2026 National Math Camps: *What even is algebra?*

Introduction to Group Theory

Hello! If you are reading me, I am guessing that you were a student in my course and already know the premise of my intent. If that is not the case, allow me to explain: I am a PDF compilation of the worksheets used by David Lieberman in his Summer 2026 National Math Camps course. The course was called "What even *is* algebra," and was an exploration into the world of groups through eight 75-minute class periods. The students were middle-school-aged mathematics enthusiasts. In class, students participated in lecture by filling out the worksheets and engaged the material through problems and exercises. I (the document) am the completion of those worksheets with a little bit extra added (aided by the instructor's hindsight).

David (remember, this is the document talking to you), hopes you enjoy these notes as much as David enjoyed teaching the course. He said if you have any questions please reach out! His most current email address will always be found on his website.

0 Good Things to Know

- A ***subset*** of a set A is a collection of elements of A. For example, the set of even integers is a subset of the set of integers. To indicate this relation, we use the symbol $\subseteq$. That is, $B \subseteq A$ means B is a subset of A.
- $\mathbb{N}$ is the set of all natural numbers.
- $\mathbb{Z}$ is the set of all integers.
- $\mathbb{Q}$ is the set of all rational numbers.
- $\mathbb{R}$ is the set of all real numbers.
- To prove an *if and only if* statement, you must prove two directions separately:

> If you want to prove something of the form
>
> "**A** is true *if and only if* **B** is true,"
>
> you can prove both of the if-then statements:
>
> "If **A** is true then **B** is true" and "If **B** is true then **A** is true"

1 In the Beginning: Operations and Groups

Definition 1.1. Let A be a set of things. An operation on A is a rule for combining any two elements of A. If combining any two elements of A always results in an element of A, we say that A is closed under the operation .

Definition 1.2. Let G be a set, and let $*$ be an operation on G such that G is closed under $*$. If the following conditions are always true, then we say that G (with the operation $*$) is a group .

- Associativity : for any elements a, b, and c in G, $(a * b) * c = a * (b * c)$
- Identity element : there is a special element that leaves elements unchanged under the operation. There is some element e in G such that $a * e = e * a = a$
- Inverses : Every element has an inverse . For any element g in G, there is an element g^{-1} such that $g * g^{-1} = 1$.

Exercise 1.3. For each of the following (and all "math problems" that you solve in life!), be sure to give an explanation for why your solution is right.

1. Is the set of integers with multiplication as the operation a group? How do you know?

   Proof. No! The integers with multiplication does not form a group. In such a structure, the inverse of 2 (for example) must be $\frac{1}{2}$. However $\frac{1}{2}$ is not an integer. So 2 does not have an inverse, which violates the third condition from Definition 1.2. □

2. We know that $g * g^{-1} = e$ for every element of a group g. Prove that it also true that $g^{-1} * g = e$.

   Proof. Suppose I pick a random element g from the group G. We know that there is some other group element g^{-1} such that $g * g^{-1} = e$. Our goal is to show that

$g^{-1} * g = e$. By the identity element property, we know that applying e foes not change $g^{-1} * g$. So we know that

$$g^{-1} * g = (g^{-1} * g) * e \qquad (1)$$

By the inverse property of groups, we know that $g^{-1} * g$ has an inverse element. Let's have y be the inverse of $(g^{-1} * g)$, which means $(g^{-1} * g) * y = e$. Use this to make a substitution into (1):

$$g^{-1} * g = (g^{-1} * g) * \big((g^{-1} * g) * y\big) \qquad (2)$$

Next use associativity to rearrange the parentheses on the right-hand side of (2), then simplify by twice using the fact that $g * g^{-1} = e$:

$$\begin{aligned} g^{-1} * g &= \Big(g^{-1} * (\cancel{g * g^{-1}}\,^{e}) * g\Big) * y \\ &= \Big(g^{-1} * g\Big) * y \end{aligned}$$

Remember that we chose y to be the inverse of $(g^{-1} * g)$. Now use that fact!

$$g^{-1} * g = \Big(g^{-1} * g\Big) * y = e.$$

Thus we have shown that $g^{-1} * g = e$, as desired. □

3. Let $A = \{a, b, c\}$. Can you define an operation on the set A that makes it a group?

Solution. There are multiple approaches here, but a straightforward way is to make a table for the operation. There are 6 possible ways to do this for the given set A, but in a sense they will all be the same (that is called foreshadowing!). Here is an example of one such table:

	a	b	c
a	c	a	b
b	a	b	***c***
c	b	c	a

(Remember that the order we apply the operation is (row) $*$ (col). For example, the red $\boldsymbol{c}$ indicates that $b * c = \boldsymbol{c}$. □

4. Give an example of a group that uses multiplication as the operation. That is, find a set of numbers and prove that the operation of multiplication is associative has an identity element, and has inverses on that set.

