MTH 530

Abstract Algebra I

By Ayman Badawi

Name: Yasmine El-Ashi

I.D. #: 7313.

Name————————————————, ID ——————————

HW ONE: MTH 530, Fall 2017

Ayman Badawi

QUESTION 1. Let $(D, *)$ be a group, F_1, F_2 be subsets of D where $F_1 \not\subseteq F_2$ and $F_2 \not\subseteq F_1$. Then $L = F_1 \cup F_2$ is a subset of D. Assume that $(F_1, *)$ and $(F_2, *)$ are groups. Prove that $(L, *)$ is never a group.

QUESTION 2. We know that if $n, m \in N^*$, then there are unique $q, r \in N$ such that $m = n \cdot q + r, 0 \leq r < n$. Now let $(D, *)$ be a group and $a \in D$ such that $|a| = k$.

(i) Assume $k < \infty$ and suppose that $a^m = e$ for some $m \in N^*$. Prove that $k \mid m$ (i.e., k is a factor of m, i.e., k divides m)

(ii) (converse of (i)). Assume $k < \infty$. Let m be a positive integer such that $k \mid m$. Prove that $a^m = e$.

(iii) Assume $k < \infty$. Prove $|a| = |a^{-1}| = k$

(iv) If $|a| = \infty$, then prove that $|a^{-1}| = \infty$

(v) Assume $|a| = \infty$. Prove that the elements of the set $\{a^0 = e, a, a^2, ..., a^n, ...\}$ are distinct. Hence $|D| = \infty$.

(vi) ((iv) might be helpful). Let F be a finite subset of D (i.e., $|F| < \infty$). Suppose that $(F, *)$ is closed (i.e, $a * b \in F$ for every $a, b \in F$). Prove that $(F, *)$ is a group

(vii) Assume that $b^2 = e$ for every $b \in D$. Prove that $(D, *)$ is abelian.

QUESTION 3. 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).

(i) What is $e \in D$?

(ii) Let $a = 12$ What is $|a|$?.

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

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

QUESTION 4. (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?

(ii) Let (D_n, o) be the symmetric group on $n - gon$. We know that $|D| = 2n$ (note that $n \geq 3$ is a positive integer). Assume that $a \in D_n$, where a is a rotation, say $a = R_{k(\frac{360}{n})}$ (i,e., rotation about the center $k\frac{360}{n}$ degrees clockwise, and assume $1 \leq k \leq n$).

a. What is a^{-1}? Is a^{-1} a rotation or a reflection?

b. ((i) might be helpful). Let $b \in D_n$, where b is a reflection. Prove that $b\ o\ a$ is a reflection.[Your proof should not exceed 2 lines].

c. ((b) and (i) might be helpful) Let $R = \{R_1, R_2, ..., R_n\}$ be the set of all rotations in D_n, note that R_i is the rotation about the center $i\frac{360}{n}$ degrees clockwise. Let $b \in D_n$ be a reflection. Prove that $\{b\ o\ R_1, b\ oR_2, ..., b\ o\ R_n\}$ 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]

d. Let $b \in D_n$ where b is a reflection. What is $|b|$?

e. Consider (D_6, o). Let $R_1 = R_{60} = (1\ 2\ 3\ 4\ 5\ 6), b = (Re)_1 = (2\ 6)(3\ 5)$ be a reflection. Note that $R_2 = R_1^2 = R_1\ o\ R_1$, and in general $R_i = R_1^i = R_{i-1}\ o\ R_1$. So you can find all the rotations (without sketching!). Now use the idea in (c) to calculate all reflections.

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`

If $a \Rightarrow c$

~~the~~ (not b) $\to$ (not a)

QUESTION 1: Let $(D,*)$ be a group, F_1, F_2 be subsets of D where $F_1 \not\subseteq F_2$ and $F_2 \not\subseteq F_1$. Then $L = F_1 \cup F_2$ is a subset of D. Assume that $(F_1,*)$ and $(F_2,*)$ are groups. Prove that $(L,*)$ is never a group.

Proof: Let $a \in F_1 \Rightarrow a \notin F_2$ since $F_1 \not\subseteq F_2$.

Let $b \in F_2 \Rightarrow b \notin F_1$ since $F_2 \not\subseteq F_1$.

Suppose $(L,*)$ is a group where $L = F_1 \cup F_2$.

Then we have: $a * b = c \in L = F_1 \cup F_2$.

$\Rightarrow a * b = c \in F_1$ or F_2.

(1) Suppose $c \in F_1$,

$$a * b = c \in F_1.$$

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

since we are assuming $(L,*)$ to be a group, we are assuming the associative and identity conditions to be valid

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

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

$$b = a^{-1} * c \in F_1$$

Since $(F_1,*)$ is a group $a \in F_1 \Rightarrow a^{-1} \in F_1$, and we have $c \in F_1 \Rightarrow a^{-1} * c \in F_1$

So $b \in F_1 \Rightarrow$ we have a contradiction since $b \notin F_1$ for $F_2 \not\subseteq F_1$.

OK

(2) Suppose $c \in F_2$,

$$a * b = c \in F_2.$$

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

since we are assuming $(L,*)$ to be a group, we are assuming the associative and identity conditions to be valid.

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

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

$$a = c * b^{-1} \in F_2.$$

Since $(F_2,*)$ is a group, $b \in F_2 \Rightarrow b^{-1} \in F_2$ and we have $c \in F_2 \Rightarrow c * b^{-1} \in F_2$.

So $a \in F_2 \Rightarrow$ we have a contradiction since $a \notin F_2$ for $F_1 \not\subseteq F_2$

5/5

$\therefore (L,*)$ can <u>never</u> be a group.

QUESTION 2: We know if $n, m \in N^*$, then there are unique $q, r \in N$ s.t. $m = q \cdot n + r$, $0 \leq r < n$. Now let $(D, *)$ be a group and $a \in D$ s.t. $|a| = k$.

(i) Assume $k < \infty$ and suppose that $a^m = e$ for some $m \in N^*$ and suppose that $a^m = e$ for some $m \in N^*$ (or k divides m). Prove that $k | m$ (i.e. k is a factor of m, or k divides m).

Proof: Suppose k does not divide m, then we can write m as $\Rightarrow m = q \cdot k + r$, where $0 \leq r < k$.

