Sabbir Ahmed

DATE: April 10, 2018

MATH 407: HW 08

3.4 **4** Show that $\mathbb{Z}_5^\times$ is not isomorphic to $\mathbb{Z}_8^\times$ by showing that the first group has an element of order 4 but the second group does not

The elements in each of the groups

$$\{[1],[2],[3],[4]\} \in \mathbb{Z}_5^\times,\ o(\mathbb{Z}_5^\times) = 4$$
$$\{[1],[3],[5],[7]\} \in \mathbb{Z}_8^\times,\ o(\mathbb{Z}_8^\times) = 4$$

In $\mathbb{Z}_5^\times$

$$[2]^4 = [1],\ o([2]) = 4$$
$$[3]^4 = [1],\ o([3]) = 4$$
$$[4]^2 = [1],\ o([4]) = 2$$

Therefore, $\mathbb{Z}_5^\times$ is a cyclic group with generators $[2]$ and $[3]$
In $\mathbb{Z}_8^\times$

$$[3]^2 = [1],\ o([3]) = 2$$
$$[5]^2 = [1],\ o([5]) = 2$$
$$[7]^2 = [1],\ o([7]) = 2$$

No elements in $\mathbb{Z}_8^\times$ is of the same order as its group order
which implies $\mathbb{Z}_8^\times$ is non-cyclic
Therefore, $\mathbb{Z}_5^\times$ is not isomorphic to $\mathbb{Z}_8^\times$ since the first group is cyclic unlike the latter $\square$

7 Let G be a group. Show that the group $(G,*)$ defined in Exercise 3 of Section 3.1 is isomorphic to G.

Given $(G,*)$ is a group where $a * b = b \cdot a$
Let $\phi : (G,*) \to (G,\cdot)$ as

$$\phi(a) = \phi(e * a)$$
$$= a * e$$

$$= a, \ \forall\, a \in (G, *)$$

We need to show $\phi(a * b) = \phi(a) \cdot \phi(b)$

$$\begin{aligned}\phi(a * b) &= b \cdot a \\ &= b * e \cdot a * a \\ &= \phi(b) \cdot \phi(a)\end{aligned}$$

$\square$

11 Let G be the set of all matrices in $GL_2(\mathbb{Z}_3)$ of the form $\begin{bmatrix} \text{m} & \text{b} \\ 0 & 1 \end{bmatrix}$. That is, $m, b \in \mathbb{Z}_3$ and $m \neq [0]_3$. Show that G is a subgroup of $GL_2(\mathbb{Z}_3)$ that is isomorphic to S_3.

Given

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} \right\}$$

The non-empty, finite set G is a subgroup if $xy^{-1} \in G, \forall\, x, y \in G$

Let $\begin{bmatrix} \text{m} & \text{b} \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \text{n} & \text{a} \\ 0 & 1 \end{bmatrix} \in G$, where $m, n \neq [0]_3$ Then

$$\begin{bmatrix} \text{m} & \text{b} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \text{n} & \text{a} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \text{mn} & \text{b+am} \\ 0 & 1 \end{bmatrix}$$

Since $m, n \neq [0]_3$, then $mn \neq [0]_3$

Therefore $\begin{bmatrix} \text{mn} & \text{b+am} \\ 0 & 1 \end{bmatrix} \in G$, and G is a subgroup of $GL_2(\mathbb{Z}_3)$

Also, if $a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$, $a, b \in G$, then

$$a^3 = \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)^3$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$b^2 = \left(\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}\right)^2$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$a^2 b = \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)^2 \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$= ba$$

Therefore, G is similar to $S_3 = \{e, a, a^2, b, ab, a^2b\}$,
where $a^3 = e$, $b^2 = e$, $ba = a^2b$

Thus, let $\phi : G \to S_3$ as

$$\phi\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = (1, 2, 3)$$

$$\phi\left(\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}\right) = (1,2)$$

Then

$$\phi\left(\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)^i \left(\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}\right)^i\right) = (1,2,3)^i(1,2)^i,\ i = 0,1,2,\ j = 0,1$$

Which is both one-to-one and onto $\square$

14 Let $G = \{x \in \mathbb{R} \mid x > 0$ and $x \neq 1\}$, and define $*$ on G by $a * b = a^{\ln b}$. Show that G is isomorphic to the multiplicative group $\mathbb{R}^\times$. (See Exercise 9 of Section 3.1.)

