Groups, Subgroups, and Cyclic Groups

1. Group Axioms

Let G be a group and $*$ be an operation defined in G. We write this group with this given operation as $(G, *)$. In every group we have 4 (but 3 important) axioms.

1. Identity: There exists a unique element $id \in G$ such that for any other element $x \in G$

$$id * x = x * id = x$$

2. Inverses: For every element $x \in G$ there exists an element $x^{-1} \in G$ such that

$$x * x^{-1} = x^{-1} * x = id$$

3. Closure: Given any two elements x and y. If $x \in G$ and $y \in G$, then

$$x * y \in G$$

for all $x, y \in G$

There is also one more important characteristic of all groups, and this is wether or not all elements of the group commute with one another.

Definition
For any two elements, $x, y \in G$, if

$$x * y = y * x$$

for all $x, y \in G$, then we say that G is an **Abelian Group**.

This will be very important to be familiar with in the future because we will encounter many interesting groups, some of which will be abelian and some of which will not be abelian.

Let's remind ourselves of some simple group examples and see how certain sets can break one or more of the groups axioms depending on what operation we define in the set.

Example 1.1

$$(\mathbb{Z}, +)$$

The identity here is the **additive identity**, 0. For any integer, a, $a^{-1} = -a$ because

$$a + a^{-1} = a + (-a) = a - a = 0$$

Finally, the integers under addition are closed because the sum of two integers is always an integer. Therefore, the integers with the operation of addition, $(\mathbb{Z}, +)$, form a group. Furthermore, this group is **abelian** because $a + b = b + a$ for all $a, b \in \mathbb{Z}$.

Example 1.2

$$(\mathbb{I} + \{1\}, \times)$$

The set of positive irrational numbers together with 1 under multiplication satisfies the first two groups axioms listed above, yet it is not a group because the set is not closed. For Example,

$$\sqrt{2} \times \sqrt{2} = 2 \text{ and } 2 \notin \mathbb{I}$$

Example 1.3

$$(\mathbb{Z}_5, +)$$

The group of integers modulo 5 is a group under the operation of addition. If we think of adding each number by adding the congruence class it belongs to, we can see that $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Any two numbers added together and reduced mod 5 will always equal $0, 1, 2, 3$ or 4 so the group is closed. The identity is 0 just like any group under addition, and every element has a unique inverse. (A homework question will be about inverses modulo n)

Example. 1.4

$$(D_4, \circ)$$

The dihedral group of order 8, or the group of rigid symmetries of a square, forms a group under the operation of composition, which we know more formally as permutation multiplication. The identity is the 'do nothing' motion (but we can also think of it as r^4). Also, each element has a unique inverse. Reflections are self-inverse and the inverse of any rotation, r^k is another rotation r^n where $k + n$ equals a multiple of 4. We have also shown that D_4 is closed since the product of rigid symmetries is a rigid symmetry.

We will soon see that for any rotation, r, and any reflection, s, we have that $srs = r^{-1}$. Although D_4 is a group, it is not **abelian**. We can see that for any two rotation, $r^k \cdot r^n = r^n \cdot r^k = r^{k+n}$, but when we consider a combination of reflections,s, and rotations,r, we see that in most cases $rs \neq sr$ so D_4 is not **abelian**.

2. Orders

Definition

The number of elements of a group is called the ***order***. For a group, G, we use $|G|$ to denote the order of G.

Example 2.1

Since $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, we say that $\mathbb{Z}_5$ has order 5 and we write $|\mathbb{Z}_5| = 5$.

Example 2.2

$D_4 = \{id, r, r^2, r^3, V, H, D, D'\}$, so we say D_4 has order 8, and we write $|D_4| = 8$. In general, $|D_n| = 2n$ which we will prove later this semester.

Definition

The ***order of an element*** g, in a group G, is the smallest positive integer n such that $g^n = id$. If no such integer exists, we say that g has infinite order. The order of an element g is denoted using $|g|$.

To find the order of an element, g, all you must do is repeatedly multiply (operate) g by itself. In other words, compute the sequence of products $g, g^2, g^3, \cdots$ until you reach the identity for the first time.

Example 2.3

Consider $(\mathbb{Z}_{10}, +)$, the group of integers modulo 10 under addition. To find $|2|$, we compute, $2 \cdot 1 = 2$, $2 \cdot 2 = 4$, $2 \cdot 3 = 6$, $2 \cdot 4 = 8$, $2 \cdot 5 = 10 = 0 \mod 10$, so we have seen that $|2| = 5$. We can also verify that $|0| = 1$, $|7| = 10$, and $|6| = 5$.

Example 2.4

In D_4, if we take the element r, we see that repeated multiplication of r by itself yields, $\{r, r^2, r^3, id\}$ so $|r| = 4$. We also know that $|s| = 2$ for any reflection, s.

