Modern Algebra

Chapter one: Group theory

Groups and subgroups
Some important groups
Lagrange theorem
The center
Homomorphisms
The isomorphism theorems.

Chapter two: Ring theory
Rings
Integral domain
Subring
Kinds of rings
Field

Chapter three: p-group and Sylow theorems
p-group
Sylow first theorem.
Sylow second theorem.
Sylow third theorem.
Modern Algebra
Chapter One
Group theory
Groups and subgroups

Definition: A binary operation \(*\) on a set is a rule that assigns to each ordered pair of elements of the set some element of the set.

Example 1: On \(\mathbb{Z}^+\), define a binary operation \(*\) by \(a*b\) equals the smaller of \(a\) and \(b\) or the common value if \(a=b\). Thus \(2*11=2\)
\[3*3=3\]

Example 2: On \(\mathbb{Z}^+\), define a binary operation \(*\) by \(a*b\) equals \(a+b\) thus \(4*7=11\).

Definition: A binary operation \(*\) on a set \(S\) is commutative if and only if \(a*b=b*a\) for all \(a,b\in S\).

Definition: A binary operation \(*\) is associative if and only if \((a*b)*c = a*(b*c)\) for all \(a,b,c\in S\).
**Definition:** If $G$ is a non-empty set and $*$ is an associated binary operation then $(G,*)$ is called a semi-group.

**Definitions:** A Group $(G,*)$ is a set $G$ together with a binary operation $*$ on $G$ which satisfied the following conditions:

1. $G$ is closed under the operation $*$.
2. The binary operation $*$ is associative.
3. There is an element $e$ in $G$ such that $e*x = x*e = x$ for all $x \in G$.

(This element $e$ is an identity element for $*$ on $G$).
4. For each $a$ in $G$, there is an element $b$ in $G$ with the property that $a*b = b*a = e$.

(The element $b$ is an inverse of $a$ with respect to $*$) and denoted by $a^{-1}$.

**If** $a*b = b*a \ \forall a,b \in G$ then $G$ is called a commutative group or a abelian group.

**Examples:** The set $\mathbb{Z}$ with operation $+$ is a group. All condition of the definition are satisfied. The group is abelian.

**Examples:** The set $\mathbb{Z}^*$ with operation multiplication is not a group. There is an identity $1$, but no inverse of $3$. 
Theorem: If \( G \) is a group with binary operation \( \ast \), then the left and right cancellation laws hold in \( G \), that is, \( a \ast b = a \ast c \) implies \( b = c \), and \( b \ast a = c \ast a \) implies \( b = c \) for \( a, b, c \in G \).

Proof: Suppose \( a \ast b = a \ast c \)

\[ \Rightarrow \text{there exist } a^{-1} \text{ such that} \]

\[ a^{-1} \ast (a \ast b) = a^{-1} \ast (a \ast c) \]

\[ (a^{-1} \ast a) \ast b = (a^{-1} \ast a) \ast c \]

\[ \Rightarrow e \ast b = e \ast c \]

\[ \Rightarrow b = c \]

Similarly, from \( b \ast a = c \ast a \Rightarrow b = c \) by multiplication by \( a^{-1} \).

Note: The group \( (G, \ast) \) is abelian if \( (a \ast b)^{-1} = a^{-1} \ast b^{-1} \)

Note: If \( (G, \ast) \) is a group s.t \( a \ast e = e \forall a \in G \) then \( G \) is abelian.

Definition: A group \( (G, \ast) \) is called a finite group if \( G \) contains a finite number of elements.

Definition: A group \( (G, \ast) \) is called an infinite group if \( G \) contains an infinite number of elements.

The number of elements of \( G \) is called the order of \( G \) denoted by \( |G| \) or \( o(G) \).
Theorem: In a group $G$ with operation $*$, there is only one identity $e$ such that $e * x = x * e = x$.

For all $x \in G$, for each $a \in G$, there is only one element $a^{-1}$ such that $a^{-1} * a = a * a^{-1} = e$

i.e., the identity and inverses are unique in a group.

Proof: Suppose $e * x = x * e = x$ and also $e_1 * x = x * e_1 = x \forall x \in G$

Now let $e$ be the identity, $e * e_1 = e_1 * e = e_1$

let $e_1$ be the identity, $e * e_1 = e_1 * e = e$

Thus $e_1 = e * e_1 = e$

and the identity of a group is unique.

Now suppose $a^{-1} * a = a * a^{-1} = e$ and $a^{-1} * a = a * a^{-1} = e$ then $a * a^{-1} = a * a^{-1} = e$

by the cancellation law

$a^{-1} = a^{-1}$

so the inverse of $a$ in a group is unique

Subgroups

Definition: Let $(G, *)$ be a group and $H$ be a non-empty set. The pair $(H, *)$ is called a subgroup iff $(H, *)$ is a group itself
denoted by $(H, *) \leq (G, *)$

Example: $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
Theorem: Let \((G, \cdot)\) be a group and \(H\) a non-empty set then \((H, \cdot')\) is called a subgroup if \(a \cdot b^{-1} \in H, \forall a, b \in H\).

Proof:
\[\forall a, b \in H \quad \text{since } H \text{ is a subgroup}
\]
Thus it is a group then \(b^{-1} \in H\) and then \(a \cdot b^{-1} \in H\) (closed)
\[\Leftarrow \quad \text{since } H \neq \emptyset \text{ then there exist at least an element}
\quad \text{say } a \in H.
\]
From above condition \(e = a \cdot a^{-1} \in H \rightarrow 1\)

For each \(b \in H \rightarrow b^{-1} = e^{-1} \cdot b^{-1} \in H \rightarrow 2\)
\(\forall a, b \in H, a \in H, b^{-1} \in H\) then \(a \cdot b^{-1} \in H \rightarrow 3\)
\(\Rightarrow H\) is a group.

Proposition: The intersection of any family of subgroups of any group is again a subgroup.

Proof:
\(\text{let } (G, \cdot) \text{ be a group}
\)
\(\text{let } \{ H_i | i \in I \} \text{ be a family of subgroups then}
\)
\[H_i = \{ H_0, H_2, H_3, \ldots \}
\]
\(\bigcap H_i \text{ is a subgroup } \iff a \cdot b^{-1} \in \bigcap H_i, \forall a, b \in H_i
\)
\(\text{let } a \in H_i, \forall i \quad \Rightarrow \quad a \cdot b^{-1} \in \bigcap H_i
\)
\(\text{let } b^{-1} \in H_i, \forall i \quad \Rightarrow \quad a \cdot b^{-1} \in \bigcap H_i
\)
\[a \cdot b^{-1} \in H_i, \forall i \quad \text{(because } H_1, H_2, \ldots \text{ are subgroups)}
\]
\[\Rightarrow a \cdot b^{-1} \in \bigcap H_i
\]
\[\Rightarrow \bigcap H_i \text{ is a subgroup.}\]