

**Student: Yu Cheng (Jade)**

**Math 611**

**Homework #2**

**September 25, 2010**

### Chapter 1.9 Homomorphisms

---

**Exercise 4:** Determine  $\text{Aut } G$  for the following groups.

**a.**  $G$  is an infinite cyclic group.

**Answer:** An infinite cyclic group is isomorphic to the additive group of integer  $\mathbb{Z}$ .  $\text{Aut } \mathbb{Z}$  contains two elements. Infinite cyclic group,  $\mathbb{Z}$ , has two generators 1 and  $-1$ . We can have  $\phi_1(1) = 1$  and  $\phi_2(1) = -1$ .

$$\begin{pmatrix} \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \\ \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \end{pmatrix}, \quad \begin{pmatrix} \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \\ \cdots & 2 & 1 & 0 & -1 & -2 & \cdots \end{pmatrix}$$

**b.**  $G$  is a cyclic group of order six.

**Answer:** Cyclic group of order  $n$  is isomorphic to  $\mathbb{Z}/n\mathbb{Z}$  written additively. So  $G \cong \mathbb{Z}/6\mathbb{Z}$ . The *theorem of automorphism group of the cyclic group* states  $\mathbb{Z}/n\mathbb{Z}$ 's automorphism group is  $(\mathbb{Z}/n\mathbb{Z})^\times$ , where  $(\mathbb{Z}/n\mathbb{Z})^\times$  is the multiplicative group of all integers modulo  $n$  which are relatively prime to  $n$ . They form a group under multiplication modulo  $n$ . For  $n = 6$ ,  $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$ . So  $\text{Aut } G$ , where  $G$  is the cyclic group of order six, has two elements. We can have  $\phi_1(1) = 1$  and  $\phi_2(1) = 5$ .

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

**c.**  $G$  is any finite cyclic group.

**Answer:** For any finite cyclic group the theorem above holds.  $\text{Aut } G = (\mathbb{Z}/n\mathbb{Z})^\times$ , where  $(\mathbb{Z}/n\mathbb{Z})^\times$  is the multiplicative group of all integers modulo  $n$  which are relatively prime to  $n$ . They form a group under multiplication modulo  $n$ . For example,  $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ .

**Exercise 5:** Determine  $\text{Aut } S_3$

**Answer:** The symmetric group  $S_3$  is a permutation group of order  $3! = 6$ . If we use the permutation cycle notation for a given permutation, the multiplication table of  $S_3$  can be expressed as below:

|           |           |           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| .         | (1)(2)(3) | (12)(3)   | (1)(23)   | (2)(13)   | (123)     | (321)     |
| (1)(2)(3) | (1)(2)(3) | (12)(3)   | (1)(23)   | (2)(13)   | (123)     | (321)     |
| (12)(3)   | (12)(3)   | (1)(2)(3) | (321)     | (123)     | (2)(13)   | (1)(23)   |
| (1)(23)   | (1)(23)   | (123)     | (1)(2)(3) | (321)     | (12)(3)   | (2)(13)   |
| (2)(13)   | (2)(13)   | (321)     | (123)     | (1)(2)(3) | (1)(23)   | (12)(3)   |
| (123)     | (123)     | (1)(23)   | (2)(13)   | (12)(3)   | (321)     | (1)(2)(3) |
| (321)     | (321)     | (2)(13)   | (12)(3)   | (1)(23)   | (1)(2)(3) | (123)     |

