Proof Collection 500 Goal

Mentee: Ryan Baldwin, rbaldwi2@swarthmore.edu

Mentor: Dr. Devlin

This is a collection of proofs I have done over the summer of 2025 as a student researcher.

Defn: Let G be a group. A set $S \subseteq G$ is "awesome" iff $\forall a, b \in S$, $aba \in S$.

0. If G is a group, a set S is "awesome" iff for all a and b in S, we have that aba is in S as well.

Note: For proofs 1-3, the group operation is written multiplicatively for simplicity.

---

1. If H is a subgroup of G, then H is awesome.

Proof. Since H is a subgroup of G, H is closed under the group operation, a priori. Let a and b be any element in H. Then the element aba is an element of H for any $a, b \in H$. $\square$

2. If G is abelian and if every element of G has order 2, then *every* subset of G is awesome.

Proof. Let S be a finite set. Then let the following map define the awesome property:

$$\begin{aligned} S \times S &\to S \\ (a, b) &\mapsto aba, \quad \forall a, b \in S \end{aligned}$$

We prove this statement by induction and construct a base case. First, we consider a subset of G with one element denoted $S_1 := \{a_1\}$. Since every element of G has order 2, every element of G is its own inverse. Hence, $(a_1, a_1) = a_1 \in S_1$.

Let us append another distinct element of $a_2 \in G$, and define $S_2 := S_1 \cup \{a_2\} = \{a_1\} \cup \{a_2\}$. Because every element of G has order 2 and the group operation is abelian, we prove this subset is awesome. We see that $(a_1, a_2) = a_1 a_2 a_1 = a_1 a_1 a_2 = (a_1)^2 a_2 = 1a_2 = a_2 \in S_2$. Furthermore, we notice that $(a_2, a_1) = a_2 a_1 a_2 = (a_2)^2 a_1 = a_1 \in S_2$.

Finally, to conclude our base case we consider the case where we append another unique element, we denote $a_3 \in G$ to the subset S_2 and define $S_3 := S_2 \cup \{a_3\}$. Similar to the subsets S_1 and S_2, the subset S_3 must also be awesome. This is because the awesome set's law of composition is abelian and every element will always have an order of 2, these two facts will have the awesome property equaling $aba = (aa)b = 1b = b$ for all a, b in S.

We induct on the number of elements in the subset, and we assume that this claim holds true for n number of unique elements in G. We will show that this claim holds true for $n + 1$ elements of G, thus proving the claim.

Let S_n be a subset of G such that it is awesome, and let a_{n+1} be an element of G that is not in S_n. We define $S_{n+1} := S_n \cup \{a_{n+1}\}$, and we aim to show that this is remains an awesome subset of G. We let a_i be any element of S_n for $1 \leq i \leq n$ and utilize the fact that any such element in the set has an order of 2. Furthermore, we recall that given a_{n+1} is an element of G, it must also have an order of 2. Now we show that the

set S_{n+1} is awesome directly. We first notice that for any $a_i \in S_n$ the awesome property $(a_i, a_{n+1}) = (a_i)a_{n+1}(a_i) = (a_i)^2 a_{n+1} = a_{n+1}$ S_{n+1} will always be true. Furthermore, we see that for any $a_i \in S_n$, the property $(a_{n+1}, a_i) = (a_{n+1})^2 a_i = a_i \in S_{n+1}$ will also always be true. Thus, it is true then that the subset S_{n+1} is an awesome set. Therefore, any subset of G with the aforementioned properties will always be an awesome set.

□

Proof 2:

Proof. Let S be an arbitrary subset of G. (Goal to prove for all $a, b \in S$ we have $(a, b) \in S$)

[Finish writing this direct proof]

□

3. Suppose G is the dihedral group with 10 elements. Suppose S contains the flip and the rotate elements. If S is awesome, show that S must contain all the elements of the group.

S must contain $\{1 = \sigma^2 = \zeta^5, \sigma, \zeta, \zeta^2, \zeta^3, \zeta^4\}$. [You proved that already]

Also! The set $\{1 = \sigma^2 = \zeta^5, \sigma, \zeta, \zeta^2, \zeta^3, \zeta^4\}$ happens to be awesome already (without needing to add anything else).

