Abstract Algebra 3/1/2019

Goal idea: Theorem 6 works and makes sense for the dihedral group D_{360} of symmetry transformations of a regular 360-gon.

Discussion: $r^{-82}r^{40}$ means rotate clockwise 40 degrees (or rotate 1 degree clockwise 40 times) and then rotate 82 degrees counterclockwise. After you do that, you end up having rotated 42 degrees counterclockwise.

This matches what you do with theorem 6: $r^{-82}r^{40} = r^{-82+40} = r^{-42}$

***

The larger group D_{360} is not abelian (commutative). You can prove this by drawing out what happens if you do $r^{90}v$ and vr^{90} (where v is a reflection in a vertical line). The two outcomes are different (rotating first then reflecting or reflecting first and then rotating). By showing these two elements $r^{90}v$ and vr^{90} of D_{360}, we have proved that D_{360} is not abelian (commutative)

The subgroup of rotations $R_{360} = \{r^n \mid n \in \mathbb{Z}\}$ is abelian. Showing an example isn't enough to prove that something is always commutative, so we need to use theorem 6:

Proof: Let $a, b \in R_{360}$. Then $a = r^i$ and $b = r^j$ for some numbers $i.j \in \mathbb{Z}$

So $ab = r^i r^j = r^{i+j}$ by theorem 6

And $ba = r^j r^i = r^{j+i}$ by theorem 6, and

$ba = r^j r^i = r^{j+i} = r^{i+j}$ because addition of integers is commutative

Therefore $ab = ba$, and hence R_{360} is abelian.

***

Next we looked at Lemma 9:

Lemma 9: In a group *G* (with the default multiplicative notation for the binary operation), and $a \in G$ then $\{a^n \mid n \in \mathbb{Z}\} \subseteq < a >$

We discussed that $\{a^n \mid n \in \mathbb{Z}\}$ is a subset of *G* and we're going to prove that it's a subset of $< a >$, but it's not until Lemma 9 that we know it's a group. Right now $\{a^n \mid n \in \mathbb{Z}\}$ is just a set.

We do know, by definition, that $< a >$ is a group, because the definition is that $< a > \subseteq G$ is the smallest subgroup of *G* that contains *a*.

Let $a^m \in \{a^n \mid n \in \mathbb{Z}\}$ be a random/arbitrary element of the set.

We're going to prove this is a subset of $< a >$ by doing it in three cases: $m < 0$, $m = 0$ and $m > 0$

Case 1: $m > 0$

Then $a^m = \underbrace{aa...a}_{m}$. We know $a \in < a >$ and $< a >$ is a group, so it is closed, thus

$a^m = \underbrace{aa...a}_{m} \in < a >$

Case 2: $m = 0$. By definition $a^0 = e$, which is the identity of *G*. We know $< a >$ is a subgroup of *G*, so $a^0 = e \in < a >$

Case 3: $m < 0$. By definition $a^m = \underbrace{a^{-1}a^{-1}...a^{-1}}_{|m|}$. Since $a \in < a >$ and $< a >$ is a group so it contains inverses, so $a^{-1} \in < a >$. Because $< a >$ is a group, it is closed, so $a^m = \underbrace{a^{-1}a^{-1}...a^{-1}}_{|m|} \in < a >$

Thus every element of $\{a^n \mid n \in \mathbb{Z}\}$ is an element of $< a >$, so $\{a^n \mid n \in \mathbb{Z}\}$ is a subset of $< a >$.

***

Lemma 10: In a group *G* (with the default multiplicative notation for the binary operation), and $a \in G$ then $\{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

So right now we know that $\{a^n \mid n \in \mathbb{Z}\}$ is a subset of *G*, but we need to prove it is a subgroup. By theorem 1, what we need to check is that the set, which we will call S: $S = \{a^n \mid n \in \mathbb{Z}\}$ is

- Closed
- Contains inverses

Let $b, c \in S$ then $b = a^i$ and $c = a^j$ for some $i, j \in \mathbb{Z}$

Then $bc = a^i a^j = a^{i+j}$ and $i + j \in \mathbb{Z}$ so $bc = a^i a^j = a^{i+j} \in \mathbb{Z}$

Thus *S* is closed.

Let $b = a^i \in S$ and $i \in \mathbb{Z}$ so $-i \in \mathbb{Z}$ and hence $a^{-i} \in S$

Further $a^i a^{-i} = a^{i-i} = a^0 = e$ and $a^{-i}a^i = a^{-i+i} = a^0 = e$, so a^{-i} is the inverse of a^i

Thus, for any element of *S*, its inverse is also in *S*.

By theorem 1, *S* is a subgroup of *G*.

***

A lemma is a helper-theorem: it is part of a theorem that helps you prove something bigger. We will use lemmas 9 and 10 to prove theorem 11:

Theorem 11: In a group G (with the default multiplicative notation for the binary operation), and $a \in G$ then $\{a^n \mid n \in \mathbb{Z}\} =< a >$

By lemma 9, $\{a^n \mid n \in \mathbb{Z}\} \subseteq < a >$ (S is a subset of $< a >$)

By lemma 10, $S = \{a^n \mid n \in \mathbb{Z}\}$ is a group (that is a subgroup of G).

By definition, $a = a^1 \in S$

By definition, $< a >$ is the smallest subgroup of G that contains a. Because it is the smallest, S can't be smaller than it (it can't be a proper subset), so the two sets (groups) have to be equal.

$\{a^n \mid n \in \mathbb{Z}\} =< a >$

***

This means that subsets generated by a single element have this very clear, well organized structure.

One example is the one we started with today: $R_{360} = \{r^n \mid n \in \mathbb{Z}\} =< r >$

All subgroups that are generated by a single element are abelian:

***

Finally, we looked at another subgroup that is generated by a single element.

Remember that we proved the following is a group:

$GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a,b,c,d \in \mathbb{R}, ad - bc \neq 0 \right\}$ (The group of invertible 2x2 matrices, with multiplication as the group operation)

The determinant of $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is 1, so $A \in GL(2,\mathbb{R})$

If you do a few calculations, you'll find:

$A^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $A^3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$ and $A^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, and you can correctly infer (we didn't prove it, but we could) that $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

So, using our previous theorems from today, we can say:

$$< A >= \{A^n \mid n \in \mathbb{Z}\} = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$$

Now, an interesting question is whether $< A >$ is commutative. $GL(2, \mathbb{R})$ is not abelian (commutative), and most matrices don't commute, but for these matrices, we can use theorem 6:

$A^i A^j = A^{i+j} = A^{j+i} = A^j A^i$, so these particular matrices are commutative with each other, and $< A >$ is abelian

***

Two questions to think about for Monday:

1. If you have a subgroup generated by a single element, will it always be abelian? Why or why not?
2. Some of the groups we have looked at in class are essentially the same as each other—they have the same number of objects, and you can match them up in a way that makes sense. Can you think of a group we have looked at so far that is essentially the same as: $< A >= \{A^n \mid n \in \mathbb{Z}\} = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$? Try to come up with an example of a group that is really similar to this one, and try to explain how the two groups are essentially the same. This is a great problem to think about, because either you will rediscover an important idea in Abstract Algebra, or you will be on your way to creating some new mathematics!