^i \in H$ where $i \neq 0$. Then $a^{-i} = (a^i)^{-1} \in H$ H a subgroup

So we have $a^i, a^{-i} \in H$, so we can find a least $n \in \mathbb{N}$ with $a^n \in H$ (well ordering principle)

Let $a^j \in H$. By division algorithm, $\exists\, q, r \in \mathbb{Z}$

$$j = nq + r, \quad 0 \leq r < n$$

Now $a^r = a^{j-nq} = a^j (a^n)^{-q} \in H$ as $a^j \in H$ and $a^n \in H$ closure

Since n is least, $r = 0$ else we contradict the minimality of n

$$r = 0 \implies j = nq$$
$$\implies n \mid j$$

We now have $\langle a^n \rangle \leq H \subseteq \langle a^n \rangle \quad \therefore H = \langle a^n \rangle$ and so cyclic

■

Examples:

1) In $\mathbb{Q}^*$, we have $\langle 2 \rangle = \{2^z, z \in \mathbb{Z}\} = \{\dots, 1/4, 1/2, 1, 2, 4, \dots\}$

2) In $\mathbb{Z}$, we have $\langle 2 \rangle = \{2z : z \in \mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$

2) In $\mathbb{Z}_6$ $\langle 2 \rangle = \{[0], [2], [4]\}$, $|\mathbb{Z}_6| < \infty$, $o(2) < \infty$

3) In $(\mathbb{Z}_7^*, \otimes)$, the element $[3]$ has order 6 as dropping '[ ]'

$$3 \neq 1, \quad 3^2 = 2 \neq 1, \quad 3^3 = 6 \neq 1, \quad 3^4 = 4 \neq 1, \quad 3^5 = 5 \neq 1, \quad 3^6 = 15 = 1$$

So $\mathbb{Z}_7^*$ has subgroups of order 1, 2, 3, 6 by Theorem, pg 30.

$\{1\} = \langle 3^6 \rangle$ has order 1

$\mathbb{Z}_7^* = \langle 3^1 \rangle$ has order 6

$\langle 3^2 \rangle = \{2, 4, 1\} = \langle 2 \rangle$ has order 3

$\langle 3^3 \rangle = \{6, 1\} = \langle 6 \rangle$ has order 2

3. Symmetric Groups

Symmetric Groups

Let X be a non-empty set $X \neq \emptyset$ (often $X = [n] = \{1, \dots, n\}, n \in \mathbb{N}$)

We write I_X for the identity map $I_X: X \to X$. If $X = [n]$, we write I_n for $I_{[n]}$

Definition Symmetry

Let X be a set. A bijection $\sigma: X \to X$ is called a symmetry

We denote by S_X the set of all bijections from X to X.

$$S_X = \{\sigma : \sigma \text{ a symmetry of } X\}$$

If $X = [n]$, we write S_n for $S_{[n]}$

Notation: The binary operation represented by '$\circ$' is composition of a function

Proposition Symmetric Group

The pair $(S_X, \circ)$ is a group, the symmetric group on X

Proof:

Let $\alpha, \beta \in S_X$. Then

$$\alpha: X \to X \quad \text{and} \quad \beta: X \to X$$

are bijections. Certainly

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

Also as α and β are bijections, so is $\alpha \circ \beta \Longrightarrow \alpha \circ \beta \in X$

Therefore $\circ$ is a binary operation on S_X

Associativity: Composition of functions is associative

Identity: $I_X \in S_X$ and for any $\alpha \in S_X$, we have

$$\alpha \circ I_X = \alpha = I_X \circ \alpha$$

Inverse: Finally, if $\alpha \in S_X$, then the inverse function $\alpha^{-1}: X \to X$ exists and is a bijection

$$\alpha^{-1} \in S_X \quad \text{and} \quad \alpha \circ \alpha^{-1} = I_X = \alpha^{-1} \circ \alpha$$

So $(S_X, \circ)$ is a group ∎

Remark:

$f, g : A \to B$, $f = g$ means $f(a) = g(a)$ $\forall a \in A$

Note: We often drop mention of '$\circ$'

Example

1) $n=1$; $S_1 = \{I_1\}$, the table is

$\circ$	I_1
I_1	I_1

(2) $n=2$

$$S_2 = \{I_2, \alpha\} \text{ where } \alpha : X_2 \to X_2 ; \alpha(1) = 2, \ \alpha(2) = 1$$

The table is

$\circ$	I_2	α
I_2	I_2	α
α	α	$\alpha \circ \alpha = I_2$

i) $\alpha^2(1) = \alpha(\alpha(1)) = \alpha(2) = 1$

ii) $\alpha^2(2) = \alpha(\alpha(2)) = \alpha(1) = 2$

(3) $n=3$, we have $I_3 \in S$, $\rho \in S$ where

$$\rho(1) = 2, \quad \rho(2) = 3, \quad \rho(3) = 1$$

Two row notation

We can write $\alpha \in S_n$ as

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots\cdots & n \\ \alpha(1) & \alpha(2) & \cdots\cdots & \alpha(n) \end{pmatrix}$$

For example in (3) above

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

Example Let $\beta \in S_4$ given by

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

This means that $\beta(1) = 2$, $\beta(2) = 3$, $\beta(3) = 4$, $\beta(4) = 1$

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

$(\beta\gamma)(1) = \beta(\gamma(1)) = \beta(2) = 3 \qquad \beta(\gamma(3)) = \beta(\gamma(3)) = \beta(4) = 2$

$(\beta\gamma)(2) = \beta(\gamma(2)) = \beta(1) = 2 \qquad \beta(\gamma(4)) = \beta(\gamma(4)) = \beta(3) = 4$

So $\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

Working out $\gamma\beta$, we have

$$\gamma\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \neq \beta\gamma$$

Remark:

If $\sigma, \tau \in S_n$, the composition is abbreviated to $\sigma\tau$ referred to as the product of σ & τ

Caution! Permutation product is applied right to left

$\sigma\tau$: Apply τ first then σ

Remark:

In two-row notation, for $\alpha \in S_n$, each element of $[n] = \{1, \cdots, n\}$ occurs exactly once on the second row

If $\alpha = \begin{pmatrix} 1 & 2 & \cdots & x & \cdots & y & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(x) & \cdots & \alpha(y) & \cdots & \alpha(n) \end{pmatrix}$

Then if $\alpha(x) = \alpha(y)$, we have $x = y$ (α is one to one)

As α is onto, any $z \in \{1, \cdots, n\}$ appears on the second row, we have

$z = \alpha(t)$ for some t, so

$$\alpha = \begin{pmatrix} 1 & \cdots & t & \cdots & n \\ \alpha(1) & \cdots & z & \cdots & \alpha(n) \end{pmatrix}$$

Note

Thus the second row is a permutation/rearrangement of the first.

As there are $n!$ permutations of n elements

$$\boxed{|S_n| = n!}$$

- $|S_1| = 1! = 1$ • $|S_2| = 2! = 4$ • $|S_3| = 3! = 6$

The 6 elements of S_3 are

$$I_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad e = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad e^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad e^3 = I_3$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Multiplication table

$\circ$	I_3	e	e^2	σ_1	σ_2	σ_3
I_3	I_3	e	e^2	σ_1	σ_2	σ_3
e	e	e_2	I_3	σ_3	σ_1	σ_2
e^2	e^2	I_3	e	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	I_3	e	e^2
σ_2	σ_2	σ_3	σ_1	e^2	I_3	e
σ_3	σ_3	σ_1	σ_2	e	e^2	I_3

As for example

$$e\sigma_1 \neq \sigma_1 e$$

S_3 is NOT commutative

Cycle Notation

Some elements in S_n can be written as cycles

For example $e \in S_3$, we write $e = (1\,2\,3)$, we mean

$$e(1) = 2, \quad e(2) = 3, \quad e(3) = 1$$

We would get same function by writing

$$(2\,3\,1), (3\,1\,2)$$

Definition Cycle

A cycle in S_n (of length $m \geq 2$)

$$\alpha = (a_1, \dots, a_m)$$

where $a_1, a_2, \dots, a_m \in \{1, \dots, n\}$ and $a_i \neq a_j$ for $i \neq j$

It is the bijection defined by

$$\alpha(a_1) = a_2 \quad \alpha(a_2) = a_3, \dots\dots, \alpha(a_{m-1}) = a_m, \quad \alpha(a_m) = a_1$$

and

$$\alpha(x) = x \qquad \forall x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_m\}$$ fixes other elements

$m \leq n$

We can write

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{m-1} \mapsto a_m \mapsto a_1$$

Cycles from left to right; they can have any starting point

Cycle decomposition

Not every permutation, however every permutation can be written as a product of of cycles

Example In S_3

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

This means $1 \mapsto 2 \mapsto 3 \mapsto 1$

In cycle notation $\rho = (1\,2\,3)$, Similarly $\rho^2 = (1\,3\,2)$

For $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$: $2 \mapsto 3 \mapsto 2$ $\quad 1 \mapsto 1$ (fixed)

$$\Longrightarrow \sigma_1 = (2, 3)$$

Similarly $\sigma_2 = (1\,3)$

$\sigma_3 = (1\,2)$

Example

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \in S_5$$

Here we have $1 \mapsto 2 \mapsto 1 \Longrightarrow (1\,2)$

$3 \mapsto 4 \mapsto 5 \mapsto 3 \Rightarrow (3\,4\,5)$

Therefore $\beta = (3\,4\,5)(1\,2)$ product is composition

Remark: In the example above product is composition

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

do next do first

operation done from right to left.

We could also have written $\beta = (1\,2)(3\,4\,5)$

Mixing notation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} = (1\,2) \in S_5$$

So we have $\sigma(1) = 2$, $\sigma(4) = 4$

You could write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}(1) = 2$

or $(1\,2)(4) = 4$

tend NOT to

Note:

1) In cycle notation, domain is understood
2) $(a_1\ a_2 \cdots a_m) = (a_2\ a_3 \cdots a_m\ a_1) = \cdots = (a_m\ a_1\ a_2 \cdots a_{m-1})$

So cycle notation is NOT unique

Examples:

1) In S_5 $\quad (3\,2\,4\,5)(1\,2\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} = (1\,4)(2\,5\,3)$ (not a cycle)

Products of cycles do not have to be cycles

Note: Compose cycles from right to left, they are functions; cycles 'cycle' from left to right

Inverse of a cycle

The inverse of the cycle

$$a_1 \mapsto a_2 \cdots \mapsto a_{m-1} \mapsto a_m \mapsto a_1$$

is the cycle

$$a_m \mapsto a_{m-1} \mapsto \cdots \mapsto a_2 \mapsto a_1 \mapsto a_m$$

Hence

$$\boxed{(a_1\,a_2 \cdots a_m)^{-1} = (a_m\,a_{m-1} \cdots a_1)}$$

Observe that

$$(a_1 \cdots a_n)(a_n\,a_{m-1} \cdots a_2\,a_1) = I_n$$

$$(a_n\,a_{m-1} \cdots a_2\,a_1)(a_1 \cdots a_n) = I_n$$

Lemma

Order of a cycle of length m is m

Proof:

Let $\alpha = (a_1 a_2 \cdots a_m) \in S_n$. Then

$$\alpha(a_1) = a_2$$
$$\alpha^2(a_1) = \alpha(\alpha(a_1)) = a_3$$
$$\alpha^{m-1}(a_1) = \alpha_m$$
$$\alpha^m(a_1) = \alpha(a_m) = a_1$$

Hence smallest k such that $\alpha^k(a_1) = a_1$ is m

Also the same argument gives $\alpha^m(a_i) = a_i \quad 1 \le i \le m$

Also $\alpha(x) = x \quad \forall x \notin \{a_1, \cdots, a_m\} \implies \alpha^m(x) = x \quad \forall x \notin \{a_1, \cdots, a_m\}$.