Proof. The dihedral group with 10 elements is $D_5 := \langle \sigma, \zeta | \sigma^2 = \zeta^5 = 1, \zeta\sigma = \sigma\zeta^4 \rangle$. Assuming that the set $S \supseteq \{\sigma, \zeta\}$ is awesome, we will show that the set must contain all powers of the generators of D_5, which will consequently prove that $S = D_5$.

Since S is an awesome set, $\sigma\zeta\sigma = \sigma(\zeta\sigma) = \sigma^2\zeta^4 = \zeta^4$ is in S. Consequently, what must follow is that $\zeta^4\zeta^4\zeta^4 = \zeta^2$ must also be an element of S. We also note that ζ^3 must also be in the set as $\sigma\zeta^2\sigma = \sigma\zeta(\zeta\sigma) = \sigma\zeta\sigma\zeta^4 = \zeta^4\zeta^4 = \zeta^3$. And because ζ^2 and ζ must be elements of S, it follows that S must contain the identity element 1 as follows: $\zeta^2\zeta\zeta^2 = 1$. Thus, $S = \{1 = \sigma^2 = \zeta^5, \sigma, \zeta, \zeta^2, \zeta^3, \zeta^4\}$.

Given that the generators of D_5 and the identity must be in S, what follows is that the remaining group elements can be generated through recursive composition. This is because if a, b, and 1 are all elements of an awesome set S, then $(1a1)(1b1) = (1)ab1$ is an element of S. Indeed, what then follows is that $\sigma\zeta, \sigma\zeta^2, \sigma\zeta^3, \sigma\zeta^4$ must be elements of S. Thus, $S = \{1, \sigma, \zeta, \zeta^2, \zeta^3, \zeta^4, \sigma\zeta, \sigma\zeta^2, \sigma\zeta^3, \sigma\zeta^4\}$ and is therefore the whole group

□

4. Suppose A_n is a sequence such that $A_0 = 1$ and that for all $n > 0$, we have $A_n = 2A_{n-1}$. Use induction to prove that for all $n \geq 0$ we have $A_n = 2^n$.

Proof. To begin the base case, we note that for the initial sequence $A_0 = 1 = 2^0$. And since the sequence follows the recurssion $A_n = 2A_{n-1}$ for all $n > 0$, for $n = 1$ we have $A_1 = 2A_0 = 2^1$. Furthermore, for $n = 2$ we see that $A_2 = 2A_1 = 2^2A_0 = 2^2$. And in a similar fashion to the previous cases, for $n = 3$ what follows is that $A_3 = 2A_2 = 2(2^2A_0) = 2^3A_0 = 2^3$.

We induct on the sequence and assume that this relation is true for the $n-1$ sequence. That is, we assume $A_{n-1} = 2^{n-1}$. Because of this assumption, we see that $A_n = 2A_{n-1} = 22^{n-1} = 2^n$. Thus, we have shown that for all $n \geq 0$, $A_n = 2^n$. Therefore, the claim is true.

□

Tasks from June 6

Redo: Finish writing the proofs of 2 and 3 (restated version of 3). ****

5. Prove that if $G = D_n$ (dihedral group with $2n$ elements) and if $S = \{\sigma, 1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}\}$, then S is awesome (????) *****

5.a Is this true: $\zeta\sigma = \sigma\zeta^{n-1} = \sigma\zeta^{-1}$

Proof. We shall prove this relation to be true by showing that their resulting clockwise-order sets are equal. Suppose we have an n-gon in a two-dimensional plane. We define σ to represent flips based off of a vertix with a position we label v_1. Furthermore, let v_1 be a vertix that is part of an ordered set of unique clockwise-oriented vertices denoted by $\{v_1, v_2, v_3, v_4, \ldots, v_n\}$. Since the n-gon is spaced on a two-dimensional plane, there can only be two flips centered on an such vertix v_i. Hence, $\sigma^2 = 1$, the identity state. Furthermore, we define ζ to represent a clockwise rotation where all vertices replace the next proceeding vertix in clockwise recession. That is, $v_1 \mapsto v_2, v_2 \mapsto v_3, v_3 \mapsto v_4, \ldots, v_{n-1} \mapsto v_n$, and $v_n \mapsto v_1$. Because the vertices of the n-sided polygon are unique, there are only n unique clockwise rotations. This then implies that $\zeta^n = 1$.

