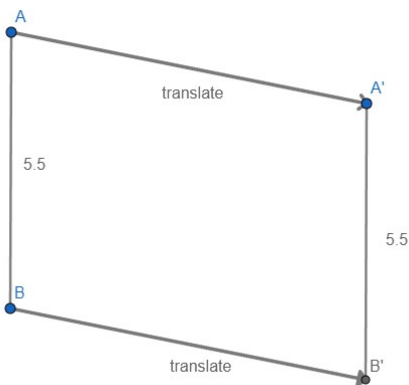


GROUP THEORY VIA SYMMETRY

MAX STEINBERG FOR THE OLGA RADKO MATH CIRCLE
ADVANCED 2

1. WARMUP: SYMMETRIES

We say a plane transformation is a **isometry** if it doesn't change the distance between two points. For example, a translation is an isometry:

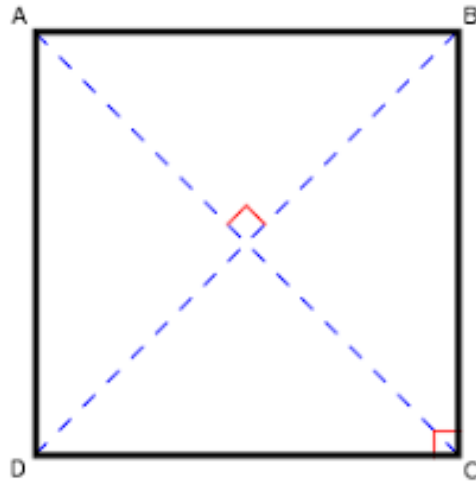


Problem 1. Are the following plane transformations isometries? Why or why not?

- (1) A rotation by some angle.
- (2) The map of the plane which takes the point (x, y) to $(2x, 2y)$.
- (3) Reflections about some line.
- (4) The map of the plane which takes the point (x, y) to $(x + y, y)$.

Solution. Yes, No, Yes, No.

We define a **symmetry** of a set of points in the plane to be a plane isometry such that every point in the set maps to another point in the set (possibly the same point). So for example, if we have a square, a symmetry of the square might be a reflection across one of the diagonals. The identity transformation counts as a symmetry.



Problem 2. Find all of the symmetries of a square. Make sure to consider all possible translations, rotations, and reflections. (*Hint: You can draw on the picture above!*)



Problem 3. Find all of the symmetries of a snowflake.

In three dimensions, all of our definitions still work as you would expect. We still only need to consider translations, rotations, and reflections.

Problem 4. Find all the symmetries of a cube.

2. GROUPS

A **group**, roughly speaking, is a set of objects together with a **binary operation**: an operation that can be applied to two elements of the set and returns an element 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 set and $+$ be a binary operation on G that returns an element of G (ie. $+: G \times G \rightarrow G$). Then if all of the following four axioms are true, we say $(G, +)$ is a group:

- (1) There must be an identity element. That is, there is some element $e \in G$ so that for every $g \in G$, $e + g = g + e = g$.
- (2) G must be closed under its binary operation. That is, for every $a, b \in G$, it must be the case that $a + b \in G$.
- (3) The binary operation must be associative. That is, for every $a, b, c \in G$, $(a + b) + c = a + (b + c)$.
- (4) Every element must have an inverse. That is, for every $a \in G$, there is some $b \in G$ 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 5. 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) $(\mathbb{R} \setminus \{0\}, \cdot)$

Solution. 1, 3, 6.

Problem 6. Groups don’t always have to be groups of numbers. Verify that the following set with a binary operation is a group (ie. go through each of the four axioms and check that they are satisfied): let $G = \{\text{odd}, \text{even}\}$ with the operator $+$ defined by $\text{odd} + \text{odd} = \text{even}$, $\text{odd} + \text{even} = \text{odd}$, $\text{even} + \text{odd} = \text{odd}$, $\text{even} + \text{even} = \text{even}$.

Problem 7. Are there any groups with 0 elements? How about 1 element? 2 elements?