   Solution. There are many choices here, so the following is not exhaustive. Here are some examples of sets of numbers that form a group with multiplication as the operation:

   - The set of all real numbers
   - The set of all rational numbers
   - The set of all complex numbers
   - The set of nonzero integers modulo p for any prime number p.
   - Choose any nonzero number n and use the set

   $$\left\{\ldots, \frac{1}{n^3}, \frac{1}{n^2}, \frac{1}{n}, 1, n, n^2, n^3, \ldots\right\}$$

   □

5. For each of the three shapes you have, describe the group of symmetries. What are the elements of the group, and what is the group operation?

   Solution. For all three groups, the operation is composition (do one then the other).

   Symmetries of an equilateral triangle:

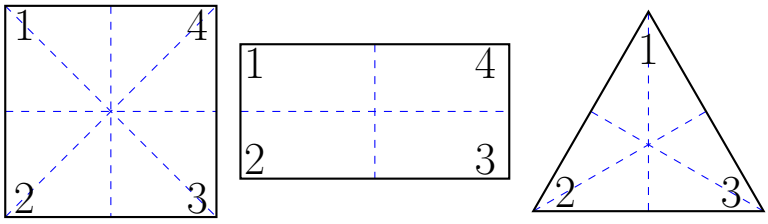
   - Identity: Do Nothing
   - Clockwise Rotations: 120°, 240°
   - Counter Clockwise Rotations: 120°, 240°
   - Reflections: There are three reflections. There is an axis of reflection through each vertex and perpendicular to the opposite side.

   Symmetries of a square:

   - Identity: Do Nothing
   - Clockwise Rotations: 90°, 180°, 270°
   - Counter Clockwise Rotations: 90°, 180°, 270°
   - Reflections: There are four of these. Their axes of reflection are the two perpendicular bisectors and the two lines connecting opposite corners.

   Symmetries of a non-square rectangle:

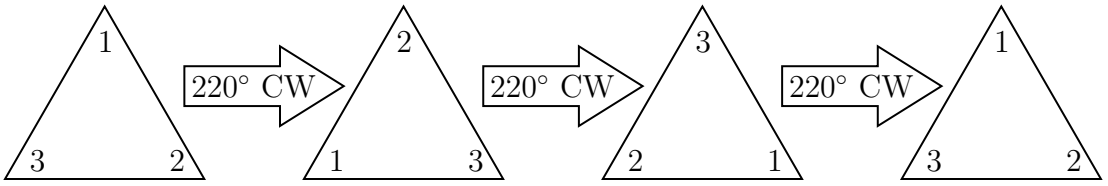
   - Identity: Do Nothing
   - Clockwise Rotations: 180°
   - Counter Clockwise Rotations: 180°
   - Reflections: There are two of these. Their axes of reflection are the two perpendicular bisectors



□

6. The ***order*** of an element of a group is the smallest number of times it takes to get to the identity by combining the element with itself. ~~What is the order of the rotations for each of the shapes?~~. Pick a non-identity element of the symmetries of the square, and find the order of it.

   Proof. There are a few answers here, but you find them all the same way. Pick a non identity element for one of the symmetry groups, and apply it repeatedly until the shape is back to where it started. For example, consider the clockwise rotation of 240° on the equilateral triangle. If you apply it to our labeled triangle once then the 2 is on top. Apply again and the 3 is on top. One more application gets the 1 back to the top, so the order of the element is 3.



□

2 Every Day I'm Shuffling: Permutation Groups

Definition 2.1. Let A and B be sets. Let f be a function whose inputs come from A and whose outputs come from B. We use the following to denote this situation:

$$f : A \to B$$

- If no two inputs share the same output, we say that the function is injective or one-to-one.
- If every element of B is the output for some input, then we say that the function is surjective or onto.
- If a function is injective and surjective, we say that the function is bijective.

We can compose two functions by using the output from one function as the input of another function. We use $\circ$ to denote the composition of functions. Specifically, we can write things like

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

Definition 2.2. We will use the symbol S_n to denote the set of all bijections from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$. We call this collection the set of permutations on {1,2,. . . , n}.

Exercise 2.3.

1. For any natural number n, how many functions are in the set S_n? Can you prove it?

   Claim: The set S_n is a set with $n!$-many elements.

   Proof. Remember that every function in S_n uses the set $\{1, 2, 3, \ldots, n\}$ as its input set, and the same for the outputs. So to identify any particular function from the set S_n, I can write down what the output is for each input.

   - Consider the input 1. Its output could be any of the n elements in the output set$\{1, 2, 3, \ldots, n\}$. Once we use an output, we cannot use it again (to maintain

a bijection).

- Now what about the input 2? We have one fewer choice in output now (since we cant repeat the output of 1). Thus there are $n-1$ choices for this output.
- For the input 3, there is one fewer choice again. Thus there are $n-2$ choices.

$$\vdots$$

keep repeating

$$\vdots$$

- By the time we get to pick the output for n, there will be only 1 choice left.

