§3.5 Cyclic Groups

Shaoyun Yi

MATH 546/701I

University of South Carolina

June 1-2, 2020

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$
- If ϕ, ψ are two group isomorphisms, then so are ϕ^{-1} and $\psi \circ \phi$.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$
- If ϕ, ψ are two group isomorphisms, then so are ϕ^{-1} and $\psi \circ \phi$.
- Several structural properties preserved by group isomorphisms

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$
- If ϕ, ψ are two group isomorphisms, then so are ϕ^{-1} and $\psi \circ \phi$.
- Several structural properties preserved by group isomorphisms
  - If $o(a) = n$ in G_1, then $o(\phi(a)) = n$ in G_2.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$
- If ϕ, ψ are two group isomorphisms, then so are ϕ^{-1} and $\psi \circ \phi$.
- Several structural properties preserved by group isomorphisms
  - If $o(a) = n$ in G_1, then $o(\phi(a)) = n$ in G_2.
  - If G_1 is abelian, then so is G_2.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$
- If ϕ, ψ are two group isomorphisms, then so are ϕ^{-1} and $\psi \circ \phi$.
- Several structural properties preserved by group isomorphisms
  - If $o(a) = n$ in G_1, then $o(\phi(a)) = n$ in G_2.
  - If G_1 is abelian, then so is G_2.
  - If G_1 is cyclic, then so is G_2.

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - well-defined
  - one-to-one and onto
    - Direct proof
    - Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$
    - If ϕ preserves the products, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.
    - If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - respects the two operations: $\phi(a * b) = \phi(a) \cdot \phi(b)$
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$
- If ϕ, ψ are two group isomorphisms, then so are ϕ^{-1} and $\psi \circ \phi$.
- Several structural properties preserved by group isomorphisms
  - If $o(a) = n$ in G_1, then $o(\phi(a)) = n$ in G_2.
  - If G_1 is abelian, then so is G_2.
  - If G_1 is cyclic, then so is G_2.
- $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

First Theorem

Theorem 1

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

- If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

- If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)
- If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)

Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?)

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?) Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$.

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.
• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)
• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?) Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$.

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.
• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)
• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.
$\langle a^m \rangle \subseteq H$:

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?) Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]

$H \subseteq \langle a^m \rangle$:

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?) Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]

$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]

$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)
Write $k = mq + r$ for $q, r \in \mathbf{Z}$ with $0 \leq r < m$.

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?) Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]

$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)

Write $k = mq + r$ for $q, r \in \mathbf{Z}$ with $0 \leq r < m$. *To show* $r = 0$. (Why?)

$$x = a^k$$

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.
• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)
• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.
$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]
$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)
Write $k = mq + r$ for $q, r \in \mathbf{Z}$ with $0 \leq r < m$. *To show* $r = 0$. (Why?)

$$x = a^k = a^{mq+r} = (a^m)^q a^r \Rightarrow a^r \in H \text{ (Why?)} \Rightarrow$$

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]

$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)
Write $k = mq + r$ for $q, r \in \mathbf{Z}$ with $0 \leq r < m$. *To show* $r = 0$. (Why?)

$$x = a^k = a^{mq+r} = (a^m)^q a^r \Rightarrow a^r \in H \text{ (Why?)} \Rightarrow r = 0 \text{ (Why?)}$$

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.

• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)

• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]

$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)
Write $k = mq + r$ for $q, r \in \mathbf{Z}$ with $0 \leq r < m$. *To show* $r = 0$. (Why?)

$$x = a^k = a^{mq+r} = (a^m)^q a^r \Rightarrow a^r \in H \text{ (Why?)} \Rightarrow r = 0 \text{ (Why?)}$$

Thus $x = (a^m)^q \in \langle a^m \rangle$.

First Theorem

Theorem 1

Every subgroup of a cyclic group G is cyclic.

Proof.

Let a be a generator of G. So $G = \langle a \rangle$. Let H be any subgroup of G.
• If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓(Why?)
• If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some n. (Why?)
Since $a^{-n} = (a^n)^{-1}$ must also belong to H, (Why?) we can assume that H contains some power a^k with $k > 0$. Let m be the smallest positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$.
$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$. (Why?) [Proposition 2 (b) in §3.2]
$H \subseteq \langle a^m \rangle$: Let $x \in H$. Then we have $x = a^k$ for some $k \in \mathbf{Z}$. (Why?)
Write $k = mq + r$ for $q, r \in \mathbf{Z}$ with $0 \leq r < m$. *To show* $r = 0$. (Why?)

$$x = a^k = a^{mq+r} = (a^m)^q a^r \Rightarrow a^r \in H \text{ (Why?)} \Rightarrow r = 0 \text{ (Why?)}$$

Thus $x = (a^m)^q \in \langle a^m \rangle$. In conclusion, $H = \langle a^m \rangle$ and so H is cyclic. □

Second Theorem

Theorem 2 (Let G be a cyclic group)

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group.

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by

$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one:

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by

$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one: By Proposition 3 (a) in §3.2, $\phi(m) \neq \phi(k)$ for $m \neq k$.
- onto:

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by
$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one: By Proposition 3 (a) in §3.2, $\phi(m) \neq \phi(k)$ for $m \neq k$.
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by

$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one: By Proposition 3 (a) in §3.2, $\phi(m) \neq \phi(k)$ for $m \neq k$.
- onto: Since $G = \langle a \rangle$.
- respects the two operations: $\phi(m + k) = a^{m+k} = a^m a^k = \phi(m)\phi(k)$.

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by

$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one: By Proposition 3 (a) in §3.2, $\phi(m) \neq \phi(k)$ for $m \neq k$.
- onto: Since $G = \langle a \rangle$.
- respects the two operations: $\phi(m + k) = a^{m+k} = a^m a^k = \phi(m)\phi(k)$.

Thus, ϕ is an isomorphism.

(b) Let $G = \langle a \rangle$ be a finite cyclic group with n elements.

Second Theorem

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by

$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one: By Proposition 3 (a) in §3.2, $\phi(m) \neq \phi(k)$ for $m \neq k$.
- onto: Since $G = \langle a \rangle$.
- respects the two operations: $\phi(m+k) = a^{m+k} = a^m a^k = \phi(m)\phi(k)$.

Thus, ϕ is an isomorphism.