Let

$$a^m = e$$

$$a^{(qk+r)} = e$$

$$a^{qk} * a^r = e$$

$$(a^k)^q * a^r = e$$

$$(e)^q * a^r = e$$

$$e * a^r = e$$

$$\Rightarrow a^r = e$$

Given $0 \leq r < k$, But here we have a contradiction since $|a| = k$, that is k is the smallest integer $\in N^*$ s.t. $a^k = e$.

$\therefore$ We must have $k | m$.

(ii) (converse of (i)) Assume $k < \infty$. Let m be a positive integer s.t. $k | m$. Prove that $a^m = e$.

Proof: suppose $m \in N^*$ s.t. $k | m \Rightarrow m = nk$ for some $n \in N^*$

$$a^m = a^{nk} = (a^k)^n = (e)^n = e$$

since $|a| = k \Rightarrow k$ is smallest +ve integer s.t. $a^k = e$

(iii) Assume $k < \infty$. Prove $|a| = |a^{-1}| = k$.

Proof: Suppose k is finite, that is $k < \infty$, and we have $|a| = k$.
we want to show that $|a^{-1}| = k$.

First, let us find $(a^{-1})^k$

$$e = a^0 = a^{(k-k)} = a^{k+(-k)} = a^k * a^{-k} = e * a^{-k} = a^{-k}.$$

$$\therefore \quad a^{-k} = e.$$

suppose $|a^{-1}| = r$, then $r < \infty$. (finite) and $r \leq k$.

(1) (Deny): suppose $r < k$, then $k = r + n$ for some +ve integer n, s.t. $n < k$.

$$r = k - n.$$

$$e = (a^{-1})^r = (a^{-1})^{(k-n)} = (a^{-1})^k * (a^{-1})^{-n}$$
$$= (a^{-1})^k * ((a^{-1})^{-1})^n$$
$$= e * a^n$$

$\Rightarrow \quad a^n = e \quad \Rightarrow$ But here we have a contradiction since $n < k$, and $|a| = k$, that is k is the smallest +ve integer s.t. $a^k = e$.

$\therefore$ we must have $r = k$. $\Rightarrow |a^{-1}| = |a| = k$.

(2) (Direct method):

$$|a^{-1}| \leq |a|.$$

$$\Rightarrow \quad |(a^{-1})^{-1}| \leq |a^{-1}|.$$

But we have $(a^{-1})^{-1} = a$

$$\therefore \quad |a| \leq |a^{-1}|$$

$$|a^{-1}| = |a| = k.$$

(iv) If $|a| = \infty$, then prove that $|a^{-1}| = \infty$

We are trying to prove the following statement:

If $|a| = \infty \Rightarrow |a^{-1}| = \infty$

$\therefore$ To prove the above statement, we can prove its contrapositive: that is show that:

if $|a^{-1}| < \infty \Rightarrow |a| < \infty$

WLOG let $|a^{-1}| = k$ where $k < \infty$

$\therefore$ using (iii) we have $|a| = |a^{-1}| = k$.

$$\Rightarrow \quad |a| = k < \infty$$

(v) Assume $|a| = \infty$. Prove that the element of the set $\{a^0 = e, a, a^2, \dots, a^n, \dots\}$ are distinct. Hence $|D| = \infty$.

Proof: Suppose $|a| = \infty$, and let $a^n = a^m$ for some $n, m \in \mathbb{Z}^+$ s.t. $n \neq m$. Let $m > n$, thus $m = n + k$ for some $k \in \mathbb{Z}^+$

we have, $a^m = a^{n+k} = a^n * a^k$

since $a^m = a^n$ then according to our assumption $a^k = e$, but this is a contradiction since $|a| = \infty$, that is there does not exist a smallest +ve integer k, s.t. $a^k = e$.

$\therefore a^n \neq a^m \;\; \forall \; n, m \in \mathbb{Z}^+$ s.t. $n \neq m \Rightarrow |D| = \infty$

since D is non-empty $a \in D$, and $(D, *)$ is a group $\Rightarrow \{a^0, a^2, \dots, a^n, \dots\} \in D$ (closed under $*$).

(vi) [(iv) might be helpful]. Let F be a finite subset of D (i.e. $|F| < \infty$). Suppose that $(F, *)$ is closed (i.e. $a * b \in F$ for every $a, b \in F$) Prove that $(F, *)$ is a group.

(1) closure: We have $a * b \in F \;\; \forall a, b \in F$, thus closure is satisfied

(2) associative: since $(D, *)$ is a group, and F is a finite subset of D, let $a, b, c \in F \Rightarrow a, b, c \in D$ since $F \subseteq D$ since D is a group, the associative condition is valid $\therefore (a * b) * c = a * (b * c) \;\; \forall a, b, c \in D$.

that is $(a * b) * c = a * (b * c) \;\; \forall a, b, c \in F$.

$\therefore$ we must have $e \in F$

(3) identity: We need to show $e \in F$

Let $a \in F$, since $(F, *)$ is closed

we have $a^0 \in F$

but $a^0 = e$, $\therefore e \in F$.

NO $a^0 = e \;\forall a \in D$ we can not claim this

(4) inverse: Let $a \in F$, we need to show that $a^{-1} \in F$

Since $(F, *)$ is closed $\Rightarrow \{e, a, a^2, \dots, a^n, \dots\} \in F$

But we know that F is finite set, $\therefore \exists m, n \in \mathbb{Z}^+$, s.t. $a^m = a^n$

Let $m > n$

$a^{m-n} = e$

$a^{m-n} \cdot a^{-1} = e \cdot a^{-1}$

$a^{(m-n)-1} = a^{-1}$

If $m - n = 1$, then $a^{-1} = a^0 = e \in F$ (as shown in (3))

If $(m-n) > 1$, then $(m-n) - 1 > 0$

$a^{(m-n)-1} \in F$ (since $(F, *)$ is closed)

$\Rightarrow a^{-1} = a^{(m-n)-1}$

$\therefore (F, *)$ is a group, and satisfies all the above conditions.

This

argument

(iii) Assume $k < \infty$. Prove $|a| = |a^{-1}| = k$.

Proof: Suppose k is finite, that is $k < \infty$, and we have $|a| = k$.
we want to show that $|a^{-1}| = k$.

First, let us find $(a^{-1})^k$

$$e = a^0 = a^{(k-k)} = a^{k+(-k)} = a^k * a^{-k} = e * a^{-k} = a^{-k}$$

$\therefore \quad a^{-k} = e.$

Suppose $|a^{-1}| = r$, then $r < \infty$ (finite) and $r \leq k$.

