Theorem: If G is a group and $a \in G$, then for all $m, n \in \mathbb{Z}$,

(i) $a^m \cdot a^n = a^{m+n}$ (additive notation: $ma + na = (m+n)a$)

(ii). $(a^m)^n = a^{mn}$ (additive notation: $n(ma) = mna$.

Proof: let's begin with a definition.

Definition: If G is a group, then for each $n \in \mathbb{N}$, a^{-n} is defined to be $(a^{-1})^n \in G$.

Let's prove that $\boxed{\text{for each } n \in \mathbb{N} \cup \{0\},\ a^n \cdot a = a \cdot a^n.}$

For each $n \in \mathbb{N} \cup \{0\}$, let $P(n)$ be the statement $a^n \cdot a = a \cdot a^n$. Clearly $P(n)$ is true for $n=0$ and $n=1$. Let $n \in \mathbb{N}$. Assume $P(n)$ is true. Then $a^n \cdot a = a \cdot a^n$. Then, $(a^n \cdot a) \cdot a = (a \cdot a^n) \cdot a$. By associativity $a^{n+1} \cdot a = a \cdot a^{n+1}$. Hence $P(n+1)$ is true. Therefore, $P(n)$ is true for each $n \in \mathbb{N} \cup \{0\}$.

Now $\boxed{\text{for each } n \in \mathbb{N} \cup \{0\}}$, let $P(n)$ be the statement $\boxed{(a^n)^{-1} = (a^{-1})^n}$. Clearly $P(n)$ is true for $n=0$ ($e^{-1} = e = (a^{-1})^0$) Also, $P(1)$ is true. Now let $n \in \mathbb{N}$. Assume $P(n)$ is true. Then $(a^n)^{-1} = (a^{-1})^n$. Observe that $(a^{n+1})^{-1} = (a^n \cdot a)^{-1} = a^{-1} \cdot (a^n)^{-1}$ $= a^{-1} \cdot (a^{-1})^n = (a^{-1})^1 \cdot (a^{-1})^n = (a^{-1})^n (a^{-1})^1 = (a^{-1})^{n+1}$. Thus $P(n+1)$ is true. Thus $P(n)$ is true for each $n \in \mathbb{N} \cup \{0\}$.

Now we will prove that $\boxed{\text{for each } n \in \mathbb{Z},\ a^{-n} = (a^{-1})^n.}$

By definition $a^{-n} = (a^{-1})^n$ for each $n \in \mathbb{N}$. Since $a^{-0} = a^0 = e = (a^{-1})^0$, the result is true for $n=0$ as well.

Now let $n \in \mathbb{Z}$ be such that $n < 0$. Then $n = -m$ for some $m \in \mathbb{N}$. Note that $a^{-n} = a^{-(-m)} = a^{m} = [(a^{-1})^{-1}]^{m} = (a^{-1})^{-m}$ (by definition) $= (a^{-1})^{n}$. Thus, $a^{-n} = (a^{-1})^{n}$ for $n < 0$.

Therefore, $a^{-n} = (a^{-1})^{n}$ for each $n \in \mathbb{Z}$.

(i) Now, let's prove that for all $m, n \in \mathbb{Z}$, $a^{m} \cdot a^{n} = a^{m+n}$.

Case 1. Suppose $m > 0$ and $n > 0$. Fix m. Let $P(n)$ be the statement $a^{m} \cdot a^{n} = a^{m+n}$. By definition $a^{m+1} = a^{m} \cdot a = a^{m} \cdot a^{1}$.

Thus $P(1)$ is true. Let $n \in \mathbb{N}$. Suppose $P(n)$ is true. Then $a^{m} \cdot a^{n} = a^{m+n}$. Note that $a^{m+n+1} = a^{\overline{m+n}+1} = a^{m+n} \cdot a = (a^{m} \cdot a^{n}) \cdot a = a^{m} \cdot (a^{n} \cdot a) = a^{m} \cdot a^{n+1}$. So, $P(n+1)$ is true. Hence $P(n)$ is true for each $n \in \mathbb{N}$. Thus $a^{m} \cdot a^{n} = a^{m+n}$ for $m, n > 0$.

Case 2. Suppose $m < 0$ and $n < 0$.

Observe that $a^{m} \cdot a^{n} = [(a^{-1})^{-1}]^{m} \cdot [(a^{-1})^{-1}]^{n} = (a^{-1})^{(-m)} \cdot (a^{-1})^{(-n)} = (a^{-1})^{[(-m)+(-n)]} = (a^{-1})^{-(m+n)} = [(a^{-1})^{-1}]^{(m+n)} = a^{m+n}$. Thus, $a^{m} \cdot a^{n} = a^{m+n}$ for $m, n < 0$.

