Groups: Symmetry and Sodoku

LA Math Circle (High School I)

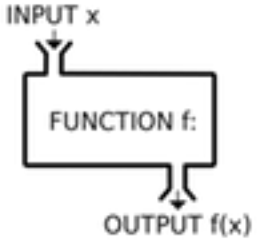
Today we will study groups, which give us a method to turn problems about symmetry, number theory, and Rubik's cubes into simple algebra problems. Permutations will come up over and over again, so we might as well start out with some:

Preliminaries on Permutations

Recall that a *set* is just a collection of objects. Here are some examples of sets:

1. The set $\mathbb{N} = \{0, 1, 2, \dots\}$ of natural numbers.
2. The set $\mathbb{R}$ of real numbers.
3. The set $\{0, 4, 7, 1\}$. Is this the same set as $\{4, 7, 0, 1\}$?
4. The set {George Washington,...} of all U.S. Presidents.

If X and Y are sets, then a function f from X to Y is a rule that assigns to every element x in the set X a unique element $f(y)$ of the set Y.



If f is a function from X to Y and g is a function from Y to Z, there is a way to construct a function $g \circ f$ from X to Z. The rule is (fill in the blank):

$$(g \circ f)(x) =$$

The way we'll write most of our functions today is in a table like this:

$$\begin{pmatrix} x_1 & x_2 & \cdots \\ f(x_1) & f(x_2) & \cdots \end{pmatrix}.$$

For example, if f is the function from the set $\{1, 2, 3\}$ to the set $\{\text{blue}, \text{green}\}$ defined by $f(1) = f(2) = \text{blue}$, and $f(3) = \text{green}$, our table would look like this:

$$\begin{pmatrix} 1 & 2 & 3 \\ \text{blue} & \text{blue} & \text{green} \end{pmatrix}.$$

Intuitively, a permutation is just a rearrangement of the elements of a set. We will view a permutation as a special kind of function from a set X to itself.

Problem 1 Which of the following functions are permutations of the set $\{1, 2, 3, 4\}$? In each case where the function is not a permutation, explain why not.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Here is the formal definition. A function f from a set X to itself is a *permutation* if it satisfies both of the following:

1. For each element y of X, there is an element x in X such that $f(x) = y$.

2. If x and x' are elements of X and $f(x) = f(x')$, then $x = x'$.

Problem 2 Prove the following facts about permutations.

(a) If f and g are permutations of the set X, then so is $f \circ g$.

(b) If f is a permutation of a set X, then f has an inverse: there is another function g such that $g \circ f = f \circ g = \text{id}_X$ (id_X is the identity function on X, defined by the rule $\text{id}_X(x) = x$).

(c) Conversely, if f is a function from the set X to itself and there is another function g from X to itself such that $f \circ g = g \circ f = \mathrm{id}_X$, then f is a permutation of X.

(d) If X is a finite set and f is a function from X to itself which satisfies (2) in the definition of permutation, then it automatically satisfies (1) as well (Hint: Pigeonhole).

Groups!

A group is a set which has a rule for multiplying and dividing its elements. The prototype for a group is example 1 below: the set of real numbers without zero. More precisely:

A *group* is a set G together with a rule $\cdot$ which assigns to every two elements g, h in G another element $g \cdot h$. This rule must satisfy:

(1) (Associativity) $(g \cdot h) \cdot k = g \cdot (h \cdot k)$

(2) (Identity) There must be an element 1 in G such that $g \cdot 1 = 1 \cdot g = g$ for every element g.

(3) (Inverses) For every element g in G, there must be an element g^{-1} in G so that $g \cdot g^{-1} = 1 = g^{-1} \cdot g$.

Examples

(1) The set $\mathbb{R} \setminus \{0\}$ of all real numbers *except* zero is a group under multiplication.

(2) The set $\mathbb{R}$ of all real numbers is *not* a group under multiplication. Why not? It is a group under the rule + though.

(3) The set S_n of all permutations of the set $\{1, 2, \ldots, n\}$ can be made

into a group called the *symmetric group*. How do you "multiply" two permutations? How many elements does this group have? (Note: we will see what's so symmetric about it later today.)

We will give more examples later, but for now let's prove a couple basic properties of all groups to get the hang of things.

Problem 3 (a) (Cancellation Law) Prove that if $g \cdot h = g \cdot k$ in a group G, then $h = k$.

(b) Prove that if g, h are elements of a group, then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

(c) Prove that $g \cdot h = h \cdot g$ in a group if and only if $g \cdot h \cdot g^{-1} \cdot h^{-1} = 1$.

(d) Prove that a group can only have one multiplicative identity element: If $1'$ is an element of G such that $g \cdot 1' = 1' \cdot g = g$ for every element of g, then $1 = 1'$.