For simplification purpose, we can use  $e = (1)(2)(3)$ ,  $\tau_1 = (12)(3)$ ,  $\tau_2 = (1)(23)$ ,  $\tau_3 = (2)(13)$ ,  $\sigma_1 = (123)$ ,  $\sigma_2 = (321)$ . The multiplication table is re-written as the following:

|            |            |            |            |            |            |            |
|------------|------------|------------|------------|------------|------------|------------|
| .          | $e$        | $\tau_1$   | $\tau_2$   | $\tau_3$   | $\sigma_1$ | $\sigma_2$ |
| $e$        | $e$        | $\tau_1$   | $\tau_2$   | $\tau_3$   | $\sigma_1$ | $\sigma_2$ |
| $\tau_1$   | $\tau_1$   | $e$        | $\sigma_2$ | $\sigma_1$ | $\tau_3$   | $\tau_2$   |
| $\tau_2$   | $\tau_2$   | $\sigma_1$ | $e$        | $\sigma_2$ | $\tau_1$   | $\tau_3$   |
| $\tau_3$   | $\tau_3$   | $\sigma_2$ | $\sigma_1$ | $e$        | $\tau_2$   | $\tau_1$   |
| $\sigma_1$ | $\sigma_1$ | $\tau_2$   | $\tau_3$   | $\tau_1$   | $\sigma_2$ | $e$        |
| $\sigma_2$ | $\sigma_2$ | $\tau_3$   | $\tau_1$   | $\tau_2$   | $e$        | $\sigma_1$ |

In this group, two elements,  $\sigma_1$  and  $\sigma_2$  have order 3; three elements  $\tau_1, \tau_2$ , and  $\tau_3$  have order 2; one element  $e$  has order 1. Isomorphisms send elements to elements with the same order. So, there are two ways to map  $\sigma_1$  and  $\sigma_2$ . Let's call the constructed automorphisms  $\phi$ . We can have  $\phi(\sigma_1) = \sigma_1$  or  $\phi(\sigma_1) = \sigma_2$ . When  $\phi(\sigma_1) = \sigma_1$ , we can construct three different automorphisms, one of which is the identity mapping:

$$\begin{pmatrix} e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \\ e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \end{pmatrix}, \begin{pmatrix} e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \\ e & \tau_2 & \tau_3 & \tau_1 & \sigma_1 & \sigma_2 \end{pmatrix}, \begin{pmatrix} e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \\ e & \tau_3 & \tau_1 & \tau_2 & \sigma_1 & \sigma_2 \end{pmatrix}$$

When  $\phi(\sigma_1) = \sigma_2$ , we can construct three different automorphisms:

$$\begin{pmatrix} e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \\ e & \tau_1 & \tau_3 & \tau_2 & \sigma_2 & \sigma_1 \end{pmatrix}, \begin{pmatrix} e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \\ e & \tau_2 & \tau_1 & \tau_3 & \sigma_2 & \sigma_1 \end{pmatrix}, \begin{pmatrix} e & \tau_1 & \tau_2 & \tau_3 & \sigma_1 & \sigma_2 \\ e & \tau_3 & \tau_2 & \tau_1 & \sigma_2 & \sigma_1 \end{pmatrix}$$

So  $\text{Aut } S_3$  has 6 elements, and they are the 6 automorphisms mapping from  $S_3$  to  $S_3$  itself as listed above.

**Exercise 6:** Let  $a \in G$ , a group, and define the *inner automorphism (or conjugation)*  $I_a$  to be the map  $x \rightarrow axa^{-1}$  in  $G$ .

- a. Verify that  $I_a$  is an automorphism.

**Answer:**

First we will show that  $I_a$  is a group homomorphism.

$$\begin{aligned} I_a(x) \cdot I_a(y) &= axa^{-1}aya^{-1} \\ &= axya^{-1} \\ &= I_a(xy). \end{aligned}$$

Then we will show that  $I_a$  is an isomorphism,  $I_a$  is a bijective group homomorphism.  $I_a$  is an onto map. For any  $y \in G$ , there is a  $x \in G$ , such that  $axa^{-1} = y$ , where  $a \in G$  is a fixed element.

