Classification results

Theorem: Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

$(\mathbb{Z},+)$ is infinite cyclic

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

Suppose G is infinite and cyclic. Then there is an isomorphism $f: \mathbb{Z} \to G$.

<u>Proof</u>: G cyclic $\Rightarrow \exists g \in G$ so that $G = \{g^n : n \in \mathbb{Z}\}$ and all <u>g^n are distinct.</u>

$$f: \mathbb{Z} \longrightarrow G$$

$$f(n) = g^n \in G.$$

$$f(n_1+n_2) = g^{n_1+n_2} = g^{n_1} g^{n_2} = f(n_1) f(n_2)$$

f is surjective because every $g_1 \in G$ is $=$ to $g_1 = g^m$ so $f(m) = g_1$.

f injective: $f(n_1) = f(n_2) \Rightarrow f(n_1) f(n_2)^{-1} = e$.

$f(n_2) = g^{n_2}$

$f(-n_2) = (g^{-n_2}) = (g^{n_2})^{-1}$

$\Rightarrow f(n_1) f(-n_2) = e$

$= f(n_1 - n_2) = e$

$g^{n_1-n_2} = e$

$\Rightarrow n_1 - n_2 = 0$

otherwise g would have finite order.

Theorem: Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

G finite cyclic of order n.

Find $f: \mathbb{Z}_n \to G$ which is an isomorphism.

$G = \langle g \rangle$. g a generator $\Leftrightarrow$ $g^n = e$, no smaller of g is the identity

$f(a) = g^a$ $\quad a \in \mathbb{Z}_n$.

$[a+kn] = [a]$

$f(a+kn) = g^{a+kn} = g^a (g^n)^k = g^a$

~~Suppose~~

~~Suppose we~~ Show surjective.

$g_1 \in G \Rightarrow g_1 = g^i$ for some i, $0 \le i < n$

$f(i) = g^i$ $\quad [i] \in \mathbb{Z}_n$.

Injective:

Suppose: $f(i) = f(j) \Rightarrow g^i = g^j \Rightarrow g^{i-j} = e$

$\Leftrightarrow n \mid (i-j)$

$\Downarrow$ $\quad \Leftrightarrow i \equiv j \bmod n$

$[i] = [j]$. $\quad [i] = [j]$ in $\mathbb{Z}_n$

$f(i+j) = g^{i+j} = g^i g^j = f(i) f(j)$.

$U(7)$ cyclic order 6 generated by 3 $\simeq \mathbb{Z}_6$

Theorem: If p is prime, any group of order p is isomorphic to $\mathbb{Z}_p$.

Proof: Suppose G has p elements. p prime.

Take $g \in G$, $g \neq e$.

$\text{order}(g) \mid |G| \Rightarrow \text{order}(g) = p$.

$G = \{1, g, g^2, \ldots, g^{p-1}\}$

G cyclic with p elements, G is isomorphic to $\mathbb{Z}_p$.

Theorem: (Cayley's Theorem) Any group G is isomorphic to a permutation group. If G is finite, it is isomorphic to a subgroup of S_n for some n.

Permutation group is a group whose elements are bijective maps $f : X \to X$ and operation is composition of functions.

Symmetries of a triangle

$\circ$	id (1)	ρ_1 (2)	ρ_2 (3)	μ_1 (4)	μ_2 (5)	μ_3 (6)
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

$$\rho_1 \leftrightarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{matrix} = (132)(456)$$

$$\mu_1 = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{matrix} = (14)(25)(36)$$

$\lambda_{\rho_1}(e) = \rho_1$

$\lambda_{\rho_1}(\rho_1) = \rho_2$ $\lambda_{\rho_1}(\rho_2) = \rho_1\rho_2 = id$

$\lambda_{\rho_1}(\mu_1) = \rho_1\mu_1 = \mu_3$ $\lambda_{\rho_1}(\mu_3) = \mu_2$

$\lambda_{\rho_1}(\mu_2) = \rho_1\mu_2 = \mu_1$

G group

Make G into a group of permutations.

Let $X = G$ (as a set).

Make a $f: X \to X$ for each $g \in G$.

Define $\lambda_g : X \to X$

$$\lambda_g(x) = gx$$

$g \longrightarrow \lambda_g$ is an isomorphism.

λ_g and $\lambda_{g'}$ are different if $g \neq g'$.

Suppose $\lambda_g = \lambda_{g'}$. Then $\underset{\substack{\shortparallel \\ g = ge}}{\lambda_g(e)} = \underset{\substack{\shortparallel \\ g'e = g'}}{\lambda_{g'}(e)}$

so $g = g'$.

$$\lambda_{g_1 g_2} = \lambda_{g_1} \circ \lambda_{g_2}$$

$$\lambda_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = g_1 \lambda_{g_2}(x)$$

$$= \lambda_{g_1}(\lambda_{g_2}(x))$$

$$= (\lambda_{g_1} \circ \lambda_{g_2})(x).$$

$\mathbb{Z}_4$ $\qquad \lambda_g : \{0,1,2,3\} \circlearrowleft \qquad X = \mathbb{Z}_4$

λ_0

λ_1

λ_2

λ_3

$$\lambda_0 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix} \qquad e$$

$$\lambda_1 = \begin{array}{cl} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix} & \begin{array}{l} \leftarrow x \\ \leftarrow \lambda_1(x) \end{array} \end{array} \qquad (0123)$$

$$\lambda_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix} \qquad (02)(13)$$

$$\lambda_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix} = (0321)$$

$\lambda_2 \stackrel{?}{=} \lambda_1 \circ \lambda_1$ $\quad (0\,1\,2\,3)(0\,1\,2\,3) = (0\,2)(1\,3) = \lambda_2$

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

(columns numbered 1 2 3 4 5 6)

id $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

ρ_1 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$

ρ_2 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix}$

$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$

$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 1 & 2 \end{pmatrix}$

$\mu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}$

id

$\rho_1 = (1\,2\,3)(4\,6\,5)$

$\rho_2 = (1\,3\,2)(4\,5\,6)$

$\left.\begin{array}{l} \mu_1 = (1\,4)(2\,5)(3\,6) \\ \mu_2 = (1\,5)(2\,6)(3\,4) \\ \mu_3 = (1\,6)(2\,4)(3\,5) \end{array}\right\}$

$\mu_1\mu_2 = (1\,4)(2\,5)(3\,6)(1\,5)(2\,6)(3\,4) = \rho_1$

$= \cancel{(3\,4)}\ (3\,1\,2)(4\,6\,5)$

$= (1\,2\,3)(4\,6\,5)$