To count the number of ways to pick outputs in this way, we multiply the number of choices. This gives us $n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1 = n!$ different bijections in S_n. □

2. Is composition an operation on S_n? If it is an operation, is S_n closed under composition?

Solution. Yes, and yes! Composition is a well defined operation on functions when the outputs of the first function are valid inputs for the second function. Since functions in S_n use the set $\{1, 2, 3, \ldots, n\}$ for the inputs *and* outputs, they will always line up in this way.

To verify that S_n is closed under composition, let's suppose that f and g are any two permutations from S_n. We must show that $h = f \circ g$ is also a permutation, or in other words we must show that $f \circ g$ is a bijection.

- Suppose that we find two whole numbers x and y between 1 and n (inclusive) such that $h(x) = h(y)$. Then $f\big(g(x)\big) = f\big(g(y)\big)$. Since f is a bijection it is injective, and thus the inputs $g(x)$ and $g(y)$ must be the same. But then we have an injective function g with $g(x) = g(y)$, so then $x = y$.

  We just showed if $h(x) = h(y)$, then $x = y$. That means $h = f \circ g$ is injective.

- Let N be any whole number between 1 and n (inclusive). If we can show that there is some input x so that $h(x) = N$, then we can conclude that h is surjective.

  Since f is, in particular, surjective, we know there is some input y such that $f(y) = N$. Because g is, in particular, surjective, we know that there is some input x such that $g(x) = y$. Now notice that

  $$h(x) = f(g(x)) = f(y) = N.$$

  So we found the desired input, which means that the composition is surjective too!

□

3. Consider the set S_4. Find a permutation that leaves other permutations unchanged after composition.

   Solution. The following permutation is the one that leaves others unchanged after composition:

   $$1 \mapsto 1$$
   $$2 \mapsto 2$$
   $$3 \mapsto 3$$
   $$4 \mapsto 4$$

□

4. Write down a permutation from the set S_4. Does this permutation have an inverse function? If so, what is the inverse?

Solution. Your solution will vary depending on your choice of permutation. Here is an example of a permutation and its inverse:

A permutation:	Its Inverse:
$1 \mapsto 3$	$1 \mapsto 2$
$2 \mapsto 1$	$2 \mapsto 4$
$3 \mapsto 4$	$3 \mapsto 1$
$4 \mapsto 2$	$4 \mapsto 3$

□

5. Consider the set S_n for an arbitrary natural number n, and the operation $\circ$. Prove that this is a group:

   (a) Convince yourself that $\circ$ is associative.

   Solution. We may happily accept that function composition is associative, though it can be proved true! It might even be a fun thing for you to do! □

   (b) Find the identity permutation e and describe it as explicitly as you can.

   Solution. The identity permutation will always be the identity function:

$$1 \mapsto 1$$
$$2 \mapsto 2$$
$$3 \mapsto 3$$
$$\vdots$$
$$n \mapsto n$$

□

   (c) Does every permutation have an inverse? If I give you a permutation, how do you find its inverse?

   Solution. Yes! To find a permutation's inverse, you reverse the arrows! □

3 Shake It Off: More Permutations

Definition 3.1. The notation

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

denotes the permutation that sends each number in the top row to the number directly below it. We call this stack notation.

The notation $(a_1\, a_2 \cdots a_t)$ refers to the (special kind of!) permutation that sends each number to the next one on the list, sends the last number to the first number, and sends unlisted numbers to themselves.
If a cycle has t-many numbers in it, we call it a t-cycle

◁ **Remark:** Remember that a cycle is a permutation, and a permutation is a function. So if we have cycles side-by-side, this refers to composition of functions, where the composition as usual goes from right to left. ▷

Exercise 3.2.

1. Write the permutation $(1\,3\,5)(2\,7) \in S_7$ in permutation stack notation.

   Solution. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 1 & 6 & 2 \end{pmatrix}$ □

2. Write the following permutation in cycle notation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 2 & 4 & 7 & 5 \end{pmatrix} \in S_7$$

   Solution. $(1\,3)(2\,6\,7\,5\,4\,2)$ □

3. List all elements of S_3 in cycle notation. What is the order of each?

   Solution. Order 1 Elements:

   - $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = (1)$

   Order 2 Elements:

   - $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1\,2)$
   - $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1\,3)$
   - $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2\,3)$

   Order 3 Elements:

   - $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1\,2\,3)$
   - $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1\,3\,2)$

   □

4. What is the inverse of $(1\,2\,3)$? What is the inverse of $(1\,2\,3\,4)$? How about $(1\,2\,3\,4\,5)^{-1}$?

   Solution. To find the inverse, you reverse the order! The inverse of $(1\,2\,3)$ is $(3\,2\,1)$, the inverse of $(1\,2\,3\,4)$ is $(4\,3\,2\,1)$, and $(1\,2\,3\,4\,5)^{-1} = (5\,4\,3\,2\,1)$. □

Definition 3.3. A permutation is odd if it is a composition of an odd number of 2-cycles, and even if it is a product of an even number of 2-cycles. Cycles are disjoint if they share no numbers in common.