Solution. No, yes, yes.

Problem 8. 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

(and continuing on, so that, for example, $a^2 \cdot a = a^3$, etc.) Does our set with this binary operation form a group? Why or why not?

Solution. Yes, this is the free group on one generator and isomorphic to \mathbb{Z} .

Problem 9. 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.

Solution. Let e, e' be identities. Then $ee' = e(e') = e' = (e)e' = e$. Let b, b' be inverses of a . Then $bab' = (ba)b' = b' = b(ab') = b$ so $b = b'$.

Problem 10. Prove $(a^{-1})^{-1} = a$ for any $a \in G$.

Solution. By the previous problem, the inverse of a is unique. So it suffices to show that a^{-1} is an inverse of a . But $a^{-1}a = aa^{-1} = e$ by definition and we are done.

3. 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.

Instead of writing out the list of elements in our group along with a multiplication table (as this is extremely repetitive and not useful), we will work with **group presentations**. Group presentations have two parts: the alphabet and the rules. Let's look at an example first with just an alphabet:

$$\langle \underbrace{a, b}_{\text{alphabet}} \rangle$$

this group is composed of all words built in the alphabet $\{a, b\}$, with the group operation being concatenation (which we will denote by \oplus). So for example, this group has the element aba , and $aba \oplus bab = ababab$. In this group, we will use e to denote the identity (so $e \oplus ab = ab$ not eab). Further, elements are required to have inverses, so we will allow a^{-1} and b^{-1} to be used in the alphabet as well, with the requirement that any time a sits next to a^{-1} they are both removed. So

$$a^{-1}bb^{-1}a \Rightarrow a^{-1} \quad \underbrace{bb^{-1}}_{\text{cancelling } b \text{ and its inverse}} \quad a \Rightarrow \quad \underbrace{a^{-1}a}_{\text{cancelling } a \text{ and its inverse}} \quad \Rightarrow e$$

Now let's add some rules.

$$\langle \underbrace{a, b}_{\text{alphabet}} \mid \underbrace{a^2, b^3}_{\text{rules}} \rangle$$

Here, we say that any time a^2 appears, we remove it. Similarly, any time b^3 appears, we remove it.

Problem 11. Simplify $ab^2b^{-1}b^{-1}ab^2aa^{-1}b$.

Solution. e .

Problem 12. Verify that the group $\langle a, b \mid a^2, b^3 \rangle$ is in fact a group. (That is, verify the group axioms from page 1.)

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**.

Problem 13. Find the order of $\langle a, b \mid a^2, b^2, aba^{-1}b^{-1} \rangle$. (Don't forget the identity element!)

Solution. 4: e, a, b, ab .

Problem 14. (Challenge problem) Explain why any group presentation satisfies the group axioms.

Problem 15. (Challenge problem) Pick two positive integers p and q . What is the order of $\langle a \mid a^p, a^q \rangle$?

Solution. $\gcd(p, q)$.

