Chapter 4

Cyclic groups

For any element $a \in G$ of a group G, we consider the powers $1, a, a^2, a^3, \ldots$ of a in the group G.

Definition 4.1. Let G be a group and $a \in G$ be an element of G. If there exists a positive integer m such that $a^m = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ times}} = 1$ then $a \in G$ is said to have *finite order*, and the *order* of $a \in G$ is defined to be the least such positive integer m. Otherwise, $a \in G$ is said to have *infinite order*.

Remark 4.2. Clearly, the order of the identity element 1 of any group G is 1.

Examples 4.3. (1) Consider the group $C_4 = \{1, -1, i, -i\}$ of the 4^{th} roots of unity. We have that

$$\begin{aligned}
1^1 &= 1 && \Rightarrow \quad 1 \ \text{ has order } 1, \\
(-1)^1 &= -1,\ (-1)^2 = 1 && \Rightarrow \quad -1 \text{ has order } 2, \\
i^1 &= i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1 && \Rightarrow \quad i \ \text{ has order } 4, \\
(-i)^1 &= -i,\ (-i)^2 = -1,\ (-i)^3 = i,\ (-i)^4 = 1 && \Rightarrow \quad -i \text{ has order } 4.
\end{aligned}$$

(2) Consider the group $\mathbb{Z}$ of integers under addition. We have that

$$2 = 2, \quad 2+2 = 4, \quad 2+2+2 = 6, \quad 2+2+2+2 = 8, \quad 2+2+2+2+2 = 10, \quad \ldots.$$

It is easy to see that there exists no positive integer m such that

$$\underbrace{2 + 2 + \cdots + 2}_{m \text{ times}} = 0.$$

Indeed, suppose that there exists a positive integer m such that this is the case. Then $2m = 0$, which gives that $m = 0$. This contradicts the assumption that m is a positive integer. Hence $2 \in \mathbb{Z}$ has infinite order.