# Contents

# Chapter 1

# Preliminary

$R \subset A \times A$ is an equivalence relations if

**Reflexive:** $\forall a \in A, (a, a) \in R$.

**Symmetric:** $(a, b) \in R \implies (b, a) \in R$.

**Transitive:** $(a, b) \in R, (b, c) \in R \implies (a, c) \in R$.

A binary relations can be also denoted as $aRb$ whenever $(a, b) \in R$.
If $A$ is a set and if $\sim$ is an equivalence relation on $A$, then the equivalence class of $a \in A$ is the set $\{x \in A \,|\, x \sim a\}$ denoted by $\mathrm{cl}(a)$.

**Theorem 1.1.** *Equivalence classes partition the set into mutually disjoint subsets and conversely, mutually disjoint subsets give rise to equivalence classes.*

If $S$ and $T$ are non-empty sets, then a mapping from $S$ to $T$ is a subset $M \subset S \times T$ such that for every $s \in S$ there is a unique $t \in T$ that $(s, t) \in M$. $\sigma : S \to T$ maybe denoted as $t = s\sigma$ or $t = \sigma(s)$.

# Chapter 2

# Group Theory

## 2.1 Introduction

**Definition:** A non-empty set of elements $G$ together with a binary operation $\circ$ are said to be a **group** if

**Closure:** $\forall a, b \in G, a \circ b \in G$.

**Associative:** $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$.

**Identity:** $\exists e \in G$ such that $\forall a \in G, a \circ e = e \circ a = a$.

**Inverse:** $\forall a \in G\ \exists b \in G$ such that $a \circ b = b \circ a = e$.

**Definition:** A group $G$ is said to be **abelian** or **commutative** if for any two element $a$ and $b$ commute. i.e. $a \circ b = b \circ a$.

**Definition:** The number of elements in a group is called the **order** of the group and it is denoted by $o(G)$.

**Definition:** Let $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. If for some choice of $a$, $G = \langle a \rangle$, then $G$ is said to be a **cyclic group**. More generally, for a set $W \subset G$, $\langle W \rangle = \bigcap W \subset H \subset GH$ where $H$ is a subgroup of $G$.

**Lemma 2.1.** *Given $a, b \in G$ the equation $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.*

## 2.2 Subgroup

**Definition:** A non-empty subset $H$ of a group $G$ is called a **subgroup** if under the product in $G$, $H$ itself forms a group.

**Lemma 2.2.** *$H$ is a subgroup of $G$ if and only if*

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

*Proof.* Add. ◻

**Lemma 2.3.** *If $H$ is a non-empty finite subset of a group $G$ and $H$ is closed under multiplication, then $H$ is a subgroup of $G$.*

*Proof.* Add. □

**Definition:** Let $G$ be a group and $H$ a subgroup of $G$. For $a, b \in G$ we say that $a$ is congruent to $b \mod H$, written as $a \equiv b \mod H$ if $ab^{-1} \in H$.

**Lemma 2.4.** *The relation $a \equiv b \mod H$ is an equivalence relation.*

*Proof.* Add. □

**Definition:** If $H$ is a subgroup of $G$ and $a \in G$, then $Ha = \{ha \,|\, h \in H\}$ is a **right coset** of $H$ in $G$. Similary, $aH = \{ah \,|\, h \in H\}$ is a **left coset** of $H$ in $G$.

**Lemma 2.5.** *For all $a \in G$,*

$$Ha = \{x \in G \,|\, a \equiv x \mod H\}$$

*Proof.* Suppose $x \in G$ and $x \equiv a \mod H$. That is, $xa^{-1} = h$ for some $h \in H$. Then, $x = ha$. Suppose $h \in H$ and $x = ha$. Then, $xa^{-1} = h$ and hence $x \equiv a \mod H$. □

This implies, two right/left coset of $H$ are either identical or disjoint.

**Lemma 2.6.** *There is a one-to-one correspondence between any two right/left cosets of $H$.*

*Proof.* Add. □

**Theorem 2.7 (Lagrange's theorem).** *If $G$ is a finite group and $H$ is a subgroup of $G$, then $o(H) \mid o(G)$.*

*Proof.* Add. ■

**Definition:** If $H$ is a subgroup of $G$, the **index** of $H$ in $G$ is the number of distince right cosets of $H$, denoted by $[G : H]$ or $i_G(H)$.

**Definition:** Let $G$ be a group and $a \in G$, then the **order** or **period** of $a$ is the least positive integer $m$ such that $a^m = e$. If no such integer exists we say that $a$ is of infinite order. The order of $a$ is denoted by $\text{ord}_G(a)$.

**Corollary 2.8.** *If $G$ is a finite group, then*

1. $o(G) = i_G(H)o(H)$.
2. $\text{ord}_G(a) \mid o(G)$.
3. $a^{o(G)} = e$.
4. *If $o(G)$ is a prime, then $G$ is cyclic.*

## 2.3 A counting principle

Let $H$ and $K$ be two subgroups of $G$, then

$$HK = \{hk \mid h \in H, k \in K\}$$

**Lemma 2.9.** *$HK$ is a subgroup of $G$ if and only if $HK = KH$.*

**Corollary 2.10.** *If $H$ and $K$ are subgroups of an abelian group $G$, then $HK$ is a subgroup of $G$.*

**Lemma 2.11.** *If $H$ and $K$ are finite subgroups $G$, then*

$$|HK| = \frac{o(H)o(K)}{o(H \cap K)}$$

*Proof.* If $h_1 \in H \cap K$ then $hk = (hh_1)(h_1^{-1}k)$. Therefore, $hk$ appears at least $o(H \cap K)$ times. If $hk = h'k'$, then $h'^{-1}h = k'k^{-1} \in H \cap K$. Let $u = h'^{-1}h$ then $h' = hu^{-1}$ and $k' = uk$. Thus, all duplicates are accounted for. □

**Corollary 2.12.** *If $H$ and $K$ are subgroups of $G$ and $o(H), o(K) > \sqrt{o(G)}$, then $H \cap K \neq \{e\}$.*

*Proof.* $HK \subset G$ therefore, $|HK| \leq o(G)$ and

$$o(G) \geq |HK| = \frac{o(H)o(K)}{o(H \cap K)} > \frac{o(G)}{o(H \cap K)}$$

which implies that $o(H \cap K) > 1$. ■