Two solutions back to back
1. By Yousuf
2. By Taha

Exam I: Abstract Algebra, MTH 320, Fall 2017

Ayman Badawi

Excellent

Score = $\frac{63}{63}$

1. Yousuf Abo Rahma

QUESTION 1. Let $D, *)$ be a group.

(i) **(5 points).** Assume that $a * b = b * a$ for some $a, b \in D$. Prove that $a * b^{-1} = b^{-1} * a$.

From the question we have $a * b = b * a$

$\Rightarrow b^{-1} * a * b * b^{-1} = b^{-1} * b * a * b^{-1}$

$\Rightarrow b^{-1} * a = a * b^{-1}$

5/5

(ii) **(5 points).** Let $C = \{x \in D \mid x * y = y * x \ \forall\, y \in D\}$. (i.e., each element in C commutates with every element in D). Prove that C is a normal subgroup of D (Hint: you may need to use part (i))

Q1 (ii) continues on back, see page 5/13

show that if $a, b \in C$ then $a * b^{-1} \in C$

let $a, b \in C \Rightarrow \forall y \in D$ we have $a * y = y * a$, $b * y = y * b$

$\Rightarrow a * b^{-1} * y = a * y * b^{-1} = y * a * b^{-1} \Rightarrow a * b^{-1} \in C$

using (i)

~~② show normality $\Rightarrow$ show $x * k * x^{-1} \in C$ $\forall x \in D, k \in C$~~

~~$\Rightarrow$ let $x, y \in D$, $k \in C \Rightarrow x * k * x^{-1} * y * (x * k * x^{-1})^{-1} = k * y * k^{-1}$~~

~~$= k^{-1} * y * k$~~

~~$= (x * k * x^{-1})^{-1} * y * x * k * x^{-1}$~~

~~$\Rightarrow x * k * x^{-1} \in C \Rightarrow C \triangleleft D$ (Note $k \in C$ can commute with any element in D this was used to do the simplification).~~

next page shorter proof

(iii) **(5 points).** Let C as in (ii). Assume that D/C is cyclic. Prove that D is an abelian group.

D/C is cyclic $\Rightarrow D/C = \langle a * C \rangle$ for some $a \in D$

$\Rightarrow$ every element $x \in D$ can be written as $x = a^i * c$ for some $i \in Z$ and $c \in C$. This is due to the fact that the union of the cosets give you the group (if countable).

$\Rightarrow$ let $x, y \in D \Rightarrow x * y = a^{i_1} * c_1 * a^{i_2} * c_2$

$= a^{i_1} * a^{i_2} * c_1 * c_2$

$= a^{i_2} * c_2 * a^{i_1} * c_1$

$= y * x$

5/5

Note that c_1, c_2 comute with every element and $a^{i_1} * a^{i_2} = a^{i_1 + i_2} = a^{i_2} * a^{i_1}$.

QUESTION 2. Let $D = (Z_6, +) \times (Z_5^*, .)$

(i) **(3 points).** Fine $|(5, 2)|$.

in Z_6: $|5| = |1| = 6$

in Z_5^*: $|2| = 4$

$\Rightarrow |(5,2)| = \text{lcm}(6,4) = 12$

(ii) **(6 points).** Construct two subgroups of D, say H_1 and H_2, such that each has 4 elements and $H_1 = F_1 \times F_2$, $H_2 = L_1 \times L_2$ for some subgroups F_1, L_1 of $(Z_6, +)$ and some subgroups F_2, L_2 of $(Z_5^*, .)$.

let $F_1 = \{0, 3\}$, $F_2 = \{1, 4\}$

$L_1 = \{0\}$, $L_2 = \{1, 2, 3, 4\}$

$\Rightarrow F_1 \times F_2$ is a sub group of order 4

$L_1 \times L_2$ is a subgroup of order 4

(iii) **(3 points)** Convince me that D does not have an element of order 24.

if D has an element of order 24 then it is cyclic, but since D has 2 distinct subgroup of order 4 then it can't be cyclic thus it can't have an element of order 24.

(iv) **(4 points).** Construct a subgroup of D, say H, such that H has 4 elements, but there is no subgroup N_1 of $(Z_6, +)$ and there is no subgroup N_2 of $(Z_5^*, .)$ such that $H = N_1 \times N_2$.

$H = \langle (3,2) \rangle = \{(3,2), (0,4), (3,3), (0,1)\}$ is of order 4 and can't be constructing by multiplying 2 subgroups,

For if $H = N_1 \times N_2$, then $|N_2| = |Z_5^*| = 4$ and $|N_1| \geq 2$, Hence $|H| \geq 8$, Impossible since $|H| = 4$.

