Group Theory (2900)

Justin Stevens

Sunday
Sep 26, 2021 - Jan 23, 2022
7:30 - 9:30 PM ET (4:30 - 6:30 PM PT)

Homework

Week: 1 2 3 4 5 6 7 8 9 10 11 12 13 14

Homework: Week 1

You have completed **9** of **9** challenge problems.
Your writing problem response has been graded.
Past Due **Oct 10**.
Request Extension

Readings

Week 1: Chapter 1, Appendix A
Week 2: Sections 1.5-2.3
Week 1 Transcript: Sun, Sep 26

Challenge Problems

Announcement 1 (38886)

Don't forget about Office Hours: an AoPS staff member will be on the message board to answer your questions in real time every day from 4:00 - 5:30 PM ET (1:00 - 2:30 PM PT) and 7:30-8:30 PM ET (4:30-5:30 PM PT).

Announcement 2 (38887)

Here is a "Week 0" handout for you to optionally review some of the logic, set theory, and material on functions that we'll be relying on through the course. You should feel free to ask any questions about this material on the Message Board.

Problem 1 – Correct! – Score: 7 / 7 (38262)

Problem: Report Error
Select all the options which are true.

A. In a group, if $gh = gk$, then $h = k$.

B. In a group, if $hg = gk$, then $h = k$.

C. In a group, if $h = k$, then $hg = gk$.

Solution:

A. True. This is the cancellation law, which we proved in class.
B. False. For instance, let the group be the triangle group, $h = \ell$ a nontrivial counterclockwise rotation, $k = r$ a nontrivial clockwise rotation, and g any reflection. Then $h \neq k$ but $hg = gk$.

C. False. We can give essentially the same counterexample as above: Let $h = \ell$ and let g be any reflection.

Your Response(s):

A. In a group, if $gh = gk$, then $h = k$.

Problem 2 – Correct! – Score: 5 / 7 (38263)

Problem: Report Error

Select all of the following which form groups.

A. The set F_A of all functions $\mathbb{R} \to \mathbb{R}$, under "pointwise" addition $+ : F_A \times F_A \to F_A$. The definition is simply $(f+g)(x) = f(x) + g(x)$.

B. The set F_B of all functions $[0, \infty) \to [0, \infty)$, under pointwise addition.

C. The set F_C of all functions $\mathbb{R} \to \mathbb{R}$, under composition.

D. The set F_D of strictly increasing functions $\mathbb{R} \to \mathbb{R}$, under composition. (Recall that a function is strictly increasing if $y > x$ implies $f(y) > f(x)$.)

Solution:

A. This is a group. The identity is the constant zero function $e(x) = 0$. The inverse of f is $-f$. Associativity follows directly from associativity of addition in $\mathbb{R}$.

One can't help but notice that we didn't use anything specific about $\mathbb{R}$ in this example. Think about how to generalize this result as far as you can! (To be continued.)

B. This is not a group. The identity element is still $e(x) = 0$, but no nonzero function has an additive inverse; for instance the inverse of $f(x) = x$ would have to be $g(x) = -x$, which is not in F_B.

C. This is not a group, because many functions, such as $f(x) = x^2$, have no compositional inverses. As we saw in class, the set of all *bijections* $\mathbb{R} \longrightarrow \mathbb{R}$ would be a perfectly good group.

D. This is also not a group. The identity function $e(x) = x$ is strictly increasing and serves as an identity for composition. If $f \in F_D$, then f is one-to-one, that is, $f(a) = f(b)$ implies $a = b$. Thus f has an inverse function of a sort; the problem is that the domain of f^{-1} is the range of f, which may not be all of $\mathbb{R}$. For instance, $f(x) = e^x$ behaves this way. Its inverse $g(x) = \ln x$ has domain only $(0, \infty)$. So again, the issue is that not every strictly increasing function defined on $\mathbb{R}$ is a bijection.

