6.3 Normal subgroups & Quotient groups

<u>Corollary</u>. If $N \lhd G$. then the <u>natural map</u>

$$\phi : G \longrightarrow G/N$$
$$g \longmapsto gN$$

is a surjective homomorphism. $\ker\phi = N$

$\phi(g_1)\phi(g_2) = g_1N \cdot g_2N = g_1g_2N = \phi(g_1g_2)$

$g \in \ker\phi \quad \phi(g) = gN = N \iff g \in N$

Every normal subgroup is the kernel of some homomorphism.

<u>Example</u>.

1 $n\mathbb{Z} := \langle n \rangle \lhd \mathbb{Z}$

$= \{ \cdots - 2n, -n, 0, n, 2n, - \}$

$\mathbb{Z}/n\mathbb{Z} := \{ i + n\mathbb{Z},\ 0 \le i \le n-1 \}$

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$i \longmapsto i + n\mathbb{Z}$$

$\ker\phi = n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

quotient groups are not subgroups

Special cases. e.g.

$$\left(\begin{array}{c} \mathbb{Z}_2 \triangleleft \mathbb{Z}_4 \\ \mathbb{Z}_4/\mathbb{Z}_2 \cong \mathbb{Z}_2 \end{array} \right)$$

2. $A_3 \triangleleft S_3$ $\quad \phi: S_3 \longrightarrow \mathbb{Z}_2$ $\quad \ker(\phi) = A_3$

[HW] $H \subset G$. $[G:H] = 2 \Rightarrow H \triangleleft G$

3. $D_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = 1 \rangle$ $\quad |D_4| = 8 = 2^3$

$D_4 = \langle e, a, a^2, a^3, b, ab, a^2b, a^3b \rangle$

$$\left(\underline{b}a^n = b^{-1}a^n = (ab)^{-1}a^{n+1} = aba^{n+1} = a^2ba^{n+2} \right)$$

non-trivial normal subgroups:

① $\{e, b, a^2b, a^2\} = N_1$

$\underline{aba^{-1}} = a \cdot ab = a^2b$

② $\{e, ab, a^3b, a^2\} = N_2$

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

③ $\{e, a, a^2, a^3\} = N_3$

④ $\{e, a^2\} = N_4 = Z(G)$

$\Leftrightarrow a^2b = ba^2$

other subgroups:

$$\left. \begin{array}{l} \{e, b\} \\ \{e, ab\} \\ \{e, a^2b\} \\ \{e, a^3b\} \end{array} \right\} \cong \mathbb{Z}_2$$

<u>not normal</u>.

For ①.②.③. $|N_i| = 4$ $|G/N| = 2$ $G/N \cong \mathbb{Z}_2$

① $N_1 = \{e.\ b.\ a^2b.\ a^2\}$ $\cong \begin{cases} \mathbb{Z}_4 \\ V \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2 \end{cases}$

$N_1 \cong D_2 \cong V$

$(A = a^2.\ B = b$ $\langle A, B \mid A^2 = B^2 = (AB)^2 = 1 \rangle)$

$D_4/N_1 = \{N_1,\ aN_1\} \cong \mathbb{Z}_2 = \{\pm 1\}$

$N_1 \cdot N_1 = N_1$ $N_1 \longrightarrow 1$

$N_1 \cdot (aN_1) = aN_1$ $aN_1 \longrightarrow -1$

$(aN_1) \cdot (aN_1) = a^2 N_1 = N_1$

	N_1	aN_1
N_1	N_1	aN_1
aN_1	aN_1	N_1

② $N_2 = \{e,\ ab.\ a^2.\ a^3b\} \cong D_2$ $(A = a^2,\ B = a^3b)$

③ $N_3 = \{e.\ a,\ a^2,\ a^3\} \cong \mathbb{Z}_4$

$D_4/N_3 = \{N_3,\ bN_3\} \cong \mathbb{Z}_2$

④ $N_4 = Z(D_4) = \{e.\ a^2\}$ $(aZ)(aZ) = a^2 Z = \{a^2, e\} = Z$

$D_4/Z(D_4) = \{Z(D_4),\ aZ(D_4).\ bZ(D_4),\ abZ(D_4)\}$

$\cong D_2$

D_4 is nonabelian. $\Rightarrow$ $D_4/Z(D_4)$ non cyclic

[HW]: $G/Z(G)$ cyclic $\Leftrightarrow$ G is abelian.