(1) (Deny): Suppose $r < k$, then $k = r + n$ for some +ve integer n, s.t. $n < k$.

$$r = k - n.$$

$$e = (a^{-1})^r = (a^{-1})^{(k-n)} = (a^{-1})^k * (a^{-1})^{-n}$$
$$= (a^{-1})^k * ((a^{-1})^{-1})^n$$
$$= (a^{-1})^k * (a)^n$$
$$= e * a^n$$

OK

$\Rightarrow \quad a^n = e \quad \Rightarrow$ But here we have a contradiction since $n < k$, and $|a| = k$, that is k is the smallest +ve integer s.t. $a^k = e$.

5/5

$\therefore$ we must have $r = k. \quad \Rightarrow |a^{-1}| = |a| = k.$

(2) (Direct method)

$$|a^{-1}| \leq |a|.$$

$$\Rightarrow \quad |(a^{-1})^{-1}| \leq |a^{-1}|.$$

But we have $(a^{-1})^{-1} = a$

$$\therefore \quad |a| \leq |a^{-1}|$$

$$|a^{-1}| = |a| = k.$$

(iv) If $|a| = \infty$, then prove that $\Rightarrow |a^{-1}| = \infty$

We are trying to prove the following statement:

If $|a| = \infty \Rightarrow |a^{-1}| = \infty$

$\therefore$ To prove the above statement, we can prove its contrapositive that is show that:

if $|a^{-1}| < \infty \Rightarrow |a| < \infty$

WLOG Let $|a^{-1}| = k$ where $k < \infty$

$\therefore$ using (iii) we have $|a| = |a^{-1}| = k$

$\Rightarrow |a| = k < \infty$

OK

5/5

(vii) Assume that $b^2 = e$ for every $b \in D$. Prove that $(D,*)$ is abelian.

Proof! To prove that $(D,*)$ is abelian we need to show

$$a*b = b*a \quad \forall a,b \in D$$

let $a,b \in D$, and let $c = a*b$, where $c \in D$ since $(D,*)$ is a group, then we have $c^2 = e$.

$$c^2 = e$$

$\therefore$

$$(a*b)*(a*b) = e$$

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

$$(a*a)*(b*a)*b = a*e$$

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

$$e*(b*a)*b = a$$

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

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

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

$$(b*a)*e = a*b$$

$$b*a = a*b.$$

Thus, we have shown that $(D,*)$ is abelian.

you do not need to write all details here!

$$a*b = b^{-1}*a^{-1}, \text{ but } b^{-1} = b,\ a^{-1} = a$$

$$= b*a$$

Question 3: Let $D = \{6, 12, 18, 24\}$.
Define $*$ on D s.t. for every $a, b \in D$ we have $a * b = a \cdot b$,
where $\cdot$ means multiplication mod. 30
Construct ~~Caley's~~ Caley's table of $(D, \cdot)$, by staring at the
table you should conclude that $(D, \cdot)$ is an abelian group.

Caley's table for $(D, \cdot)$

$\cdot$	6	12	18	24
6	6	12	18	24
12	12	24	6	18
18	18	6	24	12
24	24	18	12	6

5/5

(1) Closure: using the caley's table we can see that $\forall a, b \in D$ we have $a \cdot b \in D$

(2) Associative: Since $(\mathbb{Z}_{30}, \cdot)$ is associative, we conclude that $(D, \cdot)$ is also associative.

(3) Identity: In this case we have $e = 6$, s.t. $\forall b \in D$, we have $b \cdot 6 = 6 \cdot b$

(4) Inverse: In this case we have $6^{-1} = 6$, $12^{-1} = 18$, $18^{-1} = 12$, $24^{-1} = 24$
$\therefore \forall b \in D, \exists b^{-1} \in D$ s.t. $b^{-1} \cdot b = b \cdot b^{-1} = e$.

In addition, from the caley's table we can see that $\forall a, b \in D$ we have $a \cdot b = b \cdot a$

(i) What is $e \in D$? $e = 6$. 1/1

(ii) Let $a = 12$. What is $|a|$?

$12^1 = 12$
$12^2 = 12 \cdot 12 = 24$
$12^3 = (12)^2 \cdot 12 = 24 \cdot 12 = 18$
$12^4 = (12)^3 \cdot 12 = 18 \cdot 12 = 6 = e$

$\therefore |a| = 4$.

1/1

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

$a^2 = 24$, $a^3 = 18$, $a^4 = 6$

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

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

$24^1 = 24$

$24^2 = 24 \cdot 24 = 6$

$\therefore |24| = 2$

$24^3 = (24)^2 \cdot 24 = 6 \cdot 24 = 24$

$24^4 = (24)^3 \cdot 24 = 24 \cdot 24 = 6$

$\therefore \{a, a^2, a^3, a^4\} = \{24, 6, 24, 6\} = \{24, 6\} \subseteq D$

Different from (iii).

Question 4: (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.

- Suppose we have $y \in D$, s.t. $a*y=b$, to prove that the equation $a*x=b$ has a unique solution in D, we need to show that $x=y$.

Since $a*y=b$ and $a*x=b$.

$$a*y = a*x$$

Since a^{-1} is unique in D, multiply the above by a^{-1}

$$a^{-1}*a*y = a^{-1}*a*x$$

$$e*y = e*x$$

$$\Rightarrow y = x \text{, thus the solution is unique in D.}$$

- The solution is:

$$a*x=b$$

$$a^{-1}*a*x = a^{-1}*b$$

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

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

4/4 OK

(ii) (a) What is a^{-1}? Is a^{-1} a rotation or a ~~f~~reflection?

given $a = R_{k\left(\frac{360}{n}\right)}$ $\quad a^{-1} = R_{(n-k)\left(\frac{360}{n}\right)}$

where a^{-1} is a rotation.

(b) ~~((i) might be helpful)~~. Let $b \in D_n$ ~~where b is a reflection~~.

~~Prove that b∘a is a reflection~~.