Your Response(s):

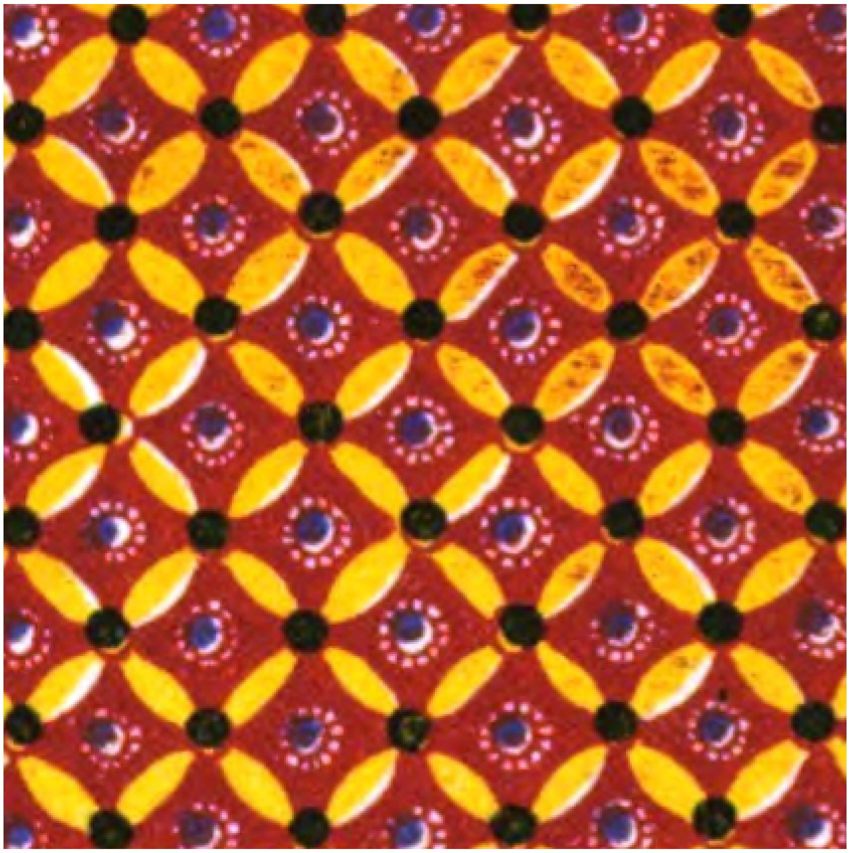
A. The set F_A of all functions $\mathbb{R} \to \mathbb{R}$, under "pointwise" addition $+ : F_A \times F_A \to F_A$. The definition is simply $(f+g)(x) = f(x) + g(x)$., D. The set F_D of strictly increasing functions $\mathbb{R} \to \mathbb{R}$, under composition. (Recall that a function is strictly increasing if $y > x$ implies $f(y) > f(x)$.)

A. The set F_A of all functions $\mathbb{R} \to \mathbb{R}$, under "pointwise" addition $+ : F_A \times F_A \to F_A$. The definition is simply $(f+g)(x) = f(x) + g(x)$.

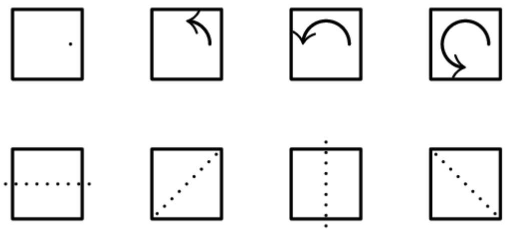
Problem 3, part (a) – Correct! – Score: 7 / 7 (38051)

Problem: Report Error

Here is a bit of a painting on the ceiling of an ancient Egyptian tomb. How many elements does its group of symmetries have? Assume that the picture is perfectly regular wherever it looks close to regular. In particular, ignore the little white crescents on the bottom-right of the purple dots in each square.



