Groups: Symmetry and Sodoku

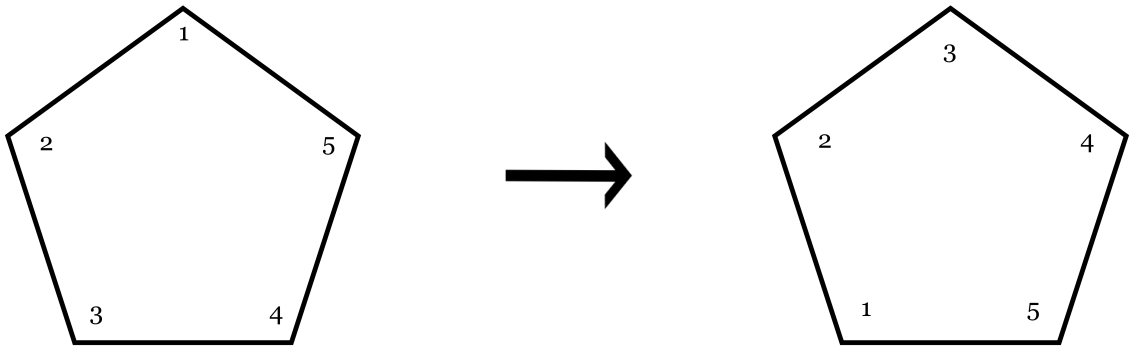
LA Math Circle (High School I)

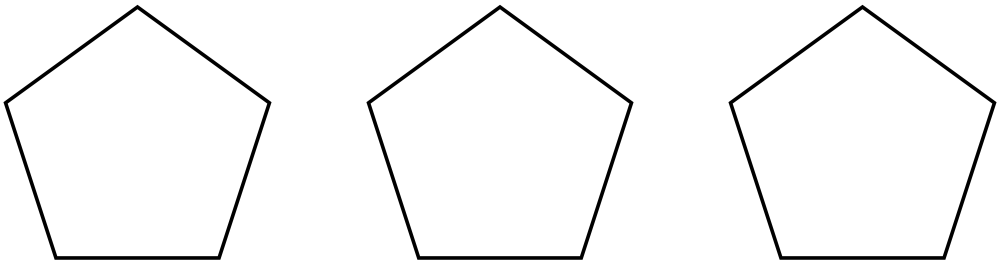
Problem 1 Let's start by taking another look at the symmetry groups of regular polygons.

(a) How many symmetries does a regular n-gon have? Explain clearly why your number is correct. Be sure to explain why there could not possibly be any symmetries that are not on your list.

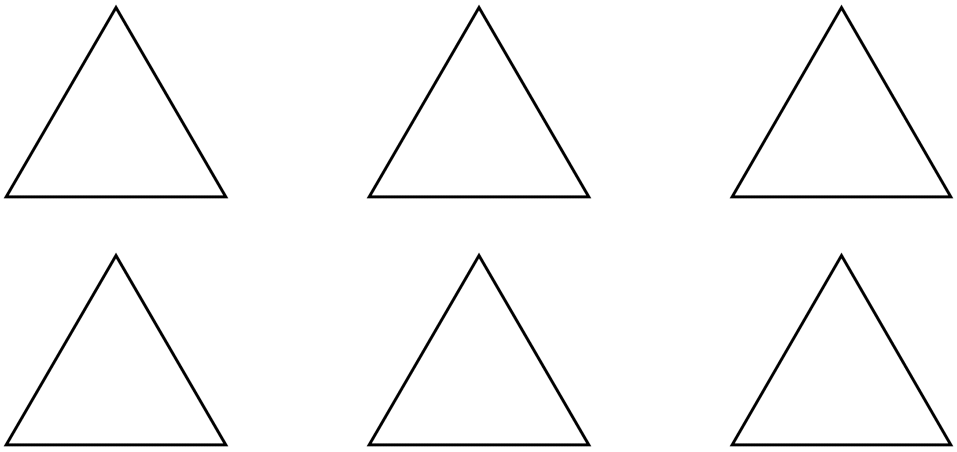
(b) How many of these symmetries are rotations? How many are reflections?

(c) Express the following symmetry of the regular pentagon in the form fr^k for some $k = 0, 1, 2, 3$ or 4 (Remember: r^k means "rotate k vertices counterclockwise," and f means "flip accross the *vertical* axis of the polygon"). Check that your answer is correct using the pentagons below.





(d) Now in the symmetry group of the equilateral triangle, express the symmetry rf in the form fr^k for some $k = 0, 1, 2$. Check that your answer is correct using the triangles below (Remember: f means "flip across the *vertical* axis").



