Name TAHA AMEEN, ID @00066555

HW One: Abstract Algebra, MTH 320,Fall 2017

Ayman Badawi

24/25

QUESTION 1. examples of groups

(i) Let $D = \{(a,b)|a \in \{1,7\}$ and $b \in \{0,2,4,6\}\}$. Define * on D such that for every $(x_1,y_1),(x_2,y_2) \in D$ we have $(x_1,y_1)*(x_2,y_2) = (x_1 \cdot x_2, x_1 \cdot y_2 + x_2 \cdot y_1)$, where $\cdot$ means multiplication module 8 and + means addition module 8. Construct the Caley's table for (D, *). Now by staring at the table, you should conclude that D is an abelian group. Note that D is associate since $(Z_8,\cdot)$ and $(Z_8,+)$ are associate (so no need to check that unless you insist!).

a. What is $e \in D$?

b. If $a = (7,4) \in D$, then what is a^{-1}?

c. If $a = (1,6) \in D$, then what is a^{-1}?

d. If $a = (1,2) \in D$, then what is $|a|$?

(ii) Let $D = \{6,12,18,24\}$. Define * on D such that for every $a,b \in D$ we have $a*b = a \cdot b$, where $\cdot$ means multiplication module 30. Construct the Caley's table of $(D,\cdot)$. By staring at the table you should conclude that $(D,\cdot)$ is an abelian group (Since $(Z_{30},\cdot)$ is associate, we conclude that $(D,\cdot)$ is associate).

a. What is $e \in D$?

b. Let $a = 12$ What is $|a|$?.

c. Let $k = |12|$, find a^2, a^3, a^4. What can you conclude about $\{a,a^2,a^3,a^4\}$

d. Let $k = |24|$, find a^2, a^3, a^4 . Is this different from (c)?

(iii) Give me an example of a group $(D,*)$ such that D has an element $a \in D$ where $a^2 * b = b * a^2$ for every $b \in D$, but $a*c \neq c*a$ for some $c \in D$.[Hint: There are many examples, for example let $D = \{f : \mathbb{R} \to \mathbb{R}$ such that f is continuous and bijective$\}$, and let $* = o$. From class notes we know that (D,o) is monoid. Since every f in D is bijective, we conclude that $f^{-1} \in D$ for every $f \in D$. Hence (D,o) is a non-abelian group, now find a and c in D]

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

We construct Cayley's Table for $(D, *)$

$*$	(1,0)	(1,2)	(1,4)	(1,6)	(7,0)	(7,2)	(7,4)	(7,6)
(1,0)	(1,0)	(1,2)	(1,4)	(1,6)	(7,0)	(7,2)	(7,4)	(7,6)
(1,2)	(1,2)	(1,4)	(1,6)	(1,0)	(7,6)	(7,0)	(7,2)	(7,4)
(1,4)	(1,4)	(1,6)	(1,0)	(1,2)	(7,4)	(7,6)	(7,0)	(7,2)
(1,6)	(1,6)	(1,0)	(1,2)	(1,4)	(7,2)	(7,4)	(7,6)	(7,0)
(7,0)	(7,0)	(7,6)	(7,4)	(7,2)	(1,0)	(1,6)	(1,4)	(1,2)
(7,2)	(7,2)	(7,0)	(7,6)	(7,4)	(1,6)	(1,4)	(1,2)	(1,0)
(7,4)	(7,4)	(7,2)	(7,0)	(7,6)	(1,4)	(1,2)	(1,0)	(1,6)
(7,6)	(7,6)	(7,4)	(7,2)	(7,0)	(1,2)	(1,0)	(1,6)	(1,4)

4/4

(a) $\underline{e = (1,0)}$ $\because (1,0) * a = a * (1,0) = a \;\forall\; a \in D.$

(b) $a = (7,4) \Rightarrow \underline{a^{-1} = (7,4)}$ $\because (7,4) * (7,4) = (1,0) = e.$
(From Cayley's Table)

(c) $a = (1,6) \Rightarrow \underline{a^{-1} = (1,2)}$ $\because (1,6) * (1,2) = (1,2) * (1,6) = (1,0)$
(From Cayley's Table)

(d) $a = (1,2)$. By construction

8/8

$a * a = (1,2) * (1,2) = (1,4)$

$a^3 = (1,4) * (1,2) = (1,6) \quad | \because a^3 = a^2 * a$

$a^4 = (1,6) * (1,2) = (1,0) \quad | \because a^4 = a^3 * a$

$\therefore a^4 = (1,0) = e$ and 4 is the smallest positive Integer such that this is True.

$\therefore |a| = |(1,2)| = \underline{4}.$

) we construct Cayley's Table for $(D, *)$

$*_{30}$	6	12	18	24
6	6	12	18	24
12	12	24	6	18
18	18	6	24	12
24	24	18	12	6

4/4

(a) $\underline{\underline{e = 6}}$ $\because 6 * a = a * 6 = a \quad \forall\ a \in D.$

i.e. $6 *_{30} a = a *_{30} 6 = a \quad \forall\ a \in D.$

(b) $a = 12.$

$$a^2 = a * a = 12 *_{30} 12 = 24$$
$$a^3 = a^2 * a = 24 *_{30} 12 = 18$$
$$a^4 = a^3 * a = 18 *_{30} 12 = 6$$

8/8

since 4 is the smallest positive integer 'n' such that $a^n = e = 6$, $\underline{\underline{|a| = 4}}$.

(c) $a = 12.$ $k = |a| = |12| = 4.$

From (b) above: $a^2 = 24$, $a^3 = 18$, $a^4 = 6$

$\therefore \{a, a^2, a^3, a^4\} = \{12, 24, 18, 6\} = \{6, 12, 18, 24\} = D.$

we get 'D' back.

$\therefore \{a, a^2, a^3, a^4\}$ is a group with Order 'k' $= 4$.

(d) $a = 24.$

$$\Rightarrow a^2 = a * a = 24 * 24 = 6$$
$$a^3 = a^2 * a = 6 * 24 = 24$$
$$a^4 = a^3 * a = 24 * 24 = 6$$

$\{a, a^2, a^3, a^4\} = \{24, 6, 24, 6\} = \{6, 24\}$ | $\because$ we do not repeat elements in a set.

→ This is a group with 2 elements. Also, $k = |a| = 2$.

$*_{30}$	6	24
6	6	24
24	24	6

→ This is different from (c) in the sense that there are only 2 elements and not 4.

→ However, here $k = |a| = 2$ and the order of the finite group is 2.

(iii) Example 1: Consider $D = \{ f : R \to \mathbb{R} \mid f$ is Continuous & Bijective$\}$

$* = \circ$ (function composition)

It is clear that D is a group with operation '$\circ$'.

Let: $a : a(x) = -x$ $\quad$ $b : b(x) \in D$ is any function in D.

$c : c(x) = 2^x$ $\cancel{\in} D$?! take $c(x) = x+1$

not in D

Then: $a^2 * b = a * a * b = (a * a) * b$ [Groups are Associative]

$= e * b = b$.

and $b * a^2 = b * a * a = b * (a * a)$

$= b * e = b$ [$\because a * a = a(a(x)) = a(-x) = -(-x)$

$= x = e$].

M/3

$\therefore a^2 * b = b * a^2 \;\forall\, b \in D$.

However: $a * c = a(c(x)) = a(\cancel{2^x}\,x+1) = \cancel{-2^x} -x-1$

$c * a = c(a(x)) = c(-x) = \cancel{2^{-x}} -x+1$

$\cancel{\because}$?!

$\therefore \exists\, c \in D$ s.t $a * c \neq c * a$.

~~Example 2: $(D, *) = (U(R^{2\times2}), \times)$~~

~~$a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $c = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. $a \neq e$. But $a^2 = e$~~

~~$\therefore a^2 * b = e * b = b$ and b~~

Name TAHA AMEEN , ID @00066555

HW One: Abstract Algebra, MTH 320, Fall 2017

Ayman Badawi

$\frac{4}{4}$

QUESTION 1. Consider the following subsets of $(Z_8, +)$: $H_0 = 0 + \{0,4\} = \{0,4\}$, $H_1 = 1 + \{0,4\} = \{1,5\}$, $H_2 = 2+\{0,4\} = \{2,6\}$, $H_3 = 3+\{0,4\} = \{3,7\}$ Let $D = \{H_0, H_1, H_2, H_3\}$. Define $*$ on D such that $H_i * H_k = (i+k)+H_0$, where $+$ means addition module 8. Construct the Caley's table of $(D,*)$. Stare at the table, you should conclude that $(D,*)$ is an abelian group. [note that $(D,*)$ is associate since $(Z_8,+)$ is associative]. Find e. For each $d \in D$ find d^{-1}. [Comments: observe What is $H_i \cap H_k$, i $\neq k$? where $0 \le i, k \le 3$. What is $H_0 \cup H_1 \cup H_2 \cup H_3$?] $\frac{5}{5}$

QUESTION 2. (i) Let $(D,*)$ be a group and $a, b \in D$. What is $(a*b)^{-1}$? Prove your claim. $\frac{4}{4}$

(ii) Let $(D,*)$ be a group such that $x^2 = e$ for every $x \in D$. Prove that D is abelian $\frac{4}{4}$

