"Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it's the only thing that ever has." – Margaret Mead

LECTURE 9

GROUPS PROPERTIES

ANDREW MISSELDINE

3.2. Definitions and Examples

Definition 3.2.16. The **order** of a group $(G, \circ)$ is the cardinality of the set $|G|$.

Example 3.2.17. The group $\mathbb{Z}_n$ under addition has order $|\mathbb{Z}_n| = n$ and the group S_n has order $|S_n| = n!$. These are both examples of **finite groups**. The groups $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under addition are all examples of groups with infinite order, which we call **infinite groups**. ■

We will now prove some very important properties about all groups. When working with generic groups multiplicative structure is used almost always. For example, we will denote $g \circ h$ in G simplify as gh and the inverse of g as g^{-1}. Also, we will use exponential notation to represent iterated products: $g^n = \underbrace{g \cdot g \cdots g}_{n \text{ times}}$ and $g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$. Although we will primarily use e for the identity of G, we might sometimes use $1 \in G$ as the identity element. In fact, we are justified in saying "the" identity elements because it is unique.

Proposition 3.2.18. *The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.*

Proof. Let $e', e'' \in G$ such that $ge' = e'g = g$ and $ge'' = e''g = g$ for all $g \in G$. Then

$$e' = e'e'' = e''.$$

□

Likewise, we can say "the" inverse of $g \in G$ since inverses are also unique.

Proposition 3.2.19. *If g is any element in a group G, then the inverse of g is unique.*

Proof. Let $g', g'' \in G$ such that $gg' = g'g = e$ and $gg'' = g''g = e$. Then

$$g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g''.$$

□

Proposition 3.2.20. *Let G be a group. For any $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.*

Proof. Since inverses are unique in groups, as shown above, it suffices to show that $h^{-1}g^{-1}$ acts like an inverse to $(gh)^{-1}$. If $h^{-1}g^{-1}$ does act like an inverse to $(gh)^{-1}$ then uniqueness of inverses demand that $(gh)^{-1} = h^{-1}g^{-1}$. Note that

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g(e)g^{-1} = gg^{-1} = e.$$

Similarly, $(h^{-1}g^{-1})(gh) = e$. Therefore, $h^{-1}g^{-1}$ is the inverse of gh. □

Proposition 3.2.21. *Let G be a group. For any $g \in G$, $(g^{-1})^{-1} = g$.*

Proof. Since inverses are unique in groups, as shown above, it suffices to show that g acts like an inverse to g^{-1}, like the previous proof. Note that

$$gg^{-1} = e = g^{-1}g.$$

Therefore, g is the inverse of g^{-1}. □

Proposition 3.2.22 (Cancellation Laws)**.** *If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.*

Proof. We will prove the case that $ab = ac$ implies that $b = c$. Multiplying both sides of the equation on the left by a^{-1} then gives

$$a^{-1}(ab) = a^{-1}(ac) \quad \Rightarrow \quad (a^{-1}a)b = (a^{-1}a)c \quad \Rightarrow \quad eb = ec \quad \Rightarrow \quad b = c.$$

The case of $ba = ca$ is handled similarly. □

This proposition tells us that the **right** and **left cancellation laws** are true in all groups. In fact, the above proof used all three axioms of group theory: associativity, identity, and inverses, to prove the cancellation laws. In some regard, any algebraic object with cancellation must be group-like.

Proposition 3.2.23. *Let G be a group and $a, b \in G$. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.*

Proof. We will prove the case that $ax = b$ has a unique solution in G. Note that $x = a^{-1}b$ is a solution the equation since

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

This shows existence of a solution. For uniqueness, if x and y are both solutions to the above equation, then $ax = b = ay$. Canceling a on the left gives $x = y$. Thus, $ax = b$ has a unique solution in G. The case of $xa = b$ is handled similarly. □

Again, we should emphasize that in the above proof we used all three axioms of group theory to solve equations. Groups are exactly the setting where we solve equations in the manner we first learned in algebra class.

Proposition 3.2.24 (Exponential Laws)**.** *In a group G, the usual exponent laws hold; that is, for all $g, h \in G$ and $m, n \in \mathbb{Z}$,*

(a) $g^m g^n = g^{m+n}$

(b) $(g^m)^n = g^{mn}$

(c) $(gh)^n = (h^{-1}g^{-1})^{-n}$. *Furthermore, if G is Abelian, then $(gh)^n = g^n h^n$.*

The proof of the above exponent laws follows from the associativity of the group and an (double) induction argument. It should be emphasized that, in general, $(gh)^n \neq g^n h^n$ in groups and commutativity in some form is needed for equality.

In fact, when a group is Abelian, additive notation is often used instead of multiplicative notation. For example, we will denote $g \circ h$ in G simplify as $g + h$ and the inverse of g as $-g$. Also, we will use multiplicative notation to represent iterated products: $ng = \underbrace{g + g + \ldots + g}_{n \text{ times}}$ and $-ng = \underbrace{-g + -g + \ldots + -g}_{n \text{ times}}$. Although we will primarily use e for the identity of G, we might sometimes use $0 \in G$ as the identity element. The three "exponent laws" look like distributive laws for additive groups: for $g, h \in G$ and $m, n \in \mathbb{Z}$, we have

(a) $mg + ng = (m + n)g$

(b) $m(ng) = (mn)g$

(c) $m(g + h) = mg + mh$.

Homework:
Judson 3.5: Pick 3 (27-30, 49), Pick 2 (31-33, 51)