"Individual commitment to a group effort - that is what makes a team work, a company work, a society work, a civilization work." – Vince Lombardi

LECTURE 7

GROUPS

ANDREW MISSELDINE

3.2. Definitions and Examples

In this chapter we introduce the most fundamental and most important structure in abstract algebra, the group.

Definition 3.2.1. A **binary operation** $\circ$ on a set G is a function $\circ : G \times G \to G$. For an element $(a,b) \in G \times G$, the image of (a,b) under $\circ$ is denoted $a \circ b$ (or just juxtaposition ab when the operation is clear from context), that is, $(a,b) \mapsto a \circ b$. We will use the notation $(G, \circ)$ to denote that G is a set and $\circ$ a binary operation on G.

Example 3.2.2. Addition and multiplication are binary operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Addition and multiplication also are binary operations on $\mathbb{Z}_n$, the set of congruence classes modulo n.

Vector addition is a binary operation on $\mathbb{R}^n$. On the other hand, scalar multiplication of vectors is not a binary operation because it is a product of a scalar and a vector producing a vector, $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$. To be a binary operation, the two factors and the product must all be elements of the same set. Likewise, the dot product of two vectors is not a binary operation since it is a function of the form $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, that is, the product is not a vector but a scalar. Conversely, the cross product on $\mathbb{R}^3$ is a binary operation $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ since the product of two vectors is a vector.

Matrix multiplication is a binary operation on the set of $n \times n$ matrices with real scalars, $M_n(\mathbb{R})$, but not on the set of all matrices because the product of two matrices might be undefined if the dimensions are incompatible. This is just a special case of function composition. Recall that B^A is the set of all functions of the form $f : A \to B$. Then while function composition does not form a binary operation for all functions since many composites are undefined, it does form a binary operation on X^X, that is, on functions of the form $f : X \to X$. ∎

Definition 3.2.3. When a binary operation $\circ$ is defined on a set X, we say that a subset $Y \subseteq X$ is **closed** under $\circ$ if the restriction of $\circ$ to Y forms a binary operation on Y, that is, if $a, b \in Y$ then $a \circ b \in Y$.

Example 3.2.4. Subtraction is a binary operation for $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Note that subtraction is NOT a binary operation for $\mathbb{N}$ since the difference of two natural numbers need not be a natural number, e.g. $3 - 7 = -4 \notin \mathbb{N}$. In other words, $\mathbb{N}$ is not closed under subtraction.

Division is not a binary operation for $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, nor $\mathbb{C}$ since division by zero is undefined. Let $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ denote the subset of nonzero numbers of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. Then division is a binary operation on $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$, but not a binary operation for $\mathbb{Z}^*$ since the quotient of two integers need not be a nonzero integer, e.g. $1 \div 2 = \dfrac{1}{2} \notin \mathbb{Z}^*$. Thus, $\mathbb{Z}^*$ is not closed under division.

The set of permutations S_X is closed under composition inside of X^X. In this case, function composition is typically called permutation multiplication. ∎

Definition 3.2.5. We say that $(G, \circ)$ is a **group** if the following three axioms are satisfied by the binary operation:

(a) (**associativity**) For all $g, h, k \in G$, it holds that
$$g \circ (h \circ k) = (g \circ h) \circ k.$$
(b) (**identity**) There exists an element $e \in G$ such that for all $g \in G$ we have
$$g \circ e = e \circ g = g.$$
(c) (**inverses**) For all $g \in G$ there is an element $g^{-1} \in G$ such that
$$g \circ g^{-1} = g^{-1} \circ g = e.$$

When the binary operation $\circ$ is clear from context, we will say that G is a group instead of $(G, \circ)$.

Furthermore, we say G is an **Abelian group** if G is a group which satisfies an additional axiom:

(d) (**commutativity**) For all $g, h \in G$, it holds that
$$g \circ h = h \circ g.$$

For Abelian groups, the operation is often denoted as $+$, the identity as 0, and the inverse of a as $-a$.

