

4. GROUPS

4.1. definition of group. A **semigroup** is a set with an associative binary operation. The way you say/write it is: $(S, *)$ is a semigroup. Or: S is a semigroup under the operation $*$. For example: The set of even integers is a semigroup under multiplication.

A **monoid** is a semigroup with an identity e . (Recall that the identity element e is unique if it exists.) For example, $(\mathbb{Z}^+, +)$ is a semigroup but not a monoid since the identity 0 is not in the set. On the other hand, \mathbb{Z}^+ is a monoid under multiplication since the multiplicative identity 1 is in the set \mathbb{Z}^+ . Note the two different wordings.

To get a group we need one more concept: the inverse.

Definition 4.1. Suppose that $(M, *)$ is a monoid with identity e . Then an **inverse** of an element $a \in M$ is defined to be an element $b \in M$ so that

$$a * b = b * a = e \quad (\text{the identity}).$$

Just like the identity, a can have at most one inverse.

Theorem 4.2. Suppose that $(M, *)$ is a monoid and $a \in M$. Then the inverse of a is unique if it exists.

Proof. Suppose that a has two inverses b, c . Then we will show that $b = c$.

Given that b is an inverse of a we get $b * a = e$. So:

$$(b * a) * c = e * c = c$$

Given that c is an inverse of a we get $a * c = e$. So:

$$b * (a * c) = b * e = b$$

By associativity of $*$, these are equal. So, $c = b$. □

Because the inverse is unique, we can write $b = a^{-1}$ if it exists.

Definition 4.3. A **group** is a pair $(G, *)$ where $*$ is a binary operation on G satisfying the following conditions.

G1. $*$ is **associative**. In other words, $(G, *)$ is a semigroup. I.e.,

$$(a * b) * c = a * (b * c)$$

for all $a, b, c \in G$.

G2. G contains an **identity** e . In other words, $(G, *)$ is a monoid.

$$e * x = x = x * e$$

for all $x \in G$.

G3. Every element of $a \in G$ has an inverse $b \in G$. I.e.,

$$(\forall a \in G)(\exists b \in G) a * b = e = b * a$$

We also say G is a group under $*$.

4.2. **examples.** Groups under addition. The following are groups.

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +)$$

The following sets are groups under multiplication:

$$\mathbb{Q}^+, \quad \mathbb{R}^+, \quad \mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$$

$GL(n, \mathbb{R})$ is the set of all $n \times n$ invertible matrices with real entries. This set forms a group under matrix multiplication.

G1 Matrix multiplication is associative. I won't prove that.

G2 I_n is the identity: $I_n A = A = A I_n$.

G3 We have inverses since we took only the invertible matrices!

There is one more property we need to show: **closure**: $a * b$ lies in the set. We need to verify that the product of two invertible matrices is invertible.

$$\begin{aligned} AB(B^{-1}A^{-1}) &= AI_n A^{-1} = AA^{-1} = I_n \\ \Rightarrow B^{-1}A^{-1} &= (AB)^{-1} \end{aligned}$$

Notation: I will switch to the standard notation ab instead of $a * b$.

4.3. **cancellation.** One of the main properties of groups is called the *cancellation property*.

Theorem 4.4. Suppose that G is a group and $a, b \in G$ are any two elements. Then there is a unique solution $x \in G$ to the equation

$$ax = b$$

In particular this means that

$$ax = ay \quad \Rightarrow \quad x = y$$

This is the *left cancellation rule*. What is the statement and proof of the right cancellation rule?

Proof. The solution of the equation $ax = b$ is $x = a^{-1}b$.

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

To see that this is the only solution, suppose that $ay = ax = b$. Then, multiplying both by a^{-1} on the left we get:

$$a^{-1}ay = a^{-1}ax$$

The LHS is $ey = y$ and the RHS is $ex = x$. So, $x = y$. □