$G$  is closed under group operation

$$\Rightarrow a^{-1}ya \in G$$

$$\Rightarrow a^{-1}ya = x \in G$$

$$\Rightarrow y = axa^{-1}, \text{ where } x \in G.$$

$I_a$  is a one-to-one map. For any  $ax_1a^{-1} = ax_2a^{-1}$ , it follows that  $x_1 = x_2$ .

$$\begin{aligned} ax_1a^{-1} &= ax_2a^{-1} \\ \Rightarrow a^{-1}(ax_1a^{-1})a &= a^{-1}(ax_2a^{-1})a \\ \Rightarrow x_1 &= x_2. \end{aligned}$$

In addition,  $I_a$  is a map from  $G$  to  $G$  itself, so  $I_a$  is an automorphism.

- b.** Show that  $a \rightarrow I_a$  is a homomorphism of  $G$  into  $\text{Aut } G$  with kernel the center  $C$  of  $G$ . Hence conclude that  $\text{Inn } G \equiv \{I_a \mid a \in G\}$  is a subgroup of  $\text{Aut } G$  with  $\text{Inn } G \cong G/C$ .

**Answer:**

We will first show that the map  $\phi: a \rightarrow I_a$  is a homomorphism. Let's call  $\phi(ab) = I_{ab}$ .

$$\begin{aligned} \phi(ab)(x) &= (ab)x(ab)^{-1} \\ \Rightarrow \phi(ab)(x) &= abxb^{-1}a^{-1}. \end{aligned}$$

$\phi(a) \circ \phi(b) = I_a \circ I_b$ , is the function composition that projects  $x$  first by  $I_b$  and then by  $I_a$ ,

$$\begin{aligned} \phi(b)(x) &= bxb^{-1} \\ \phi(a)(bxb^{-1}) &= a(bxb^{-1})a^{-1} \\ \Rightarrow (\phi(a) \circ \phi(b))(x) &= abxb^{-1}a^{-1}. \end{aligned}$$

Hence, we've shown these two maps are the same,  $\phi(ab) = \phi(a) \circ \phi(b)$ . In addition we have  $a \in G$  and  $I_a \in \text{Aut } G$ . Map  $\phi: a \rightarrow I_a$  is, therefore, a homomorphism from  $G$  into  $\text{Aut } G$ .

We will then show the kernel of this group homomorphism is the center  $C$  of  $G$ . Recall the definition of the center of a group,

$$C(G) = \{c \in G \mid cg = gc \text{ for every } g \in G\}.$$

The identity element in  $\text{Aut } G$  is the identity map,  $I_e$ , where  $I_e(x) = x$  for all  $x \in G$ . If we have  $a \in \text{Ker}(\phi)$ , we can derive that  $a$  is also in the center  $C$ ,  $a \in C$ .

$$\begin{aligned} a &\in \text{Ker}(\phi) \\ \Rightarrow I_a(x) &= axa^{-1} = x \\ \Rightarrow ax &= xa \text{ for every } x \in G \\ \Rightarrow a &\in C. \end{aligned}$$

If we have  $b \in C$ , we can derive that  $b$  is also in the kernel of  $\phi$ ,  $b \in \text{Ker}(\phi)$ .

$$\begin{aligned} b &\in C \\ \Rightarrow bx &= xb \text{ for every } x \in G \\ \Rightarrow bxb^{-1} &= x \\ \Rightarrow b &\in \text{Ker}(\phi). \end{aligned}$$

So we've shown the kernel of the group homomorphism  $\phi: a \rightarrow I_a$  from  $G$  to  $\text{Aut } G$  is  $C$  of  $G$ . According to the first isomorphism theorem  $G/\text{Ker}(\phi) = G/C$  is isomorphic to  $\text{Im}(\phi) = \{I_a \mid a \in G\}$ . In other words,  $\text{Inn } G \cong G/C$ .

- c. Verify that  $\text{Inn } G$  is a normal subgroup of  $\text{Aut } G$ .  $\text{Aut } G/\text{Inn } G$  is called the group of *outer automorphisms*.