Hence $o(\alpha) = m$

■

Example: S_3: the 6 elements of S_3 are

$$I_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad e = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \qquad e^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3) \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3) \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$o(I_3) = 1 \quad o(e) = 3 \quad o(e_2) = 3 \quad o(\sigma_1) = o(\sigma_2) = o(\sigma_3) = 2$$

Note:

1) $|S_3| = 3! = 6$ and $1, 2, 3$ are proper divisors of 6

2) S_3 is NOT commutative as for example

$$e\sigma_1 = (1\,2\,3)(2\,3) = (1\,2) = \sigma_3 \neq \sigma_1 e = \sigma_2$$

3) Cycles NOT commutative in general

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

and also $(1\,2)(3\,5) = (3\,5)(1\,2)$

Definition Disjoint Cycles

2 cycles are **disjoint** if they have no elements in common

$(a_1 \cdots a_m)$ and $(b_1 \cdots b_k)$ are **disjoint** if

$$\{a_1 \cdots a_m\} \cap \{b_1, \cdots, b_k\} = \emptyset$$

Proposition

Disjoint cycles commute i.e. $\alpha, \beta \in S_n$ are disjoint cycles then

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

Notation: For disjoint cycles α, β

Write $\alpha = (a_1 \cdots a_r)$ $\beta = (b_1 \cdots b_m)$

where $\{a_1, \cdots, a_r\} \cap \{b_1, \cdots, b_m\} = \emptyset$

Proof:

Let $x \notin \{a_1, \cdots, a_r, b_1, \cdots, b_m\}$

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

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

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

Consider $a_i \in \{b_1, \cdots, b_m\}$ we have

$$\alpha\beta(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$$ $\beta(a_i) = a_i$ β fixes a_i's

also $$\beta\alpha(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$$ $r+1 \equiv 1$

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

Similarly $(\alpha\beta)(b_j) = \beta\alpha(b_j)$ $\forall b_j \notin \{a_1, \cdots, a_r\}$

Hence as $(\alpha\beta)(y) = (\beta\alpha)(y)$ $\forall y \in \{1, \cdots, n\}$, we have

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

$\blacksquare$

Proposition Cycle decomposition

Let $\alpha \in S_n$. Then

$$\alpha = \gamma_1 \gamma_2 \cdot \dots \cdot \gamma_K$$

where $\gamma_1, \dots, \gamma_K$ are disjoint cycles.

This expression is unique except for the order in which the cycles are written

We interpret the empty product as I_n

Proof: Let $\alpha \in S_n$

Consider list of numbers $1, \dots, n$

Choose the first i in the list such that $\alpha(i) = i$ (if no such i exists then $\alpha = I_n$ and I_n is the product of 0 cycles)

Consider the list

$$i = \alpha^0(i), \quad \alpha(i), \ \alpha^2(i), \ \alpha^3(i) \dots\dots$$

list must be finite as it is contained in $\{1, \dots, n\}$ and so must contain repeats

Suppose that $\alpha^u(i)$ is the first power to be repeated and $\alpha^u(i) = \alpha^{u+v}(i)$ where $v > 0$ is the first repeat

The inverse of α^u in the group S_n is a^{-u} so that

$$i = I_n(i) = \alpha^{-u}\alpha^u(i) = \alpha^{-u}\alpha^{u+v}(i) = \alpha^{(-u)+(u+v)}(i) = \alpha^v(i)$$

the conclusion is that α^0 is the first repeated power, that is $u=0$. Also $\alpha^v(i)$ is the first repeat of the list.

$$i, \alpha(i), \alpha^2(i), \dots, \alpha^{v-1}(i)$$

are all distinct. Put $K_1 = v-1$. Let γ_1 be the cycle

$$\gamma_1 = (i, \alpha(i), \alpha^2(i), \dots, \alpha^{K_1}(i))$$

Using the division algorithm, we can show that for any $z \in \mathbb{Z}$

$$\alpha^z(i) \in \{i, \alpha(i), \alpha^2(i), \dots, \alpha^{K_1}(i)\}$$

If $\alpha(j) = j \quad \forall j$ not in the list

$$i, \alpha(i), \alpha^2(i), \dots, \alpha^{K_1}(i)$$

we stop. Otherwise pick the smallest j not in the list and consider the elements

$$j, \alpha^2(j), \ \alpha^2(j), \dots \qquad \text{of} \quad \{1, \dots, n\}$$

We cannot have

$$\alpha^u(i) = \alpha^v(j)$$

for any $0 \leq u \leq v$ as this would give

$$j = \alpha^{v-u}(i)$$

contradicting the choice of j (not on list of i)

Arguing as above, we obtain a cycle γ_2

$$\gamma_2 = (j, \alpha(j), \dots, \alpha^{k_2}(j))$$

for some k_2; notice that is cycle is disjoint to γ_1

Continuing, we obtain disjoint cycles $\gamma_1, \dots, \gamma_r$ until all elements of $\{1, \dots, n\}$ is used up and by construction

$$\alpha = \gamma_1 \cdots \gamma_r$$

Showing uniqueness, if also

$$\alpha = \delta_1 \cdots \delta_s$$

for disjoint cycles $\delta_1, \dots, \delta_s$ then notice that for any $\ell \in \{1, 2, \dots, n\}$ we have that

$$\alpha(\ell) = \ell \iff \ell \notin \gamma_i \iff \ell \notin \delta_j$$

If ℓ appears in γ_h and δ_k, then without loss of generality, we can assume that

$$\gamma_h = (\ell, \dots) = (\ell, \alpha(\ell), \dots, \alpha^p(\ell))$$

where $\alpha^{p+1}(\ell) = \ell$. But since we can also assume δ_k begins with ℓ, we have that

$$\gamma_h = \delta_k$$

Since disjoint cycles commute, we can also assume $h = k = 1$ so that by cancellation

$$\gamma_2 \cdots \gamma_r = \delta_2 \cdots \delta_s$$

An inductive argument now yields that $r = s$ (after relabelling) $\gamma_i = \delta_i$ for $1 \leq i \leq r$

∎

Definition Cycle Decomposition

The decomposition

$$\alpha = \gamma_1 \cdots \gamma_k$$

as a product of disjoint cycles is called the *cycle decomposition* of α

Example:

Write in cycle decomposition

1) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 2 & 5 & 4 & 6 & 1 \end{pmatrix} \implies \alpha = (1327)(45)$

2) $(2417)(537) = (175324)$

3) $(537)^{-1}(2417)^{-1} = ((2417)(537)) = (175324)^{-1} = (423571)$

Recall: Since disjoint cycles commute, if

γ and δ are disjoint then, $\gamma\delta = \delta\gamma$

It follows that $\boxed{(\gamma\delta)^z = \gamma^z \delta^z \qquad \forall z \in \mathbb{Z}}$

(general proof in exercises)

Example: Let $\alpha = (123)(45) \in S_5$

Recall $o(123) = 3$, $o(45) = 2$

So $\alpha \neq I_5$

$$\alpha^2 = ((123)(45))^2 = (123)^2(45)^2 = (132) \neq I_5$$
$$\alpha^3 = ((123)(45))^3 = (123)^3(45)^3 = (45) \neq I_5$$
$$\alpha^4 = ((123)(45))^4 = (123)^4(45)^4 = (123) \neq I_5$$
$$\alpha^5 = ((123)(45))^5 = (123)^5(45)^5 \quad (132)(45) \neq I_5$$
$$\alpha^6 = ((123)(45))^6 = (123)^6(45)^6 = I_5$$

so $o(\alpha) = 6 = \operatorname{lcm}\{3,2\}$

Proposition

Let $\alpha \in S_n$, $\alpha \neq I_n$. Write

$$\alpha = \gamma_1 \gamma_2 \cdots \gamma_m$$

are disjoint. Suppose the length of γ_i is l_i for $1 \leq i \leq m$. Then

$$o(\alpha) = \operatorname{lcm}\{\ell_1, \dots, \ell_m\}$$

Proof: Suppose $\alpha \in S_n$

Let the cycle decomposition of α be

$$\alpha = \gamma_1 \gamma_2 \cdots \gamma_m$$

where length of γ_i is l_i.

We know the order of γ_i

$$o(\gamma_i) = l_i \quad \forall\, 1 \leq i \leq m$$

Since disjoint cycles commute,

$$\alpha^x = (\gamma_1 \cdots \gamma_m) = \gamma_1^x \cdots \gamma_m^x \quad \text{for any } x \in \mathbb{N}$$

If x is a multiple of l_i, then $\gamma_i^x = I_n$ so that if x is a common multiple of all γ_i

$$\alpha^x = \gamma_1^x \cdots \gamma_m^x = I_n \cdots I_n = I_n$$

Suppose that $y \in \mathbb{N}$, $\alpha^y = I_n$ and y is not a common multiple of $l_1, \dots, l_m$.