(iii) Let $n \ge 2$ be a positive integer. Recall that $U(n) = \{a \in Z_n^* | gcd(a,n) = 1\}$. We know that $|U(n)| = \phi(n)$. Prove that $(U(n), .)$ is a group[Note that we proved in class that $(Z_n^*), .)$ is a group if and only if n is prime, so use similar proof and the fact I gave you that if $gcd(a,n) = 1$, then $a^{\phi(n)} = 1 \; in Z_n$ (i.e., $a^{\phi(n)} \equiv 1 \; (mod\; n)$) $\frac{4}{4}$

(iv) Let $k = |U(9)|$. What is k? Is there an element in $U(9)$ that has order k? if yes find such one. $\frac{4}{4}$

(v) Let $k = |u(8)|$. What is k? Is there an element in $U(8)$ that has order k? if yes find such one. $\frac{4}{4}$

QUESTION 3. (i) Let $(D,*)$ be a group and fix $a, b \in D$. Convince me that the equation $a * x = b$ has a unique solution in D. What is the solution? $\frac{4}{4}$

(ii) Let (D_n, o) be the symmetric group on $n - gon$. We know that $|D| = 2n$ (note that $n \ge 3$ is a positive integer). Fix $a, b, c \in D_n$, where a is a rotation, b and c are reflection.

a. Prove that $b \; o \; a$ is a reflection.[Your proof should not exceed 2 lines]. $\frac{4}{4}$

b. ((a) and (i) might be helpful) Let $R = \{R_1, R_2, ..., R_n\}$ be the set of all rotations in D_n, Prove that $\{b \; o \; R_1, b \; o R_2,$ is the set of all reflections. [This is a nice result, it means in order to get all reflections, you only need to find one reflection, say b, and then just composite b with each rotation] $\frac{4}{4}$

c. Prove that $b \; o \; c$ is a rotation (note b, c are reflections)[Remember that Yousef claimed that!. Now in view of (i) and (b), you should give an Algebraic-Proof that should not exceed 3 lines] $\frac{4}{4}$

d. Consider (D_5, o). Let $R_1 = R_{72} = (1\;2\;3\;4\;5)$, $b = (Re)_1 = (2\;5)(3\;4)$ be a reflection. Note that $R_2 = R_1^2 = R_1 \; o \; R_1$, and in general $R_i = R_1^i = R^{i-1} \; o R_1 = R_{i-1} \; o \; R_1$. So you can find all the rotations (without sketching!). Now use the idea in (b) to calculate all reflections.[I will mention more on Monday about this part] $\frac{4}{4}$

QUESTION 4. Let $(D,*)$ be a group and $a \in D$ such that $|a| = n < \infty$. Let m be a positive integer such that $gcd(m,n) = 1$. Prove that $|a^m| = n$. So if $|a| = 11$, what can you conclude about $|a^i|$, where $2 \le i \le 10$? $\frac{4}{4}$

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

EXCELLET

$\frac{53}{53}$

Answer 1) $D = \{H_0, H_1, H_2, H_3\} = \{\{0,4\},\{1,5\},\{2,6\},\{3,7\}\}$.

* Cayley's Table:

$*$	H_0 $\{0,4\}$	H_1 $\{1,5\}$	H_2 $\{2,6\}$	H_3 $\{3,7\}$
$H_0: \{0,4\}$	$\{0,4\}$	$\{1,5\}$	$\{2,6\}$	$\{3,7\}$
$H_1: \{1,5\}$	$\{1,5\}$	$\{2,6\}$	$\{3,7\}$	$\{0,4\}$
$H_2: \{2,6\}$	$\{2,6\}$	$\{3,7\}$	$\{0,4\}$	$\{1,5\}$
$H_3: \{3,7\}$	$\{3,7\}$	$\{0,4\}$	$\{1,5\}$	$\{2,6\}$

4/4

$H_i * H_k = (i +_8 k) +_8 H_0$. we use the fact that $\{a,b\} = \{b,a\}$.

→ It is clear from the table that $\underline{\underline{e = H_0 = \{0,4\}}}$.

1/1

Finding $d^{-1}\ \forall\ d \in D$:

d	d^{-1}
$\{0,4\}$	$\{0,4\}$
$\{1,5\}$	$\{3,7\}$
$\{2,6\}$	$\{2,6\}$
$\{3,7\}$	$\{1,5\}$

4/4

→ Observation:

$H_i \cap H_k = \phi \quad \forall\ 0 \le i,k \le 3$.

$\bigcup_{i=1}^{3} H_i = \{0,1,2,3,4,5,6,7\}$

$\therefore$ H_0, H_1, H_2, H_3 form a partition for Z_8.

Answer 2:

(i) Claim: $(a*b)^{-1} = b^{-1} * a^{-1}$

Proof: $(a*b)*(b^{-1}*a^{-1})$

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

$= a*e*a^{-1}$

$= a*a^{-1}$

$= e$.

4/4

$\therefore$ Since the Inverse is Unique,

$(a*b)^{-1} = b^{-1}*a^{-1}$. ∎

(ii) Given: $x^2 = e \ \forall \ x \in D$.

$x * x = e \Rightarrow x = x^{-1} \ \forall \ x \in D$ —— (1).

consider $a, b \in D$. $\therefore a * b \in D \because D$ is closed under '$*$'.

Good

4/4

$a * b = (a * b)^{-1}$ [From (1) Above]

$= b^{-1} * a^{-1}$ [From Q2(i)]

$= b * a$ [From (1) Above] ■

$\therefore$ D is Abelian.

(iii) consider $U(n) = \{a \in Z_n^* \mid gcd(a, n) = 1\}$.

To Prove: $U(n)$ is a group.

I. CLOSURE: Let $a, b \in U(n)$. $\therefore gcd(a,n) = gcd(b,n) = 1$.

$gcd(a,n) = 1$ and $gcd(b,n) = 1 \Rightarrow gcd(a \cdot b, n) = 1$

(Here, Mutiplication is normal). (Fact from Number Theory)

$gcd(a*b, n) = gcd(ab \bmod n, n) = gcd(ab, n) = 1$.

(By Euclidean Algorithm)

Since $gcd(a*b, n) = 1$, $a*b \in U(n) \ \forall \ a, b \in U(n)$

Hence, $U(n)$ is closed.

II. ASSOCIATIVITY: It is clear $\because U(n) \subseteq Z_n^* \subset Z$.

III. IDENTITY: $e = 1 \wedge e \in U(n) \because gcd(1, n) = 1 \ \forall \ n$.

IV. INVERSE: $gcd(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1$ (Fact)

4/4

$\therefore a^{\phi(n)} = 1 = e \ \forall \ a \in U(n)$.

Good

$a^{\phi(n)} = a^{1+\phi(n)-1} = a^1 * a^{\phi(n)-1} = e$

AND $a^{\phi(n)} = a^{\phi(n)-1+1} = a^{\phi(n)-1} * a^1 = e$.

[Note: $a^{\phi(n)-1} \in U(n) \because U(n)$ is closed as proved above].

$\therefore \exists \ a^{-1} = a^{\phi(n)-1} \in U(n) \ \forall \ a \in D(= U(n))$ ■

(iv) $U(9) = \{1,2,4,5,7,8\}$ and $k = |U(9)| = 6$.

YES. $\exists\ \underline{\underline{a=2}} \in U(9)$ s.t. $|a| = k = 6$. This is shown as follows:

$2^1 = 2$. $2^2 = 2*2 = 4$. $2^3 = 2^2 * 2 = 4*2 = 8$

$2^4 = 2^3 * 2 = 8*2 = 7$. $2^5 = 2^4 * 2 = 7*2 = 5$

$2^6 = 2^5 * 2 = 5*2 = \underline{\underline{1 = e}}$. $\therefore \underline{|2| = 6 = k}$.

Excellent!!

$\frac{4}{4}$

(v) $U(8) = \{1,3,5,7\}$ and $k = |U(8)| = 4$.

No.

$|a| \neq k\ \forall\ a \in U(8)$. This is shown as follows:

1: $|1| = 1$ (Identity Element)

3: $3^1 = 3$. $3^2 = 3*3 = 1 \Longrightarrow |3| = 2$.

5: $5^1 = 5$. $5^2 = 5*5 = 1 \Longrightarrow |5| = 2$.

7: $7^1 = 7$. $7^2 = 7*7 = 1 \Longrightarrow |7| = 2$.

$\therefore$ There is no element in $U(n)\big|_{n=8}$ of order 'k'.

$\frac{4}{4}$

Answer 3) (i) $(D,*)$ is a group and $a, b \in D$. We have to prove the existence and uniqueness of the solution to $a*x = b$.

DENY.

$\therefore \exists\ x_1, x_2 \in D$ s.t. $a * x_1 = a * x_2 = b$.

But, multiplying by a^{-1} from the left yields:

$$a^{-1} * a * x_1 = a^{-1} * a * x_2 = a^{-1} * b.$$

$$\therefore\ e * x_1 = e * x_2 = a^{-1} * b$$

$$\therefore\ x_1 = x_2 = a^{-1} * b.$$

$\frac{4}{4}$

$\therefore$ Since $x_1 = x_2$, the solution is Unique.

and the solution to $a*x = b$ is:

$$x = a^{-1} * b \quad \blacksquare$$

(iii) $(D_n, \circ)$ is the dihedral group of Order $2n$.