**Answer:**

Let have  $x, a \in G$ ,  $\phi_a \in \text{Inn } G$  and  $\theta \in \text{Aut } G$ . We need to show  $\theta \circ \phi_a \circ \theta^{-1} \in \text{Inn } G$ . Since  $\theta$  is a homomorphism,  $\theta(p \cdot q) = \theta(p) \cdot \theta(q)$ , and  $\theta(p^{-1}) = \theta^{-1}(p)$ , where  $p, q \in G$ .

$$\begin{aligned} \theta \circ \phi_a \circ \theta^{-1}(x) &= \theta \circ \phi_a(\theta^{-1}(x)) \\ &= \theta(a \cdot \theta^{-1}(x) \cdot a^{-1}) \\ &= \theta(a) \cdot \theta(\theta^{-1}(x)) \cdot \theta(a^{-1}) \\ &= \theta(a) \cdot x \cdot \theta(a^{-1}) \\ &= \theta(a) \cdot x \cdot \theta^{-1}(a). \end{aligned}$$

Therefore,  $\text{Inn } G$  is conjugate over  $\text{Aut } G$ ,  $\text{Inn } G$  is a normal subgroup of  $\text{Aut } G$ , with the quotient group  $\text{Aut } G/\text{Inn } G$ , the outer automorphisms.

**Exercise 11:** Let  $G$  be a finite group,  $\alpha$  an automorphism of  $G$  and set  $I = \{g \in G \mid \alpha(g) = g^{-1}\}$ .

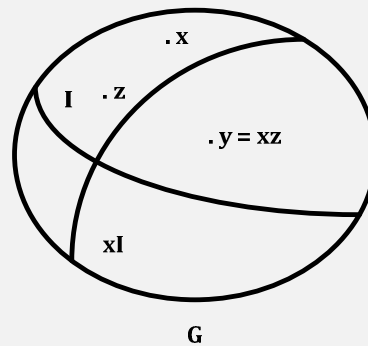
a. Suppose  $|I| > 3/4|G|$ , show that  $G$  is abelian.

**Answer:**

First I'll fix an element  $x$  in  $I$ , and construct a subset of  $G$ ,  $xI = \{g \in G \mid g = xi, \forall i \in I\}$ . It is easy to show that  $|I| = |xI|$ . Let's say  $I = \{i_1, i_2, \dots, i_n\}$ ,  $|I| \neq |xI|$  if and only if no two elements become the same after the left multiplication with  $x$ . If there are two elements becoming the same, we have the following conclusion.

$$\begin{aligned} xi_p &= xi_q \\ \Rightarrow x^{-1}xi_p &= x^{-1}xi_q \\ \Rightarrow i_p &= i_q. \end{aligned}$$

This is a conflict, no two elements in a set are the same. So  $|I| = |xI|$ . Now we have the following configuration of the group  $G$ .



Meanwhile, since  $|I| > 3/4|G|$ , we have  $|I| = |xI| > 3/4|G|$ . Clearly the intersection of  $I$  and  $xI$  has to be more than  $1/2|G|$ .

$$\begin{aligned} |I| + |xI| - |I \cap xI| &= |I \cup xI| \leq |G| \\ \Rightarrow |I \cap xI| &\geq |I| + |xI| - |G| \\ &> \frac{3}{4}|G| + \frac{3}{4}|G| - |G| \\ &= \frac{1}{2}|G|. \end{aligned}$$

Let's pick an element  $y \in I \cap xI$ . Since  $y \in xI$ ,  $y$  can be written as  $y = xz$ , for some  $z \in I$ .

$$\begin{aligned} xy \in I &\Rightarrow \alpha(xy) = (xy)^{-1} = y^{-1}x^{-1} \\ x \in I, y \in I &\Rightarrow \alpha(xy) = \alpha(x)\alpha(y) = x^{-1}y^{-1} \\ \Rightarrow y^{-1}x^{-1} &= x^{-1}y^{-1} \end{aligned}$$

$$\Rightarrow yy^{-1}x^{-1}y = yx^{-1}y^{-1}y$$

$$\Rightarrow yx = xy.$$

Hence we conclude that for any  $y \in I \cap xI$ ,  $y$  is commutative with  $x$ . In other words  $I \cap xI$  is contained in the centralizer of  $x$ ,

$$I \cap xI \subseteq C_G(x).$$

As we know centralizer is a subgroup,  $C_G(x) \leq G$ . According to Lagrange's theorem, the order of the subgroup must divide the order of the group. Since  $|C_G(x)|$  is greater than half the order of the group, it must be the whole group.