Since γ_i's commute with each other, we can assume that l_1 does not divide y

$$y = q l_1 + r \quad \text{where } 0 < r < l_1$$

We know that $\gamma_1^y = \gamma_1^r$. Let

$$\gamma_1 = (a_1 a_2 \cdots a_{l_1})$$

Since the γ_i are disjoint, a_1 does not appear in $\gamma_2, \dots, \gamma_m$. Thus

$$\gamma_j^y(a_1) = a_1 \quad \text{for } 2 \leq j \leq m$$

Now

$$\begin{aligned}
\alpha^y(a_1) &= (\gamma_1^y \gamma_2^y \cdots \gamma_m^y)(a_1) \\
&= \gamma_1^y(\gamma_2^y(\cdots(\gamma_m^y(a_1))\cdots)) \\
&= \gamma_1^y \gamma_2^y(\cdots(\gamma_{m-1}^y(a_1))\cdots)) \\
&= \cdots \gamma_1^y(a_1) = \gamma_1^r(a_1) = a_{1+r} \neq a_1
\end{aligned}$$

Thus $a^y \neq I_n$ ※ contradiction

Thus $\alpha^x = I_n \iff x$ is a multiple of $l_i \quad 1 \leq i \leq n$

Hence order is the least x

$$o(a) = \operatorname{lcm}\{l_1, \dots, l_m\}$$

■

Example

(1) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 1 & 6 & 5 & 2 \end{pmatrix} \in S_7$

$\alpha = (1\,7\,2\,4)(5\,6)$

$o(\alpha) = \operatorname{lcm}\{4,2\} = 4$

(2) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 1 & 4 & 5 & 3 & 10 & 6 & 9 & 8 & 11 & 7 \end{pmatrix}$

$\beta = (2\,1)(3\,4\,5)(6\,10\,11\,7)(8\,9)$

$o(\beta) = \operatorname{lcm}(2,3,4,2) = 12$

Warning: Powers of cycles do **not** have to be cycles, e.g

$$(1\,2\,3\,4)^2 = (1\,3)(2\,4)$$

Transposition

Definition Transposition

A **transposition** is a cycle of length 2

If $\alpha = (u, v)$ is a transposition,

$o(\alpha) = 2 \Rightarrow \alpha = \alpha^{-1}$

$\Rightarrow \alpha$ is self inverse

We have $(u\,v)^{-1} = (v\,u) = (u\,v)$

Let $(1\,2\,3\,4) \in S_4$

Then $(1234) = (1\,4)(1\,3)(1\,2)$

Fact: For any $(a_1 \cdots a_m) \in S_n$, $(a_1 \cdots a_m) = (a_m\, a_1)(a_{m-1}\, a_1) \cdots (a_3\, a_1)(a_2\, a_1)$

product of transpositions

Proposition

If $\alpha \in S_n$ then α is a product of transpositions

Proof: We regard I_n as a product of 0 transpositions (also for $n \geq 2$, $I_n = (1\,2)(2\,1)$)

Let $\alpha \neq I_n$, then $\alpha = \gamma_1 \cdots \gamma_k$ for some disjoint cycles γ_i, $1 \leq i \leq k$

Replace each γ_i by a product of transpositions above ■

Example:

With $\beta = (1\,2)(3\,4\,5)(6\,10\,11\,7)(8\,9) = (1\,2)(5\,3)(4\,3)(7\,6)(10\,6)(8\,9)$

Remark:

1) Transposition representation NOT disjoint

2) NOT unique. β can be written as

$$\beta = (3\,2)(1\,3)(5\,2)(4\,2)(3\,2)(7\,6)(11\,6)(10\,6)(8\,9)$$

Definition Transposition number

The transposition number $T(\sigma)$ of an arbitrary permutation $\sigma \in S_n$ is defined to be the non-negative integer computed by decomposing σ into disjoint cycles and taking the following sum

$$T(\sigma) = \sum_{r=1}^{n} (r-1)(\#r\text{-cycles})$$

In other words, we take weighted sum of the number of disjoint cycles, where the weights are what we believe to be number of transpositions to factorise each cycle

Note: Since the decomposition into disjoint cycles is unique, $T(\sigma)$ is unique (well-defined)

Also $T(I_n) = 0$

Example

(1) $\sigma \in S_{10}$

$$\sigma = (3\,8)(1\,7\,9)(2\,5\,4\,10\,6)$$

$$T(\sigma) = 1.1 + 2.1 + 4.1 = 7$$

(2) $\sigma \in S_{15}$

$$\sigma = (3\,8)(1\,7\,9)(2\,5\,4\,10\,6)(11\,12\,13\,14\,15)$$

$$T(\sigma) = 1.1 + 2.1 + 4.2 = 11$$

Note: $T(\sigma)$ is the minimum number of transpositions to completely factorize σ.

Theorem Parity Theorem

Let $\sigma \in S_n$. The number of transposition in any complete factorization of σ has the same parity as $T(\sigma)$

i.e. it is always even or odd

Proof: Proof has 2 parts

Part 1: Consider $\sigma \in S_n$ being multiplied by a transposition $\tau = (a\,b)$ to form

$$\sigma' = \tau\sigma$$

When σ is decomposed into disjoint cycles, there are 2 cases

1) CASE 1: a, b contained in same cycle

$$(a\,b)(a\,c_1 \cdots\cdots c_r)(b\,d_1 \cdots\cdots d_s) = (b\,d_1 \cdots d_s\,a\,c_1 \cdots c_r)$$

$$T(\sigma') = T(\sigma) + 1$$

2) CASE 2: a, b are contained in the same cycle

$$(a\,b)(a\,c_1 \cdots\cdots c_r\,b\,d_1 \cdots\cdots d_s) = (b\,d_1 \cdots\cdots d_s)(a\,c_1 \cdots\cdots c_r)$$

$$T(\sigma') = T(\sigma) - 1$$

Thus multiplying any permutation changes its parity

Part 2: Using induction, let $P(K)$ be the statement

"If σ is a product of K transpositions then K has same parity as $T(\sigma)$"

The base case $P(1)$ is true as a transposition being a 2 cycle has transposition number 1

For inductive step, suppose $P(K)$ is true and σ is a product of $K+1$ transpositions.

$$\sigma = \tau_{K+1}\tau_K \cdots\cdots \tau_1$$

Since transpositions are self inverse

$$\tau_{K+1}\sigma = \tau_K \cdots\cdots \tau_1$$

Hence by the induction hypothesis, $T(\tau_{K+1}\sigma)$ has the same parity as K. Therefore by part 1,

$T(\sigma)$ has opposite parity to $K \Rightarrow$ same parity as $K+1$

$\Rightarrow P(K+1)$ is true ■

Definition Sign

Let $\alpha \in S_n$. Then α is even/odd if α is product of even/odd number of transpositions

The sign of α denoted $sgn(\alpha)$ is defined by

So $sg: S_n \to \{1,-1\}$

$$sgn(\alpha) = \begin{cases} 1 & \alpha \text{ is even} \\ -1 & \alpha \text{ is odd} \end{cases}$$

Example S_3

Evens: I_3, $e=(1\,2\,3)=(1\,3)(1\,2)$ $e^2=(1\,3\,2)=(1\,2)(2\,1)$

Odds: $\sigma_1=(2\,3)$ $\sigma_2=(1\,3)$ $\sigma_3=(1\,2)$

Consider $\alpha, \beta \in S_n$. Write

$\alpha = \mu_1 \cdots \mu_r$, $\beta = \nu_1 \cdots \nu_s$ where μ_i, ν_j are transpositions

$1 \le i \le r$, $1 \le j \le s$

Then $\alpha\beta = \mu_1 \cdots \mu_r \nu_1 \cdots \nu_s$ is a product of $r+s$ transpositions

α	β	$\alpha\beta$
even	even	even
even	odd	odd
odd	even	odd
odd	odd	even

$sgn(\alpha)$	$sgn(\beta)$	$sgn(\alpha\beta)$
1	1	1
1	-1	-1
-1	1	-1
-1	-1	1

Definition

Let $n \in \mathbb{N}$. Then

$$A_n = \{\alpha \in S_n : \alpha \text{ is even}\}$$

Proposition Alternating Group

We have $A \le S_n$

Proof:

I_n is even $\Rightarrow I_n \in A_n$

Let $\alpha, \beta \in A_n$. Then α, β are even. From the table

$$\alpha, \beta \in A_n \Rightarrow \alpha\beta \text{ is even}$$
$$\Rightarrow \alpha\beta \in A_n$$

Still with $\alpha \in A_n$, write $\alpha = \mu_1 \cdots \mu_r$ where μ_i are transpositions and r is even

Then $\alpha^{-1} = (\mu_1 \mu_2 \cdots \mu_r)^{-1} = (\mu_r^{-1} \mu_{r-1}^{-1} \cdots \mu_2^{-1} \mu_1^{-1}) = \mu_r \mu_{r-1} \cdots \mu_2 \mu_1$ is a product of even transpositions

Hence

$$\alpha^{-1} \in A_n$$

Therefore $\quad A_n \leq S_n$

$\blacksquare$

Note:

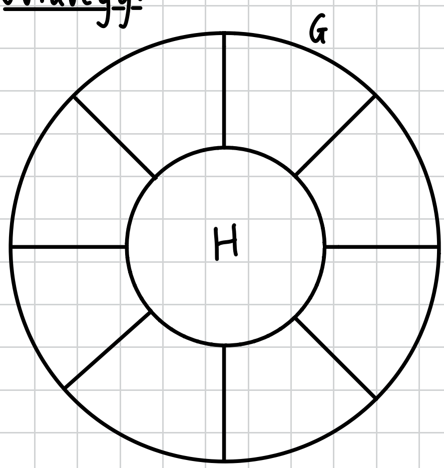
$A_3 = \{I_3, \rho, \rho^2\} = \langle \rho \rangle$ and $|A_3| = 3 = \frac{6}{2} = \frac{|S_3|}{2}$

4. Cosets and Lagrange's Theorem

<u>Lagrange's Theorem</u>: Let G be a finite set, $H \leq G$. Then,

$$|H| \, \big| \, |G|$$

<u>Strategy</u>:



Partition G into blocks of the same size, one of which is H

Cosets

Definition Left Coset

Let G be a group, $H \leq G$ and $a \in G$

The left coset with coset leader a is

$$aH = \{ah : h \in H\}$$

<u>Note</u>:

$$eH = \{eh : h \in H\} = \{h \in H\} = H$$

So H is a left coset

<u>Example</u>:

1) Group S_3, subgroup $H = \{I_3, \sigma_2\} = \langle \sigma_2 \rangle$

$$I_3 H = \{I_3 I_3, I_3 \sigma_2\} = \{I_3 \sigma_2\} = H$$

$$\rho H = \{\rho I_3, \rho \sigma_2\} = \{\rho, \sigma_1\}$$

$$\rho^2 H = \{\rho^2 I_3, \rho^2 \sigma_2\} = \{\rho^2, \sigma_3\}$$

$$\sigma_1 H = \{\sigma_1 I_3, \sigma_1 \sigma_2\} = \{\sigma_1, \rho\} = \rho H$$

$$\sigma_2 H = \{\sigma_2 I_3, \sigma_2 \sigma_3\} = \{\sigma_2 I_3\} = H$$

$$\sigma_3 H = \{\sigma_3 I_3, \sigma_3 \sigma_2\} = \{\sigma_3, \rho^2\} = \rho^2 H$$

Notice:

(a) Coset leader NOT unique:

$$I_3 H = \sigma_2 H = H$$

$$\sigma_1 H = \rho H$$

$$\sigma_3 H = \rho^2 H$$

(b) Distinct cosets are disjoint

(c) Cosets have the same size $|\mu H| = 2 = |H| \quad \forall \mu \in S_3$

(d) $S_3 = H \cup \rho H \cup \rho H$

Example:

Group $(\mathbb{R}^*, \times)$, subgroup $(\mathbb{R}^+, \times)$

$$r\mathbb{R}^+ = \{rs : s \in \mathbb{R}^+\} = \{rs : s > 0\} = \begin{cases} \mathbb{R}^+ & \text{if} \quad r > 0 \\ \mathbb{R}^- & \text{if} \quad r < 0 \end{cases}$$

where $\mathbb{R}^- = \{r \in \mathbb{R} : r < 0\}$

Let $r > 0$. Then $rs > 0$ for all $s > 0$; if $h > 0$, then $h = r\frac{h}{r} \in r\mathbb{R} \Rightarrow r\mathbb{R}^+ = \mathbb{R}^+$

Similarly for $r < 0$

Notice:

(a) Coset leaders are NOT unique:

$$1\mathbb{R}^+ = 2\mathbb{R}^+, \text{ etc}$$

(b) Distinct cosets are disjoint

(c) Cosets have the same size: $\exists$ bijection $\mathbb{R}^+ \longrightarrow \mathbb{R}^-$; $x \mapsto x$;

(d) $\mathbb{R}^* = \mathbb{R}^+ \cup \mathbb{R}^-$

Lemma The coset lemma

Let $H \leq G$ where G is a group

Define relation $\sim_H$ on G by the rule:

$$a \sim_H b \iff b^{-1}a \in H$$

Then $\sim_H$ is an equivalence relation on G and

$$[a] = aH$$

proof: Let $a \in G$. Then

Reflexive: $a^{-1}a = e \in H$ so $a \sim_H a$

Symmetry: Suppose that $a \sim_H b$. So $b^{-1}a \in H$. Then $(b^{-1}a) \in H$ as $H \leq G$.

