Definition A non-empty set G with a binary operation (called multiplication) $\cdot : G \times G \to G$ is called a group if

1. multiplication is closed in G,
$$a \cdot b \in G \quad \forall a, b \in G;$$
2. multiplication is associative
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad a, b, c \in G;$$
3. there is an identity element e
$$e \cdot a = a \cdot e = a \quad \forall a \in G;$$
4. for every element a, there is an inverse a^{-1}
$$a \cdot a^{-1} = a^{-1} a = e.$$

Definition A group is abelian if the multiplication is commutative.

Definition If group is finite then the number of elements is called the order of the group.

1. Groups: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$,$(\mathbb{R},+)$ and $(\mathbb{C},+)$, identity is 0 and inverse of a is $-a$.
2. Groups: $(\mathbb{Q}^*,\times)$,$(\mathbb{R}^*,\times)$ and $(\mathbb{C}^*,\times)$, identity is 1 and inverse of a is $1/a$.
3. Finite groups:
   - 3.1 Trivial $G=\{e\}$, $e\cdot e=1$
   - 3.2 $G=\{e,a\}$, $a^2=e$
   - 3.3 $G=\{e,a,b\}$, $ab=ba=e$
   - 3.4 $C_n=\left\{e,a,a^2,\ldots,a^{n-1}\right\}$, $a^n=e$
   - 3.5 D_n generated by a and b such that $a^n=b^2=e$ and $ab=ba^{-1}$.
4. Matrix Groups: $(M_n,+)$, $GL(n,\mathbb{R})$, $O(n)$, $SO(n)$, $GL\left(n,\mathbb{C}\right)$, $U(n)$, $SU(n)$
5. Permutation Group S_n.
6. Transformation Groups: Euclidean group $E\left(n\right)$, Lorentz group $O\left(1,3\right)$ etc.

Groups

Properties

1. Identity is unique
2. Inverse is unique
3. Cancellation Laws: $ab = ac \implies b = c$ and $ab = cb \implies a = c$
4. $\left(a^{-1}\right)^{-1} = a$
5. $(ab)^{-1} = b^{-1}a^{-1}$
6. Rearrangement theorem: Each row of the multiplication table contains all elements. A row can't have an element appering twice or more.

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Examples

1. Trivial subgroups: G and $\{e\}$

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Examples

1. Trivial subgroups: G and $\{e\}$
2. $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$. Also $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^*, \times)$

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Examples

1. Trivial subgroups: G and $\{e\}$
2. $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$. Also $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^*, \times)$
3. $H = \{5n \mid n \in \mathbb{Z}\}$ is subgroup of $(\mathbb{Z}, +)$.

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Examples

1. Trivial subgroups: G and $\{e\}$
2. $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$. Also $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^*, \times)$
3. $H = \{5n \mid n \in \mathbb{Z}\}$ is subgroup of $(\mathbb{Z}, +)$.
4. Subgroups in D_3 are $\{e, a, a^2\}$, $\{e, b\}$, $\{e, ab\}$ and $\{e, a^2 b\}$

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Examples

1. Trivial subgroups: G and $\{e\}$
2. $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$. Also $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^*, \times)$
3. $H = \{5n \mid n \in \mathbb{Z}\}$ is subgroup of $(\mathbb{Z}, +)$.
4. Subgroups in D_3 are $\{e, a, a^2\}$, $\{e, b\}$, $\{e, ab\}$ and $\{e, a^2b\}$
5. $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad \neq 0, b \in \mathbb{R} \right\}$ and $K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$ in $GL(2)$

Definition A subset H of a group G is called a subgroup of G if H is a group by itself with the same group multiplication.

Theorem A subset H of a group G is subgroup of G iff

1. multiplication is closed in H;
2. for each $a \in H$, a^{-1} is also in H.

If the group is finite then only the first condition is sufficient.