(b) Let $G = \langle a \rangle$ be a finite cyclic group with n elements. Define

$$\phi : \mathbf{Z}_n \to G \text{ by } \phi([m]) = a^m, \text{ for all } [m] \in \mathbf{Z}_n.$$

Theorem 2 (Let G be a cyclic group)

(a) *If G is infinite, then $G \cong \mathbf{Z}$.*

(b) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

(a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define $\phi : \mathbf{Z} \to G$ by

$$\phi(m) = a^m, \text{ for all } m \in \mathbf{Z}.$$

- well-defined: Trivial
- one-to-one: By Proposition 3 (a) in §3.2, $\phi(m) \neq \phi(k)$ for $m \neq k$.
- onto: Since $G = \langle a \rangle$.
- respects the two operations: $\phi(m+k) = a^{m+k} = a^m a^k = \phi(m)\phi(k)$.

Thus, ϕ is an isomorphism.

(b) Let $G = \langle a \rangle$ be a finite cyclic group with n elements. Define

$$\phi : \mathbf{Z}_n \to G \text{ by } \phi([m]) = a^m, \text{ for all } [m] \in \mathbf{Z}_n.$$

Goal: *To show* ϕ is an isomorphism.

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined:

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one:

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with $\uparrow$]
- onto:

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with $\uparrow$]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with $\uparrow$]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) =$$

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with ↑]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) =$$

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with $\uparrow$]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) = a^{m+k}$$

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with ↑]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) = a^{m+k} = a^m a^k$$

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with ↑]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) = a^{m+k} = a^m a^k = \phi([m])\phi([k]).$$

Proof of Thm 2 (b) cont.: *To show* ϕ is an isomorphism

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with $\uparrow$]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) = a^{m+k} = a^m a^k = \phi([m])\phi([k]).$$

Thus, ϕ is an isomorphism.

Corollary 3

Proof of Thm 2 (b) cont.: *To show ϕ is an isomorphism*

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with ↑]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) = a^{m+k} = a^m a^k = \phi([m])\phi([k]).$$

Thus, ϕ is an isomorphism.

Corollary 3

(a) *Any two infinite cyclic groups are isomorphic to each other. (Why?)*

Proof of Thm 2 (b) cont.: *To show ϕ is an isomorphism*

Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$, for all $[m] \in \mathbf{Z}_n$.

- well-defined: If $[k] = [m]$, i.e., $k \equiv m \pmod{n}$, then $a^k = a^m$. (Why?)
- one-to-one: If $\phi([k]) = \phi([m])$, then $[k] = [m]$. (Why?) [Same with $\uparrow$]
- onto: Since $G = \langle a \rangle$.
- respects the two operations:

$$\phi([m] + [k]) = \phi([m + k]) = a^{m+k} = a^m a^k = \phi([m])\phi([k]).$$

Thus, ϕ is an isomorphism.

Corollary 3

(a) *Any two infinite cyclic groups are isomorphic to each other. (Why?)*

(b) *Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.*

The subgroups of $\mathbf{Z}$

Note 1

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$. *(Check it!)*

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$. *(Check it!)*
- $m\mathbf{Z} = n\mathbf{Z}$ *if and only if* $m = \pm n$.

Corollary 4

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$. *(Check it!)*
- $m\mathbf{Z} = n\mathbf{Z}$ *if and only if* $m = \pm n$.

Corollary 4

$m\mathbf{Z} \cong \mathbf{Z}$. *(Why?)* [

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$. *(Check it!)*
- $m\mathbf{Z} = n\mathbf{Z}$ *if and only if* $m = \pm n$.

Corollary 4

$m\mathbf{Z} \cong \mathbf{Z}$. *(Why?)* *[*$m\mathbf{Z}$ *is an infinite cyclic group &*

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$. *(Check it!)*
- $m\mathbf{Z} = n\mathbf{Z}$ *if and only if* $m = \pm n$.

Corollary 4

$m\mathbf{Z} \cong \mathbf{Z}$. *(Why?)* *[m$\mathbf{Z}$ is an infinite cyclic group & Theorem 2 (a).]*

Remark 1

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$*, for* $m \in \mathbf{Z}$*.*
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$*. (Check it!)*
- $m\mathbf{Z} = n\mathbf{Z}$ *if and only if* $m = \pm n$*.*

Corollary 4

$m\mathbf{Z} \cong \mathbf{Z}$. *(Why?)* *[*$m\mathbf{Z}$ *is an infinite cyclic group & Theorem 2 (a).]*

Remark 1

In the case of infinite groups, it is possible to have a proper subgroup that is isomorphic to the entire group.

Question 1

The subgroups of $\mathbf{Z}$

Note 1

- *The subgroups of* $\mathbf{Z}$ *have the form* $m\mathbf{Z} = \langle m \rangle$, *for* $m \in \mathbf{Z}$.
- $m\mathbf{Z} \subseteq n\mathbf{Z}$ *if and only if* $n|m$. *(Check it!)*
- $m\mathbf{Z} = n\mathbf{Z}$ *if and only if* $m = \pm n$.

Corollary 4

$m\mathbf{Z} \cong \mathbf{Z}$. *(Why?)* *[*$m\mathbf{Z}$ *is an infinite cyclic group & Theorem 2 (a).]*

Remark 1

In the case of infinite groups, it is possible to have a proper subgroup that is isomorphic to the entire group.

Question 1

What are all the subgroups of $\mathbf{Z}_n$?

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z}$

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution.

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n) | b$.

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n) | b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n) | b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct.

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n) | b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$:

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?)

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m,n)|b$.
By Theorem 10 in Chapter 1, there are (m,n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m,n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?) $\Rightarrow \langle [m]_n \rangle \subseteq \langle [d]_n \rangle$ (Why?)
$\langle [d]_n \rangle \subseteq \langle [m]_n \rangle$:

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?) $\Rightarrow \langle [m]_n \rangle \subseteq \langle [d]_n \rangle$ (Why?)
$\langle [d]_n \rangle \subseteq \langle [m]_n \rangle$: $d = sm + tn$ for some $s, t \in \mathbf{Z}$. (Why?)