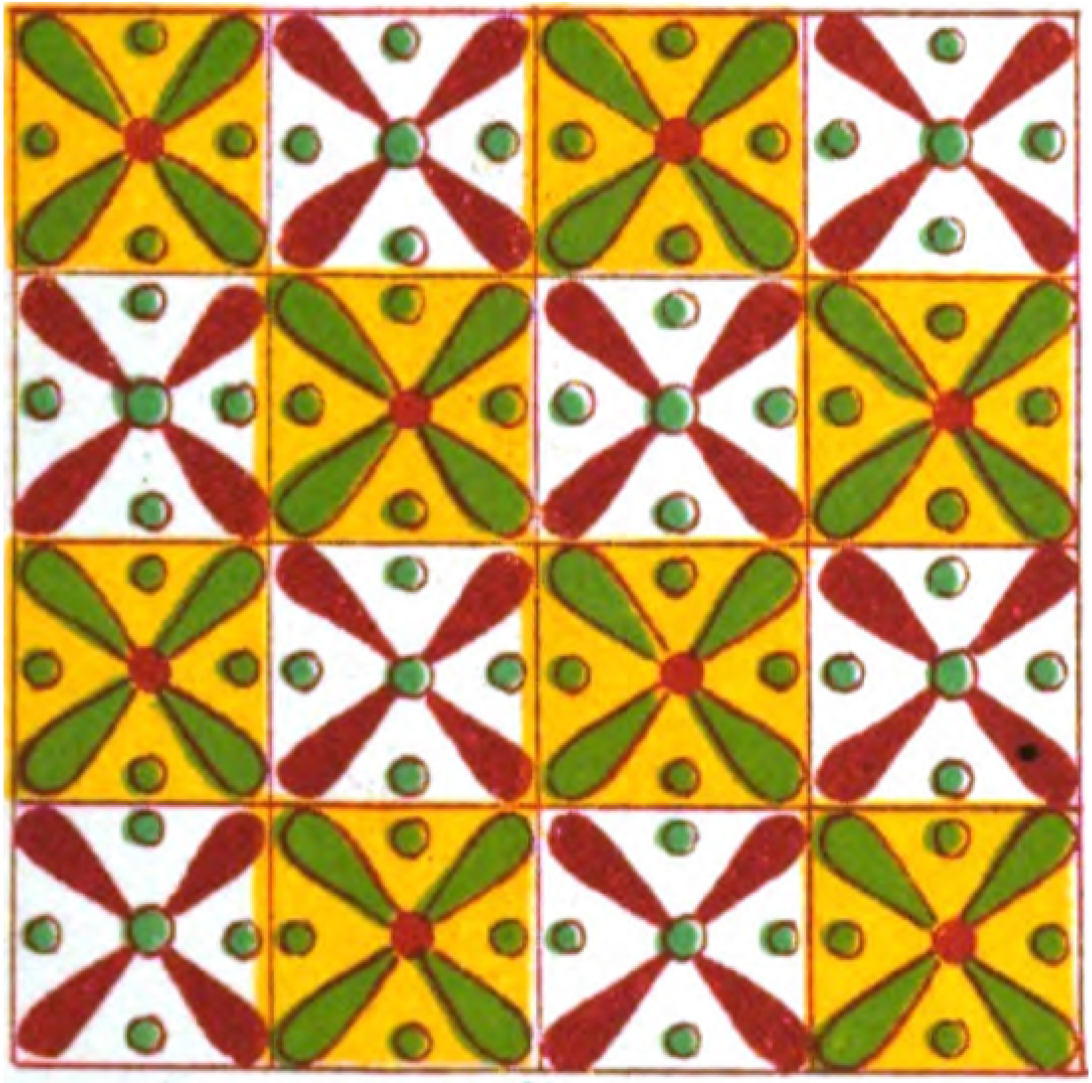
Solution:
There are the four rotations through multiples of $\pi/2$ (including the identity map), as well as reflections through lines through the midpoints of two opposite sides or through two opposite vertices. Thus there are eight total symmetries:



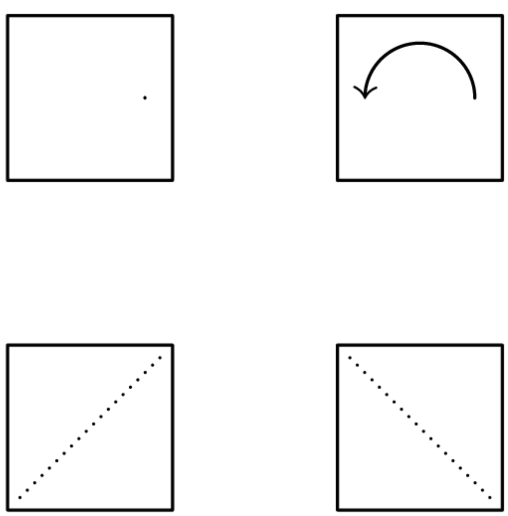
Your Response(s):
8

Problem 3, part (b) – Correct! – Score: 7 / 7 (38052)

Problem: Report Error
How many elements does this painting's group of symmetries have? Assume that the picture is perfectly regular wherever it looks close to regular, and consider the color of tiles to be part of the structure of the painting.



Solution:
In this case, besides the identity transformation, we have only the reflections through diagonal lines and the rotations through an angle π. The other rotations and reflections send tiles with yellow backgrounds to tiles with white backgrounds, so they aren't symmetries.



Your Response(s):

4

Problem 4 – Correct! – Score: 7 / 7 (38037)

Problem: Report Error

Suppose that $aba^{-1} = b^2$ in some group G. Compute a^nba^{-n} as a power of b.

Solution:

Notice first that

$$a^nba^{-n} = a^{n-1}(aba^{-1})a^{1-n} = a^{n-1}b^2a^{1-n} = (a^{n-1}ba^{1-n})^2,$$

which sets us up for a proof by induction. Incrementing n is squaring our answer, so we'll prove that $a^nba^{-n} = b^{2^n}$.

The base case, where $n = 1$, is given. For the inductive step, assuming $a^{n-1}ba^{1-n} = b^{2^{n-1}}$, the calculation above shows

$$a^nba^{-n} = (a^{n-1}ba^{1-n})^2 = \left(b^{2^{n-1}}\right)^2 = b^{2^n},$$

as desired.

Hint(s): Can you use induction here?

Your Response(s):

b^(2^n)

Problem 5, part (a) – Correct! – Score: 5 / 7 (38040)

Problem: Report Error

Consider the following partially-filled Cayley table:

	e	x	x^2	x^3	y	xy	x^2y	x^3y
e								
x				e				
x^2								
x^3								
y		x^3y			x^2			
xy						x^2		
x^2y								
x^3y								

Express x^2yx^2 in the form x^ay^b, using the smallest nonnegative exponents possible. You may simplify 0s and 1s away, so for instance you may write $x^1y^2 = xy^2$ and $x^1y^0 = x$.

Solution:

From the table we have $yx = x^3y$, so

$$yx^2 = (yx)x = (x^3y)x = x^3(yx) = x^3(x^3y) = x^6y,$$

where we've made three uses of associativity. Thus, $x^2yx^2 = x^2(x^6y) = x^8y$. We also have $x^4 = e$, so $x^8y = y$.

Your Response(s):

y^5

y

Problem 5, part (b) – Correct! – Score: 5 / 7 (38041)

Problem:

Report Error

Consider the following partially-filled Cayley table:

	e	x	x^2	x^3	y	xy	x^2y	x^3y
e								
x				e				
x^2								
x^3								
y		x^3y			x^2			
xy						x^2		
x^2y								
x^3y								

Fill in the seventh row of the table, writing every entry in the form x^ay^b for $a \in \{0,1,2,3\}$ and $b \in \{0,1\}$.

	e	x	x^2	x^3	y	xy	x^2y	x^3y
e								
x				e				
x^2								
x^3								
y		x^3y			x^2			
xy						x^2		
x^2y	$x^{2}y^{1}$	$x^{1}y^{1}$	$x^{0}y^{1}$	$x^{3}y^{1}$	$x^{0}y^{0}$	$x^{3}y^{0}$	$x^{2}y^{0}$	$x^{1}y^{0}$
x^3y								

