Group Theory

Jonathan Gribbins

Contents

1 Introduction to Groups

1.1 Basic Axioms

A group is one of the fundamental algebraic objects studied in abstract algebra. Groups are sets coupled with a binary operation in the ordered pair $(G, \star)$, where $\star$ is a **binary operation**—

(1) A *binary operation* is a function on a set G mapping $G \times G$ to G: $\star : G \times G \to G$. This operation upon an ordered pair in G is denoted $\star(a, b)$ for $a, b \in G$.

(2) A binary operation is *associative* if for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

(3) Two elements $a, b \in G$ *commute* if $a \star b = b \star a$. A binary operation is *commutative* if $\forall a, b \in G, a \star b = b \star a$.

A **group** is an ordered pair of a set and a binary operation upon this set $(G, \star)$ such that three axioms are fulfilled:

(1) G is **associative**, so for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

(2) There is some element $e \in G$ such that for all elements $a \in G$, $a \star e = a$.

(3) For all $a \in G$, there is some element $a^{-1} \in G$ such that $a \star a^{-1} = e$.

A group G is called **abelian** or **commutative** if for all $a, b \in G$, $a \star b = b \star a$.

It can be shown that for any group G under binary operation $\star$,

(1) The identity (e) of G is unique.

(2) For each $a \in G$, a^{-1} is unique.

(3) $(a^{-1})^{-1} = a$ for all $a \in G$.

(4) $(a \star b)^{-1} = (b)^{-1} \star (a)^{-1}$.

(5) For any $a_1, a_2, a_3, ...a_n \in G$, the value of $a_1 \star a_2 \star a_3 \star ... \star a_n$ does not vary based on parentheses or brackets.

Because of **(5)**, for any element $a \in G$, the product of $n \in Z^+$ as $(a \star a \star a...(ntimes))$ can be denoted a^n. Additionally, if we let a be the inverse x^{-1} of an element $x \in G$, we would denote the nth product of x^{-1} as x^{-n}. The identity of a group G can be denoted a^0 for all $a \in G$.

Order of an element $x \in G$: The order of an element $x \in G$ is the *smallest positive integer* n such that $x^n = 1$ (where is the identity of G). This integer is also denoted $|x|$. If there is no integer n such that $x^n = 1$, x is said to be of infinite order.

Cayley table of group G The *Cayley, multiplication, or group table* of a finite group $G = \{g_1, g_2, g_3, ...g_n\}$ is an $n \times n$ table where the entry at location (i, j) in the table is equal to $g_i g_j$.

1.2 Dihedral Groups

Dihedral groups are groups that describe the symmetries of simple planar polygons. For all $n \in Z^+$ with $n \geq 3$, the *dihedral group* D_{2n} is the group that describes its symmetries. A **symmetry** of an n-gon is a *rigid motion on the n-gon that leaves the n-gon in the same "orientation" (non-pointwise) of the original n-gon.*

Formally, these symmetries are described as permutations upon the vertices of the n-gon, described by the set $\{1, 2, 3, ..., n\}$. A symmetry s that moves the vertex i from its original position to the position of (arbitrary) vertex j, then the *permutation* σ sends i to j, and moves the rest of the vertices with the same permutation.

For instance, if s is the symmetry describing the rotation of an n-gon by $2\pi/n$ radians, then the permutation σ sends each element $i \in \{1, 2, 3, ..., n\}; i > n$ to $i + 1$, and sends n to 1.

For D_{2n} and any symmetries $s, t \in D_{2n}$, st is the symmetry resulting after applying t then s to the n-gon. Symmetries on a n-gon are functions on the n-gon, so the combination of these symmetries is just function composition—as a result, they are inherently associative. The inverse of a symmetry in D_{2n} is the symmetry that "reverses" the actions that the original symmetry wrought upon the n-gon.

$$|D_{2n}| = 2n,$$

so the group D_{2n} is generally called the *dihedral group of order 2n.* If r describes a rotation of an n-gon one-n^{th} way around the n-gon, and s describes a flip about a line bisecting the first vertex, the some rules of these elements of D_{2n} are

(1) $1, r, r^2, ..., r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.

