Corr If $|G| = p$ where p is prime then $G \cong \mathbb{Z}_p$

Proof: Cor. 6.12 says if $|G| = p \Rightarrow G$ cyclic. ∎

Thm The isomorphism of groups determines an equivlance relation on the class of all groups.

Proof: Homework.

Ex

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

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

$\mathbb{Z}_3$

	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)

Theorem (Cayley's) : Every group is isomorphic to a group of permutations.

Proof:

Let G be a group, we construct a group $\hat{G}$ of permutations s.t. $G \cong \hat{G}$. For any $g \in G$ define

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

λ_g is a permutation of G since:

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

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

$$\lambda_g(b) = gg^{-1}a = a \quad .$$

$\hat{G} = \{ \lambda_g \mid g \in G \}$ ← This is a set of permutation maps $G \to G$, show $\hat{G}$ is a group (with operation of composition)

- Closure under composition:

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

- identity

$$\lambda_e(a) = ea = a \qquad (e \in G \text{ identity})$$

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

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

$$\therefore \lambda_{g^{-1}} \circ \lambda_g = \lambda_e$$

$\therefore$ $\hat{G}$ is a group of permutations

Define an isomorphism:

$$\lambda_g : G \to G$$
$\uparrow$ permutation

$$\phi : G \to \bar{G}$$
$$g \mapsto \lambda_g$$

- Group op. preserved $(g, h \in G)$

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

- 1-1 If $\phi(g)(a) = \phi(h)(a) \quad \forall a \in G$

$$\Rightarrow \quad \lambda_g(a) = \lambda_h(a)$$
$$ga = ha$$
$$\Rightarrow \quad g = h$$

- onto For any $\lambda_g \in \bar{G}$ $\quad \phi(g) = \lambda_g$.

$\blacksquare$

Direct Products

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

$\uparrow$ cartesian product.

External Direct Product

<u>Def</u> $(G, \cdot)$, $(H, \circ)$ groups define

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

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

Proposition $G \times H$ 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 $G \times H$

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

- 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 $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$ 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.

$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$, if $G_1 = \cdots = G_n$ Then write G^n where $G = G_i \ \forall i$

Theorem Take $(g,h) \in G \times H$. If $|g| = r < \infty$, $|h| = s < \infty$ then $|(g,h)| = \operatorname{lcm}(r,s)$.

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

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

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

Then $|g| \mid n$ and $|h| \mid n \Rightarrow r \mid n, s \mid n$

Since $|(g,h)| = n \Rightarrow n$ is the least integer s.t. $(g,h)^n = (e_G, e_H)$

$n \leq m$ and $n \mid m$

But $r \mid n, s \mid n \Rightarrow n$ is a common mult. of r and s

$m \leq n$ since $m = \text{lcm}(r,s)$

$\Rightarrow m = n$. $\blacksquare$