Solution:

We notice that x has order 4, and $yx = x^3y = x^{-1}y$. This lets us move y "through" powers of x. So we can always push y to the end of the word. Furthermore $y^2 = x^2$, so we never need more than one copy of y. Therefore we have the ability to write any element in the form x^ay or x^a.

	e	x	x^2	x^3	y	xy	x^2y	x^3y
e	e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	x^3	e	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	x^2	x	e	x^3
xy	xy	y	x^3y	x^2y	x^3	x^2	x	e
x^2y	x^2y	xy	y	x^3y	e	x^3	x^2	x
x^3y	x^3y	x^2y	xy	y	x	e	x^3	x^2

Your Response(s):

	e	x	x^2	x^3	y	xy	x^2y	x^3y
e								
x				e				
x^2								
x^3								
y		x^3y			x^2			
xy						x^2		
x^2y	x^2y^1	x^3y^1	x^0y^1	x^1y^1	x^0y^0	x^3y^0	x^2y^0	x^1y^0
x^3y								

	e	x	x^2	x^3	y	xy	x^2y	x^3y
e								
x				e				
x^2								
x^3								
y		x^3y			x^2			
xy						x^2		
x^2y	x^2y^1	x^1y^1	x^0y^1	x^3y^1	x^0y^0	x^3y^0	x^2y^0	x^1y^0
x^3y								

Problem 6 – Completed – Score: 3 / 3 (38048)

Problem: Report Error

Let X be a set equipped with some binary operation $\star : X \times X \to X$ and assume that $e \in X$ is an identity element for this product. Assume that $\star$ is associative, but don't assume that every element has an inverse, so X may not be a group. If $a, b \in X$ are a pair such that

$$aba = a$$
$$ab^2a = e$$

Prove that $ab = ba = e$.

Solution:

One product is given by

$$ab = (ab)e = (ab)(ab^2a) = (aba)(b^2a) = (a)(b^2a) = ab^2a = e.$$

The other comes by reversing the order,

$$ba = e(ba) = (ab^2a)ba = (ab^2)(aba) = (ab^2)(a) = ab^2a = e.$$

As a side remark, a set X with an associative binary operation admitting an identity element is called a *monoid*. All groups are monoids, but not all monoids are groups.

Your Response:

You know that $ae = ea = a$ from the definition of an identity element. Using $ae = a$ and comparing that to $aba = a$, you can see that $ba = e$. Similarly, using $ea = a$ and comparing that to $aba = a$, you can see that $ab = e$. By the transitive property, $ab = ba = e$.

Problem 7 – Completed – Score: 3 / 3 (38050)

Problem: Report Error

The Heisenberg group $H = (\mathbb{R}^3, \cdot)$ is the set $\mathbb{R}^3$ with the binary operation $\cdot : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ given by

$$(a, b, c) \cdot (x, y, z) = (a + x, b + y + az, c + z).$$

Show that H is a group.

Solution:
The origin $(0, 0, 0)$ is the identity element, since

$$(a, b, c) \cdot (0, 0, 0) = (a + 0, b + 0 + a0, c + 0)$$

and

$$(0, 0, 0) \cdot (x, y, z) = (0 + x, 0 + y + 0z, 0 + z).$$

For inverses, we must thus solve $(a + x, b + y + az, c + z) = (0, 0, 0)$ for x, y, z and for a, b, c. We easily find $x = -a, z = -c$ or $a = -x, c = -z$, which leads respectively to $y = -b - az = b + ac$ and $b = -y - az = -y + xz$. Thus every element has a right inverse and a left inverse, which implies the two one-sided inverses coincide, so H has inverses.