$$|C_G(x)| \geq |I \cap xI| > \frac{1}{2}|G|$$

$$\Rightarrow C_G(x) = G.$$

So  $x$  is commutative with the entire group  $G$ . Therefore  $x \in C(G)$  for any  $x \in I$ , where  $C(G)$  is a subgroup of  $G$ , namely the center of  $G$ . In other words,  $I \subseteq C(G)$ .

$$I \subseteq C(G)$$

$$\Rightarrow \frac{3}{4}|G| < |I| \leq |C(G)|$$

$$\Rightarrow |C(G)| > \frac{1}{2}|G|$$

$$\Rightarrow C(G) = G.$$

By definition, the center of a group is a commutative subgroup, therefore  $G$  is abelian.

- b.** If  $|I| = 3/4|G|$ , show that  $G$  has an abelian subgroup of index 2.

**Answer:** Follow the same logic as the previous question, we have  $|I \cap xI| \geq 1/2|G|$ .

$$|I| + |xI| - |I \cap xI| = |I \cup xI| \leq |G|$$

$$\Rightarrow |I \cap xI| \geq |I| + |xI| - |G|$$

$$\geq \frac{3}{4}|G| + \frac{3}{4}|G| - |G|$$

$$= \frac{1}{2}|G|.$$

Further, every element in  $|I \cap xI|$  is commutative with the fixed element,  $x$ , which was used to construct the set  $xI$ . We derived that  $I \cap xI \subseteq C_G(x)$ .

$$|I \cap xI| \geq \frac{1}{2}|G|$$

$$\Rightarrow C_G(x) \geq \frac{1}{2}|G|.$$

Case #1: If  $C_G(x) = 1/2|G|$ , then we have  $|I \cap xI| = |C_G(x)| = 1/2|G|$ . So we've found a subgroup  $C_G(x) = I \cap xI$  of  $G$  that has an index of 2. We can prove that  $I \cap xI$  is commutative. Let's have  $xi_1, xi_2, xi \in I \cap xI$ , where  $i_1, i_2, i \in I$ . We will first show  $xi = ix$ .

$$xi \in I \cap xI$$

$$\Rightarrow \alpha(xi) = (xi)^{-1} = i^{-1}x^{-1}$$

$$\alpha(xi) = \alpha(x)\alpha(i) = x^{-1}i^{-1}$$

$$\Rightarrow i^{-1}x^{-1} = x^{-1}i^{-1}$$

$$\Rightarrow xi = ix.$$

Now, we will show  $I \cap xI$  is commutative. Since  $I \cap xI$  is a subgroup, it is closed under the group operation.

$$xi_1xi_2 \in I \cap xI$$

$$\Rightarrow xi_1xi_2 \in I$$

$$\Rightarrow \alpha(xi_1xi_2) = \alpha(xi_1i_2x) = (xi_1i_2x)^{-1} = x^{-1}i_2^{-1}i_1^{-1}x^{-1}$$

$$\alpha(xi_1xi_2) = \alpha(x)\alpha(i_1)\alpha(i_2)\alpha(x) = x^{-1}i_1^{-1}i_2^{-1}x^{-1}$$

$$\Rightarrow x^{-1}i_2^{-1}i_1^{-1}x^{-1} = x^{-1}i_1^{-1}i_2^{-1}x^{-1}$$

$$\Rightarrow i_1^{-1}i_2^{-1} = i_1^{-1}i_2^{-1}$$

$$\Rightarrow i_1i_2 = i_2i_1$$

$$\Rightarrow x^2i_1i_2 = x^2i_2i_1$$

$$\Rightarrow xi_1xi_2 = xi_2xi_1.$$

Hence we've shown if  $C_G(x) = 1/2|G|$ ,  $I \cap xI = C_G(x)$  is what we're looking for.  $I \cap xI = C_G(x) \leq G$ ,  $I \cap xI = C_G(x)$  is commutative, and  $[G: I \cap xI] = [G: C_G(x)] = 2$ .

