

## MATH 417, HOMEWORK 11

CHARLES ANCEL

**Exercise 1.** Let  $G$  be a group, with subgroup  $H \leq G$ . Let  $\lambda : G \rightarrow \text{Sym}(G/H)$  be the left-coset action, defined by  $\lambda(g)(aH) := gaH$ . Show that  $\ker(\lambda) = \bigcap_{g \in G} gHg^{-1}$ .

---

### SOLUTION

**Lemma:** By definition, the kernel of a homomorphism  $\lambda$  is:

$$\ker(\lambda) = \{g \in G \mid \lambda(g) = \text{id}\}$$

where  $\text{id}$  is the identity permutation on  $G/H$ .

To prove that  $\ker(\lambda) = \bigcap_{g \in G} gHg^{-1}$ , we need to analyze the kernel of the homomorphism  $\lambda : G \rightarrow \text{Sym}(G/H)$ .

Since  $\lambda(g)$  acts on the cosets by  $\lambda(g)(aH) = gaH$ , we have:

$$\lambda(g) = \text{id} \iff gaH = aH \quad \forall aH \in G/H.$$

This implies  $gaH = aH$  for all  $aH \in G/H$ , meaning  $g \in H^a = aHa^{-1}$  for all  $a \in G$ .

Therefore,  $g$  must belong to the intersection of all conjugates of  $H$  in  $G$ :

$$\ker(\lambda) = \bigcap_{a \in G} aHa^{-1}.$$

Thus, we have shown that  $\ker(\lambda) = \bigcap_{g \in G} gHg^{-1}$ .

**Exercise 2.** Let  $G$  be a group with subgroup  $H \leq G$ , and let  $K = \ker(\lambda)$  as in the previous problem. Suppose  $H$  has finite index in  $G$ , and write  $m = [G : H]$ . Show that  $G/K$  is isomorphic to a subgroup of  $\text{Sym}(G/H)$ . Use this to show that  $[G : K]$  divides  $m!$ , and then use this to show that  $[H : K]$  divides  $(m - 1)!$ .

---

### SOLUTION

**First Isomorphism Theorem:** The First Isomorphism Theorem states that if  $\phi : G \rightarrow G'$  is a homomorphism with kernel  $\ker(\phi)$ , then the quotient group  $G/\ker(\phi)$  is isomorphic to the image of  $\phi$ , i.e.,  $G/\ker(\phi) \cong \text{Im}(\phi)$ .

Since  $\lambda : G \rightarrow \text{Sym}(G/H)$  is a homomorphism, and  $K = \ker(\lambda)$ , by the First Isomorphism Theorem, we have:

$$G/K \cong \lambda(G) \leq \text{Sym}(G/H).$$

Therefore,  $G/K$  is isomorphic to a subgroup of  $\text{Sym}(G/H)$ .

The order of  $\text{Sym}(G/H)$  is  $m!$ . Hence,  $|G/K|$  divides  $|\text{Sym}(G/H)| = m!$ . Therefore:

$$[G : K] \mid m!.$$

Next, since  $K \leq H$  and  $[G : H] = m$ , we have:

$$[G : K] = [G : H] \cdot [H : K] = m \cdot [H : K].$$

Given that  $[G : K] \mid m!$ , it follows that:

$$m \cdot [H : K] \mid m!.$$

Dividing both sides by  $m$ :

$$[H : K] \mid (m - 1)!.$$

**Exercise 3.** Show that if  $G$  is a finite group, and if  $p$  is the smallest prime which divides the order of  $G$ , then any subgroup  $H$  of  $G$  of index  $p$  is normal in  $G$ . (Hint: use the previous exercise to show that  $H = K$ .)

---

### SOLUTION

**First Isomorphism Theorem:** The First Isomorphism Theorem states that if  $\phi : G \rightarrow G'$  is a homomorphism with kernel  $\ker(\phi)$ , then the quotient group  $G/\ker(\phi)$  is isomorphic to the image of  $\phi$ , i.e.,  $G/\ker(\phi) \cong \text{Im}(\phi)$ .