Case 3: $m = 0$ or $n = 0$. Obvious.

Case 4: Suppose $m > 0$ and $n < 0$.

Fix $n (< 0)$. Let $P(m)$ be the statement $a^{m} \cdot a^{n} = a^{m+n}$.

Since $n < 0$, $n = -k$ for some $k \in \mathbb{N}$. Observe that $a \cdot a^{n} = a \cdot a^{-k} = a \cdot (a^{-1})^{k} = a \cdot (a^{k})^{-1} = (a^{-1})^{-1} \cdot (a^{k})^{-1} = (a^{k} \cdot a^{-1})^{-1}$ (note that $\forall\, x, y \in G$, $(xy)^{-1} = y^{-1} \cdot x^{-1}$) $= (a^{k-1} \cdot a \cdot a^{-1})^{-1} = (a^{k-1})^{-1}$ (note that since $k \in \mathbb{N}$, $k-1 \in \mathbb{N} \cup \{0\}$) $= (a^{-1})^{k-1} = a^{-(k-1)} = a^{-k+1} = a^{n+1} = a^{1+n}$. Thus $P(1)$ is true.

Now let $m \in \mathbb{N}$. Suppose $P(m)$ is true. Then $a^m \cdot a^n = a^{m+n}$.
Now if $m+n \geq 0$, then $a^{m+1} \cdot a^n = (a^m \cdot a)\cdot a^n = (a\cdot a^m)\cdot a^n = a\cdot(a^m\cdot a^n) =$
$a \cdot a^{m+n} \overset{\text{case 1.}}{=} a^{1+m+n} = a^{\overline{m+1}+n}$ and if $m+n<0$, then $a^{m+1}\cdot a^n =$
$(a^m\cdot a)\cdot a^n = a\cdot(a^m \cdot a^n) = a\cdot a^{m+n} = a\cdot[(a^{-1})^{-1}]^{m+n} = a\cdot (a^{-1})^{-(m+n)} = (a^{-1})^{-1}\cdot(a^{-1})^{-(m+n)}$
$= (a^{-1})^{-1}\cdot[a^{-(m+n)}]^{-1} = (a^{-(m+n)}\cdot a^{-1})^{-1}$ $(\forall x,y\in G,\ (xy)^{-1} = y^{-1}x^{-1})$ $=$
$[a^{-(m+n)-1}\cdot a\cdot a^{-1}]^{-1} = [a^{-(m+n)-1}]^{-1} = (a^{-1})^{-(m+n)-1} = a^{-[-(m+n)-1]} =$
$a^{(m+n)+1} = a^{\overline{m+1}+n}$. Thus $P(m+1)$ is true.
Therefore, $a^m\cdot a^n = a^{m+n}$ for all $m>0$ and $n<0$.

Case 5: Suppose $m<0$ and $n>0$.

Fix $m\,(<0)$. Let $P(n)$ be the statement $a^m\cdot a^n = a^{m+n}$.
Since $m<0$, $m=-k$ for some $k\in\mathbb{N}$. Observe that $a^m\cdot a =$
$a^{-k}\cdot a = (a^{-1})^k\cdot a = (a^{-1})^k\cdot(a^{-1})^{-1} = (a^k)^{-1}\cdot(a^{-1})^{-1} = (a^{-1}\cdot a^k)^{-1} =$
$(a^{-1}\cdot a^{k-1}\cdot a)^{-1} = (a^{-1} a\cdot a^{k-1})^{-1}$ (note that $k-1\geq 0$) $= (a^{k-1})^{-1} = (a^{-1})^{k-1}$
$= a^{-(k-1)} = a^{-k+1} = a^{m+1}$. Thus, $P(1)$ is true.