QUESTION 3. (i) **(4 points).** Is $(Z_7^*, .)$ group-isomorphic to $(U(9), .)$? If yes, then prove it. If no, then tell me why not?

$(Z_7^*, \cdot) = \langle 3 \rangle \cong (Z_6, +)$ and $U(9) \cong (Z_6, +)$

$\Downarrow$ Since $|3| = 6$

$\Downarrow$ $9 = 3^2$ and 9 is odd $\Rightarrow U(9)$ is cyclic with $\phi(9) = 6$ eliment

Since both are cyclic with 6-eliment we ~~t~~ they are isomorphic

i.e $(Z_7^*, \cdot) \cong (Z_6, +) \cong (U(9), \cdot)$

(ii) **(4 points).** Is $(Z_{41}^*, .)$ group-isomorphic to $(U(75), .)$? If yes, then prove it. If no, then tell me why not?

No it is not $\cancel{Z}^*_{41} \cong U(41) \Rightarrow$ cyclic

while $75 = 3 \times 5^2$ ~~$\Rightarrow$~~ $U(75)$ is not cyclic

$\Rightarrow$ they are not isomorphic

(iii) **(6 points).** Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 9 & 8 & 2 & 6 & 5 & 1 \end{pmatrix} \in S_9$. Find $|f|$. Is $f \in A_9$? explain

$f = (1\ 3\ 4\ 9)(8\ 5)(6\ 2\ 7) \Rightarrow |f| = \text{lcm}\{4, 2, 3\} = 12$

$\Downarrow$ 5 (2-cycles) $\Downarrow$ 1 (2-cycles) $\Downarrow$ 4 (2-cycles)

$\Rightarrow f$ can be written as 10 (2-cycles) $\Rightarrow f \in A_9$.

(iv) **(6 points).** Let $(D, *)$ be a group. Assume that $a * b = b * a$ for some $a, b \in D$, $|a| = n$, and $|b| = m$. Let $u = lcm[n, m]$. Prove that D has a cyclic subgroup with u elements. (Hint: You may need the fact: if $d = gcd(n, m)$, then $gcd(\frac{n}{d}, m) = 1$ OR $gcd(n, \frac{m}{d}) = 1$).

~~let d= ... (this assumption doesn't always the problem) and d = gcd ...~~

~~$\Rightarrow gcd(\frac{n}{d}, m) = 1$~~

et $d = gcd(m,n)$ and let $gcd(\frac{n}{d}, m) = 1$ (the same way can be done with $gcd(n, \frac{m}{d}) = 1$)

$\Rightarrow |a^d| = \frac{n}{gcd(n,d)} = \frac{n}{d}$ and since $|b| = m$ and $a*b = b*a$ and $gcd(\frac{n}{d}, m) = 1$

we have $|a^d * b| = \frac{n}{d} \times m = \frac{nm}{d} = lcm(m, n)$

$\Rightarrow \langle a^d * b \rangle$ is a cyclic subgroup of D with $u = lcm(m,n)$ eliment

In case $gcd(\frac{m}{d}, n) = 1$ we take $\langle a * b^d \rangle$.

QUESTION 4. (i) **(6 points)**. Is there a group-homomorphism $f : (Z_{18}, +) \to (Z_9, +)$ such that f is nontrivial and f is not ONTO? If yes, then construct such f and find $Range(f)$ and $Ker(f)$. If such f does not exist, EXPLAIN.

$f(1^{i}) = 1^{3i} \Rightarrow f(1^{i_1} *_1 1^{i_2}) = f(1^{i_1+i_2}) = 1^{3i_1+3i_2} = 1^{3i_1} *_2 1^{3i_2}$
$= f(1^{i_1}) *_2 f(1^{i_2})$

$\Rightarrow f$ is a homomorphism

Range$(f) = \langle 3 \rangle = \{3, 6, 0\}$, Ker$(f) = \{3, 6, 9, 12, 15, 0\}$

Yes, there is.

(ii) **(6 points)**. Let $(D, *)$ be a group with 155 elements. Assume that H is a normal subgroup of D with 5 elements. Prove that H is the only subgroup of D with 5 elements. If $a \in D \setminus H$ and $|a| \neq 31$, prove that D is cyclic.

