§3.5 Cyclic Groups

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

Review

- $(G_1, *) \cong (G_2, \cdot)$: A group isomorphism $\phi : G_1 \to G_2$ satisfies
  - i) well-defined
  - ii) one-to-one and onto
    - 1) Direct proof
    - 2) Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}$, $\phi\phi^{-1} = 1_{G_2}$
    - 3) 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 $x \in G_1$.
    - 4) If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.
  - iii) 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 $n \in \mathbf{Z}$.
  - $n = 0$: $\phi(e_1) = e_2$ $\rightsquigarrow$ preserve the identity
  - $n = -1$: $\phi(a^{-1}) = (\phi(a))^{-1}$ $\rightsquigarrow$ preserve inverses
- Some 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 (resp. cyclic), then so is G_2.

  $\rightsquigarrow$ Prove that two groups are not isomorphic. (Examples in #11/15)
- $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

1st Theorem

Every subgroup of a cyclic group G is cyclic.

Proof: Let $G = \langle a \rangle$ for some $a \in G$, and let H be any subgroup of G.

- If H is the trivial subgroup consisting only of e, then $H = \langle e \rangle$. ✓
- If H is nontrivial, then it contains $b \neq e$. So $b = a^n$ for some $n \in \mathbf{Z}$.

Since $a^{-n} = (a^n)^{-1} \in H$, we can assume that H contains a^ℓ with $\ell > 0$.

Let m be the smallest positive integer s.t. $a^m \in H$. To show $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$: It is clear since $a^m \in H$ and H is a subgroup of G.

$H \subseteq \langle a^m \rangle$: For any $x \in H$, we have $x = a^k$ for some $k \in \mathbf{Z}$.

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

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

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

2nd Theorem

Let G be a cyclic group. $\begin{cases} \text{i)} & \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{ii)} & \text{If } |G| = n < \infty, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$

$\star_{\text{i)}}$ Any two infinite cyclic groups are isomorphic to each other.

$\star_{\text{ii)}}$ Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.

Proof: i) Let $G = \langle a \rangle$. Define $\phi\colon \mathbf{Z} \to G$ by $\phi(m) = a^m$ for all $m \in \mathbf{Z}$.

- well-defined: Since $G = \langle a \rangle$.
- respects the two operations: $\phi(m+k) = a^{m+k} = a^m a^k = \phi(m)\phi(k)$
- one-to-one: $\phi(m) = a^m = e$ implies $m = 0$.
- onto: Since $G = \langle a \rangle$. $\rightsquigarrow$ Thus ϕ is an isomorphism. □

ii) Let $G = \langle a \rangle$ with $|G| = n < \infty$. Define $\phi : \mathbf{Z}_n \to G$ by $\phi([m]) = a^m$ for all $[m] \in \mathbf{Z}_n$. To show ϕ is an isomorphism:

- well-defined: If $[k] = [m]$, then $a^k = a^m$.
- respects the two operations: $\phi([m] + [k]) = \cdots = \phi([m])\phi([k])$
- one-to-one: $\phi([m]) = a^m = e \quad \rightsquigarrow n|m$, i.e., $[m] = [0]$.
- onto: Since $G = \langle a \rangle$. □

The Subgroups of $\mathbf{Z}$

Recall that every subgroup of a cyclic group G is cyclic. (1st Theorem)

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

ii) $m\mathbf{Z} \subseteq n\mathbf{Z}$ if and only if $n|m$.

iii) $m\mathbf{Z} = n\mathbf{Z}$ if and only if $m = \pm n$.

Proof: i) ✓ ii) $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow m = kn$ for some $k \in \mathbf{Z}$ iii) follows from ii). □

$$m\mathbf{Z} \cong \mathbf{Z} \quad \text{for } m \neq 0.$$

Proof: $m\mathbf{Z}$ is an infinite cyclic group and so $m\mathbf{Z} \cong \mathbf{Z}$ by 2nd Theorem i).

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

Recall that for a finite cyclic group G with $|G| = n$, we have $G \cong \mathbf{Z}_n$.

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

The Subgroups of $\mathbf{Z}_n$

Recall that every subgroup of a cyclic group G is cyclic. (1st Theorem)

For each $[k] \in \mathbf{Z}_n$, we obtain the cyclic subgroup $\langle [k] \rangle$ generated by $[k]$.

