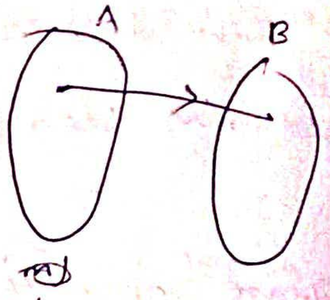
Math foundation

$A \times B = \{(a, b) : a \in A, b \in B\}$.

$f : A \to B$



Binary relation. $\rho \subseteq A \times A$

Binary operation : $* \; A \times A \to A$

$|A| = m$

$|B| = n$

$\therefore$ no of mapping $= n^m$

$|P(A)| = 2^n$

$|P(A \times A)| = 2^{n^2}$

$\phi + {}^nC_0 + {}^nC_1 + {}^nC_2 + \cdots + {}^nC_n = 2^n$.

$\therefore$ No of binary relation $= 2^{n^2}$.

$\therefore$ No of binary operation $= n^{n^2}$

$|A \times A| = n^2$

$|A| = n$.

$S \neq \phi$ $(S, *) \to$ groupoid

$* : S \times S \to S$.

Semigroup

$(S, *) \to$ Semigroup.

$(a * b) * c = a * (b * c) \;\forall\; a, b, c \in S$

$\to$ associative binary operation.

If binary operation is associative on nonempty set S, the $(S, *)$ is semigroup.

Monoid

$(S, *)$ $S \neq \phi$

$\exists e \in S$ s.t. $a * e = e * a = a$ $\forall e, a \in S$.

for $(\mathbb{Z}, +) \to 0$ is identity element

$(\mathbb{Z}, \cdot) \to 1$ " "

If there is an identity element and ~~the~~ it is a semigroup, it is a monoid.

$(\mathbb{Z}, +)$ ~~there~~ s.t. $a \in \mathbb{Z}, \exists (-a) \in \mathbb{Z}$

$a + (-a) = (-a) + a = 0$

$\{\mathbb{R} - \{0\}, \cdot\} \Rightarrow$ ~~is~~ also has such property.

Group

$G \neq \phi$. $* : G * G \longrightarrow G$

$(G, *)$ will be group if

1) $(a * b) * c = a * (b * c)$ $\forall a, b, c \in G$

2) for any $a \in G$, $\exists e \in G$ s.t $a * e = e * a$

3) for any $a \in G$, $\exists b \in G$ s.t $a * b = b * a = e$.

$\therefore b = a^{-1}$.

Example

$(\mathbb{R},+)$, $\{\{\mathbb{R}-0\},\cdot\}$ are groups. $\Big\}$ identity elem
$(\mathbb{Q},+)$, $(\mathbb{C},+)$ $\quad$ 0.

$(\mathbb{Q},\cdot)$ is not group.
$\{\{\mathbb{Q}-0\},\cdot\}$ is group.

$(\mathbb{C},\cdot)$ is not group
$(\mathbb{C}-\{0\},\cdot)$ is group.

Finite group

$S=\{1,-1,i,-i\}$

$(S,\cdot)$ is a group. 1 is identity element.

Order of group $= |G| = n$.

$a \equiv b \pmod{n}$

$\hookrightarrow$ $a-b$ is divisible by n.

Anti symmetric : $a \rho b, b \rho a \rightarrow a = b$.

Reflexive + Anti symmetric + transitive $\rightarrow$ Partially order Relation.

" + Symmetric + transitive $\rightarrow$ Equivalence relation.

$a \rho b \Leftrightarrow a - b$ is divisible by n is an equivalence relation. but not partially order.

$a \rho b \Leftrightarrow a = b$ is both partially order and equivalence relation.

Q.) ρ. $S \neq \emptyset$

$[a]_\rho = \{x \in S : a \rho x\} \rightarrow$ Equivalence class.

$[0] = \{nt : t \in \mathbb{Z}\}$

$[1] = \{nt + 1 : t \in \mathbb{Z}\}$

$\vdots$

$[n-1]$

$[n] = [0]$.

$[1] = [n+1]$

$\vdots$

etc.

\# $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$.

$[a] + [b] = [a+b] \ \forall [a], [b] \in \mathbb{Z}_n$] group.

$\mathbb{Z}_n$

$[a] . [b] = [a.b] \ \forall [a], [b] \in \mathbb{Z}_n$. does not form a group because every element does not have identity.

Commutative Group and Non commutative group.

abelian

non-abelian.

~~Non com~~

$(G, *)$

$a * b = b * a \;\; \forall\, a, b \in G. \longrightarrow$ Commutative group.

$(\mathbb{Z}, +)$, $\mathbb{R}$ is commutative.

Non commutative on Matrix

$GL(n.$

$GL_n(\mathbb{R}) := \{A \in M_{n \times n}(\mathbb{R}) : \det(A) \neq 0\}$

$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det(A) = 1\}.$

Permutation $(X \neq \emptyset)$

$f: X \longrightarrow X$. bijective mapping.

$X = \{1, 2, 3 \ldots, n\}$

$$\begin{pmatrix} 1, & 2, & 3 & \ldots, & n \\ 2, & 3 & \ldots & \ldots & 1 \end{pmatrix}$$

$G = \{f: X \longrightarrow X\} \longrightarrow$ Infinite non commutative group

$(f \circ g) \circ h = f \circ (g \circ h)$