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?) $\Rightarrow \langle [m]_n \rangle \subseteq \langle [d]_n \rangle$ (Why?)
$\langle [d]_n \rangle \subseteq \langle [m]_n \rangle$: $d = sm + tn$ for some $s, t \in \mathbf{Z}$. (Why?) $\Rightarrow [d]_n \in \langle [m]_n \rangle$.
$|\langle [m]_n \rangle| = n/d$:

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?) $\Rightarrow \langle [m]_n \rangle \subseteq \langle [d]_n \rangle$ (Why?)
$\langle [d]_n \rangle \subseteq \langle [m]_n \rangle$: $d = sm + tn$ for some $s, t \in \mathbf{Z}$. (Why?) $\Rightarrow [d]_n \in \langle [m]_n \rangle$.
$|\langle [m]_n \rangle| = n/d$: The order of $[d]_n$ is n/d, and so $[m]_n$ has order n/d. $\square$

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?) $\Rightarrow \langle [m]_n \rangle \subseteq \langle [d]_n \rangle$ (Why?)
$\langle [d]_n \rangle \subseteq \langle [m]_n \rangle$: $d = sm + tn$ for some $s, t \in \mathbf{Z}$. (Why?) $\Rightarrow [d]_n \in \langle [m]_n \rangle$.
$|\langle [m]_n \rangle| = n/d$: The order of $[d]_n$ is n/d, and so $[m]_n$ has order n/d. □

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

The subgroups of $\mathbf{Z}_n$

$[b] = k[m]$ for some $k \in \mathbf{Z} \Leftrightarrow mx \equiv b \pmod{n}$ has a solution. $\Leftrightarrow (m, n)|b$.
By Theorem 10 in Chapter 1, there are (m, n) distinct solutions modulo n.
We also know that every subgroup of $\mathbf{Z}_n$ is cyclic. (Why?)
For each $[k]_n \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k]_n \rangle$ generated by $[k]_n$.

Note 2

It is possible to have $\langle [k]_n \rangle = \langle [l]_n \rangle$ for certain choices of $[k]_n, [l]_n \in \mathbf{Z}_n$, so these subgroups are not all distinct. In $\mathbf{Z}_3$, we have $\langle [1]_3 \rangle = \langle [2]_3 \rangle = \mathbf{Z}_3$

Proposition 1 (In additive notation: $G = \mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

$\langle [m]_n \rangle \subseteq \langle [d]_n \rangle$: $d|m \Rightarrow [m]_n \in \langle [d]_n \rangle$ (Why?) $\Rightarrow \langle [m]_n \rangle \subseteq \langle [d]_n \rangle$ (Why?)
$\langle [d]_n \rangle \subseteq \langle [m]_n \rangle$: $d = sm + tn$ for some $s, t \in \mathbf{Z}$. (Why?) $\Rightarrow [d]_n \in \langle [m]_n \rangle$.
$|\langle [m]_n \rangle| = n/d$: The order of $[d]_n$ is n/d, and so $[m]_n$ has order n/d. □

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.
$d = \gcd(m, n)$: Then $\langle a^m \rangle = \langle a^d \rangle$. And $o(a^m) = |\langle a^m \rangle| = |\langle a^d \rangle| = n/d$.

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n$ *if and only if* $\gcd(k, n) = 1$.

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n$ *if and only if* $\gcd(k, n) = 1$.

(b) *If* H *is any subgroup of* $\mathbf{Z}_n$, *then* $H = \langle [d]_n \rangle$ *for some divisor* d *of* n.

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n$ *if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n$ *if and only if* $\gcd(k, n) = 1$.

(b) *If* H *is any subgroup of* $\mathbf{Z}_n$, *then* $H = \langle [d]_n \rangle$ *for some divisor* d *of* n.

(c) *If* $d_1 | n$ *and* $d_2 | n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ *if and only if* $d_2 | d_1$.

(c)' *If* $d_1 | n$ *and* $d_2 | n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle$

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k,n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \stackrel{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k,n) \stackrel{!}{=} 1$ (Why?) (

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$*.*

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic &

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1$

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q$

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle$

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n$ *if and only if* $\gcd(k, n) = 1$.

(b) *If* H *is any subgroup of* $\mathbf{Z}_n$, *then* $H = \langle [d]_n \rangle$ *for some divisor* d *of* n.

(c) *If* $d_1 | n$ *and* $d_2 | n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ *if and only if* $d_2 | d_1$.

(c)' *If* $d_1 | n$ *and* $d_2 | n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \stackrel{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \stackrel{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle$

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k,n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k,n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k,n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n$

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k,n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k,n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k,n)$.✓

(c)$\Leftarrow$: $d_2|d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = q d_2 + nt$ for some $t \in \mathbf{Z}$,

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = q d_2 + nt$ for some $t \in \mathbf{Z}$, and so $d_2 | d_1$. (Why?)

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2|d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = q d_2 + nt$ for some $t \in \mathbf{Z}$, and so $d_2|d_1$. (Why?)

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(a)

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

(c)' *If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k, n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k, n)$.✓

(c)$\Leftarrow$: $d_2 | d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = q d_2 + nt$ for some $t \in \mathbf{Z}$, and so $d_2 | d_1$. (Why?)

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(a) The element a^k generates G if and only if $\gcd(k, n) = 1$.

(b)

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k,n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k,n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k,n)$.✓

(c)$\Leftarrow$: $d_2|d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv qd_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = qd_2 + nt$ for some $t \in \mathbf{Z}$, and so $d_2|d_1$. (Why?)

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(a) The element a^k generates G if and only if $\gcd(k,n) = 1$.

(b) If H is any subgroup of G, then $H = \langle a^d \rangle$ for some divisor d of n.

(c)

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k,n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k,n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k,n)$.✓

(c)$\Leftarrow$: $d_2|d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = q d_2 + nt$ for some $t \in \mathbf{Z}$, and so $d_2|d_1$. (Why?)

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(a) The element a^k generates G if and only if $\gcd(k,n) = 1$.

(b) If H is any subgroup of G, then $H = \langle a^d \rangle$ for some divisor d of n.

(c) If $d_1|n$ and $d_2|n$, then $\langle a^{d_1} \rangle \subseteq \langle a^{d_2} \rangle$ if and only if $d_2|d_1$.

(c)'

The subgroups of $\mathbf{Z}_n$ cont.

Corollary 5 (In additive notation: $G = \mathbf{Z}_n$)

(a) *The element $[k]_n$ generates $\mathbf{Z}_n$ if and only if* $\gcd(k,n) = 1$.

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

(a) $\langle [k]_n \rangle = \langle [d]_n \rangle \overset{!}{=} \langle [1]_n \rangle \Leftrightarrow d = \gcd(k,n) \overset{!}{=} 1$ (Why?) (see Eg. 15 in §3.2)

(b) Every subgroup of $\mathbf{Z}_n$ is cyclic & $\langle [k]_n \rangle = \langle [d]_n \rangle$ with $d = \gcd(k,n)$.✓

(c)$\Leftarrow$: $d_2|d_1 \Rightarrow d_1 = d_2 q \Rightarrow [d_1]_n \in \langle [d_2]_n \rangle \Rightarrow \langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ (Why?)