$r^n = R_{n\left(\frac{360}{n}\right)} = R_{360} = e = r^0$

Let $r = R_{\left(\frac{360}{n}\right)}$

given $a = R_{k\left(\frac{360}{n}\right)}$

$$\therefore a = \underbrace{r \circ r \circ \ldots \circ r}_{k \text{ times}} = r^k$$

$$a \circ a^{-1} = \underbrace{r \circ r \circ \ldots \circ r}_{k \text{ times}} \circ \underbrace{r \circ r \circ \ldots \circ r}_{(n-k) \text{ times}}$$

$$= r^k \circ r^{(n-k)} = r^{k+(n-k)} = r^n = e.$$

$$a^{-1} \circ a = r^{(n-k)} \circ r^k = r^{(n-k)+k} = r^n = e.$$

(ii)(b) [(i) might be helpful]. Let $b \in D_n$, where b is a reflection.
Prove that $b \circ a$ is a reflection.

Proof: let $c = b \circ a$, and suppose c is a rotation,
thus we can write c as : $c = r^m$ for some $1 \leq m \leq n$.
let $a = r^k$, and $a^{-1} = r^{n-k}$

$b \circ a = c$

$b \circ a = r^m$

using (i) we have:

$b = r^m \circ a^{-1} = r^m \circ r^{(n-k)}$

$\Rightarrow b = r^{m+(n-k)}$ $\therefore$ we have b represented as a rotation, but this gives us a contradiction, Since b is a reflection.

4/4

$\therefore$ $c = b \circ a$ must be a reflection.

(c) [(b) and (i) might be helpful]
Let $R = \{R_1, R_2, \ldots, R_n\}$ be the set of all rotations in D_n, note that R_i is the rotation about the center $i\frac{360}{n}$ degrees clockwise. Let $b \in D_n$ be a reflection. Prove that $\{b \circ R_1, b \circ R_2, \ldots, b \circ R_n\}$ is the set of all reflections.

Proof:

(1) Using (b) $\{b \circ R_1, b \circ R_2, \ldots, b \circ R_n\}$ is a set of reflections, since $\{R_1, R_2, \ldots, R_n\}$ is the set of all rotations in D_n.

(2) In addition, $\{R_1, R_2, \ldots, R_n\}$ consists of distinct elements and since we are just composing them with b, then $\{b \circ R_1, b \circ R_2, \ldots, b \circ R_n\}$ the set of n reflections, also consists of n distinct elements, which are all the reflections in D_n.

4/4

(d) Let $b \in D_n$ where b is a reflection. What is $|b|$?

$$b \circ b = e$$
$$\Rightarrow b \circ b = b^2 \quad \therefore \quad |b| = 2$$

(e) Consider $(D_6, \circ)$. Let $R_1 = R_{60} = (1\,2\,3\,4\,5\,6)$

$b = (Re)_1 = (26)(35)$ be a reflection.

Note that $R_2 = R_1^2 = R_1 \circ R_1$ and in general $R_i = R_1^i$
$= R_{i-1} \circ R_1$

Now use the idea in (c) to calculate all reflections.

Let $R = \{R_1, R_2, R_3, R_4, R_5, R_6\}$ be the set of all rotations in D_6.

$Re = \{b \circ R_1, b \circ R_2, b \circ R_3, b \circ R_4, b \circ R_5, b \circ R_6\}$ be the set of all reflections in D_6.

$R_1 = (1\,2\,3\,4\,5\,6)$

$R_2 = R_1 \circ R_1 = (123456) \circ (123456)$
$= (1\,3\,5)(2\,4\,6)$

$R_3 = R_2 \circ R_1 = [(1\,3\,5)(246)] \circ (1\,2\,3\,4\,5\,6)$
$= (1\,4)(2\,5)(3\,6)$

$R_4 = R_3 \circ R_1 = [(1\,4)(2\,5)(36)] \circ (1\,2\,3\,4\,5\,6)$
$= (1\,5\,3)(2\,6\,4)$

$R_5 = R_4 \circ R_1 = [(1\,5\,3)(2\,6\,4)] \circ (1\,2\,3\,4\,5\,6)$
$= (1\,6\,5\,4\,3\,2)$

$R_6 = R_5 \circ R_1 = (1\,6\,5\,4\,3\,2) \circ (1\,2\,3\,4\,5\,6)$
$= (1) = e$

$b \circ R_1 = [(2\,6)(35)] \circ (1\,2\,3\,4\,5\,6)$
$= (1\,6)(2\,5)(3\,4)$

4/4

$b \circ R_2 = [(2\,6)(3\,5)] \circ [(1\,3\,5)(2\,4\,6)]$
$= (1\,5)(2\,4)$

$b \circ R_3 = [(26)(35)] \circ [(1\,4)(2\,5)(36)]$
$= (1\,4)(2\,3)(5\,6)$

$b \circ R_4 = [(2\,6)\,(3\,5)] \circ [(1\,5\,3)\,(2\,6\,4)]$

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

$b \circ R_5 = [(2\,6)\,(3\,5)] \circ [(1\,6\,5\,4\,3\,2)]$

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

$b \circ R_6 = b \circ e = b = (2\,6)\,(3\,5)$

MTH 530

Abstract Algebra I.

Ayman Badawi.

65

~~70~~

75

Name: Yasmine El-Ashi

I.D.#: 7313.

tion 1 :(i) Let $(D,*)$ be a group. Fix a positive integer m and let $F = \{a \in D \mid a^m = e\}$. Prove that $(F,*)$ is a subgroup of D.

(1) Closure : Let $a \in F \Rightarrow a \in D$ s.t. $a^m = e$.

Let $b \in F \Rightarrow b \in D$ s.t. $b^m = e$.

Show that $a*b \in F$

Since $a \in D$ and $b \in D$, we have $a*b \in D$.

since $(D,*)$ is a group.

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

Since $(a*b) \in D$ s.t. $(a*b)^m = e \Rightarrow a*b \in F$

$\therefore (F,*)$ is closed.

(2) Associative : Since $F \subseteq D$ and D is a group, then $(F,*)$ is associative.

(3) Identity : We need to show that $e \in F$

We have $e \in D$, and $e^m = e$ where m is a positive integer

$\Rightarrow e \in F$.

(4) Inverse: Let $a \in F$, we need to show that $a^{-1} \in F$

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

$\Rightarrow a^{-1} \in F$.

Since all the above conditions are satisfied $\Rightarrow (F,*)$ is a group

Since $F \subseteq D$, where $(D,*)$ is a group $\Rightarrow (F,*)$ is a subgroup of D.

