MT2213 - Group Theory

Nachiketa Kulkarni

Contents

Chapter 1

Definitions

1.1 Groups

A non-empty set G is a group, is considered to be a group with an operation $\star$ if to every pair $(x, y) \in G \times G$ and element $x \star y \in G$ is assigned, satisfying the following axioms:

1. **Associativity:** $\forall\ x, y, z \in G$, $x \star (y \star z) = (x \star y) \star z = x \star y \star z$
2. **Existence of Identity:** There exists an element $e \in G$ such that $e \star g = g \star e = g$
3. **Existence of Inverse:** For every element $x \in G$ there exists an element $x^{-1} \in G$ such that $x \star x^{-1} = e = x^{-1} \star x$, where $e \in G$ is the identity element of the group.

It is represented as $(G, \star)$. Some properties of groups:

1. **Uniqueness of Identity:** The identity element of a group is unique. Consider $e_1, e_2 \in G, e_1 \neq e_2$ and both are identity elements. Let $x \in G$, then $e_1 \star x = e_2 \star x = x$. This also implies that $e_1 = e_2$, hence the identity element is unique.
2. **Uniqueness of Inverse:** The inverse of an element in a group is unique. Consider $x \in G$, and $y_1, y_2 \in G$ are inverses of x. Then, $x \star y_1 = e = y_1 \star x$ and $x \star y_2 = e = y_2 \star x$. Now, $y_1 = y_1 \star e = y_1 \star (x \star y_2) = (y_1 \star x) \star y_2 = e \star y_2 = y_2$. Hence, the inverse of an element is unique.

1.1.1 Examples:

1. $(\mathbb{Z}, +)$ is a group:
   (a) Associativity: Addition is associative.
   (b) Identity: 0 is the identity. Let $x \in Z$. Now $0 + x = x + 0 = x$. Hence, it is an identity.
   (c) Inverse: Let $x \in \mathbb{Z}$. Now, $x + (-x) = (-x) + x = 0$, where 0 is the additive identity.
2. $(\mathbb{Q}^+, \times)$ is a group:
   (a) Associativity: Multiplication is associative.
   (b) Identity: 1 is the identity: Let $x \in \mathbb{Q}^+$. Now, $1 \times x = x \times 1 = x$. Hence, it is an identity.
   (c) Inverse: Let $x \in \mathbb{Q}^+$, Now, $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$, where 1 is the multiplicative identity.

3. $(GL(n, \mathbb{R}), \times)$ is a group, where $\times$ is matrix multiplication (or combination of linear transformations):
   (a) Associativity: Matrix multiplication is associative.
   (b) Identity: I_n is the identity matrix.
   (c) Inverse: Let $A \in GL(n, \mathbb{R})$, then $A \times A^{-1} = A^{-1} \times A = I_n$.

Check if:

1. $(\mathbb{R}, \times)$ is a group or not.

   $0 \in \mathbb{R}$, 0 does not have an inverse. Hence, it is not a group.
2. $(\mathbb{C}, \times)$ is a group or not.

   $0 \in \mathbb{C}$, 0 does not have an inverse. Hence, it is not a group.
3. $(\mathbb{R}/\{0\}, \times)$ is a group or not.

   Yes its a group:
   (a) Associativity: Multiplication is associative.
   (b) Identity: 1 is an identity: Let $x \in \mathbb{R}/\{0\}$. Now, $1 \times x = x \times 1 = x$. Hence, it is an identity.
   (c) Inverse: Let $x \in \mathbb{R}/\{0\}$, Now, $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$, where 1 is the multiplicative inverse.
4. $(\mathbb{C}/\{0\}, \times)$ is a group or not.

   Yes it is a group:
   (a) Associativity: Multiplication is associative.
   (b) Identity: 1 is an identity: Let $x \in \mathbb{C}/\{0\}$. Now, $1 \times x = x \times 1 = x$. Hence, it is an identity.
   (c) Inverse: Let $x \in \mathbb{C}/\{0\}$, Now, $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$, where 1 is the multiplicative inverse.

