CSCI 698 Teaching Notes

Matin Amini

1 Abstract Algebra (Group Theory) Introduction

Throughout different parts of mathematics, common structures seem to appear everywhere. Abstract algebra aims to provide a theory to capture the properties of such structures. One area of abstract algebra is group theory. Before diving into formal definition, let us see some structures from different parts of mathematics.

$$(\mathbb{R}, +), (\mathbb{R} - \{\}, \times), (\mathbb{GL}_n(\mathbb{R}), .), (Perm_n, \circ)$$

Each of the tuples show a set with a pairwise operation defined over that set. The first example $\mathbb{R}$ denotes the real numbers with the operation of addition. The second example is real numbers except zero with the operation of multiplication. The third example $\mathbb{GL}_n(\mathbb{R}$ denotes all $n \times n$ real entries invertible matrices with the operation of matrix multiplication. At last, $Perm_n$ denotes all permutations over $\{1, \ldots, n\}$ with the operation of function composition.

Note that each of these operations are closed with respect to their sets: adding to real numbers yields a real number, multiplying two nonzero real numbers yields a nonzero real number, multiplying two $n \times n$ invertible matrices yields an $n \times n$ invertible matrix and composing two permutations over $\{1, \ldots, n\}$ yields a permutation over $\{1, \ldots, n\}$ (as they are both injective and surjective functions).

The first property we discuss is associativity. A function $f : A \times A \to A$ is associative if for all $a, b, c \in A$, we have $f(a, f(b, c)) = f(f(a, b), c)$. One could see that subtraction is not an associative property for example: $3 - (5 - 7) \neq (3 - 5) - 7$. Observe that addition, multiplication, matrix multiplication and function composition are all well known associative properties.

$$a, b, c \in \mathbb{R} \implies (a + b) + c = a + (b + c)$$
$$a, b, c \in \mathbb{R} - \{0\} \implies (ab)c = a(bc)$$
$$M_1, M_2, M_3 \in \mathbb{GL}_n(\mathbb{R}) \implies M_1(M_2M_3) = (M_1M_2)M_3$$
$$\sigma_1, \sigma_2, \sigma_3 \in Perm_n \implies \sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$$

The second property is that each of these sets contains an identity element. A function $f : A \times A \to A$ has an identity element if there exists $e \in A$ such that $f(a, e) = f(e, a) = a$ for all $a \in A$. For example addition over positive integers does not have an identity element (since the only identity element for addition is 0). We can see that all our examples have an identity element.

$$a \in \mathbb{R} \implies a + 0 = 0 + a = a$$
$$a \in \mathbb{R} - \{0\} \implies a \times 1 = 1 \times a = a$$
$$M \in \mathbb{GL}_n(\mathbb{R}) \implies MI_n = I_nM = M$$
$$\sigma \in Perm_n \implies \sigma \circ id = id \circ \sigma = \sigma$$

where $I_n \in \mathbb{GL}_n(\mathbb{R})$ is the $n \times n$ identity matrix and $id : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is the identity permutation taking each element to itself.

The third property is that each element has an inverse with respect to the pairwise operation in the set. $a \in A$ has an inverse with respect to $f : A \times A \to A$ if there exists $b \in A$ such that $f(a, b) = f(b, a) = e$ where e is the identity element in A with respect to f. For example, addition over the set of nonnegative real numbers has an identity element but only 0 has an inverse with respect to addition in that set. Again, in all of our examples, all elements have an inverse.

$$a \in \mathbb{R} \implies -a \in \mathbb{R} \wedge a + (-a) = -a + a = 0$$

$$a \in \mathbb{R} - \{0\} \implies \frac{1}{a} \in \mathbb{R} - \{0\} \wedge \frac{1}{a} \times a = a \times \frac{1}{a} = 1$$
$$M \in \mathbb{GL}_n(\mathbb{R}) \implies M^{-1} \in \mathbb{GL}_n(\mathbb{R}) \wedge MM^{-1} = M^{-1}M = I_n$$
$$\sigma \in Perm_n \implies \sigma^{-1} \in Perm_n \wedge \sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = id$$

M^{-1} exists because $M \in \mathbb{GL}_n(\mathbb{R})$ and since M^{-1} is also invertible and $n \times n$ we have $M^{-1} \in \mathbb{GL}_n(\mathbb{R})$. Also each permutation has an inverse with the same domain because it is injective and surjective and we can easily see that the inverse is also a permutation and in $Perm_n$.

Now we are ready to define groups: A set G with a pairwise operation . over G is a a group if . is associative, there exists an identity element in G with respect to . and each element in G has an inverse in G with respect to . operation. These structures are next to ubiquitous in different areas of mathematics.

Let us see a simple example of a theorem in group theory.

Theorem 1. *If a group $(G, .)$ is finite with size $|G| = n$, each $g \in G$ has a nonnegative integer order denoted by $o(g)$ where if $o(g) = m$ then m is the smallest element such that $g^m = e$ (e is the identity and such m must exist) and g^m just denotes $m - 1$ times application of . for $m > 1$ and $g^1 = a, g^0 = e$. Furthermore $o(g)|n$ for all $g \in G$*

That means that in finite groups applying . to one element enough number of times will yield the identity. Furthermore $o(g)$ always divides the size of the group in finite groups. Particular application in our example would be that applying a permutation enough number of times will yield the identity permutation. Moreover $o(\sigma)|n!$ since $|Perm_n| = n!$.

References