If it can be shown that $v_2 \mapsto v_1$ in a clockwise-orientation for each relation, then the resulting clockwise-order sets are equal and thus the relations are equivalent. Let us start with a flip σ centered on v_1 (that is, v_1 is fixed). After doing this, we rotate the n-gon clockwise by one vertix (i.e. performing ζ) and have v_2 take the original position of v_1. In a clockwise rotation, $v_2 \mapsto v_1$ with v_2 in the original position of v_1 . We recall that because all vertices are ordered uniquely, the n-gon must have a clockwise rotation on the given set $\{v_2, v_1, v_n, v_{n-1}, \ldots, v_3\}$.

Now let us start with an inverse rotation by one vertix (denoted by ζ^{-1}) centered on v_1. It follows that v_2 must then take the original position of v_1, and we have $v_1 \mapsto v_2$ clockwise-facing, where v_2 is in the position of what used to be v_1. We then compose a flip centered on the *position* of what used to be v_1. We see that $v_2 \mapsto v_1$ must then be true, and given v_2 remains in the original position of v_1, we obtain the following set that defines where every vertix will map to when composed with a clockwise rotation: $\{v_2, v_1, v_n, v_{n-1}, \ldots, v_3\}$. Given that these two sets are equivalent, it follows that $\zeta\sigma = \sigma\zeta^{-1}$. And since one couter-clockwise rotation is the same as $n-1$ clockwise rotations, we know that $\zeta^{-1} = \zeta^{n-1}$. Therefore, $\zeta\sigma = \sigma\zeta^{n-1} = \sigma\zeta^{-1}$ for any n-gon.

□

5.b What's $\zeta^a\sigma\zeta^a$?

Proof. We prove this by induction. By problem 5.a, we know that $\zeta\sigma = \sigma\zeta^{n-1}$ for all $n \geq 3$. We consider the base case $\zeta\sigma\zeta$, where we set $\zeta^3 = 1$. We see that $(\zeta\sigma)\zeta = (\sigma\zeta^{3-1})\zeta = \sigma\zeta^3 = \sigma$.

We induct on the exponent of ζ and assume this relation holds up to m. W shall prove this relation holds for $m+1$ and therefore for all $m \geq 3$. We notice that $\zeta^{m+1}\sigma\zeta^{m+1} = \zeta^1(\zeta^m\sigma\zeta^m)\zeta^1 = \zeta^1\sigma\zeta^1 = \sigma$. Therefore, $\zeta^m\sigma\zeta^m = \sigma$ for all $m \geq 3$.

□

5.c What's $\sigma\zeta^a\sigma$?

Proof. We prove this by induction on the exponent of ζ. Considering the base case $\sigma\zeta\sigma$ with the determined relation from problem 5.a, we see that $\sigma\zeta\sigma = \sigma(\zeta\sigma) = \sigma\sigma\zeta^{n-1} = \zeta^{1(n-1)}$ for all $n \geq 3$.

Assume this holds for all exponents of ζ up to m such that $\sigma\zeta^m\sigma = \zeta^{m(n-1)}$ for all $n \geq 3$. We shall prove that this hold for the $m+1$ exponent, and thus all exponents of ζ. We see that $\sigma\zeta^{m+1}\sigma = \sigma\zeta^m(\zeta\sigma) = \sigma\zeta^m\sigma\zeta^{n-1}$. We employ our inductive hypothesis and observe that $(\sigma\zeta^m\sigma)\zeta^{n-1} = \zeta^{m(n-1)}\zeta^{n-1} = \zeta^{(m+1)(n-1)}$. Thus, we have shown that for all $n \geq 3$, $\sigma\zeta^m\sigma = \zeta^{m(n-1)}$ for all $m \geq 1$. □