1. Find one example of each type of element in S_5 or explain why there is none:

   (a) A 2-cycle

   (b) A 3-cycle

   (c) A 4-cycle

   (d) A 5-cycle

   (e) A 6-cycle

   (f) A product of disjoint transpositions

   (g) A product of a 3-cycle and a disjoint 2-cycle.

   (h) A product of 2 disjoint 3-cycles.

Solution. Note that some of these may have any number of valid answers:

(a) $\begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix} = (2\,4)$

(b) $\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix} = (1\,4\,3)$

(c) $\begin{pmatrix}1&2&3&4&5\\5&1&2&4&3\end{pmatrix} = (1\,5\,3\,2)$

(d) $\begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix} = (1\,4\,5\,3\,2)$

(e) Not possible! Using cycle notation, a 6-cycle would have 6 slots to fill. Since we can only use the numbers 1, 2, 3, 4, and 5, we would have to repeat a number in the cycle notation, which means it is not a cycle!

(f) $(2\,5)(4\,3) = \begin{pmatrix}1&2&3&4&5\\1&5&4&3&2\end{pmatrix}$

(g) $(1\,3\,5)(2\,4) = \begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix}$

(h) Cannot be done! To write two disjoint 3-cycles, we would need to pick two groups of three whole numbers from 1 to 5 with no overlaps. There are not enough numbers to do that!

□

2. For each example in (1), find the order of the element.

Solution. We omit parts (e) and (h), as no such elements exist:

(a) $(2\,4)(2\,4) = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix} = e$, so the order is 2.

(b) $(1\,4\,3)(1\,4\,3) = (1\,3\,4)$, and $(1\,4\,3)(1\,4\,3)(1\,4\,3) = e$, so the order is 3

(c) The order of any 4-cycle is 4. Can you prove it?

(d) The order of any 5-cycle is 5. Can you prove it?

(f) The product $(2\,5)(4\,3)$ is the permutation "Swap positions 4 and 3, then swap positions 2 and 5." If you do it twice, it "undoes" both swaps. Thus we conclude that the order is 2.

(g) Think about the order of each of the parts: the order of $(2\,4)$ is 2 and the order of $(1\,3\,5)$ is 3. This means that $(2\,4)^n = e$ whenever n is even, and $(1\,3\,5)^m = e$ whenever m is divisible by 3. 6 is the smallest number that is divisible by 2 and

3, so it is the smallest value we could use for n and m. This means that the order $(1\,3\,5)(2\,4)$ is 6.

Comment from the Author: *In parts (f) and (g) directly above, one might find a pattern beginning to emerge. Can you find a method for calculating the order of a product of cycles? Can you prove that your method always gives the right order?* □

3. What are all possible orders of elements in S_5?

Solution. The smallest order an element can have in S_5 (or any group) is 1. The identity element always has order 1. We can also find cycles of order 2, 3, 4, and 5. We also saw above that the order $(1\,3\,5)(2\,4)$ is 6. Can we find any elements with larger order than 6?

In hindsight, this question was more about vibes than it was rigor. To prove anything about possible orders of elements, we need to use the following fact:

> **Theorem 3.4.** *Let n be any positive integer. Every element of S_n can be written as a product of disjoint cycles. (This disjoint cycle representation is unique up to some mild conditions about the irrelevance rearranging.)*

□

4. ~~What are all possible orders of cyclic subgroups elements of S_5.~~

I did not mean to include this question. Though maybe you can learn more about groups until you are able to answer it!

5. For each example in (1), write the element as a product of ~~transpositions~~ 2-cycles. Which are even and which are odd?

Solution.

(a) $(2\,4)$ is odd

(b) $(1\,4\,3) = (1\,3)(1\,4)$ is even.

(c) $(1\,5\,3\,2) = (1\,2)(1\,3)(1\,5)$ is odd.

(d) $(1\,4\,5\,3\,2) = (1\,5)(1\,3)(1\,2)(1\,4)$ is even.

(f) $(2\,5)(4\,3)$ is even

(g) $(1\,3\,5)(2\,4) = (1\,5)(1\,3)(2\,4)$ is odd.

□

4 What's Purple and Commutes? [1]

Definition 4.1.

- Let G be a group with operation $*$, and let H be a subset of G. If H with the same operation $*$ is also a group , we say H is a subgroup of G.
- The number of elements in a group is called the order of the group . If G is a group we denote this by $|G|$

Exercise 4.2.

