GROUP THEORY AND SYMMETRY

MAX STEINBERG FOR THE OLGA RADKO MATH CIRCLE
ADVANCED

1. Groups

A **group** is a set of objects together with a **binary operation**: an operation that can be applied to two elements of the set. We typically write a group like $(\mathbb{Z}, +)$, where the first item is the set $(\mathbb{Z})$ and the second is the operation (addition, $+$). There are some **group axioms** that every group must follow in order to be considered a group. Let $(G, +)$ be a group. Then the following must all be true:

(1) There must be an identity element. That is, there is some element $e \in G$ so that $\forall g \in G$, $e + g = g + e = g$.
(2) G must be closed under its binary operation. That is, $\forall a, b \in G$, it must be the case that $a+b \in G$.
(3) The binary operation must be associative. That is, $\forall a, b, c \in G$, $(a + b) + c = a + (b + c)$.
(4) Every element must have an inverse. That is, $\forall a \in G$, $\exists b \in G$ so that $a + b = b + a = e$.

You may notice $x + y$ may not equal $y + x$ (ie. our binary operation need not be commutative). If $x + y = y + x$ for every x, y in our group, our group is called "abelian."

Problem 1. Which of the following are groups? Why or why not?

(1) $(\mathbb{Z}, +)$
(2) $(\mathbb{Z}, \cdot)$
(3) $(\mathbb{R}, +)$
(4) $(\mathbb{R}, \cdot)$
(5) $(\mathbb{R} \setminus \{0\}, +)$
(6) $(\mathbb{R} \setminus \{0\}, \cdot)$

Problem 2. Groups don't always have to be groups of numbers. Let us take the set $\{e, a, b, a^2, b^2, \dots\}$ as our set, and define our binary operation as follows:

$\times$	e	a	b
e	e	a	b
a	a	a^2	e
b	b	e	b^2

Does our set with this binary operation form a group?

Problem 3. Let $(G, \cdot)$ be a group. Is the identity of G unique? Let $a \in G$. Is the inverse of a unique? Prove your answer.

2. Group Presentations

As of right now, it might seem difficult to write down exactly what a group is. It's not easy to say or write "the set of $\{e, a, b, a^2, b^2, \dots\}$ with this multiplication table". So let's come up with a method of writing down certain kinds of groups in ways that are easy to deal with. We will start by defining a **free group**. First, the **free group on** 1 **generator** is the group in Problem 2. You may notice that $a \times b = b \times a = e$, so by the Group Axiom 4, b is the inverse of a, so let's b as a^{-1}. Thus, our group is $\{e, a, a^{-1}, a^2, a^{-2}, \dots\}$. We call a a **generator**. So we can define the **free group on** 2 **generators** as $\{e, a, b, a^{-1}, b^{-1}, a^2, b^2, a^{-2}, b^{-2}, \dots\}$. But what is $a \times b$? We can simply let $a \times b = ab$, a new element. At this point it is unwieldy to write out the set because of how many different things we have in the set. So we simply write $\langle a, b\rangle$ to denote the free group on generators a, b. For n generators, we simply write $\langle a_1, a_2, \dots, a_n\rangle$.