Hence $a^{-1}(b^{-1})^{-1} = a^{-1}b \in H \implies b \sim_H a$ closure under inverse

Transitivity: Suppose $a, b, c \in H$ and $a \sim_H b \sim_H c \implies b^{-1}a \in H,\ c^{-1}b \in H$

$\implies c^{-1}bb^{-1}a \in H$ closure

$\implies c^{-1}a \in H$

$\implies a \sim_H c$

Hence $\sim_H$ is an equivalence relation

We have $[a] = \{b \in G : b \sim_H a\}$

$= \{b \in G : a^{-1}b \in H\}$

$= \{b \in G : a^{-1}b = h \in H\}$

$= \{b \in G : b = ah, h \in H\}$

$= aH$

■

Reminder: For any equivalence relations we have

$$a \sim b \iff [a] = [b] \iff b \in [a]$$

$$\iff a \in [b]$$

Corollary

Let $H \leq G$ where G is a group and let $a, b, c \in G$

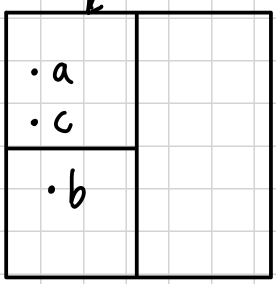
1) $a \in aH$
2) $c \in aH \iff cH = aH$
3) $aH = bH \iff aH \cap bH \neq \phi$
4) $aH = bH \iff b^{-1}a \in H$
5) $aH = H \iff a \in H$

Proof:

(1) $a \in [a] = aH$ as $a \sim_H a$

(2) $c \in aH = [a] \iff cH = [c] = [a] = aH$

aH=cH



(3) Equivalence classes partition a set

(4) $aH = bH \iff [a] = [b]$

$\iff a \sim_H b$

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

(5) $aH = H \iff aH = eH$

$\iff e^{-1}a \in H$

$\iff a \in H$

■

Lemma

Let $H \leq G$ where G is a group. For any $a, b \in G$

$$|aH| = |bH| = |H|$$

proof: Define function

$$\lambda_b : H \longrightarrow bH$$
$$\lambda_b(b) = bh$$

Onto: Clearly λ_b is onto since if $bh \in bH$, $bh = \lambda_b(h)$

One-to-One:

If $\lambda_b(h) = \lambda_b(k) \implies bh = bk$ left cancelation

$\implies h = k$

Hence λ_b is a bijection $\implies |H| = |bH|$

Hence for any $a, b \in H$, $|H| = |bH| = |aH|$

Definition Index

If $H \leq G$ then $[G:H]$ is the number of left cosets of H in G

$[G:H]$ is the index of H in G

Lagrange's Theorem

Theorem Lagrange's Theorem

Let G be finite group and $H \leq G$. Then the order of H divides order of G

$$|H| \mid |G|$$

Moreover

$$\frac{|G|}{|H|} = [G:H]$$

Proof: Let $k = [G:H]$ and $a_1 H = H, a_2 H, \dots, a_k H$ be distinct left cosets of H in G

By lemma above

$$|a_i H| = |H| \; ; \; 1 \leq i \leq k$$

and

$$a_i H \cap a_j H = \phi \; ; \; 1 \leq i < j \leq k$$

For any $g \in G$, we have $g \in gH$. Hence

$$G = H \dot{\cup} a_2 H \dot{\cup} \cdots \dot{\cup} a_k H$$

and then

$$\begin{aligned} |G| &= |H| + |a_2 H| + |a_3 H| + \cdots + |a_k H| \\ &= |H| + \cdots + |H| \quad (k \text{ terms}) \\ &= k|H| \end{aligned}$$

So $|H| \mid |G|$ and $\dfrac{|G|}{|H|} = k = [G:H]$

$\blacksquare$

Note: We could also have used right cosets

Definition Right Coset

Let G be a group, $H \leq G$ and $a \in G$

The **right coset** with coset leader a is

$$Ha = \{ha : h \in H\}$$

The dual argument leads to Lagrange's Theorem

Consequently: if G is a finite group and $H \leq G$ then

$$\boxed{\text{number of left cosets} = \text{number of right cosets of } H \text{ in } G}$$

Exercises

Application of Lagrange's Theorem

G is a group, $a \in G$

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is the cyclic subgroup generated by a

If G is finite then $o(a)$ is finite and if $o(a) = n$, then

$$n = |\langle a \rangle| \text{ and } \langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$$

Corollary Order Corollary

Let G be a finite group and let $a \in G$

Then $o(a)$ divides $|G|$

Proof:

We have $|\langle a \rangle| = o(a)$ and $|\langle a \rangle| \mid |G|$ by Lagrange's Theorem

Consequently $a^{|G|} = e$ from remainder lemma. ∎

Corollary

Let $|G| = p$ where p is prime. Then G is cyclic and generated by any of its non-identity elements

proof: Let $|G| = p$ where p is prime. Let $a \in G$ and $a \neq e$

Since $o(a) \mid G$ and $o(a) \neq 1$, we have $o(a) = p$

So $|\langle a \rangle| = o(a) = p = |G|$. Hence $G = \langle a \rangle$ ∎

Corollary

Let $n \geq 2$. Then $A_n = \frac{n!}{2}$

Proof: Recall $A_n = \{\alpha \in S_n : \alpha \text{ is even}\}$

Let $O_n = \{\alpha \in S_n : \alpha \text{ is odd}\} = S_n \setminus A_n$

So $S_n = A_n \dot{\cup} O_n$ (disjoint union) $\implies |S_n| = |A_n| + |O|_n$

Claim: $O_n = (12)A_n$

We have $(12)A_n = \{(12)\alpha : \alpha \in A_n\} \subseteq O_n$

$$O_n = \{(12)\underbrace{(12)\beta}_{\text{even}} : \beta \in O_n\} \qquad (12)(12) = I_n$$

$$\subseteq (12)A_n$$

Hence $(12)A_n \subseteq O_n$

By lemma above

$$|A_n| = |(12)A_n| = |O_n| \implies |S_n| = |A_n| + |O_n|$$

$$\implies |S_n| = n! = 2|A_n|$$

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

■

Theorem Fermat's Little Theorem

Let p be prime and $a \in \mathbb{Z}$. Then

$$a \equiv a^p \pmod{p}$$

Proof:

If $a \equiv 0 \pmod{p}$ then result is clear

If $a \not\equiv 0 \pmod{p}$ then $[a] \in \mathbb{Z}_p^*$

$|\mathbb{Z}|_p = p-1$ so $[a]^{p-1} = [1] \implies [a^{p-1}] = [1]$

$$\implies a^{p-1} \equiv 1 \pmod{p}$$

Hence $a^p \equiv a \pmod{p}$

■

5. Normal Subgroups and Conjugacy

Definition Conjugate

Let G be a group and let $a, g \in G$. Then

gag^{-1} is a **conjugate** of a

Define a relation $\sim$ on G by

$$a \sim b \iff b \text{ is conjugate of } a$$
$$\iff b = gag^{-1} \text{ for some } g \in G$$

Note: $g^{-1}ag$ is also a conjugate of a as

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

Lemma

$\sim$ is an equivalence relation

Proof: Let $a, b, c \in G$

Reflexivity: We have $a = eae^{-1} \Rightarrow a \sim a$

Symmetry: Suppose $a \sim b$. So $b = gag^{-1}$ some $g \in G$. Then

$$a = g^{-1}bg \Rightarrow b \sim a$$

Transitivity: Suppose $a \sim b$ and $b \sim c$. Then $b = gag^{-1}$, $c = hbh^{-1}$ for some $g, h \in G$

So $$c = hbh^{-1} = h(gag^{-1})h^{-1}$$
$$= (hg)a(g^{-1}h^{-1})$$
$$= (hg)a(hg)^{-1}$$

$\Rightarrow a \sim c$

Equivalence classes:

$$[a] = \{b \in G : a \sim b\} = \{gag^{-1} : g \in G\}$$

Definition Conjugacy Class

The equivalence classes under $\sim$ are called **conjugacy classes**

$$[a] = \{b \in G : a \sim b\} = \{gag^{-1} : g \in G\}$$

Example:

1) If G is commutative and $a \sim b$, then

$$b = gag^{-1} = agg^{-1} = ae = a$$

So $\sim$ is an equality relation

2) Let $A, P \in GL(n, \mathbb{R})$. Then

$$\det(PAP^{-1}) = \det P \det A \det P^{-1}$$
$$= (\det P)(\det P^{-1})(\det A)$$
$$= \det(PP^{-1})\det(A)$$
$$= \det I^{n} \det A$$
$$= \det A$$

Hence if $A \in SL(n, \mathbb{R})$, then if $A \sim B$, then $B \in SL(n, \mathbb{R})$

3) In S_6 with $\beta = (1\,2)(3\,5\,4) \Longrightarrow \beta^{-1} = (1\,2)(3\,4\,5)$

Let $\alpha = (1\,2\,5)$

Then

$$\beta^{-1}\alpha\beta = (1\,2)(3\,5\,4)(1\,2\,5)(1\,2)(3\,4\,5)$$
$$= (1\,4\,2) = (2\,1\,4)$$
$$= (\beta(1)\;\; \beta(2)\;\; \beta(5))$$

4) Let $\alpha = (a_1 \cdots\cdots a_k) \in S_n$. Let $\gamma \in S_n$

We claim: $\gamma\alpha\gamma^{-1} = (\gamma(a_1)\; \gamma(a_2) \cdots\cdots \gamma(a_k))$

proof: Suppose $x = \gamma(a_i) \quad 1 \le i \le k$

Then $(\gamma\alpha\gamma^{-1})(x) = \gamma\alpha\gamma^{-1}\gamma(a_i) = \gamma\alpha(a_i) = \gamma(a_{i+1})$

So $(\gamma\alpha\gamma^{-1})(\gamma(a_i)) = \gamma(a_{i+1}) \qquad k+1 \equiv a$