(e) Use part (d) together with the rules $r^3 = 1$ and $f^2 = 1$ to complete the multiplication table of the symmetry group of the triangle:

$\circ$	1	r	r^2	f	fr	fr^2
1						
r						
r^2						
f						
fr						
fr^2						

(f) Explain why, for $n \geq 4$, there are permutations of the n vertices of a regular n-gon which cannot be realized as symmetries of the n-gon (Note: a numerical answer is alright, but include a geometric reason too).

Problem 2 (Sodoku Rule) Note that your multiplication table in 1(e) looks sort of like a completed sodoku puzzle: each row of the table contains each element of the group exactly one time. Prove that this is always true. (Hint: Explain why it is enough to show that if $g_1 \neq g_2$, then $gg_1 \neq gg_2$.)

First Row	g_1	g_2	$\cdots$	g_n
Another Row	gg_1	gg_2	$\cdots$	gg_n

Problem 3 (a) Use the Sodoku rule to complete the following group multiplication tables (Note that the Sodoku rule also holds for each column – there is exactly one occurrence of each element on each row and each column):

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1		
b	b		1	
c	c			1

$\cdot$	1	a	b	c	d
1	1	a	b		
a	a				b
b		c		d	
c		1			
d			1		

$\cdot$	a	b	c	d	e	f	g	h
a								
b		a					e	
c		h				e		a
d	d				h			
e			f	c				
f			g	a	c			
g		e	d		a			
h					f			

(These problems were taken from the following handout on Professor Tim Reluga's website: `http://www.math.psu.edu/treluga/311w/group_sudoku.pdf`)

(b) Determine all possible multiplication tables for a group with 3 elements.

Problem 4 (Some AMC type problems) Compute:

(a) $3^{31} \mod 7$

(b) $29^{25} \mod 11$

(c) $128^{129} \mod 17$

Problem 5 (Fermat's Little Theorem) The first half of this problem is to show that whenever p is a prime number, $\mathbb{Z}/p\mathbb{Z}$ with zero removed forms a group under multiplication (compare to problem 4).

(a) Recall from last year that whenever p is a prime number, if p divides the product ab, then p divides a or p divides b. This means that in $\mathbb{Z}/p\mathbb{Z}$, if $\overline{a} \cdot \overline{b} = \overline{0}$, then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. Use this to prove the cancellation law in $\mathbb{Z}/p\mathbb{Z}$. That is, prove:

$$\text{If } \overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c} \text{ and } \overline{a} \neq 0, \text{ then } \overline{b} = \overline{c}.$$

(b) Use (a) and the pigeonhole principle to show that every $\overline{a} \neq \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. Conclude that $\mathbb{Z}/p\mathbb{Z}$ without $\overline{0}$ is a group under multiplication.

(c) Suppose $\overline{a}$ is in $\mathbb{Z}/p\mathbb{Z}$ and $\overline{a} \neq 0$. Use the Sodoku rule to simplify the product $\overline{a}^{p-1} \cdot \overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1} = (\overline{a} \cdot \overline{1})(\overline{a} \cdot \overline{2}) \cdots (\overline{a}\overline{p-1})$. Once you've done this, deduce Fermat's little theorem: $\overline{a}^{p-1} = \overline{1}$, or $a^{p-1} \equiv 1 \mod p$ when a is not divisible by p.

(d) Use your deep newfound knowledge to re-solve problem 4.

Problem 6 (Cyclic groups – Application to Rubik's Cube) (a) Let's start by thinking about mattress rotations. A normal rectangular mattress like the one shown below has four sensible ways it can be put on a bed. Some people like to flip or rotate their mattress occasionally to make sure it wears evenly. The problem is, they usually rotate the mattress once every month or so, so they tend to forget which way they flipped the mattress the last time. So it is natural to ask whether there is some ideal maneuver of the mattress that you can repeat each month, and which cycles through all possible mattress orientations. Do you think there is an ideal maneuver? Why or why not?

(b) A group G is said to be *cyclic* if there is some element g in G such that every other element can be written as g^n for some n. That is, the set G is equal to the set $\{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}$. The element g is called a *generator* of the group. Is the additive group of integers cyclic? If so, what is a generator? Is the additive group $\mathbb{Z}/n\mathbb{Z}$ cyclic? (Note: If the group G is additive we write ng instead of g^n.)

(c) Explain the following sentence: "There is an ideal mattress flip if and only if the symmetry group of a mattress is cyclic. Furthermore, an ideal mattress flip would be a generator of the group of symmetries."

(d) There are four symmetries of a mattress, $1, r, f, fr$, where r is the rotation by 180° and f means flip upside down across the vertical axis of symmetry. Complete the group multiplication table for the symmetry group of a mattress. Is this a cyclic group? That is, is there an ideal mattress flip?

