

1.

We use induction to prove that for a group $G, g \in G$, and two integers a, b ,

$$g^{a+b} = g^a \cdot g^b$$

$\forall g \in G \forall a \in \mathbb{Z} \forall b \in \mathbb{Z}^+ \cup \{0\}$, we have

Base case: $b = 0$

$$g^{a+0} = g^a = g^a \cdot 1 = g^a \cdot g^0$$

Inductive steps: Suppose $g^{a+b} = g^a \cdot g^b$, we have

$$g^{a+(b+1)} = g^{(a+b)+1} = g \cdot g^{(a-1)+(b+1)} = g \cdot g^{a-1} \cdot g^{b+1} = g^a \cdot g^{b+1}.$$

Therefore,

$$\forall g \in G \forall a \in \mathbb{Z} \forall b \in \mathbb{Z}^+ \cup \{0\} : g^{a+b} = g^a \cdot g^b$$

$\forall g \in G \forall a \in \mathbb{Z} \forall b \in \mathbb{Z}^-$. Since $b \in \mathbb{Z}^-$, $-b \in \mathbb{Z}^+$,

$$g^{a+b} = (g^{-1})^{-a-b} \stackrel{(2)}{=} (g^{-1})^{-a} \cdot (g^{-1})^{-b} = g^a \cdot g^b$$

We also use induction to prove that for a group $G, g \in G$, and two integers a, b ,

$$g^{ab} = (g^a)^b$$

$\forall g \in G \forall a \in \mathbb{Z} \forall b \in \mathbb{Z}^+ \cup \{0\}$, we have

Base case: $b = 0$

$$g^{a \cdot 0} = g^0 = 1 = (g^a)^0 = (g^a)^b$$

Inductive steps: Suppose $g^{a \cdot b} = (g^a)^b$, then

$$g^{a \cdot (b+1)} = g^{a \cdot b + a} = g^{a \cdot b} \cdot g^a = (g^a)^b \cdot (g^a)^1 = (g^a)^{b+1}$$

Therefore,

$$\forall g \in G \forall a \in \mathbb{Z} \forall b \in \mathbb{Z}^+ \cup \{0\} : g^{ab} = (g^a)^b$$

$\forall g \in G \forall a \in \mathbb{Z} \forall b \in \mathbb{Z}^-$. Since $b \in \mathbb{Z}^-$, $-b \in \mathbb{Z}^+$,

$$g^{ab} = g^{(-a)(-b)} = (g^{-a})^{(-b)} = ((g^a)^{-1})^{-b} = (g^a)^{(-1)(-b)} = (g^a)^b$$

We also use induction to prove that for a group $G, g, h \in G$ such that $g \cdot h = h \cdot g$ and an integer a ,

$$(gh)^a = g^a \cdot h^a$$

First, we want to prove that for positive a

$$h \cdot g^a = g^a \cdot h \tag{1}$$

also using induction, which will be included along the main proof

$\forall g, h \in G \forall a \in \mathbb{Z}^+ \cup \{0\}$, we have

Base case: $a = 0$

$$h \cdot g^0 = h \cdot 1 = 1 \cdot h = g^0 \cdot h$$

$$(gh)^0 = 1 = 1 \cdot 1 = g^0 \cdot h^0$$

Inductive steps: Suppose $h \cdot g^a = g^a \cdot h$ and $(gh)^a = g^a \cdot h^a$, then

$$h \cdot g^{a+1} = h \cdot g \cdot g^a = h \cdot g^a \cdot g = g^a \cdot h \cdot g = g^a \cdot g \cdot h = g^{a+1} \cdot h, \text{ which prove (1)}$$

$$(gh)^{(a+1)} = (gh) \cdot (gh)^a = g \cdot h \cdot g^a \cdot h^a = g \cdot g^a \cdot h \cdot h^a = g^{a+1} \cdot h^{a+1}$$

$\forall g, h \in G \forall a \in \mathbb{Z}^-$. Since $a \in \mathbb{Z}^-$, $-a \in \mathbb{Z}^+$,

$$(gh)^a = (gh)^{(-1)(-a)} = ((hg)^{-1})^{-a} = (g^{-1} \cdot h^{-1})^{-a} = (g^{-1})^{-a} \cdot (h^{-1})^{-a} = g^a \cdot h^a$$

2.

To prove a and b has the same order, it is sufficient to prove that $a^n = 1 \iff b^n = 1$ where n is finite because:

a. If there don't exist finite n such that $a^n = 1$ then there also don't exist finite m such that $b^m = 1$ or else $a^m = 1$ which is a contradiction

b. If $\text{ord}(a) = n$ then $b^n = 1$ which means that $\text{ord}(b) \leq n$. If there exist $m \in \mathbb{N}$ such that $m < n$ satisfies then $a^m = 1$ which is a contradiction.

1. Suppose g has order n and n is finite, then

$$\begin{aligned} g^n &= 1 \\ \implies g^n \cdot g^{-n} &= 1 \\ \implies (g^{-1})^n &= 1 \end{aligned}$$

If g^{-1} has order n where n is finite then $(g^{-1})^{-1} = g$ has order n as well.