(e) Prove that if g, h are elements of a group G, then there is another element of the group k such that $g \cdot k = h$. Prove also that there is an element k' of G such that $k' \cdot g = h$. Does k have to be the same as k'? Why don't we write $k = \frac{h}{g}$?

Group Multiplication Tables

If $G = \{g_1, g_2, \ldots, g_n\}$ is a group, we can create the group multiplication table for G which looks as follows:

$\cdot$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 \cdot g_1$	$g_1 \cdot g_2$	$\cdots$	$g_1 \cdot g_n$
g_2	$g_2 \cdot g_1$	$g_2 \cdot g_2$	$\cdots$	$g_2 \cdot g_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
g_n	$g_n \cdot g_1$	$g_n \cdot g_2$	$\cdots$	$g_n \cdot g_n$

For example, we have all seen the following group whose addition table is

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

This group is called $\mathbb{Z}/4\mathbb{Z}$. The rule for addition is: add the elements and then take the remainder mod 4. More generally, we have a group $\mathbb{Z}/n\mathbb{Z}$ for every n. Recall that there's also a rule for multiplication on $\mathbb{Z}/n\mathbb{Z}$ as well. You might wonder: is $\mathbb{Z}/n\mathbb{Z}$ a group with respect to multiplication when we take away zero?

Problem 4 Fill in the following multiplication tables. The first is for $\mathbb{Z}/5\mathbb{Z}$ without zero and the second is for $\mathbb{Z}/6\mathbb{Z}$ without zero. Are these groups?

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				
$\overline{4}$				

$\mathbb{Z}/5\mathbb{Z}$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$					
$\overline{2}$					
$\overline{3}$					
$\overline{4}$					
$\overline{5}$					

$\mathbb{Z}/6\mathbb{Z}$

Problem 5 (Symmetry Groups) Perhaps the most important reason we study groups is because they give us a way of describing symmetry. In mathematics, a symmetry of an object is a way of transforming the object without changing its overall shape. The set of symmetries of an object always forms a group.

In this problem, you will use the cutouts on your table to understand the group of symmetries of an equilateral triangle and a regular pentagon.

(a) How many elements are there in the symmetry group of an equilateral triangle? How about a regular pentagon?

(b) Note that each symmetry of an equilateral triangle or a regular pentagon is a permutation of its vertices. Can all possible permutations of the vertices of the triangle be achieved in this way? How about the pentagon?

(c) Note that each symmetry of an equilateral triangle takes the following form: rotate 60° clockwise 0 times, 1 time, or 2 times, then possibly flip upside down. If f and g are symmetries of an object, then $g \circ f$ means "first do f, then do g" (Note the weird order. Also, we might just right gf if we're lazy). Thus if r is the symmetry "rotate 60° counter-clockwise" and f is the symmetry "flip upside down," then the following is a list of all symmetries of the triangle:

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

(Note: r^2 means "do symmetry r twice"). Fill in the multiplication table of symmetry group of the triangle:

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

Hint: Just figure out what rf is, the rest is algebra.

(d) In the symmetry group of the pentagon, let $r =$ "rotate 72° counter-clockwise" and $f =$ "flip upside down." Again, note that every symmetry can be written as either r^k or fr^k for $k = 0, 1, 2, 3$, or 4. Write rf in this form.

Problem 6 (Sodoku Rule) Note that each row in your multiplication table in 5(c) is a permutation of the first row. Prove that this is always true. (Why is this called the Sodoku rule? Hint: Look back at the definition of permutation, then look at problems 3(a) and 3(e).)

Problem 7(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 8 (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.

Problem 9 (Basic Number Theory from Perspective of Group Theory) If H is a subset of a group G, we say that H is a *subgroup* of G if: (a) $1 \in H$, (b) whenever a, b are elements of H, $a \cdot b$ is also an element of H, and (c) whenever a is an element of H, a^{-1} is also an element of H.

(a) The set $\mathbb{Z}$ of integers is a group under $+$. If n is an integer, show that $n\mathbb{Z} = \{nx | x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ (ask someone if you don't know what this notation means).

(b) Show that all subgroups of $\mathbb{Z}$ have this form (Hint: division with remainder).

(c) If a, b are integers, show that $a\mathbb{Z} + b\mathbb{Z} = \{ax + by | x, y \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

(d) By (a) and (b), if a, b are integers, then there is another integer d such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Prove that d is a greatest common divisor of a and b (Prove that d divides a and b, and if e is another number that divides a and b, then e divides d).

(e) Prove that if a and b have no common divisors except 1, then there are integers x and y such that $ax + by = 1$.

(f) Use (e) to prove that if p is prime and $p|ab$, then $p|a$ or $p|b$.