Every Group is isomorphic to a group of permutations

Ex| $\mathbb{Z}_3 \cong G = \{(0), (012), (021)\}$ (012 → 1, 021 → 2)

$(012)(012) = (021)$

$\mathbb{Z}_3$

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

G

	(0)	(012)	(021)
(0)	(0)	(012)	(021)
(012)	(012)	(021)	(0)
(021)	(021)	(0)	(012)

Thm (Cayley's) | Every group is isomorphic to a group of permutations.

Proof:

Let G be a group, we want to construct a group of permutations, $\tilde{G}$ s.t. $G \cong \tilde{G}$.

For any $g \in G$:

$$\lambda_g : G \to G$$
$$a \mapsto ga$$

Claim: $\hat{G} = \{\lambda_g \mid g \in G\}$ forms a group of permutations (of G as a set)

Show λ_g is bijective $\forall g \in G$

1-1: $\lambda_g(a) = \lambda_g(b) \Rightarrow ga = gb \Rightarrow a = b$ ✓

onto: For $a \in G$ $\exists\ b = g^{-1}a$ s.t $a = \lambda_g(b) = g \cdot (g^{-1}a) = a$ ✓

$\therefore \tilde{G} = \{ \lambda_g \mid g \in G \}$ is a set of permutation maps $G \to G$.

Show $\tilde{G}$ is a group

- Check closure under composition (for $a \in G$)

$$\lambda_g \circ \lambda_h(a) = \lambda_g(\lambda_h(a)) = \lambda_g(ha) = gha = \lambda_{gh}(a)$$

$$\therefore \quad \lambda_g \circ \lambda_h = \lambda_{gh} \in \tilde{G} \quad \checkmark$$

- identity (e = identity of G)

$$\lambda_e(a) = ea = a$$

$\uparrow$ $\therefore$ this is identity permutation $G \to G$

$\cup$

- inverses: $(\lambda_g)^{-1} = \lambda_{g^{-1}}$ since

$$\lambda_{g^{-1}} \circ \lambda_g(a) = \lambda_{g^{-1}}(ga) = g^{-1}ga = a = gg^{-1}a$$
$$= \lambda_g \circ \lambda_{g^{-1}}(a)$$
$$= \lambda_e(a)$$

$$\lambda_{g^{-1}} \circ \lambda_g = \lambda_g \circ \lambda_{g^{-1}} = \lambda_e \quad \therefore (\lambda_g)^{-1} = \lambda_{g^{-1}} \quad \cup$$

$\therefore$ $\tilde{G}$ is a group of permutations.

Define an isomorphism

$$\phi : G \longrightarrow \tilde{G}$$
$$g \mapsto \lambda_g$$

Show ϕ is an isomorphism $g, h \in G$

$$\phi(gh) = \lambda_{gh} = \lambda_g \circ \lambda_h = \phi(g) \circ \phi(h)$$

☺

- ϕ is 1-1 if $\phi(g)(a) = \phi(h)(a) \quad \forall a \in G$

$$\lambda_g(a) = \lambda_h(a)$$
$$ga = ha$$
$$g = h \quad \therefore \text{ 1-1} \quad ☺$$

- ϕ is onto : For any $\lambda_g \in \widehat{G}$

$$\phi(g) = \lambda_g \quad ☺$$

∎

Direct products

- Given groups G, H we construct a group from $G \times H$ ↑ Cartesian product

External Direct product

Def $(G, \cdot), (H, \circ)$ groups define

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$ with binary operation

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$$

Prop. $G \times H$ is a group with ↑ operation.

Proof: • closed since G, H closed

- (e_G, e_H) is identity in $G \times H$
- $(g,h)^{-1} = (g^{-1}, h^{-1})$ in $G \times H$

$$(g^{-1}, h^{-1})(g,h) = (g^{-1}g, h^{-1}h) = (e_G, e_H)$$
$$= (g,h)(g^{-1}, h^{-1})$$

- Op. is associative since it is associative in each component.