2. Suppose g has order n and n is finite that is $g^n = 1$ then

$$\begin{aligned} h \cdot h^{-1} &= 1 \\ \implies h \cdot g^n \cdot h^{-1} &= 1 \\ \implies (hgh^{-1})^n &= 1 \end{aligned}$$

Suppose hgh^{-1} has order n and n is finite then

$$\begin{aligned} (hgh^{-1})^n &= 1 \\ \implies h \cdot g^n \cdot h^{-1} &= 1 \\ \implies h^{-1} \cdot h \cdot g^n \cdot h^{-1} \cdot h &= h^{-1} \cdot h \\ \implies g^n &= 1 \end{aligned}$$

3. Suppose gh has order n and n is finite, then

$$\begin{aligned} (gh)^n &= 1 \\ \implies (gh)^{-n}(gh)^n &= (gh)^{-n} \\ \implies 1 &= (gh)^{-n} \\ \implies 1 &= h^{-n} \cdot g^{-n} \\ \implies h^n \cdot g^n &= h^n \cdot h^{-n} \cdot g^{-n} \cdot g^n \\ \implies (hg)^n &= 1 \end{aligned}$$

WLOG, hg has order n and n is finite implies gh has order n .

4. If $g = g^{-1}$ then $g^2 = 1$ which means that g must have an order that is less than 2, which means g must have order 1 or 2.

3.

Let g, h be arbitrary elements in group G . Then $g \cdot h$ is also an element in G , which means that

$$\begin{aligned}(gh)^2 &= 1 \\ \implies ghgh &= 1 \\ \implies ghghhg &= hg \\ \implies ghgg &= hg \\ \implies gh &= hg\end{aligned}$$

Consider the dihedral group of a hexagon. Which means that for each rotation R on the hexagon, $R^6 = 1$ and for all reflection r on the hexagon, $r^2 = 1 \implies r^6 = 1$. But dihedral group is not abelian, for example:

Consider the dihefral group of a hexagon.

Let R_i denotes the rotation by angle $i \cdot \frac{2\pi}{6}$ and r_i denotes the reflection in

the line at angle $i \cdot \frac{\pi}{6}$ with respect to a fixed line passing through the center and one vertex of the hexagon. We have:

$$r_1 \cdot R_1 = r_2 \neq R_1 \cdot r_1 = r_0$$

4.

1. If there is $0 \leq a < b < n \in \mathbb{N}$ such that $g^a = g^b$ then $g^{b-a} = 1$ which has $0 < b - a < n$ is a contradiction because g has order n
2. Similarly, if there is $a < b \in \mathbb{Z}$ such that $g^a = g^b$ then $g^{b-a} = 1$, which means that g has order $b - a$ which is a contradiction.
3. From the definition, we have

$$\exists t \in \mathbb{Z} : a = tn + r$$

$$\begin{aligned} g^n &= 1 \\ \implies g^{tn} &= 1 \\ \implies g^{a-r} &= 1 \\ \implies g^a &= g^r \end{aligned}$$

If there is $a < b$ such that $g^a = g^b$ and a, b has different remainder when divided by n then

$$\exists x, y \in \mathbb{Z} : b - a = xn + y$$

where $0 < y < n$

$$\begin{aligned} g^a &= g^b \\ \implies g^{b-a} &= 1 \\ \implies g^{xn+y} &= 1 \\ \implies g^{xn} \cdot g^y &= 1 \\ \implies g^y &= 1 \end{aligned}$$

which is a contradiction because g has order $n > y$. Therefore, the function is injective.

It is obviously well-defined because for each $a, b \in \mathbb{Z}$ such that $a - b$ is divisible by $n : g^a = g^b$.

$\forall a \in \mathbb{Z} : a$ has a remainder when being divided by n , therefore g^a is in the image of the function. Hence $\{g^a \mid a \in \mathbb{Z}\}$ is the image of the function.

4. From part 1 the size of subset $\{g^a \mid a \in \mathbb{Z}\}$ is larger or equal to n because $\{1, g, g^2, \dots, g^{n-1}\} \subset \{g^a \mid a \in \mathbb{Z}\}$. But since $\forall b \in \mathbb{Z} : \exists x, y \in \mathbb{Z} : b = xn + y$ where $0 \leq y < n$ which means that $g^b = g^y$. Since g^y is already an element in the subset, the subset cannot have another element in \mathbb{Z} , hence has size n .

5.

Consider the set $\{g \in G \mid g \neq g^{-1}\}$. Since g and g^{-1} are uniquely determined by each other and if g is in the set then because $g^{-1} \neq (g^{-1})^{-1} = g$, g^{-1} is also in the set. Therefore, the set always has even size.

Since G has even order, the set contains elements that have $g = g^{-1}$ also has even size. But $1 = 1^{-1}$, therefore, the set contains elements that have $g = g^{-1}$ must have more than 1 elements. Hence, there is another element other than 1 satisfies $g = g^{-1}$ which is equivalent to $g^2 = 1$. Therefore, that element has order 2.

6.

Since the operation is already associative, what we need to prove are

1. If $e \cdot a = a$ then $a \cdot e = a = e \cdot a$

2. If $h \cdot g = e$ then $g \cdot h = e = h \cdot g$

Since $h \in G$, there exists t such that $t \cdot h = e$

Because the operation is already operative, if $h \cdot g = e$, then

$$\begin{aligned}h \cdot g &= e \\ \implies h \cdot g \cdot h &= e \cdot h \\ \implies t \cdot h \cdot g \cdot h &= t \cdot h \\ \implies e \cdot g \cdot h &= t \cdot h \\ \implies g \cdot h &= e\end{aligned}$$

which prove 2.

Since $a \in G$, there exists b such that $a \cdot b = b \cdot a = e$

Because the operation is already operative, if $e \cdot a = a$, then

$$\begin{aligned}e \cdot a &= a \\ \implies b \cdot e \cdot a &= b \cdot a \\ \implies b \cdot e \cdot a &= e \\ \implies a \cdot b \cdot e \cdot a &= a \cdot e \\ \implies e \cdot e \cdot a &= a \cdot e \\ \implies e \cdot a &= a \cdot e\end{aligned}$$

which prove 1.