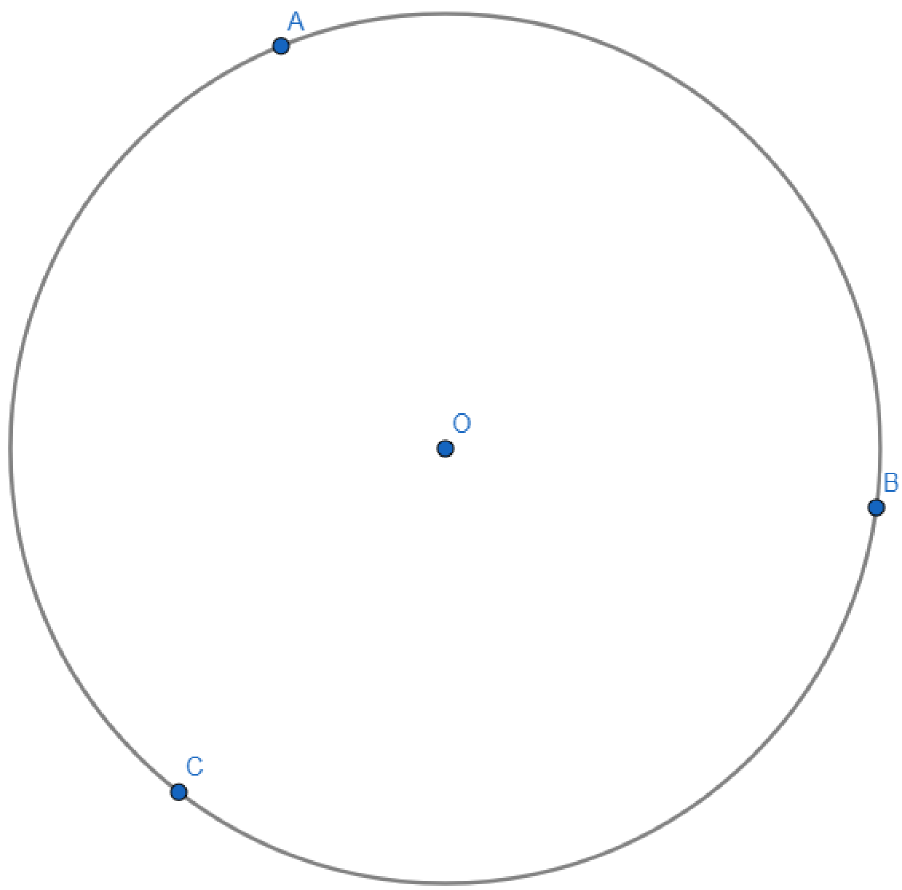
Problem 4. Describe the group $\langle a, b, c, d, e, \dots, z\rangle$. Name some elements of this group. What is $mathematics \times algebra$? Does this make sense in this group?

Let's add one more thing to our group presentation idea. What if we have the group $\{e, a, a^2\}$ where $a \times a^2 = a^2 \times a = e$. This is not a free group because $a^3 = e$, but it is a group (check this). How should we represent it? It's actually very easy. We just write $\langle a|a^3 = e\rangle$, or just $\langle a|a^3\rangle$.

Problem 5. Describe the group $\langle a, b|a^2, b^2\rangle$.

3. Symmetries

Now that we got through all that abstract nonsense, let's do some geometry.