[illegible] OK 5/5

You prove it from Scratch: Use (a^-1 * b in F)

Let a, b in F. We show a^{-1}* b in F. Since a, b in F, we have a^m = b^m = e.

Since D is abelian, (a^{-1}*b)^m = (a^{-1})^m * b^m = (a^m)^{-1}*b^m = (e)^{-1} * e = e * e = e.

Thus a^{-1} * b is in F.

(ii) Fix a positive integer n. We know that the equation $x^n - 1$ has exactly n distinct solutions over the complex $\mathbb{C}$. Now let $F = \{a \in \mathbb{C}^* \mid a^n - 1 = 0\}$. Prove that $(F, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$, where $\cdot$ is the normal complex multiplication.

Let Prove

Proof: Let $F = \{a \in \mathbb{C}^* \mid a^n - 1 = 0\}$

Since $x^n - 1 = 0$ has exactly n distinct solutions $\in \mathbb{C}$ and since $x = 0$ cannot be a solution for $x^n - 1 = 0$ $\Rightarrow$ the solutions live in $\mathbb{C}^*$.

$\therefore |F| = n < \infty \Rightarrow F$ is finite.

So we only need to show that $(F, \cdot)$ is closed:

Let $a \in F \Rightarrow a \in \mathbb{C}^*$ s.t. $a^n - 1 = 0 \Rightarrow a^n = 1$.

Let $b \in F \Rightarrow b \in \mathbb{C}^*$ s.t. $b^n - 1 = 0 \Rightarrow b^n = 1$.

show that $(a \cdot b) \in F$, since $a \in \mathbb{C}^*, b \in \mathbb{C}^* \Rightarrow ab \in \mathbb{C}^*$ ($(\mathbb{C}^*, \cdot)$ is a group)

and $(ab)^n - 1 = a^n b^n - 1 = (1)(1) - 1 = 1 - 1 = 0$.

$\Rightarrow (a \cdot b) \in F \Rightarrow (F, \cdot)$ is closed.

Since $F \subseteq \mathbb{C}^*$, s.t. $|F| < \infty$ and $(F, \cdot)$ is closed $\Rightarrow$ $(F, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

5/5

Good. So you did not prove it from scratch. You used the result that a finite subset of a group is a subgroup iff it is closed.

(iii) We know $(\mathbb{Q}^*, \cdot)$ is a group. Does $\mathbb{Q}^*$ have a finite subgroup? If yes, what is it?

Yes $\mathbb{Q}^*$ have a finite subgroup, ex: $(\mathbb{Z}_5^*, \cdot)$

NO NO NO

the binary operation on z_5 is not the same binary operation on Q^* !!

$\{-1, 1\}$

0/5

(iv) Construct a non-abelian group D, with exactly 96 elements such that D has an abelian subgroup with 12 elements.

Let $D := (\mathbb{Z}_8, +) \times (\mathbb{Z}_{13}^*, \cdot)$, where $n = |\mathbb{Z}_8|$, $m = |\mathbb{Z}_{13}^*|$

Now $\therefore |D| = n \times m$

$\therefore |D| = 8 \times 12 = 96$

Let $F := (\mathbb{Z}_3, +) \times (U(8), \cdot)$ be a subgroup of D.

$|U(8)| = \phi(8) = (2-1)^{(3-1)} = 2^2 = 4$

$|\mathbb{Z}_3| = 3$

$\therefore |F| = |\mathbb{Z}_3| \times |U(8)|$

$= 3 \times 4 = 12$

~~$D = \mathbb{Z}_{12}^*$~~

$D = (\mathbb{Z}_{12}, +) \times (D_4, \circ)$

0/5

Note that D_4 is the symmetric group on 4-gon (it has 8 elements

$(D,*)$ be a grup and $a \in D$, s.t. $|a| = k < \infty$, $k \neq 1$.
rove that $F = \{a, a^2, \dots, e = a^k\}$ is a subgroup of D.

we have $|F| = k < \infty \Rightarrow$ the set F is finite,
So we only need to show that F is closed.

Let $a^i \in F$ and $a^j \in F$, show $a^i * a^j \in F$.

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

Let $i + j = m$, m can be written as $m = qk + r$, where $q, r \in N$.

$a^{(i+j)} = a^m = a^{(qk+r)} = a^{qk} \cdot a^r = e \cdot a^r = a^r$

since $r = \bmod k$, is the remainder of m/k.

and $r \leq k$

5/5

$\Rightarrow a^i * a^j = a^r \in F$

Since $|F| < \infty$ and F is closed $\Rightarrow F$ is a subgrup of $(D, *)$.

(Vi) Let F_1 be a subgroup of $(D_1, *_1)$ and F_2 be a subgroup of $(D_2, *_2)$. Prove that $F_1 \times F_2$ is a subgrup of $D_1 \times D_2$.

Since $(D_1, *_1)$ and $(D_2, *_2)$ are both groups $\Rightarrow (D_1 \times D_2, *)$ is a group

We have F_1 is a subgroup of $(D_1, *_1) \Rightarrow F_1 \subseteq D_1$ and $(F_1, *_1)$ is a group.

We have F_2 is a subgroup of $(D_2, *_2) \Rightarrow F_2 \subseteq D_2$ and $(F_2, *_2)$ is a group

Since $(F_1, *_1)$ and $(F_2, *_2)$ are both groups $\Rightarrow (F_1 \times F_2, *)$ is a group
and since $F_1 \subseteq D_1$ and $F_2 \subseteq D_2 \Rightarrow (F_1 \times F_2) \subseteq (D_1 \times D_2)$.

$\therefore (F_1 \times F_2, *)$ is a subgroup of $(D_1 \times D_2, *)$

OK

~~Now~~ again show $a^{-1} * b \in D$ ~~$\forall a, b \in D$~~

$a = (x_1, y_1)$, $b = (x_2, y_2)$

$a^{-1} = (x_1^{-1}, y_1^{-1}) \times (x_2, y_2) = (x_1^{-1} x_2, y_1^{-1} y_2) \in F_1 \times F_2$

(vii) Give me an example of two groups, say D_1, D_2 where $D_1 \times D_2$ has a subgroup L, But there are no subgroups F_1 of D_1 and F_2 of D_2 s.t. $L = F_1 \times F_2$
[Hint: Consider $(\mathbb{Z}_2,+) \times (\mathbb{Z}_4,+)$]
~~let $\alpha = (1,1)$~~ and ~~$k = (1,1)$~~.