NOTE: I. We define $R = \{R_1, R_2, \ldots, R_n\}$ and $Re = \{(Re)_1, (Re)_2, \ldots, (Re)_n\}$

II. It is clear that $R \cup (Re) = D_n$ and $R \cap Re = \phi$.

III. Also, $|R| = |Re| = n$. $\therefore \forall\ 1 \le i, j \le n,\ i \ne j \Rightarrow R_i \ne R_j$

★ IV. $R < D_n$. Since R is a finite subset, it is sufficient to check closure, which is clear.

$\therefore (R, \circ) < (D_n, \circ)$ [R is a Subgroup of D_n].

(a): TWO LINE PROOF to Prove that $b \circ a$ is a Reflection : $b = d * a^{-1}$.

LINE 1: DENY. $\therefore b * a = d$ is assumed to be a rotation. Then, ~~$b = d * d$~~.

LINE 2: But $a^{-1}, d \in R$ and R is closed $\Rightarrow b \in R$. CONTRADICTION!

Excellent $\therefore d \notin R \Longrightarrow d \in (Re)$. ($\because$ of II Above). ■

4/4

(b): Using (a) Above: $\{b*R_1, b*R_2, \ldots, b*R_n\} \cap R = \phi$.

$\therefore \{b*R_1, b*R_2, \ldots, b*R_n\} \subseteq Re$.

Assume $b*R_i = b*R_j$ for some $i \ne j$.

Then $b^{-1}*b*R_i = b^{-1}*b*R_j \Rightarrow e*R_i = e*R_j \Rightarrow R_i = R_j$.

This is a contradiction because we know $R_i \ne R_j\ \forall\ i \ne j$ as $|R| = n$.

$\therefore b*R_i \ne b*R_j \quad \forall\ i \ne j$

$\therefore |\{b*R_1, b*R_2, \ldots, b*R_n\}| = n$ and $\{b*R_1, \ldots, b*R_n\} \subseteq Re$.

$\therefore \{b*R_1, b*R_2, \ldots, b*R_n\} = Re$ is the set of all Reflections. ■

(c): Using (a) and (b) above:

LINE 1: $b, c \in (Re) \Rightarrow \exists\ k \in R$ s.t. $c = b*k$. $\therefore b^{-1}*c = b^{-1}*b*k$

LINE 2: $\therefore b^{-1}*c = e*k = k \Rightarrow b^{-1}*c \in R$. [$\because k \in R$]

LINE 3: But, $b \in Re \Rightarrow |b| = 2 \Rightarrow b = b^{-1} \Rightarrow b^{-1}*c = b*c \in R$ ■

4/4

$\therefore b*c \in R \quad \forall\ b, c \in Re$.

(d) Consider $(D_5, \circ)$: $R_1 = (1\ 2\ 3\ 4\ 5) \wedge (Re)_1 = (2\ 5)(3\ 4)$

From (b): we have: $(Re)_k = (Re)_1 * R_k$

Using fact that: $R_k = R_{k-1} * R_1$,

$$(Re)_k = ((Re)_1 * R_{k-1}) * R_1$$

4/4

$\therefore (Re)_k = (Re)_{k-1} * R_1$. We use this result as follows:

$\rightarrow (Re)_2 = (Re)_1 \circ R_1 = (2\ 5)(3\ 4) \circ (1\ 2\ 3\ 4\ 5) = (1\ 5)(2\ 4)$

$\rightarrow (Re)_3 = (Re)_2 \circ R_1 = (1\ 5)(2\ 4) \circ (1\ 2\ 3\ 4\ 5) = (1\ 4)(2\ 3)$

$\rightarrow (Re)_4 = (Re)_3 \circ R_1 = (1\ 4)(2\ 3) \circ (1\ 2\ 3\ 4\ 5) = (1\ 3)(4\ 5)$

$\rightarrow (Re)_5 = (Re)_4 \circ R_1 = (1\ 3)(4\ 5) \circ (1\ 2\ 3\ 4\ 5) = (1\ 2)(3\ 5)$

$\{(Re)_1, (Re)_2, (Re)_3, (Re)_4, (Re)_5\}$ is the set of all Reflections for D_5. $\therefore Re = \{(2\,5)(3\,4), (1\,5)(2\,4), (1\,4)(2\,3), (1\,3)(4\,5), (1\,2)(3\,5)\}$

Answer 4) $|a| = n < \infty \Rightarrow a^n = e$ — (1)

Let $|a^m| = k \Rightarrow (a^m)^k = e$ — (2)

From (1) and (2): $(a^m)^k = e \Rightarrow a^{mk} = e$.

$$\therefore n \mid mk \Longrightarrow n \mid k \quad \because \gcd(m, n) = 1.$$

4/4

Further, $(a^n) = e \Rightarrow (a^n)^m = e^m = e$.

$$\therefore (a^m)^k = e \text{ and } (a^m)^n = (a^n)^m = e.$$

$\therefore k \mid n$ ($\because$ Order of $a^m = k$)

$n \mid k \wedge k \mid n \Longrightarrow n = k$.

$$\therefore |a^m| = k = n. \quad \therefore |a^m| = n$$

$\gcd(i, 11) = 1 \ \forall\ 2 \le i \le 10$. $\therefore |a| = 11 \Rightarrow |a^i| = 11 \ \forall\ 2 \le i \le 10$.

Ayah Bawadi, ID 72735

HW THREE: Abstract Algebra, MTH 320,Fall 2017

Ayman Badawi

QUESTION 1. (i) (Very useful result) Let $(D, *)$ be a group with $n < \infty$ elements and let $a \in D$. Prove that $a^n = e$ for every $a \in D$ [Max 3 lines proof]

(ii) (Nice problem) Let $(D, *)$ be a group such that $|D| = q_1q_2$ where q_1, q_2 are primes. Assume $a, b \in D$ such that $a^{22} = a^{15}$, $b^{43} = b^{32}$, and $a * b = b * a$. Find $|D|$. I claim that $D = \{c, c^2, ..., c^{q_1q_2} = e\}$ for some $c \in D$. Prove my claim.[Max 6 lines] $a \neq e$ $b \neq e$

QUESTION 2. (i) (How to check for subgroups) Let $(D, *)$ be an abelian group. Fix a positive integer m and let $F = \{a \in D \mid a^m = e\}$. Prove that $(F, *)$ is a subgroup of D. (Two lines proof. Note that F need not be a finite set. An example of an infinite F will be given during the course)

(ii) (How to check for subgroups) Fix a positive integer n. We know that the equation $x^n - 1 = 0$ has exactly n distinct solutions over the complex C. Now let $F = \{a \in C^* \mid a^n - 1 = 0\}$. Prove that $(F, .)$ is a subgroup of $(C^*, .)$ (Two lines proof. (Note that $(C*, .)$ is an abelian group)

QUESTION 3. (Radicals). Let $(D, *)$ be a group such that $|D| = n < \infty$. Let m be a positive integer such that $gcd(n, m) = 1$. Let $a \in D$. Prove that there exists an element $b \in D$ such that $b^m = a$ (i.e., $\sqrt[m]{a} \in D$, where $\sqrt[m]{a} = b \in D$ means $b^m = a$)(three lines proof. You may need the fact from number theory or discrete math that says if $gcd(m, n) = k$, then there are two integers w, x in Z such that $k = wm + xn$)

QUESTION 4. Given f_1, f_2, and f_3 are bijection functions on a set with 6 elements, where $f_1 = (3\ 5)$, $f_2 = (3\ 1\ 4\ 2)$, and $f_3 = (6\ 4\ 5\ 3)$

a) Find $f_1\ o\ f_3$

b) Find $f_2\ o\ f_1$

c) Find $f_3\ o\ f_2$

QUESTION 5. (i) Given $H = \{0, 4, 8\}$ is a subgroup of $(Z_{12}, +)$. Find all distinct left cosets of H in D.

(ii) Let $(D, *)$ be a group and assume that for some $a, b \in D$, we have $a * b = b * a$, $|a| = 9$ and $|b| = 8$

a. Find $|a^6|$

b. Find $|b^3|$

c. Find $|a^6 * b^3|$

d. Give me an element $c \in D$ such that $|c| = 36$ (note that, as I explained in the class, if a group has an element of order k, then the group must have a subgroup of order k, namely $H = \{a, a^2, ..., a^k = e\}$, where $|a| = k$. So if my claim is right, then D must have a subgroup with 36 elements)

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

Question 1: (i)

Let $(D, *)$ be agroup , $|D| = n$, $a \in D$.

prove that $\boxed{a^n = e}$

Proof :

Let $(D, *)$ be agroup , $|D| = n$, $a \in D$, wher $|a| \mid n$.

we want to show $a^n = e$.

Assume $|a| = k$. , since $k \mid n$ — why!

means $n = k * m$. $a^k = e$

$\Rightarrow$

$$a^n = a^{km}$$

$$= (a^k)^m$$

$$= (e)^m$$

$$\boxed{a^n = e}$$

$\therefore$ $\boxed{a^n = e}$

$H = \{a, a^2, \dots, a^k = e\}$ is a subgroup of D $\Rightarrow$ with $\underline{k}$ elements

$\xrightarrow{\text{Lagrange}}$ $k \mid n$ $\Rightarrow$ $a^n = e$

(ii) $|D| = q_1 q_2$, q_1 & q_2 are prime numbers.

$a^{22} = a^{15}$ $\Rightarrow$ means a^{15} is the inverse of a^{22}.