It is possible to have $\langle [k] \rangle = \langle [\ell] \rangle$, e.g., $\langle [k] \rangle = \langle [\ell] \rangle = \mathbf{Z}_n$ for $[k], [\ell] \in \mathbf{Z}_n^\times$.

In $\mathbf{Z}_n$, let $d = (k, n)$. Then $\langle [k] \rangle = \langle [d] \rangle$. And so $|\langle [k] \rangle| = |\langle [d] \rangle| = n/d$.

Proof: $\langle [k] \rangle \subseteq \langle [d] \rangle$: $d|k \quad \rightsquigarrow [k] \in \langle [d] \rangle \quad \rightsquigarrow \langle [k] \rangle \subseteq \langle [d] \rangle$

$\langle [d] \rangle \subseteq \langle [k] \rangle$: $d = sk + tn$ for $s, t \in \mathbf{Z}$. $\quad \rightsquigarrow [d] \in \langle [k] \rangle \quad \rightsquigarrow \langle [d] \rangle \subseteq \langle [k] \rangle$

The order of $[d]$ is n/d, and so $[k]$ has order n/d. □

i) $\mathbf{Z}_n = \langle [k] \rangle \quad \Leftrightarrow \quad [k] \in \mathbf{Z}_n^\times \quad \Leftrightarrow \quad (k, n) = 1$

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

iii) If $d_1|n$ and $d_2|n$, then $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle$ if and only if $d_2|d_1$.

iii)' If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1] \rangle \neq \langle [d_2] \rangle$.

Proof: ii) $\langle [k] \rangle = \langle [d] \rangle, d = (k, n)$ iii) $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle \Leftrightarrow d_1 = md_2, m \in \mathbf{Z}$

Multiplicative Version for a Finite Cyclic Group of Order n

Recall that for a finite cyclic group G with $|G| = n$, we have $G \cong \mathbf{Z}_n$.

In $\mathbf{Z}_n$, let $d = (k, n)$. Then $\langle [k] \rangle = \langle [d] \rangle$. And so $|\langle [k] \rangle| = |\langle [d] \rangle| = n/d$.

Multiplicative version: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

Let $d = (k, n)$. Then $\langle a^k \rangle = \langle a^d \rangle$. And so $o(a^k) = |\langle a^k \rangle| = |\langle a^d \rangle| = n/d$.

i) $\mathbf{Z}_n = \langle [k] \rangle \quad \Leftrightarrow \quad [k] \in \mathbf{Z}_n^\times \quad \Leftrightarrow \quad (k, n) = 1$

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

iii) If $d_1 | n$ and $d_2 | n$, then $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle$ if and only if $d_2 | d_1$.

iii)' If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1] \rangle \neq \langle [d_2] \rangle$.

Multiplicative version: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

i) $G = \langle a^k \rangle \quad \Leftrightarrow \quad (k, n) = 1$.

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

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

iii)' 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

Recall that in $\mathbf{Z}_n$, let $d = (k, n)$. Then $\langle [k]_n \rangle = \langle [d]_n \rangle$.

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

A: $4|24$: So $\langle [k]_{24} \rangle = \langle [4]_{24} \rangle$ if and only if $(k, 24) = 4$. It follows that

$$(\frac{k}{4}, 6) = 1 \qquad \rightsquigarrow \frac{k}{4} = 1, 5.$$

Thus the possible choices are $[k]_{24} = [4]_{24}, [20]_{24}$. □

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

A: $4 \nmid 18$, but $(4, 18) = 2$. So $\langle [k]_{18} \rangle = \langle [4]_{18} \rangle = \langle [2]_{18} \rangle \Leftrightarrow (k, 18) = 2$

$$\rightsquigarrow (\frac{k}{2}, 9) = 1 \qquad \rightsquigarrow \frac{k}{2} = 1, 2, 4, 5, 7, 8.$$

. $\rightsquigarrow$ The possible choices are $[k]_{18} = [2]_{18}, [4]_{18}, [8]_{18}, [10]_{18}, [14]_{18}, [16]_{18}$.

Q: Can we list **all** the subgroups of $\mathbf{Z}_{18}$?