Consider $(\mathbb{Z}_2,+) \times (\mathbb{Z}_4,+)$.

$\mathbb{Z}_2 = \{0,1\}$, $\mathbb{Z}_4 = \{0,1,2,3\}$.

$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}$.

Let $a = (1,1)$

Let $n = |1|$ $\qquad$ $m = |1|$

$1^2 = 1+1 = 2 \bmod 2 = 0 = e_1$ $\qquad$ $1^2 = 1+1 = 2$

$n = 2$ $\qquad$ $1^3 = 2+1 = 3$

$1^4 = 3+1 = 4 \bmod 4 = 0 = e_2$.

$m = 4$.

$\therefore |a| = |(1,1)| = \dfrac{nm}{\gcd(n,m)} = \dfrac{2 \cdot 4}{\gcd(2,4)} = \dfrac{8}{2} = 4$

$\therefore k = 4$

Let $L = \{a, a^2, a^3, a^4 = e\}$.

$a = (1,1)$

$a^2 = (1,1)+(1,1) = (1+1, 1+1) = (0,2)$.

$a^3 = (0,2)+(1,1) = (0+1, 2+1) = (1,3)$.

$a^4 = (1,3)+(1,1) = (1+1, 3+1) = (0,0) = e$.

$L = \{(1,1), (0,2), (1,3), (0,0)\}$

$= \{(0,0), (0,2), (1,1), (1,3)\}$.

$\therefore$ But there are no subgroups F_1 of D_1 and F_2 of D_2 s.t. $L = F_1 \times F_2$.

Ok

4/4

n 2 : Let $D = (Z_4, +) \times (U(20), \cdot)$ $(+ \bmod 4, \cdot \bmod 20)$

$Z_4 = \{0, 1, 2, 3\}$

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$|D| = |Z_4| \times |U(20)| = 4 \times 8 = 32$

5/5

(ii) What is $|(2,19)|$?

Let $n = |2|$

$2^2 = 2 + 2 = 4 \bmod (4) = 0 = e_1$

$\therefore |2| = 2$

Let $m = |19|$

$19^2 = 19 \cdot 19 = 361 \bmod 20$
$= 1 = e_2$

$|19| = 2$

$$|(2,19)| = \frac{nm}{\gcd(n,m)} = \frac{2 \times 2}{\gcd(2,2)} = \frac{4}{2} = 2$$

5/5

$|(2,19)| = 2$

(iii) What is $|(3,3)|$?

Let $n = |3|$

$3^2 = 3 + 3 = 6 \bmod 4 = 2$

$3^3 = 2 + 3 = 5 \bmod 4 = 1$

$3^4 = 1 + 3 = 4 \bmod 4 = 0 = e_1$

$\therefore |3| = 4$

Let $m = |3|$

$3^2 = 3 \cdot 3 = 9$

$3^3 = 9 \cdot 3 = 27 \bmod 20 = 7$

$3^4 = 7 \cdot 3 = 21 \bmod 20 = 1 = e_2$

$|3| = 4$

5/5

$$|(3,3)| = \frac{nm}{\gcd(n,m)} = \frac{4 \times 4}{\gcd(4,4)} = \frac{16}{4} = 4$$

$\therefore |(3,3)| = 4$

Question 3 :

(i) What is the meaning of $\frac{2}{7}$ in Z_{15} ?

5/5 $\frac{2}{7}$ in Z_{15} means, $(7^{-1}.2) \bmod 15$. (where . means multiplication mod 15)

(ii) Why is $\frac{5}{6}$ undefined (no meaning) in Z_{15}?

5/5 $\frac{5}{6}$ is undefined in Z_{15} since 6^{-1} is undefined in $(Z_{15}, \cdot)$

(iii) complete the sentence $\frac{a}{b}$ is defined (i.e. has one and

5/5 only one meaning) in Z_n if and only if $b \in U(n)$ ....

(iv) Let $D = U(Z_{15}^{2\times 2})$. Is $A = \begin{bmatrix} 1 & 2 \\ 6 & 12 \end{bmatrix} \in D$?

$|A| = (1.12) - (2.6) = 12 - 12 = 0 \notin U(15)$

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

$\Rightarrow$ A has no inverse.

Is $B = \begin{bmatrix} 3 & 1 \\ 8 & 5 \end{bmatrix} \in D$?

$|B| = (3.5) - (1.8) = 15 - 8 = 7 \in U(15)$.

$\Rightarrow$ B has an inverse.

$B^{-1} = |B|^{-1} \begin{bmatrix} 5 & -1 \\ -8 & 3 \end{bmatrix} = 7^{-1} \begin{bmatrix} 5 & -1 \\ -8 & 3 \end{bmatrix}$.

$7^{-1} = (7^{\phi(15)-1}) (\bmod 15)$

$15 = 3 \cdot 5 \qquad p_1 = 3,\ \alpha_1 = 1, \quad p_2 = 5,\ \alpha_2 = 1$.

5/5 $\phi(15) = (p_1 - 1) p_1^{(\alpha_1 - 1)} \cdot (p_2 - 1) p_2^{(\alpha_2 - 1)}$

$= (3-1)(3)^0 \cdot (5-1)(5)^0 = (2.1).(4.1) = 8$

$7^{\phi(15)-1} = 7^{(8-1)} = 7^7 = (7 \times 7 \times 7 \times 7 \times 7 \times 7 \times 7) \bmod (15)$.

$(4 \times 4 \times 4 \times 7)$

$1 \times 13 = \underline{\underline{13}}$

$\therefore 7^{-1} = 13$.

$B^{-1} = 13 \begin{bmatrix} 5 & 14 \\ 7 & 3 \end{bmatrix} = \begin{bmatrix} 65 & 182 \\ 91 & 39 \end{bmatrix} (\bmod 15) = \begin{bmatrix} 5 & 2 \\ 1 & 9 \end{bmatrix}$

D. $U(\mathbb{Z}_9^{3\times3})$

Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 4 & 0 \\ 3 & 3 & 2 \end{bmatrix}$. Convince me that $A \in D$.

$U(9) = \{1, 2, 4, 5, 7, 8\}$.