Examples

1. Trivial subgroups: G and $\{e\}$
2. $(\mathbb{Z},+) \subset (\mathbb{Q},+) \subset (\mathbb{R},+) \subset (\mathbb{C},+)$. Also $(\mathbb{Q}^*,\times) \subset (\mathbb{R}^*,\times) \subset (\mathbb{C}^*,\times)$
3. $H = \{5n \mid n \in \mathbb{Z}\}$ is subgroup of $(\mathbb{Z},+)$.
4. Subgroups in D_3 are $\{e, a, a^2\}$, $\{e, b\}$, $\{e, ab\}$ and $\{e, a^2 b\}$
5. $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad \neq 0, b \in \mathbb{R} \right\}$ and $K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$ in $GL(2)$
6. $GL(n) \supset O(n) \supset SO(n) \supset C_6 \supset C_3$

Cosets

Definition If H is a subgroup of a group G, and $a \in G$, then a right coset of subgroup H, denoted as Ha, is defined as $Ha = \{ha \mid h \in H\}$.

Cosets

Definition If H is a subgroup of a group G, and $a \in G$, then a right coset of subgroup H, denoted as Ha, is defined as $Ha = \{ha \mid h \in H\}$.

Theorem If $a, b \in G$, and H is a subgroup of G, then Ha and Hb are either equal of disjoint.

Cosets

Definition If H is a subgroup of a group G, and $a \in G$, then a right coset of subgroup H, denoted as Ha, is defined as $Ha = \{ha \mid h \in H\}$.

Theorem If $a, b \in G$, and H is a subgroup of G, then Ha and Hb are either equal of disjoint.

Theorem There is a one-one correspondance between two right cosets of H in G.

Cosets

Definition If H is a subgroup of a group G, and $a \in G$, then a right coset of subgroup H, denoted as Ha, is defined as $Ha = \{ha \mid h \in H\}$.

Theorem If $a, b \in G$, and H is a subgroup of G, then Ha and Hb are either equal of disjoint.

Theorem There is a one-one correspondance between two right cosets of H in G.

Theorem $\mathcal{O}(H) \mid \mathcal{O}(G)$ if G is finite.

In general, right coset Ha is not equal to aH. Example: $H = \{e, \sigma\}$ in C_{3v}.

Normal/Invariant Subgroups

Definition A subgroup N of G is normal subgroup if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Normal/Invariant Subgroups

Definition A subgroup N of G is normal subgroup if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Theorem N is a normal subgroup in G if and only if $gNg^{-1} = N$.

Normal/Invariant Subgroups

Definition A subgroup N of G is normal subgroup if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Theorem N is a normal subgroup in G if and only if $gNg^{-1} = N$.

Theorem N is a normal subgroup in G iff every right coset Na is equal to the left coset aN in G.

Normal/Invariant Subgroups

Definition A subgroup N of G is normal subgroup if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Theorem N is a normal subgroup in G if and only if $gNg^{-1} = N$.

Theorem N is a normal subgroup in G iff every right coset Na is equal to the left coset aN in G.

Definition $A, B \subset G$. Define product $AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\}$

Normal/Invariant Subgroups

Definition A subgroup N of G is normal subgroup if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Theorem N is a normal subgroup in G if and only if $gNg^{-1} = N$.

Theorem N is a normal subgroup in G iff every right coset Na is equal to the left coset aN in G.

Definition $A, B \subset G$. Define product
$AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\}$

Theorem N is a normal subgroup in G iff product of two right cosets of N is a right coset of N.

Factor Groups

Definition A collection of the cosets of a normal subgroup N in G is a group with product of sets as the binary operation. This group is called as factor group and is denoted by G/N.

Factor Groups

Definition A collection of the cosets of a normal subgroup N in G is a group with product of sets as the binary operation. This group is called as factor group and is denoted by G/N.

Example $G = S_3 = \{e, \psi, \psi^2, \sigma, \sigma\psi, \sigma\psi^2\}$. Check that $N = \{e, \psi, \psi^2\}$ is a normal subgroup with two cosets $Ne = N$ and $N\sigma$. The factor group $G/N = \{N, N\sigma\}$.

Factor Groups

Definition A collection of the cosets of a normal subgroup N in G is a group with product of sets as the binary operation. This group is called as factor group and is denoted by G/N.

Example $G = S_3 = \{e, \psi, \psi^2, \sigma, \sigma\psi, \sigma\psi^2\}$. Check that $N = \{e, \psi, \psi^2\}$ is a normal subgroup with two cosets $Ne = N$ and $N\sigma$. The factor group $G/N = \{N, N\sigma\}$.