Case #2: If  $C_G(x) > 1/2|G|$ , then just like the previous question, we can derive that  $G$  is an abelian group. We can prove that under this condition,  $I \cap xI$  is a abelian subgroup of  $G$ . Since  $G$  is abelian, we just need to show that  $I \cap xI$  is a subgroup of  $G$ ,  $I \cap xI \leq G$ .

First we will show that  $I \cap xI$  is closed under the group operation. We will show  $xi_1xi_2 \in I$  first.

$$(xi_1xi_2)^{-1} = (i_2xi_1x)^{-1} = x^{-1}i_1^{-1}x^{-1}i_2^{-1}$$

$$\alpha(xi_1xi_2) = \alpha(x)\alpha(i_1)\alpha(x)\alpha(i_2) = x^{-1}i_1^{-1}x^{-1}i_2^{-1}$$

$$\alpha(xi_1xi_2) = (xi_1xi_2)^{-1}$$

$$\Rightarrow xi_1xi_2 \in I.$$

At the same time, we can show  $xi_1xi_2 \in xI$  as well

$$\alpha(i_1xi_2) = \alpha(i_2xi_1) = i_2^{-1}x^{-1}i_1^{-1} = (i_1xi_2)^{-1}$$

$$\Rightarrow i_1xi_2 \in I$$

$$\Rightarrow xi_1xi_2 \in xI.$$

Together we have,  $xi_1xi_2 \in I \cap xI$ .  $I \cap xI$  is closed under the group operation. Also it is clear that the inverse of  $xi$  is in  $I \cap xI$ .

$$\alpha((xi)^{-1}) = \alpha(i^{-1}x^{-1}) = ix = xi \Rightarrow (xi)^{-1} \in I$$

$$\alpha(x^{-1}i^{-1}x^{-1}) = xix = (x^{-1}i^{-1}x^{-1})^{-1}$$

$$\Rightarrow x^{-1}i^{-1}x^{-1} \in I$$

$$\Rightarrow x(x^{-1}i^{-1}x^{-1}) = (xi)^{-1} \in xI$$

$$\Rightarrow (xi)^{-1} \in I \cap xI.$$

At this point, we've shown that if  $C_G(x) > 1/2|G|$ ,  $G$  is an abelian group, and  $I \cap xI$  is a subgroup of  $G$ . Since  $3/4|G| \geq |I \cap xI| \geq 1/2|G|$ , and a subgroup can't be larger than half of the size,  $|I \cap xI| = 1/2|G|$ .

In summary of Case #1 and Case #2, regardless of  $G$  is an abelian group, or non-abelian group with a 3-4 automorphism,  $I \cap xI$  forms an abelian subgroup of  $G$  with an index of 2.

## Course Website Exercises

---

**Exercise 2:** Let  $G$  be a simple group with more than 2 elements. Suppose  $\varphi: G \rightarrow S_k$  is a homomorphism.

- a. Show that  $\varphi(G) \leq A_k$ .



**Answer:**

Since  $\varphi: G \rightarrow S_k$  is a homomorphism, according to the first isomorphism theorem, the quotient group of the kernel of this homomorphism is isomorphic to the image of this homomorphism

$$G/\text{Ker}(\varphi) \cong \text{Img}(\varphi) \leq S_k$$

$\text{Ker}(\varphi) \triangleleft G$  because the kernel of a homomorphism is a normal subgroup. Since  $G$  contains only two normal subgroups, the trivial normal subgroup,  $\{e\}$ , and itself. Hence,  $\text{Ker}(\varphi)$  is either  $\{e\}$  or  $G$ . If  $\text{Ker}(\varphi) = G$ , we have the following conclusion, and we are done.

