19/09

Proof of (ii)

$$\{H \leq G \mid K \leq H\} \xrightarrow{\tilde{\phi}} \{H' \leq G'\} \xrightarrow{\tilde{\psi}} \{H \leq G \mid K \subseteq H\} \xrightarrow{\tilde{\phi}} \{H' \leq G'\}$$

$$\tilde{\phi} : H \longrightarrow \phi(H)$$

$$\tilde{\psi} : H' \longrightarrow \phi^{-1}(H')$$

$$\tilde{\psi} \circ \tilde{\phi}(H) = \tilde{\psi}(\phi(H))$$

$$= \phi^{-1}(\phi(H)) = H \quad \text{[Exercise]}$$

$$\tilde{\phi} \circ \tilde{\psi}(H') = \tilde{\phi}(\phi^{-1}(H'))$$

$$= \phi(\phi^{-1}(H'))$$

$$= H' \quad (\text{since } \phi \text{ is onto})$$

Take $H \trianglelefteq G$

Using the bijection proved above, there exists $H' \leq G'$ s.t. $\phi^{-1}(H') = H$ and

$H' = \phi(H)$

Now $H = \phi^{-1}(H') \trianglelefteq G$

By part-(d) : $H' = \phi(H) \trianglelefteq G$

Conversely, if $\phi(H) \trianglelefteq G'$, then $H = \phi^{-1}(\phi(H)) \trianglelefteq G$ by part-(c).

Products of groups

Let $G_1, G_2, \dots, G_n$ be groups

Define $G = G_1 \times G_2 \times \dots \times G_n$

$= \{(g_1, \dots, g_n) \mid g_1 \in G_1, \dots, g_n \in G_n\}$

Define a binary operation on G as

$(g_1, g_2, \dots, g_n) \cdot (g_1', g_2', \dots, g_n')$

$= (g_1 g_1', g_2 g_2', \dots, g_n g_n')$

Closure: Trivial from group property of multiplication

Associativity:

$((g_1, g_2 \dots, g_n) \circ (g_1', g_2', \dots, g_n')) \circ (g_1'', \dots g_n'')$

$= (g_1 g_1', \dots, g_n g_n') \circ (g_1'', \dots, g_n'')$

$= (g_1 g_1' g_1'', \dots, g_n g_n' g_n'')$

$(g_1, g_2, \dots, g_n) \circ ((g_1', g_2', \dots, g_n') \circ (g_1'', \dots, g_n''))$

$= (g_1, g_2 \dots, g_n) \circ (g_1' g_1'', \dots, g_n' g_n'')$

$= (g_1 g_1' g_1'', \dots, g_n g_n' g_n'')$

Identity

$1_G = (1_{G_1}, 1_{G_2}, \dots, 1_{G_n})$

$(g_1, g_2, \dots, g_n)(1_{G_1}, \dots, 1_{G_n}) = (g_1, g_2, \dots, g_n)$

$(1_{G_1}, \dots, 1_{G_n})(g_1, g_2, \dots, g_n) = (g_1, g_2, \dots, g_n)$

Inverse

$(g_1, g_2, \dots, g_n) \circ (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}) = 1_G$

G is a group of order $\prod_{i=1}^{n} |G_i|$

Examples

Let C_m denote the cyclic group of order m for any $m \geq 1$.

$C_2 \times C_3$ is a cyclic group of order 6

Let $C_2 = \langle x \rangle$
$C_3 = \langle y \rangle$

Let $(x^t, y^t) = (1, 1)$

$\Rightarrow x^t = 1 , y^t = 1$

$\Rightarrow t | 2 , t | 3$

$\Rightarrow 6 | t$

$(x, y)^6 = (x^6 y^6) = 1$

$\Rightarrow o(x, y) \leq 6$

$\Rightarrow o(x, y) = 6$

Proposition

$C_m \times C_n$ is a cyclic group of order $mn \iff \gcd(m, n) = 1$

Suppose $\gcd(m, n) = 1$
and $C_m = \langle x \rangle$, $C_n = \langle y \rangle$

Then $o(x, y) = m \cdot n$

Hence $C_m \times C_n$ is a cyclic group of order mn

Suppose $\gcd(m, n) = d > 1$
$C_m = \langle x \rangle$, $C_n = \langle y \rangle$

$o(x^{m/d}, 1) = d$
and $o(1, y^{n/d}) = d$

$C_m \times C_n$ has atleast two cyclic subgroups of order d.