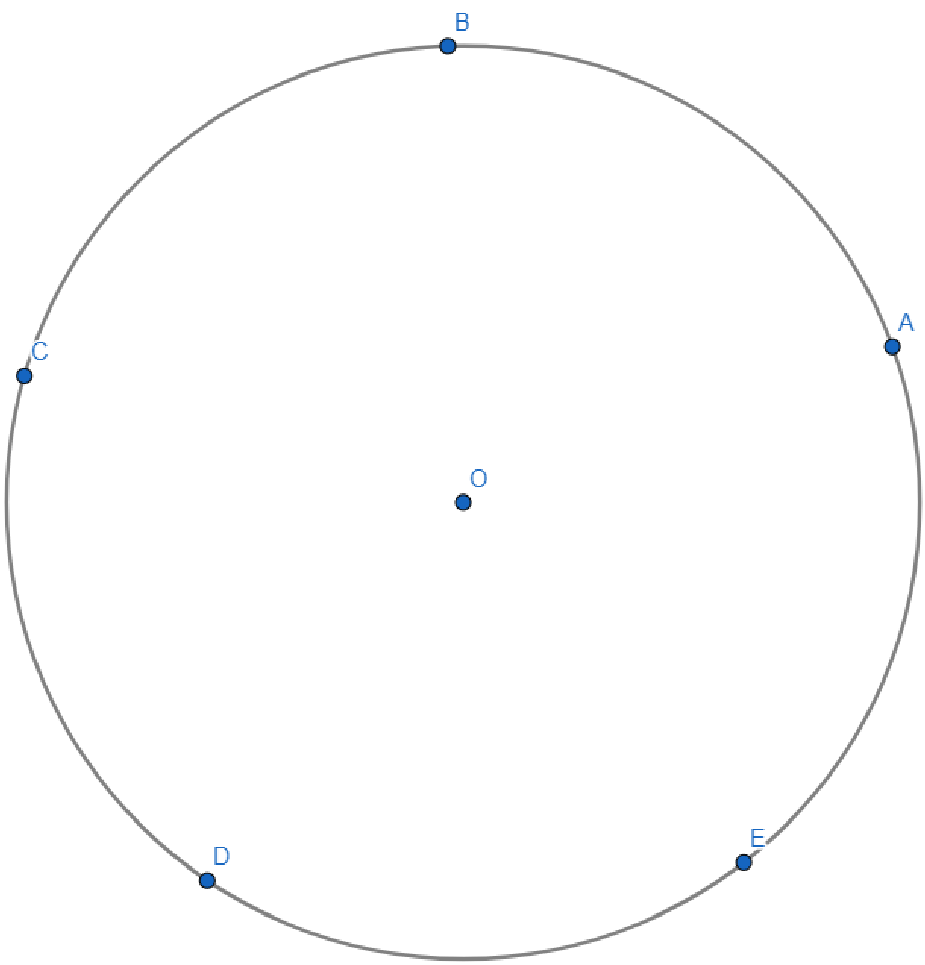


Let's think about how these three points, A, B, C, are symmetric. There is reflectional symmetry, but we will ignore it for now and only focus on the threefold rotational symmetry. How could we *represent* this symmetry? As you may have guessed, we can form a group out of this symmetry. A **symmetry** on a set of points is a plane isometry which leaves the points fixed. That is a lot of complicated words to say a symmetry is a rotation, reflection, or translation, which moves the points to other points within the set (or to the same point). Thus, under this definition, the identity transformation is a symmetry. We can denote this as e. Furthermore, we can rotate by $\frac{2\pi}{3}$ about O to send $A \to B, B \to C, C \to A$, so this is also a symmetry. We can denote this r (for "rotation").

Problem 6. If we define a binary operation as composition (eg. $e \times e = e \circ e$), write out our multiplication table for $\{e, r\}$.

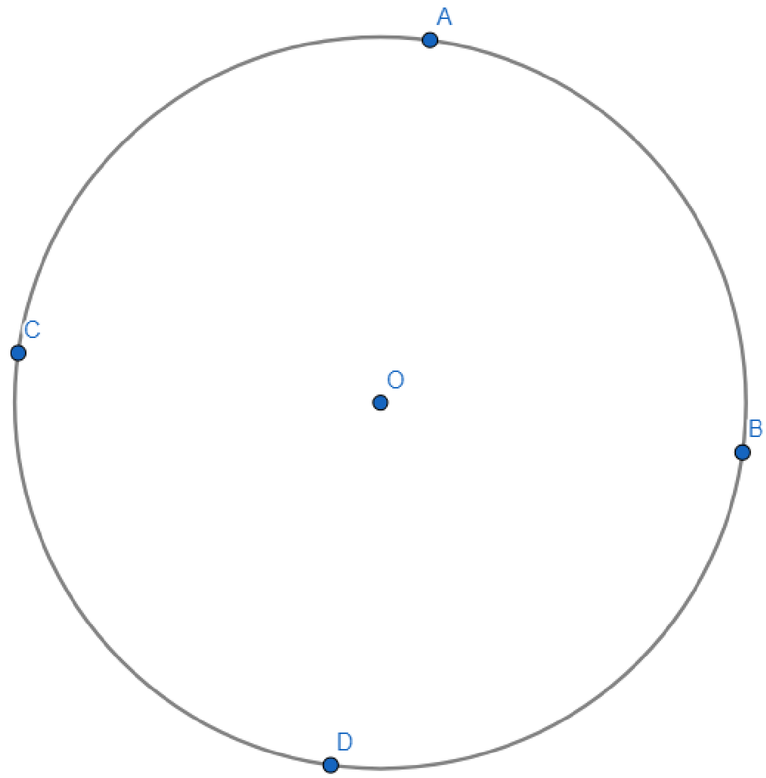
$\times$	e	r
e		
r		

Problem 7. What is r^3? With this knowledge, how can we write a presentation for the symmetry group of this figure above?



Problem 8. Write the rotational symmetry group for the above figure.

Problem 9. (Challenge problem) Write the symmetry group for the three points on a circle (make sure to include the reflectional symmetry).



Problem 10. (Challenge problem) Write the symmetry group for the above figure (make sure to include the reflectional symmetry).