If $x \notin \{\gamma(a_1), \cdots, \gamma(a_k)\}$ then $\gamma^{-1}(x) \notin \{a_1, \cdots a_n\}$

Then $\gamma\alpha\gamma^{-1}(x) = \gamma\gamma^{-1}(x) = x$ as α leaves $\gamma^{-1}(x)$ fixed and

$$(\gamma(a_1) \cdots \gamma(a_k))(x) = x$$

So $\gamma\alpha\gamma^{-1} = (\gamma(a_1) \cdots\cdots \gamma(a_k))$

$\blacksquare$

Example

$\alpha = (1\,3)(2\,6)$: Cycle type is $[2,2]$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 2 & 5 & 1 & 7 & 9 & 8 & 6 \end{pmatrix} = (1\,4\,5)(2\,3)(6\,7\,9)$$

Cycle type: $[3,3,2]$

Theorem

Let $\alpha, \beta \in S_n$. Then,

$$\alpha \sim \beta \iff \alpha \text{ and } \beta \text{ have the same cycle type}$$

Proof:

If $\alpha = \gamma_1 \gamma_2 \cdots\cdots \gamma_k$ $\leftarrow$ cycle decomposition, length of γ_i is l_i

Then $\delta^{-1}\alpha\delta = \delta\gamma_1 \cdots \gamma_k \delta^{-1} = \delta\gamma_1 I_n \gamma_2 I_n \cdots\cdots I_n \gamma_k \delta^{-1}$

$$= (\delta\gamma_1\delta^{-1})(\delta\gamma_2\delta^{-1}) \cdots\cdots (\delta\gamma_k\delta^{-1})$$

We have $\delta\gamma_i\delta^{-1}$ is a cycle of l_i

Moreover if $\gamma_k = (x_1^k, \ldots\ldots, x_{l_k}^k)$, then

$$\delta\gamma_i\delta^{-1} = (\delta(x_1^i), \ldots\ldots \delta(x_{l_i}^i)) \text{ and } \delta\gamma_j\delta^{-1} = (\delta(x_1^j) \cdots\cdots \delta(x_{l_j}^j))$$

These cycles must be disjoint, for if

$$\delta(x_u^i) = \delta(x_v^j) \implies x_u^i = x_v^j \quad \text{by definition of bijection}$$

Hence $\beta = \delta\alpha\delta^{-1}$ and α have the same cycle type

The converse is also true. Suppose that

$$\beta = \mu_1 \cdots\cdots \mu_m$$

is a disjoint decomposition of β with the same cycle type as α, so that the length of μ_i is l_i for $1 \le i \le m$.

Write

$$\mu_k = (y_1^k \cdots\cdots y_{l_k}^k)$$

Then

$$|\{x_1^1, \ldots\ldots, x_{l_1}^1, \ldots\ldots, x_{l_m}^m\}| = |\{y_1^1, \ldots\ldots y_{l_1}^1, \ldots\ldots y_{l_m}^m\}|$$
$$= l_1 + \cdots\cdots + l_m$$

Let $\theta: (\{1,\dots,n\} \setminus \{x_1^1, \dots, x_{\ell_1}^1, \dots, x_{\ell_m}^m\})$

$\longrightarrow (\{1,\dots,n\} \setminus \{y_1^1, \dots, y_{\ell_1}^1, \dots, y_{\ell_m}^m\})$ be a bijection.

Define $\delta \in S_n$ by

$$\delta(x_j^i) = y_j^i$$

and for $z \notin \{x_1^1, \dots, x_{\ell_1}^1, \dots, x_1^m, \dots, x_{\ell_m}^m\}$

$$\delta(z) = \theta(z)$$

Then,

$$\delta\alpha\delta^{-1} = \delta\gamma_1 \cdots \gamma_m\delta^{-1}$$
$$= (\delta\gamma_1\delta^{-1}) \cdots (\delta\gamma_m\delta^{-1}) = \mu_1 \cdots \mu_m$$
$$= \beta$$

■

Example:

Let $K = \{I_4, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

$K \leq A_4$ as every element of K is self inverse, $I_4 \in K$

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

$\Rightarrow$ Multiplication is closed on K and $K \leq A_4$

Further, if $(a\,b)(c\,d) \in K$, then for $\gamma \in S_4$

$$\gamma(a\,b)(c\,d)\gamma^{-1} = \gamma(a\,b)\gamma^{-1}\gamma(c\,d)$$
$$= (\gamma(a)\ \gamma(b))(\gamma(c)\ \gamma(d)) \in K$$

Theorem

A_4 has no order 6 subgroup.

We have $|A_4| = \frac{4!}{2} = 12$

Proof: The cycle types of non-identity elements of S_4 are

$$[2],\ [2,2],\ [3],\ [4]$$

Elements of cycle type $[2]$ are of form $(a\,b)$ even

Elements of cycle type $[4]$ are of form $(a\,b\,c\,d) = (a\,d)(a\,c)(a\,b)$ odd

Elements of cycle type $[2,2]$ are of form $(a\,b)(c\,d)$ even

Elements of cycle type [2] are of form $(a\,b\,c) = (a\,c)(a\,b)$ even

So the elements of A_4 are: $\left\{\begin{array}{l} I_4, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,3\,2), \\ (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3) \end{array}\right\}$

So suppose $H \leq A_4$, $|H| = 6$. If H contains 2 elements of type [2,2], it must contain the third as

$$(a\,b)(c\,d)(a\,c)(b\,d) = (a\,d)(c\,b) \quad \text{closure}$$

Also all elements of [2,2] type are self inverse. Hence

$$K = \{I_4, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq H \quad \text{contradicting Lagrange's Theorem.}$$

as $4 \nmid 6$, $|K| \nmid |H|$

If $(1\,2)(3\,4) \in H$ and $\alpha = (a\,b\,c) \in H$, then

$$\alpha(1\,2)(3\,4)\alpha^{-1} \in H \implies (\alpha(1)\;\alpha(2))(\alpha(3)\;\alpha(4)) \in H$$

Can only have one [2,2] element. To avoid contradiction, we have

$$(1\,2)(3\,4) = (\alpha(1)\;\alpha(2))(\alpha(3)\;\alpha(4))$$

We could have

$$(1\,2) = (\alpha(1)\;\alpha(2)) \qquad (3\,4) = (\alpha(3)\;\alpha(4)) \quad \text{- contradiction}$$

or

$$(1\,2) = (\alpha(3)\;\alpha(4)) \text{ and } (3\,4) = (\alpha(1)\;\alpha(2)) \quad \text{- contradiction}$$

So H consists entirely of identity and 3-cycles. But 3 cycles come in pairs

$$\implies |H| = \text{odd}$$

$$\implies \text{contradiction}$$

Hence no such H exists. $\blacksquare$

Normal Subgroups

Definition Normal Subgroup

Let G be a group and $H \leq G$.

Then H is a normal subgroup of G denoted $H \trianglelefteq G$ if

$$\forall g \in G \ \forall h \in H, \ ghg^{-1} \in H \qquad \text{closed under conjugation}$$

i.e. H is a union of conjugacy classes

Example:

(1) $H \leq G$ where G is commutative.

Therefore for any $g \in G$, $h \in H$,

$$ghg^{-1} = hgg^{-1} = h. \text{ So } H \trianglelefteq G$$

2) We always have $\{e\} \trianglelefteq G$, $G \trianglelefteq G$ since $geg^{-1} = e$

3) For $\alpha \in S_n$ and $\beta \in A_n$

$$\begin{aligned} sg(\alpha\beta\alpha^{-1}) &= sg(\alpha)sg(\beta)sg(\alpha^{-1}) \\ &= sg(\alpha)sg(\alpha^{-1}) \\ &= sg(\alpha\alpha^{-1}) \\ &= sg(I_n) = 1 \end{aligned}$$

$\Longrightarrow \alpha\beta\alpha^{-1} \in A_n$ and $A_n \trianglelefteq S_n$

4) Let $H = \{I_3, \sigma_2\}$

$$\rho\sigma_2\rho^{-1} = \rho\sigma_2\rho^2 = \sigma_3 \notin H. \text{ So } H \ntrianglelefteq S_3$$

5) $SL(n,\mathbb{R}) \leq GL(n,\mathbb{R})$

If $A \in SL(n,\mathbb{R})$ and $P \in GL(n,\mathbb{R})$ then

$$\det(A) = \det(PAP^{-1}), \text{ we have } P^{-1}AP \in SL(n,\mathbb{R})$$

So $SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$

Simple Groups

Definition

A group G is simple if $\{e\}$ and G are the only normal subgroup of G

Proposition

A_4 is not simple

Proof: We have shown

$$K \trianglelefteq A_4$$

∎

6. Homomorphisms

Homomorphisms and isomorphisms

Definition Homomorphism and isomorphism

Let $(G, \circ)$ and $(H, *)$ be groups and let
$$\theta : G \to H$$
be a map.

i) θ is a (group) **homomorphism** if $\forall a, b \in G$,
$$\theta(a \circ b) = \theta(a) * \theta(b)$$

ii) θ is an **isomorphism** if θ is a homomorphism and θ is a bijection

$$\begin{array}{c|c} \circ & b \\ \hline a & a \circ b \end{array} \qquad \begin{array}{c|c} * & \theta(b) \\ \hline \theta(a) & \theta(a) * \theta(b) = \theta(a \circ b) \end{array}$$

Examples:

i) Let $G = \{e\}$, $H = \{f\}$ be trivial groups. Then
$$\theta : G \to H$$
$$\theta(e) = f$$
is a homomorphism since only products in G are
$$ee = e \quad \text{and} \quad \theta(ee) = \theta(e) = f = ff = \theta(e)\theta(e)$$
Clearly θ is a bijection $\Longrightarrow$ isomorphism

ii) $\alpha : T = \{1, -1\} \longrightarrow \{I_3, \sigma_1\}$ given by
$$\alpha(1) = I_3 \qquad \alpha(-1) = \sigma_1$$
is an isomorphism

proof: Clearly α is a bijection. We have
$$\alpha(1 \cdot 1) = \alpha(1) = I_3 = I_3 I_3 = \alpha(1)\alpha(1)$$
$$\alpha(1(-1)) = \alpha(-1) = \sigma_1 = I_3 \sigma_1 = \alpha(1)\alpha(-1)$$
$\alpha((-1)\,1)$ similar

$$\alpha((-1)(-1)) = \alpha(1) = I_3 = \sigma_1\sigma_1 = \alpha(-1)\alpha(-1)$$

Hence α is an isomorphism $\blacksquare$

(3) $\theta : \mathbb{R} \to \mathbb{R}^*$ given by

$\theta(x) = e^x$

is a homomorphism since

$$\forall x,y \quad \theta(x+y) = e^{x+y} = e^x e^y = \theta(x)\theta(y)$$

θ is not onto since $\operatorname{Im}\theta = \mathbb{R}^+ \implies$ not an isomorphism

