FEBRUARY 13 NOTES

1. Section 3: Fundamental Theorems About Groups

Today, we're going to prove several results about groups. Recall the definition of a group:

Definition 1.1. 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.

There are several things that *follow* from this definition, i.e. several properties of groups that we can prove with just these three axioms.

Theorem 1.2. *Suppose $(G, \star)$ is a group. The identity element $e \in G$ is unique.*

Before the proof, some commentary on uniqueness: when we say something like 'the identity is unique' we mean that there is only *one* element $e \in G$ satisfying the identity axiom. To prove a statement like this, we want to assume that there exist two elements satisfying the property, and then prove those elements are the same.

Proof. Suppose $e, e' \in G$ are two elements satisfying $e \star x = x \star e = x$ and $e' \star x = x \star e' = x$ for all $x \in G$. Using the first equation with $x = e'$, we see that
$$e \star e' = e' \star e = e'$$
and from the second equation with $x = e$, we see that
$$e' \star e = e \star e' = e$$
and therefore $e = e \star e' = e'$ so $e = e'$. $\square$

Theorem 1.3. *Suppose $(G, \star)$ is a group and $x \in G$ is any element. Then, the inverse of x is unique.*

Proof. Suppose $x \in G$ and there exists two elements y, y' such that $x \star y = y \star x = e$ and $x \star y' = y' \star x = e$. These equations imply that
$$x \star y = x \star y'.$$

Now, we'll algebraically manipulate this to conclude that $y = y'$, first starring both sides with y on the left:

$$\begin{aligned} & y \star (x \star y) = y \star (x \star y') \\ & \implies (y \star x) \star y = (y \star x) \star y' \qquad \text{by associativity} \\ & \implies e \star y = e \star y' \qquad \text{by the definition of inverse} \\ & \implies y = y' \qquad \text{by definition of identity} \end{aligned}$$

Therefore, $y = y'$ so the inverse of x is unique. □

Theorem 1.4. *If $(G, \star)$ is a group and $x \in G$, then $(x^{-1})^{-1} = x$. (In words: the inverse of x^{-1} is just x.)*

Proof. The previous theorem tells us that inverses are unique, so we must only verify that x satisfies the necessary property to be the inverse of x^{-1}. But, because x^{-1} is the inverse of x, we know $x^{-1} \star x = x \star x^{-1} = e$, so x satisfies the property to be the inverse of x^{-1}. □

We will now draw a consequence of the previous Theorem. Results that are consequences of things we've already shown are called *corollaries.*

Corollary 1.5. Suppose $(G < \star)$ is a group. If $x_1, x_2 \in G$ such that $x_1^{-1} = x_2^{-1}$, then $x_1 = x_2$. In other words, no two *different* elements can have the same inverse.

Proof. If $x_1^{-1} = x_2^{-1}$, then $(x_1^{-1})^{-1} = (x_2^{-1})^{-1}$, so by the previous theorem, $x_1 = x_2$. □

Theorem 1.6. *If $(G, \star)$ is a group and $x, y \in G$, then $(x \star y)^{-1} = y^{-1} \star x^{-1}$.*

Proof. We prove this again by verifying the inverse property. We must show that $(x \star y) \star (y^{-1} \star x^{-1}) = e$ and similarly $(y^{-1} \star x^{-1}) \star (x \star y) = e$. We'll verify the first equation together and leave the second one as an exercise. We compute:

$$\begin{aligned} (x \star y) \star (y^{-1} \star x^{-1}) &= ((x \star y) \star y^{-1}) \star x^{-1} \qquad \text{by associativity} \\ &= (x \star (y \star y^{-1})) \star x^{-1} \qquad \text{by associativity} \\ &= (x \star e) \star x^{-1} \qquad \text{by definition of inverse} \\ &= x \star x^{-1} \qquad \text{by definition of identity} \\ &= e \qquad \text{by definition of inverse} \end{aligned}$$

Therefore, we have shown that $(x \star y) \star (y^{-1} \star x^{-1}) = e$. Similarly, one can show that $(y^{-1} \star x^{-1}) \star (x \star y) = e$ and therefore $y^{-1} \star x^{-1}$ is the inverse of $x \star y$. □

Are you tired of checking two equalities to prove the identity and inverse properties? Let's show that it suffices to only check one. First, a definition:

Definition 1.7. If $(G, \star)$ is a group and $x \in G$, an element $y \in G$ such that $x \star y = e$ is called a **right inverse** of x. If $y \star x = e$, then y is called a **left inverse** of x.