4. SYMMETRIES

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

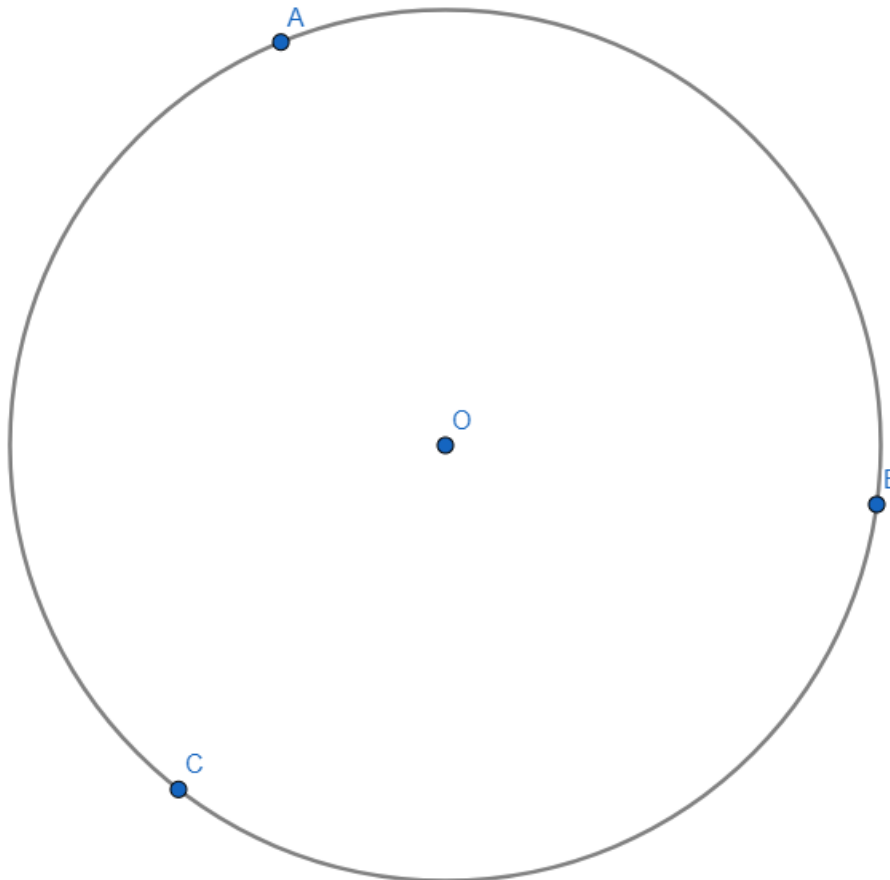


Figure 1

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 in a plane 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 $A \rightarrow B, B \rightarrow C, C \rightarrow A$, so this is also a symmetry. We can denote this r (for "rotation").

Problem 16. If we define a binary operation as composition (eg. $e \times e = eoe$), write out our multiplication table for $\{e, r, r^2\}$.

\times	e	r	r^2
e			
r			
r^2			

Problem 17. What is r^3 ? With this knowledge, how can we write a presentation for the rotational symmetry group of this figure above?