6. If S is awesome and $x \in S$, then for all $n \geq 1$ the element $x^{3^n} \in S$. (e.g., x^3 and x^9 and x^{27})

Proof. We prove this claim through induction. We first note that $x^1 = x^{3^0} \in S$. We also note that $(x, x) = xxx = x^{3^1} \in S$. Furthermore, we see that $(x^3, x^3) = x^3x^3x^3 = x^{3^2} \in S$. We induct on x^3 raised to some power, and assume this relation holds true for m. We shall prove that this claim is true for the $m+1$ power. Since x^{3^m} is in an awesome set S, the element (x^{3^m}, x^{3^m}) must also be in S. Hence, we know that $(x^{3^m}, x^{3^m}) = x^{3^m}x^{3^m}x^{3^m} = x^{3^{m+1}}$ is an element that lies in S. Therefore, x^{3^n} will be an element of an awesome set S for all $n \geq 0$. □

6.a (side-quest) Show that $x^5 \in S$.

Proof. We prove this directly. Let S be an awesome set and suppose $x \in S$. Given that S is awesome, We know that $xxx = x^3$ must lie in S. Furthermore, since x and x^3 are elements of S, we know then that $(x, x^3) = x(x^3)x = x^5$ must also be in S. Thus, x^5 is in S. □

7. Show that $x^{2n+1} \in S$ for all $n \geq 0$. (Use induction please)

Proof. Let $x \in S$. Because S is an awesome set, we know that x, x^3, x^7, and x^{15} must also be elements of S.

We induct on the exponent of x and assume this relation holds for any odd degree $2n-1$ for all $n \geq 0$. We shall prove this holds for all odd degrees $2n+1$ for all $n \geq 0$. Since x^{2n-1} and x are elements of S, $(x, x^{2n-1}) = xx^{2n-1}x = x^{2n+1}$ must also be in S. Thus, x^{2n+1} for all $n \geq 0$ must be in S.

□

8. If x has finite order and its order is an odd number, then show that $1 \in S$.

Proof. Let $S \subseteq G$ be an awesome set of a group with a multiplicative law of composition. By the previous inductive proof, we know that if an element of degree 1 is in an awesome set, all odd powers of said element are also in the awesome set. Thus, let $x \in S$ be an element of G with finite odd order n. Consider the element $(x^n, x^n) = (x^n)x^n(x^n) = x^{3n}$ which must be in S. Through algebraic manipulation, we see that $x^{3n} = (x^n)^3 = 1^3$. Thus, $1 \in S$. □

9. If x has finite order and its order is an odd number, then show that for all $m \geq 0$, we have $x^{2m} \in S$.

Proof. Let x be an element of an awesome set S with odd order $n \geq 0$. By the previous constructive proof, we know that if an element of finite, odd order is in an aweomse set, then 1 must be in the awesome set. Thus, 1 must be in S. Since x and 1 are in S, what must follow is that $(x, 1) = x1x = x^2$ is in S.

We induct on the exponent and assume that this holds true up to $2(m-1)$ where $n \neq m \geq 0$, and we shall prove this is true for degree $2m$. Because we assumed that $x^{2(m-1)} \in S$, we note that $(x, x^{2(m-1)}) = xx^{2(m-1)}x = x^{1+2m-2+1} = x^{2m}$ must also be in S. Thus, $x^{2m} \in S$ for all $m \geq 0$. □

10. If x has finite order and its order is an odd number, then show that for all $m \geq 0$, we have $x^m \in S$ (and $x^{-1} \in S$).*****

11. If G is a group with $|G|$ odd, then every element of G has finite order and that order is odd.*****

Proof. Let G be a group of finite odd order. Since G having finite order, let

$$|G| = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_n^{k_n}, \quad \text{where each} \quad p_i^{k_i} \quad \text{is a powered-prime.}$$

□

Nudge for 11: Cauchy's theorem??? Lagrange's theorem

12. Question: if a group has a prime order, does it have to be cyclic?

Proof. Let G be a group such that $|G| = p$ for some prime p. Notice that because p is prime its factorization is $p = 1p$. Since the order of every element in G must divide the order of the group and the identity element is the only element of order 1, any other element of G must have order p. . Thus, let $a \in G$ be an element of order p that is not the identity. What follows is that $\langle a \rangle$ generates group G, and thus G must be cyclic. □

Rework the above proof. Also why is $\langle a \rangle = G$? (Hint: how many elements are in the set $\langle a \rangle$?)