* Deny that H is the only sub group of D with 5 element $\Rightarrow$ $\exists H_2$ such that $|H_2| = |H| = 5$ and since 5 is prime then both are disjoint cyclic $\Rightarrow |H H_2| = \frac{25}{|H \cap H_2|} = 25$ and since $H \triangleleft D$, $HH_2 < D$ yet $25 \nmid 155$ (contradiction) $\Rightarrow$ H is the only sub group of order 5.

* H has the only elements of order 5 $\Rightarrow a \in D \setminus H \Rightarrow |a| \neq 5, |a| \neq 1$ and since $|a| \neq 31$ the only remaining divisor of 155 is 155 itself $\Rightarrow |a| = 155 \Rightarrow D = \langle a \rangle$ is cyclic.

(iii) **(Bonus 7 points)**. Let H be a subgroup of a group $(D, *)$. Assume that for each $a \in D \setminus H$, we have $x_1 * x_2 * x_3 * x_4 \in a * H$ for every $x_1, x_2, x_3, x_4 \in a * H$ (note that $x_1, ..., x_4$ need not be distinct). Prove that H is a normal subgroup of D.

Idea: Let $h \in H$ and $a \in D \setminus H$, show $a h a^{-1} = h_1 \in H$.

First: observe $a \in a*H \Rightarrow$ (by hypothesis) $a^4 \in a*H \Rightarrow a^4 = a*n$ (some $n \in H$) $\Rightarrow a^3 = n \in H$. Hence $n^{-1} = a^{-3} \in H$.

Now $\underbrace{(a*h)*(a*h*a^{-3})*a^2}_{4 \text{ elements in } a*H} = a*h_2$ (some $h_2 \in H$)

$\Rightarrow h*(a*h)*a^{-1} = h_2$ (cancel a from both sides)

$\Rightarrow (a*h)*a^{-1} = h^{-1}*h_2 = h_1 \in H$

$\Rightarrow a*h = h_1*a$. Done.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

Q1 (ii) continues here

To show $C \lhd D$ we show that $\forall a \in D$
$a * C = C * a$. ~~[illegible]~~
$\Rightarrow$ let $a \in D$, $c \in C$ show that $a * c * a^{-1} \in C$.
$a * c * a^{-1} = a * a^{-1} * c = c \in C$. $\Rightarrow C \lhd D$.

Exam I: Abstract Algebra, MTH 320, Fall 2017

Excellent

Ayman Badawi

2. Taha Ameen

Score = $\frac{60}{63}$

QUESTION 1. Let $D, *)$ be a group.

(i) **(5 points).** Assume that $a * b = b * a$ for some $a, b \in D$. Prove that $a * b^{-1} = b^{-1} * a$.

$a * b = b * a \Rightarrow a * b * b^{-1} = b * a * b^{-1}$

$\therefore a * e = b * a * b^{-1} \Rightarrow a = b * a * b^{-1}$

4/4

$\because b^{-1} * a = (b^{-1} * b) * a * b^{-1}$

$\therefore b^{-1} * a = a * b^{-1}$ ■

(ii) **(5 points).** Let $C = \{x \in D \mid x * y = y * x \ \forall\, y \in D\}$. (i.e., each element in C commutes with every element in D). Prove that C is a normal subgroup of D (Hint: you may need to use part (i))

I. We show $C < D$. Let $a, b \in C$ $\therefore a * x = x * a$, $b * x = x * b$ $\forall x \in D$

To Prove: $b^{-1} * a \in C$. i.e $(b^{-1} * a) * x = x * (b^{-1} * a)$ $\forall x \in D$

Proof: $(b^{-1} * a) * x = b^{-1} * x * a$ $(\because a * x = x * a)$

$= x * (b^{-1} * a)$ ■ (By Part (i))

$\therefore C \lhd D$. To Prove: $x * C = C * x$ $\forall x \in D$.

Proof: $x * C = \{x * c_1 \mid c_1 \in C\}$. But $x * c_1 = c_1 * x$

4/4

$= \{c_1 * x \mid c_1 \in C\} = C * x$ ■ $\therefore C \lhd D$.

(iii) **(5 points).** Let C as in (ii). Assume that D/C is cyclic. Prove that D is an abelian group.

D/C is cyclic. $\therefore$ Since $D/C = \{a * C \mid a \in D\}$ is cyclic:

~~Let $D/C = \{C, C_1, C_2, C_3 \ldots\}$. $C_1 = a_1 * C$ ...~~

elements in C commute with every element. To Show: $a * b = b * a$ $\forall a, b \in D$.