∎

Ex) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

$|\mathbb{Z}_2 \times \mathbb{Z}_2| = |\mathbb{Z}_4| = 4$ but $\mathbb{Z}_2 \times \mathbb{Z}_2 \neq \mathbb{Z}_4$

Since $|(a,b)| \leq 2 \quad \forall (a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ $\therefore$ $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic

$\therefore$ not isomorphic to $\mathbb{Z}_4$ which is cyclic.

$$\prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n \quad \text{(for groups } G_1, \ldots, G_n\text{)}$$

If $G_1 = \cdots = G_n$, then write G^n where $G = G_i$

i.e $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ times}}$

Thm) Take $(g,h) \in G \times H$. If $|g| = r < \infty$, $|h| = s < \infty$

then $|(g,h)| = \operatorname{lcm}(r,s)$.

Proof: Let $m = \operatorname{lcm}(r,s)$, $n = |(g,h)|$

$(g,h)^m = (g^m, h^m) = (e_G, e_H)$

$(g,h)^n = (g^n, h^n) = (e_G, e_H)$ — could have $m > n$; show $m = n$

$\therefore |g| \mid n \;,\quad |h| \mid n$

$\Rightarrow \quad r \mid n \;,\quad s \mid n$

$\Rightarrow$ n is a common multiple of r and s

but $\quad m = \operatorname{lcm}(r,s) \quad m \le n$

but n is the least positive integer s.t. $(g,h)^n = (e_G, e_H)$

$n \le m$

$\Rightarrow \quad m = n. \quad \therefore |(g,h)| = \operatorname{lcm}(r,s)$

∎

Cor Let $(g_1, \dots, g_n) \in \prod_{i=1}^{n} G_i$ and if $|g_i| = r_i < \infty$ in G_i

then $|(g_1, \dots, g_n)| = \operatorname{lcm}(r_1, \dots, r_n|$ in $\prod_{i=1}^{n} G_i$.

Ex $(8, 56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$

$|(8,56)| = \operatorname{lcm}(|8|, |56|) = \operatorname{lcm}(3, 15) = 15.$

$|8| = 3 \;,\quad |56| = \dfrac{60}{\gcd(56, 60)} = 15$

Ex $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \langle (1,1) \rangle \simeq \mathbb{Z}_6$

|

$= \{(1,1), (0,2), (1,0), (0,1), (1,2), (0,0)\}$

Thm The group $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m,n) = 1$.

$\Leftrightarrow$ $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic

Proof: Show $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Rightarrow \gcd(m,n) = 1$

Show contrapositive: If $\gcd(m,n) = d > 1 \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is <u>not</u> cyclic.

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

$\Rightarrow$ $m \mid \frac{mn}{d}$, $n \mid \frac{mn}{d}$

since $d \mid m$, $d \mid n$

Let $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$

$\therefore$

$$\underbrace{(a,b) + \cdots + (a,b)}_{\frac{mn}{d}} = (0,0)$$

Since $\frac{nm}{d} \cdot a = \left(\frac{n}{d}\right) ma = 0 \bmod m$

and $\frac{nm}{d} \cdot b = \frac{m}{d} na = 0 \bmod n$,

but $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn > \frac{mn}{d}$ $\therefore$ $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Now other direction

If $\gcd(m,n) = 1$ then $|(1,1)| = \operatorname{lcm}(\underset{\in \mathbb{Z}_m}{|1|}, \underset{\in \mathbb{Z}_n}{|1|})$

$= \operatorname{lcm}(m,n) = mn$

$\therefore$ $\mathbb{Z}_m \times \mathbb{Z}_n \cong \langle (1,1) \rangle$ is cyclic $\therefore \cong \mathbb{Z}_{mn}$.

$\langle a \rangle = \{a, a^2, \dots, a^n\}$ ($a^n = e$) : if $|G| = n$, $a \in G$

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

Corollary

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\gcd(n_i, n_j) = 1 \quad \forall i \neq j$.

Proof: by Theorem above.

Cor If $m = p_1^{d_1} \cdots p_k^{d_k}$, p_i's are distinct primes

then $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{d_1}} \times \cdots \times \mathbb{Z}_{p_k^{d_k}}$

Proof: $\gcd(p_i^{d_i}, p_j^{d_j}) = 1 \quad \forall i \neq j$

Internal Direct product

- Break down a given group into the direct product of smaller groups.

Def Let G be a group, with subgroups H, K s.t.

- $G = HK = \{hk \mid h \in H, k \in K\}$
- $H \cap K = \{e\}$
- $hk = kh \quad \forall k \in K, h \in H$

G is the internal direct product of H and K

Ex $U(8) = \{1, 3, 5, 7\}$ is internal direct product

of $H = \{1, 3\}$, $K = \{1, 5\}$