(c)$\Rightarrow$: $[d_1]_n \in \langle [d_2]_n \rangle \Rightarrow [d_1]_n = q[d_2]_n \Rightarrow d_1 \equiv q d_2 \pmod{n}$ for $q \in \mathbf{Z}$.
It follows that $d_1 = q d_2 + nt$ for some $t \in \mathbf{Z}$, and so $d_2|d_1$. (Why?)

In multiplicative notation: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(a) The element a^k generates G if and only if $\gcd(k,n) = 1$.

(b) If H is any subgroup of G, then $H = \langle a^d \rangle$ for some divisor d of n.

(c) If $d_1|n$ and $d_2|n$, then $\langle a^{d_1} \rangle \subseteq \langle a^{d_2} \rangle$ if and only if $d_2|d_1$.

(c)' If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle$.

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4 | 24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$.

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$. This means that $4|k$ but $\gcd(\frac{k}{4}, 6) = 1$.

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$. This means that $4|k$ but $\gcd(\frac{k}{4}, 6) = 1$. The possible choices are $k = 4, 20$.

Example 7

Let $G = \mathbf{Z}_{18}$. List all possible choices of $[k]_{18}$ such that $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle$.

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$. This means that $4|k$ but $\gcd(\frac{k}{4}, 6) = 1$. The possible choices are $k = 4, 20$.

Example 7

Let $G = \mathbf{Z}_{18}$. List all possible choices of $[k]_{18}$ such that $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle$.
$4 \nmid 18$, but $\gcd(4, 18) = 2$, so $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle \Leftrightarrow \gcd(k, 18) = 2$. (Why?)

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$. This means that $4|k$ but $\gcd(\frac{k}{4}, 6) = 1$. The possible choices are $k = 4, 20$.

Example 7

Let $G = \mathbf{Z}_{18}$. List all possible choices of $[k]_{18}$ such that $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle$.
$4 \nmid 18$, but $\gcd(4, 18) = 2$, so $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle \Leftrightarrow \gcd(k, 18) = 2$. (Why?)
It follows that $2|k$ but $\gcd(\frac{k}{2}, 9) = 1$.

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$. This means that $4|k$ but $\gcd(\frac{k}{4}, 6) = 1$. The possible choices are $k = 4, 20$.

Example 7

Let $G = \mathbf{Z}_{18}$. List all possible choices of $[k]_{18}$ such that $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle$.
$4 \nmid 18$, but $\gcd(4, 18) = 2$, so $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle \Leftrightarrow \gcd(k, 18) = 2$. (Why?)
It follows that $2|k$ but $\gcd(\frac{k}{2}, 9) = 1$. The possible choices are

$$k = 2, 4, 8, 10, 14, 16.$$

Question 2

Examples

Example 6

Let $G = \mathbf{Z}_{24}$. List all possible choices of $[k]_{24}$ such that $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$.
$4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $\gcd(k, 24) = 4$. This means that $4|k$ but $\gcd(\frac{k}{4}, 6) = 1$. The possible choices are $k = 4, 20$.

Example 7

Let $G = \mathbf{Z}_{18}$. List all possible choices of $[k]_{18}$ such that $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle$.
$4 \nmid 18$, but $\gcd(4, 18) = 2$, so $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle \Leftrightarrow \gcd(k, 18) = 2$. (Why?)
It follows that $2|k$ but $\gcd(\frac{k}{2}, 9) = 1$. The possible choices are

$$k = 2, 4, 8, 10, 14, 16.$$

Question 2

List **all** *the subgroups of* $\mathbf{Z}_{18}$*?*

List **all** the subgroups of $\mathbf{Z}_{18}$

Note 3 (Corollary 5)

- $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, *i.e.*, $[k]_n \in \mathbf{Z}_n^\times$.
- *Every subgroup of* $\mathbf{Z}_n$ *is of the form* $\langle [d]_n \rangle$ *where* $d|n$.
- *If* $d_1|n$ *and* $d_2|n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
- *If* $d_1|n$ *and* $d_2|n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

List **all** the subgroups of $\mathbf{Z}_{18}$

Note 3 (Corollary 5)

- $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, *i.e.*, $[k]_n \in \mathbf{Z}_n^\times$.
- *Every subgroup of* $\mathbf{Z}_n$ *is of the form* $\langle [d]_n \rangle$ *where* $d|n$.
- *If* $d_1|n$ *and* $d_2|n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
- *If* $d_1|n$ *and* $d_2|n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

So, the subgroups of $\mathbf{Z}_n$ are in one to one correspondence with the divisors of n.

List **all** the subgroups of $\mathbf{Z}_{18}$

Note 3 (Corollary 5)

- $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k,n) = 1$, *i.e.*, $[k]_n \in \mathbf{Z}_n^\times$.
- *Every subgroup of* $\mathbf{Z}_n$ *is of the form* $\langle [d]_n \rangle$ *where* $d|n$.
- *If* $d_1|n$ *and* $d_2|n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
- *If* $d_1|n$ *and* $d_2|n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

So, the subgroups of $\mathbf{Z}_n$ are in one to one correspondence with the divisors of n.
The divisors of 18 are: 1, 2, 3, 6, 9, 18. So the subgroups of $\mathbf{Z}_{18}$ are:

List **all** the subgroups of $\mathbf{Z}_{18}$

Note 3 (Corollary 5)

- $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k,n) = 1$, *i.e.*, $[k]_n \in \mathbf{Z}_n^\times$.
- *Every subgroup of $\mathbf{Z}_n$ is of the form $\langle [d]_n \rangle$ where $d|n$.*
- *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.*
- *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

So, the subgroups of $\mathbf{Z}_n$ are in one to one correspondence with the divisors of n. The divisors of 18 are: 1, 2, 3, 6, 9, 18. So the subgroups of $\mathbf{Z}_{18}$ are:

$[d]_{18}$	$\langle [d]_{18} \rangle$	$\lvert\langle [d]_{18} \rangle\rvert$
$[1]$	$\mathbf{Z}_{18}$	18
$[2]$	$\{[0],[2],[4],[6],[8],[10],[12],[14],[16]\}$	9
$[3]$	$\{[0],[3],[6],[9],[12],[15]\}$	6
$[6]$	$\{[0],[6],[12]\}$	3
$[9]$	$\{[0],[9]\}$	2
$[18]$	$\{[0]\}$	1

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular,

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top,

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom,

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.
$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$, $i = 0, 1, 2$ and $j = 0, 1$.