$a_1 * C = a_k^x * C$ for some a_k (the generator).

$a_2 * C = a_k^y * C$ $(\because D/C$ is cyclic$)$.

$\therefore a_1 = a_k^x * c_1$ for some $c_1 \in C$.

5/5

$a_2 = a_k^y * c_2$ for some $c_2 \in C$.

see Page 10/13

$a_1 * a_2 = (a_k^x * c_1) * (a_k^y * c_2) = a_k^x * a_k^y * c_1 * c_2$

(CP TO)

QUESTION 2. Let $D = (Z_6, +) \times (Z_5^*, .)$

(i) (3 points). Fine $|(5, 2)|$. $|(5,2)| = LCM(|5|, |2|)$.

But: $5 \in Z_6 \Rightarrow |5| = 6$ // $(\because |5| = |5^{-1}| = |1| = 6 \because 6 = <1>)$

$2 \in Z_5^* \Rightarrow |2| = 4$ // $(\because 2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1)$

3/3 $\therefore LCM(6,4) = 12 \Rightarrow |(5,2)| = 12$ //

(ii) (6 points). Construct two subgroups of D, say H_1 and H_2, such that each has 4 elements and $H_1 = F_1 \times F_2$, $H_2 = L_1 \times L_2$ for some subgroups F_1, L_1 of $(Z_6, +)$ and some subgroups F_2, L_2 of $(Z_5^*, .)$.

$H_1 = F_1 \times F_2$, $H_2 = L_1 \times L_2$.

— Constructing H_1:

$\boxed{\text{Pick } F_1 = \{0,3\},\ F_2 = \{1,4\}}$. Note: $F_1 < Z_6$, $F_2 < Z_5^*$

6/6 $\therefore F_1 \times F_2 < (Z_6, +) \times (Z_5^*, *) \Rightarrow H_1 = F_1 \times F_2 < D$ (by Theorem: $A < X, B < Y \Downarrow A \times B < X \times Y$)

$|H_1| = 2 * 2 = 4$ ✓

— Constructing H_2:

$\boxed{L_1 = \{0\},\ L_2 = \mathbb{Z}_5^*}$ $\therefore L_1 \times L_2 < D_2$ $\because L_1 < \mathbb{Z}_6$, $L_2 < \mathbb{Z}_5^*$

$\therefore H_2 = L_1 \times L_2 < D_2$ //

(iii) (3 points) Convince me that D does not have an element of order 24.

3/3 $|D| = 24$. In other words we show D is NOT Cyclic.
($\therefore$ It cannot have element of ~~order~~ 24)

Maximum possible Order of an Element in D:

Let $\mathbb{Z}_6 = <a>$, $(\mathbb{Z}_5^*, *) = <b>$ (They are both cyclic)

But $gcd(|a|,|b|) = gcd(6,4) = 2$

$\therefore |(a,b)| = LCM(|a|,|b|) = \frac{|a||b|}{gcd(|a|,|b|)}$ $\therefore |(a,b)| = 12$ at max $\Rightarrow$ NEVER Cyclic

(iv) (4 points). Construct a subgroup of D, say H, such that H has 4 elements, but there is no subgroup N_1 of $(Z_6, +)$ and there is no subgroup N_2 of $(Z_5^*, .)$ such that $H = N_1 \times N_2$.

~~Consider $H = \{(0,1), (2,3), (3,4), (5,2)\}$~~

	(0,1)	(2,3)	(3,4)	(5,2)
(0,1)	(0,1)	(2,3)	(3,4)	(5,2)
(2,3)	(2,3)			
(3,4)	(3,4)			
(5,2)	(5,2)			

H must Contain Identity

$\therefore (0,1) \in H$.

Consider Subgroups ~~(non trivial)~~:

$(\mathbb{Z}_6, +)$: $\{0,3\}$, $\{0,2,4\}$, $\{0,1,2,3,4,5\}$; $\{0\}$

$(\mathbb{Z}_5^*, *)$: $\{1,4\}$, $\{1,2,3,4\}$, $\{1\}$

$\therefore$ We must form a group which is not $\{0,3\} \times \{1,4\}$.

See page 10/13

QUESTION 3. (i) **(4 points).** Is $(Z_7^*, .)$ group-isomorphic to $(U(9), .)$? If yes, then prove it. If no, then tell me why not?

YES:

$|Z_7^*| = 6$ and $Z_7^* = U(7)$. $\therefore \phi(7) = 7-1 = 6$

$|U(9)| = \phi(9) = 6$. $\therefore$ Both are CYCLIC and BOTH ORDERS $= 6$.

