CHAPTER II: GROUPS

Section 1: Basics
Section 2: Cyclic Groups

In the last section we saw several examples of groups and stated the group axioms. In this section we will obtain our first theorems about these new objects. Several of these results we have encountered already, but didn't take the time to state officially. In most of these theorems and examples, we will denote the group operation multiplicatively (i.e. using juxtaposition).

Theorem 1: Let G be a group and let $a,b \in G$.

(a) The identity element is unique.
(b) Inverses are unique.
(c) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: (a) Suppose G has two identity elements, say e_1 and e_2. Then since e_1 is the identity, $e_2 e_1 = e_2$, and since e_2 is the identity, $e_2 e_1 = e_1$. Therefore, $e_1 = e_2$.

(b) Let $x \in G$ and suppose it has two inverses, a and b. Then

$$xa = e$$
$$bxa = be$$
$$a = b$$

(c) Since $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$, and inverses are unique, $(ab)^{-1} = b^{-1}a^{-1}$.

Recall that we have already discussed the *order of an element* of a group. This first came up regarding permutations, and then in more generality on the midterm exam. We now state the definition for the order of a group.

Definition: The ***order*** of a group is its size or cardinality. We denote the order of group G by $|G|$.

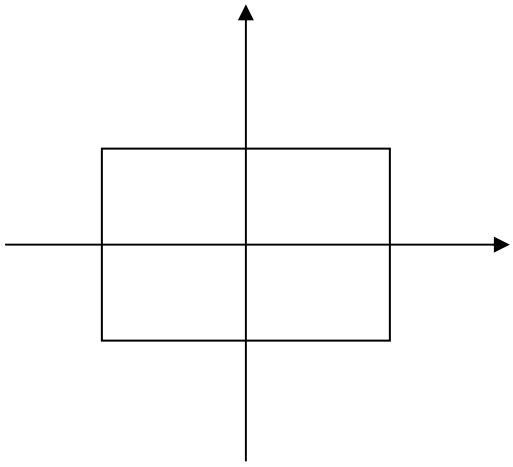
This is our second encounter with the term "order." We'll relate the two definitions in short order.

Example 1: For any natural number n, $\mathbb{Z}_n$ (under modular addition) has n elements. This gives us examples of a group with each order 1, 2, 3, ….

Someone once said, "Poetry is the art of giving different names to the same thing." Mathematician Henri Poincaré (1854-1912) said in contrast, "Mathematics is the art of giving the same name to different things." What Poincaré was referring to is the unique ability of mathematics to take many different things – or more to the point many things that SEEM different – and treat them similarly; to see the hidden patterns and the underlying structure of diverse objects; to see order where there appears to be none. In other words, one of the most powerful aspects to mathematics is its abstraction. Abstraction allows us to see different objects similarly and in some cases to use what we know about some things and apply them to others that have the same structure.

One of the ways we do this is with groups. Two sets of objects can be different but have the same structure. Alternately, two objects can appear similar, but have different structure. To better understand this, consider a rectangular card. Intuitively, we know that this is a symmetric object, but what's makes it symmetric? One way to define a symmetry on an object is to specify what rigid motions can be performed on the object and leave it unchanged. In other words, suppose you left a rectangular card on the table and left the room. There are a few things I could do to the card while you were gone that you would not be able to detect upon your return. That's the key idea: *a symmetry is an undetectable motion.*

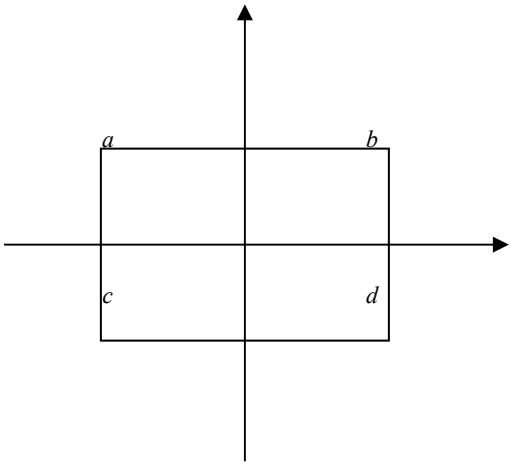
For clarity, suppose we orient the card in the plane so that its "center" is at the origin (see figure).



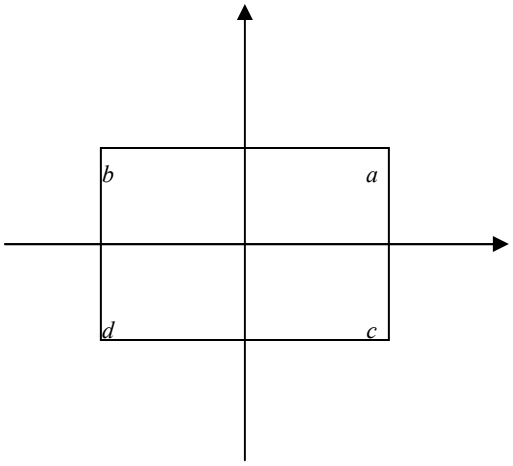
I could rotate the rectangular card across the horizontal axis, and it would appear unchanged. I could also rotate it across the vertical axis. Can you think of any other motions that would leave the rectangular card unchanged? (There are two more.) I invite you to try and come up with them before you continue reading.

