If G is a group, an **automorphism** of G is an isomorphism from G to G.

1. If G is any group, and a is any element of G, prove that $f(x) = axa^{-1}$ is an automorphism of G. We call this *conjugation* by b.

   Proof. We need to show that f is a bijecton function and satisfy that $f(xy) = f(x)f(y)$ such that x, y are both in G. Let $x, y \in G$ and $f(x) = f(y)$.

$$\begin{aligned} axa^{-1} &= aya^{-1} \\ a^{-1}axa^{-1} &= a^{-1}aya^{-1} \\ xa^{-1} &= ya^{-1} \\ xa^{-1}a &= ya^{-1}a \\ x &= y \end{aligned}$$

   Hence, f is injective. Then, let us prove that for every $y \in G$ there exists x in G such that $f(x) = y$. We have $x = a^{-1}ya$ satisfy the statement. $y = a(a^{-1}ya)a^{-1} = f(x)$ Hence, f is surjective and hence bijective.

   Lastly, we need to show that $f(xy) = f(x)f(y)$ for all $x, y \in G$.

$$\begin{aligned} f(xy) &= a(xy)a^{-1} \\ &= axya^{-1} \\ f(x)f(y) &= axa^{-1}aya^{-1} \\ &= axeya^{-1} \\ &= axya^{-1} \end{aligned}$$

   Hence, f is isomorphism for all $x, y \in G$. Therefore, f is an automorphism of G. ■

2. Since each automorphism of G is a bijective function from G to G, it is a *permutation* of G. Define Aut(G) as the set of all automorphisms of G. Prove Aut(G)$\leq S_G$.

   Proof. First, we need to show that $Aut(G)$ is a nonempty subset of S_G. We can say that $\epsilon \in Aut(G)$ if G is a isomorphism of G. Consider the identity function for G: $\epsilon(x) = x$. If $\epsilon(x) = \epsilon(y)$, then $x = y$. Hence the function is injective. For every y in G, there exists an element $x \in G$ such that $\epsilon(y) = y$. Hence, the function is surjective and therefore bijective. Lastly, we know that $\epsilon(xy) = xy = \epsilon(x)\epsilon(y)$. Therefore, ϵ is a isomorphism from G to G and hence $Aut(G)$ is a nonempty subset of S_G.

   Second, we need to show $Aut(G)$ is closed under composition. Let $f, g \in Aut(G)$, and we need to prove that the operation $f \circ g$ is in $Aut(G)$. That is, it is a automorphisms of G, an isomorphism from G to G. Since both f and g are bijective, their composition will be bijective, which implies $f \circ g(x) \in Aut(G)$ and $Aut(G)$ is closed under composition.

Third, we need to show that the inverse of $Aut(G)$ is in $Aut(G)$. Let $f \in Aut(G)$, then we need to prove f^{-1} in $Aut(G)$, f^{-1} is an isomorphism from G to G. Let $f^{-1}(x) = f^{-1}(y)$ such that $x, y \in G$. Since f is bijective, we have:

$$\begin{aligned} f^{-1}(x) &= f^{-1}(y) \\ f(f^{-1}(x)) &= f(f^{-1}(y)) \\ \epsilon(x) &= \epsilon(y) \\ x &= y \end{aligned}$$

Hence f^{-1} is injective. Now we need to show that for all $y \in G$, there exists $x \in G$ such that $f^{-1}(x) = y$. Since f is surjective, there must exist $x \in G$ such that $f(y) = x$, implying that $y = f^{-1}x$. Hence, f^{-1} is surjective and therefore bijective.

To show that f^{-1} is isomorphism to G, we also need to show that $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Let $a, b \in G$ such that $f^{-1}x = a$ and $f^{-1}y = b$. $f^{-1}(x)f^{-1}(y) = ab$.Since f is an isomorphism, we know that $f(ab) = f(a)f(b) = xy$. Then $f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(x)$. Hence, the inverse of $f \in Aut(G)$ is in G. Therefore, Aut(G) is a subgroup of G.

■

3. We'll prove some basic properties of order. Let $a, b, c \in G$. Show that

   (a) $\text{ord}(a) = \text{ord}(bab^{-1})$

   Proof. Let $ord(a) = x$ such that x is the smallest positive integer that the equation holds.Then $a^x = e$. Need to show that $(bab^{-1})^x = e$.

$$\begin{aligned} (bab^{-1})^x &= (bab^{-1})(bab^{-1})...(bab^{-1}) \\ &= bab^{-1}bab^{-1}...bab^{-1} \\ &= ba(b^{-1}b)ab^{-1}...bab^{-1} \\ &= ba^x b^{-1} \\ &= beb^{-1} \\ &= e \end{aligned}$$