Finally, for associativity we calculate

$$[(a, b, c) \cdot (x, y, z)] \cdot (\alpha, \beta, \gamma) = (a+x, b+y+az, c+z) \cdot (\alpha, \beta, \gamma) = (a+x+\alpha, b+y+az+\beta+(a+x)\gamma, c+z+\gamma)$$

and

$$(a, b, c) \cdot [(x, y, z) \cdot (\alpha, \beta, \gamma)] = (a, b, c) \cdot (x+\alpha, y+\beta+x\gamma, z+\gamma) = (a+x+\alpha, b+y+\beta+x\gamma+a(z+\gamma), c+z+\gamma).$$

The two three-fold products are equal.

A less technical way of proving associativity, if you're familiar with multiplying matrices, is to notice that this is merely the matrix product where (a, b, c) corresponds to the matrix

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

There are many interesting groups of matrices, but we won't focus on them in this course.

Your Response:
Since we are given that H is a magma, we just need to hunt for an identity, show there exists inverses for every element of H, and prove that the binary operation is associative. It is easily seen that $(0, 0, 0)$ serves as the identity. Also, the unique inverse for any arbitrary ordered triplet (x, y, z) is just $(-x, xz - y, -z)$. After showing that $[(a, b, c) \cdot (x, y, z)] \cdot (d, e, f) = (a + d + x, b + y + az + e + af + fx, c + f + z) = (a, b, c)[\cdot(x, y, z) \cdot (d, e, f)]$, we can conclude that the binary operation is associative. Thus, H is a group.

Problem 8 – Graded – Technical: 6 / 7 – Style: 0.9 / 1 (38049)

Problem: Report Error

We saw in class that the symmetry group of the triangle is non-Abelian. Prove that there exists no non-Abelian group of smaller order.

Note: you may use any result proved in class without re-proving it, but you must clearly state what result you're using.

Explain, in words, how you solved this problem. Use complete sentences. Write as though the person reading is one of your *classmates who has not seen the problem before. Include any important observations you made and explain why you are doing anything that isn't totally obvious. To learn more about how writing problems work, you can go here.*

Solution:
The symmetry group of the triangle has order 6. We will show that any group of order less than 6 is Abelian.

The only group $\{e\}$ of order 1 has the trivial binary operation $e \cdot e = e$, and it's Abelian. The only group $\{e, x\}$ of order 2 has the binary operation $x \cdot x = e$, since by cancellation we can't have $x^2 = x$. A group of order 3 has elements $\{e, x, y\}$. By cancellation we can't have $xy = x$ or $xy = y$ so $xy = e$, or in other words, $y = x^{-1}$. Then the group must be $\{e, x, x^{-1}\}$. Since x and x^{-1} commute, this group is also Abelian.

In class we found both groups of order 4 and observed these are both Abelian.

Now assume we have a group of order 5 that is non-Abelian. Such a group has two non-commuting elements, x and y. That means that the set $\{e, x, y, xy, yx\}$ contains 5 distinct elements. We can begin to write the Cayley table for this supposed group as

	e	x	y	xy	yx
e	e	x	y	xy	yx
x	x		xy		
y	y	yx			
xy	xy				
yx	yx				

Consider x^2. Since this shares a row with x and xy and a column with x and yx, we know x^2 must either be e or y. If $x^2 = y$, then

$$xy = xx^2 = x^2x = yx,$$

which contradicts that x and y don't commute. Thus x^2 must be e:

	e	x	y	xy	yx
e	e	x	y	xy	yx
x	x	e	xy		
y	y	yx			
xy	xy				
yx	yx				

Focusing on the second column: we know that $(yx)x = y(xx) = y$, so we fill this in.

	e	x	y	xy	yx
e	e	x	y	xy	yx
x	x	e	xy		
y	y	yx			
xy	xy				
yx	yx	y			

However, this leaves no value available for $(xy)x$, since $x, e, yx,$ and y appear in its row and xy appears in its column. This contradicts that x and y do not commute. Therefore there is no non-Abelian group of order 5.

Since no group of order less than 6 is Abelian, and rotations and reflections do not commute in the triangle group as shown by our Cayley table in class, the symmetry group of the triangle must be the smallest non-Abelian group.

