Week 1

Introduction to Groups

Definition of a group:
A **group** G is a nonempty set together with a multiplication $G \times G \to G$ satisfying

1. $(ab)c = a(bc) \forall a, b, c, \in G$, (Associativity)
2. there exists $e \in G$ such that $ea = ae = a \forall a \in G$, (Identity)
3. and for every $a \in G$ there exists $b \in G$ such that $ab = ba = e$. (Inverse)

Example of a group:
Let $\mathbb{R}^* = \mathbb{R}^\dagger = \{a \in \mathbb{R} : a \neq 0\}$ together with multiplication on $\mathbb{R}$.
Associativity is immediate.
The identity is $1 \in \mathbb{R}^*$.
For every $a \in \mathbb{R}^*$, $\frac{1}{a} \in \mathbb{R}$ and $a(\frac{1}{a}) = \frac{1}{a}(a) = 1$.
So $\mathbb{R}^*$ is a group.

Remark: When we need to highlight the group multiplication we write a group as a pair of the set and the multiplication, e.g., $(\mathbb{R}, +), (\mathbb{R}, \cdot)$.
From now on, G is **always** a group.

Theorem 1.1
There is a unique identity element in G.

Theorem 1.2 Cancellation
Suppose $ba = ca$ for $a, b, c \in G$. Then $b = c$

Proof. Let $d \in G$ be an inverse for a, i.e. $da = ad = e$. Multiplying on the right by d, we obtain

$$\begin{aligned}(ba)d = (ca)d &\implies b(ad) = c(ad)\\ &\implies be = ce\\ &\implies b = c.\end{aligned}$$

□

Theorem 1.3 Uniqueness of Inverses
For every $a \in G$ there is a unique element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

Proof. Suppose $a \in G$ and $b, b' \in G$ are inverses of a, then

$$ba = e = b'a \implies b = b'$$

(by theorem 1.2) □

Example of inverses in different groups:

1. For $b \in \mathbb{R}^*$, $b^{-1} = \frac{1}{b}$.
2. For $b \in \mathbb{R}$ under addition $b^{-1} = -b$.
3. For $b \in \mathbb{Z}_n$, $b^{-1} = n - b$.

Example of groups using a field F:

1. $(F, +)$ is a group (Imitate $(\mathbb{R}, +)$).
2. $(F^*, \cdot)$ where $F^* = F^\dagger = \{a \in F : a \neq 0\}$ is a group. In particular, if p is a prime number, then $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ is a group.
3. The set of $m \times n$ matrices with entries in F, $M_{mn}(F)$ is a group under addition. When $n = 1$, $M_{m1}(F) = F^m$.
4. The set of invertible $m \times n$ matrices with entries in F, $GL(n, F) = \{A \in M_{mn}(F) : \det(A) \neq 0\}$ together with matrix multiplication is called (rank n) **general linear group** (over F). The identity matrix $I \in GL(n, F)$ is the identity. $\det(A) \neq 0 \implies \exists A^{-1} \in GL(n, F)$ such that $AA^{-1} = A^{-1}A = I$.

Example of the symmetries of the equilateral triangle:
Let $\sigma =$ flip through the vertical axis. Let $\rho =$ rotation by $\frac{2\pi}{3}$.
We can compose two symmetries, e.g., $\sigma\rho = \sigma \cdot \rho$.
We can show that the symmetries given by σ and ρ under composition are $\{e, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$ where $e =$ doing nothing.
We call this set D_3. It forms a group under composition. Clearly $\rho^3 = \rho\rho\rho = e$, $\sigma^2 = \sigma\sigma = e$, and $\sigma\rho\sigma = \rho^2 = \rho^{-1}$.

Definition of a dihedral group:
The **dihedral group** of order $2n$ is defined by

$$D_n = \{e, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}$$

where $p^n = e$, $\sigma^2 = e$, and $\sigma\rho\sigma = \rho^{-1}$. This is a group with the multiplication given by $\sigma\rho\sigma = \rho^{-1}$.

Remark: D_n is the group of symmetries of a regular n-gon.