$\theta : \mathbb{R} \to \mathbb{R}^+$ is a bijection $\implies$ isomorphism

4) $\det : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ is homomorphism

$$\det(AB) = \det A \det B$$

Note: det is not an isomorphism for $n \geq 2$

ex: $$\det\begin{pmatrix} 1 & & & 0 \\ & 2 & & \\ & & 1 & \\ 0 & & & \ddots & \\ & & & & 1 \end{pmatrix} = 2 = \det\begin{pmatrix} 2 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & \ddots & \\ & & & & 1 \end{pmatrix}$$ (not 1-1)

5) $\theta : K \longrightarrow T = \{1, -1\}$ given by

$\theta(e) = \theta(a) = 1$, $\theta(b) = \theta(c) = -1$

is a homomorphism

proof:

1) $\theta(ae) = \theta(a) = 1 = 1 \cdot 1 = \theta(a)\theta(e)$. Similar for $ea \in K$

Lemma

$\theta: G \to H$ is a homomorphism. Then, $\forall g \in G$, $z \in \mathbb{Z}$

i) $\theta(e_G) = e_H$

ii) $\theta(g^{-1}) = \theta(g)^{-1}$

iii) $\theta(g^z) = \theta(g)^z$

Proof:

i) $\theta(e_G) = \theta(e_G e_G)$

$= \theta(e_G)\theta(e_G)$ $\quad \theta$ is a homomorphism

$\Longrightarrow e_H\theta(e_G) = \theta(e_G)\theta(e_G)$ $\quad$ since $e_H\theta(e_G) = \theta(e_G)$

$\Longrightarrow e_H = \theta(e_G)$ $\quad$ by right cancellation in H

The only idempotent element (element that squares to itself) is the group identity)

ii) We have $e_H = \theta(e_g) = \theta(gg^{-1}) = \theta(g^{-1}g) \quad \forall g \in G$

So $e_H = \theta(g)\theta(g^{-1}) = \theta(g^{-1})\theta(g)$ as θ is a homomorphism

$\Longrightarrow \theta(g^{-1}) = (\theta(g))^{-1}$

iii) $\theta(g^0) = \theta(e_G) = e_H = \theta(g)^0$ by (i)

For any $n \in \mathbb{N}$

$$\theta(g^n) = \theta(\underbrace{g \cdots g}_{n}) = \theta(g)\theta(\underbrace{g \cdots g}_{n-1}) = \theta(g)^n$$

$$\theta(g^{-n}) = \theta((g^{-1})^n) = (\theta(g^{-1}))^n$$

$$= (\theta(g)^{-1})^n \quad \text{by ii}$$

$$= \theta(g)^{-n}$$

■

Isomorphic Groups

Definition Isomorphic

A group G is isomorphic to a group H if

$\exists$ an isomorphism $\theta: G \to H$.

We write $G \cong H$

Lemma

If G, H and K are groups then

i) $I_G : G \to G$ is an isomorphism

ii) If $\theta : G \to H$ is an isomorphism, then $\theta^{-1} : H \to G$ is also an isomorphism

iii) If $\theta : G \to H$, $\psi : H \to K$ are isomorphisms, then

$$\psi\theta : G \to K \text{ is an isomorphism}$$

Proof:

i) $I_G : G \to G$ is a bijection.

For any $a, b \in G$, $I_G(ab) = I_G(a) I_G(b)$

So I_G is a homomorphism $\Longrightarrow$ hence an isomorphism

$$\Longrightarrow G \cong G$$

ii) θ, θ^{-1} are mutually inverse. So $\theta^{-1} : H \to G$ is a bijection

Let $h, k \in H$. Since θ is onto, $\exists\, h', k' \in G$ with

$$\theta(h') = h \qquad \theta(k') = k$$

Then $\theta(h'k') = \theta(h')\theta(k') = hk$

So $\theta^{-1}(h)\theta^{-1}(k) = h'k' = \theta^{-1}(hk) \Longrightarrow \theta^{-1}$ is an isomorphism

$$\Longrightarrow H \cong G$$

iii) For any $g, h \in G$,

$$\begin{aligned}(\psi\theta)(gh) &= \psi(\theta(gh)) \\ &= \psi(\theta(g)\theta(h)) \\ &= \psi(\theta(g))\psi(\theta(h)) \\ &= (\psi\theta)(g)\,(\psi\theta)(h)\end{aligned}$$

$$G \xrightarrow{\theta} H \xrightarrow{\psi} K$$

$\Longrightarrow$ composition of homomorphism is a homomorphism

Composition of bijection is a bijection $\Longrightarrow$ $\psi\theta$ is a bijection

$\Longrightarrow$ $\psi\theta$ is a isomorphism ∎

Corollary

The relation $\cong$ (isomorphic) is an equivalence relation on the class of all groups

proof:

Let G, H, K be groups.

Reflexive: By i) of previous lemma, $I_G : G \to G$ is an isomorphism

$$\Longrightarrow G \cong G$$

Symmetry: If $G \cong H$, $\exists$ an isomorphism, $\theta : G \to H$

Then, by (ii) by lemma, $\theta^{-1} : H \to G$ is also an isomorphism

$\Longrightarrow H \cong G$

Transitivity: $G \cong H$ and $H \cong K$ $\Longrightarrow \exists\, \theta : G \to H$ and $\psi : H \to K$ such that

θ and ψ are isomorphism

$\Longrightarrow \psi\theta : G \to K$ is an isomorphism by iii

$\Longrightarrow G \cong K$

■

Properties shared by isomorphic groups

Theorem Properties of Isomorphism

Let $G \cong H$ and let $\alpha : G \to H$ be an isomorphism

1) order of G = order of H ; $|G| = |H|$

2) G is commutative $\Longleftrightarrow$ H is commutative

3) Let $a \in G$. Then $o(a) = o(\alpha(a))$

4) G is cyclic $\Leftrightarrow$ H is cyclic

Proof:

1) true since α is a bijection

2) Suppose G is commutative.

Let $a, b \in H$. Since α is onto, $\exists\, a', b' \in G$ such that

$$\alpha(a') = a \qquad \alpha(b') = b$$

Then $ab = \alpha(a')\alpha(b') = \alpha(a'b')$

$$= \alpha(b'a')$$

$$= \alpha(b')\alpha(a')$$

$$= ba$$

$\Longrightarrow$ H is commutative.

For converse, if H is commutative, then use the fact

$$\alpha^{-1}: H \longrightarrow G$$

is an isomorphism

3) $a^n = e_G \Longleftrightarrow \alpha(a^n) = \alpha(e_G)$ as α is 1-1

$\Longleftrightarrow \alpha(a)^n = e_H$

4) If G is cyclic, $G = \langle a \rangle = \{a^z : z \in \mathbb{Z}\}$

Then $H = \{\alpha(a^z) : z \in \mathbb{Z}\}$ since $H = \alpha(\theta)$

So $H = \{\alpha(a^z) : z \in \mathbb{Z}\} = \{\alpha(a)^z : z \in \mathbb{Z}\} = \langle \theta(a) \rangle \Longrightarrow$ H is cyclic

For converse, use the fact $\alpha^{-1}: H \rightarrow G$ is also an isomorphism ■

Showing groups are isomorphic/are not isomorphic

To show $G \cong H$, we must find an isomorphism between them

Example

1) $(\mathbb{R}, +)$ and $(\mathbb{R}, \times)$ are isomorphic as

$$\theta: \mathbb{R} \longrightarrow \mathbb{R}^+$$

$$\theta(x) = e^x$$

is an isomorphism

2) If $G = \langle a \rangle$ and $H = \langle b \rangle$ are cyclic groups of order n, then $G \cong H$

Define $\alpha: G \rightarrow H$ by $\alpha(a^i) = b^i$

We have $a^i = a^j \Longleftrightarrow i \equiv j \pmod{n}$

$\Longleftrightarrow b^i = b^j$

$\iff \alpha(a^i) = \alpha(a^j)$ well defined

Clearly α is onto $(b^i = \alpha(a^i))$

For any a^i, a^k, we have $\alpha(a^i a^k) = \alpha(a^{i+k})$

$$= b^{i+k} = b^i b^k = \alpha(a^i)\alpha(a^k)$$

Hence α is an isomorphic

To show $G \ncong H$, not isomorphic, we must find a property preserved by isomorphisms that one group has but the other does not

Example

(1) $\mathbb{R} \ncong S_n$ as $\mathbb{R}$ is infinite, $|S_n| = n! < \infty$

(2) $S_n \ncong S_m$ if $n \neq m$ as $|S_n| = n! \neq m! = |S_m|$

(3) $S_3 \ncong \mathbb{Z}_6$ as S_3 not commutative but $\mathbb{Z}_6$ is

(4) $K \ncong \mathbb{Z}_4$ as K is not cyclic but $\mathbb{Z}_4$ is

(5) $\mathbb{R}^* \ncong \mathbb{R}^+$ as $\mathbb{R}^*$ has an element of order 2 (namely $-1 \in \mathbb{R}$) but $\mathbb{R}^+$ does not

(6) $\mathbb{R}^+ \ncong \mathbb{Q}^+$ as for all $r \in \mathbb{R}^+$, $\exists \sqrt{r} \in \mathbb{R}^+$ and $(\sqrt{r})^2 = r$

But $\nexists q \in \mathbb{Q}^+$ with $q^2 = 2$

Also could say $|\mathbb{Q}^+| \neq |\mathbb{R}^+|$

Automorphisms and inner automorphism

Definition Automorphism

An automorphism of G is an isomorphism $G \to G$.

we denote by $Aut(G)$ the set of all automorphism

Proposition

$Aut(G)$ forms a group under $\circ$ composition

<u>proof</u>: We show $Aut(G) \leq S_G$

<u>Identity</u>: We know $I_G \in Aut(G)$

<u>Closure</u>: If $\theta, \psi \in Aut(G)$, then θ, ψ are isomorphism

$\Rightarrow \theta\psi : G \to G$ is an isomorphism

$\Rightarrow \theta\psi \in Aut(G)$

Inverse: $\theta^{-1} : G \to G$ is an isomorphism

$\Rightarrow \theta^{-1} \in Aut(G)$

■

Let G be a group, $a \in G$. Define

$$\boxed{\begin{array}{l} \psi_a : G \longrightarrow G \\ \psi_a(g) = aga^{-1} \end{array}}$$

inner automorphism

Proposition

$\psi_a \in Aut(G)$

Proof:

homomorphism: $\psi_a(gh) = agha^{-1} = ageha^{-1} = (aga^{-1})(aha^{-1}) = \psi_a(g)\psi_a(h)$

one-to-one: $\psi_a(g) = \psi_a(h) \Rightarrow aga^{-1} = aha^{-1}$

$\Rightarrow g = h$ by cancellation

onto: For any $g \in G$, we have

$$\psi_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = (aa^{-1})g(aa^{-1}) = ege = g$$

■

Definition Set of all inner automorphisms

The set $Inn(G) = \{\psi_a : a \in G\}$ is the set of all inner automorphism of G

Remark: If G is commutative, then for any ψ_a

$$\psi_a(g) = aga^{-1} = gaa^{-1} = g = I_G(g)$$

so that $\psi_a = I_g \Rightarrow Inn(G) = \{I_G\}$

Example:

For $\alpha \in S_n$

$$\psi_\alpha(a_1 a_2 \cdots a_m) = \alpha(a_1 \cdots\cdots a_m)\alpha^{-1} = (\alpha(a_1)\ \alpha(a_2) \cdots\cdots \alpha(a_m))$$

then if $\beta = \gamma_1\gamma_2\cdots\gamma_k$ is a cycle decomposition, then

$$\psi_\alpha(\beta) = \psi_\alpha(\gamma_1\gamma_2\cdots\gamma_k)$$
$$= \psi_\alpha(\gamma_1)\cdots\psi_\alpha(\gamma_k)$$

$\Longrightarrow \psi_\alpha$ preserves cycle type

Proposition

Let G be a group. Then

$$\mathrm{Inn}\, G \leq \mathrm{Aut}\, G \leq S_G$$

proof:

Identity: $I_G = \psi_e \in \mathrm{Inn}(G)$; $\psi_e(g) = ege^{-1} = g$

Closure: Let $\psi_a, \psi_b \in \mathrm{Inn}\, G$

Let $g \in G$. Then

$$\psi_a\psi_b(g) = \psi_a(bgb^{-1})$$
$$= a(bgb^{-1})a^{-1}$$
$$= abg(ab)^{-1} = \psi_{ab}(g)$$

$\Longrightarrow \psi_a\psi_b = \psi_{ab} \in \mathrm{Inn}\, G$

Inverse:

$$\psi_a\psi_{a^{-1}} = \psi_{aa^{-1}} = \psi_e = I_G = \psi_{aa^{-1}} = \psi_a\psi_{a^{-1}}$$

$\Rightarrow (\psi_a)^{-1} = \psi_{a^{-1}} \in \mathrm{Inn}(G)$

Properties preserved by homomorphisms

Theorem Properties Preserved by onto homomorphisms

Let G, H be groups, $\alpha : G \to H$ be an onto homomorphism

1) $|G| \geq |H|$
2) G is commutative $\Longrightarrow$ H is commutative
3) Let $a \in G$. If $o(a) = n$, then $o(\alpha(a)) = n$
4) G is cyclic $\Longrightarrow$ H is cyclic

Proof:

1) True since α is an onto function

2) Suppose G is commutative. Let $a,b \in H$. Since α is onto, $\exists\, a', b' \in G$ such that

$$\alpha(a') = a \quad , \quad \alpha(b') = b.$$

Then

$$ab = \alpha(a')\alpha(b') = \alpha(a'b') = \alpha(b'a') = \alpha(b')\alpha(a') = ba$$

G commutative

3)
$$o(a) = n \implies a^n = e_G$$
$$\implies \alpha(a^n) = \alpha(e_G)$$
$$\implies \alpha(a)^n = e_H$$
$$\implies o(\alpha(a)) \mid n$$

4) G is cyclic $\implies \exists\, a \in G$ s.t

$$G = \langle a \rangle = \{a^z : z \in \mathbb{Z}\}$$

Then

$$H = Im(\alpha) = \{\alpha(a^z) : z \in \mathbb{Z}\}$$ onto
$$= \{(\alpha(a))^z : z \in \mathbb{Z}\} = \{b^z : z \in \mathbb{Z}\}$$
$$= \langle b \rangle$$

where $b = \alpha(a) \implies H$ is cyclic. ■

7. Quotients Groups and the Fundamental Theorem of Homomorphisms

Kernels and Images

Definition Images and Kernels

Let G, H be groups and let $\theta: G \to H$ be a homomorphism

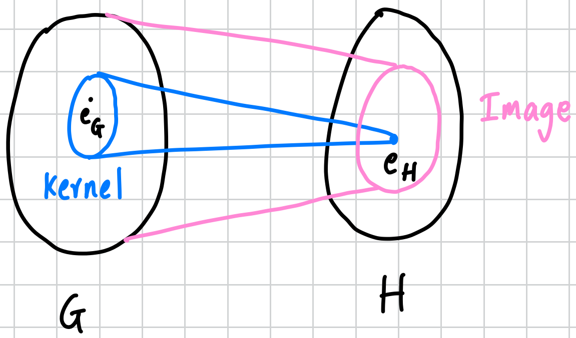
Kernel of θ: $Ker(\theta) = \{g \in G : \theta(g) = e\}$

Image of θ: $Im(\theta) : \{\theta(g) : g \in G\}$

$Im\theta$ is the homomorphic image of G

By defn

$ker\theta \leq G$ and $Im\theta \leq H$



Example:

1) $\theta : GL(2,\mathbb{R}) \to \mathbb{R}^*$ given by $\theta(A) = \det A$. Then

i) θ is a homomorphism

ii) $ker\,\theta = SL(2,\mathbb{R})$

iii) $Im\,\theta = \mathbb{R}^* \implies \theta$ is onto

proof:

i) homomorphism: Let $A, B \in GL(2,\mathbb{R})$

$$\theta(AB) = \det(AB) = \det(A)\det(B) = \theta(a)\theta(b)$$

ii) $A \in ker(\theta) \iff \theta(A) = 1$

$\iff \det(A) = 1$

$\iff A \in SL(2,\mathbb{R})$

So $A \in ker\theta$

iii) Let $r \in \mathbb{R}^*$. Then $\exists \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$ and

$$\theta\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} = r \implies \theta \text{ is onto}$$
$$\implies \text{Im}\,\theta = \mathbb{R}^*$$

Lemma

Let G, H be groups, $\theta : G \to H$ a homomorphisms. Then,

1) $\theta(a) = \theta(b) \iff a^{-1}b \in \text{Ker}\,\theta$

2) θ is 1-1 $\iff \text{Ker}(\theta) = \{e_G\}$

proof:

1) We know from Lemma pg

$$\begin{aligned}
\theta(a) = \theta(b) &\iff \theta(a^{-1})\theta(b) = \theta(a^{-1})\theta(b) \\
&\iff \theta(a^{-1}a) = \theta(a^{-1}b) \\
&\iff \theta(e_G) = \theta(e_H) \\
&\iff e_H = \theta(a^{-1}b) \\
&\iff a^{-1}b \in \text{Ker}\,\theta
\end{aligned}$$

2) We know $e_G \in \text{Ker}\,\theta$

Suppose θ is 1-1. $\forall g \in \text{Ker}\,\theta$, we have

$$\begin{aligned}
\theta(g) = e_H = \theta(e_G) &\implies g = e_G \quad (\theta \text{ is } 1\text{-}1) \\
&\implies \text{Ker}\,\theta = e_G
\end{aligned}$$

Conversely suppose $\text{Ker}\,\theta = \{e_G\}$

Then, $$\begin{aligned}
\theta(a) = \theta(b) &\implies \theta(a^{-1}b) = e_H \\
&\implies a^{-1}b \in \text{Ker}\,\theta \\
&\implies a^{-1}b = e_G \\
&\implies a = b
\end{aligned}$$

Therefore θ is 1-1

■

Lemma

Let G and H be groups, let $\theta : G \longrightarrow H$ be a homomorphism

Then, $\ker\theta \trianglelefteq G$ and $\mathrm{Im}\,\theta \leq H$

<u>proof</u>:

We have from Lemma 6.3, that $\theta(e_G) = e_H$

<u>Ker θ</u>:

<u>Identity</u>: So $e_G \in \ker\theta$ as $\ker(\theta) = \{ g \in G : \theta(g) = e_H \}$ and $\theta(e_G) = e_H$

<u>Closure</u>: $a, b \in \ker\theta$. Then $\theta(a)\theta(b) = e_H e_H = e_H$

<u>Inverse</u>: $\theta(a^{-1}) = (\theta(a))^{-1} = e_H^{-1} = e_H$

<u>Conjugacy</u>: Let $g, h \in G$ $h \in \ker\theta$

$$\begin{aligned} \theta(ghg^{-1}) &= \theta(g)\theta(h)\theta(g^{-1}) \\ &= \theta(g)\, e_H\, \theta(g^{-1}) \quad \text{as } h \in \ker\theta \\ &= \theta(g)\theta(g^{-1}) \\ &= \theta(g)\theta(g)^{-1} = e_H \end{aligned}$$

$\implies ghg^{-1} \in \ker\theta$

$\implies \ker\theta \trianglelefteq G$

<u>Im θ</u>:

<u>Identity</u>: $e_H \in \mathrm{Im}\,\theta$

<u>Closure</u>: Let $g, h \in \mathrm{Im}\,\theta = \{\theta(k) : k \in G\}$

So $\exists\, a, b \in G$ with $g = \theta(a)$ and $h = \theta(a)$

$$gh = \theta(a)\theta(b) = \theta(ab) \in \mathrm{Im}\,\theta$$

<u>Inverse</u>: $g^{-1} = (\theta(a))^{-1} = \theta(a^{-1}) \in \mathrm{Im}(\theta)$

$\blacksquare$

Construction of Quotient Groups

Let $N \trianglelefteq G$. We let

$$G/N = \{aN : a \in G\}$$

Define product

$$(aN)(bN) = abN$$

multiplication in G

Lemma Well-Defined

$aN = cN$ and $bN = dN \implies abN = cdN$ well defined

proof: We have $c^{-1}a \in N$ and $d^{-1}b \in N$

Now
$$(cd)^{-1}(ab) = d^{-1}c^{-1}ab = d^{-1}(bb^{-1})c^{-1}ab$$
$$= \underbrace{(d^{-1}b)}_{\in N}\underbrace{(b^{-1}(c^{-1}a)b)}_{\in N} = (d^{-1}b)(b^{-1}(c^{-1}a)(b^{-1})^{-1})$$

$\in N$

$\therefore (cd)^{-1}ab \in N \implies abN = cdN$ ∎

Proposition

Let $N \trianglelefteq G$. Then G/N is a group under $(aN)(bN) = abN$

Identity: $I_{G/N} = N = eN$

Inverse: $(aN)^{-1} = a^{-1}N \quad \forall a \in G$

proof:

Associativity: Let $aN, bN, cN \in G/N$

Then $(aN)(bNcN) = aNbcN = (a(bc))N = ((ab)c)N$
$$= (ab)NcN = (aNbN)cN$$

Identity: $\forall\, aN \in G/N$

$$aN \cdot N = aNeN = aeN = aN = eaN = eNaN$$
$$= NaN$$

Inverse: $(aN)(a^{-1}N) = aa^{-1}N = eN = N = a^{-1}aN = (a^{-1}N)(aN) \Longrightarrow (aN)^{-1} = (aN)$

Definition Quotient Groups

G/N is the quotient group or factor group of G by N

Example:

$\det: GL(2,\mathbb{R}) \longrightarrow \mathbb{R}^*$ is a homomorphism

$\operatorname{Ker}\det = SL(2,\mathbb{R}) = S$. So

$$S \trianglelefteq G = GL(2,\mathbb{R})$$

Further for any $A, B \in GL(2,\mathbb{R})$

$$AS = BS \iff B^{-1}A \in S \qquad \text{cosets}$$
$$\iff \det B^{-1}A = 1$$
$$\iff \det B = \det A$$

We have

$G/S = \{AS : A \in G\}$ and

$$(AS)(BS) = (AB)S$$

So it seems $G/S \cong \mathbb{R}^*$

Proposition

Let $N \trianglelefteq G$. Then

$$\nu_N : G \longrightarrow G/N$$
$$\nu_N(g) = gN$$

is an onto homomorphism with $\operatorname{Ker}\nu_N = N$

proof:

homomorphism: $\forall\, g, h \in G$, we have

$$\nu_N(gh) = ghN = gNhN = \nu_N(g)\nu_N(h)$$

onto: Let $gN \in G/N$. Then $gN = \nu_N(g) \Longrightarrow \nu_N$ is onto

Finally

$$n \in \operatorname{Ker}\nu_N \iff \nu_N(n) = N \iff nN = N \iff n \in N. \quad \therefore \operatorname{Ker}\nu_N = N.$$

■

Note $G/N = \operatorname{Im} \nu_N$

We now know

$\{\text{Kernels of homomorphism}\} = \{\text{normal subgroups}\}$

$\{\text{quotient groups}\} \subseteq \{\text{homomorphic groups}\}$

Theorem Fundamental Theorem of Homomorphisms (FTH)

Let G and H be groups and let $\theta: G \to H$ be a homomorphism.