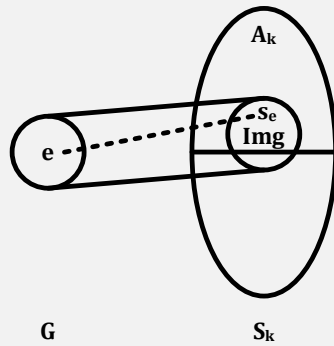
$$\left| \frac{G}{\text{Ker}(\varphi)} \right| = \left| \frac{G}{G} \right| = 1 = |\text{Img}(\varphi)|$$

$$\Rightarrow \text{Img}(\varphi) = \{s_e\} < A_k$$

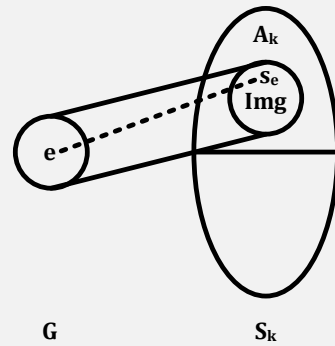
$$\Rightarrow \text{Img}(\varphi) \leq A_k.$$

If  $\text{Ker}(\varphi) = \{e\}$ , we have a situation that  $s_e \in A_k, s_e \in \text{Img}(\varphi)$  and we want to determine whether or not  $\text{Img}(\varphi) \leq A_k$ . Since  $A_k \cap \text{Img}(\varphi) \neq \emptyset$ , the relationship of  $A_k$  and  $\text{Img}(\varphi)$  is one of the two illustrated below:

Case #1:

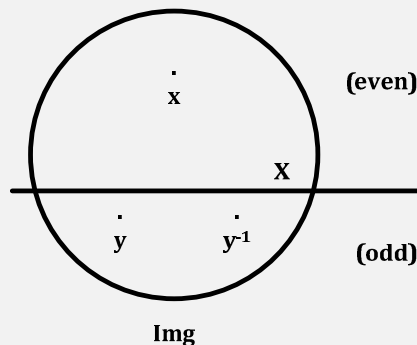


Case #2:



Let's assume it is Case #1,  $\text{Img}(\varphi) \not\leq A_k$ . Let's call  $A_k \cap \text{Img}(\varphi) = X$ . Since  $A_k < S_k$  and  $\text{Img}(\varphi) \leq S_k$ , the intersection,  $X$ , is also a subgroup of  $S_k$ ,  $X < \text{Img}(\varphi) \leq S_k$ . This is based on the fact that intersection of subgroups is also a subgroup.

In fact, we can show that  $X$  is a normal subgroup of  $\text{Img}(\varphi)$ ,  $X \triangleleft \text{Img}(\varphi)$ . Let have  $x, y \in \text{Img}(\varphi)$  and  $x \in X$  but  $y \notin X$ .



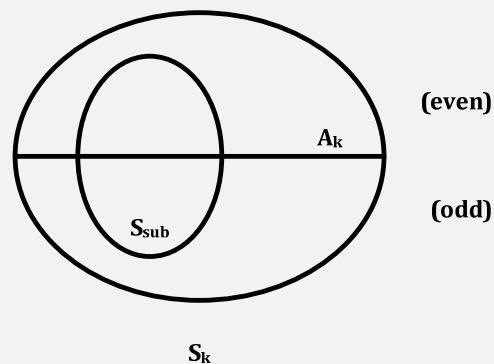
$x$  is an even permutation and  $y$  is an odd permutation.  $y^{-1}$  is also an odd permutation since the inverse of an odd permutation is still odd.  $xyx^{-1}$  is even, because the composition of two odd permutations and an even permutation is even. So we have the following conclusion:

$$y \circ x \circ y^{-1} \in X$$

$$\Rightarrow X \triangleleft \text{Img}(\varphi).$$

On the other hand, Since  $G/\text{Ker}(\varphi) \cong \text{Img}(\varphi)$  and  $\text{Ker}(\varphi) = \{e\}$ , we have  $G \cong \text{Img}(\varphi)$ . According to the problem set,  $G$  is a simple group. Hence,  $\text{Img}(\varphi)$  is also a simple group. By definition, simple groups do not have proper normal subgroups other than the trivial group. In other words,  $X = \{s_e\}$ .