Example 3.2.6. The structures $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all Abelian groups, where the identity element is 0 and the inverse of x is just $-x$. The structure $(\mathbb{N}, +)$ is not a group because not all elements have an additive inverse, e.g. $-1 \notin \mathbb{N}$. The set $\mathbb{Z}^+$ of positive integers with addition is also not a group since it has no identity element.

Similarly, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are all Abelian groups, where the identity element is 1 and the inverse of x is just $1/x$, but $(\mathbb{N}^*, \cdot)$ and $(\mathbb{Z}^*, \cdot)$ are not because not all elements have inverses.

The structures $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, and $(\mathbb{C}, -)$ are not groups. Although each set has an identity[†] and all elements have inverses, the operation is not associative. Note that $3 - (2 - 1) = 3 - 1 = 2 \neq 0 = 1 - 1 = (3 - 2) - 1$. Of course, the operation of subtraction is noncommutative.

The structure $(X^X, \circ)$ where $\circ$ is just function composition and $(S_X, \circ)$ with permutation multiplication (function composition) are both non-Abelian groups since their binary operation is noncommutative. The group S_X is called the **symmetric group** on X. ∎

Example 3.2.7. The set of congruence classes modulo n, $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ is an Abelian group under addition. The identity element of $\mathbb{Z}_n$ is the congruence class of all multiples of n, namely $[0]$. For a congruence class $[k]$, the inverse is the class $[-k]$. The fact that addition is associative and commutative is an immediate consequence of associativity and commutativity on $(\mathbb{Z}, +)$ and the division algorithm.

When working with $\mathbb{Z}_n$, it is common to identify a class $[k]$ with its unique representative between 0 and n, that is, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$ and $k + \ell$ is the unique representative of $[k + \ell]$ between 0 and n. With this notation, the identity of $\mathbb{Z}_n$ is 0 and the inverse of k is $n - k$.

Let $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ (the book uses the notation $U(n)$ to denote the set of **units** in $\mathbb{Z}_n$). Then $(\mathbb{Z}_n^*, \cdot)$ is also an Abelian group where the identity is 1. The Euclidean algorithm is used to compute inverses in this group because it computes a linear combination $ak + bn = 1$ which implies that $ak = 1 - bn$, that is, $ak \equiv 1 \pmod{n}$. Thus, $a = k^{-1}$. ∎

[†]Actually, these algebraic structures only have a **right identity**, that is, an element e such that $g \circ e = g, \forall g \in G$. Similarly, we can define a **left identity** as an element e such that $e \circ g, \forall g \in G$. A left- or right-identity is called a **one-sided identity**. The identity defined in Definition 3.2.5 could more precisely be called a **two-sided identity**. It can be proven that with an associative operation, a one-sided identity is necessarily a two-sided identity is unique. Analogous definitions and statement can be said about one- and two-sided inverses.

The importance of the group structure is that groups are exactly the setting where we can solve equations.

Example 3.2.8. Solve the equation $2x + 1 \equiv 5 \pmod 7$ for x.

To begin we apply the additive inverse of 1 to both sides of the equation:

$$\begin{aligned} (2x+1)+(-1) &\equiv 5+(-1) \pmod 7 \\ 2x+(1+(-1)) &\equiv 4 \pmod 7 \\ 2x+0 &\equiv 4 \pmod 7 \\ 2x &\equiv 4 \pmod 7 \end{aligned}$$

Notice that to "move" 1 to the other side of the equation we used inverses, associativity, and identity.

The Euclidean algorithm (or guess-and-check) can be used to show that $(4)2 + (-1)7 = 1$. Thus, $2^{-1} \equiv 4 \pmod 7$.

$$\begin{aligned} (4)(2x) &\equiv 4(4) \pmod 7 \\ (4 \cdot 2)x &\equiv 16 \pmod 7 \\ 8x &\equiv 16 \pmod 7 \\ x &\equiv \boxed{2} \pmod 7 \end{aligned}$$

■

Homework:
Judson 3.5 : 1, Pick 2 (7, 10, 12-14), Pick 2 (19-24)