$\therefore$ Both are Isomorphic to $(\mathbb{Z}_6, +) \Rightarrow$ They are Isomorphic to each other.

4/4

(ii) **(4 points).** Is $(Z_{41}^*, .)$ group-isomorphic to $(U(75), .)$? If yes, then prove it. If no, then tell me why not?

NO. $(\mathbb{Z}_{41}^*, *) = (U(41), *)$ and 41 is prime $\therefore (\mathbb{Z}_{41}^*, *)$ is cyclic.

$U(75) = U(3*5^2)$ is not of the form $p^m, 2p^m, 2, 4$.

$\therefore U(75)$ is NOT Cyclic.

4/4

(iii) **(6 points).** Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 9 & 8 & 2 & 6 & 5 & 1 \end{pmatrix} \in S_9$. Find $|f|$. Is $f \in A_9$? explain

$f = (1\ 3\ 4\ 9)(2\ 7\ 6)(5\ 8)$. (Disjoint)

$\therefore |f| = LCM(4,3,2) = 12$.

Rewrite f:

$f = (1\ 9)\circ(1\ 4)\circ(1\ 3)\circ(2\ 6)\circ(2\ 7)\circ(5\ 8)$

$= 6$ 2-Cycles. $\therefore f \in A_9$. It is Even because it is compose of 6 2-Cycles.

(iv) **(6 points).** Let $(D, *)$ be a group. Assume that $a * b = b * a$ for some $a, b \in D$, $|a| = n$, and $|b| = m$. Let $u = lcm[n, m]$. Prove that D has a cyclic subgroup with u elements. (Hint: You may need the fact: if $d = gcd(n, m)$, then $gcd(\frac{n}{d}, m) = 1$ OR $gcd(n, \frac{m}{d}) = 1$).

$a, b \in D$. $a*b = b*a$. $|a| = n$, $|b| = m$, $u = lcm(n, m)$

We prove: $\exists\ x \in D$ st $|x| = u$. $\therefore \langle u \rangle$ is our Subgroup

Case I: $gcd(m, n) = 1$.

Then $|a*b| = |a||b| = \alpha u$ for some α.

0/6

Then $|\langle a*b \rangle| = \alpha u \Rightarrow \exists$ a Subgroup (Unique) of order u inside this. $\because u | (\alpha u)$

Case II: $gcd(m, n) = d$.

Note: $m n = d u$

$\longleftarrow$ (Contd. on previous Page)

see page 13/13

QUESTION 4. (i) **(6 points)**. Is there a group-homomorphism $f : (Z_{18}, +) \to (Z_9, +)$ such that f is nontrivial and f is not ONTO? If yes, then construct such f and find $Range(f)$ and $Ker(f)$. If such f does not exist, EXPLAIN.

$|Range(f)| \mid |\mathbb{Z}_9|$ and $|Range(f)| \mid |\mathbb{Z}_{18}|$ $\therefore |Range(f)|$ divides 9 and 18.

6/6

$\therefore |Range(f)| = 3$ $\because$ NOT ONTO.

$|\mathbb{Z}_9/Ker(f)| \cong Range(f) \Rightarrow \frac{|\mathbb{Z}_9|}{|Ker(f)|} = 3 \Rightarrow |Ker(f)| = 6$

Since $\mathbb{Z}_9$, $\mathbb{Z}_{18}$ are cyclic, they have unique cyclic subgroups of order 3, 6 : $<1^{\frac{9}{3}}>$ and $<1^{18/6}>$.

Contd. on previous page. See page 11/13

(ii) **(6 points)**. Let $(D, *)$ be a group with 155 elements. Assume that H is a normal subgroup of D with 5 elements. If $a \in D \setminus H$ and $|a| \neq 31$, prove that D is cyclic. Prove that H is the only subgroup of D with 5 elements.

$|D| = 155 = 5 * 31$. $H \triangleleft D$, $|H| = 5$.

Deny. $\therefore \exists N < D$ st $|N| = 5$. $(N \neq H)$

$\therefore NH < D$ (By Homework) and $|NH| = \frac{|N||H|}{|N \cap H|}$

But $N \cap H = \{e\}$ by assumption $\Rightarrow |NH| = 25$.