Example $G = (\mathbb{Z}, +)$. $N = \{5k \mid k \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ is normal in G. The distinct cosets are $N = N0, N1, N2, N3, N4$ such that $Np = \{5k + p \mid k \in \mathbb{Z}\}$. For example, $N2 = \{\ldots, -3, 2, 7, 12, \ldots\}$. Then $G/N = \{N0, N1, N2, N3, N4\}$

Homomorphism

Definition A mapping f from a group $(G, \odot)$ to a group $(\bar{G}, \otimes)$ is called homomorphism if $\forall a, b \in G$, $f(a \odot b) = f(a) \otimes f(b)$. (For brevity, $f(ab) = f(a)f(b)$)

Homomorphism

Definition A mapping f from a group $(G, \odot)$ to a group $(\bar{G}, \otimes)$ is called **homomorphism** if $\forall a, b \in G$, $f(a \odot b) = f(a) \otimes f(b)$. (For brevity, $f(ab) = f(a)f(b)$)

Theorem If $f : G \to \bar{G}$ is a homomorphism, then

1. $f(e) = \bar{e}$.
2. $f\left(a^{-1}\right) = [f(a)]^{-1}$

Homomorphism

Definition A mapping f from a group $(G, \odot)$ to a group $(\bar{G}, \otimes)$ is called homomorphism if $\forall a, b \in G$, $f(a \odot b) = f(a) \otimes f(b)$. (For brevity, $f(ab) = f(a)f(b)$)

Theorem If $f : G \to \bar{G}$ is a homomorphism, then

1. $f(e) = \bar{e}$.
2. $f\left(a^{-1}\right) = [f(a)]^{-1}$

Definition If $f : G \to \bar{G}$ is a homomorphism, then the kernel K of f is defined as $K = \{x \in G \mid f(x) = \bar{e}\}$.

Homomorphism

Definition A mapping f from a group $(G, \odot)$ to a group $(\bar{G}, \otimes)$ is called **homomorphism** if $\forall a, b \in G$, $f(a \odot b) = f(a) \otimes f(b)$. (For brevity, $f(ab) = f(a)f(b)$)

Theorem If $f : G \to \bar{G}$ is a homomorphism, then

1. $f(e) = \bar{e}$.
2. $f\left(a^{-1}\right) = [f(a)]^{-1}$

Definition If $f : G \to \bar{G}$ is a homomorphism, then the **kernel** K of f is defined as $K = \{x \in G \mid f(x) = \bar{e}\}$.

Theorem Kernel of a homomorphism $f : G \to \bar{G}$ is a normal subgroup of G.

Homomorphism

Definition A mapping f from a group $(G, \odot)$ to a group $(\bar{G}, \otimes)$ is called homomorphism if $\forall a, b \in G$, $f(a \odot b) = f(a) \otimes f(b)$. (For brevity, $f(ab) = f(a)f(b)$)

Theorem If $f : G \to \bar{G}$ is a homomorphism, then

1. $f(e) = \bar{e}$.
2. $f\left(a^{-1}\right) = [f(a)]^{-1}$

Definition If $f : G \to \bar{G}$ is a homomorphism, then the kernel K of f is defined as $K = \{x \in G \mid f(x) = \bar{e}\}$.

Theorem Kernel of a homomorphism $f : G \to \bar{G}$ is a normal subgroup of G.

Definition A homomorphism f is called an isomorphism if f is one-one.

Homomorphism

Definition A mapping f from a group $(G, \odot)$ to a group $(\bar{G}, \otimes)$ is called homomorphism if $\forall a, b \in G$, $f(a \odot b) = f(a) \otimes f(b)$. (For brevity, $f(ab) = f(a)f(b)$)

Theorem If $f : G \to \bar{G}$ is a homomorphism, then

1. $f(e) = \bar{e}$.
2. $f\left(a^{-1}\right) = [f(a)]^{-1}$

Definition If $f : G \to \bar{G}$ is a homomorphism, then the kernel K of f is defined as $K = \{x \in G \mid f(x) = \bar{e}\}$.

Theorem Kernel of a homomorphism $f : G \to \bar{G}$ is a normal subgroup of G.

Definition A homomorphism f is called an isomorphism if f is one-one.

Definition Two groups G and $\bar{G}$ are isomorphic if there exists an isomorphism from G onto $\bar{G}$.