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.
$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$, $i = 0, 1, 2$ and $j = 0, 1$.
Each of these divisors generates a subgroup.

Note:

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.
$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$, $i = 0, 1, 2$ and $j = 0, 1$.
Each of these divisors generates a subgroup.

Note: $1\mathbf{Z}_{20} = \langle [1]_{20} \rangle = \mathbf{Z}_{20}$ (entire group) and

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.
$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$, $i = 0, 1, 2$ and $j = 0, 1$.
Each of these divisors generates a subgroup.

Note: $1\mathbf{Z}_{20} = \langle [1]_{20} \rangle = \mathbf{Z}_{20}$ (entire group) and $20\mathbf{Z}_{20} = \langle [0]_{20} \rangle = \{[0]_{20}\}$.

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.
$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$, $i = 0, 1, 2$ and $j = 0, 1$.
Each of these divisors generates a subgroup.

Note: $1\mathbf{Z}_{20} = \langle [1]_{20} \rangle = \mathbf{Z}_{20}$ (entire group) and $20\mathbf{Z}_{20} = \langle [0]_{20} \rangle = \{[0]_{20}\}$.
Corollary 5 (c): If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.

Subgroup diagram

Notation: $m\mathbf{Z}_n = \langle [m]_n \rangle$ consisting of all multiples of $[m]_n$ in $\mathbf{Z}_n$.

Definition 8

For small n, we can easily give a diagram showing all subgroups of $\mathbf{Z}_n$ and the inclusion relations between them. This is called a **subgroup diagram**.

In particular, larger subgroups on top, smaller subgroups on the bottom, a line connecting two subgroups indicates that the subgroup on the bottom is contained in the subgroup on the top.

Example 9 (The subgroup diagram of $\mathbf{Z}_{20}$)

The subgroups are obtained from the divisors of 20: 1, 2, 4, 5, 10, 20.
$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$, $i = 0, 1, 2$ and $j = 0, 1$.
Each of these divisors generates a subgroup.

Note: $1\mathbf{Z}_{20} = \langle [1]_{20} \rangle = \mathbf{Z}_{20}$ (entire group) and $20\mathbf{Z}_{20} = \langle [0]_{20} \rangle = \{[0]_{20}\}$.
Corollary 5 (c): If $d_1 | n$ and $d_2 | n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.
That is, smaller divisors of n correspond to larger subgroups.

Example 9 cont.: The subgroup diagram of $\mathbf{Z}_{20}$

Example 9 cont.: The subgroup diagram of $\mathbf{Z}_{20}$

$$\begin{tikzcd}[arrows=-]
 & & \mathbf{Z}_{20} = 1\mathbf{Z}_{20} \arrow[dl] \arrow[dr] & \\
 & 2\mathbf{Z}_{20} \arrow[dl] \arrow[dr] & & 5\mathbf{Z}_{20} \arrow[dl] \\
4\mathbf{Z}_{20} \arrow[dr] & & 10\mathbf{Z}_{20} \arrow[dl] & \\
 & 20\mathbf{Z}_{20} = \langle [0]_{20} \rangle = \{[0]_{20}\} & &
\end{tikzcd}$$

Example: The subgroup diagram of $\mathbf{Z}_{27}$

Example: The subgroup diagram of $\mathbf{Z}_{27}$

$27 = 3^3$: Think about any divisor $d = 3^i$, $i = 0, 1, 2, 3$.

Example: The subgroup diagram of $\mathbf{Z}_{27}$

$27 = 3^3$: Think about any divisor $d = 3^i$, $i = 0, 1, 2, 3$.

$$\begin{tikzcd}
\mathbf{Z}_{27} \arrow[d, dash] \\
3\mathbf{Z}_{27} \arrow[d, dash] \\
9\mathbf{Z}_{27} \arrow[d, dash] \\
\langle [0]_{27} \rangle = \{[0]_{27}\}
\end{tikzcd}$$

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.
- The operation is componentwise multiplication:

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.
- The operation is componentwise multiplication:
$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.
- The operation is componentwise multiplication:
$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$
- The order of an element is the least common multiple of the orders of each component.

Theorem 11

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.
- The operation is componentwise multiplication:

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

- The order of an element is the least common multiple of the orders of each component.

Theorem 11

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}, \text{ where } p_1 < p_2 < \ldots < p_m.$$

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.
- The operation is componentwise multiplication:
$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$
- The order of an element is the least common multiple of the orders of each component.

Theorem 11

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then
$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}, \text{ where } p_1 < p_2 < \ldots < p_m.$$

RHS: The element $([1], [1], \ldots, [1])$ has order n. (Why?) &

Direct product of cyclic groups

Recall that we introduced the direct product of two groups in §3.3. In fact, this definition can be extended to the direct product of n groups. (How?)

Definition 10

The direct product $G_1 \times \cdots \times G_n$ of n groups $G_1, \ldots, G_n$ is defined as follows:

- The elements are n-tuples $(g_1, \ldots, g_n)$, where $g_i \in G_i$ for each i.
- The operation is componentwise multiplication:

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

- The order of an element is the least common multiple of the orders of each component.

Theorem 11

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}, \text{ where } p_1 < p_2 < \ldots < p_m.$$

RHS: The element $([1], [1], \ldots, [1])$ has order n. (Why?) & Thm 2 (b) $\square$

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \le n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a, n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)
Since an isomorphism preserves generators.

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)
Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n.

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)
Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\operatorname{lcm}[o(g_1), \ldots, o(g_m)] = n$.

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n)=1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \textit{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)
Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\mathrm{lcm}[o(g_1), \ldots, o(g_m)] = n$.
It implies that $o(g_i) = p_i^{\alpha_i}$ for each i. (Why?)

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \le n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier) Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\mathrm{lcm}[o(g_1), \ldots, o(g_m)] = n$. It implies that $o(g_i) = p_i^{\alpha_i}$ for each i. (Why?) Thus g_i is a generator in $\mathbf{Z}_{p_i^{\alpha_i}}$ for each i.

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a, n) = 1 \text{ and } 0 < a \le n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier) Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\mathrm{lcm}[o(g_1), \ldots, o(g_m)] = n$. It implies that $o(g_i) = p_i^{\alpha_i}$ for each i. (Why?) Thus g_i is a generator in $\mathbf{Z}_{p_i{}^{\alpha_i}}$ for each i. The total number of possible generators is equal to the product of the number of generators in each component.

