Name: Connor Raymond Stewart
ID: 101041125

MATH 3101 Assignment 6:

① list all the elements of the Subgroup $\langle[8]\rangle$ in the group $\mathbb{Z}_{18}$ under addition. Also, State the order of this Subgroup:

test each integer:

$8\cdot0\equiv0 \pmod{18}$
$8\cdot1\equiv8 \pmod{18}$
$8\cdot2\equiv16 \pmod{18}$
$8\cdot3\equiv6 \pmod{18}$
$8\cdot4\equiv14 \pmod{18}$
$8\cdot5\equiv4 \pmod{18}$
$8\cdot6\equiv12 \pmod{18}$
$8\cdot7\equiv2 \pmod{18}$
$8\cdot8\equiv10 \pmod{18}$

thus:

$\langle[8]\rangle=\{[0],[2],[4],[6],[8],[10],[12],[14],[16]\}$

this is the Same group as generated by $gcd(18,2)=[2]$

the order is: $|\langle[8]\rangle|=9$

② a) Consider the Subset $H=\{[0],[4],[8]\}$ of $\mathbb{Z}_{12}$. Show that H is a Subgroup of $\mathbb{Z}_{12}$:

$\mathbb{Z}_{12}=\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\}$

to be a Subgroup, $H\subseteq\mathbb{Z}_{12}$

$\{[0],[4],[8]\}\subseteq\mathbb{Z}_{12}$ ∴ it's a Subset

Check group Conditions: ($\mathbb{Z}_n$ is abelian group over Addition, So check addition)

a) H is nonempty: (also See table)

H has 3 elements ∴ $H\neq$ nil, So True

b) $x\in H$ & $y\in H$ imply $xy\in H$: (also See table)

$0\cdot4=0\cdot8=4\cdot0=8\cdot0=0\in H$

$4\cdot8=8\cdot4=32\equiv8$ mod $12\rightarrow 8\in H$

$8\cdot8=64\equiv4$ mod $12\rightarrow 4\in H$

∴ True by exhaustion

c) $x\in H$ implies $x^{-1}\in H$:

+	[0]	[4]	[8]
[0]	[0]	[4]	[8]
[4]	[4]	[8]	[0]
[8]	[8]	[0]	[4]

(this proves b) for addition)

it is evident H Contains the inverse for each of its elements.

Old Sol^{n}

new Sol$^{\underline{n}}$

② a) Edits:

We can see that $\mathbb{Z}_{12}$ has the divisors of 1, 2, 3, 4, 6, 12:

using a divisor of 4, we get a subgroup of:

$\langle [3] \rangle = \{[0], [4], [8]\}$

as 12 mod $12 \equiv 0$

this is the same Sol$^{\underline{n}}$ as H

We know $\mathbb{Z}_{12}$ is a cyclic subgroup since there's a unique subgroup of order p for each divisor p of 12:

$\{[0]\}, 1$

$\{[0], [6]\}, 2$

$\{[0], [4], [8]\}, 3 \rightarrow = H$

$\{[0], [3], [6], [9]\}, 4$

$\{[0], [2], [4], [6], [8], [10]\}, 6$

$\mathbb{Z}_{12}, 12$

$\therefore$ H is a subgroup of $\mathbb{Z}_{12}$ as $\mathbb{Z}_{12}$ is cyclic & H is the subgroup when n=12 is divided into 3 parts

b)

As can be seen above

$\{[0], [5], [10]\}$ is not in the list of subgroups of $\mathbb{Z}_{12}$

$\therefore$ I not a subgroup of $\mathbb{Z}_{12}$

Old Sol'n

X	[0]	[4]	[8]
[0]	[0]	[0]	[0]
[4]	[0]	[4]	[8]
[8]	[0]	[8]	[4]

this Shows b, c for multiplication (example)

