FEBRUARY 6 NOTES

1. Section 2: Groups

We started class working through several problems related to Section 1. If you missed class, please take a look at Worksheet 1 and its solutions posted on Canvas.

Reminders from last time:

Definition 1.1. Let S be a set. A **binary operation $\star$ on S** is a function that associates to each ordered pair (s_1, s_2) of elements in S an element $s_1 \star s_2 \in S$. In function notation, a binary operation is a function

$$\star : S \times S \to S$$

$$(s_1, s_2) \mapsto s_1 \star s_2.$$

Definition 1.2. A binary operation $\star$ on a set S is **commutative** if, for every $s_1, s_2 \in S$,

$$s_1 \star s_2 = s_2 \star s_1.$$

It is **associative** if, for every $s_1, s_2, s_3 \in S$,

$$(s_1 \star s_2) \star s_3 = s_1 \star (s_2 \star s_3).$$

We now define the main object of study in this class, a *group*.

Definition 1.3. A **group** is a set G with a binary operation $\star$ on G such that:

(1) (associativity) $\star$ is associative, i.e. for every $x, y, z \in G$,

$$(x \star y) \star z = x \star (y \star z).$$

(2) (identity) there is an element $e \in G$ such that, for any $x \in G$,

$$x \star e = e \star x = x.$$

The element $e \in G$ is called the **identity element** or **identity of** G.

(3) (inverses) for each element $x \in G$, there is an element $y \in G$ such that

$$x \star y = y \star x = e.$$

The element y is called the **inverse** of x and is denoted by $y = x^{-1}$ or $y = -x$, depending on the context.

We denote groups by $(G, \star)$ or just by G if $\star$ is 'clear from context.'

For a general group G, $\star$ does not have to be commutative. We have a special name for the groups where $\star$ is commutative.

Definition 1.4. If $(G, \star)$ is a group and $\star$ is commutative, then G is called an **abelian** group.

Example 1.5. $(\mathbb{Z}, +)$ is a group. We will prove this by verifying the axioms.

(1) The operation $+$ is a binary operation on $\mathbb{Z}$ and it is associative: for any $x, y, z \in \mathbb{Z}$, we have $(x + y) + z = x + (y + z)$.
(2) There is an identity element in $\mathbb{Z}$ called 0: $0 + x = x + 0 = x$ for any $x \in \mathbb{Z}$.
(3) Every $x \in \mathbb{Z}$ has an inverse $-x \in \mathbb{Z}$ satisfying $x + (-x) = (-x) + x = 0$.

Because all of the axioms are true, $(\mathbb{Z}, +)$ is a group. Because addition is commutative, it is an abelian group. Similarly, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are abelian groups.

Example 1.6. $(\mathbb{Z}, \times)$ is **not** a group. We know $\times$ is associative, so the binary operation is associative, and there is an identity element 1 satisfying $1 \times x = x \times 1 = x$ for any $x \in \mathbb{Z}$. *However,* not all elements have inverses. The inverse of $x \in \mathbb{Z}$ must be some element $y \in \mathbb{Z}$ such that $x \times y = 1$. If $x = 2$, then this has *no inverse* because there is no element $y \in \mathbb{Z}$ such that $2 \times y = 1$.

Example 1.7. $(\mathbb{Q}, \times)$ is **not** a group. As above, $\times$ is associative and the identity is 1. *However,* still not all elements have inverses. The inverse of $x \in \mathbb{Z}$ must be some element $y \in \mathbb{Z}$ such that $x \times y = 1$. If $x = 0$, then this has *no inverse* because there is no element $y \in \mathbb{Z}$ such that $0 \times y = 1$.

However, if we remove 0 in some way, we do get a group: for example, $(\mathbb{Q}^+, \times)$ is a group. We already know $\times$ is associative and the identity is 1, and for any $x \in \mathbb{Q}^+$, the number $1/x \in \mathbb{Q}^+$ is the inverse: $x \times 1/x = 1/x \times x = 1$.

In general, to show something is a group, check the three properties *in order*. To show something is not a group, you must show that one of the properties is not true by giving a counterexample.