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right), \textit{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)
Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\operatorname{lcm}[o(g_1), \ldots, o(g_m)] = n$. It implies that $o(g_i) = p_i^{\alpha_i}$ for each i. (Why?) Thus g_i is a generator in $\mathbf{Z}_{p_i{}^{\alpha_i}}$ for each i. The total number of possible generators is equal to the product of the number of generators in each component.
For any prime p, the elements that are *not* generators are the multiples of p in $\mathbf{Z}_{p^\alpha}$, (Why?)

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right), \textit{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier)
Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\operatorname{lcm}[o(g_1), \ldots, o(g_m)] = n$.
It implies that $o(g_i) = p_i^{\alpha_i}$ for each i. (Why?) Thus g_i is a generator in $\mathbf{Z}_{{p_i}^{\alpha_i}}$ for each i. The total number of possible generators is equal to the product of the number of generators in each component.
For any prime p, the elements that are *not* generators are the multiples of p in $\mathbf{Z}_{p^\alpha}$, (Why?) and there are $p^{\alpha-1}$ such multiples in $\mathbf{Z}_{p^\alpha}$. (Why?)

Revisit Euler's totient function $\varphi(n)$, for $n \in \mathbf{Z}^+$

$\varphi(n) := \#\{a \mid (a,n)=1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| = \#$ of generators of $\mathbf{Z}_n$

Corollary 12 (Proposition 8 in Chapter 1)

Let $n \in \mathbf{Z}^+$ which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right), \text{ where } p_1 < p_2 < \ldots < p_m.$$

Use $\mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \cong \mathbf{Z}_n$ to count the generators of $\mathbf{Z}_n$. (Easier) Since an isomorphism preserves generators. An element g of this direct product is a generator $\Leftrightarrow$ it has order n. So $\mathrm{lcm}[o(g_1), \ldots, o(g_m)] = n$. It implies that $o(g_i) = p_i^{\alpha_i}$ for each i. (Why?) Thus g_i is a generator in $\mathbf{Z}_{p_i^{\alpha_i}}$ for each i. The total number of possible generators is equal to the product of the number of generators in each component.

For any prime p, the elements that are *not* generators are the multiples of p in $\mathbf{Z}_{p^\alpha}$, (Why?) and there are $p^{\alpha-1}$ such multiples in $\mathbf{Z}_{p^\alpha}$. (Why?) Thus

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right).$$

Examples

Lemma 13

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$.

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$?

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

By Theorem 11, we have $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$.

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

By Theorem 11, we have $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. By Lemma 13, we then have $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$.

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

By Theorem 11, we have $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. By Lemma 13, we then have $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is easy to see that $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. (What is ϕ?)

Example 15 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$?

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

By Theorem 11, we have $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. By Lemma 13, we then have $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is easy to see that $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. (What is ϕ?)

Example 15 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$? No!)

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

By Theorem 11, we have $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. By Lemma 13, we then have $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is easy to see that $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. (What is ϕ?)

Example 15 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$? No!)

Similarly, $\mathbf{Z}_4 \times \mathbf{Z}_{15} \cong \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ and $\mathbf{Z}_6 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_5$.

Examples

Lemma 13

If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$. (What is ϕ?)

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism. (Check it!)

Example 14 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$? Yes!)

By Theorem 11, we have $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. By Lemma 13, we then have $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is easy to see that $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. (What is ϕ?)

Example 15 (Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$? No!)

Similarly, $\mathbf{Z}_4 \times \mathbf{Z}_{15} \cong \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ and $\mathbf{Z}_6 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_5$. The first has an element of order 4, while the second has none.

Exponent of group G

If G is a finite group, then each element of G must have finite order.

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Since $o(a)$ is a divisor of $|G|$ for any $a \in G$, and so N is a divisor of $|G|$.

Definition 16

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Since $o(a)$ is a divisor of $|G|$ for any $a \in G$, and so N is a divisor of $|G|$.

Definition 16

Let G be a group. If there exists a $N \in \mathbf{Z}^+$ such that $a^N = e$ for all $a \in G$, then the smallest such positive integer is called the **exponent** of G.

Example 17

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Since $o(a)$ is a divisor of $|G|$ for any $a \in G$, and so N is a divisor of $|G|$.

Definition 16

Let G be a group. If there exists a $N \in \mathbf{Z}^+$ such that $a^N = e$ for all $a \in G$, then the smallest such positive integer is called the **exponent** of G.

Example 17

The exponent of any finite group is the least common multiple of the orders of its elements.

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Since $o(a)$ is a divisor of $|G|$ for any $a \in G$, and so N is a divisor of $|G|$.

Definition 16

Let G be a group. If there exists a $N \in \mathbf{Z}^+$ such that $a^N = e$ for all $a \in G$, then the smallest such positive integer is called the **exponent** of G.

Example 17

The exponent of any finite group is the least common multiple of the orders of its elements. Thus the exponent of S_3 is 6. (Why?)

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Since $o(a)$ is a divisor of $|G|$ for any $a \in G$, and so N is a divisor of $|G|$.

Definition 16

Let G be a group. If there exists a $N \in \mathbf{Z}^+$ such that $a^N = e$ for all $a \in G$, then the smallest such positive integer is called the **exponent** of G.

Example 17

The exponent of any finite group is the least common multiple of the orders of its elements. Thus the exponent of S_3 is 6. (Why?)
The exponent of $\mathbf{Z}_2 \times \mathbf{Z}_2$ is 2. (Why?)

Exponent of group G

If G is a finite group, then each element of G must have finite order.
If N is the least common multiple of the integers $o(a)$, for all $a \in G$, then

$$a^N = e \text{ for all } a \in G.$$

Since $o(a)$ is a divisor of $|G|$ for any $a \in G$, and so N is a divisor of $|G|$.

Definition 16

Let G be a group. If there exists a $N \in \mathbf{Z}^+$ such that $a^N = e$ for all $a \in G$, then the smallest such positive integer is called the **exponent** of G.

Example 17

The exponent of any finite group is the least common multiple of the orders of its elements. Thus the exponent of S_3 is 6. (Why?)
The exponent of $\mathbf{Z}_2 \times \mathbf{Z}_2$ is 2. (Why?)
The exponent of $\mathbf{Z}_2 \times \mathbf{Z}_3$ is 6. (Why?)

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?)

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand,

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k | mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?)

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} =$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m =$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m =$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k | mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} =$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

A similar argument shows that $m|k$,

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

A similar argument shows that $m|k$, and then $mn|k$ (Why?).

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

A similar argument shows that $m|k$, and then $mn|k$ (Why?). So $k = mn$.

Proposition 2 (Let G be a finite abelian group.)

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

A similar argument shows that $m|k$, and then $mn|k$ (Why?). So $k = mn$.