Let  $G$  be a finite group, and let  $p$  be the smallest prime dividing the order of  $G$ . Suppose  $H$  is a subgroup of  $G$  with  $[G : H] = p$ . From Exercise 2, we know that:

$$G/H \cong \text{Sym}(G/H).$$

Since  $[G : H] = p$ ,  $G/H$  has  $p$  elements, and  $p$  is the smallest prime dividing  $|G|$ ,  $\text{Sym}(G/H)$  is isomorphic to  $S_p$ , the symmetric group on  $p$  elements. Note that  $S_p$  has order  $p!$ .

By the previous exercise,  $[H : K]$  divides  $(p - 1)!$ . Since  $H$  has index  $p$ , the subgroup  $K$  must be  $H$  itself because any smaller index would contradict  $p$  being the smallest prime. Hence,  $H = K$ , and  $H$  is normal in  $G$ .

**Exercise 4.** Count the number of elements in:

- a.  $S_6$  with cycle structure  $3 + 3$ .
- b.  $S_6$  with cycle structure  $2 + 2 + 2$ .
- c.  $S_8$  with cycle structure  $3 + 3 + 1 + 1$ .

### SOLUTION

**Lemma:** To count the number of elements with a specific cycle structure in a symmetric group  $S_n$ , we use the following formula:

$$\frac{n!}{\prod_i (n_i \cdot c_i)}$$

where  $n_i$  is the length of the  $i$ -th cycle and  $c_i$  is the number of cycles of length  $n_i$ .

- a. To find the number of elements in  $S_6$  with cycle structure  $3 + 3$ :

$$\frac{1}{2} \binom{6}{3} \cdot \binom{3}{3}$$

Here, the  $\binom{6}{3}$  chooses which 3 elements are in the first 3-cycle, and the  $\binom{3}{3}$  chooses the elements for the second 3-cycle. Dividing by 2 accounts for the fact that the two 3-cycles can be chosen in any order:

$$= \frac{1}{2} \cdot 20 \cdot 1 = 10.$$

- b. To find the number of elements in  $S_6$  with cycle structure  $2 + 2 + 2$ :

$$\frac{1}{3!} \binom{6}{2} \binom{4}{2} \binom{2}{2}$$

Here, the  $\binom{6}{2}$  chooses which 2 elements are in the first 2-cycle,  $\binom{4}{2}$  for the second 2-cycle, and  $\binom{2}{2}$  for the third 2-cycle. Dividing by 3! accounts for the fact that the three 2-cycles can be chosen in any order:

$$= \frac{1}{6} \cdot 15 \cdot 6 \cdot 1 = 15.$$

- c. To find the number of elements in  $S_8$  with cycle structure  $3 + 3 + 1 + 1$ :

$$\frac{1}{2!} \binom{8}{3} \binom{5}{3} \binom{2}{1} \binom{1}{1}$$

Here, the  $\binom{8}{3}$  chooses which 3 elements are in the first 3-cycle,  $\binom{5}{3}$  for the second 3-cycle,  $\binom{2}{1}$  for the first 1-cycle, and  $\binom{1}{1}$  for the second 1-cycle. Dividing by 2! accounts for the fact that the two 3-cycles can be chosen in any order:

$$= \frac{1}{2} \cdot 56 \cdot 10 \cdot 2 \cdot 1 = 280.$$

**Exercise 5.1.9.** A subgroup  $H$  of  $S_n$  is called transitive if the standard action by  $H$  on  $\{1, \dots, n\}$  is transitive. Show that the transitive subgroups of  $S_3$  are  $A_3$  and  $S_3$ .

---

SOLUTION

**Definition of Transitivity:** A group  $G$  acting on a set  $X$  is said to be transitive if for any  $x, y \in X$ , there exists a  $g \in G$  such that  $g \cdot x = y$ . This means there is only one orbit under the action of  $G$  on  $X$ .

The group  $S_3$  is the symmetric group on 3 elements, and  $A_3$  is the alternating group on 3 elements. A subgroup  $H$  of  $S_3$  is transitive if it acts transitively on  $\{1, 2, 3\}$ .

Consider the elements of  $S_3$ :  $\{e, (12), (13), (23), (123), (132)\}$ .