$a^{22} \cdot a^{-15} = a^{7} \Rightarrow e$ $\Rightarrow |a| = 7$

$b^{43} = b^{32}$ $\Rightarrow$ means $b^{43} * b^{-32} \Rightarrow b^{11} = e$. $\Rightarrow |b| = 11$

$a * b = b * a$ $\Rightarrow$ means the group D is abelian

Find $|D| = ??$ where $D = \{c_1, c_2, \text{----} c^{q_1 q_2} = e\}$

let $C = a * b$.

$|c| = |a * b|$

$|c| = |a| * |b|$ $\nearrow$ because the group of abelian.

$= 7 * 11$

$|c| = 77$

$\therefore$ $\boxed{|c| = 77}$

$c^{q_1 q_2} = e$ $\Leftarrow$ given.

(gcd between a, b $= 1$)

$|c| = q_1 q_2$ where q_1 & q_2 are primes

$|c| = 7 \cdot 11 = 77$ the $q_1 = 7$ & $q_2 = 11$.

$|c| = |D| = 77$ $\therefore$ $|D| = 77$.

Q2 (i) $(D,*)$ an abelian group , $F=\{a\in D \mid a^m=e\}$

prove $(F,*)$ is a subgroup.

let $a,b\in F$, we need to show $(a^{-1}*b)\in F$

$a^m=e$, $b^m=e$

we want to

Find $(a^{-1}*b)^m = ?$

$= (a^{-1})^m * (b)^m$ → because the group is abelian

$= (a^{-1})^m * e$

$= (a^m)^{-1} * e$

$\Downarrow$

$= (e)^{-1} * e$

$= \boxed{e}$

$\therefore (a^{-1}*b)\in F$

$\therefore$ F is a subgroup of D.

(ii) Question#(2) $x^n - 1 = 0$ has exactly n distinct solution over the Complex C. , $F = \{a \in C^* \mid a^n - 1 = 0\}$ prove $(F, \cdot)$ is a subgroup of $(C^*, \cdot)$. Note $(C^*, \cdot)$ is abelian group.

* The only axiom you need to check to proof that F is a subgroup from C is the clouser.

Proof: let $a, b \in F$

$$a^{n-1} = 0 \Rightarrow a^n = 1$$

$$b^n = 1.$$

We want to show that $(a*b)^n \in F$.

$$(a*b)^n$$

$$= a^n * b^n$$

$$= 1 * 1$$

$$= 1$$

$\therefore (a*b)^n \in F$

$\therefore$ F is a subgroup of C.

Question 3: $(D,*)$ be a group, $|D|=n$, $\gcd(n,m)=1$

$a^n = e$.

Let $a, b \in D$.

$|a| = k$

We need to show that $\boxed{b^m = a}$

$a^k = e$

$(\gcd(m,n)=k) \Rightarrow K = wm + xn$

$\boxed{K=1}$.

$$1 = wm + xn$$

$$a^1 = a^{wm+xn}$$

$$a = a^{wm} * a^{xn}$$

$$a = (a^w)^m * (a^n)^x$$

$$\Downarrow$$

$$e$$

$$a = (a^w)^m * e$$

let $b = a^w$

$$a = (b)^w * e.$$

$$\therefore a = (b)^w$$

Question # (4) Given f_1, f_2 & f_3. are bijection functions

$f_1 = (3\,5)$, $f_2 = (3\,1\,4\,2)$, $f_3 = (6\,4\,5\,3)$.

(a) $f_1 \circ f_3 = (3\,5)\circ(6\,4\,5\,3)$

$= (3\,6\,4)$

(b) $f_2 \circ f_1 = (3\,1\,4\,2)\circ(3\,5)$

$(1\,4\,2\,3\,5)$

(c) $f_3 \circ f_2 = (6\,4\,5\,3)\circ(3\,1\,4\,2)$

$= (1\,5\,3)(2\,6\,4)$

Question (5): $H = \{0,4,8\}$ subgroup of $(\mathbb{Z}_{12}, +)$

(i)

$L * H = ?$

$H_1 = 2 +_{12} \{0,4,8\} = \{2,6,10\}$

$H_2 = 3 +_{12} \{0,4,8\} = \{3,7,11\}$

$H_3 = 5 +_{12} \{0,4,8\} = \{5,9,1\}$

$L(H) = \{H_0, H_1, H_2, H_3\}$

+ The Trivial Coset $H_0 = \{0,4,8\}$

(ii) ⇒ Question (5)

$(D,*)$ is a group, $a \& b \in D$, we have $\underbrace{a*b=b*a}$

$|a|=9$, $|b|=8$.
The group is abelian

(a) $|a^6| =$ $m=6$. $n=9$ $= \dfrac{9}{\gcd(9,6=3)} = 3$ $|a^m| = \dfrac{n}{\gcd(m,n)}$

So, $\boxed{|a^6|=3}$

(b) $|b^3| \Rightarrow$ $m=3$ $n=8$ $\Rightarrow \dfrac{8}{\gcd(8,3=1)} = \dfrac{8}{1} = 8$

So, $\boxed{|b^3|=8}$

(c) Find $|a^6 * b^3| = |a^6| * |b^3| = 3*8 = 24$.

$\boxed{|a^6*b^3| = 24}$ $=$ $3*8=24$

(d) let $d \& g \in D$.
$c \in D$, $|c|=36$
$c = d*g$, let $|d|=9$, let $|g|=4$
$|c| = |d*g|$
$|c| = |d|*|g|$ → we will choose 2 numbers are relatively prime $\gcd=1$.
$36 = 9*4$,

According to the Result that we proved in the class which is
$a,b \in D$, $|a|=m$, $|b|=n$, $\gcd(m,n)=1$
then $|a*b| = nm$.
and if the group has an element with order 36 So, the subgroup must have an element with the same order $\underline{\underline{36}}$.

but $|d| = 9 = |a|$
and $|g| = 4 = |b^2| = \dfrac{|b|}{\gcd(2,|b|)} = \dfrac{8}{\gcd(2,8)} = \dfrac{8}{2} = 4$.

So, $|c| = |a*b^2|$
$c = a*b^2$.

ANSWER 1: (i) $|D| = n < \infty$. Let $a \in D$. $|a| = k \Rightarrow k|n$

$\therefore \exists\, q \in \mathbb{Z}$ s.t. $n = kq$ Lagrange Show that

$\therefore a^n = a^{kq} = (a^k)^q = e^q = e$. $\therefore a^n = e \;\forall\, a \in D$.

k elements $\{a, a^2, \ldots, a^k = e\} < D$ with

(ii) $|D| = n = q_1 q_2$ where q_1 and q_2 are prime.

$a^{22} = a^{15} \Rightarrow a^{-15} * a^{22} = a^{-15} * a^{15} \Rightarrow a^7 = e$. $\therefore |a|$ divides 7.

Since 7 is prime and $a \neq e$, $|a| = 7$.

Similarly, $b^{43} = b^{32} \Rightarrow b^{-32} * b^{43} = b^{-32} * b^{32} \Rightarrow b^{11} = e$. $\therefore |b|$ divides 11.

Since 11 is prime and $b \neq e$, $|b| = 11$.

$a, b \in D \Rightarrow |a|\,\big|\, n$ and $|b|\,\big|\, n$. $\therefore 7|n$ and $11|n$.

Since $n = q_1 q_2$ AND Prime Factorization is Unique,

$n = 7(11) = 77$. $\therefore |D| = 77$ //

Proof that $D = \{c, c^2, c^3, \ldots, c^{q_1 q_2} = e\}$ for some $c \in D$:

$\exists\, c = (a * b) \in D$. Since $\gcd(|a|, |b|) = \gcd(7, 11) = 1$

AND $a * b = b * a$, $|c| = |a||b| = 7(11) = 77 = q_1 q_2$

$\therefore$ Consider $L = \{c, c^2, c^3, \ldots, c^{77} = e\} \subseteq D$ and $|L| = q_1 q_2$

$\therefore L = D$. $c = a * b$.

ANSWER 2 (i) $(D, *)$ is Abelian. $F = \{a \in D \mid a^m = e\}$

To Prove: $a^{-1} * b \in F$.

$(a^{-1})^m = (a^m)^{-1} = e^{-1} = e \Longrightarrow a^{-1} \in F$.

Consider $b \in F$ [$\because b^m = e$]. $(a^{-1} * b)^m = (a^{-1})^m * (b)^m$

$= e * e = e$. //

This is only True because D is Abelian.

$\therefore a^{-1} * b \in F$. $\therefore F < D$.

(a) $|a^6| = \dfrac{|a|}{\gcd(6,|a|)} = \dfrac{9}{\gcd(6,9)} = \dfrac{9}{3} = 3$ //

(b) $|b^3| = \dfrac{|b|}{\gcd(3,|b|)} = \dfrac{8}{\gcd(3,8)} = \dfrac{8}{1} = 8$ //

(c) $|a^6 * b^3| = |a^6| * |b^3|$ $\left[\because \gcd(|a^6|,|b^3|) = \gcd(8,3) = 1 \right.$ AND D is Abelian $\left.\right]$

$= 8(3) = 24$ //

(d) CLAIM : $\exists\ c = a * b^2$ s.t. $|c| = 36$.

$\rightarrow$ $|a| = 9$ and $|b^2| = \dfrac{|b|}{\gcd(2,|b|)} = \dfrac{8}{2} = 4$.

