Theorem 10.1-2 Suppose $\phi : G_1 \to G_2$ is a group homomorphism.

$x \in G$

$x^k = e$

1. $\phi(e_1) = e_2$.
2. $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbf{Z}$.
3. If $m = |\phi(g)|$ and $n = |g|$, then m divides n.
4. $Ker(\phi)$ is a subgroup of G_1; $\phi(a) = \phi(b)$ if and only if $aKer(\phi) = bKer(\phi)$.
5. Cor If $|Ker(\phi)| = n$, then f is an n to 1 function, and $n|\phi(H)| = |H|$. In particular, ϕ is 1-1 if and only if $\boxed{|Ker(\phi)| = 1}$.
6. If H is a (cyclic, Abelian) subgroup of G_1, then $\phi(H) = \{\phi(a) : a \in H\}$ is a (cyclic, Abelian) subgroup of G_2; if H is a normal subgroup in G_1 then $\phi(H)$ is a normal subgroup in $\boxed{\phi(G_1)}$. $\not\leq G_2$
7. If K is a (normal) subgroup of G_2, then $\phi^{-1}(K) = \{a \in G_1 : \phi(a) \in K\}$ is a (normal) subgroup of G_1. In particular, $Ker(\phi)$ is normal in G.

$\to \phi(0) = \varepsilon \to$ identity $\quad \phi(0) = \phi(1+1) = (1,2)\circ(1,2) = \varepsilon$

Remark Consider $\phi : \mathbf{Z}_2 \to S_3$ such that $\phi(1) = (1,2)$. Then $H = \mathbf{Z}_2$ is a normal subgroup in $\mathbf{Z}_2$, but $\boxed{\phi(\mathbf{Z}_2) = \{\varepsilon, (1,2)\}}$ is not a normal subgroup in S_3.

Proof

~~Let $\phi(e_1) = y \in G_2$~~ Note:

(1) $e_2 \phi(e_1) = \phi(e_1) = \phi(e_1 * e_1) = \phi(e_1) * \phi(e_1)$

$\therefore e_2 = \phi(e_1)$ by Cancellation in G_2

(2) $\phi(g^n) = \phi(\underbrace{g * \cdots * g}_{n}) = \phi(g)^n$ if $n \in \mathbb{N}$.

$\cancel{\phi(g^n)}$ $\phi(g^0) = \phi(e_1) = e_2 = \phi(g)^0$

To study ~~with~~ $\phi(g^{-n})$ $n \in \mathbb{N}$.

Consider $\phi(g^n g^{-n}) = \phi(e_1) = e_2$

$\phi(g^n)\phi(g^{-n})$

$\phi(g)^n \phi(g^{-n})$

$\therefore$ ~~$\phi(g^n)$~~ $\phi(g^{-n}) = \phi(g)^{-n}$

$y^n \cdot \phi(g^{-n}) = e_2$

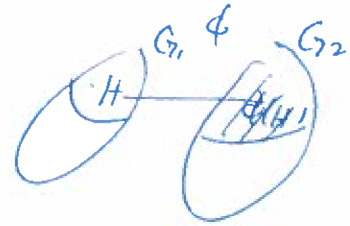
$\phi(g^{-n}) = y^{-n}$

Proof (7): Suppose $K \leq G_2$ ($K \trianglelefteq G_2$).

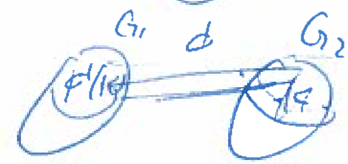
Then $\phi^{-1}(K) = \{ a \in G_1 : \phi(a) \in K \} \subseteq G_1$

is a subgroup (normal subgroup) of G_1.

Remark: i.e., $a \in \phi^{-1}(K)$ means $\phi(a) \in K$.



① Prove $\phi^{-1}(K) \leq G_1$



Step 1: $e_1 \in \phi^{-1}(K) \because \phi(e_1) = e_2 \in K$ (ϕ subgroup)

Step 2: Suppose $a, b \in \phi^{-1}(K)$.

$\phi(a), \phi(b) \in K$.

~~$\phi(ab^{-1}) \in K$~~ $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \in K \quad \because K$ is a subgroup.

$\therefore ab^{-1} \in \phi^{-1}(K)$

Normality. Assume K is normal in G_2.

i.e., for any $k \in K$, $g \in G_2$, then $gkg^{-1} \in K$.

~~To prove~~ Consider $\phi^{-1}(K)$.

Let $h \in \phi^{-1}(K)$ and let $a \in G_1$

i.e., $\phi(h) \in K$, $\phi(a) \in G_2$.