$\therefore$ It is proven true that H is a Subgroup of $\mathbb{Z}_{12}$ by theorm 3.11
It has been proven for addition & multiplication, but note multiplication is not a group overall $\mathbb{Z}_n$ & we could prove other $*$ as well)

b) Explain why the set $I = \{[0],[5],[10]\}$ is not a Subgroup of $\mathbb{Z}_{12}$:
by Condition b in Theorm 3.11:
$x \in H$ & $y \in H$ imply $x * y \in H$
yet we note:
let $x = 5$, $y = 10$ then:
$x+y = 5+10 = 15 \equiv 3 \text{ mod } 12 \rightarrow 3 \notin H$
thus:
we see a Contradiction, as $x+y$ is not Closed under addition in $\mathbb{Z}_{12}$

③ Consider the Subset:

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\} \text{ of } M_{2\times 2}(\mathbb{R})$$

Show that H is a Subgroup of $M_{2\times2}(\mathbb{R})$: (use Theorm 3.11)

I) H is nonempty:
we Know $e \in H$ by the Condition of groups

II) $x, y \in H$ imply $xy \in H$:
let $H_1, H_2 \in H$:

$$H_1 * H_2 = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} * \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 * a_2 & 0 \\ 0 & b_1 * b_2 \end{bmatrix}$$

Note:

$$\det(H_1 * H_2) = \frac{1}{(a_1 * a_2)(b_1 * b_2) - 0^2}\left(a_1 * a_2 + \cancel{b_1 * b_2}\right) = 1$$

Hence, Closure under the group operation is proven true

III) $x \in H$ implies $x^{-1} \in H$:

let $x = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $a, b \in \mathbb{R}$

Note:
$\det x^{-1} = \frac{1}{1/ab}\left(1/ab\right) = 1$
thus the Subgr. matrix is Closed under all inverses.

$$x^{-1} = \frac{\operatorname{Adj}(A)}{\det(A)} = \frac{1}{ad - 0^2}\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix} = \frac{1}{ab}\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix} = \begin{bmatrix} -1/b & 0 \\ 0 & -1/a \end{bmatrix} \in H$$

thus, H is a Subgroup of $M_{2\times 2}(\mathbb{R})$

(4) list all of the Subgroups of $\mathbb{Z}_{24}$. List all of the generators of $\mathbb{Z}_{24}$:

for all $H=\{x\in\mathbb{Z}_{24} \mid x=a^n \text{ for } n\in\mathbb{Z}\}$: (Subgroups)

Subgroups:

$\{[0]\}, 1$

$\{[0],[12]\}, 2$

$\{[0],[8],[16]\}, 3$

$\{[0],[6],[12],[18]\}, 4$

$\{[0],[4],[8],[12],[16],[20]\}, 6$

$\{[0],[3],[6],[9],[12],[15],[18],[21]\}, 8$

$\{[0],[2],[4],[6],[8],[10],[12],[14],[16],[18],[20],[22]\}, 12$

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

Find all distinct Generators:

$\mathbb{Z}_n=\{[0],[1],\dots,[n-1]\}$

i is a generator of $\mathbb{Z}_n$ iff $\gcd(i,n)=1$

for $\mathbb{Z}_{24}$, $n=24$:

$(1,24)=1$

$(5,24)=1$

$(7,24)=1$

$\cancel{(9,24)=3}$

$\cancel{(10,24)=2}$

$(11,24)=1$

$(13,24)=1$

$\cancel{(15,24)=3}$

$(17,24)=1$

$(19,24)=1$

$\cancel{(21,24)=3}$

$(23,24)=1$

Set of generators $=[1],[5],[7],[11],[13],[17],[19],[23]$

⑤ let $G=\langle a\rangle$ be a cyclic group of order 153. Compute $|a^{87}|$:

$(a^{87})^n = 153$

Euclid's Alg.: ↳ $(a^{87})^n \equiv 0 \mod 153$

$$\begin{bmatrix} 153=(1)(87)+66 \\ 87=66(1)+21 \\ 66=21(3)+3 \\ 21=\boxed{3}(7) \end{bmatrix}$$

$\rightarrow 0 \equiv 87n \mod 153$, let $n=51$

$\equiv 87\cdot 51 \mod 153$

$\equiv 4437 \mod 153$

$\equiv 0 \mod 153$

$(a^{87})^{51} = a^{4437} = e$

▸ $\gcd(87,153)=3$ thus the solution is not $n=153$

↳ from above, we see that $n=51$ thus: $(153/3=51)$

$|a^{87}|=51$, it follows that a^{87} is a generator of $G=\langle a^3\rangle$

⑥ Determine whether the following statements are true or false. Justify your responses:

a) let p be a prime. Then $\mathbb{Z}_p$ contains exactly two subgroups:

$H=\{x\in G \mid x=a^n \text{ for } n\in\mathbb{Z}_p\}$

Since p is prime, it's only divisible by itself & 1

thus, since subgroups contain elements based off factors of n, if $n=p$ & p has no factors, no extra subgroups exist.