1.1.2 Abelian Groups

A group $(G, \star)$ is said to be abelian if the operation $\star$ is commutative, i.e., $x \star y = y \star x$, $\forall x, y \in G$.

1.1.3 Conjugate

Consider a group $(G, \star)$. For $x, y \in G$, y is said to be conjugate of x if there exists an element $a \in G$ such that:

$$y = a \star x \star a^{-1}$$

Note: For a given a, the conjugate of x is unique. i.e., if we consider conjugate to be a function f_a, then f_a is a bijection.

1.1.4 Order of a Group

The order of a group G is the number of elements in the group. It is denoted by $|G|$. A group G is said to be finite if the number of elements in it is finite. Otherwise, it is said to be infinite.

1.1.5 Cyclic Group

A group $(G, \star)$ is said to be cyclic if there exists an element $a \in G$ such that every element of G can be written as a power of a. Let, $G = \langle g \rangle$ by a cyclic group of order n. Then, $G = \{e, g, g^2, \ldots, g^{n-1}\}$.

Properties of Cyclic Groups

1. All cyclic groups are abelian.
2. $n = \min\{m \in \mathbb{N} \,|\, g^m = 1\}$.

   Proof: As the order of G is finite, there exists $a, b \in \mathbb{N}$ such that $g^a = g^b$. This implies: $g^{a-b} = 1$.
   $$\therefore \exists\, n := \min\{m \in \mathbb{N} \,|\, g^m = 1\}$$
3.

1.1.6 Sub-groups

Consider a group $(G, \star)$. A non-empty subset H is a subgroup of G if H is a group with the same operation $\star$ as G. It is represented as $H \leq G$.

A few properties of subgroups:

1. **Identity:** The identity element of G is also the identity element of H.
2. **Inverse:** If $x \in H$, then $x^{-1} \in H$.

Minimal and Maximal Subgroups

The Minimal subgroup $U \neq 1$ is known as a minimal subgroup of group G if no other non-trivial subgroup of G is contained in U.

The Maximal subgroup $U \neq G$ is known as the maximal subgroup of group G if U is not contained in any other subgroup of G.

Theorem

Let A and B be subgroups of G. Then AB is a subgroup of G if and only if $AB = BA$.

Proof: From $AB \leq G$ we get:

$$(AB) = (AB)^{-1} = B^{-1}A^{-1} = BA$$

If $BA = AB$:

$$(AB)(AB) = A(BA)B = A(AB)B = AABB = AB$$

and

$$(AB)^{-1} = B^{-1}A^{-1} = BA = AB$$

Therefore, $AB \leq G$

Theorem

Let A and B be finite subgroups of G. Then,

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}$$

Proof: If we consider an equivalence relation on the Cartesian Product $A \times B$:

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1b_1 = a_2b_2$$

Then $|AB|$ is the number of equivalence classes in $A \times B$. Let $(a_1, b_1) \in A \times B$. The equivalence class:

$$\{(a_2, b_2) \,|\, a_1b_1 = a_2b_2\}$$

which contains exactly $|A \cap B|$ elements:

$$\begin{aligned} a_2b_2 = a_1b_1 &\Leftrightarrow a_1^{-1}a_2 = b_1b_2^{-1} \\ &\Leftrightarrow a_2 = a_1d \text{ and } b_2 = db_1 \text{ for some } d \in A \cap B \end{aligned}$$

1.1.7 Cosets

Let $(G, \star)$ be a group. Consider H be a subgroup of G and $a \in G$. The subset $aH = \{ah|h \in H\}$ is known as the left coset of H containing a. Similarly, the subset $Ha = \{ah|h \in H\}$ is known as the right coset of H containing a.

Properties of Cosets

1. The application $Hx \to (Hx)^{-1} = x^{-1}H$ defines a bijective relation from the set of Right Cosets of H to the set of Left Cosets of H.