   Next, we need to show that x is the smallest positive integer such that $(bab^{-1})^x = e$. Suppose there exists a positive integer y such that $(bab^{-1})^y = e$ and $y < x$. Then, we can write $a^y = b^{-1}ba^y b^{-1}b = b^{-1}(bab^{-1})^y b = b^{-1}eb = e$, which contradicts the fact that x is the smallest positive integer such that $a^x = e$. Therefore, x is the smallest positive integer such that $(bab^{-1})^x = e$. Therefore, the order of (bab^{-1}) is x, which equals to the order of a. ■

(b) $\text{ord}(a^{-1}) = \text{ord}(a)$

Proof. Let $ord(a) = x$ such that x is the smallest positive integer that the equation holds.Then $a^x = e$. Need to show that $(a^{-1})^x = e$. According to the law of exponents, we know that $(a^{-1})^x = (a^x)^{-1} = e^{-1} = e$.
Next, we need to show that x is the smallest positive integer such that $(a^{-1})^x = e$. Suppose there exists a positive integer y such that $(a^{-1})^y = e$ and $y < x$. Then, we can write $a^y = ((a^{-1})^y)^{-1} = e^{-1} = e$, which contradicts the fact that x is the smallest positive integer such that $a^x = e$. Therefore, x is the smallest positive integer such that $(a^{-1})^x = e$. Therefore, the order of (a^{-1}) is x, which equals to the order of a. ■

4. Now show

(a) $\text{ord}(ab) = \text{ord}(ba)$

Proof. Let $ord(ab) = x$ such that x is the smallest positive integer that the equation holds.Then $(ab)^x = e$. Need to show that $(ba)^x = e$.

$$\begin{aligned} (ab)^x &= (ab)(ab)(ab)...(ab) \\ &= a(ba)(ba)b...(ab)b \\ &= a(ba)^{x-1}b \end{aligned}$$

Since $a(ba)^{x-1}b = (ab)^x = e$. $(ba)^{x-1}$ must be $a^{-1}b^{-1}$, which equals to $(ba)^{-1}$. Since $(ba)^{x-1} = (ba)^{-1}$, we can conclude that $(ba)^x = (ba)^{-1}(ba) = e$.
Next, we need to show that x is the smallest positive integer such that $(ba)^x = e$. Suppose there exists a positive integer y such that $(ba)^y = e$ and $y < x$. Then, we can write $(ab)^y = a(ba)^{y-1}b = a(ba)^y(ba)^{-1}b = a(ba)^{-1}b = aa^{-1}b^{-1}b = e$, which contradicts the fact that x is the smallest positive integer such that $(ab)^x = e$. Therefore, x is the smallest positive integer such that $(ba)^x = e$. Therefore, the order of ba is x, which equals to the order of ab. ■

(b) $\text{ord}(abc) = \text{ord}(cab) = \text{ord}(bca)$
Let $ord(abc) = x$ such that x is the smallest positive integer that the equation holds.Then $(abc)^x = e$. Need to show that $(cab)^x = (bca)^x = e$.

$$\begin{aligned} (abc)^x &= (abc)(abc)(abc)...(abc) \\ &= ab(cab)(cab)...(cab)c \\ &= ab(cab)^{x-1}c \end{aligned}$$

Since $ab(cab)^{x-1}c = (abc)^x = e$, $(cab)^{x-1}$ must equal to $b^{-1}a^{-1}c^{-1} = (cab)^{-1}$. Since $(cab)^{x-1} = (cab)^{-1}$, $(cab)^x = (cab)^{-1}(cab) = e$. Similarly, we can get that $(bca)^x = e$ as well by realizing that $a(bca)^{n-1}bc = e$, $(bca)^{n-1} = (bca)^{-1}$ and $(bca)^x = e$.

Next, we need to show that x is the smallest positive integer such that $(cab)^x = e$. Suppose there exists a positive integer y such that $(cab)^y = e$ and $y < x$. Then, we can write $(abc)^y = ab(cab)^{y-1}c = ab(cab)^{y-1}c = ab(cab)^y(cab)^{-1}c = ab(cab)^{-1}c = e$, which contradicts the fact that x is the smallest positive integer such that $(abc)^x = e$. Therefore, x is the smallest positive integer such that $(cab)^x = e$. Similarly, x is the smallest positive integer such that $(bca)^x = e$.

Therefore, the order of abc is x, which equals to the order of cab and bca.

5. Let $a \in G$, and of finite order. Prove that if a is the *only* element of order k in G, then a is in the center of G.

Proof. To prove that $a \in G$ is in the center of G, we need to show that for all $b \in G$,$ab = ba$. We proved in 3(a) that $\text{ord}(a) = \text{ord}(bab^{-1})$ for all $a, b \in G$. However, we know that a is the only element of order k in G, which implies that $a = bab^{-1}$.

$$\begin{aligned} a &= bab^{-1} \\ ab &= bab^{-1}b \\ ab &= ba \end{aligned}$$

Therefore, a is in the center of G. ■