Ok, the third rigid undetectable motion (i.e. symmetry) of the rectangular card is the rotation around its center by $180°$. It could be argued that this opens up infinitely-many symmetries formed by rotating the card around it's center by $360°$, $540°$, $720°$, etc. But it turns out to be useful to only consider the symmetries that are essentially different; rotating by $180°$ and rotating by $540°$ produce the same result, so we think of them as the same. However, we do need to consider $360°$. This is the same as not moving the card at all (i.e. rotating by $0°$), which of course would be an undetectable motion. So we have four symmetries of the rectangle: the non-motion (rotating around the center by $0°$), rotating around the center by $180°$, rotating across the horizontal axis, and rotating across the vertical axis. I'll denote the four symmetries by I, R_{180}, R_h, and R_v (respectively).

We have a natural operation on these four objects; namely composition. Note that this set is closed under composition. To see this, you have to track where each corner goes as you move the card. To make this clear, let's label the corners with a, b, c, and d as shown.



Note that the corners are NOT really labeled, because if they were, you'd be able to detect the undetectable motion when you returned to the room! But to work out the "multiplication" table, labeling the corners proves helpful. For instance, if I rotate the card $180°$ and then rotate around the horizontal axis (in other words, if I perform $R_h \circ R_{180}$), the final result would be the figure:



This matches the symmetry R_v. The rest of the products are indicated with the following table:

	I	R_{180}	R_h	R_v
I	I	R_{180}	R_h	R_v
R_{180}	R_{180}	I	R_v	R_h
R_h	R_h	R_v	I	R_{180}
R_v	R_v	R_h	R_{180}	I

From this table, we can see that this operation is associative (as it should be since composition of functions is an associative operation in general) and commutative. The identity element is I (naturally), and each element has an inverse. Therefore, $\{I, R_{180}, R_h, R_v\}$ forms an abelian group under this operation.

But wait, we have already seen a group with four elements: $\mathbb{Z}_4$. Even though these group consist of different objects (symmetries of the rectangle and congruence classes modulo 4), maybe the groups are the same. Maybe their structure is the same. We (of course) have a mathematical way of determining whether this is true or not. We have a term for groups that are "the same."

Definition: Let G and H be two groups. We say that G and H are ***isomorphic*** if there exists a bijection (i.e. a one-to-one and onto mapping) $\varphi : G \to H$ that preserves the group operations. In other words, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. The map φ is called an ***isomorphism***.

I want to point out that there are two different group operations in this definition, both denoted by juxtaposition. In the equation $\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)$, the operation on the left hand side is in G and the operation on the right hand side is in H.

There are many consequences when two groups are isomorphic since their structures must be the same. Here are a few.

Theorem 2: If $\varphi: G \to H$ is an isomorphism of groups G and H and let e_G and e_H be the respective identity elements. Then $\varphi(e_G)=e_H$ and $\varphi(g^{-1})=\varphi(g)^{-1}$ for each $g \in G$.

Proof: Let $h \in H$. Since φ is onto, there exists a $g \in G$ such that $\varphi(g)=h$. Then $\varphi(e_G)h=\varphi(e_G)\varphi(g)=\varphi(e_Gg)=\varphi(g)=h$. By the uniqueness of the identity element, this means that $\varphi(e_G)=e_H$. Also, $\varphi(g^{-1})\varphi(g)=\varphi(g^{-1}g)=\varphi(e_G)=e_H$ which shows that $\varphi(g^{-1})=\varphi(g)^{-1}$.

Theorem 3: If G and H are isomorphic, then they are either both abelian or both not abelian.

Proof: Let $\varphi: G \to H$ be an isomorphism of groups G and H. We want to show that G is abelian if and only if H is abelian. First assume G is abelian and let $h_1, h_2 \in H$. Since φ is onto, there exist $g_1, g_2 \in G$ such that $\varphi(g_1)=h_1$ and $\varphi(g_2)=h_2$. Then

$$h_1h_2=\varphi(g_1)\varphi(g_2)=\varphi(g_1g_2)=\varphi(g_2g_1)=\varphi(g_2)\varphi(g_1)=h_2h_1,$$

which means H is abelian.

Now assume H is the abelian group and let $g_1, g_2 \in G$. Then there exist $h_1, h_2 \in H$ such that $\varphi(g_1)=h_1$ and $\varphi(g_2)=h_2$ and we have

$$\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)=h_1h_2=h_2h_1=\varphi(g_2)\varphi(g_1)=\varphi(g_2g_1).$$

Since $\varphi: G \to H$ is one-to-one, this means that $g_1g_2=g_2g_1$ and hence G is abelian.