Now we are ready to talk about subgroups. This is one of the most important topics in group theory and will lead to many fascinating theoretic discoveries.

Definition

If a subset H of a group G (which we write as $H \subseteq G$) is itself a group under the operation defined in G, we say that H is a ***subgroup*** of G.

3. Subgroups

Notation

For any element, g, in a group, we let $\langle g \rangle$ denote the set $\{g^n : n \in \mathbb{Z}\}$. This is just the set created by repeated multiplication of g by itself until we reach the identity. It is important to notice that the definition above states that n is an integer. This means we can compute negative powers of g as well. You may still be confused so let's see some examples.

Example 3.1

In $(\mathbb{Z}_{10}, +)$, we saw that $|2| = 5$. The set generated by repeated addition of 2 is now more simply written as $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$

Example 3.2

In $\mathbb{Z}$, if we pick 1, we see that $\langle 1 \rangle = \mathbb{Z}$. Note: We are generating all of $\mathbb{Z}$ because we are computing positive **and** negative powers of 1. In this group, something like $1^{-3} = (-3) \cdot 1$ and $1^5 = (5) \cdot 1$ because the operation is addition and 1^k means add one to itself k times.

Example 3.3

In Example 2.4 we saw that for $r \in D_4$, $|r| = 4$. Now we can write $\langle r \rangle = \{r, r^2, r^3, id\}$.

Example 3.4

If you are familiar with the imaginary number ,$i = \sqrt{-1}$, you can recall that $i \in \mathbb{C}$. We know (but have not proven) that $(\mathbb{C}, \times)$ is a group under complex multiplication. So when we consider $\langle i \rangle = \{i, -1, -i, 1\}$, we see that $\langle i \rangle \subseteq (\mathbb{C}, \times)$. Clearly we have identity since $1 \in \langle i \rangle$. Check for yourself that every element has a unique inverse and that $\langle i \rangle$ is closed under multiplication.

It is important to observe that these sets we have generated are indeed groups themselves under given the operation defined. $\langle 2 \rangle \subseteq (\mathbb{Z}_{10}, +)$ and $\langle 2 \rangle$ is a group under addition modulo 10. Verify for yourself that it is closed.

We also see that $\langle r \rangle \subseteq D_4$ and $\langle r \rangle$ is a group under permutation multiplication, or rigid symmetries of a square. We can now see that when we have any group element $g \in G$, we can compute $\langle g \rangle$ and realize that $\langle g \rangle$ is **ALWAYS** a subgroup of G. We can use this generating method to find tons of interesting subgroups/groups.

We write this as $\langle g \rangle \subseteq G$, and we can call $\langle g \rangle$ the **cyclic subgroup generated by g**.

Note: *This complicated and wordy definition is not important, it makes communicating ideas easier but it is more important to understand the concepts and not to memorize the way to say things.*

4. Cyclic Groups

Definition

If there exists a group element $g \in G$ such that $\langle g \rangle = G$, we call the group G a **cyclic group**. We call the element that generates the whole group a **generator** of G. (A cyclic group may have more than one generator, and in certain cases, groups of infinite orders can be cyclic.) Examples will make this very clear.

Example 4.1

Returning to $(\mathbb{Z}_{10}, +)$, we saw that $\langle 2 \rangle$ generated a subgroup of $(\mathbb{Z}_{10}, +)$ but did not generate the whole group. Let's consider a different element of this group. Observe that by repeatedly adding 7 to itself and reducing mod 10 we see that

$$\langle 7 \rangle = \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\} = \mathbb{Z}_{10}$$

So indeed $(\mathbb{Z}_{10}, +)$ is a cyclic group. We can say that $\mathbb{Z}_{10}$ is a cyclic group generated by 7, but it is often easier to say 7 is a generator of $\mathbb{Z}_{10}$. This implies that the group is cyclic. Are there any other generators for $\mathbb{Z}_{10}$?

Example 4.2

Considering $(\mathbb{Z}, +)$ again, we recall from example 3.2 that

$$\langle 1 \rangle = \mathbb{Z}$$

So we can see that 1 is a generator of $\mathbb{Z}$, therefore $(\mathbb{Z}, +)$ is cyclic. Note that $|\mathbb{Z}| = \infty$ so it is indeed possible for groups of infinite order to be cyclic.

Example 4.3

In order to examine more cyclic groups we will need to introduce 'U-groups'. I will briefly introduce it here and go into more detail later. We refer to 'U-groups' as the group of units mod some number. It is written as $U(n)$ and means, the group of positive integers relatively prime to n, under multiplication modulo n.

Take $U(9)$ for example. $U(9) = \{1, 2, 4, 5, 7, 8\}$ is a cyclic group, and a quick computation will show us that for $2 \in U(9)$:

$$\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\} = U(9)$$

If this seems very confusing don't worry. It is very confusing and we will spend more time learning the details of 'U-groups' later on.