1. Suppose $(G, *)$ is an abelian group. Prove that $(a \cdot b)^n = a^n \cdot b^n$ for all $a, b \in G$ and for all natural numbers n.

   Proof. We start with two elements a and b from an abelian group. We will start with $a^n \cdot b^n$ and manipulate it until we have shown it is equal to $(a \cdot b)^n$. First check out this:

   $$\begin{aligned} a^n \cdot b^n &= (\underbrace{a \cdot \cdots \cdot a}_{n \text{ times}}) \cdot (\underbrace{b \cdot \cdots \cdot b}_{n \text{ times}}) \\ &= (\underbrace{a \cdot \cdots \cdot a}_{n-1 \text{ times}}) \cdot (a \cdot b) \cdot (\underbrace{b \cdot \cdots \cdot b}_{n-1 \text{ times}}) && \text{(Associativity of the group)} \\ &= (a \cdot b)(\underbrace{a \cdot \cdots \cdot a}_{n-1 \text{ times}}) \cdot (\underbrace{b \cdot \cdots \cdot b}_{n-1 \text{ times}}) && \text{(Group is abelian)} \end{aligned}$$

   To summarize what we did, we expanded the powers, then pulled-out the middle pairing of $a \cdot b$ (associativity) and moved it to the front (abelian). Repeat this process on the remaining expanded part of the product $n-1$-more times and you are left with

   $$a^n \cdot b^n = \underbrace{(a \cdot b) \cdot \cdots \cdot (a \cdot b)}_{n \text{ times}}$$

   By the definition of exponential notation, this means that $(a \cdot b)^n = a^n \cdot b^n$. □

2. Suppose G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$. Show that G must be abelian.

   Proof. Let a and b be any elements from this group G. We want to prove that $a \cdot b = b \cdot a$. We know that $(a \cdot b)^2 = a^2 \cdot b^2$. Let's muck about with inverses and see if we get our desired result:

$$\begin{aligned}
(a \cdot b)^2 &= a^2 \cdot b^2 \\
(a \cdot b) \cdot (a \cdot b) &= a \cdot a \cdot b \cdot b \\
a^{-1} \cdot a \cdot b \cdot a \cdot b \cdot b^{-1} &= a^{-1} \cdot a \cdot a \cdot b \cdot b \cdot b^{-1} \\
e \cdot b \cdot a \cdot e &= e \cdot a \cdot b \cdot e \\
b \cdot a \cdot &= \cdot a \cdot b
\end{aligned}$$

   So we have derived the equality $a \cdot b = b \cdot a$, which means the group is abelian. □

3. Suppose $(G, *)$ is a group such that $|G|$ is finite, and let g be any element of G. Prove there is some positive integer N such that $g^N = e$.

   Proof. Remark: The proof of this one ended up being much more involved than I originally anticipated. Though we skipped it in class, below is the proof of this fact. Also to make notation easier and more readable, we adopt the following convention:

$$(x^{-1})^k = x^{-k}$$

   Let G be a group such that $|G| = n$ is finite. That is, G has a finite number of elements, and that number is n. Let g be any element of this group, and consider the following list of elements of G:

$$g, g^2, g^3, g^4, \ldots, g^n, g^{n+1}$$

   This list has $n + 1$ things in it, while the group G has n-many elements. Thus there must be at least two things on our list that are the same (Pigeon Hole Principle!). Let's call these two powers g^a and g^b, where $a < b$. We start with the equality

$$g^a = g^b$$

Multiply on the right by g^{-1} a-times on both sides of the equality and simplify:

$$\begin{aligned} g^a g^{-a} &= g^b g^{-a} \\ (gg^{-1})^a &= g^{b-a} g^a g^{-a} \\ e^a &= g^{b-a}(gg^{-1})^a \\ e &= g^{b-a} e^a \\ e &= g^{b-a} \end{aligned}$$

So we found a power $N = b - a$ such that $g^N = e$. So we conclude that every element of G has such a power N. □

4. Show that if every element of the group G is its own inverse, then G is abelian.

   Let G be a group where every element is its own inverse. Let a and b be any two elements of G. We want to show that $ab = ba$. Note that $(ab)(ab) = e$, since every element is its own inverse. Lets start there and do some manipulating:

$$\begin{aligned} (ab)(ab) &= e && \\ a(ba)b &= e && \text{(Associativity)} \\ aa(ba)b &= ae && \text{(multiply on left by } a\text{)} \\ (ba)b &= a && \text{(Simplify)} \\ (ba)bb &= ab && \text{(multiply on right by } b\text{)} \\ ba &= ab && \text{(Simplify)} \end{aligned}$$

   We have done it! We showed that $ab = ba$ for any elements a and b from the group G. So we conclude that the group is abelian.

Theorem 4.3. ***The Subgroup Test***

Let $(G, *)$ be a group and let H be a non-empty subset of G. If H is closed under the operation $*$ and every element in H as an inverse that is also in H, then $(H, *)$ is a group.