$\cdot$	1	r	f	fr
1				
r				
f				
fr				

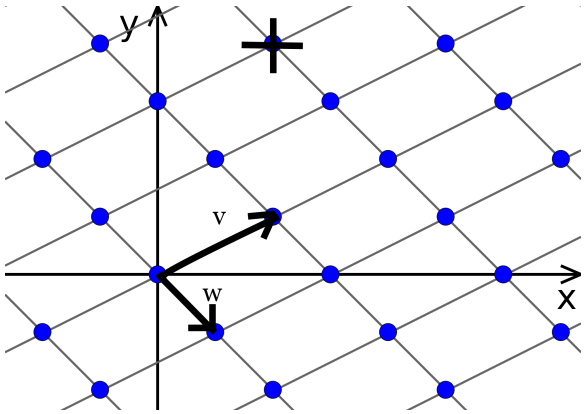
(e) What would it mean if the group of moves of a Rubik's cube was cyclic? Do you think it is?

(f) Prove that any cyclic group G is commutative: $x \cdot y = y \cdot x$ for every two elements x, y in G (Hint: Take a generator g, then write $x = g^n$ and $y = g^m$ for some integers n, m).

(g) Start with a Rubik's cube in a solved position. Is there a single move that you can repeat over and over again which cycles through all possible positions of the Rubik's cube?

Problem 7 (Introduction to Wallpaper Groups) If you haven't already, you may hear at some point in your life that there are only 17 distinct wallpaper patterns. It's actually sort of hard to make this statement precise. For instance, if I have a wallpaper pattern with flamingos on it, should I automatically consider it distinct from a wallpaper pattern with roses? The answer of course is no, if I automatically considered these different, then there would certainly be infinitely many distinct wallpaper patterns. The way to make this statement precise is with group theory. Each wallpaper pattern has a symmetry group, and what we really mean is that there are only 17 different symmetry groups a wallpaper pattern can have. In this problem, we will prove something called the Crystallographic Restriction Theorem, which is an important step in classifying the wallpaper groups as well as studying crystals in chemistry.

(a) A lattice is a set of points which repeats indefinitely in two different directions. The way to define a lattice mathematically is to use vectors. Specifically, we take two nonzero vectors $\vec{v}, \vec{w}$ which are *not parallel*, and then consider the set of all vectors of the form $n\vec{v} + m\vec{w}$ for integers n and m. The set looks like this:



Spend a moment convincing yourself that the set of dots is exactly the set of

all vectors of the form $n\vec{v} + m\vec{w}$. Find the specific integers n and m for the point with the cross through it in the picture above (Note: this is really an exercise in how well you know your vector addition).

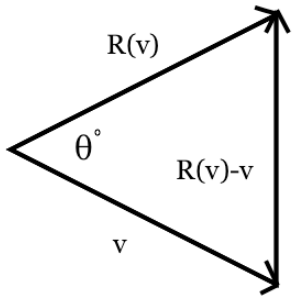
(b) Think about the possible types of symmetries of a lattice. Could a lattice have translational symmetry? Rotational symmetry? Reflective symmetry?

The crystallographic restriction theorem states that it is only possible for a lattice to have a rotational symmetry of $0°, 60°, 90°, 120°$, or $180°$. Another way to say this is that a lattice can only have a 1-fold, 2-fold, 3-fold, 4-fold, or 6-fold rotational symmetry. Interestingly, a 5-fold symmetry is impossible. For this reason, it is impossible to find a wallpaper pattern which is invariant under $72° = (360/5)°$ rotation. Interesting, isn't it?

(c) Prove that a lattice is "closed under addition and subtraction." That is, if we have some lattice, and if $\vec{a}$ and $\vec{b}$ are in the lattice, then so are $\vec{a} + \vec{b}$ and $\vec{a} - \vec{b}$ (Hint: Start by letting $\vec{v}$ and $\vec{w}$ be as in the definition of a lattice. Then we can write $a = n\vec{v} + m\vec{w}$ and $b = n'\vec{v} + m'\vec{w}$, then...).

(d) Any lattice contains a nonzero vector with minimal possible length: the only vector in the lattice which is shorter is the zero vector. Note that if R is a rotational symmetry of a given lattice of degree $\theta°$, and if v is a vector in the lattice with minimal possible length, then we can say several things: First, $R(v)$ is in the lattice, and it has the same length as v. Next, by (c),

the vector $R(v) - v$ is in the lattice. Together, $v, R(v)$, and $R(v) - v$ fit into a picture like the one below. Note that the length of the side $R(v) - v$ must be at least as long as v and $R(v)$. Use some trigonometry and one of the basic facts about isosceles triangles to prove that $\theta \geq 60$.



(e) Draw a similar diagram to rule at $\theta = 72$. This time, show that if $\theta = 72$, then $R^2(v) + v$ is in the lattice and has shorter length than v, which is impossible. From (d) and (e), deduce the crystallographic restriction theorem.