Modern Algebra

content

1 Group Theory **2**

1.1 Semi-Group and Group 2

1.1.1 Difinition of Groop 2

1.1.2 Property of Group 3

1.2 Subgroup 3

1.3 Homomorphism and Isomorphism 4

1.4 Cyclic Group 4

1.4.1 Difinition and Property of Cyclic Group 4

1.4.2 Residue Class Group 5

1 Group Theory

1.1 Semi-Group and Group

1.1.1 Difinition of Groop

Suppose $\mathbb{S}\neq\emptyset$, difine an algebraic operation called mutiplication ,marked as $\cdot$, and this operation satisfies closure and associtive law , then $(\mathbb{S},\cdot)$ is a **semi-group**

Closure:

$$\forall a, b \in \mathbb{S}\ ,\ a\cdot b \in \mathbb{S}$$

Associative Law:

$$\forall a, b, c \in \mathbb{S}\ ,\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$$

for a semi-group $G(\mathbb{S},\ \cdot\ )$, if it satisfies

$$\exists e \in G\ ,\ \forall a \in G\ \Rightarrow\ e\cdot a = a$$

and

$$\forall a \in G\ ,\ \exists b \in G\ \Rightarrow\ b\cdot\ a = e$$

it is a group , and e is a left identity element , b is a left inverse element

Generally if G is a **group** it will satisfies
(1)G satisfies closure
(2)G satisfies asscoiative law
(3)there is a identity element in G
(4)there is an inverse element for each element in G

If a group G satisfies law of communication , G is a **Abelain Group**

law of communication:

$$\forall a, b \in \mathbb{S}\ \Rightarrow\ a\cdot b = b\cdot a$$

1.1.2 Property of Group

The number of elements in G expresses **the order of** G , marked as $|G|$, if $|G|$=∞ , G is a infinite group , if $|G| < \infty$, G is a finite group

For $G(\mathbb{S}, \ \cdot \ )$, $a \in G$

$$\overbrace{a \cdot a \cdot \cdots \cdot a}^{n} = a^n$$

For $G(\mathbb{S}, \ + \ )$, $a \in G$

$$\overbrace{a + a + \cdots + a}^{n} = na$$

$\forall G$, G is a group , then G satisfies **Cancellation law**

$$ax = ax' \ \Leftrightarrow \ x = x'$$

Note: if G is not a Abelian group , left cancellation law is satisfied does not mean right cancellation law is satisfied

If a set $G \neq \emptyset$ and the operation in G satisfies closure and associative law ,then

$if \ G \ is \ a \ group \ \Leftrightarrow \ \forall a, b \in G \ , \ ax = b \ and \ ya = b \ have \ solution$

Corollary:
If a set $G \neq \emptyset$ and the operation in G satisfies closure and associative law and G is a group $\Leftrightarrow$ G satisfies cancellation law

1.2 Subgroup

if $H \subset G$ and H with the operation in G is also form a group , H is a **subgroup** of G

if e is an identity element in G , then e is also an identity element in H
if a$\in$ H , $a^{-1} \in G$ and it is a inverse elenment of a , then $a^{-1} \in H$

if $H \in G$, and $H \neq \emptyset$, H is a subqroup of $G \Leftrightarrow$

$$\forall a, b \in H \ , \ ab \in H$$

$$\forall a \in H \ , \ a^{-1} \in H$$

Corollary:

(1) if $H \subset G$, and $H \neq \emptyset$, H is a subqroup of $G \Leftrightarrow$

$$\forall a, b \in H \ , \ ab^{-1} \in H$$

(2) if $H \subset G$, $H \neq \emptyset$ and $|H| < \infty$, H is a subqroup of $G \Leftrightarrow$

$$\forall a, b \in H \ , \ ab \in H$$

1.3 Homomorphism and Isomorphism

Suppose $G(\mathbb{S}, \ \cdot \ )$ and $G'(\mathbb{S}', \ \odot \ )$, $\exists \ f : \ \mathbb{S} \to \mathbb{S}'$, $\forall a, b \in \mathbb{S}$, let

$$f(a \cdot b) = f(a) \odot f(b)$$

then this f is **homomorphic mapping** , G and G' are homomorphic
if f is a bijection , f is also a **isomorphic mapping** , G and ceG' are isomorphic

if $G = G'$, f is self-homomorphic or self-isomorphic mapping

1.4 Cyclic Group

1.4.1 Difinition and Property of Cyclic Group

if $\exists g \in G$ and $G = \{\cdots g^{-1}, g^0, g^1, \cdots\}$, G is a **cyclic group** , g is a **generator** of G

if G is a cyclic group and $|G| = n \Rightarrow G = \{g^0, g^1, \cdots, g^{n-1}\}$

if $\exists$d> 0 , let $g^d = e$, d_{min} is the order of g , marked as $|g|$

Theorem:

(1) if G is a cyclic group and $|G|$=n $\Rightarrow \forall g \in G$, $|g|$=n

(2) if $|g|$=n , $g^d = e \Rightarrow n \mid d$

(3) if $|g|$=n $\Rightarrow |a^k| = \frac{n}{(n,k)}$
(4) if $|G|$=n , $\forall H \subset G \Rightarrow |H| \in \mathcal{D}(n)$

Prove:

1.4.2 Residue Class Group

$$\mathbb{S} = \{\overline{0}, \overline{1}, \cdots \overline{p-1}\}$$

is a residue system mod p , if p is a prime , then $\mathbb{S}$ and $\cdot$ or $+$ form a cyclic group , marked as $G(\mathbb{S}, \cdot)$ or $G(\mathbb{S}, +)$, $|G| = p$

Prove:

$$\begin{aligned}
(1) \text{ closure:} & \\
& \because \mathbb{Z} \subset \mathbb{S} \\
& \quad \mathbb{Z} \times \mathbb{Z} \subset \mathbb{Z} \\
& \therefore \forall a, b \in \mathbb{S} \text{ , } ab \in \mathbb{S} \\
(2) \text{ associative law:} & \\
& \quad \text{obviously} \\
(3) \text{ identity element:} & \\
& \quad e = \overline{1} \\
(4) \text{ inverse element:} & \\
& \because \forall a \in \mathbb{S}, (a, p) = 1 \\
& \therefore \exists u, v \in \mathbb{Z} \\
\text{let} \quad & \quad up + va = 1 \\
& \therefore va \equiv 1 (mod\ p)
\end{aligned}$$