2. If the set of Right Cosets of H in G is finite, then the number of Right Cosets of H in G is called the inedex of H in G.

3. One of the cosets is the subgroup H itself. $eH = He = H$, where e is the identity element of the group G.

4. For all $x \in G$, as $x = ex \in Hx$, the right cosets of H cover the set G.

5. For $x, y \in G$,
$$Hx = Hy \Leftrightarrow yx^{-1} \in H \Leftrightarrow y \in Hx$$
Hence, any two right cosets are either disjoint or equal.

Lagrange's Theorem

Let H be a subgroup of the finite group G. Then,

$$|G| = |H|\,|G:H|$$

i.e., $|H|$ and $|G:H|$ are divisors of H.
As a consequence, we get the following:

> For every finite G and every $g \in G$, the order of g divides $|G|$.

Transversal Set

Let H be a subgroup of G. A set S is considered as the transversal set of H in G if S contains exactly one element from each right coset of H in G. Similarly, the left transversal set of H in G contains exactly one element from each left coset of H in G.

Theorem: Let $S \subseteq G$. Then, S is a transversal set of H in G if and only if $G = SH$ and $st^{-1} \notin H$ for all $s \neq t$ and $s, t \in S$.

Dedekind Identity

Let $G = AB$ where $A, B \leq G$. Then every subgroup H of G, such that $A \leq H \leq G$ has the following property:
$$H = A\,(H \cap B)$$

1.2 Homomorphisms and Normal Subgroups

Let G and H be groups. A map $\phi : G \to H$ is said to be a homomorphism if:

$$\phi\,(x \star y) = \phi\,(x) \star \phi\,(y)$$

for all $x, y \in G$. Let $\phi : G \to H$. Let, $X \subseteq G$ and $Y \subseteq H$. Also, let e_G is the identity element of G and e_H is the identity element of H. Then, we define the following:

- $\phi\,(X) := \{\phi\,(x)\,|\; x \in X\}$
- $\phi^{-1}\,(Y) := \{x \in G\,|\,\phi\,(x) \in Y\}$
- $\ker \phi := \{x \in G\,|\,\phi\,(x) = e_H\}$
- $\text{Im}\ \phi := \phi\,(G)$

1.2.1 Properties of Homomorphisms

1. If the homomorphism ϕ is bijective, then the inverse map ϕ^{-1} is also a homomorphism.

   Proof: Let $x, y \in H$.

$$\phi^{-1}(x) \star \phi^{-1}(y) = \phi^{-1}(x \star y)$$
$$\phi\left(\phi^{-1}(x) \star \phi^{-1}(y)\right) = \phi\left(\phi^{-1}(x)\right) \star \phi\left(\phi^{-1}(y)\right) = x \star y$$

2. $\phi(e_G) = e_H$
3. $\phi(x^{-1}) = (\phi(x))^{-1}$
4. $\phi(\langle X \rangle) = \langle \phi(X) \rangle$
5. Let $N = \ker \phi$. Then for all $x \in G$

$$Nx = \{y \in G \,|\, \phi(x) = \phi(y)\} = xN$$

   Proof:

$$\begin{aligned}\phi(x) = \phi(y) &\iff \phi(y)(\phi(x))^{-1} = 1 \iff \phi(y)\,\phi\left(x^{-1}\right) \\ &\iff \phi\left(yx^{-1}\right) = 1 \qquad \iff yx^{-1} \in N \\ &\iff y \in Nx\end{aligned}$$

1.2.2 Normal Subgroups

A subgroup N of a group G is said to be normal if for all $x \in G$, $Nx = xN$. We write $N \trianglelefteq G$.

If $N \trianglelefteq G$, then the set of left cosets and right cosets of N in G are the same. Another way to define normal subgroups is, $\forall x \in G$:

$$Nx = xN \iff N = x^{-1}Nx \iff N = N^x$$