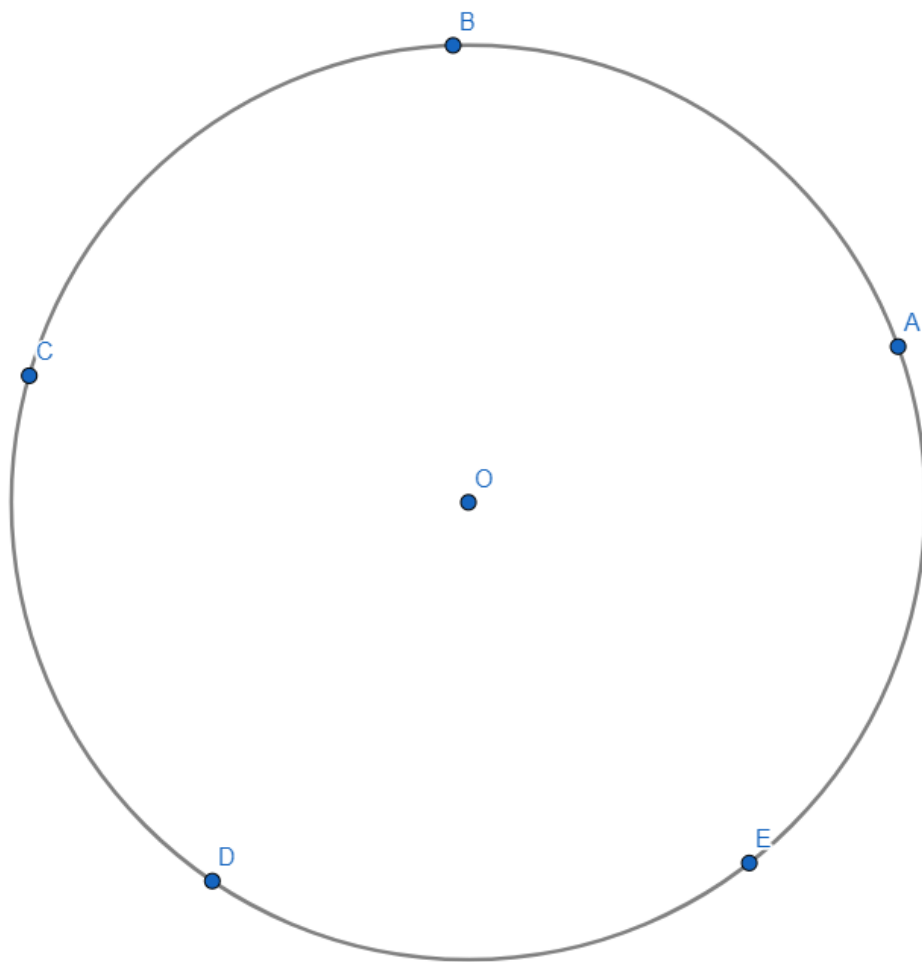


Figure 2

Problem 18. Write the rotational symmetry group for Figure 2.

Problem 19. (Challenge problem) Write the full symmetry group for Figure 1 on a circle (make sure to include the reflectal symmetry).

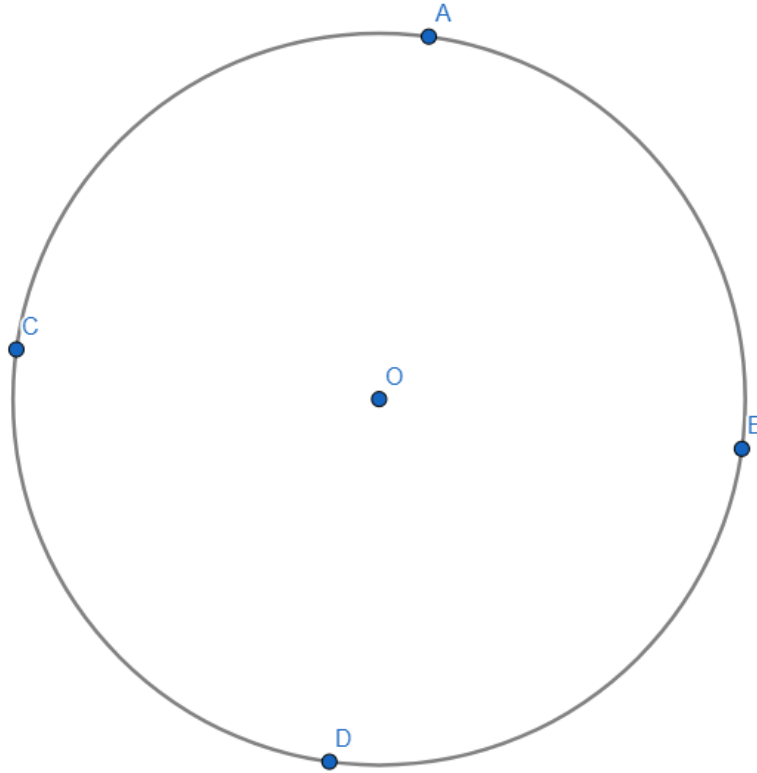


Figure 3

Problem 20. (Challenge problem) Write the full symmetry group for Figure 3 (make sure to include the reflectional symmetry).

5. "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.

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

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

Problem 21. Consider the group $G = \langle a | a^k \rangle$ for some $k > 1$. Describe all the subgroups of G .