(2) $|s| = 2$.

(3) For any i, $s \neq r^i$.

(4) $sr^i \neq sr^j$ for any $0 \geq i, j \geq n - 1; i \neq j$, so

$$D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}.$$

Each element in D_{2n} can be *uniquely expressed by* $s^k r^i$ with $k = 0 or 1$ and $0 \geq i \geq n - 1$.

(5) $r^i s = sr^{-i}$ for all $0 \geq i \geq n$.

Based on these rules, any element of D_{2n} can be expressed in terms of r and s only—because of this fact, we call r and s **generators** of the group D_{2n}. Formally speaking, a subset $S \subseteq G$ with the property that *every element of* G *can be written as a finite product of elements of* S *and their inverses* is said to be a **generator** of G, and **generates** G. For instance, the set $\{1\}$ generates the set Z of all integers because all integers can be expressed as a finite sum of $+1$s and -1s.

The set S that generates a group G can be notated by $G = \langle S \rangle$, which is read G *is the set generated by* S. For D_{2n}, the set $S = \{r, s\}$ generates D_{2n}, so

$$D_{2n} = \langle S \rangle = \langle \{r, s\} \rangle.$$

Any equation satisfied by the generators in a group are called **relations**. For D_{2n}, $S = \{r, s\}$, $r^n = 1$, $s^2 = 1$, and $rs = sr^{-1}$ are the relations of D_{2n}.

If a group is generated by a set S and some relations in that set, $R_1, R_2, R_3, ..., R_n$, then the group can be shown as a **presentation** of S and the relations as

$$G = \langle S | R_1, R_2, R_3, ..., R_n \rangle.$$

For D_{2n}, one presentation is

$$D_{2n} = \langle r, s | r^n = 1, s^2 = 1, rs = sr^{-1} \rangle.$$

These presentations are very useful for determining certain properties of a group, as they can usually be applied to find implicit relations that are not outright stated.

1.3 Symmetry Groups

Let Ω be some non-empty set and let S_Ω be the set of bijections mapping from $\Omega \to \Omega$. S_Ω is a group under function composition, as for some permutations $\sigma, \tau \in S_\Omega$, $\sigma : \Omega \to \Omega$ and $\tau : \Omega \to \Omega$, so $\sigma \circ \tau : \Omega \to \Omega$ and $\tau \circ \sigma : \Omega \to \Omega$ by the rules of composition of bijections. For any permutation $\sigma \in S_\Omega$, there is some $\sigma^{-1} \in S_\Omega$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$, where 1 is the identity permutation where $\forall a \in \Omega, 1(a) = a$.

This group S_Ω is called the *symmetric group of set* Ω. When $\Omega = \{1, 2, ..., n\}$, then S_Ω is called S_n or *the symmetric group of order n*. The actual order of S_n is $n!$, but the behaviors of *any symmetric group is based upon the order of the group it operates on* so we call it order n.

An order to notate these different permutations, we use *cycle notation*. A **cycle** is a string of integers

$$(a_1 a_2 ... a_m)$$

where each $a_i, 1 \geq i < m$ is sent to a_{i+1} and a_m is sent to a_1. For each $\sigma \in S_n$, the numbers 1 to n are grouped into k cycles of the previous form. These cycles can be used for some $x \in \{1, 2, ..., n\}$ where $\sigma(x)$ takes x from its original position in a cycle to the number to the right of it, or the first number in its cycle if it is the farthest right number.

The *length* of a cycle is the amount of elements in S that are in said cycle. A cycle of length t is called a t-cycle. Two cycles are *disjoint* if they have no elements in common. 1-cycles are generally omitted from cycle notation.