Edit: though it may seem silly to think that one would consider the case of the empty set, we must be clear that H is a non-empty subset of G. For a group must have at least one element, otherwise it is nothing at all! This is a subtle but important fact to consider, for example, in the proof of the following problem about the center of a group. Hence I have added the italicized text above.

Proof. Suppose we have a group $(G, *)$ and a subset $H \subseteq G$ that satisfies the following two properties:

- **Property 1:** H is closed under the operation $*$. That is, if x and y are elements of H, then $x * y$ is an element of H.
- **Property 2:** Every element of H has an inverse in H. That is, if x is any element of H, then x^{-1} is also an element of H.

To prove that $(H, *)$ is a group, we will use the above assumptions to prove each of the four properties that define a group:

0. H **is closed under the operation** $*$: this is directly assumed by **Property 1**.
1. **The operation is associative:** This is inherited from the fact that associativity of the operation holds in the group G. Let a, b, and c be any elements of H. Since $H \subseteq G$, we know a, b, and c are also elements of G. Because G is a group, we know that $a * (b * c) = (a * b) * c$, so associativity holds true in $(H, *)$.
2. **Every element has an inverse:** This is true because of **Property 2**. Every element of H has an inverse in H.
3. **There is an identity element in** H**:** Pick any element h in H. **Property 2** tells us that h^{-1} is an element of H. **Property 1** then tells us that $h * h^{-1}$ is also an element of H. Since $h * h^{-1} = e_G$, we conclude that H contains the identity element.

We have shown that H is closed under the operation $*$, satisfies associativity, contains the inverse of each of its elements, and contains the identity element. Therefore we conclude that $(H, *)$ is a group. □

1. The center $Z(G)$ of a group G is defined by $Z(G) = \{z \in G \mid zx = xz \ \forall x \in G\}$. Prove that $Z(G)$ is a subgroup of G.

   Remark: The center of a group is the set of elements that commute with every other element of the group.

   Proof. Let G be a group. We will use our new Subgroup Test Theorem to show that the center is a subgroup of G. To apply the test, we need to check the following properties:

   (a) $Z(G)$ is closed under the operation of G.

   (b) $Z(G)$ contains the inverse of each of of its elements.

   To show that (a) is true, we must prove that the product of two elements of the center is again in the center. Let z and w be any two elements of the center. We must show that their product zw commutes with all other elements of G. To that end, let x be any element of G. Let's do some algebraic manipulation!

$$\begin{aligned}
(zw)x &= z(wx) && \text{(By associativity of } G\text{)} \\
&= z(xw) && \text{(Since } w \text{ is in the center, it commutes)} \\
&= (zx)w && \text{(By associativity of } G\text{)} \\
&= (xz)w && \text{(Since } z \text{ is in the center, it commutes)} \\
&= x(zw) && \text{(By associativity of } G\text{)}
\end{aligned}$$

   So $(zw)x = x(zw)$ for any element x in G. Thus the product is in the center $Z(G)$.

   Now we need to show that $Z(G)$ contains the inverse of each of of its elements. In other words, for any z in $Z(G)$, we must prove z^{-1} commutes with all elements of G:

   Let z be an element of $Z(G)$ and let x be any element of G. Time for some more algebraic manipulation!

$$
\begin{aligned}
z^{-1}x &= (z^{-1}x)e_G && \text{(Applying identity element does not change things)} \\
&= (z^{-1}x)(zz^{-1}) && (zz^{-1} = e_G) \\
&= (z^{-1})(xz)z^{-1} && \text{(Associativity)} \\
&= (z^{-1})(zx)z^{-1} && \text{(Since } z \text{ is in the center, it commutes)} \\
&= (z^{-1}z)(xz^{-1}) && \text{(Associativity)} \\
&= e_g(xz^{-1}) && (z^{-1}z = e_G) \\
&= xz^{-1} && \text{(Applying identity element does not change things)}
\end{aligned}
$$

So we have shown that $z^{-1}x = xz^{-1}$ for any x in G. Therefore we conclude that z^{-1} is in the center $Z(G)$.

We have shown that $Z(G)$ satisfies both (a) and (b), which means that we can conclude that $Z(G)$ is a subgroup of G.....Right?

...

...

...

Right?

...

...

...

...

...

...

...

...

...

...

. . .

. . .

Wrong!!!!

Did you spot it? We missed something very slight and very subtle. For a hint at what we missed, check the blue text in Theorem 4.3 above. Then come back here. It's OK. I'll wait for you to read it before I go on:

. . . . . .

. . . . . .

. . . . . .

. . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . .

..

.

