SEPTEMBER 5 NOTES

1. 1.1: Introduction to groups: Basic axioms and examples

Definition 1.1. A **binary operation** $\star$ on a set G is a function $\star : G \times G \to G$. We denote $\star(a, b)$ by $a \star b$.

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

If $a, b \in G$ satisfy $a \star b = b \star a$, we say a and b **commute**. If this holds for every $a, b \in G$, we say $\star$ is **commutative.**

Example 1.2.
(1) $+$ and $\times$ are associative and commutative operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.
(2) $-$ is not associative nor commutative on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.

Definition 1.3. If $H \subset G$ and $\star$ is a binary operation on G such that the restriction of $\star$ is a binary operation on H, i.e. for all $a, b \in H$, $a \star b \in H$, then H is **closed** under $\star$. If $\star$ is an associative or commutative operation on G, and H is closed under $\star$, then it is also associative or commutative on H.

Definition 1.4. A **group** is a set G with binary operation $\star$ such that:

(1) $\star$ is associative;
(2) there exists an element $e \in G$, called the *identity* element, such that for all $a \in G$, $a \star e = e \star a = a$;
(3) for each $a \in G$, there exists an element $a^{-1} \in G$ called the *inverse* of a such that $a \star a^{-1} = a^{-1} \star a = e$.

If $\star$ is commutative, we say that G is an **abelian** group.

Example 1.5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$.

$\mathbb{Q} - \{0\}$ or $\mathbb{Q}^+$ are groups under $\times$ with $e = 1$ and $a^{-1} = \frac{1}{a}$. $\mathbb{Z} - \{0\}$ is not a group under $\times$ because most elements do not have inverses. $\mathbb{Q}$ is not a group under $\times$ because 0 does not have an inverse.

Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. This is a group under $+ \pmod{n}$, addition modulo n.[1]

We prove some properties of the identity and inverse elements:

Proposition 1.6. *Suppose G is a group with binary operation $\star$. Then:*

(1) the identity $e \in G$ is unique;
(2) for each $a \in G$, a^{-1} is unique;
(3) for each $a \in G$, $(a^{-1})^{-1} = a$;
(4) for $a, b \in G$, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Proof. We prove only (1) and (2). For (1), suppose e and e' are two identity elements. Then, $e \star e' = e$ by the second group axiom, but $e \star e' = e'$ also by the second axiom. Therefore, $e = e'$ so the identity is unique.

[1] Dummit and Foote calls this group $\mathbb{Z}/n\mathbb{Z}$.

For (2), suppose b and c are two inverses of a. Let $e \in G$ be the identity. By the third group axiom, $a \star b = e$ and $c \star a = e$. Therefore,

$$\begin{aligned} c &= c \star e \quad \text{by definition of } e \\ &= c \star (a \star b) \\ &= (c \star a) \star b \quad \text{by associativity} \\ &= e \star b \\ &= b \quad \text{by definition of } e \end{aligned}$$

and hence $b = c$ so the inverse is unique. □

For simplicity of notation, we will use the following as we proceed:

- If G is a group under some form of addition, we will write $+$ for $\star$ and write $e = 0$, the inverse of an element a by $-a$, and $a + a + \cdots + a$ (n a's) will be written as na.
- If G is a group with any other binary operation $\star$ or a general abstract group, we will use the notation implicit in multiplication for $\star$. To denote $a \star b$, we will simply write ab. The identity will be called 1, and the inverse of an element a will be a^{-1}. To represent $aa \dots a$ (n a's), we will use a^n. Similarly, $a^{-1} \dots a^{-1} = a^{-n}$. We use the notation $a^0 = 1$.
- We often will not write the binary operation with the set and it is assumed to be implicit. In other words, there is only one natural choice of operation that makes the set a group (for instance, if we just write $G = \mathbb{Z}$, the binary operation is understood to be addition).

Now, let us prove additional properties.

Proposition 1.7. *For a group G with $a, b, c \in G$, if $ab = ac$, then $b = c$. Similarly, if $ac = bc$, then $a = b$.*

Proof. These are known as the *cancellation laws.* We prove only the first one: suppose $ab = ac$. Multiply both sides on the left by a^{-1}, apply associativity and the inverse axiom and then the identity axiom to conclude $b = c$. □

Definition 1.8. If G is a group and $x \in G$, we define the **order** of x to be the smallest positive integer n such that $x^n = 1$. We denote this by $|x|$. If no such integer exists, we say x has infinite order.

Example 1.9.
- For any group G, $|x| = 1$ if and only if $x = 1$.
- In $\mathbb{Z}$, every nonzero element has infinite order.
- In $\mathbb{Z}_n$, every element has order at most n because $nx = 0 \pmod n$.

Definition 1.10. For any finite group $G = \{g_1 = 1, g_2, \dots, g_n\}$, the **multiplication table** of G is the $n \times n$ matrix whose ijth entry is $g_i g_j$.

2. 1.2: Dihedral groups

Given the notation in the previous section, we introduce an important example of a group in this section.

Let $n \in \mathbb{Z}$ be a positive integer $n \geq 3$. Let D_{2n} be the set of symmetries of a regular n-gon. (A *symmetry* is a rigid motion of the n-gon moving it so that it fits back in its original position.) This will be called the **dihedral group.**

We may describe each symmetry by labeling the vertices of the n-gon $1, 2, \dots, n$. Any symmetry will be determined by the ending configuration, so we can decide to either flip the shape over (reversing the orientation of the triple $n - 1 - 2$) or keep it in its original orientation, and then we may move the vertex labeled 1 to the original position of any other vertex $1, 2, \dots, n$ by a rotation of some multiple of $2\pi/n$ radians. If we denote by s the symmetry flipping the shape over through the axis of symmetry through vertex 1, and then denote by r the rotation clockwise by $2\pi/n$ radians, we have just shown that the dihedral group has $2n$ elements, given by:

$1, r, r^2, \dots, r^{n-1}$ (the n rotations, including $1 =$ doing nothing), $s, sr, sr^2, \dots, sr^{n-1}$ (the symmetries by first flipping the shape over and then rotating).

You should convince yourself of the following properties:

(1) $1, r, r^2, \dots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
(2) $|s| = 2$
(3) $s \neq r^i$ for any i, and further $sr^i \neq sr^j$ for $i \neq j$ with $0 \leq i, j \leq n-1$
(4) $rs = sr^{-1} = sr^{n-1}$
(5) $r^i s = sr^{n-i}$ for all $0 \leq i \leq n$

By (3), we may write each element of the dihedral group uniquely as $s^k r^i$ for $k \in \{0, 1\}$ and $i \in \{0, \dots, n\}$:

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

and by (4) and (5) we can determine the product of any two elements in D_{2n}.