Assume $\phi : G \to \mathbb{R}^\times$ is one-to-one and onto
Let $y \neq 0 \in \mathbb{R}^\times$, such that $e^y > 0 \in G$

$$\begin{aligned} \phi(e^y) &= \ln e^y \\ &= y \end{aligned}$$

$\square$

17 Let $\phi : G_1 \to G_2$ be a group isomorphism. Prove that if H is a subgroup of G_1, then $\phi(H) = \{y \in G_2 \mid y = \phi(h)$ for some $h \in H\}$ is a subgroup of G_2.

Since $\phi : G_1 \to G_2$ is a group isomorphism, $\phi(e_1) = e_2$
Since H is a subgroup,

$$\begin{aligned} e_1 &\in H \\ \Rightarrow e_2 &\in \phi(H) \end{aligned}$$

A non-empty set G is a subgroup if $xy^{-1} \in G$, $\forall\, x, y \in G$
Let $x, y \in \phi(H)$
Then, there exists $h_1, h_2 \in H$, such that

$$\begin{aligned} \phi(h_1) &= x \\ \phi(h_2) &= y \end{aligned}$$

Also, since ϕ is homomorphic,

$$\begin{aligned}\phi(h_2^{-1}) &= (\phi(h_2))^{-1} \\ &= y^{-1} \\ \phi(h_1 h_2^{-1}) &= \phi(h_1)\phi(h_2^{-1}) \\ &= xy^{-1}\end{aligned}$$

Since H is a subgroup, $h_1 h_2^{-1} \in H$, $\forall\, h_1, h_2 \in H$
Therefore,

$$\begin{aligned}\phi(h_1 h_2^{-1}) &= xy^{-1} \\ &\in \phi(H)\end{aligned}$$

That is, $\phi(h_1 h_2^{-1}) \in \phi(H)$, $\forall\, x, y \in \phi(H)$ $\square$

24 Let $G = \mathbb{R} - \{-1\}$. Define $*$ on G by $a * b = a + b + ab$. Show that G is isomorphic to the multiplicative group $\mathbb{R}^\times$. (See Exercise 13 of Section 3.1.)
Hint: Remember that an isomorphism maps identity to identity. Use this fact to help find the necessary mapping.

Let $\phi : G \to \mathbb{R}^\times$ as $\phi(a) = 1 + a$

Let $a = b$
Then, $1 + a = 1 + b$
Therefore, $\phi(a) = \phi(b)$ and ϕ is well defined

Let $\phi(a) = \phi(b)$
Then $1 + a = 1 + b$, which implies $a = b$
Therefore, ϕ is one-to-one

Let $x \in \mathbb{R}^\times$
Therefore, $x \neq 0$ and $\exists y = x - 1 \in G$
Since $\phi(x - 1) = 1 + x - 1 = x$, ϕ is also onto

To show $\phi(a * b) = \phi(a)\phi(b)$, consider

$$\phi(a * b) = 1 + (a * b)$$

$$
\begin{aligned}
&= 1 + a + b + ab \\
&= (1+a)(1+b) \\
&= \phi(a)\phi(b)
\end{aligned}
$$

Therefore, $G \cong \mathbb{R}^{\times}$ □

26 Let G_1 and G_2 be groups. A function from G into G_2 that preserves products but is not necessarily a one-to-one correspondence will be called a group homomorphism, from the Greek word *homos* meaning same. Show that $\phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^{\times}$ defined by $\phi(A) = \det(A)$ for all matrices $A \in \mathrm{GL}_2(\mathbb{R})$ is a group homomorphism.

Consider $\phi(A) = \det(A)$
Since $\mathrm{GL}_2(\mathbb{R})$ is a field, it is also abelian, and therefore

$$\det(AB) = \det(A)\det(B)$$

Thus,

$$
\begin{aligned}
\phi(AB) &= \det(AB) \\
&= \det(A)\det(B) \\
&= \phi(A)\phi(B)
\end{aligned}
$$

□

3.5 **2** Let G be a group and let $a \in G$ be an element of order 30. List the powers of a that have order 2, order 3 or order 5.