Theorem 1.8. *Suppose $(G, \star)$ is a group and $x \in G$. If there exists $y \in G$ such that $x \star y = e$ or $y \star x = e$, then $y = x^{-1}$.*

Proof. Suppose first that $x \star y = e$. We know there exists some element x^{-1} in G, and we want to show that $y = x^{-1}$. If we star both sides of the equation $x \star y = e$ on the left with x^{-1}, we can algebraically manipulate this:

$$\begin{aligned}
&x^{-1} \star (x \star y) = x^{-1} \star e \\
&\implies (x^{-1} \star x) \star y = x^{-1} \qquad \text{by associativity and definition of identity} \\
&\implies e \star y = x^{-1} \qquad \text{by definition of inverse} \\
&\implies y = x^{-1} \qquad \text{by definition of identity}
\end{aligned}$$

and therefore $y = x^{-1}$.

Similarly, if we start with $y \star x = e$, we can star both sides on the right with x^{-1} to conclude that $y = x^{-1}$. □

This theorem tells us that, if $y \in G$ is a left *or* right inverse of $x \in G$, then y is actually the inverse of x. So, to verify any element is an inverse, you just need to verify that $x \star y = e$ or $y \star x = e$ (not both!).

Example 1.9. In linear algebra, you learned to find the inverse of a matrix $A \in GL_n(\mathbb{R})$ by solving the equation $AB = I$ for B. This method computes a *right* inverse for A, but because $(GL_n(\mathbb{R}), \times)$ is a group, this right inverse is actually the *inverse*, i.e. $AB = I$ *and* $BA = I$ (even though we never checked the equation $BA = I$).

This method of proof can be used more generally to prove something on your homework:

Theorem 1.10 (The Cancellation Laws.)**.** *Suppose $(G, \star)$ is a group and $x, y, z \in G$.*

(1) If $x \star y = x \star z$, then $y = z$.
(2) If $x \star y = z \star y$, then $x = z$.

Definition 1.11. If G is a set with binary operation $\star$ and $e \in G$ an element such that $x \star e = x$ for all $x \in G$, then e is called a **right identity.** If $e \star x = x$ for all $x \in G$, then e is called a **left identity.**

Theorem 1.12. *Suppose G is a set with associative binary operation $\star$. If $e \in G$ is a right identity (respectively, left) and every element $x \in G$ has a right inverse (respectively, left), then e is both a left and right identity and the inverses are both left and right inverses. Therefore, G is a group.*

Proof. We will prove this assuming that e is a right identity and that every element $x \in G$ has a right inverse, i.e. an element x^{-1} such that $x \star x^{-1} = e$ (the left case is similar). Suppose that $x \star e = x$ for all $x \in G$. We need to show that $e \star x = x$.

Starting with the equation $x \star e = x$, if $x = e$, we obtain $e \star e = e$. Because x has a right inverse x^{-1}, we know that $x \star x^{-1} = e$. If we plug this in for the second and third e in the equation $e \star e = e$, we get

$$e \star (x \star x^{-1}) = x \star x^{-1}.$$

Now, using associativity, we know this implies

$$(e \star x) \star x^{-1} = x \star x^{-1}.$$

Now, let's multiply both sides by the right inverse of x^{-1}, use associativity, and then the definition of inverse to conclude $(e \star x) \star e = x \star e$. Using that e was the right identity, this implies that $e \star x = x$.

So, only assuming that G has a right identity and every element has a right inverse, we've shown that the right identity is in fact a two-sided identity. Now, we need to show that, if x^{-1} is the right inverse of x, then $x^{-1} \star x = e$. This will show that x^{-1} is actually the left inverse of x and therefore a two-sided inverse. We know x^{-1} has some right inverse, which we will call y, such that $x^{-1} \star y = e$. So, we want to show that $x = y$. But, because $x \star x^{-1} = e$, we know $(x \star x^{-1}) \star y = e \star y$. Using associativity and the definition of right inverse and the right identity property of e, the left hand side becomes x. Because we already proved that e was a two-sided identity, the right hand side is just y, so we conclude $x = y$. Therefore, $x \star x^{-1} = x^{-1} \star x = e$ and we have shown that G is a group! $\square$

What is the point of everything we just did? We could in fact re-define a group:

Definition 1.13. A group G is a set with associative binary operation $\star$ such that G has a *right* identity element and every element $x \in G$ has a *right* inverse.

Equivalently, one could replace both 'rights' by 'lefts.'

In words, this is saying that you don't need to check both equations to show something is an inverse or an identity; it suffices to check just one for each.