Then, $\ker\theta \trianglelefteq G$, $\operatorname{Im}\theta \leq H$ and $G/_{\ker\theta} \cong \operatorname{Im}\theta$

proof: From Lemma 7.4, we have $\ker\theta \trianglelefteq G$ and $\operatorname{Im}\theta \leq H$

Let $N = \ker\theta$. We want to show $G/N \cong \operatorname{Im}\theta$

Define $\bar{\theta}: G/N \to \operatorname{Im}\theta$ by

$$\bar{\theta}(aN) = \theta(a)$$

1-1 and well-defined: $\forall\, aN, bN \in G/N$

$$\begin{aligned} aN = bN &\iff b^{-1}a \in N \\ &\iff \theta(b^{-1}a) = e_H \quad \text{as } N = \ker\theta \\ &\iff \theta(b)^{-1}\theta(a) = e_H \\ &\iff \theta(a) = \theta(b) \\ &\iff \bar{\theta}(aN) = \bar{\theta}(bN) \end{aligned}$$

$\Rightarrow$: $\bar{\theta}$ is well defined

$\Leftarrow$: $\bar{\theta}$ is 1-1

Onto: $\forall\, h \in \operatorname{Im}\theta$, we have

$h = \theta(a) = \bar{\theta}(aN)$ so $\bar{\theta}$ is onto

homomorphism: $$\begin{aligned} \bar{\theta}(aNbN) &= \bar{\theta}(abN) \\ &= \theta(ab) \\ &= \theta(a)\theta(b) \\ &= \bar{\theta}(aN)\bar{\theta}(bN) \end{aligned}$$

■

Example:

We have $\det: GL(2,\mathbb{R}) \longrightarrow \mathbb{R}^*$ is an onto homomorphism so $\operatorname{im}\det = \mathbb{R}^*$

$$\ker\det = SL(2,\mathbb{R})$$

Let $G = GL(2,\mathbb{R})$, $S = SL(2,\mathbb{R})$

Then by FTH, $G/S \cong \mathbb{R}^*$

$$\overline{\det}: G/S \to \mathbb{R}^*; \ \overline{\det}(AS) = \det(A)$$

Applications of FTH: Examples

1) Show that for any $n \geq 2$,

$$A_n \trianglelefteq S_n \quad \text{and} \quad S_n/A_n \cong T$$

where $T = \{1, -1\}$

<u>proof</u>: Recall the sign function sg

$$sg: S_n \longrightarrow T$$

$$sg(\alpha) = \begin{cases} 1 & \alpha \text{ is even} \\ -1 & \alpha \text{ is odd} \end{cases}$$

We drew a table

$sg\,\alpha$	$sg\,\beta$	$sg(\alpha\beta)$
1	1	1
1	-1	-1
-1	1	-1
-1	-1	-1

Clear from table,

$$sg(\alpha\beta) = sg(\alpha)\,sg(\beta) \qquad \forall \alpha, \beta \in S_n$$

$\Longrightarrow$ sg is a homomorphism.

Further

$$\alpha \in \ker(sg) \iff sg\,\alpha = 1$$

$$\iff \alpha \in A_n$$

So $A_n = \ker(sg)$

<u>Onto</u>: We have

$$1 = sg(I_n) \quad \text{and} \quad -1 = sg((1,2))$$

$$\Longrightarrow Im(sg) = \{1,-1\} = T$$

By FTH,

$$\ker(sg) = A_n \trianglelefteq S_n$$

$$S_n/\ker(sg) \cong Im(sg) \Longrightarrow S_n/A_n \cong T$$

■

2) Show that $SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$ and

$$GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^*$$

<u>proof</u>: We find an onto homomorphism: $\theta : GL(n,\mathbb{R}) \longrightarrow \mathbb{R}^*$ such that

$$\operatorname{Ker}\theta = SL(n,\mathbb{R}).$$

Consider $\det : GL(n,\mathbb{R}) \longrightarrow \mathbb{R}^*$

$$A \longmapsto \det A$$

<u>homomorphism</u>: $\det AB = \det A \det B \quad \forall A,B \in GL(n,\mathbb{R})$

<u>onto</u>: $\forall r \in \mathbb{R}^*, \exists \begin{pmatrix} r & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in GL(n,\mathbb{R})$ such that

$$\det \begin{pmatrix} r & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix} = r \Longrightarrow \det \text{ is onto}$$

$$\Longrightarrow Im \det = \mathbb{R}^*$$

We have

$$A \in \ker\det \Longleftrightarrow \det A = 1$$

$$\Longleftrightarrow A \in SL(n,\mathbb{R})$$

So $SL(n,\mathbb{R}) = \ker\det$.

By FTH; $\ker\det \trianglelefteq GL(n,\mathbb{R}) \Longrightarrow SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$

$$GL(n,\mathbb{R})/\ker\det \cong Im\det \Longrightarrow GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^*$$

■

3) Show that $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and

$$\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n$$

where $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$

<u>proof</u>: Define

$$\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$
$$\alpha(z) = [z]$$

<u>homomorphism</u>: $\forall z, w \in \mathbb{Z}$,

$$\alpha(z+w) = [z+w] = [z] \oplus [w] = \alpha(z) \oplus \alpha(w)$$

<u>onto</u>: $\forall [z] \in \mathbb{Z}_n$, $\exists z \in \mathbb{Z}$ such that $[z] = \alpha(z)$

$$\Rightarrow \alpha \text{ is onto}$$

$$\Rightarrow \operatorname{Im}\alpha = \mathbb{Z}_n$$

Finally $\forall z \in \mathbb{Z}$,

$$\begin{aligned} z \in \operatorname{Ker}\alpha &\iff \alpha(z) = [0] \\ &\iff [z] = [0] \\ &\iff z \equiv 0 \pmod n \\ &\iff n \mid z \\ &\iff z \in n\mathbb{Z} \end{aligned}$$

So $\operatorname{Ker}\alpha = n\mathbb{Z}$

By FTH,

$$\operatorname{Ker}\alpha \trianglelefteq \mathbb{Z} \Rightarrow n\mathbb{Z} \trianglelefteq \mathbb{Z}$$

$$\mathbb{Z}/_{\operatorname{Ker}\alpha} \cong \operatorname{Im}\alpha \Rightarrow \mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n \quad \blacksquare$$

Direct Product Groups

For any subsets $A \subseteq G$, $B \subseteq G$ of a group G, define

$$\boxed{AB = \{ab : a \in A,\ b \in B\}}$$

Definition Internal Direct Product

Let G be a group, $H \leq G$, $K \leq G$.

We say G is the internal direct product of H and K if

(i) $H \trianglelefteq G$, $K \trianglelefteq G$;

(ii) $H \cap K = \{e\}$

(iii) $G = HK = \{g = hk : h \in H,\ k \in K\}$

Proposition

Let G be the internal direct product of subgroups $H \leq G$, $K \leq G$.

i) $\forall g \in G$, the expression of g as

$$g = hk$$

for $h \in H$ and $k \in K$ is unique

ii) If $h \in H$, $k \in K \implies hk = kh$

iii) $G \cong H \times K$

iv) $G/H \cong K$

Proof:

i) If $\forall g \in G$, $g = hk = h'k'$ where $h', h \in H$, $k, k' \in K$.

Then $\underbrace{(h')^{-1}h}_{\in H} = \underbrace{k'(k^{-1})}_{\in K} \in H \cap K = \{e\} \implies (h')^{-1}h = k'(k^{-1}) = e$

$$\implies h = h' \text{ and } k = k'$$

ii) Suppose $h \in H$, $k \in K$. Consider $(hk)(kh)^{-1}$

$$(hk)(hk)^{-1} = hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})}_{\substack{\in K \\ \text{normal}}}\underbrace{k^{-1}}_{\in K} = \underbrace{h}_{\in H}\underbrace{(kh^{-1}k^{-1})}_{\substack{\in K \\ \text{normal}}} \in H \cap K = \{e\}$$

$$\implies hk = kh$$

iii) Define $\psi: G \longrightarrow H \times K$ by

$$\psi(g) = (h,k) \quad \text{where } g = hk,\ h \in H,\ k \in K$$

<u>Well-defined</u>: By part i,

$$hk = h'k' \Rightarrow h = h',\ k = k'$$
$$\Rightarrow (h,k) = (h',k')$$

<u>one-to-one</u>: $\psi(hk) = \psi(h'k') \Rightarrow (h,k) = (h',k')$
$$\Rightarrow h = h',\ k = k'$$
$$\Rightarrow hk = h'k'$$

<u>onto</u>: Since $G = HK$, $\forall (h,k) \in H \times K$, $\exists\ g = hk$ s.t $\psi(g) = (h,k)$

Hence ψ is a bijection.

<u>homomorphism</u>: $\psi((hk)(ab)) = \psi(hakb)$
$$= (ha, kb) \qquad h,a \in H,\ k,b \in K$$
$$= (h,k)(a,b) \qquad \text{external direct product}$$
$$= \psi(hk)\psi(ab)$$

Therefore ψ is an isomorphism and

$$G \cong H \times K$$

iv) Define $\theta: G \to K$

$$\theta(hk) = k \qquad h \in H,\ k \in K$$

<u>well-defined</u>: By part i)

$$hk = h'k' \Rightarrow k = k'$$

<u>onto</u>: $\forall k \in K, \exists ek \in G = HK$ s.t $\theta(ek) = k$

$$\Rightarrow \operatorname{Im}\theta = K$$

<u>homomorphism</u>: $\theta((hk)(ab)) = \theta(hakb) = kb$
$$= \theta(hk)\theta(ab)$$

Finally $hk \in \ker\theta \Leftrightarrow \theta(hk) = e \Leftrightarrow k = e \Leftrightarrow hk = h \in H$

Hence $\ker\theta = H$ and by FTH, $G/H \cong K$ ■