4. determinant of A in $GL(n, k)$

$$GL(n, k) \xrightarrow{\det} k$$

$$A \longmapsto \det(A)$$

$$[\ \det(AB) = \det(A)\det(B)\ ]$$

$$\ker(\det) = SL(n, k)$$

$$\Rightarrow SL(n, k) \triangleleft GL(n, k)$$

$$(\ \det(gAg^{-1}) = \det(A)\ )$$

① $GL(n, k)/SL(n, k) \cong k^*$ $\qquad M \in GL$

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

$$M = (r^{\frac{1}{n}} e^{i\theta/n}) \cdot A \qquad A \in SL$$

② $U(n)/SU(n) \cong U(1)$ $\qquad U(n)$: $AA^* = 1$

$|\det A| = 1$

SU: $\det = 1$

③ $O(n)/SO(n) = \{SO(n), PSO(n)\} \cong \mathbb{Z}_2$

$(\det P = -1)$

5. Euclidean group E^3

$$g = \{R_\alpha | \vec{\tau}\} \quad g\cdot\vec{r} = R_\alpha\cdot\vec{r} + \vec{\tau}$$

$$\{e|\vec{0}\} = \underbrace{\{R_\alpha|\tau\}}_{g}\underbrace{\{R_\beta|\tau'\}}_{g^{-1}} = \{\underbrace{R_\alpha R_\beta}_{e} | \underbrace{R_\alpha\tau' + \tau}_{\vec{0}}\}$$

$$\Rightarrow g^{-1} = \{R_\alpha^{-1} | -R_\alpha^{-1}\tau\}$$

Consider the translation subgroup $T := \langle \vec{t}_1, \vec{t}_2, \vec{t}_3 \rangle$

($\vec{t}_i$ primitive lattice vectors) $\{e|t\} \in T$

$$\{R_\alpha|\tau\}\{e|t\}\{R_\alpha^{-1} | -R_\alpha^{-1}\tau\}$$
$$= \{R_\alpha|\tau\}\{R_\alpha^{-1} | -R_\alpha^{-1}\tau + t\}$$
$$= \{e | R_\alpha(-R_\alpha^{-1}\tau + t) + \tau\}$$
$$= \{e | R_\alpha t\} \in T^3$$

$$\Rightarrow g T^3 g^{-1} = T^3 \quad \forall g \in G.$$

$$\Rightarrow T^3 \triangleleft E^3$$

6 $\{1\} \triangleleft G$, $G \triangleleft G$ trivial normal subgroups

(Def) A group with no nontrivial normal subgroups is called a <u>simple group</u>.

① $\mathbb{Z}_p \cong \mu_p$ with p prime $H \subset \mathbb{Z}_p$ $|H| = 1$ or p

$H = \{1\}$ or $\mathbb{Z}_p$

② ~~Atternating~~ Alternating groups A_n

$A_3 \cong \mathbb{Z}_3$ A_3 is simple

$D_4 \cong V \triangleleft A_4$ A_4 is not simple

$A_{n\geq 5}$ are simple

6.4 Quotient groups and short exact sequences

Theorem (1st isomorphism theorem) Rotman

$\mu : G \to G'$ homomorphism with kernel K

$\Rightarrow K \trianglelefteq G$, and $G/K \overset{\varphi}{\cong} \mathrm{im}(\mu)$

Proof. $\varphi : G/K \longrightarrow \mathrm{im}\,\mu$

$gK \longmapsto \mu(g)$

① φ is well-defined. $(g_1K = g_2K \Rightarrow \overset{\varphi(g_1K) = \varphi(g_2K)}{\mu(g_1) = \mu(g_2)})$

$g_1K = g_2K \Rightarrow \exists k \in K \;\; g_1 = g_2 k$

$\Rightarrow g_2^{-1} g_1 = k \in K$

$\Rightarrow \mu(g_2^{-1} g_1) = \mu(g_2)^{-1}\mu(g_1) = 1_{G'}$

$\Rightarrow \mu(g_1) = \mu(g_2)$

② φ is a homomorphism.

