Definition

Let G be a group and $x \in G$. The element x is said to be of finite order if there exists a positive integer n such that $x^n = e$

If x is of finite order, then the order of x denoted by $o(x)$ is given by

$$o(x) = \min \{ n \mid x^n = e \}$$

04/08

Definition

Let S be any non-empty set. A relation $\sim$ is a subset of $S \times S$.

$$\sim \subseteq \{ (a,b) \mid a \in S, b \in S \}$$

We write $a \sim b \iff (a,b) \in \sim$

- A relation is said to be reflexive if $a \sim a \ \forall a \in S$
- A relation is said to be symmetric if $a \sim b \Rightarrow b \sim a$ where $a, b \in S$
- A relation is said to be transitive if $(a,b) \in \sim$ and $(b,c) \in \sim \Rightarrow (a,c) \in \sim$

Notation $\rightarrow$ $\mathbb{R}^{\times} \rightarrow (\mathbb{R} \setminus \{0\}, \cdot)$

- If all three conditions are satisfied, it is an equivalence relation.

Examples

- Let $S = \mathbb{Z}$ and $a \sim b \iff a \equiv b \pmod{n}$

  $\sim$ is an equivalence relation.

- Let $S = \mathbb{Q}$. $a \sim b \iff a - b \in \mathbb{Z}$

  $\sim$ is an equivalence relation.

Definition

Let S be a set and $\sim$ be an equivalence relation on S.

For $x \in S$, we define the equivalence class of x, denoted by C_x as

$$C_x = \{ y \in S \mid x \sim y \}$$

Proposition

Let S be a non-empty set and $\sim$ be an equivalence relation on S. Then

$$C_x = C_y \quad \text{(or)} \quad C_x \cap C_y = \phi$$

Proof: Let $x, y \in S$ and suppose $C_x \cap C_y \neq \phi$

$\exists\ z \in S$ such that $z \in C_x \cap C_y$

Let $m \in C_x$ (arbitrary m)

$\Rightarrow x \sim m$

$\Rightarrow x \sim z$ $(z \in C_x \cap C_y)$

$\Rightarrow m \sim z$ (transitive)

We have $z \sim y$ $(z \in C_x \cap C_y)$

$\Rightarrow m \sim y$ (transitive)

$\Rightarrow m \in C_y$

$\Rightarrow C_x \subseteq C_y$

Similarly, let $m \in C_y$

$\Rightarrow m \sim y$

$\Rightarrow y \sim z$

$\Rightarrow m \sim z$

We have $z \sim x$

$\Rightarrow m \sim x$

$\Rightarrow m \in C_x$

$\Rightarrow C_y \subseteq C_x$

$\Rightarrow C_x = C_y$

So, either $C_x = C_y$, or our assumption is false

$\Rightarrow C_x \cap C_y = \phi$

- $\bigcup_{x \in S} C_x = S$

$c_i \in S \quad \forall i$

$\Rightarrow \bigcup_{i \in S} c_i \subseteq S$

Let $y \in S$

$y \in C_y$ (∵ reflexive)

$C_y \subseteq \bigcup_{i \in S} C_i$

- $\mathbb{C}^{\times}$ $\quad a \sim b \iff f(a) = f(b)$

$C_a = \{ y \in S \mid f(a) = f(y) \} = f^{-1}(t)$
$t \in f(S)$

Definition

Let $f : A \to B$ be a function. We define the fibres of f as $f^{-1}(t) = \{ a \in A \mid f(a) = t \}$

$| \; | : \mathbb{C}^{\times} \to \mathbb{R}$

$a \to |a|$

Definition

Let S be a set. A collection of subsets $\mathcal{F}$ is called a partition of S if

- $S = \bigcup_{c \in \mathcal{F}} c$
- For $A, B \in \mathcal{F}$, $A = B$ or $A \cap B = \emptyset$

More examples of groups

- Let $\sim$ be the relation on $\mathbb{Z}$ given by

  $a \sim b \iff a \equiv b \pmod{n}$

  Equivalence class c_i for this is denoted by $[i]$

- Define $\mathbb{Z}/n\mathbb{Z} = \{ [0], \ldots, [n-1] \}$ (or)
  $\{ [i] \mid i \in \mathbb{Z} \}$

- Define $+$ on $\mathbb{Z}/n\mathbb{Z}$: $[a] + [b] = [a+b]$

- If $[a] = [a']$ and $[b] = [b']$
  - $[a+b] = [a'+b']$ $\leftarrow$ closed
- If $[a] = [a'] \Rightarrow n \mid a - a'$

Associative : $[a]+([b]+[c]) = ([a]+[b])+[c]$

- $[a]+[0] = [a+0] = [a]$
  $[0]+[a] = [0+a] = [a]$ } Identity
- $[-a] = [n-a]$ $\leftarrow$ inverse of $[a]$

Group of units in $\mathbb{Z}/n\mathbb{Z}$

Define $U(n) = \{ [a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1 \}$

Define $\cdot$ on $U(n)$ as

$$[a][b] = [ab]$$

- If $[a] = [a']$ and $[b] = [b']$, then
  $[ab] = [a'b'] \Leftrightarrow n \mid ab - a'b'$

Add $a'b$ and subtract $a'b$

So, $\cdot$ is well-defined

- $([a][b])[c] = [a]([b][c])$ [Associative]
- Identity $\rightarrow [1]$
- Let $[a] \in U(n)$. Then $\gcd(a, n) = 1$

$\exists\, x, y \in \mathbb{Z}$ such that $ax + ny = 1$

$\Rightarrow ny = 1 - ax$

$\Rightarrow n \mid 1 - ax \Rightarrow [1] = [ax]$

$\Rightarrow [a]^{-1} = [x]$