# The Lecture Title

Scribe: Your Name

**Date**: Day, Mon, Date Year

## 1 Unit 3 - Group Theory and Friends

**Definition.** A **group** is a set $A$ and an binary operation $\cdot$ (we denote this $G = (A, \cdot)$) where the following four properties hold:

1. *Closure.* A is closed under $\cdot$, that is, if elements $a_1, a_2 \in A$ then $a_1 \cdot a_2 \in A$.
2. *Associativity.* The operation $\cdot$ is associative, that is, if elements $a, b, c \in A$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. *Identity.* There exists an element $e \in A$ such that $e \cdot a = a \cdot e = a$.
4. *Inverse.* There exists an element $a^{-1} \in A$ for any element $a$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Note that *commutativity* is **NOT** a necessary property of a group. We call groups such that for elements $a, b \in A$ such that $a \cdot b = b \cdot a$ are *abelian* or commutative.

Here are some examples of sets that are groupsThis is a group. /not groups:

- $G = (\mathbb{Z}, +)$. Yes! All these properties hold.
- $G = (\mathbb{Z}, \times)$. No! $0$ does not have a multiplicative inverse, and in fact, no element has an inverse other than $\pm 1$.
- $G = (\mathbb{Q}, \times)$. No! $0$ does not have a multiplicative iverse.
- $G = (\mathbb{R}, +)$. Yes! Same reasons as the first group.
- $G = (\{\text{set of all 2-by-2 matrices with integer elements}\}, \cdot)$ No! Not all of these matrices are invertible (have determinant zero).
- $G = (\{\text{set of all 2-by-2 matrices with determinant } 1\}, \cdot)$. Yes! This is actually a special group, $SL(2)$.

**Definition.** A **subgroup** $H$ of $G$ is $H = (B, \cdot)$ where $B \subseteq A$. These groups must have the same operation, and $H$ must also be a group.

An example of a subgroup: $(5\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$, as it retains all the properties of $\mathbb{Z}$.

**Defintion.** A **coset** $a \cdot H$ of a subgroup $H$ is the set of elements $\{a \cdot h | h \in H\}$ and $a \in G$.

For example, take the example $2+5\mathbb{Z} = \{2, 7, 12, 17, \ldots, -3, -8, -13, -18 \ldots\}$. These are the integers that are $\equiv 2 \bmod 5$. Similarly, we can form three other unique cosets (that are 1, 3, and 4 mod 5). Note that cosets are **not** generally groups, as this coset is clearly not a group (no identity, not closed under addition, etc.)

Let's consider the following statements:

- Cosets $a \cdot H \cap b \cdot H = \emptyset$ if $a \neq b$. This is not always true - as a counterexample, consider $2 + 5\mathbb{Z}$ and $7 + 5\mathbb{Z}$.
- If $a \cdot H \cap b \cdot H \neq \emptyset$, then $a \cdot H = b \cdot H$.
- If $H$ is finite, $|a \cdot H| = |H|$. This is true -
- Every $g \in G$ is in $a \cdot H$ for some $a$. Obviously not always true, but if it were, we could actually solve for $a$.

If ALL of these statements are true, then we can conclude that $|G|$ is divisble by $a \cdot H$, and furthermore, $|H||G|$.