$\rightarrow$ $\gcd(|a|, |b^2|) = \gcd(9,4) = 1$

$\rightarrow$ The Group is Abelian.

$\therefore$ ~~gcd~~ $|c| = |a * b^2| = |a| * |b^2| = 9(4) = 36.$

Hence, D does have a subgroup with 36 Elements.

(ii) $|F| = n < \infty \Rightarrow$ It is sufficient to check closure.

$F = \{a \in \mathbb{C}^* \mid a^n - 1 = 0\}$. Fix $a, b \in F$.

- $a \in F \Rightarrow a^n - 1 = 0 \Rightarrow a^n = 1$. Similarly, $b \in F \Rightarrow b^n = 1$.
- $a * b \Rightarrow (ab)^n - 1 = a^n b^n - 1$ ($\because$ Abelian Group).

$$= (1)(1) - 1 = 1 - 1 = 0 \,//$$

$\therefore a * b \in F \;\forall a, b \in F$. Hence $F < D$. ■

ANSWER 3: $|D| = n$. $a, b \in D \Rightarrow a^n = b^n = e$.

Consider: $a^1 = a^{wm + xn}$ ($\because \gcd(m,n) = 1 \Rightarrow \exists w, x \in \mathbb{Z}$ s.t $wm + xn = 1$)

$$= a^{wm} * a^{xn} = (a^w)^m * (a^n)^x = (a^w)^m * e^x.$$

$\therefore a = (a^w)^m$. $\exists b = a^w \in D$ s.t $a = b^m$ ■

ANSWER 4: $f_1 = (3\ 5)$, $f_2 = (3\ 1\ 4\ 2)$, $f_3 = (6\ 4\ 5\ 3)$

(a) $f_1 \circ f_3 = (3\ 5) \circ (6\ 4\ 5\ 3) = \underline{(3\ 6\ 4)}$

(b) $f_2 \circ f_1 = (3\ 1\ 4\ 2) \circ (3\ 5) = \underline{(1\ 4\ 2\ 3\ 5)}$

(c) $f_3 \circ f_2 = (6\ 4\ 5\ 3) \circ (3\ 1\ 4\ 2) = \cancel{(1\ 2\ 6\ 4}(1\ 5\ 3)(2\ 6\ 4)$

$\therefore f_3 \circ f_2 = \underline{(1\ 5\ 3)(2\ 6\ 4)}$

ANSWER 5 (i) We repeatedly choose $a \in D \setminus H_i$. $\underline{H_0 = \{0, 4, 8\}}$

$a = 1 \Rightarrow 1 * H = 1 * \{0, 4, 8\} = \{1, 5, 9\} = H_1$

$a = 2 \Rightarrow 2 * H = 2 * \{0, 4, 8\} = \{2, 6, 10\} = H_2$

$a = 3 \Rightarrow 3 * H = 3 * \{0, 4, 8\} = \{3, 7, 11\} = H_3$

$\therefore L(H) = \{H_0, H_1, H_2, H_3\} \,//$

(ii) $a * b = b * a$. $|a| = 9$, $|b| = 8$.

Name TAHA AMEEN , ID @000 66 555

HW THREE: Abstract Algebra, MTH 320,Fall 2017

$\frac{56}{60}$

Ayman Badawi

QUESTION 1. (i) (Very useful result) Let $(D, *)$ be a group with $n < \infty$ elements and let $a \in D$. Prove that $a^n = e$ for every $a \in D$ [Max 3 lines proof]

(ii) (Nice problem) Let $(D, *)$ be a group such that $|D| = q_1q_2$ where q_1, q_2 are primes. Assume that for some $a, b \in D$, where $a \neq e$ and $b \neq e$, we have $a^{22} = a^{15}$, $b^{43} = b^{32}$, and $a * b = b * a$. Find $|D|$. I claim that $D = \{c, c^2, ..., c^{q_1q_2} = e\}$ for some $c \in D$. Prove my claim.[Max 6 lines]

QUESTION 2. (i) (How to check for subgroups) Let $(D, *)$ be an abelian group. Fix a positive integer m and let $F = \{a \in D \mid a^m = e\}$. Prove that $(F, *)$ is a subgroup of D. (Two lines proof. Note that F need not be a finite set. An example of an infinite F will be given during the course)

(ii) (How to check for subgroups) Fix a positive integer n. We know that the equation $x^n - 1 = 0$ has exactly n distinct solutions over the complex C. Now let $F = \{a \in C^* \mid a^n - 1 = 0\}$. Prove that $(F, .)$ is a subgroup of $(C^*, .)$ (Two lines proof. (Note that $(C*, .)$ is an abelian group)

QUESTION 3. (Radicals). Let $(D, *)$ be a group such that $|D| = n < \infty$. Let m be a positive integer such that $gcd(n, m) = 1$. Let $a \in D$. Prove that there exists an element $b \in D$ such that $b^m = a$ (i.e., $\sqrt[m]{a} \in D$, where $\sqrt[m]{a} = b \in D$ means $b^m = a$)(three lines proof. You may need the fact from number theory or discrete math that says if $gcd(m, n) = k$, then there are two integers w, x in Z such that $k = wm + xn$)

QUESTION 4. Given f_1, f_2, and f_3 are bijection functions on a set with 6 elements, where $f_1 = (3\ 5)$, $f_2 = (3\ 1\ 4\ 2)$, and $f_3 = (6\ 4\ 5\ 3)$

a) Find $f_1\ o\ f_3$

b) Find $f_2\ o\ f_1$

c) Find $f_3\ o\ f_2$

QUESTION 5. (i) Given $H = \{0, 4, 8\}$ is a subgroup of $(Z_{12}, +)$. Find all distinct left cosets of H in D.

(ii) Let $(D, *)$ be a group and assume that for some $a, b \in D$, we have $a * b = b * a$, $|a| = 9$ and $|b| = 8$

a. Find $|a^6|$

b. Find $|b^3|$

c. Find $|a^6 * b^3|$

d. Give me an element $c \in D$ such that $|c| = 36$ (note that, as I explained in the class, if a group has an element of order k, then the group must have a subgroup of order k, namely $H = \{a, a^2, ..., a^k = e\}$, where $|a| = k$. So if my claim is right, then D must have a subgroup with 36 elements)

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

Name IAHA AMEEN, ID 66555

HW Four Abstract Algebra, MTH 320,Fall 2017

Ayman Badawi

QUESTION 1. Consider the group $D = (\frac{Q}{Z}, \triangle)$, as usual for every $a, b \in Q$ we have $(a + Z))\triangle(b + Z) = (a + b) + Z$

(i) We know $x = \frac{8}{12} + Z \in D$. Find $|x|$.

(ii) Let $F = \{y \in D \mid |y| = 12\}$. Find $|F|$.

(iii) Fix an integer $m \in N^*$ and let $F = \{y \in D \mid |y| = m\}$. Can you guess what is $|F|$?

(iv) For each $n \in N^*$, construct a subgroup of D with n elements.

QUESTION 2. Let $(D, *)$ be a group with 12 elements and suppose that $D = \{a, a^2, ..., a^{12} = e\}$ (note that D must be abelian). Let $H = \{a, a^4, a^8\}$.

(i) Construct the Caley's table of H to convince me that it is a subgroup of D.

(ii) So now we know that $H \triangleleft D$. Find all elements of D/H. Construct the Caley's table of $(D/H, \triangle)$.

(iii) For each $x \in D/H$, find $|x|$.

QUESTION 3. Let $D = (U(15), .)$. It is trivial to notice that $H = \{1, 14\} \triangleleft D$. Construct the Caley's table of $(\frac{D}{H}, \triangle)$

QUESTION 4. Let $(D, *)$ be a group, $H \triangleleft D$, and $a \in D$. Suppose that $|a| = n < \infty$. We know that $x = a * H \in D/H$. Let $m = |x|$. Prove that $m \mid n$. (Max 2 lines proof. Note that x^k mean $a * H \triangle a * H \triangle \cdots \triangle a * H = a^k * H$)

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

50/50

(1) $D = (\mathbb{Q}/\mathbb{Z}, \Delta)$

(i) $x = \frac{8}{12} + \mathbb{Z}$. To find: $|x|$

$$|x| = \frac{12}{\gcd(8,12)} = \frac{12}{4} = 3.$$

(Verification):

$x^1 = \frac{8}{12} + \mathbb{Z}$. $\quad x^2 = (\frac{8}{12} + \mathbb{Z}) \Delta (\frac{8}{12} + \mathbb{Z}) = \frac{16}{12} + \mathbb{Z}$.

$$x^3 = x^2 \Delta x = (\frac{16}{12} + \mathbb{Z}) \Delta (\frac{8}{12} + \mathbb{Z}) = \frac{24}{12} + \mathbb{Z} = 2 + \mathbb{Z} = \mathbb{Z}$$

(ii) $F = \{y \in D \mid |y| = 12\}$. To find: $|F|$

- We use fact: $\forall y = \frac{p}{q} + \mathbb{Z}$ $(q \neq 0)$, $|y| = \frac{q}{\gcd(p,q)} = 12$
- Clearly, $F = \{\frac{1}{12} + \mathbb{Z}, \frac{5}{12} + \mathbb{Z}, \frac{7}{12} + \mathbb{Z}, \frac{11}{12} + \mathbb{Z}\}$.
- The numerators are relatively prime. $\therefore \gcd = 1 \Rightarrow |y| = 12$.
- Although $|\frac{2}{24} + \mathbb{Z}| = 12$, etc. $\frac{2}{24} + \mathbb{Z} = \frac{1}{12} + \mathbb{Z}$ and we do not repeat elements in a set. $\quad \therefore |F| = 4$.

