Lecture - 10/1 4/10/05

Monoid homomorphism: M, N monoids

$$M \xrightarrow{f} N \begin{cases} f(e_M) = e_N \\ f(x, y) = f(x) \cdot f(y) \quad \forall\, x, y \in M. \end{cases}$$

A Monoid homomorphism which is bijective is called monoid isomorphism.

The following properties of monoid homomorphism can be proved:

1. $f(x_1, x_2 \ldots x_n) = f(x_1)\, f(x_2) \ldots f(x_n)$
2. $f(x^n) = (f(x))^n \quad n \in \mathbb{N}.$
3. $x \in M^\times \implies f(x) \in N^\times$ and $f(x^{-1}) = f(x)^{-1}$

$$f(x^n) = f(x)^n \quad \forall\, n \in \mathbb{Z}$$

Composition of a monoid homomorphism is also a homomorphism.

$$g \cdot f : M \xrightarrow{f} N \xrightarrow{g} L$$

$f^\times : M^\times \longrightarrow N^\times$ is a group homomorphism because $M^\times, N^\times$ are groups.

$\mathrm{Hom}(M, N)$ = set of all monoid homomorphisms from M to $N \subseteq N^M$

$\mathrm{End}(M, M)$ = set of all monoid homomorphisms from M to $M \subseteq M^M$ (Endomorphism)

$(\mathrm{End}(M), \circ)$ is a submonoid of M^M

$\mathrm{Aut}(M)$ = set of all isomorphism from M to M
$\subseteq \mathrm{End}(M)$

In fact, $\mathrm{End}(M)^\times = \mathrm{Aut}(M)$

Given any monoid M which is bijective to a set X through a map f.

$$f : M \longrightarrow X \quad \text{bijective}$$

$\cancel{f^{-1}(x)}$

For any $x, y \in X$, $f^{-1}(x), f^{-1}(y) \in M$.

Define the binary operation in X as

$$x \cdot y = f(f^{-1}(x)\, f^{-1}(y))$$

For example: $(\mathbb{R}, +) \longrightarrow (0,1)$

Example: $\mathbb{P}$ = the set of all prime numbers

$$\mathbb{N}^* \longrightarrow \mathbb{N}^{(\mathbb{P})}$$

(p tuples with only finitely many elements are not zero)

$(n_p)_{p \in \mathbb{P}}$, $n_p = 0$ for almost all $p \in \mathbb{P}$.

Define a map ϕ as

$$(\mathbb{N}^*, \circ) \xrightarrow{\phi} (\mathbb{N}^{(\mathbb{P})}, +)$$

$$n = \prod_{p\in\mathbb{P}} p^{v_p(n)} \xrightarrow{\phi} \left(v_p(n)\right)_{p\in\mathbb{P}}$$

$$\begin{aligned}\phi(m\cdot n) &= \phi(n) + \phi(m) = \left(v_p(n)\right)_{p\in\mathbb{P}} + \left(v_p(m)\right)_{p\in\mathbb{P}} \\ &= \left(v_p(n) + v_p(m)\right)_{p\in\mathbb{P}} \\ &= \left(v_p(mn)\right)_{p\in\mathbb{P}}\end{aligned}$$

Also note that ϕ is invertible.

$$\prod_{p\in\mathbb{P}} p^{\alpha_p} \xleftarrow{\phi^{-1}} (\alpha_p)_{p\in\mathbb{P}} \implies \phi \text{ is automorphism}$$

For any monoid factorial $M \underset{\text{bijective}}{\cong} M^\times \times (\mathbb{N}^{(I)}, +)$ for some I.

$$\varepsilon(x) \prod_{p\in\mathbb{P}} p^{v_p(x)} = x \longmapsto \left(\varepsilon(x), v_p(x)\right)$$

Also there is monoid automorphism between

$$(\mathbb{Z}^*, \cdot) \longrightarrow \underbrace{(\mathbb{Z}^\times, \cdot)}_{(\{\pm 1\}, \cdot)} \times (\mathbb{N}^{(\mathbb{P})}, +)$$

$$z = \varepsilon(z) \prod_{p\in\mathbb{P}} p^{v_p(z)} \longrightarrow \left(\varepsilon(z), v_p(z)\right)_{p\in\mathbb{P}}$$

isomorphism

Monoid automorphism between

$$(\mathbb{Z}^\times \times \mathbb{Z}^{(\mathbb{P})}) \longrightarrow (\mathbb{Q}^*, \cdot)$$

Note $x \in \mathbb{Q}$, then

$$x = \frac{a}{b} = \frac{\varepsilon(a) \prod_{p\in\mathbb{P}} p^{v_p(a)}}{\varepsilon(b) \prod_{p\in\mathbb{P}} p^{v_p(b)}}$$

$$\left(\varepsilon(x), \left(v_p(x)\right)_{p\in\mathbb{P}}\right) \longrightarrow \varepsilon(x) \prod_{p\in\mathbb{P}} p^{v_p(x)}$$

$v_p(x) \in \mathbb{Z}$

Another example:

X any set $\quad (P(X), \cup) \longrightarrow (P(X), \cap)$

$$A \longrightarrow (X - A)$$

$\hookrightarrow$ monoid automorphism.

$(\mathbb{R}, +) \longrightarrow (\mathbb{R}^*_+, \cdot)$ monoid

Let $a \in \mathbb{R}$, $a > 0$, $a \neq 1$, then

$$\left.\begin{array}{l} x \longrightarrow a^x \\ \log_a y \longleftarrow y \end{array}\right\} \text{monoid automorphism}$$

Another example: $\quad ((\mathrm{End}(\mathbb{N}), +), \circ) \cong (\mathbb{N}, +)$

$$\phi \longrightarrow \phi(1)$$

$$(\mathrm{Aut}(\mathrm{Id}_{\mathbb{N}}, +), \circ) \cong \{1\}$$

More isomorphism examples:

$((\mathrm{End}(\mathbb{N})^*, \cdot), \circ) \xrightarrow{\cong} (\mathbb{N}^{\mathbb{P}}, \circ)$

$((\mathrm{Aut}(\mathbb{N}^*), \cdot), \circ) \xrightarrow{\cong} \cancel{(\mathbb{N}^{\mathbb{P}}, \circ)}\ S(\mathbb{P})$ $\hookrightarrow$ Permutation on $\mathbb{P}$.

$$\phi \longrightarrow \phi|\mathbb{P}.$$

$$\phi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$$

Category: $\mathcal{C}$ Consits of data

(a) objects $obj(\mathcal{C})$ objects need not be sets

(b) $X, Y \in obj(\mathcal{C})$ there is a set $Hom_{\mathcal{C}}(X,Y)$

Its elements are called <u>morphisms</u> in $\mathcal{C}$.

(c) $X, Y, Z \in obj(\mathcal{C})$, there is a map

$$Hom_{\mathcal{C}}(X,Y) * Hom_{\mathcal{C}}(Y,Z) \longrightarrow Hom_{\mathcal{C}}(X,Z)$$

$$(\phi, \psi) \longmapsto \psi \circ \phi$$

which satisfies

A. $\forall\ X \in obj(\mathcal{C}) \quad \exists\ id_X \in Hom_{\mathcal{C}}(X,X)$

$$id_X \circ \phi = \phi, \quad \phi \circ id_X = \phi$$

B. Operation in $(\mathcal{C})$ is associative

$\hookrightarrow$ Composition

Examples: (1) Category of sets: objects are sets
(2) Category of monoids: objects are monoids

$Hom_{\mathcal{C}}(X,Y)$: set of monoid homomorphisms.