Hence $C_m \times C_n$ is not cyclic $(\Rightarrow \Leftarrow)$

$\Rightarrow \gcd(m, n) = 1$

Examples

Let $G_1, G_2, \ldots, G_n$ be groups and

$G = G_1 \times G_2 \times \cdots \times G_n$

Then $o(g_1, \ldots, g_n) = \text{lcm}(o(g_1), \ldots, o(g_n))$

Proof

Denote $s = o(g_1, \ldots, g_n)$

$o(g_i) = r_i \quad \forall\, i = 1 \text{ to } n$

$r = \text{lcm}(o(g_1), \ldots, o(g_n))$

$$(g_1, \ldots, g_n)^r = (g_1^r, \ldots, g_n^r)$$
$$= 1$$

$\Rightarrow s \leq r$

$$(g_1, \ldots, g_n)^s = 1$$

$\Rightarrow o(g_i) \mid g_i \Rightarrow r_i \mid s \quad \forall\, i = 1 \text{ to } n$

$\Rightarrow \text{lcm}(r_i) \mid s$

$\Rightarrow r \mid s$

$\Rightarrow r = s = \text{lcm}(o(g_1), \ldots, o(g_n))$

Exercise!!

Let $C_{m_1}, \ldots, C_{m_n}$ be cyclic groups of orders $m_1, m_2, \ldots, m_n$ respectively. Then $C_{m_1} \times C_{m_2} \times \cdots \times C_{m_n}$ is a cyclic group $\Leftrightarrow \gcd(m_i, m_j) = 1 \ \forall\, i, j$

Let $H, K \leq G$. We define HK as

$HK = \{hk \mid h \in H, k \in K\}$

(Proposition) $\quad |HK| = \dfrac{|H|\,|K|}{|H \cap K|}$

(Proof) We define a map $\phi : H \times K \to G$
$(h, k) \mapsto hk$

$Im\ \phi = HK$

$\varphi : H \times K \to HK$

$$H \times K = \bigsqcup_{x \in HK} \varphi^{-1}(x)$$

Note that $|H \times K| = \sum_{x \in HK} |\varphi^{-1}(x)|$

claim :- $|\varphi^{-1}(x)| = |H \cap K|$

In particular, we prove that for $x \in HK$

$$\varphi^{-1}(x) = \{ (hd, d^{-1}k) \mid d \in H \cap K \}$$

$$|\varphi^{-1}(hK)| = |H \cap K|$$

($\Rightarrow$) Now, $\varphi(hd, d^{-1}k) = hk$

$\Rightarrow (hd, d^{-1}k) \in \varphi^{-1}(hk)$

($\Leftarrow$)

suppose $(h', k') \in \varphi^{-1}(hk)$

$\Rightarrow \varphi(h'k') = hk = h'k'$

$h^{-1}h' = k(k')^{-1} = d$ (say)

$d \in H$ and $d \in K$

$\Rightarrow d \in H \cap K$

$h' = hd$, $k' = d^{-1}k$

$\Rightarrow \varphi^{-1}(hk) \in (hd, d^{-1}k)$

$|H \times K| = |HK|\ |H \cap K|$

$$\Rightarrow |HK| = \frac{|H \times K|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|}$$

Theorem

Let $H, K \leq G$ and $\phi : H \times K \to G$ given by

$(h, k) \longmapsto hk$ $\qquad (\operatorname{Im}\phi = HK)$

Then

(a) ϕ is injective $\iff$ $H \cap K = \{1\}$

(b) ϕ is a homomorphism $\iff$ $hk = kh$ $\quad \forall h \in H$ and $k \in K$

(c) $H \trianglelefteq G \implies HK \leq G$

(d) ϕ is an isomorphism $\iff$ (i) $H, K \trianglelefteq G$
(ii) $H \cap K = \{1\}$
(iii) $G = HK$

$G_1 \times G_1 \to$ External product
$HK \to$ Internal product

(Proof)

(a) Suppose ϕ is injective

$$|HK| = \frac{|H||K|}{|H \cap K|} \quad \iff \quad |H \cap K| = 1$$

because $|H \times K| = |H||K|$
$= |HK|$
~~bijection~~
injection

$\implies H \cap K = \{1\}$

(b) $\phi((b, k)(h, a)) = \phi(b, k)\,\phi(h, a)$

$\forall\, b, h \in H$ and $k, a \in K$

$= \phi(bh, ka) \qquad = (bk)(ha)$

$= bhka$

$\implies hk = kh$

Converse is just backtracking

(c) Non-empty $\to \{1\} \in HK$

~~(h,k)~~ Let $hk,\ h'k' \in HK$

$hkh'k' = h\,h''\,k\,k' = h^{\circ}k^{\circ} \in HK$

★ $kH = Hk$

for $h' \in H$ $\ \exists\, h'' \in H$ s.t $kh' = h''k$