Proposition 2 (Let G be a finite abelian group.)

(a) *The exponent of G is equal to the order of any element of G of largest order.*

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

A similar argument shows that $m|k$, and then $mn|k$ (Why?). So $k = mn$.

Proposition 2 (Let G be a finite abelian group.)

(a) *The exponent of G is equal to the order of any element of G of largest order.*

(b) *The group G is cyclic if and only if its exponent is equal to its order.*

Characterize cyclic groups among all finite abelian groups

Lemma 18 (Question (12) in Homework 3)

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$. Then $(ab)^{mn} = e$. (Why?) Say $o(ab) = k$, then $k|mn$. On the other hand, $(ab)^k = e \Rightarrow a^k = b^{-k}$. (Why?) Therefore

$$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e \Rightarrow n|km \Rightarrow n|k \text{ (Why?)}$$

A similar argument shows that $m|k$, and then $mn|k$ (Why?). So $k = mn$.

Proposition 2 (Let G be a finite abelian group.)

(a) *The exponent of G is equal to the order of any element of G of largest order.*

(b) *The group G is cyclic if and only if its exponent is equal to its order.*

Using this concept of the "**exponent**" of a group, we just characterize cyclic groups among all finite abelian groups in Proposition 2 (b).

Proof of Proposition 2

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G.

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G.
Proof by contradiction:

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$.

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a)$ =the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?) Then $o(a^{p^{\alpha}}) = n$ and $o(b^m) = p^{\beta}$,

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G.
Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^\alpha n$ and $o(b) = p^\beta m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)
Then $o(a^{p^\alpha}) = n$ and $o(b^m) = p^\beta$, so these orders are relatively prime.

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^\alpha n$ and $o(b) = p^\beta m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?) Then $o(a^{p^\alpha}) = n$ and $o(b^m) = p^\beta$, so these orders are relatively prime. It follows from Lemma 18 that $o(a^{p^\alpha} b^m) = np^\beta$

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G.
Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)
Then $o(a^{p^{\alpha}}) = n$ and $o(b^m) = p^{\beta}$, so these orders are relatively prime.
It follows from Lemma 18 that $o(a^{p^{\alpha}} b^m) = np^{\beta} > o(a)$: contradiction.

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^\alpha n$ and $o(b) = p^\beta m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?) Then $o(a^{p^\alpha}) = n$ and $o(b^m) = p^\beta$, so these orders are relatively prime. It follows from Lemma 18 that $o(a^{p^\alpha} b^m) = np^\beta > o(a)$: contradiction. Thus $o(b) | o(a)$ for all $b \in G$,

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?) Then $o(a^{p^{\alpha}}) = n$ and $o(b^m) = p^{\beta}$, so these orders are relatively prime. It follows from Lemma 18 that $o(a^{p^{\alpha}} b^m) = np^{\beta} > o(a)$: contradiction. Thus $o(b)|o(a)$ for all $b \in G$, and $o(a)$ is therefore the exponent of G.

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G.
Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)
Then $o(a^{p^{\alpha}}) = n$ and $o(b^{m}) = p^{\beta}$, so these orders are relatively prime.
It follows from Lemma 18 that $o(a^{p^{\alpha}} b^{m}) = np^{\beta} > o(a)$: contradiction.
Thus $o(b) | o(a)$ for all $b \in G$, and $o(a)$ is therefore the exponent of G.

(b) Part (b) follows immediately from part (a). (Why?)

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a) =$the exponent of G.
Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)
Then $o(a^{p^{\alpha}}) = n$ and $o(b^m) = p^{\beta}$, so these orders are relatively prime.
It follows from Lemma 18 that $o(a^{p^{\alpha}} b^m) = np^{\beta} > o(a)$: contradiction.
Thus $o(b)|o(a)$ for all $b \in G$, and $o(a)$ is therefore the exponent of G.

(b) Part (b) follows immediately from part (a). (Why?)

G is cyclic if and only if there exists an element of order $|G|$.

Question 3

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a)$ =the exponent of G. Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?) Then $o(a^{p^{\alpha}}) = n$ and $o(b^m) = p^{\beta}$, so these orders are relatively prime. It follows from Lemma 18 that $o(a^{p^{\alpha}} b^m) = np^{\beta} > o(a)$: contradiction. Thus $o(b)|o(a)$ for all $b \in G$, and $o(a)$ is therefore the exponent of G.

(b) Part (b) follows immediately from part (a). (Why?)

G is cyclic if and only if there exists an element of order $|G|$.

Question 3

When is $\mathbf{Z}_n^{\times}$ *cyclic?*

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a)$ =the exponent of G.
Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^{\alpha} n$ and $o(b) = p^{\beta} m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)
Then $o(a^{p^{\alpha}}) = n$ and $o(b^m) = p^{\beta}$, so these orders are relatively prime.
It follows from Lemma 18 that $o(a^{p^{\alpha}} b^m) = np^{\beta} > o(a)$: contradiction.
Thus $o(b) | o(a)$ for all $b \in G$, and $o(a)$ is therefore the exponent of G.

(b) Part (b) follows immediately from part (a). (Why?)

G is cyclic if and only if there exists an element of order $|G|$.

Question 3

When is $\mathbf{Z}_n^{\times}$ *cyclic?*

Theorem 19 (The Primitive Root Theorem)

$\mathbf{Z}_n^{\times}$ *is cyclic if and only if* $n = 1, 2, 4, p^k$ *or* $2p^k$ *where* p *is any odd prime.*

Proof of Proposition 2

(a) Assume $o(a)$ has the largest order. *To show* $o(a)$ =the exponent of G.
Proof by contradiction: Let $b \in G$ and suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p with $o(a) = p^\alpha n$ and $o(b) = p^\beta m$, where $(p, n) = (p, m) = 1$ and $\beta > \alpha \geq 0$. (Why?)
Then $o(a^{p^\alpha}) = n$ and $o(b^m) = p^\beta$, so these orders are relatively prime.
It follows from Lemma 18 that $o(a^{p^\alpha} b^m) = np^\beta > o(a)$: contradiction.
Thus $o(b)|o(a)$ for all $b \in G$, and $o(a)$ is therefore the exponent of G.

(b) Part (b) follows immediately from part (a). (Why?)

G is cyclic if and only if there exists an element of order $|G|$.