Example: List all the Subgroups of $\mathbf{Z}_{18}$

In $\mathbf{Z}_n$, let $d = (k, n)$. Then $\langle [k] \rangle = \langle [d] \rangle$ of order n/d. Furthermore,

i) $\mathbf{Z}_n = \langle [k] \rangle \quad \Leftrightarrow \quad [k] \in \mathbf{Z}_n^\times \Leftrightarrow (k, n) = 1$

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

iii) If $d_1 | n$ and $d_2 | n$, then $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle$ if and only if $d_2 | d_1$.

iii)' If $d_1 | n$ and $d_2 | n$ and $d_1 \neq d_2$, then $\langle [d_1] \rangle \neq \langle [d_2] \rangle$.

The divisors of 18 are 1, 2, 3, 6, 9, 18. So the subgroups of $\mathbf{Z}_{18}$ are:

$[d]_{18}$	$\langle [d]_{18} \rangle$	$\lvert \langle [d]_{18} \rangle \rvert = 18/d$
$[1]$	$\mathbf{Z}_{18}$	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

Q: How can we connect all of them by iii)?

Subgroup Diagram

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**.

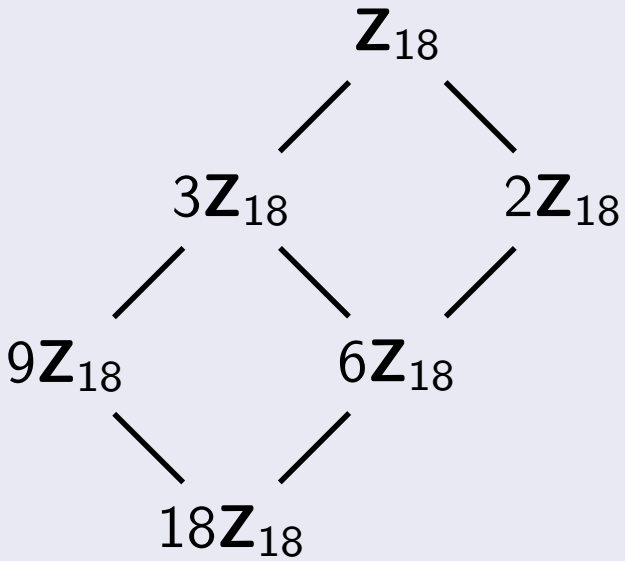
Larger subgroups on top, smaller subgroups on bottom. A line connecting two subgroups $\rightsquigarrow$ the subgroup on bottom is contained in the one on top.

The subgroup diagram of $\mathbf{Z}_{18}$ (using $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle \Leftrightarrow d_2 | d_1$):

The subgroups are obtained from the divisors of 18: 1, 2, 3, 6, 9, 18.

$18 = 2^1 \cdot 3^2$: Think about any divisor $d = 2^i 3^j$ with $i = 0, 1$ and $j = 0, 1, 2$.

Note: $1\mathbf{Z}_{18} = \langle [1]_{18} \rangle = \mathbf{Z}_{18}$ (entire group) and $18\mathbf{Z}_{18} = \langle [0]_{18} \rangle = \{[0]_{18}\}$.