$$(a^{15})^2 = e$$

$$
\begin{aligned}
(a^{10})^3 &= e \\
(a^{20})^3 &= e
\end{aligned}
$$

$$
\begin{aligned}
(a^{6})^5 &= e \\
(a^{12})^5 &= e \\
(a^{18})^5 &= e
\end{aligned}
$$

$$(a^{24})^5 = e$$

Therefore,

the powers of a of order 2 is a^{15}

the powers of a of order 3 are a^{10}, a^{20}

the powers of a of order 5 are $a^6, a^{12}, a^{18}, a^{24}$ $\square$

3 Give the subgroup diagrams of the following groups.

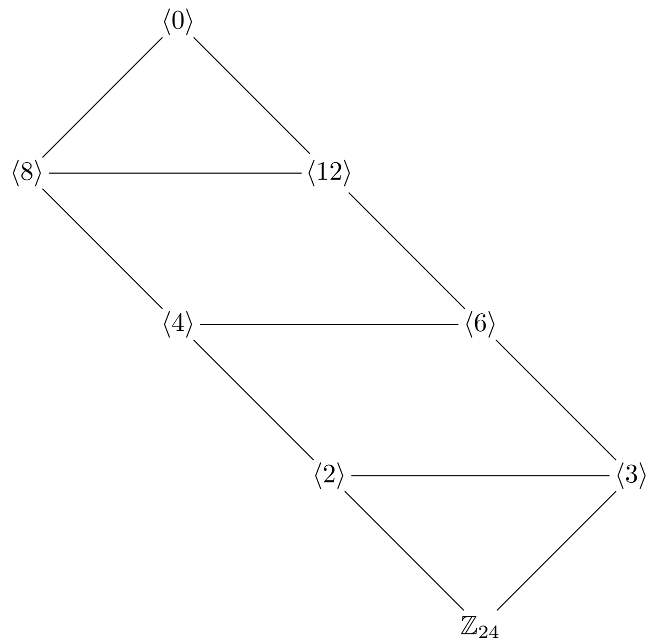
a $\mathbb{Z}_{24}$

The generators of $\mathbb{Z}_{24}$ are $\langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, \langle 8\rangle, \langle 12\rangle, \langle 0\rangle$

$$\begin{aligned}
\langle 1\rangle &= \mathbb{Z}_{24} \\
\langle 2\rangle &= \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 0\} \\
\langle 3\rangle &= \{3, 6, 9, 12, 15, 18, 21, 0\} \\
\langle 4\rangle &= \{4, 8, 12, 16, 20, 0\} \\
\langle 6\rangle &= \{6, 12, 18, 0\} \\
\langle 8\rangle &= \{8, 16, 0\} \\
\langle 12\rangle &= \{12, 0\} \\
\langle 0\rangle &= \{0\}
\end{aligned}$$

$\square$

Figure 1: Subgroup Diagram of $\mathbb{Z}_{24}$



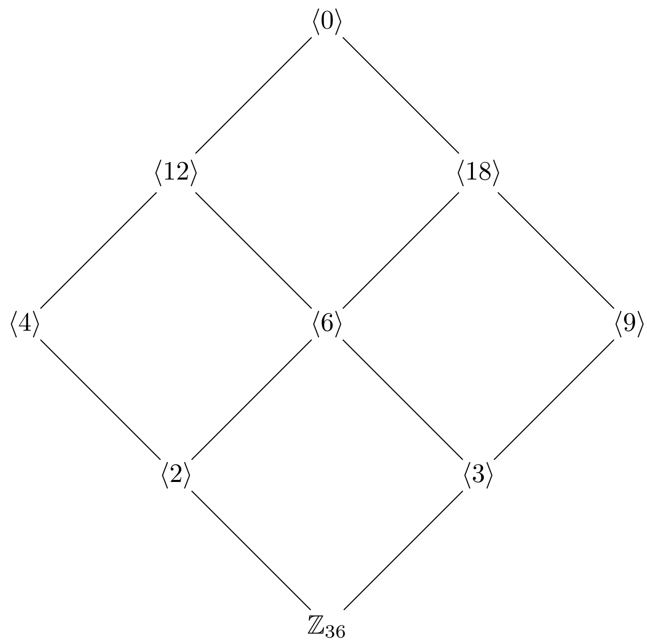
b $\mathbb{Z}_{36}$

The generators of $\mathbb{Z}_{36}$ are $\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 6 \rangle, \langle 9 \rangle, \langle 12 \rangle, \langle 18 \rangle, \langle 0 \rangle$

$$
\begin{aligned}
\langle 1 \rangle &= \mathbb{Z}_{36} \\
\langle 2 \rangle &= \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 0\} \\
\langle 3 \rangle &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 0\} \\
\langle 4 \rangle &= \{4, 8, 12, 16, 20, 24, 28, 32, 0\} \\
\langle 6 \rangle &= \{6, 12, 18, 24, 30, 0\} \\
\langle 9 \rangle &= \{9, 18, 27, 0\} \\
\langle 12 \rangle &= \{12, 24, 0\} \\
\langle 18 \rangle &= \{18, 0\} \\
\langle 0 \rangle &= \{0\}
\end{aligned}
$$