Welcome back! As I was saying, we missed something! Our proof only works if $Z(G)$ is non-empty to begin with. What if there is a group that doesn't have any elements that commute with everything else? Then we can't do any of the things we just did that start with "Let z be an element of the center $Z(G)$," since there is no such z to pick. That would be rather unfortunate. . . . . .

Alas we have nothing to fear! The center $Z(G)$ can never be empty, as e_G is always an element of $Z(G)$. Now we are truly done with the proof. □

Footnotes for Handout 4:

[1] An abeleian grape.

5 There and Back Again: Functions From Group to Group

Definition 5.1.

- Let $(G, *)$ and $(H, \star)$ be groups, and let ϕ be a function from G to H. That is,

$$\phi : G \to H$$

  We say that ϕ is a group homomorphism if the following is always true: for any elements a and b in the group G,

$$\phi(a * b) = \phi(a) \star \phi(b) \qquad \text{(Homomorphism Property)}$$

- If ϕ is a group homomorphism and it is bijective, we say that ϕ is an isomorphism.

- The kernel of a group homomorphism is the set of all inputs whose output is the identity element (of the output group). We denote this set by $\ker(\phi)$.

Example: An example of homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Q}, +)$ is "take the reciprocal of the input." In other words, $\phi : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ where $\phi(n) = \frac{1}{n}$ is a homomorphism.

Claim: Isomorphisms preserve structures!

Example: Suppose we have an isomorphism $\phi : (G, *) \to (H, \star)$, and suppose we know that $(H, \star)$ is abelian. For any elements a and b of G, notice that

$$\begin{aligned} \phi(a * b) &= \phi(a) \star \phi(b) && \text{(homomorphism property)} \\ &= \phi(b) \star \phi(a) && (H \text{ is abelian}) \\ &= \phi(b * a) && \text{(homomorphism property)} \end{aligned}$$

So $\phi(a * b) = \phi(b * a)$. Since ϕ is an isomorphism, it is injective. Since we have two inputs with the same output it must be the case that the inputs are the same. Thus $a * b = b * a$, which means that $(G, *)$ is abeleian too!

Just about any property we have talked about so far is preserved by isomorphisms. Things like order (both of the group and of an element), being abelian, etc., along with the structures preserved by homorphisms in general (identity (see problem 2), inverses, operation).

Exercise 5.2.

1. For each of the following functions, determine if they are a group homomorphism. Are any of them isomorphisms?

   (a) $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $\phi(x) = 5x$

   Solution. ϕ is an injective group homomorphism that is not surjective:

   - ϕ is a group homomorphism: let a and b be any two integers. We need to check that $\phi(a + b) = \phi(a) + \phi(b)$. With that in mind, notice that

   $$\begin{aligned}\phi(a+b) &= 5(a+b)\\ &= 5a + 5b\\ &= \phi(a) + \phi(b).\end{aligned}$$

     Hey look at that! we just showed that ϕ is a homomorphism.
   - ϕ is also an injective! Suppose $a \neq b$. Then $5a \neq 5b$. In other words, if $a \neq b$, then $\phi(a) \neq \phi(b)$. That means ϕ is injective.
   - ϕ is not surjective. Every output is a multiple of 5, so (for example) there is no choice for a that yields $\phi(a) = 17$.

   □

   (b) $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $\phi(x) = x + 1$

   Not a homomorphism, because $\phi(0) \neq 1$.

   (c) $\phi : (\mathbb{Z}, +) \to (\mathbb{R}, +)$, $\phi(x) = e^x$

   Not a homomorphism, because $\phi(0) \neq 1$.

   (d) $\phi : (\mathbb{Z}_6, +) \to (\mathbb{Z}_2, +)$, $\phi(x) = x \mod 2$

   This is a surjective group homomorphism that is not injective.

   (e) $\phi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$, $\phi(x) = 10^x$

   Proof. This is an isomorphism!!!!!

   Let a and b be any two real numbers.

- ϕ is a homomorphism, since

$$\begin{aligned}\phi(a) \times \phi(b) &= 10^a \times 10^b \\ &= 10^{a+b} \\ &= \phi(a+b).\end{aligned}$$

- ϕ is surjective: let y be any positive real in the output group. Then you can choose $x = \log_{10}(y)$, and you will find that $\phi(x) = y$.
- ϕ is injective: if $a \neq b$ then $10^a \neq 10^b$.