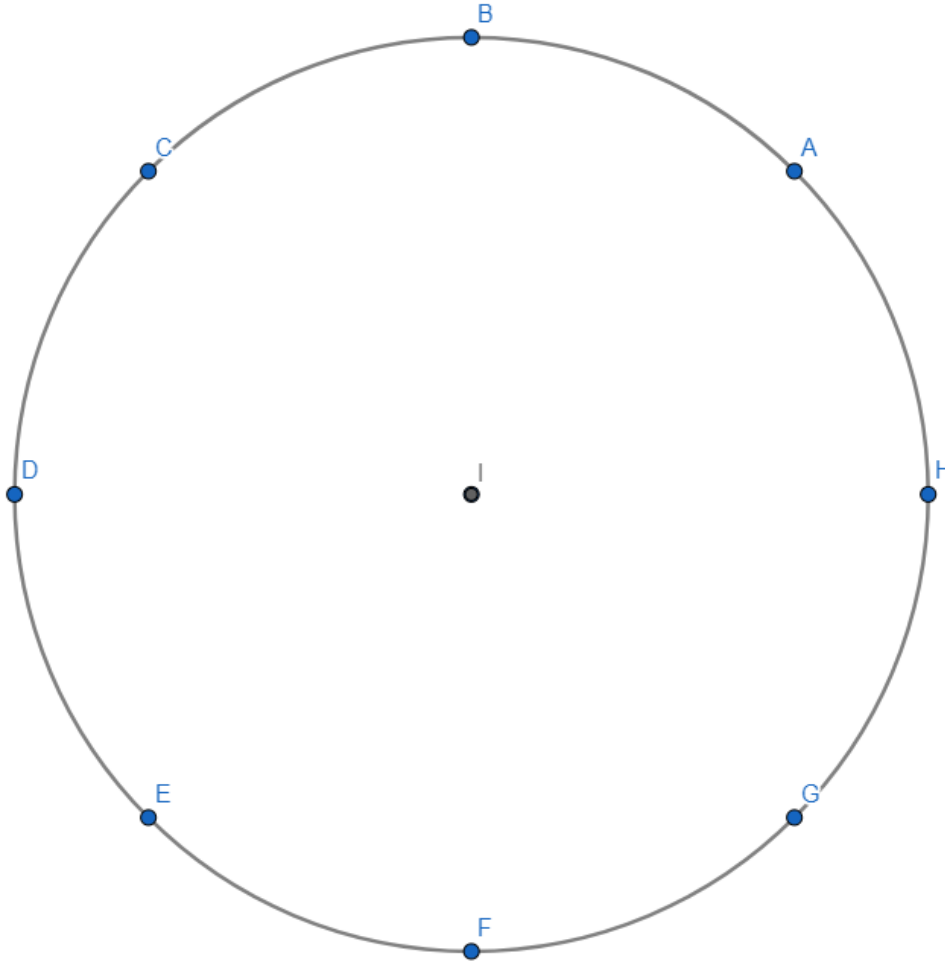


Figure 4

Problem 22. Let G be the rotational symmetry group of Figure 4. What are the subgroups of G ?

Problem 23. For each subgroup you found in Problem 22, draw a figure with rotational symmetry group equal to that subgroup.

Problem 24. Generalise the previous three problems. That is, given a positive integer k , draw a polygon with k points, and find the rotational symmetry group G of that polygon. Find, with proof, all figures that have a rotational group equal to a subgroup of G .

6. CHALLENGE PROBLEMS

Problem 25. Prove that for any prime p , the set $G = \{1, 2, 3, 4, \dots, p-1\}$ with multiplication modulo p forms a group.

Problem 26. Let G be a finite group and $a \in G$. Prove there is an integer $0 < k < |G|$ so that $a^k = e$.

Problem 27. Prove Fermat's Little Theorem: for any prime number p and any integer $a > 0$, $a^p \equiv a \pmod{p}$.

Problem 28. Prove Lagrange's Theorem: Let G be a finite group and let F be a subgroup of G . Then F is a finite group and $|F|$ divides $|G|$.

7. EXTRA CHALLENGING VERY HARD CHALLENGE PROBLEMS

Problem 29. Show that if K and N are two finite subgroups of a group G of relatively prime orders, then $K \cap N = \{e\}$.

Problem 30. Show that if a group G has only finite number of subgroups, then G is finite.

Problem 31. Show that if $a^2 = e$ for all elements a of a group G , then G is abelian (ie. $ab = ba$ for every $a, b \in G$).

Problem 32. Prove that if G is a finite group of even order, then G contains an element a such that $a^2 = e$ and $a \neq e$.