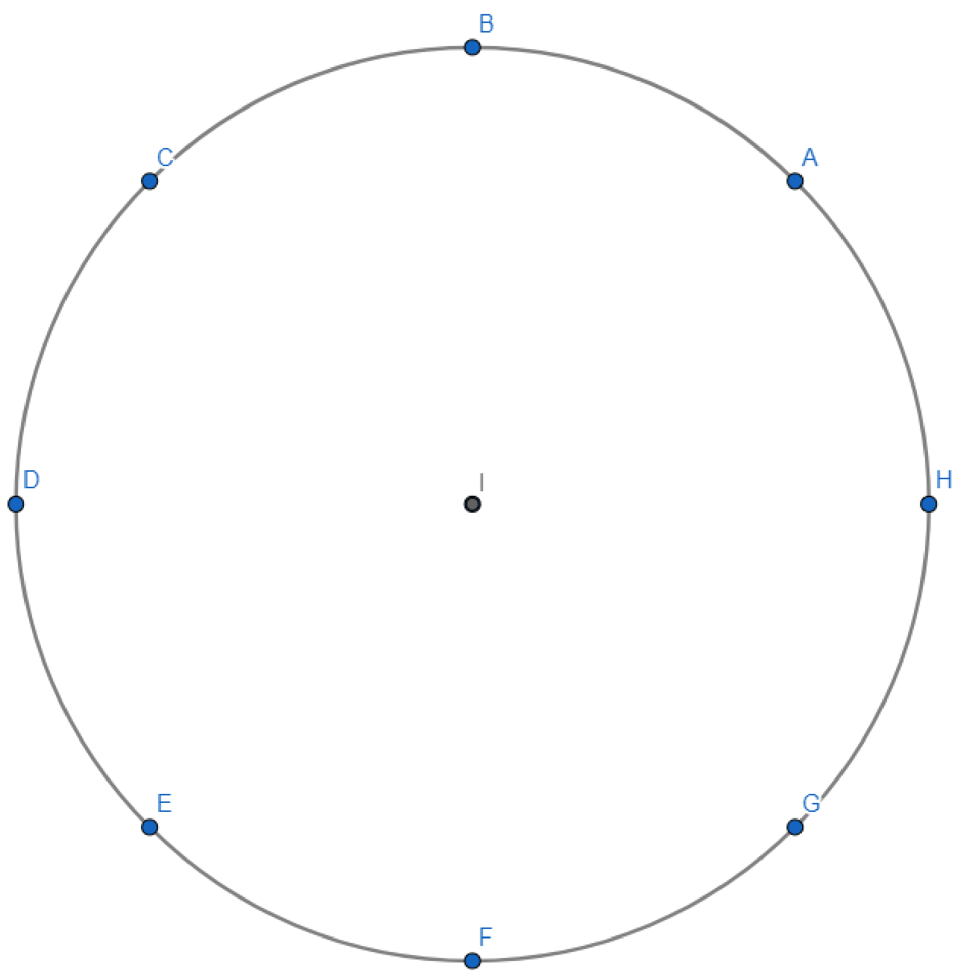
4. "Sub"-symmetries and Subgroups

Let $(G, \cdot)$ be a group, and let $F \subset G$ (and $F \neq G$). If $(F, \cdot)$ is a group (ie. it satisfies the Group Axioms), we call F a **proper subgroup** of G. It is true that G is a **subgroup** of G, but it is not a *proper* subgroup. Let us introduce some useful terminology. The **order** of a group, denoted by $|G|$, is the size of G as a set. This is only a useful idea if $|G|$ is finite, in which case G is known as a **finite group**.

Theorem. (Lagrange) Let G be a finite group and let F be a subgroup. Then F is a finite group and $|F|$ divides $|G|$.

We will not be proving this, but you may use it.

Problem 11. Consider the group $G = \langle a | a^k \rangle$ for some $k > 1$. Describe all the subgroups of G.



Problem 12. Let G be the rotational symmetry group of the above figure. What are the subgroups of G?

Problem 13. For each subgroup you found in Problem 12, draw a figure with rotational symmetry group equal to that subgroup.

Problem 14. This is a little bit of a different topic but it is a very interesting application of basic group theory. The following are facts you may use:

(1) For any prime p, the set $G = \{1, 2, 3, 4, \ldots, p-1\}$ with multiplication modulo p form a group.
(2) For any $a \in G$, there is an integer $k > 0$ so that $a^k \equiv 1 \mod p$.

Prove Fermat's Little Theorem: for any prime number p and any integer $a > 0$, $a^p \equiv a \mod p$.