So $\phi(aha^{-1}) = \phi(a)\phi(h)\phi(a)^{-1} \in K$

$\phi(aha^{-1}) \in K \quad \because K$ is normal

$\therefore aha^{-1} \in \phi^{-1}(K)$

Factor Group ✓ → subgroup in G_2

Theorem 10.3 If $\phi : G_1 \to G_2$, then the map $\Phi : G_1/Ker(\phi) \to \phi(G_1)$ defined by $\Phi(gKer(\phi)) = \phi(g)$ is an isomorphsim from $G_1/Ker(\phi)$ to $\phi(G_1)$.

Proof. Let $K = Ker(\phi)$.

(1) Φ is well-defined because $\Phi(aK) = \Phi(bK)$ implies ...

(2) Φ is 1-1 because ...

(3) Φ is onto because ...

(4) $\Phi(aKbK) = ... = \phi(aK)\phi(bK)$.

Let $K = Ker(\phi)$

(1) Suppose $aK = bK$. Then $a^{-1}b \in K$.

Thus $e_2 = \phi(a^{-1}b) = \phi(a)^{-1}\phi(b)$ Thus $\phi(a) = \phi(b)$

~~Need to show~~ ∴ $\Phi(aK) = \Phi(bK)$, ~~i.e., $\phi(a) = \phi(b)$~~

(2) Suppose $aK, bK \in G_1/K$. and $\phi(aK) = \phi(bK)$.

i.e., $\phi(a) = \phi(b)$ ∴ $e_2 = \phi(a)^{-1}\phi(b) = \phi(a^{-1}b)$

∴ $a^{-1}b \in K$.

∴ $aK = bK$.

---

(3) Φ is onto because for any $\phi(a) \in \phi(G_1)$

We have $aK \in G_1/K$ s.t. $\Phi(aK) = \phi(a)$

(4) Φ For any $aK, bK \in G_1/K$.

$\Phi(aK) * \Phi(bK) = \phi(a)\phi(b) = \phi(ab)$

$\Phi((aK)(bK)) = \Phi(abK) = \phi(ab)$

Chapter 11 Fundamental Theorem of Finitely Generated Abelian Group

Theorem 11.1 Every finitely generated Abelian group is isomorphic to a direct product of $\mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_k} \oplus \mathbf{Z}^\beta$, where $m_j = p_j^{n_j}$ for some prime number p_j and positive integer n_j for each j, and a nonnegative integer β known as the Betti number.

Corollary If G is a finite Abelian group, and m divides $|G|$, then G has a subgroup of order m. (But, there may not be an element of order m.)

Example: ① $\mathbb{Z}_n$ is "singly" generated

$\mathbb{Z}_n = \langle 1 \rangle$.

② $\mathbb{Z} = \langle 1 \rangle$

③ $\mathbb{Z}_m \oplus \mathbb{Z}_n = \langle (1,1) \rangle$ if $\gcd(m,n)=1$.

④ $\mathbb{Z}_m \oplus \mathbb{Z}_n = \langle \{(1,0), (0,1)\} \rangle$

$\gcd(m,n)=d>1$

$= \{ m_1(1,0) + m_2(0,1) : m_1 \in \mathbb{Z}_m, m_2 \in \mathbb{Z}_n \}$

$= \{ (r,s) : r \in \mathbb{Z}_m, s \in \mathbb{Z}_n \}$

⑤ ~~$(\mathbb{R}^n, +)$ is generated~~

$\underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$ under addition

is generated by $\{(1,0,\cdots,0),(0,1,0,\cdots,0),\cdots,(0,\cdots,0,1)\}$

or $\{(1,0,\cdots,0),(1,1,0,\cdots,0),\cdots,(1,1,\cdots,1)\}$

$\mathbb{Z} \oplus \mathbb{Z} = \langle \{(1,0),(1,1)\} \rangle$

$(3,4) = -(1,0) + \underbrace{(1,1) + \cdots + (1,1)}$

$(\mathbb{R},+)$ is not finitely generated.

Suppose

$\mathbb{R} = \langle \{r_1, \cdots, r_m\} \rangle$

$= \{ k_1 r_1 + k_2 r_2 + \cdots + k_m r_m : k_1, \cdots, k_m \in \mathbb{Z} \}$

$$\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{\beta}$$

$$= \{(1,0,\dots,0),(0,1,0,\dots,0)\ \dots\ (0,\dots,1)\}$$

<u>Example</u> 26 G is finitely generated abelian group.

with order ~~$16 \cdot 3^2$~~ $2^4, 3^2$

Then G is isomorphic to one of the following.

Case 1 $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

$\mathbb{Z}_2$

Case 2 $\mathbb{Z}_9$

$G \simeq H_1 \oplus H_2$

$H_1 = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_9$

$H_2 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

~~H_3~~ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$

or $\mathbb{Z}_8 \oplus \mathbb{Z}_2$

or $\mathbb{Z}_{16}$

In each case, $\exists$

$H \leq G$

$|H| = 2^2 \cdot 3$