$9 = 3^2 \qquad p_1 = 3, \quad \alpha_1 = 2$

$\phi(9) = (p_1 - 1)\, p_1^{(\alpha_1 - 1)} = (3-1) \cdot 3^1 = (2)\cdot(3) = 6$

$|A| = 1 \cdot \begin{vmatrix} 4 & 0 \\ 3 & 2 \end{vmatrix} = 1 \cdot [(4 \cdot 2) - (0 \cdot 3)] = 1 \cdot 8 = 8 \in U(9)$.

since $|A| \in U(9) \Rightarrow$ A is invertible $\Rightarrow A \in D$.

5/5

Find A^{-1} [apply row operations $[A \mid I_3]$ till we get $[I_3 \mid A^{-1}]$.

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 3 & 3 & 2 & 0 & 0 & 1 \end{array}\right] \quad -2R_1 + R_2 \to R_2 \Rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 4 & 0 & 7 & 1 & 0 \\ 3 & 3 & 2 & 0 & 0 & 1 \end{array}\right]$$

$4^{-1} = 4^{\phi(9)-1} = 4^{6-1} = 4^5 = (\underbrace{4 \times 4}\times\underbrace{4 \times 4} \times 4) \bmod 9$

$(\underbrace{7 \times 7} \times 4) \bmod 9$

$(4 \times 4) \bmod 9 = 7$

$$4^{-1}R_2 \Rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 7 & 0 \\ 3 & 3 & 2 & 0 & 0 & 1 \end{array}\right]$$

$$-3R_1 + R_3 \to R_3 \Rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 7 & 0 \\ 0 & 3 & 2 & 6 & 0 & 1 \end{array}\right]$$

$$-3R_2 + R_3 \to R_3 \Rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 7 & 0 \\ 0 & 0 & 2 & 3 & 6 & 1 \end{array}\right]$$

$2^{-1} = 2^{\phi(9)-1} = 2^5 = 32 \bmod 9 = 5$

$$2^{-1}R_3 \Rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 7 & 0 \\ 0 & 0 & 1 & 6 & 3 & 5 \end{array}\right] \qquad \therefore A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 4 & 7 & 0 \\ 6 & 3 & 5 \end{bmatrix}$$

(VI) Let A as in (V). Solve over Z_9. Find x_1, x_2, x_3 in Z_9

s.t. $A \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 \\ 7 \\ 9 \end{bmatrix}$ [Hint: Multiply both sides of the equation by A^{-1}].

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = A^{-1} \begin{bmatrix} 2 \\ 7 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 4 & 7 & 0 \\ 6 & 3 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 7 \\ 9 \end{bmatrix}$$

$$= \begin{bmatrix} 2 \\ 3 \\ 6 \end{bmatrix}$$

$\therefore x_1 = 2, \quad x_2 = 3, \quad x_3 = 6$ in Z_9.

5/5

Name NAVEED AHMED, ID ~~[illegible]~~ 37868

HW III: MTH 530, Fall 2017

Ayman Badawi

QUESTION 1. Let $(D, *)$ be a group (D need not be abelian). Assume $|a| = 27$ for some $a \in D$. Prove that D has a subgroup with 9 elements.(Max 3 lines proof])

QUESTION 2. Let $(D, *)$ be an abelian group with 35 elements. Prove that there is an element $a \in D$ such that $D = \{a, a^2, ..., a^{35}\}$(Max 5 lines proof])

QUESTION 3. Let $(D, *)$ be a group with $n < \infty$ elements. Prove that $a^n = e$ for every $a \in D$ (Max 3 lines proof])

QUESTION 4. Let $D = (Z_{12}, *) \times (U(5), .)$

a) Find $|(4, 2)|$ (note $1 \in (Z_{12}, +)$ and $|1| = 12$)

b)Convince me that D has a subgroup with 24 elements.

QUESTION 5. Let $(D, *)$ be a group such that $|D| = q_1 q_2$ 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 $a^{22} = a^5$, $b^{16} = b^9$, and $a * b = b * a$. Find $|D|$. I claim that $D = \{c, c^2, ..., c^{q_1 q_2} = e\}$ for some $c \in D$. Prove my claim.(Max 6 lines)

QUESTION 6. Given $H = \{0, 5, 10\}$ is a subgroup of $(Z_{15}, +)$. Find all distinct left cosets of H in D.

QUESTION 7. (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 $k = wm + xn$)

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

6) $H = \{0, 5, 10\} \leq (\mathbb{Z}_{15}, +)$ 37/40

$0 + H = \{0, 5, 10\}$; $1 + H = \{1, 6, 11\}$; $2 + H = \{2, 7, 12\}$,

4/4 $3 + H = \{3, 8, 13\}$; $4 + H = \{4, 9, 14\}$

7) $|(D, *)| = n$, $\gcd(m, n) = 1$ and $a \in D$. Prove; $\exists b \in G : b^m = a$

$\gcd(m, n) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z} : mx + ny = 1$

Then $a^{1} = a^{mx+ny} = a^{mx} * a^{ny}$

$\Rightarrow a = a^{mx} * e$

4/4 $\Rightarrow a = (a^x)^m$. Let $b = a^x$ and we are done.

$\Rightarrow a = b^m$ QED

5) $(D, *) : |D| = q_1 q_2$

$a^{22} = a^5 \Rightarrow a^{17} = e$; $b^{16} = b^9 \Rightarrow b^7 = e \Rightarrow |a| = 17$; $|b| = 7$ ($b \neq e$)

($\because$ $|a| \mid 17$ and $a \neq e$, so $|a| = 17$, and $|b| \mid 17$ and $b \neq e$, so $|b| = 7$)

OK $|a * b| = |a| * |b| = 17 \times 7 = 119$. $119 \mid q_1 q_2 \Rightarrow q_1 = 7, q_2 = 17$.

$\therefore |D| = q_1 q_2 = 7 \cdot 17 = 119$. Let $a * b = c$, then

4/4 $D = \langle c \rangle = \{c, c^2, \ldots, c^{q_1 q_2 = 119} = e\}$. QED

4) $D = (\mathbb{Z}_{12}, *) \times (U(5), \cdot)$ 4

a) $|(4, 2)| = \dfrac{|4| \times |2|}{\gcd(|4|, |2|)} = \dfrac{3 \times 3}{3} = 3$.

4/4

b) Let the subgroup be H.

$|H| = 24 \Rightarrow 24 \mid |D|$ ($\because D$ is Abelian and finite)

4/4 $|D| = 12 \times 4 = 48$. and $24 \mid 48$.

$\Rightarrow \exists H : H \leq D$. QED

3) $|D| = n$. Let $a \in D$ such that $|a| = m$.

