Lectures in Group Theory

MOHAMMED ALABBOOD

University of Basrah-College of Science
Department of Mathematics

May 18, 2020

Invertible elements in a monoid

Definition: An element g in a monoid $(G, *)$ with identity e is called **invertible** if $\exists\, g' \in G : g * g' = g' * g = e$.
Remark: g' in the above definition (if exists) is called an **inverse** of g, and we will write $g' = g^{-1}$. The set of all invertible elements in a monoid $(G, *)$ is denoted by $G^{\times}$.
Example1: $(\mathbb{Z}, +)$ is monoids with identity 0, and $\mathbb{Z}^{\times} = \mathbb{Z}$.
Note that, for all $a \in \mathbb{Z} : a^{-1} = -a$.
Example2: $(\mathbb{Z}, \cdot)$ is monoids with identity 1, and $\mathbb{Z}^{\times} = \{-1, 1\}$.
Note that, $(-1) \cdot (-1) = 1 \cdot 1 = 1$.
Theorem: In a monoid $(G, *)$, the identity element is unique.
Proof: Let e, e' be two identities of G. Then $e' = e * e' = e' * e = e$ $\square$
Theorem: In a monoid $(G, *)$ with identity e, the inverse of $g \in G$ (if exists) is unique.
Proof: Let g', g'' be two inverses of g. Then $g * g' = g' * g = e = g * g'' = g'' * g$. So

$$g'' = g'' * e = g'' * (g * g') = (g'' * g) * g' = e * g' = g' \square$$

More examples

Example (Cancelation laws): In a monoid $(G, *)$ with identity e, if g is invertible, then for all $a, b \in G$:

$$a * g = b * g \text{ or } g * a = g * b \text{ implies } a = b.$$

Proof: Let $a * g = b * g$. Then

$$(a*g)*g^{-1} = (b*g)*g^{-1} \Rightarrow a*(g*g^{-1}) = b*(g*g^{-1}) \Rightarrow a*e = b*e \Rightarrow a = b.$$

Similarly, we can prove that $g * a = g * b \Rightarrow a = b$.

Example: In a monoid $(G, *)$ with identity e, if a, b are invertible elements. Then $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof: Let $A = a * b$ and $B = b^{-1} * a^{-1}$. It is enough to prove that $A * B = e = B * A$ and hence $A^{-1} = B$.

$$A * B = (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$
$$= a * e * a^{-1} = a * a^{-1} = e.$$

Similarly, we prove that $B * A = e$.

Groups

Definition: A monoid $(G, *)$ whose all elements are invertible is called a **group**.

Example1: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are groups.

Example2: $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$ and $(\mathbb{C}\backslash\{0\}, \cdot)$ are groups.

Example3: $(\mathbb{Z}\backslash\{0\}, \cdot)$ is a monoid, but it is not group.

Note that $2 \in \mathbb{Z}\backslash\{0\}$ is not invertible, that is, there is no $k \in \mathbb{Z}\backslash\{0\}$ such that $k \cdot 2 = 2 \cdot k = 1$.

Remark: Let G be a non-empty set, and $*$ is a binary operation on G. Then $(G, *)$ is a group if and only if

1. $\forall\, a, b \in G : a * b \in G$,
2. $\forall\, a, b, c \in G : a * (b * c) = (a * b) * c$,
3. $\exists\, e \in G : a * e = e * a = a \,\forall\, a \in G$.
4. $\forall\, a \in G \,\exists\, a' \in G$ (denoted by a^{-1}) $: a * a' = a' * a = e$.