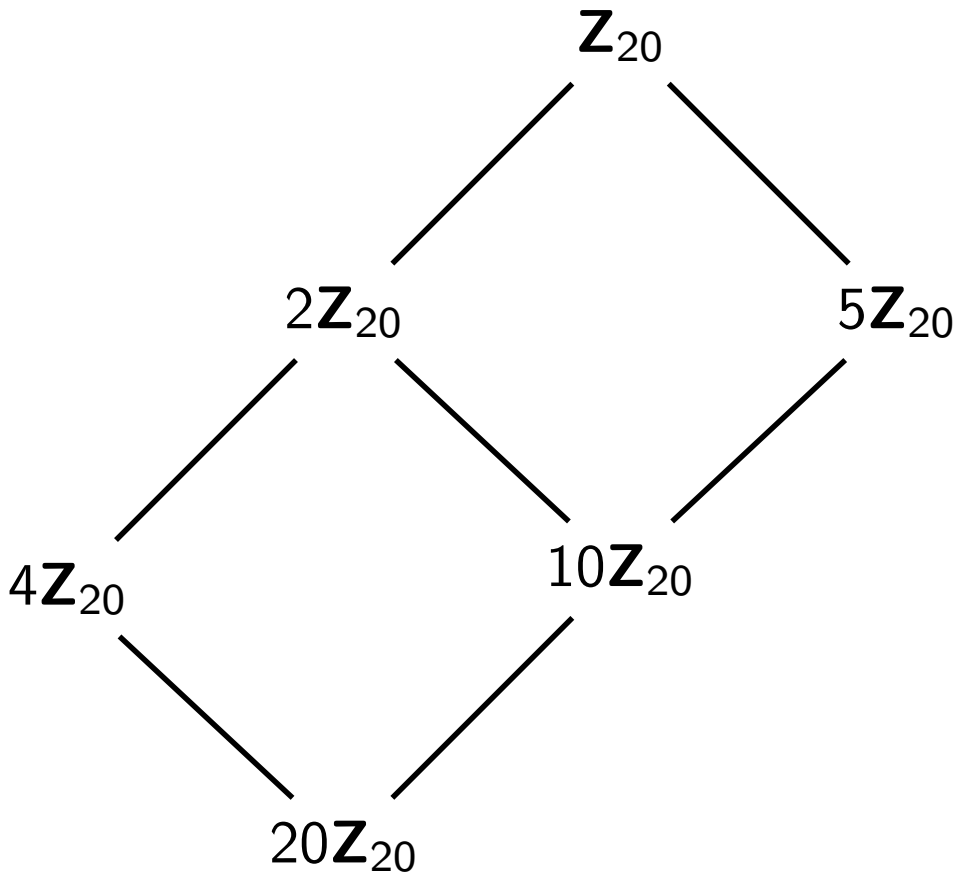


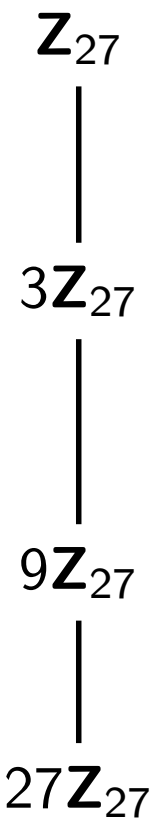
Examples: The Subgroup Diagrams of $\mathbf{Z}_{20}$ and $\mathbf{Z}_{27}$

If $d_1|n$ and $d_2|n$, then $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle$ if and only if $d_2|d_1$.

$20 = 2^2 \cdot 5^1$: Think about any divisor $d = 2^i 5^j$ with $i = 0, 1, 2$ and $j = 0, 1$.

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





Direct Product of Cyclic Groups

Recall that we introduced the direct product of two groups in §3.3.

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 **lcm** of the orders of each component.

$\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $(m, n) = 1 \rightsquigarrow \mathbf{Z}_{m_1 \cdots m_k} \cong \mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_k}$ if $(m_i, m_j) = 1, i \neq j$

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

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

Proof: The element $([1], [1], \ldots, [1])$ has order n in RHS (of order n). □

For example, $\mathbf{Z}_{18} \cong \mathbf{Z}_2 \times \mathbf{Z}_9$. However, $\mathbf{Z}_{18} \ncong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3$.

Revisit Euler's Totient Function $\varphi(n)$

$\varphi(n) := \#\{a\colon (a,n) = 1 \text{ and } 0 < a \leq n\} = |\mathbf{Z}_n^\times| =$ no. of generators of $\mathbf{Z}_n$

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

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

Proof: 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 $\mathbf{Z}_n$, since an isomorphism preserves generators.

$g = (g_1, \ldots, g_m)$ is a generator $\Leftrightarrow$ it has order n : $[o(g_1), \ldots, o(g_m)] = n$

$\rightsquigarrow o(g_i) = p_i^{\alpha_i}$ for each i [Why?] Thus g_i is a generator in $\mathbf{Z}_{p_i{}^{\alpha_i}}$ for each i.

$\rightsquigarrow$ 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 $\mathbf{Z}_{p^\alpha}$, and there are $p^{\alpha-1}$ such multiples in $\mathbf{Z}_{p^\alpha}$. Thus

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

□

$\mathbf{Z}_{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}} \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}$

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

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

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

To show ϕ is a group isomorphism. (HW) □

$\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_{20}$

$\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ and $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. Then by $(\star\star)$ we have

$$\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \quad \text{and} \quad \mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5.$$

Finally, it is easy to see that $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$.