(iii) $m \in \mathbb{N}^*$ and $F = \{y \in D \mid |y| = m\}$. What is $|F|$?

- It is clear that $F = \{\frac{p}{m} + \mathbb{Z} \mid \gcd(p, m) = 1\}$.
- $\therefore |F| = |U(m)| = \phi(m)$.

(iv) Consider $n \in \mathbb{N}^*$. We wish to construct a subgroup of order n.

- If we can find an element of order 'n', we are done.
- Clearly, $\frac{1}{n} + \mathbb{Z} \in D$. and $|\frac{1}{n} + \mathbb{Z}| = n$ $\because \gcd(1,n) = 1 \; \forall n$.

$\therefore \forall n \in \mathbb{N}^* \quad \exists H = \{(\frac{1}{n} + \mathbb{Z}), (\frac{1}{n} + \mathbb{Z})^2, \dots (\frac{1}{n} + \mathbb{Z})^n = e\} < D$

- This reduces to :

$\forall n \in \mathbb{N}^{+} \quad \exists\ H = \left\{ \frac{1}{n} + \mathbb{Z}, \frac{2}{n} + \mathbb{Z}, \frac{3}{n} + \mathbb{Z}, \ldots, \underbrace{\frac{n}{n} + \mathbb{Z}}_{= 1+\mathbb{Z} = \mathbb{Z} = e} \right\} < D$

② $D = \{ a, a^2, a^3, \ldots, a^{12} = e \}$

$H = \{ a^4, a^8, a^{12} \}$

c i) Cayley's Table of H.

$*$	a^4	a^8	a^{12}
a^4	a^8	a^{12}	a^4
a^8	a^{12}	a^4	a^8
a^{12}	a^4	a^8	a^{12}

It is clear that H is a group with identity $e = a^{12}$.

$\therefore$ Since $H \subset D$ and H is a group, $H < D$.

(ii) Since D is Abelian : $H < D \implies H \lhd D$.

To find : D/H and Cayley's Table of $(D/H, \Delta)$

$H = H_0 = \{ a^4, a^8, a^{12} \}$. $\longrightarrow$ we repeatedly pick elements in D (a_k) but not in $\bigcup_{i=0}^{k-1} H_i$ to find H_k.

$H_1 = a_1 * H_0 = \{ a^5, a^9, a^1 \}$

$H_2 = a_2 * H_0 = \{ a^6, a^{10}, a^2 \}$ $\longrightarrow$ we have 4 cosets. This is as expected $\because \frac{|D|}{|H|} = \frac{12}{3} = 4$.

$H_3 = a_3 * H_0 = \{ a^7, a^{11}, a^3 \}$

Δ	H_0	H_1	H_2	H_3
H_0	H_0	H_1	H_2	H_3
H_1	H_1	H_2	H_3	H_0
H_2	H_2	H_3	H_0	H_1
H_3	H_3	H_0	H_1	H_2

* Sample calculation

$H_1 \Delta H_2 = (a^1 * H_0) \Delta (a^2 * H_0)$

$= (a^1 * a^2) * H_0$

$= a^3 * H_0$

$= H_3$ //.

(iii) To find: $\forall\, x \in D/H$, $|x|$:

• H_0: $|H_0| = 1$ $\because H_0 = e$.

• H_1: $H_1^2 = H_2$; $H_1^3 = H_2 \Delta H_1 = H_3$, $H_1^4 = H_0 = e$
$\therefore |H_1| = 4$

• H_2: $H_2^2 = H_2 \Delta H_2 = H_0 = e$.
$\therefore |H_2| = 2$

• H_3: $H_3^2 = H_2$; $H_3^3 = H_2 \Delta H_3 = H_1$; $H_3^4 = H_0 = e$.
$\therefore |H_3| = 4$

(3) $D = U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

• $H_0 = H = \{1, 14\} \triangleleft D$

• $H_1 = 2 * H_0 = \{2, 13\}$

• $H_2 = 4 * H_0 = \{4, 11\}$

• $H_3 = 7 * H_0 = \{7, 8\}$

Δ	H_0	H_1	H_2	H_3
H_0	H_0	H_1	H_2	H_3
H_1	H_1	H_2	H_3	H_0
H_2	H_2	H_3	H_0	H_1
H_3	H_3	H_0	H_1	H_2

→ It is clear from cayley's Table that $(D/H, \Delta)$ is a group with identity H_0.

(4) $H \triangleleft D$. $|a| = n < \infty$. $x = a * H \in D/H$, $|x| = m$

To Prove: $m \mid n$.

$|x| = m \Rightarrow x^m = e_\Delta = H$. If we can show that $x^n = e_\Delta$, then $m \mid n$.

$x^n = a^n * H = e * H = H$ $(\because |a| = n)$

$\therefore x^n = e_\Delta$ $\therefore m \mid n$.

Name TAHA AMEEN, ID @00066555

HW FIVE Abstract Algebra, MTH 320, Fall 2017

Ayman Badawi

5

QUESTION 1. a) Let $(D, *)$ be a group with a normal subgroup H. Assume that $a * h = h * a$ for every $a \in D$ and for every $h \in H$ (note that we can conclude that $h_1 * h_2 = h_2 * h_1$ for every $h_1, h_2 \in H$). Assume that D/H is cyclic. Prove that D is an abelian group. (max 6 lines)

10 5 b) Let $(D, *)$ be a group. Given $N \triangleleft D$ and $H < D$. Prove that $NH = \{nh \mid n \in N \text{ and } h \in H\}$ is a subgroup of D and if $H \triangleleft D$, then $NH \triangleleft D$. 5

5 **QUESTION 2.** Let $(D, *)$ be a group with 25 elements. Assume that D has a unique subgroup of order 5. Prove that D is cyclic. (Max 3 lines)

QUESTION 3. a) Convince me that $(C^*, .)$ is not cyclic. (Max 2 lines)

5 b) Convince me that $(Q^*, .)$ is not cyclic. (Max 2 lines)

5 c) Convince me that $(Q, +)$ is not cyclic. (Max 5 lines)

5 d) Is $U(18)$ cyclic? explain

5 e) Is $U(16)$ cyclic? explain

QUESTION 4. a) Prove that S_{17} has an abelian subgroup, say H, with 70 elements. Can you say more about H?

5 b) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 1 & 8 & 7 & 6 & 2 \end{pmatrix} \in S_8$. Find $|f|$. Is $f \in A_8$? explain

5 c) Let $n = max\{|f|$, where $f \in A_9\}$. Find the value of n.

5 d) Let $f \in S_n$ $(n \geq 3)$ be an odd function. Prove that $|f|$ is an even number. (Max one line (maybe 2 lines)

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

55/55

Answer 1) (a) Given: $(D, *)$ is a group. $H \lhd D$.

$a * h = h * a \quad \forall h \in H, \forall a \in D$.

D/H is cyclic

To Prove: D is Abelian, i.e. $a_1 * a_2 = a_2 * a_1 \;\; \forall a_1, a_2 \in D$

→ Consider $D/H = \{H_1, H_2, \dots, H_k, \dots\} = \langle H_k \rangle$ where $H_n = a_n * H$.

$\therefore \; D/H = \{H_k^1, H_k^2, H_k^3 \dots\} = \{a_k^1 * H, a_k^2 * H, a_k^3 * H, \dots\}$

$\therefore \; a_1 * H = a_k^x * H$

$a_2 * H = a_k^y * H$ for some $x, y \in \mathbb{Z}$.

$\therefore \; a_1 \in a_k^x * H$ and $a_2 \in a_k^y * H \implies a_1 = a_k^x * h_1, \; a_2 = a_k^y * h_2$

$$
\begin{aligned}
\therefore \; a_1 * a_2 = a_k^x * h_1 * a_k^y * h_2 &= a_k^x * a_k^y * h_1 * h_2 \\
&= a_k^{x+y} * h_1 * h_2 \\
&= a_k^{y+x} * h_2 * h_1 \quad (\because H \text{ is Abelian}) \\
&= a_k^y * a_k^x * h_2 * h_1 \\
&= a_k^y * h_2 * a_k^x * h_1 \\
&= a_2 * a_1 \quad \blacksquare
\end{aligned}
$$

5/5

(b) Given: $N \lhd D$, $H < D$.

To Prove: (I) $NH < D$, (II) $H \lhd D \to NH \lhd D$.

(I)

$NH = \{nh \mid n \in N \text{ and } h \in H\}$. We pick two arbitrary elements of NH: $\alpha = n_a h_b$, $\beta = n_c h_d$.

If $\beta^{-1} * \alpha \in NH$, $NH < D$.