Now let $n\in\mathbb{N}$. Assume $P(n)$ is true. Then $a^m\cdot a^n = a^{m+n}$.
Now if $m+n\geq0$, then $a^m\cdot a^{n+1} = a^m\cdot(a^n\cdot a) = (a^m\cdot a^n)\cdot a \overset{\text{case 1}}{=} a^{m+n}\cdot a$
$= a^{m+n+1} = a^{m+\overline{n+1}}$ and if $m+n<0$, then $a^m\cdot a^{n+1} = a^m\cdot(a^n\cdot a) =$
$(a^m\cdot a^n)\cdot a = a^{m+n}\cdot a = [(a^{-1})^{-1}]^{m+n}\cdot(a^{-1})^{-1} = (a^{-1})^{-(m+n)}\cdot(a^{-1})^{-1} =$
$(a^{-(m+n)})^{-1}\cdot(a^{-1})^{-1}$ (note that $m+n<0$ and hence $-(m+n)>0$) $=$
$[a^{-1}\cdot a^{-(m+n)}]^{-1} = [a^{-1}\cdot a^{-(m+n)-1}\cdot a]^{-1} = [a^{-1}\cdot a\cdot a^{-(m+n)-1}]^{-1} = [a^{-(m+n)-1}]^{-1}$
$= (a^{-1})^{-((m+n)+1)} = a^{-(-(m+n+1))} = a^{m+n+1} = a^{m+\overline{n+1}}$. Thus $P(n+1)$ is true.

Therefore $a^m \cdot a^n = a^{m+n}$ for all $m<0$ and $n>0$.

Thus, we proved that for each $m, n \in \mathbb{Z}$, $a^m \cdot a^n = a^{m+n}$.

(ii). Now, let's prove that for all $m, n \in \mathbb{Z}$, $(a^m)^n = a^{mn}$.

If $m=0$, then $(a^m)^n = (a^0)^n = e^n = e = a^0 = a^{0 \cdot n}$. Thus, the result holds for $m=0$.

Now suppose that $m>0$ and $n \in \mathbb{Z}$. For each $m \in \mathbb{N}$, let $P(m)$ be the statement $(a^m)^n = a^{mn}$. Note that $(a^1)^n = a^n = a^{1 \cdot n}$ if $n \geq 0$ and $(a^1)^n = (a)^{-|n|} = (a^{-1})^{|n|} = a^{-|n|} = a^n = a^{1 \cdot n}$.

Hence $P(1)$ is true.

Now let $m \in \mathbb{N}$. Suppose $P(m)$ is true. Then $(a^m)^n = a^{mn}$.

Observe that for each $x, y \in G$, if $xy = yx$ then $xy^n = y^n x$ for each $n \in \mathbb{N}$. Clearly $xy^1 = xy = yx = y^1 x$. Suppose $xy^n = y^n x$ for some $n \in \mathbb{N}$. Note that $(xy^n) \cdot y = (y^n x) \cdot y = y^n (xy) = y^n (yx) = (y^n \cdot y)x = y^{n+1} x$. Thus $xy^{n+1} = y^{n+1} x$. Hence by induction $xy^n = y^n x$ for all $n \in \mathbb{N}$.

As a result, if $xy = yx$, then $(xy)^n = x^n y^n$. Clearly $(xy)^1 = xy = x^1 \cdot y^1$. Suppose $(xy)^n = x^n y^n$. Note that $(xy)^{n+1} = (xy)^n (xy) = (x^n y^n)(yx) = x^n (y^{n+1} x) = x^n (x y^{n+1}) = (x^n \cdot x) y^{n+1} = x^{n+1} y^{n+1}$. Thus, by induction $(xy)^n = x^n y^n$ for each $n \in \mathbb{N}$ provided $xy = yx$.

The above two results hold for each $n \in \mathbb{Z}$. For if $xy = yx$, then $xy^{-1} = y^{-1}x$ and $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$ $(xy = yx \Rightarrow (xy)^{-1} = (yx)^{-1} \Rightarrow y^{-1}x^{-1} = x^{-1}y^{-1})$

For each $n \in \mathbb{N}$, let $P(n)$ be the statement $xy^{-n} = y^{-n}x$.
Since $xy = yx$, $xy^{-1} = y^{-1}x$. So $P(1)$ is true. Suppose $xy^{-n} = y^{-n}x$.
Notice that $(xy^{-n})y^{-1} = (y^{-n} \cdot x) \cdot y^{-1} = y^{-n}(xy^{-1}) = y^{-n}(y^{-1}x) = y^{-n} \cdot y^{-1} \cdot x = y^{-(n+1)}x$. Also, $(xy^{-n}) \cdot y^{-1} = xy^{-n} \cdot y^{-1} = xy^{-(n+1)}$. Thus $xy^{-(n+1)} = y^{-(n+1)}x$.
Thus, by induction $xy^{-n} = y^{-n}x$ for all $n \in \mathbb{N}$.
So, $xy^{n} = y^{n}x$ for all $n \in \mathbb{Z}$.