□

2. Let $(G, *)$ and $(H, \star)$ be groups, where e_G and e_H are the identity elements of G and H respectively. Let $\phi : G \to H$ be a group homomorphism, and prove the following:

   (a) $\phi(e_G) = e_H$

   Proof. Using the homomorphism property, the identity elements e_G and e_H, and the three defining properties of groups, we can manipulate our way from $\phi(e_G)$ to e_H via a string of equalities:

$$\begin{aligned}
\phi(e_G) &= \phi(e_G) \star e_H && \text{(Apply identity element of } H\text{)} \\
&= \phi(e_G) \star \Big(\phi(e_G) \star [\phi(e_G)]^{-1}\Big) && (e_H = \phi(e_G) \star [\phi(e_G)]^{-1}) \\
&= \Big(\phi(e_G) \star \phi(e_G)\Big) \star [\phi(e_G)]^{-1} && \text{(Associativity)} \\
&= \big(\phi(e_G * e_G)\big) \star [\phi(e_G)]^{-1} && \text{(Homomorphism property)} \\
&= \big(\phi(e_G)\big) \star [\phi(e_G)]^{-1} && (e_G * e_G = e_G) \\
&= e_H && \text{(Property of Inverses in } H\text{)}
\end{aligned}$$

   Thus we conclude that $\phi(e_G) = e_H$. □

   (b) $\ker(\phi)$ is a subgroup of G. (Use the subgroup test!)

   Proof. We have a group G and a subset $ker(G) \subseteq G$. To show that $\ker(\phi)$ is a subgroup, we must verify the following:

- $\ker(\phi)$ is closed under the operation $*$: Let x and y be elements of the kernel. We must show that $x*y$ is also in the kernel. Because ϕ is a homomorphism, we know that $\phi(x*y) = \phi(x) \star \phi(y)$. Because x and y are in the kernel, we know that $\phi(x) = e_H$ and $\phi(y) = e_H$. So

$$\phi(x*y) = \phi(x) \star \phi(y) = e_h \star e_H = e_H$$

  So $x*y$ is in the kernel, and we conclude that the kernel is closed under $*$.

- Every element in $\ker(\phi)$ has an inverse that is also in $\ker(\phi)$: Let x be any element of $ker(G)$. We must show that x^{-1} is also in the kernel. As a result of part (a), we know that $\phi(e_G) = e_H$. Let's start there and do some algebraic manipulation:

$$\begin{aligned}
e_H &= \phi(e_G) \\
&= \phi(x * x^{-1}) && \text{(Inverses: } x * x^{-1} = e_G\text{)} \\
&= \phi(x) \star \phi(x^{-1}) && \text{(Homomorphism property)} \\
&= e_H \star \phi(x^{-1}) && (x \in \ker(\phi), \text{ so } \phi(x) = e_H) \\
&= \phi(x^{-1}) && \text{(Identity element property)}
\end{aligned}$$

  So $\phi(x^{-1}) = e_H$, and we conclude that x^{-1} is in the kernel of ϕ.

We proved that $\ker(\phi)$ is closed under $*$ and always contains its elements inverses. So by the Subgroup Theorem, we conclude that $\ker(\phi)$ is a subgroup of G. □

(c) ~~Show that ϕ is an injective homomorphism if and only if $\ker(\phi) = e_G$.~~
Show that a homomorphism $\phi : G \to H$ is injective if and only if $\ker(\phi) = \{e_H\}$. (Reworded for better clarity and fixed a clerical typo)

Proof. See remarks in Section 0 about proving "if and only if" statements.

For the forward direction, we must prove the following statement:

If a homomorphism $\phi : G \to H$ is injective, *then* $\ker(\phi) = \{e_H\}$.

Suppose we have an injective homomorphism $\phi : G \to H$. As we saw in part (a), since ϕ is a homomorphism we know that $\phi(e_G) = e_H$. So e_G is an element of $\ker(\phi)$. Because ϕ is injective, no other input can share the output e_H. Therefore e_H is the *only* element of $\ker(\phi)$. In other words, $\ker(\phi) = \{e_G\}$.

For the reverse direction, we must prove the following statement:

If $\ker(\phi) = \{e_H\}$, *then* a homomorphism $\phi : G \to H$ is injective.

Suppose we have a homomorphism $\phi : G \to H$ whose kernel is $\ker(\phi) = \{e_G\}$. We want to prove that ϕ is injective. To do that, we will show that $\phi(x) = \phi(y)$ implies $x = y$. So suppose we have two inputs x and y from G such that $\phi(x) = \phi(y)$. Let's get to algebraically manipulating things!

$$\begin{aligned}
\phi(x) &= \phi(y) && \\
\phi(x)\phi(y^{-1}) &= \phi(y)\phi(y^{-1}) && \\
\phi(xy^{-1}) &= \phi(yy^{-1}) && \text{(Homomorphism Property)} \\
\phi(xy^{-1}) &= \phi(e_G) && \\
\phi(xy^{-1}) &= e_H && \text{(Part (a): } \phi(e_H) = e_H\text{)}
\end{aligned}$$

Since $\phi(xy^{-1}) = e_H$, we know that xy^{-1} is in the kernel $\ker(\phi)$. Since the kernel contains only the identity element, that means that it must be true that $xy^{-1} = e_G$. Multiply by y on both sides to get $x = y$. Therefore we conclude that ϕ is injective.

Having proved the forward and reverse directions, we conclude that the original statement is true. □