SIDENOTE

Incidentally we can show that the triangle group is the unique non-Abelian group of order 6 by using our argument from above. Assume that we are given a non-Abelian group of order $6.$ Then there are elements x and y that do not commute and we can reproduce the partial Cayley table from above with an extra column and row. The elements x and y are interchangeable at this point. Either $x^2 = y^2 = e$ or one of these elements, say x has order greater than $2.$

If $x^2 = y^2 = e$ we get

	e	x	y	xy	yx	$\bullet$
e	e	x	y	xy	yx	
x	x	e	xy	y		
y	y	yx	e		x	
xy	xy		x		e	
yx	yx	y		e		
$\bullet$						

This sixth element is some new $z = xyx = yxy$ and the Cayley table is

	e	x	y	xy	yx	z
e	e	x	y	xy	yx	z
x	x	e	xy	y	z	yx
y	y	yx	e	z	x	xy
xy	xy	z	x	yx	e	y
yx	yx	y	z	e	xy	x
z	z	xy	yx	x	y	e

This is the symmetry group of the triangle with reflections x, y, and z and nontrivial rotations xy and yx.

Alternatively $x^2 \neq e$ so the sixth element is x^2.

	e	x	y	xy	yx	x^2
e	e	x	y	xy	yx	x^2
x	x	x^2	xy			
y	y	yx				
xy	xy					
yx	yx					
x^2	x^2					

If $(xy)x = e$ then

$$y = (x^{-1}x)y(xx^{-1}) = x^{-1}((xy)x)x^{-1} = x^{-2},$$

but this would make x and y commute, since $xx^{-2} = x^{-1} = x^{-2}x$. Likewise if $(yx)x = e$ then x and y commute. Therefore $(x^2)x = e$ and x has order $3.$

	e	x	y	xy	yx	x^2
e	e	x	y	xy	yx	x^2
x	x	x^2	yx			e
y	y	xy				
xy	xy					
yx	yx					
x^2	x^2	e		y		x

Now looking at products in the x-row we see $x(yx) = y$ and $x(xy) = yx$.

	e	x	y	xy	yx	x^2
e	e	x	y	xy	yx	x^2
x	x	x^2	xy	yx	y	e
y	y	yx				yx
xy	xy					y
yx	yx					xy
x^2	x^2	e	yx	y	xy	x

At this point we note that y^2 must be a power of x, but if $y^2 = x$ or $y^2 = x^2$ then y commutes with x. Therefore $y^2 = e$ and we get

	e	x	y	xy	yx	x^2
e	e	x	y	xy	yx	x^2
x	x	x^2	xy	yx	y	e
y	y	yx	e	x^2	x	xy
xy	xy	y	x	e	x^2	yx
yx	yx	xy	x^2	x	e	y
x^2	x^2	e	yx	y	xy	x

This is also the Cayley table for the symmetry group of the triangle where x is a rotation and y is a reflection.

Hint(s): How did we find the order 4 groups? Can we do something similar for groups of other orders?

Your Response:
The order of the symmetry group of the triangle, which I will refer to as the "triangle group" for consolidation purposes, is 6. So I need to show that groups of order $1, 3, 4, 5$ are Abelian. Groups with order 1 are Abelian because they have one element, e, and commutativity holds with $e * e = e = e * e$. In Week 2's class, we proved that every group of prime order is Abelian, so groups of order 2,3, and 5 are Abelian. In Week 1, we found Cayley tables for a group with order 4. These tables showed that groups with order 4 are Abelian.

Technical Score: 6 / 7
Style Score: 0.9 / 1
Comments:
Good job! First of all, you noticed that the trivial group (this is what we call the group of order 1) is obviously Abelian, since it contains only the identity element.

Then, you considered the groups of prime order and cleverly used Lagrange's theorem to show that they're Abelian as well. Moreover, you have proved a more general result - all groups of order p where p is prime are Abelian.

That said, as of the end of Week 1, you had not yet proved Lagrange's theorem, which makes this problem a bit too easy. In general, one good reason to not use results from further in the course is to get more familiar with all sorts of techniques. In this problem, you are given the opportunity to practice thinking about groups in terms of Cayley tables. This can sometimes be a good point of view. While it is a more "brute force"-y type of method, it can help you gain intuition in problems where you are not sure how to begin, so it's a powerful thing to have in your arsenal.