But $25 \nmid 155$. (By Lagrange, we cannot have a subgroup of order 25). $\therefore N$ does not exist

see page 12/13 (PTO)

(iii) **(Bonus 7 points)**. Let H be a subgroup of a group $(D, *)$. Assume that for each $a \in D \setminus H$, we have $x_1 * x_2 * x_3 * x_4 \in a * H$ for every $x_1, x_2, x_3, x_4 \in a * H$ (note that $x_1, ..., x_4$ need not be distinct). Prove that H is a normal subgroup of D.

see page 4/13

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

Q1(iii) Continues

$$= a_k^{x+y} * c_1 * c_2$$

$$= a_k^{y+x} * c_2 * c_1$$

$$= a_k^{y} * a_k^{x} * c_2 * c_1$$

$$= a_k^{y} * c_2 * a_k^{x} * c_1$$

$$= a_2 * a_1$$

$\therefore a_1 * a_2 = a_2 * a_1 \quad \forall\, a_1, a_2 \in D$

D is Abelian.

If $L = N_1 \times N_2 \Rightarrow N_2 = Z_5^*$, and $|N_1| \geq 2$
$\Rightarrow |L| \geq 8$, Impossible since $|L| = 4$

Let $x = (3,2) \Rightarrow |x| = 4$.

Q2 (iv) $\rightarrow$

$H = \{(0,1),$ ~~(1,2), (4,4), (2,2~~ ~~(3,2) (0,4), (0,3)~~

Now $\{x, x^2, x^3, x^4 = (0,1)\} \leq \{(3,2), (0,4), (3,3), (0,1)\} = L$

Should have structure: $\{e, a, b, ab\}$.

But $a^{-1} = ab \Rightarrow (a^2)^{-1} = b$.

and $(b^2)^{-1} = a$.

not clean!

$\longrightarrow \therefore a^2 = e$ (or) $a^2 = b$ (or) $a^2 = ab$.

~~Makes it Cyclic~~

Q4(i) continues

$\therefore$ If such a homomorphism Exists:

Range $(f) = \{0, 3, 6\}$

Ker $(f) = \{0, 3, 6, 9, 12, 15\}$

we want to maintain that $|f(a)| \,|\, |a|$
and $f(a^{-1}) = [f(a)]^{-1}$

$\therefore$ Possible orders of remaining elements in $\mathbb{Z}_{18}$:
$2, 3, 6, 9, 18$

clearly: $f(1) = 3$. (generator to generator).

In all cases $|f(a)| = 3$.

$\therefore$ Only problem can arise when $|a| = 2$ in $\mathbb{Z}_{18}$.
This never happens $\because$ only $|9|$ in $\mathbb{Z}_{18}$ is 2
and it is mapped to e_2.

$\therefore f(1) = 3$

and $f(1^i) = 3^i \pmod 6$.

checking for homomorphism:

$f(a*b) = f(1^i * 1^j) = f(1^{i+j})$

$= 3^{i+j} \mod 6$

$= 3^i * 3^j$ ~~mod~~

$= f(1^i) * f(1^j)$ $(* = +_6)$.

Q4(ii) continues

$\therefore$ ~~H~~ H is Unique.

Part II:

To Prove: $|a| \neq 31 \Longrightarrow$ D is Cyclic

$|D| = 155$.

Let $a \in D$.

$|a| = \underbrace{1}_{\downarrow \text{ Identity}}$ (or) $\underbrace{5}_{\downarrow \text{ Elements in } H}$ (or) $\underbrace{31}_{\downarrow \text{ NONE}}$ (or) 155

($\because$ H is Unique)

So we have 4 elements of order 5.

$\therefore \exists$ 150 elements in D s.t ~~for~~ their order is 155.

Pick any one, call it 'a'.

$|a| = 155 = |D|$

$\Downarrow$

D is Cyclic ■

Q3(iv) Continues

Strategy:

Find an element of order $\frac{n}{d}$

and an element of order m $(=b)$

Then $\gcd\left(\frac{n}{d}, m\right) = 1 \implies$ we can use same process as Case I.

a^m will do:

$\because |a| = n \implies$ ~~fat~~ $|a^m| = \frac{n}{\gcd(m,n)} = \frac{n}{d}$

$\therefore$ Our generator is : $a^m * b$.

- $a * b = b * a \implies a^m * b = b * a^m$.
- $\gcd\left(\frac{n}{d}, m\right) = 1$.

$\therefore |a^m * b| = |a^m||b| = \left(\frac{n}{d}\right)(m) = u$.

$\therefore H = \langle a^m * b \rangle$

i.e $\langle a^{|b|} * b \rangle$ and $|H| = u$

■