$\underline{\varphi(g_1K \cdot g_2K)} = \varphi(g_1g_2K) = \mu(g_1g_2)$

$= \mu(g_1)\mu(g_2) = \underline{\varphi(g_1K)\varphi(g_2K)}$

③ a. $\mathrm{im}\,\varphi = \mathrm{im}\,\mu$ surjective

b. $\varphi(g_1K) = \varphi(g_2K) \overset{!}{\Leftrightarrow} \mu(g_1) = \mu(g_2)$ injective

RHS $\Leftrightarrow \mu(g_1 g_2^{-1}) = 1_{G'}$

$\Rightarrow g_1 g_2^{-1} \in K$

a + b : φ is an isomorphism. $\Rightarrow g_1K = g_2K$

Summary:

$$\begin{tikzcd} G \arrow[r, "\mu"] \arrow[dr, "\nu"', "\text{surj.}"] & G' \\ & G/K \arrow[u, "\varphi"', "\text{inj.}"] \end{tikzcd}$$

$\nu: g \mapsto gK$

$\mu = \varphi \circ \nu$ commutative

Now we introduce a sequence of homomorphisms

$$\cdots \; G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

The sequence is <u>exact at G_i</u> if

$$\mathrm{im}\, f_{i-1} = \ker f_i$$

A <u>short exact sequence</u> (正合序列) (SES) is of the form

$$\underset{0}{1} \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \underset{0}{1}$$

① 1 represents trivial group. $\{1\}$

0 : abelian groups "+" as group multiplication

② $1 \to G_1$: inclusion map .

$G_3 \to 1$: trivial homomorphism

$\}$ unique

Exactness at G_i :

1 G_1 : $\ker f_1 = \{1\}_{G_1} \Rightarrow f_1$ is <u>injective</u>

2. G_2 : $\ker f_2 = \mathrm{im}\, f_1$

3. G_3: $\ker f_3 \equiv G_3 = \mathrm{im}\, f_2 \Rightarrow f_2$ is <u>surjective</u>

Now consider a homomorphism $\mu : G \to G'$

$K = \ker \mu$.

We have

inclusion map

$$1 \longrightarrow K \xhookrightarrow{i} G \xrightarrow{\mu} \operatorname{im}\mu \longrightarrow 1$$

$\cong G/K$

Exactness check:

① K. $\ker i = \{1_G\}$ ✓

② G: $\ker \mu = \operatorname{im} i = K$ ✓

③ $\operatorname{im}\mu$: $\ker(\operatorname{im}\mu \to 1) = \operatorname{im}\mu$ ✓

1st isomorphism theorem $\Rightarrow$

$$\boxed{1 \longrightarrow K \longrightarrow G \longrightarrow G/K \longrightarrow 1}$$

<u>Remarks</u>.

1. If we have SES.

$$1 \longrightarrow N \xrightarrow{f_1} G \xrightarrow{f_2} Q \longrightarrow 1$$

$\operatorname{im} f_1 = \ker f_2$

$f_2 : G \to Q$

then $N \cong H \triangleleft G$ (it is iso. ~~to~~ the kernel of homomorphism $G \to Q$)

We sometimes write Q as $G/f_1(N)$

where $f: N \xrightarrow{f} G$ is an injective homomorphism.

"G is an extension of Q by N"

Example.

1. $1 \longrightarrow \underset{(G_2)}{G_1} \longrightarrow G_1 \times G_2 \longrightarrow \underset{(G_1)}{G_2} \longrightarrow 1$

$$\mu: G_1 \times G_2 \longrightarrow G_2 \qquad \begin{pmatrix} g_1 \in G_1 \\ g_2 \in G_2 \end{pmatrix}$$
$$(g_1, g_2) \longmapsto g_2$$

2. $\varphi: \mu_4 \longrightarrow \mu_2 \qquad (\mathbb{Z}_4 \longrightarrow \mathbb{Z}_2)$

$$w \longmapsto w^2 \qquad w = e^{i\frac{2\pi}{4}}$$

$$\ker \varphi = \{\pm 1\} \cong \mathbb{Z}_2$$

$$1 \longrightarrow \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \longrightarrow 1$$

in general $1 \longrightarrow \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n^2} \longrightarrow \mathbb{Z}_n \longrightarrow 1$

$$(\varphi: \mu_{n^2} \longrightarrow \mu_n)$$
$$z \longmapsto z^n$$