Since $p=(1)(p)$ though, exactly two subgroups exist, namely:

$\{[0]\}, 1$ and $\mathbb{Z}_p, p$

Thus, $\mathbb{Z}_p$ contains exactly two subgroups

∴ True

b) let G be a group, & let $a\in G$. Then a generates a cyclic subgroup of G:

for all $a\in G$, $n\in\mathbb{Z}$

$a^n \in G$ (Closure)

Since G is a group

↳ $\langle a\rangle$ is thus a subset of G

We also know it is a subgroup of G:

I) $e=a^0\in G$ (nonempty)

II) $a^n, a^k\in G$ so $a^n a^k = a^{\overbrace{n+k}^{\text{Note: } n+k\in\mathbb{Z}}} \in G$ (closure)

III) if $a^n\in G$, then $a^{-n}\in G$ (inverse)

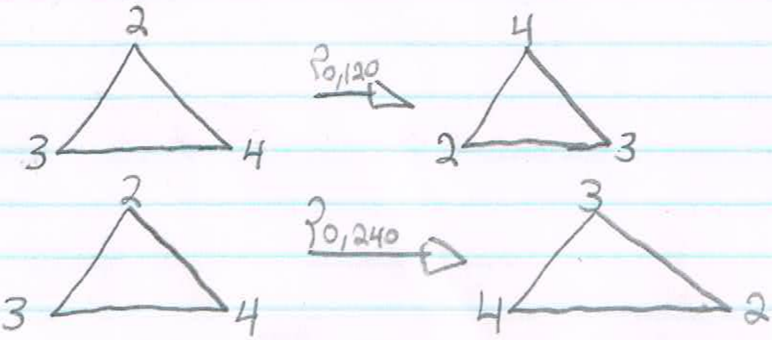
↳ see: $a^n\cdot a^{-n}=e$

∴ It's a cyclic subgroup

∴ True

c) In D_3, $\rho_{0,120}^{234} = \varepsilon$:

$\langle\langle \rho_{0,120} \rangle\rangle = \{\varepsilon, \rho_{0,120}, \rho_{0,240}\}$ Since



$\rho_{0,120}^{234} = (\rho_{0,120})^{234} \to 120^\circ \cdot 234 = 28080^\circ$ rotation

full rotation is 360° & $\rho_{0,360} = \varepsilon$ as a full rotation about the centre is the same as ε.

thus:

$28080 \pmod{360^\circ} \equiv 0 \pmod{360^\circ}$

$\therefore \rho_{0,120}^{234} \equiv \rho_{0,360} \pmod{360^\circ} \equiv \varepsilon \pmod{360^\circ}$

$\therefore$ True

d) If a Subgroup H of a group G is cyclic, then G must also be cyclic:

We know that the integers are an infinite cyclic group (under addition)

All integers can be written by adding or subtracting one

We also know that the real numbers cannot be cyclic under addition:

Suppose $\mathbb{R}$ is cyclic under addition

let $x \in \mathbb{R}$, then $\mathbb{R} = \langle x \rangle = \{n \cdot x \mid n \in \mathbb{Z}\}$

Note: $\frac{1}{2}x \in \mathbb{R}$, but $\frac{1}{2}x \notin \langle x \rangle$ as $\frac{1}{2}x = nx,\ n \in \mathbb{Z}$

Since $x \neq 0$ & $\frac{1}{2} = n$, a contradiction is evident

$\therefore$ $\mathbb{R}$ is not cyclic under addition

It is known that the integers are a Subgroup of the Real numbers

thus if $H = \mathbb{Z}$ & $G = \mathbb{R}$, we note that:

H is cyclic & G is Not cyclic

$\therefore$ False by Counterexample