$K \le H = \langle a \rangle = \{ a^m : m \in \mathbb{Z} \}$

Corollary Let $a \in G$ has order n. The following conditions are equivalent.

(1) $\langle a^i \rangle = \langle a^j \rangle$. $= \langle a^d \rangle$ with $d = \gcd(n,i) = \gcd(n,j)$

(2) $|a^i| = |a^j|$. $= n/d$ with $d = \gcd(n,i) = \gcd(n,j)$

(3) $\gcd(n,i) = \gcd(n,j)$.

Corollary Let $a \in G$ has order n. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n,j) = 1$.

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

Case 1° $H = \{ a, a^2, \dots, a^n = e \} \cong \mathbb{Z}_n$

$K \le H$. $K = \langle a^k \rangle$ ✓

Case 2° $H = \{ a^m : m \in \mathbb{Z}_{\neq} \}$ is infinite

$\cong \mathbb{Z}$.

$K \le H$, $K = \langle a^k \rangle$.

Case 2a $K = \{ a^0 = e \}$ ✓

~~$K = \{ a^1 \}$~~ $a^p \in K$

$p \neq 0$

Suppose $c \in G$ of order d not $\langle a \rangle \cup \langle b \rangle$.

Then $\langle c \rangle$ will contain yet another $\phi(d)$ generators that are of order d not in $\langle a \rangle \cup \langle b \rangle$

Repeating this. we will exhaust all the order d elements because G is finite.

If we repeat the process for m times then the number of elements in G of order d is $m\phi(d)$.

Definition (Euler ϕ function) Define $\phi(1) = 1$ and $\phi(n)$ equals the number of integers smaller than n are relatively prime to n for every positive integer $n > 1$.

Theorem Let $G = \langle a \rangle$ be a cyclic group of order n.

$\langle a \rangle = H$ of size d

- If d is a divisor of n, the number of elements of order d in G is $\phi(d)$.
- Consequently, in a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Example

	Z_n	# of generators
$\phi(1) = 1$	$Z_1 = \{\bar{0}\}$	1
$\phi(2) = 1$	$Z_2 = \{\bar{0}, \bar{1}\}$	1
$\phi(3) = 2$	$Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$	2
$\phi(4) = 2$	$Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$	2
$\phi(5) = 4$	$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$	4
$\phi(6) = 2$	$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$	2

Remark. p prime $\phi(p) = p - 1$ $Z_p = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$.

generators.

Proof: Let S be the set of elements of order d, where $d \mid n$.

If $a \in S$, then $\langle a \rangle = H$ is a subgroup of order d.

and $\phi(d)$ so many elements in H will have order d.

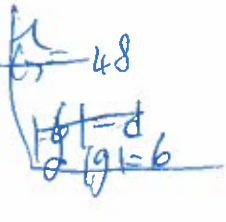
$G = \langle a \rangle$

generators of H

Moreover, if $b \in G$ has order d, then

then $\langle a \rangle = \langle b \rangle$ $\therefore$ $b \in \langle a \rangle$ is one of the $\phi(d)$ generators.

In general suppose G is a finite group. $d \mid |G|$ and let $S = \{g \in G : |g| = d\}$



If no element in S, then $|S| = 0$ is a multiple of $\phi(d)$.

Suppose $a \in S$. Then $\exists$ $\phi(d)$ so many elements in $\langle a \rangle$ with order d.

If no other elements in G has order d, then I am done.

Suppose b is another elements in G with order d. Then $\langle b \rangle$ contains another collection of $\phi(d)$ generators.

$\therefore$ $|S|$ is a ~~multiple of~~ $\phi(d)$.

Chapter 5 Groups of permutations (bijections)

Basic notation and ideas

We study the most "general type" of groups - groups of permutations (bijections).

Definition A bijection from a set A to itself is also called a permutation

Theorem Let A be a set, and let S_A be the set of permutations on A, i.e., bijections from A to A. Then S_A is a group under function composition.

Examples (Important) S_1, S_2, S_3, S_4.

Let $A \neq \phi$ be a set.

Define $S_A = \{ f : f$ is a bijection from A to $A \}$

It is a group under function composition.

(G0) If $f, g : A \to A$ bijection then $f \circ g$ is a bijection.

(G1) $(f \circ g) \circ h = f \circ (g \circ h)$ for any functions $f, g, h : A \to A$

(G2) Let $\tau : A \to A$ be defined $\tau(x) = x \quad \forall x \in A$.

Is the identify function in S_A such that $\tau \circ f = f \circ \tau$.

(G3) If $f \in S_A$, then the inverse function $f^{-1} : A \to A$ exists such that $f \circ f^{-1} = \tau = f^{-1} \circ f$.

If $|A| = n$, we may assume $A = \{1, \cdots, n\}$.

and S_n is used to denote S_A

Cayley Theorem

Definition If A has n elements, we may assume $A = \{1, \ldots, n\}$, and write S_A as S_n, *the symmetric group of degree n*, which has $n!$ elements.

Elements in S_A can be written as $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & & i_n \end{pmatrix}$

Remark The group S_A is not Abelian if A has more than 2 elements.

Theorem 6.1 Every group is isomorphic to a subgroup of S_A.