$\square$

Figure 2: Subgroup Diagram of $\mathbb{Z}_{36}$



10 Find all cyclic subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_3$

All the cyclic subgroups by checking the multiples of all elements in the group

$$\begin{aligned}
\langle(0,0)\rangle &= \{(0,0)\} \\
\langle(0,1)\rangle &= \{(0,0),(0,1),(0,2)\} \\
&= \langle(0,2)\rangle \\
\langle(1,0)\rangle &= \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0)\} \\
&= \langle(5,0)\rangle \\
\langle(1,1)\rangle &= \{(0,0),(1,1),(2,2),(3,0),(4,1),(5,2)\} \\
&= \langle(5,2)\rangle \\
\langle(1,2)\rangle &= \{(0,0),(1,2),(2,1),(3,0),(4,2),(5,1)\} \\
&= \langle(5,1)\rangle \\
\langle(2,0)\rangle &= \{(0,0),(2,0),(4,0)\} \\
&= \langle(4,0)\rangle \\
\langle(2,1)\rangle &= \{(0,0),(2,1),(4,2)\} \\
&= \langle(4,2)\rangle \\
\langle(2,2)\rangle &= \{(0,0),(2,2),(4,1)\} \\
&= \langle(4,1)\rangle
\end{aligned}$$

$$\begin{aligned}\langle(3,0)\rangle &= \{(0,0),(3,0)\}\\ \langle(3,1)\rangle &= \{(0,0),(3,1),(0,2),(3,0),(0,1),(3,2)\}\\ &= \langle(3,2)\rangle\end{aligned}$$ □

12 Let a, b be positive integers, and let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. Use Proposition 3.5.5 to prove that $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_d \times \mathbb{Z}_m$

□

13 Show that in a finite cyclic group of order n, the equation $x^m = e$ has exactly m solutions, for each positive integer m that is a divisor of n.

□

17 Let G be the set of all 3×3 matrices of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$.

a Show that if $a, b, c \in \mathbb{Z}_3$, the G is a group with exponent 3.

Consider

$$\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\right)^2 = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & a+a & b+ac+b \\ 0 & 1 & c+c \\ 0 & 0 & 1 \end{bmatrix}$$

$$\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\right)^3 = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a+a & b+ac+b \\ 0 & 1 & c+c \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix}$$

Since G has an exponent of 3,

$$\begin{bmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \square$$

b Show that if $a, b, c \in \mathbb{Z}_2$, the G is a group with exponent 4.

Consider

$$\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\right)^2 = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & a+a & b+ac+b \\ 0 & 1 & c+c \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\left(\begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right)^2 = \begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & \text{ac+ac} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \square$$

19 Let $n = 2^k$ for $k > 2$. Prove that $\mathbb{Z}_n^\times$ is not cyclic.

Hint: Show that ± 1 satisfy the equation $x^2 = 1$, and that this is impossible in any cyclic group.

Let $x = \frac{n}{2} + 1$. Then

$$x = \left(\frac{n}{2} + 1\right)^2$$

$$= \left(\frac{2^k}{2} + 1\right)^2$$

$$= (2^{k-1} + 1)^2$$

$$= 2^{2k-2} + 1 + 2^k$$

$$= 1 + 2^k(2^k + 1)$$

Therefore, $x^2 - 1 \equiv 0 \pmod{2^k}$, or $x^2 = 1$

Now let $x = \frac{n}{2} - 1$. Then

$$x = \left(\frac{n}{2} - 1\right)^2$$

$$= \left(\frac{2^k}{2} - 1\right)^2$$

$$= (2^{k-1} - 1)^2$$

$$= 2^{2k-2} + 1 - 2^k$$

$$= 1 + 2^k(2^k - 1)$$

Therefore, $x^2 - 1 \equiv 0 \pmod{2^k}$, or $x^2 = 1$

Therefore, the solutions to $x^2 = 1$ are $\pm 1, \frac{n}{2} \pm 1$

Therefore, the order of $\mathbb{Z}_n^\times$ are even, which is not possible in a cyclic group

Therefore, $\mathbb{Z}_n^\times$ is not cyclic (by contradiction) $\square$