5/5

$$
\begin{aligned}
\therefore \; \beta^{-1} * \alpha &= h_d^{-1} * \underline{n_c^{-1} * n_a} * h_b \\
&= h_d^{-1} * n_k * h_b \quad \Big| \; \because N \text{ is a group. } n_k \in N. \\
&= n_k * h_t * h_b \quad \Big| \; \because N \lhd D \Rightarrow n * h_1 = h_2 * n.
\end{aligned}
$$

$= n_k * h_m \quad | \because H$ is a group $\Rightarrow h_m \in H$

But $n_k * h_m \in NH$. $\therefore NH < D$ ■

(II) $H \lhd D \longrightarrow NH \lhd D$, let $a \in D$

$$a * NH = \{a * n_a h_b \mid n_a \in N \wedge h_b \in H\}$$
$$= \{a * n_a * h_b\} = \{n_c * a * h_b\} \quad | \because N \lhd D$$
$$= \{n_c * h_d * a \mid n_c \in N \wedge h_d \in H\} \quad | \because H \lhd D$$
$$= NH * a \quad \text{(By Definition)}$$

5/5

$\therefore NH \lhd D$ ■

Answer 02) $(D,*)$ is a group.

Given : $|D| = 25$. $\exists! \, H < D$ s.t $|H| = 5$

To Prove : D is Cyclic, i.e. $\exists \, a \in D$ s.t. $|a| = |D| = 25$.

Proof : $h \in H \Rightarrow |h| = 1$ (or) 5. $h \neq e \Rightarrow |h| = 5$.

$\therefore H = \langle h \rangle$ is Unique. —— (1).

Choose $a \in D \setminus H$. $|a| = 5$ (or) 25 $\because a \neq e$.

$|a| \neq 5 \because |a| = 5 \longrightarrow \langle a \rangle = A < D \wedge |A| = 5$
$A \neq H$ (Contradiction)

5/5

$\therefore |a| = 25 \Longrightarrow \langle a \rangle = D$. $\therefore$ D is Cyclic. ■

Answer 03: (a) To Show : $(\mathbb{C}^*, \cdot)$ is Not Cyclic.

Deny. $\therefore \exists \, a, a^{-1}$ s.t $\langle a \rangle = \langle a^{-1} \rangle = \mathbb{C}^*$. (Unique a, a^{-1}).

5/5 Then $\forall \, c \, (\neq a, a^{-1}) \in \mathbb{C}^*$, $|c| = \infty$.

But $\exists \, -1 \in \mathbb{C}^* \wedge i \in \mathbb{C}^*$ s.t $|-1| = 2 \wedge |i| = 4$.

Contradiction!

$\therefore (\mathbb{C}^*, \cdot)$ is not cyclic.

(b) $(\mathbb{Q}^*, *)$ is not cyclic.

Deny. $\therefore \exists!\ a, a^{-1}$ s.t. $\mathbb{Q}^* = \langle a \rangle = \langle a^{-1} \rangle$

$\Longrightarrow \forall c \neq e \in \mathbb{Q}^*, \ |c| = \infty.$

But $\exists (-1) \in \mathbb{Q}^*$ s.t $|-1| = 2$. contradiction!

5/5 $\therefore (\mathbb{Q}^*, *)$ cannot be cyclic.

(c) To show: $(\mathbb{Q}, +)$ is not cyclic.

Deny. $\therefore \exists!\ a, a^{-1}$ s.t. $\mathbb{Q} = \langle a \rangle = \langle a^{-1} \rangle$. 5/5

Case I: $a \neq 0$. $\frac{a}{2} \in \mathbb{Q}\ \forall a \in \mathbb{Q}$. $\left(\frac{a}{2} = \sqrt{a}\right)$, where $\sqrt{a}$ means $\exists b \in (\mathbb{Q}, +)$ s.t. $b + b = a$

clearly $\langle a \rangle \subset \langle \frac{a}{2} \rangle$. ok

i.e. $\frac{a}{2}$ generates all elements that a generates and more.

Contradiction

Case II: $a = 0$.

But $a^m = 0\ \forall m$. $\therefore 0$ cannot be a generator

(The Identity can never be the generator).

$\therefore (\mathbb{Q}, +)$ cannot be cyclic.

(d) To check: Is $U(18)$ cyclic?

$U(18) = \{1, 5, 7, 11, 13, 17\}$ and $\phi(18) = 6$. 5/5

$\therefore \forall a \in U(18) \setminus \{e\}, \ |a| = 2, 3, 6.$

clearly, $\exists\ 11 \in U(18)$ s.t. $11^2 = 13\ (\neq e)$, $11^3 = 17\ (\neq e)$, $11^6 = 1 = e$.

$\therefore U(18) = \langle 11 \rangle$ and $U(18)$ is cyclic. ■

5/5

(e) To check: Is $U(16)$ cyclic?

$U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$ and $\phi(16) = 8$.

$\therefore \forall a \in U(16) \setminus \{e\}, \ |a| = 2, 4, 8.$

we search for $a \in U(16)$ s.t $|a| = \phi(16)$.

However, $|1| = 1$, $|3| = 4$, $|5| = 4$, $|7| = 2$, $|9| = 2$, $|11| = 4$, $|13| = 4$ and $|15| = 2$. $\therefore \sim[\exists\, a \in U(16) \text{ s.t } |a| = \phi(16)]$

$\therefore U(16)$ cannot be Cyclic ■

Answer 4) (a) To Prove: $\exists\, H < S_{17}$ st $|H| = 70$.

Consider $h = (1\,2\,3\,4\,5\,6\,7)(8\,9\,10\,11\,12\,13\,14\,15\,16\,17) \in S_{17}$.

$|h| = LCM(7, 10) = 70$ ($\because h = \alpha \circ \beta$ as Above, $\alpha \cap \beta = \phi$).

$\therefore \exists\, H = \langle h \rangle < S_{17}$. $H = \{h, h^2, h^3, \dots, h^{70} = e\}$.

5/5

H is cyclic. $\therefore$ H is Abelian. ■

(b) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 1 & 8 & 7 & 6 & 2 \end{pmatrix}$ $\rightarrow |f| = 6$

4/5

$\Rightarrow f = (1\;3\;4)(2\;5\;8)(6\;7)$

$= (1\;4) \circ (1\;3) \circ (2\;8) \circ (2\;5) \circ (6\;7) = 5$ 2-Cycles.

$\therefore f$ is Odd $\Longrightarrow f \notin A_8$ ■ and $|f| = 6$

(c) $n = \max\{|f|,\ f \in A_9\}$.

Notice: All Elements in f are Compositions of:

(a_1)

$(a_1\;a_2\;a_3)$

$(a_1\;a_2\;a_3\;a_4\;a_5)$

$(a_1\;a_2\;a_3\;a_4\;a_5\;a_6\;a_7)$

$(a_1\;a_2\;a_3\;a_4\;a_5\;a_6\;a_7\;a_8\;a_9)$

5/5

The maximum no. of Elements we can have in permutation notation such that there are NO Overlaps ($\Rightarrow$ as Disjoint Permutation) is $f = (a_1\;a_2\;a_3) \circ (a_4\;a_5\;a_6\;a_7\;a_8)$. Then $|f| = LCM(3, 5) = 15$.

→ This has to be the Maximum Order.

→ In all other cases, compositions can be reduced by writing them as disjoint permutations and 15 is the maximum order for the disjoint case.

$\therefore n = 15$.

(d) $f \in S_n \setminus A_n$. To Prove: $|f|$ is Even.

PROOF: We use the result from previous homework:

$H \lhd D,\ a \in D,\ x = a * H \in D/H \implies |x| \,\big|\, |a|$. —— (1)

(i.e. Order of the coset in D/H divides Order of every representative of this coset in D.)

$A_n \lhd S_n,\ f \in S_n$, let $x = f \circ A_n \implies |x| \,\big|\, |f|$ (From (1))

But x is the set of all odd functions.

$|x| = |f \circ A_n| = 2$. $\left(\because |S_n/A_n| = \frac{|S_n|}{|A_n|} = 2.\ \therefore x \neq e \in S_n/A_n \Downarrow |x| = 2\right)$.

$\therefore 2 \,\big|\, |f| \implies |f|$ is Even. ■

V. good

5/5

Name *Taha Ameen*, ID *66555*

49/50

HW SIX, Abstract Algebra, MTH 320, Fall 2017

Ayman Badawi

QUESTION 1. Assume $(D, *)$ is a group with p^5 elements for some prime number p. Assume D has a normal cyclic subgroup H with p^4 elements and D has a normal subgroup F with p elements such that $F \not\subseteq H$. Prove that D is abelian but not cyclic.

QUESTION 2. (VERY IMPORTANT)

Let $(D, *)$ be a group

(i) Let $m \in D$ be fixed and define $f : (D, *) \to (D, *)$ such that $f(a) = m * a * m^{-1}$ for every $a \in D$. Prove that f is a group-isomorphism.

(ii) Let $a \in D$ and assume that $|a| = k < \infty$. Prove that $|a| = |d * a * d^{-1}|$ for every $d \in D$.

(iii) Define $f : (D, *) \to (D, *)$ such that $f(a) = a^2$ for every $a \in D$. Prove that f is a group-homomorphism if and only if D is abelian.

(iv) Assume that D has 10 elements and $D = < a >$ for some $a \in D$. Define $f : (D, *) \to (D, *)$ such that $f(a) = a^3$. Find $f(b)$ for every $b \in D$. Convince me that f is a group-isomorphism. Find Range(f) and Ker(f)

(v) Assume that H is a subgroup of D with m ($finite$) elements. Prove that $d * H * d^{-1}$ is a subgroup of D with m elements. Now, convince me that if F is the only subgroup of D with k element (k is $finite$), then F must be normal in D.