13. Question: if S is an awesome subset of $\mathbb{Z}/15\mathbb{Z}$ and $3 \in S$, then what can we say about S? [What else would have to be in there? Does S have to be a subgroup?] ****

14. Reading: what's a "direct product"? What's a "semi-direct product"? Get a few examples of each. (*Read a bit, much is done.)

Bonus: 15. Is the subset of integers as a ring an awesome set, but a group? Matrices that do that??// what would the ring need to satisfy, both literally and consequently?

16. Multiplication is aba, does addition be really nice?? Does it have to be different... Is addition like a subgroup???? Not a subgrin, or ideal, it's kind of something different.

Q. Since $S_3 \cong D_3$, does there exist a nice pattern ("structure") of subsets in the symmetric group like the dihedral group up to the n-th case where these subsets are guaranteed awesome... Even though $S_n \cong D_n$ is false?

We consider the dihedral group $D_3 = \langle x, y | x^2 = y^3 = 1 \quad \text{and} \quad yx = xy^2 \rangle$.

(*Not sure how one could generalize finding the *aba*-set of a general group G, but)

We consider the *aba*-set $S := \{x, xy, xy^2\} \subseteq D_3$. We know this set to be *aba*-closed by not only itself, but the entire dihedral group.

Since S is *aba*-closed with the entire group, one idea that comes to mind is that of an analog to a two-sided *coset* of a group—however, recall that S is not a group at all as it lacks the identity element. We will refer to these "cosets" as *semi-cosets*.

We want to be able to recognize things like subgroups in a general group, so we observe what happens when we attempt to redefine these semi-cosets using the maximal *aba*-set S with the elements of D_3.

We compute the following:

- $1S1 = 1S = S1 = S$
- $ySy = yS = Sy = S$
- $y^2Sy^2 = y^2S = Sy^2 = S$
- $xSx = S$; but $xS = Sx = \{1, y, y^2\} \neq S$
- $(xy)S(xy) = S$; but $(xy)S = S(xy) = \{1, y, y^2\} \neq S$
- $(xy^2)S(xy^2) = S$; but $(xy^2)S = S(xy^2) = \{1, y, y^2\} \neq S$

Let D_3/L_{D_3-L} be the set of *aba*-closed semi-cosets with chosen representatives such that they leave the coset unchaged.

More generally speaking,

$$\{g \in G : gL_{(aba)} = L_{(aba)}g = L_{(aba)}\}.$$

Because $L_{(aba)}$ is an *aba*-closed semi-coset with collected group elements. Composition can be defined as

$$(aL_{(aba)})(bL_{(aba)}) = a(L_{(aba)}b)L_{(aba)} = a(bL_{(aba)})L_{(aba)} = (ab)L_{(aba)}L_{(aba)} = (ab)L_{(aba)}.$$

Going back to our example with D_3/L_{D_3-L}, the set then

$$\{1, y, y^2\}$$

The MC-set $L_{aba} = \{x, xy, xy^2\} \subseteq D_3$ is maximal via direct construction. are precisely the elements of D_3 such that for each $g \in \{1, y, y^2\}$, this "strong conjugation" by g preserves S in its entirety:

$$gSg = gS = Sg = S.$$

We see that the set of such elements forms a subgroup. So, we claim that $D_3/L_{D_3-L} \cong \langle y | y^3 = 1 \rangle \cong C_3$.

Lemma.

$$(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes_\psi \mathbb{Z}/3\mathbb{Z}$$