Question 3

When is $\mathbf{Z}_n^\times$ *cyclic?*

Theorem 19 (The Primitive Root Theorem)

$\mathbf{Z}_n^\times$ *is cyclic if and only if* $n = 1, 2, 4, p^k$ *or* $2p^k$ *where* p *is any odd prime.*

However, we won't prove or use this theorem in this course.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$\mathbf{Z}_{15}^{\times} = \{[1], [2], [4], [7], [8], [11], [13], [14]\} =$

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \{\pm[1], \pm[2], \pm[4], \pm[7]\}.$$

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \{\pm[1], \pm[2], \pm[4], \pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or*

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \{\pm[1], \pm[2], \pm[4], \pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e.,*

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \{\pm[1], \pm[2], \pm[4], \pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If* $o([2]) = 8$, *then it means that the group is cyclic.*
- *If* $o([2]) \neq 8$, *then we need to try other elements, until we either find one that has order* 8, *or exhaust all the possible elements and show that neither one of them has order* 8, *i.e., the group is not cyclic.*

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1],$

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) [

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle[2]\rangle]$

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) [$\because$ $[4],[8] \in \langle [2] \rangle$]

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$,

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4], [8]$. (Why?) $[\because [4],[8] \in \langle [2] \rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle [2] \rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$),

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) [$\because$ $[4],[8] \in \langle [2] \rangle$]

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle [2] \rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

(v) $[13] = -[2], [13]^4 = ([-2])^4 = [16] = [1]$,

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle[2]\rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

(v) $[13] = -[2], [13]^4 = ([-2])^4 = [16] = [1]$, so $o([13]) \leq 4 \because$

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle [2] \rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

(v) $[13] = -[2], [13]^4 = ([-2])^4 = [16] = [1]$, so $o([13]) \leq 4 \because o([13]) | 4$.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle[2]\rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

(v) $[13] = -[2], [13]^4 = ([-2])^4 = [16] = [1]$, so $o([13]) \leq 4 \because o([13])|4$.

(vi) $[14] = [-1], [14]^2 = [1]$,

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle [2] \rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

(v) $[13] = -[2], [13]^4 = ([-2])^4 = [16] = [1]$, so $o([13]) \leq 4 \because o([13]) | 4$.

(vi) $[14] = [-1], [14]^2 = [1]$, so $o([14]) = 2$.

Example: $\mathbf{Z}_{15}^{\times}$ is not cyclic.

$$\mathbf{Z}_{15}^{\times} = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \{\pm[1],\pm[2],\pm[4],\pm[7]\}.$$

Since $|\mathbf{Z}_{15}^{\times}| = 8$, we need to check if there is an element of order 8 or not.

Note 4

- *If $o([2]) = 8$, then it means that the group is cyclic.*
- *If $o([2]) \neq 8$, then we need to try other elements, until we either find one that has order 8, or exhaust all the possible elements and show that neither one of them has order 8, i.e., the group is not cyclic.*

(i) $[2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, so $o([2]) = 4$.

(ii) There is no need to try $[4],[8]$. (Why?) $[\because [4],[8] \in \langle [2] \rangle]$

(iii) $[7]^2 = [49] = [4], [7]^3 = [28] = [13], [7]^4 = [91] = [1]$, so $o([7]) = 4$.

(iv) $[11]^2 = [121] = [1]$ (or $[11]^2 = ([-4])^2 = [16] = [1]$), so $o([11]) = 2$.

(v) $[13] = -[2], [13]^4 = ([-2])^4 = [16] = [1]$, so $o([13]) \leq 4 \because o([13]) | 4$.

(vi) $[14] = [-1], [14]^2 = [1]$, so $o([14]) = 2$.

In conclusion, there is no element of order 8, thus the group is not cyclic.

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6.$

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)
  (b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1],$

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) •

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) $\bullet$ $[4] \in \langle [2] \rangle$ & $\bullet$

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$,

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$:

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$,

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)

(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:

(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.

(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.

(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$, so $o([3]) = 6$. (Why?)

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)
(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:
(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.
(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.
(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$, so $o([3]) = 6$. (Why?)
Therefore $\mathbf{Z}_{14}^\times$ is cyclic (and $[3]_{14}$ is a generator).

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)
   (b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:
   (i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.
   (ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.
   (iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

   Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$, so $o([3]) = 6$. (Why?)
   Therefore $\mathbf{Z}_{14}^\times$ is cyclic (and $[3]_{14}$ is a generator).

V. By II. (a), we conclude that $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$.

Remark 2

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)
   (b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:
   (i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.
   (ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.
   (iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

   Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$, so $o([3]) = 6$. (Why?)
   Therefore $\mathbf{Z}_{14}^\times$ is cyclic (and $[3]_{14}$ is a generator).

V. By II. (a), we conclude that $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$.

Remark 2

$\mathbf{Z}_7^\times$ and $\mathbf{Z}_{14}^\times$ are both cyclic with order 6.

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)
(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:
(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.
(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.
(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$, so $o([3]) = 6$. (Why?)
Therefore $\mathbf{Z}_{14}^\times$ is cyclic (and $[3]_{14}$ is a generator).

V. By II. (a), we conclude that $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$.

Remark 2

$\mathbf{Z}_7^\times$ and $\mathbf{Z}_{14}^\times$ are both cyclic with order 6. They are both isomorphic to $\mathbf{Z}_6$,

Example: $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we can list the elements of each group.

$$\mathbf{Z}_7^\times = \{[1],[2],[3],[4],[5],[6]\} \qquad \mathbf{Z}_{14}^\times = \{[1],[3],[5],[9],[11],[13]\}$$

II. (a) If both of them are cyclic, then they are isomorphic. (Why?)
(b) If one is cyclic and the other is not, then they are not isomorphic.

III. Check $\mathbf{Z}_7^\times$:
(i) $[2]^2 = [4], [2]^3 = [1]$, so $o([2]) = 3$.
(ii) $o([4]) = 3$. (Why?) • $[4] \in \langle [2] \rangle$ & • Lagrange's Theorem.
(iii) $[3]^2 = [9] = [2], [3]^3 = [6]$, so $o([3]) = 6$. (Why?) [Lagrange's Thm]

Therefore $\mathbf{Z}_7^\times$ is cyclic (and $[3]_7$ is a generator).

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9], [3]^3 = [27] = [13]$, so $o([3]) = 6$. (Why?)
Therefore $\mathbf{Z}_{14}^\times$ is cyclic (and $[3]_{14}$ is a generator).

V. By II. (a), we conclude that $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$.

Remark 2

$\mathbf{Z}_7^\times$ and $\mathbf{Z}_{14}^\times$ are both cyclic with order 6. They are both isomorphic to $\mathbf{Z}_6$, and therefore they are isomorphic to each other.