Back to our question: Are the two groups $\{I, R_{180}, R_h, R_v\}$ and $\mathbb{Z}_4$ the same? Notice that in $\{I, R_{180}, R_h, R_v\}$, every element is its own inverse. In other words, $x^2 = I$ for every element x in $\{I, R_{180}, R_h, R_v\}$. Now suppose that $\{I, R_{180}, R_h, R_v\}$ and $\mathbb{Z}_4$ are isomorphic, with isomorphism φ. Notice then that

$$0 = \varphi(I) = \varphi(x^2) = \varphi(x \circ x) = \varphi(x) + \varphi(x).$$

(Again, note the different group operations; composition in $\{I, R_{180}, R_h, R_v\}$ and addition in $\mathbb{Z}_4$.) Therefore, since every non-identity element in $\{I, R_{180}, R_h, R_v\}$ has order 2, every non-zero element in $\mathbb{Z}_4$ would also have to be of order 2. But we know this isn't the case (the element [3] has order 4). So $\{I, R_{180}, R_h, R_v\}$ and $\mathbb{Z}_4$ are not isomorphic groups.

Definition: A nonempty subset H of a group G is called a ***subgroup*** if H is itself a group under the operation of G.

Theorem 4 (Subgroup Test): A nonempty subset H of G is a subgroup of G if and only if

(1) H is closed under the operation of G, and

(2) For each $h \in H$, h^{-1} is also in H.

In most groups, there are many subgroups. In any group G, G itself and $\{e\}$ are subgroups.

Definition: Let G be a group. For any element $g \in G$, the ***cyclic subgroup generated by*** g is formed by taking all powers of g. This is denoted by $\langle g \rangle$. So

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}.$$

(We are using the standard exponential rules here such as $g^0 = e$, $g^{-k} = (g^k)^{-1}$, and $g^k g^l = g^{k+l}$. Also, this notation is written multiplicatively, but that doesn't mean the operation HAS to be multiplication. If the operation is addition, we could write $\langle g \rangle = \{kg : k \in \mathbb{Z}\}$.) If $\langle g \rangle = G$, then

we say that G is a ***cyclic group*** and g is a ***generator***. Finally, the ***order*** of an element g is the order (size) of cyclic subgroup generated by g.

This brings us back to the two different uses of the word "order." Clearly the order of an element (the size of its cyclic subgroup) – if it is finite – will be the smallest power of that element that equals the identity. Cyclic groups are very important, but even more impressive, they are also fully understood. The next result tells us that cyclic groups are completely classified by their order. By the way, we denote the fact that two groups G and H are isomorphic by $G \cong H$.

Theorem 5: If G is an infinite cyclic group, then $G \cong \mathbb{Z}$ is isomorphic to $\mathbb{Z}$. If G is a finite cyclic group of order n, then $G \cong \mathbb{Z}_n$.

Proof: I will provide the first part and leave the second as an exercise. Let G be an infinite cyclic group and let $g \in G$ be a generator. (So $G = \langle g \rangle$.) To show that $G \cong \mathbb{Z}$, we need to define a bijection from one group to the other and show that the group operation is preserved. Define $\varphi : \mathbb{Z} \to G$ by $\varphi(k) = g^k$. This map is onto by the definition of $\langle g \rangle$ and since G is an infinite cyclic group, all the powers of g are distinct, so φ is one-to-one. Also, $\varphi(k+l) = g^{k+l} = g^k g^l = \varphi(k)\varphi(l)$, so φ is an isomorphism.

Example 2: Since $\mathbb{Z}_n$ is cyclic for any n, we should be able to find a generator. Consider $\mathbb{Z}_{10}$. Let's look at the "powers" of $[2]$. Recall that the operation in this group is addition.

$0[2] = [0]$ $\quad$ $1[2] = [2]$ $\quad$ $2[2] = [4]$
$3[2] = [6]$ $\quad$ $4[2] = [8]$ $\quad$ $5[2] = [10] = [0]$

So $\langle [2] \rangle = \{[0],[2],[4],[6],[8]\} \neq \mathbb{Z}_{10}$. Hence $[2]$ is NOT a generator of $\mathbb{Z}_{10}$. But since

$0[3] = [0]$ $\quad$ $1[3] = [3]$ $\quad$ $2[3] = [6]$ $\quad$ $3[3] = [9]$ $\quad$ $4[3] = [2]$
$5[3] = [5]$ $\quad$ $6[3] = [8]$ $\quad$ $7[3] = [1]$ $\quad$ $8[3] = [4]$ $\quad$ $9[3] = [7]$ $\quad$ $10[3] = [0]$,

the element $[3]$ is a generator of $\mathbb{Z}_{10}$. We should note that the generator of a cyclic group is not necessarily unique. It's possible that other elements could generate $\mathbb{Z}_{10}$.