We also have the fact that for any subgroup,  $S_{\text{sub}}$  of  $S_n$ , it contains all even permutations or it contains exactly half even permutations and half odd permutations. It is clear a subgroup may contain all even permutations, such as  $A_k$ . If there is an odd permutation  $s_{\text{odd}}$ , we can construct a map from  $S_{\text{sub}}$  to  $S_{\text{sub}}$ ,  $\rho: s \mapsto s_{\text{odd}} \circ s$ . This map sends all even permutations to an odd permutation, and odd permutations to an even permutation. So these two kinds of permutations need to have exactly the same counts.



Since the even permutation subgroup of  $\text{Img}(\varphi)$  contains only one element,  $s_e$ , we can derive  $|\text{Img}(\varphi)| = 2 = |G|$ . According to the question, however,  $|G| > 2$ . This is a conflict. Case #1 is not true. Therefore, we've shown  $\text{Img}(\varphi) \leq A_k$  for  $\text{Ker}(\varphi) = \{e\}$  as illustrated in Case #2.

In summary, we've proven  $\text{Img}(\varphi) \leq A_k$  regardless of  $\text{Ker}(\varphi) = \{e\}$  or  $\text{Ker}(\varphi) = G$  for simple group  $G$ , with  $|G| > 2$ .

- b.** Use this to show that if  $H < G$ , where  $[G:H] = k$ , then  $|G| \leq k!/2$ .

**Answer:** According to Theorem 16 in the lecture, there is a group homomorphism from  $G$  to  $S_k$ ,  $\phi: G \rightarrow S_k$ , defined as  $g \mapsto \lambda_g$ , where  $\lambda_g(xH) = gxH$  for all  $x \in G$ . Let's call the kernel of this homomorphism  $N$ . We can construct the quotient group  $G/N$  since  $N$  is a normal subgroup of  $G$ . According to the first isomorphism theorem,  $G/N \cong K$ , where  $K \leq S_k$ .

Since  $G$  is a simple group, the only normal subgroups it has are the trivial group,  $\{e\}$ , and itself. If  $N = \{e\}$ , as we've shown in the previous question when  $N = \text{Ker}(\phi) = \{e\}$ , we have:

$$\begin{aligned} G &\cong \text{Img}(\phi) \leq A_k \\ \Rightarrow |G| &\leq |A_k| \\ \Rightarrow |G| &\leq \frac{k!}{2}. \end{aligned}$$

When  $N = G$  it implies that  $g \mapsto \lambda_e$ , where  $\lambda_e(xH) = gxH = xH$  for all  $x \in G$ . In other words, according to the theorem 16,

$$N = \text{Ker}(\phi) = \text{Core}_G(H) = G$$

This is a conflict. Based on the definition of  $\text{Core}_G(H)$ , it is the largest normal subgroup of  $G$  contained in  $H$ . Since  $H$  is a proper subgroup of  $G$ ,  $\text{Core}_G(H)$  has to be a proper subgroup of  $G$  as well.

$$\begin{aligned} H &< G, N \leq H \\ \Rightarrow N &< G. \end{aligned}$$

In summary, if a simple group  $G$  has a proper subgroup  $H$  with index  $k$ , the group homomorphism  $\phi: G \rightarrow S_k$ , defined as  $g \mapsto \lambda_g$ , where  $\lambda_g(xH) = gxH$  for all  $x \in G$ , has a trivial kernel. And the following statement holds:

$$\begin{aligned} G &\cong \text{Img}(\phi) \leq A_k \\ \Rightarrow |G| = |\text{Img}(\phi)| &\leq \frac{k!}{2}. \end{aligned}$$