(vi) Assume $|D| = 5^3 \cdot 7^2$. Assume that D has a normal cyclic subgroup, say H, of order 7^2 and D has a normal abelian subgroup, say F, of order 5^3. Up to isomorphism find all possibilities of the group structure of D.

(vii) Assume $|D| = p \cdot q$ for some prime numbers p, q. Assume that D has a normal subgroup, say H, of order p and D has a normal subgroup, say F, of order q. Prove that D is cyclic.

QUESTION 3. (Important) Let $S = \{0, 1, 3, ..., 17\}$. Then we view S_{18} as the set of all bijective functions from S ONTO S, and recall that (S_{18}, o) is a group. Let $D = \{f : (Z_{18}, +) \to (Z_{18}, +) \mid f \text{ is a group} - \text{isomorphism}\}$. Hence $D \subset S_{18}$.

(i) Let $K : (Z_{18}, +) \to (Z_{18}, +)$ such that $K(1) = 1^5 = 5$. Is $K \in D$? EXPLAIN. Find $K(a)$ for every $a \in Z_{18}$. If $K \in D$, then find $|K|$.

(ii) Prove that (D, o) is a cyclic subgroups of S_{18} with exactly 6 elements. Hence $D =< f >$ for some $f \in D$. Give me such f.

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

ANSWER 1 :

Given: $|D| = p^5$. $H \triangleleft D$; $|H| = p^4$; H is cyclic.

$F \triangleleft D$; $|F| = p$; $F \nsubseteq H$

To Prove: D is Abelian and Not cyclic.

Strategy: We show $D \cong Z_{p^4} \times Z_p$:

Proof: $|F| = p \Rightarrow F$ is cyclic $\because p$ is prime.

clearly, $F \cap H = \{e\}$ | $\because |F| = p$, $F \nsubseteq H$.

and $F * H = D$ | $\because |F*H| = \frac{|F||H|}{|F \cap H|} = |F||H| = p p^4 = p^5$

$\therefore D \cong H \times F$

But, $H \cong \mathbb{Z}_{p^4}$ and $F \cong \mathbb{Z}_p$

$\therefore D \cong \mathbb{Z}_{p^4} \times \mathbb{Z}_p$. Since $\gcd(p, p^4) = p \neq 1$,

D is Abelian but not cyclic. ■

$\frac{5}{5}$

ANSWER 2

(i): Step I: Showing that f is a homomorphism

$f(a*b) = m*(a*b)*m^{-1}$

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

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

$= f(a) * f(b)$.

Let $a \in \ker(f)$. Then $f(a) = e$, $mam^{-1} = e \Rightarrow a = e$, $\ker(f) = \{e\}$

$\frac{4}{2}$

Step II: Equal Cardinality

Clear, As $|D| = |D|$ → that does not make f 1-1

Step III: ONTO : $\forall x (= m*a_i*m^{-1}) \in \text{Range}(f)$

$\exists a_i \in \text{Domain}(f)$ s.t. $f(a_i) = x$.

$\therefore$ f is an Isomorphism ■

(ii) $a \in D$, $|a| = k < \infty$. To Show: $|a| = |d * a * d^{-1}|$, $d \in D$.

Proof: consider the group Isomorphism $f: D \longrightarrow D$
s.t. $f(a) = d * a * d^{-1}$ for any $d \in D$.

By Property of Isomorphisms,

4/4 $|f(a)| = |a| \implies |d * a * d^{-1}| = |a|$ ■

(iii) $f: D \longrightarrow D$; $f(a) = a^2$. To Prove: Homomorphism $\Leftrightarrow$ Abelian.

Proof: PART 1: Assume f is a Homomorphism. Show D is Abelian.

$\forall a, b \in D$: $f(a * b) = (a * b) * (a * b)$ —(1)

and $f(a) * f(b) = (a * a) * (b * b)$. —(2)

But (1) and (2) are Equal $\because$ f is a homomorphism

$\therefore$ $a * b * a * b = a * a * b * b$

$\Rightarrow$ $b * a = a * b$ | Left and Right Cancellation

$\therefore$ D is Abelian.

4/4 PART 2: Assume D is Abelian. Show f is a Homomorphism

$f(a * b) = (a * b) * (a * b) = a * (b * a) * b = a * (a * b) * b$

$\therefore$ $f(a * b) = (a * a) * (b * b) = f(a) * f(b)$

$\therefore$ f is a Homomorphism. ■

(iv) $D = \langle a \rangle$; $|D| = |a| = 10$; $f(a) = a^3$.

4/4 To Show: f is a group Isomorphism

Since $\langle a \rangle = \langle a^3 \rangle$, $\Big|$ $\because |a^3| = \dfrac{|a|}{\gcd(3,10)} = \dfrac{|a|}{1} = 10$

Both $\langle a \rangle = D$
AND $\langle a^3 \rangle = f(D)$ are Isomorphic to $\mathbb{Z}_{10}$ and Therefore
$\because b = a^i \Rightarrow f(b) = a^{3i}$ $\forall b$, Isomorphic to each other.

$\therefore$ f is a Group Isomorphism.

<u>To Find</u>: Range(f) and Ker(f)

Since f is one-to-one: $Ker(f) = \{e\}$

Since $|Range(f)| = |D|/|Ker(f)|$ $Range(f) = D$ //

<u>(v)</u> $H < D$, $|H| = m$. <u>To Prove</u>: $d * H * d^{-1} < D$.

Since dHd^{-1} is finite, it is sufficient to show closure.

Let $x, y \in dHd^{-1} \implies x = d * h_i * d^{-1}$, $y = d * h_j * d^{-1}$

Then $x * y = (d * h_i * d^{-1}) * (d * h_j * d^{-1})$

$= d * (h_i * h_j) * d^{-1}$

4/4 $= d * (h_k) * d^{-1}$, $h_k \in H$ $\because$ H is a group.

$\therefore$ $d * H * d^{-1}$ is a group.

Consider the isomorphism $f(h) = d * h * d^{-1}$.

Then $H \cong dHd^{-1} \implies |d * H * d^{-1}| = |H| = m$.

<u>Part II</u>: Let $|F| = k$. If there are no other subgroups of order k, then F is normal:

<u>Proof</u>: $F < D$. Further $d * F * d^{-1} < D$ & $|d * F * d^{-1}| = |F|$.

But, this group is Unique $\implies$ $F = d * F * d^{-1}$

$\therefore$ $F * d = d * F \implies$ F is normal ■

4/4

<u>(vi)</u> $|D| = 5^3 7^2$. $|H| = 7^2$ (Cyclic), $|F| = 5^3$ (Abelian)

Clearly, $H \cong \mathbb{Z}_{7^2}$

and $F \cong \mathbb{Z}_{5^3}$ (OR) $\mathbb{Z}_{5^2} \times \mathbb{Z}_5$ (OR) $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\therefore$ Classification:

① $D \cong \mathbb{Z}_{7^2} \times \mathbb{Z}_{5^3}$ (OR) ② $D \cong \mathbb{Z}_{7^2} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5$ (OR) ③ $D \cong \mathbb{Z}_{7^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

(vii) $|D| = pq$, $H \triangleleft D$, $|H| = p$, $F \triangleleft D$, $|F| = q$

To prove: D is cyclic

clearly, $H \not\subseteq F$ and $F \not\subseteq H$ ($\because |F|, |H|$ are prime)

$$H \cap F = \{e\} \Rightarrow |HF| = \frac{|H||F|}{|H \cap F|} = \frac{pq}{1} = pq.$$

$\therefore HF = D$ and $H \cap F = \{e\}$.

$\therefore D \cong F \times H \cong \mathbb{Z}_q \times \mathbb{Z}_p$ ($\because F$ and H are cyclic).

Further, $\gcd(q,p) = 1$ $\because q$ and p are prime.

$\therefore D$ is cyclic ∎

5/5

ANSWER 3: (i) $S = \{0,1,2,3,\ldots,17\}$; $D = \{f : (\mathbb{Z}_{18},+) \to (\mathbb{Z}_{18},+)$ | f is a Group Isomorphism$\}$.

$K(1) = 1^5 \Rightarrow K(1^i) = [K(1)]^i = (5)^i$

$$\therefore K = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 0 & 5 & 10 & 15 & 2 & 7 & 12 & 17 & 4 & 9 & 14 & 1 & 6 & 11 & 16 & 3 & 8 & 13 \end{pmatrix}$$

Clearly, K is one-to-one and onto. $K(a*b) = K(1^i * 1^j)$

$$= K(1^{i+j}) = 5^{i+j} = 5^i * 5^j = K(a) * K(b)$$

$\therefore K$ is a group Isomorphism.

$\therefore K = (1\ 5\ 7\ 17\ 13\ 11)(2\ 10\ 14\ 16\ 8\ 4)(3\ 15)(6\ 12)$

$\Rightarrow |K| = \mathrm{LCM}(6,6,2,2) = 6$. $\therefore |K| = 6$ //

(ii) There are exactly $\phi(18) = 6$ Generators of $\mathbb{Z}_{18}$.

$\therefore$ There are 6 possible Isomorphisms: $f(1) = x$, $x \in U(18)$.

$\therefore |D| = 6$. From (i) above, $\exists\, k \in D$ st $|k| = 6$.

$\therefore D = \langle k \rangle$,

where $k = (1\ 5\ 7\ 17\ 13\ 11)(2\ 10\ 14\ 16\ 8\ 4)(3\ 15)(6\ 12)$