- $S_3$  itself is transitive since any element can be mapped to any other element by some permutation.
- $A_3$  consists of  $\{e, (123), (132)\}$ , which are the even permutations.  $A_3$  is also transitive as it can map any element to any other element using these even permutations.

Any other proper subgroup of  $S_3$  would be of order 2 or less and thus cannot act transitively on 3 elements. Hence, the transitive subgroups of  $S_3$  are  $A_3$  and  $S_3$ .

**Exercise 6.** Identify  $D_4$  with a subgroup of  $SO(3)$ . For each element  $g \in D_4$ , compute the set  $\text{CL}_{SO(3)}(g) \cap D_4$ , and in each case determine whether it is equal to  $\text{CL}_{D_4}(g)$ .

---

### SOLUTION

**Conjugacy Class:** The conjugacy class of an element  $g$  in a group  $G$  is the set of elements that are conjugate to  $g$ , i.e.,  $\text{CL}_G(g) = \{xgx^{-1} \mid x \in G\}$ .

The dihedral group  $D_4$  consists of the symmetries of a square, which can be embedded in  $SO(3)$  as rotations. We identify  $D_4$  with a subgroup of  $SO(3)$ .

- $e$ : Identity element.  $\text{CL}_{SO(3)}(e) \cap D_4 = \{e\} = \text{CL}_{D_4}(e)$ .
- $r_{90}, r_{270}$ : Rotations by  $90^\circ$  and  $270^\circ$ . Both have the same conjugacy class in  $D_4$  and in  $SO(3)$ .  $\text{CL}_{SO(3)}(r_{90}) \cap D_4 = \{r_{90}, r_{270}\} = \text{CL}_{D_4}(r_{90})$ .
- $r_{180}$ : Rotation by  $180^\circ$ .  $\text{CL}_{SO(3)}(r_{180}) \cap D_4 = \{r_{180}\} = \text{CL}_{D_4}(r_{180})$ .
- Reflections  $s_x, s_y, s_{d1}, s_{d2}$ : Each reflection forms its own conjugacy class.  $\text{CL}_{SO(3)}(s_x) \cap D_4 = \{s_x\} = \text{CL}_{D_4}(s_x)$ , similarly for other reflections.

In all cases,  $\text{CL}_{SO(3)}(g) \cap D_4 = \text{CL}_{D_4}(g)$ , showing that the conjugacy classes within  $D_4$  remain unchanged when considering the conjugacy classes within  $SO(3)$  and intersecting back with  $D_4$ .

**Exercise 5.2.1.** How many necklaces can be made with six beads of three different colors.

---

### SOLUTION

**Polya's Enumeration Theorem:** Polya's Enumeration Theorem is a combinatorial method used to count the number of distinct objects under group actions, taking symmetries into account. It involves using cycle index polynomials to calculate the number of distinct colorings or arrangements.

The number of distinct necklaces with six beads and three different colors can be calculated using Polya's Enumeration Theorem.

Let the colors be  $a, b, c$ . We need to count the number of distinct necklaces up to rotation.

The group of rotations of a six-bead necklace is  $C_6$ , the cyclic group of order 6. The cycle index polynomial for  $C_6$  is:

$$Z(C_6) = \frac{1}{6}(x_1^6 + 2x_3^2 + 3x_2^3)$$

Substituting  $x_i = a^i + b^i + c^i$ , we get:

$$Z(C_6) = \frac{1}{6}((a + b + c)^6 + 2(a^3 + b^3 + c^3)^2 + 3(a^2 + b^2 + c^2)^3)$$

We expand this expression:

$$Z(C_6) = \frac{1}{6}(a^6 + b^6 + c^6 + 6a^5b + 6a^5c + 6b^5a + 6b^5c + 6c^5a + 6c^5b + 15a^4b^2 + 15a^4c^2 + 15b^4a^2 + 15b^4c^2 + 15c^4a^2 + 15c^4b^2 + 20a^3b^3 + 20a^3c^3 + 20b^3c^3 + 15a^2b^2c^2).$$

After simplifying and adding the coefficients, we count the distinct colorings. After calculation, we find there are 92 distinct necklaces.

Therefore, the number of distinct necklaces that can be made with six beads of three different colors is 92.