For each $n \in \mathbb{N}$, let $P(n)$ be the statement $(xy)^{-n} = x^{-n}y^{-n}$.
Since $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$, $P(1)$ is true. Suppose $(xy)^{-n} = x^{-n} \cdot y^{-n}$.
Note that $(xy)^{-(n+1)} = (xy)^{(-n)+(-1)} = (xy)^{-n} \cdot (xy)^{-1} = x^{-n} y^{-n} y^{-1} x^{-1} = x^{-n} \cdot y^{(-n)+(-1)} \cdot x^{-1} = x^{-n} y^{-(n+1)} x^{-1} = x^{-n} \cdot x^{-1} y^{-(n+1)}$ (since $xy = yx$, $x^{-1}y = yx^{-1}$. We now know that if $\alpha\beta = \beta\alpha$, then $\alpha\beta^{-n} = \beta^{-n}\alpha$ for $n \in \mathbb{Z}$) $= x^{-(n+1)} y^{-(n+1)}$. Thus $P(n+1)$ is true. Hence, by induction, $(xy)^{-n} = x^{-n} \cdot y^{-n}$ for all $n \in \mathbb{N}$.

Now, let's prove that $(a^m)^n = a^{mn} \Rightarrow (a^{m+1})^n = a^{(m+1)n}$.
Recall that at the beginning we proved that for $m \in \mathbb{N} \cup \{0\}$, $a^m \cdot a = a \cdot a^m$. That is for $m \in \mathbb{N} \cup \{0\}$ a and a^m are commute.
Notice that $(a^{m+1})^n = (a^m \cdot a)^n = (a^m)^n \cdot a^n = a^{mn} \cdot a^n = a^{mn+n} = a^{n(m+1)} = a^{(m+1)n}$. Hence $P(m+1)$ is true. Thus, for $m > 0$, and $n \in \mathbb{Z}$, $(a^m)^n = a^{mn}$.

Now suppose $m < 0$. Then $m = -k$ for some $k \in \mathbb{N}$. Notice that $(a^m)^n = (a^{-k})^n = [(a^{-1})^k]^n = (a^{-1})^{kn}$ (we just proved that for any $a \in G$, $m \in \mathbb{N}$ and $n \in \mathbb{Z}$, $(a^m)^n = a^{mn}$. So, put $a = a^{-1}$) $= a^{-kn} = a^{(-k)n} = a^{mn}$. This completes the proof of (ii).

Using (i) now you can prove that $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$ is a subgroup of G, where $a \in G$.

FINAL EXAM - 2021

03. (c). Let G be a group of order 2021. Show that G has at least one proper subgroup and that every proper subgroup of G is cyclic.

Solution: Let G be a group of order 2021. Note that $2021 = 43 \times 47$. Clearly $43, 47$ are primes. Since $|G| = 2021 > 1$, there exists $a \in G \setminus \{e\}$. Clearly $|\langle a \rangle| \,\big|\, |G|$. Hence $|\langle a\rangle| \in \{1, 43, 47, 2021\}$.

Since $a \neq e$, $|\langle a \rangle| \neq 1$. Thus $|\langle a \rangle| \in \{43, 47, 2021\}$.

Case 1: Suppose that $|\langle a \rangle| = 43$. Then $\langle a \rangle$ is a proper subgroup of G.

Case 2: Suppose that $|\langle a \rangle| = 47$. Then $\langle a \rangle$ is a proper subgroup of G.

Case 3: Finally suppose that $|\langle a \rangle| = 2021$. Then $G = \langle a \rangle$ and hence G is cyclic. Consider $a^{43} \in G$. Notice that $(a^{43})^{47} = a^{2021} = e$ and $(a^{43})^k \neq e$ for each k such that $1 \leq k \leq 46$. This is because a is a generator of G (what if $(a^{43})^k = e$ for some $1 \leq k \leq 46$?). Thus, $\langle a^{43} \rangle$ is a proper subgroup of order 47.

Similarly $\langle a^{47} \rangle$ is a proper subgroup of order 43.

Hence, in each case, G has at least one proper subgroup.

Now let H be a proper subgroup of G. Let us show (2) that H is cyclic. Since H is a proper subgroup of G, $|H| \neq 1$ and $|H| \neq 2021$. Thus $|H| = 43$ or $|H| = 47$. Since 43 and 47 are primes, and any group of prime order is cyclic, H is cyclic.

Therefore, every proper subgroup of G is cyclic.