$\mathbf{Z}_4 \times \mathbf{Z}_{15} \ncong \mathbf{Z}_6 \times \mathbf{Z}_{10}$

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 a Group G

Let G be a finite group of order n. For any $a \in G, o(a)|n$.

If N is the least common multiple (lcm) of $o(a)$ for all $a \in G$, then

$$a^N = e \text{ for all } a \in G. \quad \text{In particular, } N \text{ is a divisor of } |G|.$$

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.

The exponent of any **finite** group is the lcm of the orders of its elements.

For example, the exponent of S_3 is 6; the exponent of $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ is 4.

Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$.
Let $o(a) = m$ and $o(b) = n$. If $\gcd(m, n) = 1$, then $o(ab) = mn$.

Proof: Let $k = o(ab)$. To show $k = mn$. Since $(ab)^{mn} \stackrel{?}{=} e \quad \rightsquigarrow k|mn$.

$(ab)^k = e \rightsquigarrow (ab)^{mk} = e \rightsquigarrow (ab)^{mk} \stackrel{?}{=} a^{mk}b^{mk} = b^{mk} = e \rightsquigarrow n|mk \rightsquigarrow n|k$

$\rightsquigarrow (ab)^{nk} = e \rightsquigarrow (ab)^{nk} \stackrel{?}{=} a^{nk}b^{nk} = a^{nk} = e \rightsquigarrow m|nk \rightsquigarrow m|k \quad \stackrel{!}{\rightsquigarrow} mn|k$

Characterize Cyclic Groups Among all Finite Abelian Groups

Let G be a finite abelian group. The exponent of $G = \max\{o(a) : a \in G\}$.

In particular, G is cyclic **if and only if** its exponent is equal to its order.

Proof: Let $o(a)$ be the largest order. To show $o(a) =$ the exponent of G.

It suffices to show that $o(b)|o(a)$ for all $b \in G$. Proof by **contradiction:**

Suppose that $o(b)$ is not a divisor of $o(a)$. Then there exists a prime p:

$$o(a) = p^\alpha n, \ o(b) = p^\beta m, \quad \text{where } (p, n) = (p, m) = 1 \text{ and } \beta > \alpha \geq 0.$$

$\rightsquigarrow$ $o(a^{p^\alpha}) = n$ and $o(b^m) = p^\beta$. And so these orders are relatively prime.

$\rightsquigarrow$ $o(a^{p^\alpha} b^m) = np^\beta$ [Why?] We obtain a **contradiction** since $np^\beta > o(a)$.

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

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.

We will **NOT** prove or use it in this course, but a bonus project for you.

$\mathbf{Z}_{15}^{\times} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$ is not cyclic.

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

A sort of algorithm to attack this type of question:

- If $o([2]) = 8$, then 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 $[4], [8]$ since $[4], [8] \in \langle [2] \rangle$.

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) There is no need to try $[13]$ since $[13] \in \langle [7] \rangle$.

vi) $[14]^2 = [-1]^2 = [1]$, so $o([14]) = 2$.

In conclusion, there is no element of order 8, thus the group is not cyclic.

Prove that $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$ Without Constructing a Function ϕ

I. $|\mathbf{Z}_7^\times| = |\mathbf{Z}_{14}^\times| = 6$. In fact, we have

$$\mathbf{Z}_7^\times = \{[1], [2], [3], [4], [5], [6]\}, \quad \mathbf{Z}_{14}^\times = \{[1], [3], [5], [9], [11], [13]\}.$$

II. 1) If both of them are cyclic, then they are isomorphic.

2) 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) $[3]^2 = [9] = [2]$, $[3]^3 = [6]$, so $o([3]) = 6$. [Why?] (Lagrange's Thm)

Therefore $\mathbf{Z}_7^\times$ is cyclic.

IV. Check $\mathbf{Z}_{14}^\times$: $[3]^2 = [9]$, $[3]^3 = [13]$, so $o([3]) = 6$. $\rightsquigarrow \mathbf{Z}_{14}^\times$ is cyclic.

V. By II. 1), we conclude that $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times \cong \mathbf{Z}_6$. □