So keep this in mind for future writing problems: try to solve it just with what you learned up to that class. Give this problem another go, by using the hint given in the problem statements and see if you can set up Cayley tables for groups of orders 3 and 5.

Note that you had a type in your second sentence as you wrote "$1, 3, 4, 5$" instead of "$1, 2, 3, 4, 5$". Also, if you are using $\LaTeX$, try to use it for all mathematical expressions. For example, "order 4" should be "order 4".

Keep working hard!

You have thanked the grader!

Problem 9 (38053)

Problem: Report Error

Here are some relatively simple results to try proving, to get practice writing group theory proofs and examples. Make sure to hide your answers so as not to steal all the fun; on the other hand, you should feel free to discuss others' solutions once you've tried these out!

1. Prove that $(g^{-1})^n = (g^n)^{-1}$ for any element g in any group, and any natural number n. You should focus particularly on what exactly is obvious or not obvious here. What concept from basic algebra does this show will work in any group?
2. Can a group have two different identity elements? Can an element of a group G have two different inverses? Two different *right* inverses? A right inverse that's distinct from the left inverse? What if $(G, \cdot)$ is not necessarily a group, but just a set with an associative binary operation and an identity element? (Pick your preferred questions out of here!) A left inverse of g is h such that $hg = e$, and a right inverse is h such that $gh = e$.
3. Give a careful proof by induction of the (admittedly silly) result that x commutes with x^n for every x in a group G and every $n \in \mathbb{Z}$. To make this precise, first give a precise inductive definition of x^n, which is strictly speaking necessary since the binary operation doesn't give us a way to directly multiply n things together.
4. On a similar note, prove that associativity implies 4-associativity, that is, prove that any way of multiplying together four elements of a group in a given order gives the same answer. (It is possible, but very technical, to extend this to n-associativity!)

Discussion Problem:

This is a **Discussion** problem. Use the discuss button to visit the discussion thread for this problem and work with your classmates. You can post full or partial solutions, but please surround them in `[hide][/hide]` tags as a courtesy to students who do not want the problem to be spoiled.

Problem 10 (38054)

Problem: Report Error

Salt crystals typically array themselves in a cubic lattice. Find a way to describe the symmetry group of the infinite cubic lattice.

Discussion Problem:

This is a **Discussion** problem. Use the discuss button to visit the discussion thread for this problem and work with your classmates. You can post full or partial solutions, but please surround them in `[hide][/hide]` tags as a courtesy to students who do not want the problem to be spoiled.

Problem 11 (38241)

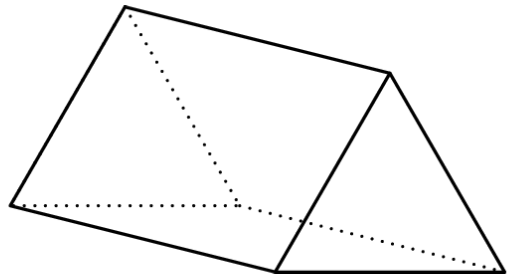
Problem: Report Error

Let's have a symmetry group party! Describe the symmetry group of the object posted above you, and then post an object of your own for the next poster to describe the symmetry group of. Try to provide an object that's different from anything we've seen before.

What does "describe" mean? Well, a perfect description is a Cayley table, but you don't need to go that far. Try to count the number of elements if the group is finite, and give a geometric description of what kind of elements the group has, as we've seen examples with rotations, reflections, translations, and so on as symmetries earlier.

Note that it's not always obvious from a picture what the symmetries of an object should be. Part of your answer should be explaining what you've decided symmetries should preserve!

I'll start. Here's one of my favorite objects, a triangular prism:



Discussion Problem:
This is a **Discussion** problem. Use the discuss button to visit the discussion thread for this problem and work with your classmates.