Proof. Use the Left (or right) regular representation of G

$S_1 = \{(1)\}$ $\quad S_2 = \{(1\,2), (1\,2)\} \cong \mathbb{Z}_2$ (τ, σ)

$*$	τ	σ
τ	τ	σ
σ	σ	τ

$S_3 = \{(1\,2\,3), (1\,2\,3), (1\,2\,3), (1\,2\,3), (1\,2\,3), (1\,2\,3)\}$

If $n \leq 2$, then S_n is Abelian

If $n = 3$

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

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

$\therefore S_3$ not Abelian

If $n > 3$

Consider $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$

$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 1 & 2 & 4 & \cdots & n \end{pmatrix}$

$\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}$

$\therefore S_n$ is not Abelian

Proof of Cayley Theorem :

Let $(G, *)$ be a group.

I will show that $(G, *)$ is isomorphic to a subgroup H of S_G : set of all bijections from G to G.

(which has $n!$ element if $|G| = n$.
& is infinite if $|G|$ is infinite)

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

$S_{\mathbb{Z}_3}$ = set of bijections from $\mathbb{Z}_3$ to $\mathbb{Z}_3$

has 6 elements

Define ① $\Phi : (G, *) \to (S_G, \circ)$
by the following rule :

$$\Phi(g) = \psi_g : G \to G \qquad \forall g \in G$$

$$\psi_g(x) = g * x \quad \text{for all } x \in G$$

To prove ψ_g is a well-defined bijection.

1° $\forall x \in G$, $\psi_g(x) = g(x) \in G$. is uniquely determined
So ψ_g is well-defined

2° 1-1 : $\psi_g(x) = \psi_g(y)$

$gx = gy$

$\therefore x = y$ by cancellation.

3° Onto : Suppose $y \in G$.
Let $x = g^{-1}y \in G$
so that $\psi_g(x) = gx = g(g^{-1}y) = y$.

$g \xrightarrow{\Phi} \boxed{\Phi(g) \to \psi_g}$

Φ in G ; Φ in S_A

Let $H = \{\psi_g : g \in G\}$

To prove: 1° $H \leq S_G$

2° $(G, *) \cong (H, \circ)$

To prove 1°a $H \neq \phi$ because $e \in G$

So that $\psi_e \in H$.

In fact $\psi_e(x) = ex = x \quad \forall x \in G$

So ψ_e is the identity function in S_G.

1°b Let $\psi_g, \psi_h \in H$.

Then $\psi_g \circ \psi_h(x) = \psi_g(hx) = ghx \quad \forall x \in G$

$= kx$ if $k = gh$

$\therefore \psi_g \circ \psi_h = \psi_k$

$\therefore \psi_g \circ \psi_h \in H$

1°c If $\psi_g \in H$, consider ψ_ℓ with $\ell = g^{-1}$.

Then $\psi_g \circ \psi_\ell(x) = \psi_g(\ell x) = g\ell x = gg^{-1}x = x \quad \forall x$.

$\therefore \psi_g^{-1} = \psi_\ell$ for some $\ell = g^{-1} \in G$

$\therefore \psi_g \in H$

$\psi_\ell \circ \psi_g(x)$

$= \ell g x = g^{-1} g x = x$.

$\therefore \psi_\ell \circ \psi_g = \bar{1}$

$\psi_g \circ \psi_\ell = \bar{1}$

} the identity function

Finally: prove that

$$\bar{\Phi} : (G, *) \longrightarrow (H, \circ)$$

defined by $\bar{\Phi}(g) = \psi_g$ is a group isomorphism.

Have to prove

2.a $\bar{\Phi}$ is a bijection, and

2.b $\bar{\Phi}(g_1 * g_2) = \bar{\Phi}(g_1) \circ \bar{\Phi}(g_2) \quad \forall g_1, g_2 \in G$

2.a. For every $\psi_g \in H$, let $g \in G$ so that

$\bar{\Phi}(g) = \psi_g$. $\therefore \bar{\Phi}$ is onto.

Suppose $\bar{\Phi}(g_1) = \bar{\Phi}(g_2)$.

i.e., $\psi_{g_1} = \psi_{g_2}$.

Then $g_1 = \psi_{g_1}(e) = \psi_{g_2}(e) = g_2$ $\therefore$ $g_1 = g_2$

$\therefore$ 1-1

2.b Suppose $g_1, g_2 \in G$.

$\bar{\Phi}(g_1 g_2) = \psi_{(g_1 g_2)} : G \to G$

& $\bar{\Phi}(g_1) \circ \bar{\Phi}(g_2) = \psi_{g_1} \circ \psi_{g_2} : G \to G$

Now. $\forall x \in G$ ~~$\psi_{g_1 g_2}(x) = (g_1 g_2)x$~~ $\Longrightarrow$ always the same.

$\psi_{g_1} \psi_{g_2}(x) = \psi_{g_1}(g_2 x) = g_1(g_2 x)$.

$\therefore$ $\bar{\Phi}(g_1 * g_2) = \bar{\Phi}(g_1) * \bar{\Phi}(g_2)$. $\forall g_1, g_2 \in G$