$\Rightarrow m \mid n \Rightarrow n = km$.

4/4 $\Rightarrow a^n = a^{km} = (a^m)^k = e$. QED

1) $|a| = 27$, $a \in D \Rightarrow 27 \mid |D|$.

$a^{27} = e$

4/4 $\Rightarrow (a^3)^9 = e$

Let the subgroup be $H = \{a^3, (a^3)^2, (a^3)^3, \ldots, (a^3)^9 = e\}$. QED

2) $|(D, *)| = 35$. D is Abelian.

$\Rightarrow \exists\ H \leq D$ s.t. $|H| = 7$ and $\exists F \leq D$ s.t. $|F| = 5$.

$|H|$ and $|F|$ are prime, so $H = \{c, c^2, c^3, \ldots c^7 = e\}$.

and $F = \{b, b^2, b^3, b^4, b^5 = e\}$

$\Rightarrow \exists\ c \in H, b \in F$ such that $|c| = 7$ and $|b| = 5$.

$\Rightarrow |c * b| = 35$.

Let $c * b = a$.

Then $D = \{a, a^2, \ldots, a^{35}\}$. QED.

MTH 530

Abstract Algebra I.

By: Ayman Badawi

HW 4.

Name: Yasmine ElAshi

I.D. : 73B.

$\frac{45}{50}$

Name ____________________, ID __________

HW IV: MTH 530, Fall 2017

Ayman Badawi

QUESTION 1. (Example of infinite group where each element has a finite order) We know that if $F1$ and F_2 are subgroups of a group D, then $F_1 \cup F_2$ need not be a subgroup of D. Now for each $n \in N^*$, let $F_n = \{x \in C^* | x^n = 1\}$.

5 a) Prove that $L = \cup_{i=1}^{\infty} F_i$ is a subgroup of $(C^*, .)$

5 b) For each $n \in N^*$, show that L has an element of order n (Hint: What is that order of $e^{\frac{2\pi i}{n}}$ where $i = \sqrt{-1}$)?

5 c) For each $n \in N^*$, how many elements of order n does L have?

QUESTION 2. (Example of infinite group where each element has a finite order) Consider the group $D = (\frac{Q}{Z}, \triangle)$, as usual for every $a, b \in Q$ we have $(a + Z))\triangle(b + Z) = (a + b) + Z$

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

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

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

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

10 **QUESTION 3.** Let $D = (Z_4, +) \times (Z_5^*, .)$ and $H = \{(a, b) \mid a \in \{0, 2\}, b \in \{1, 4\}\}$. Then $H \triangleleft D$ (you do not need to check this). Let $F = D/H$. Find the elements of the group $(D/H, \triangle)$. Find $|F|$. Construct the Caley table of F and for each $a \in F$ find $|a|$.

5 **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

Question 1: (Example of infinite group where each element has a finite order). We know that F_1 and F_2 are subgroups of D, then $F_1 \cup F_2$ need not be a subgroup of D.

Now for each $n \in \mathbb{N}^*$, let $F_n = \{x \in \mathbb{C}^* \mid x^n = 1\}$.

(a) Prove that $L = \bigcup_{i=1}^{\infty} F_i$ is a subgroup of $(\mathbb{C}^*, \cdot)$

Using Q1(i) from HW2, we have that if $(D,*)$ is an abelian group, and we fix a positive integer m, s.t. $F = \{a \in D \mid a^m = e\}$ then $(F,*)$ is a subgroup of D.

In this case, we have $D = \mathbb{C}^*$, $F = F_n$, and $e = 1$.

$\therefore$ $(F_n, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

We need to show that $L = \bigcup_{i=1}^{\infty} F_i$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

Let $a \in L$

$\Rightarrow a \in \bigcup_{i=1}^{\infty} F_i \Rightarrow a \in F_i$ for some $i \in \mathbb{N}^*$

since F_i is a subgroup of $\mathbb{C}^*$

$\Rightarrow a^{-1} \in F_i$ for some $i \in \mathbb{N}^*$

$\therefore (a^{-1})^i = 1$.

Let $b \in L$

$\Rightarrow b \in \bigcup_{i=1}^{\infty} F_i \Rightarrow b \in F_j$ for some $j \in \mathbb{N}^*$

$\Rightarrow b^j = 1$.

we have $n = ij \in \mathbb{N}^*$, we need to show $a^{-1}b \in L$.

$(a^{-1}b)^n = (a^{-1} \cdot b)^{ij} = (a^{-1})^{ij} b^{ij} = [(a^{-1})^i]^j \cdot (b^j)^i = (1)^j \cdot (1)^i = 1$.

since $\mathbb{C}^*$ is abelian

$\Rightarrow a^{-1}b \in F_n$ for some $n \in \mathbb{N}^*$

$\Rightarrow a^{-1}b \in \bigcup_{i=1}^{\infty} F_i = L$.

$\therefore$ we have shown that $L = \bigcup_{i=1}^{\infty} F_i$ is a subgroup of $(\mathbb{C}^*, \cdot)$

✓ Good

4/4

(b) For each $n \in \mathbb{N}^*$ show that L has an element of order n
(Hint: what is the order of $e^{\frac{2\pi i}{n}}$ where $i = \sqrt{-1}$).

Let $x = e^{\frac{2\pi i}{n}}$, $x^n = e^{\left(\frac{2\pi i}{\cancel{n}}\right)\cancel{n}}$

$= e^{2\pi i} = \cos(2\pi) + i\cancel{\sin(2\pi)}^{0} = 1$

4/4 : For each $n \in \mathbb{N}^*$ L has an element $x = e^{\frac{2\pi i}{n}}$ of order n.

(c) For each $n \in \mathbb{N}^*$, how many elements of order n does L have?

Let $F_n = \{x \in \mathbb{C}^* \mid x^n = 1\} \subseteq L$.

Let $x = e^{\frac{2\pi i}{n}}$, then $x^k = e^{\frac{2\pi k i}{n}}$ for some $k \in \mathbb{N}^*$

$(x^k)^n = \left(e^{\frac{2\pi k i}{\cancel{n}}}\right)^{\cancel{n}} = \cos(2\pi k) + i\cancel{\sin(2\pi k)}^{0} = 1$.

$\Rightarrow |F_n| = \infty$

Let $n \in \mathbb{N}^*$

~~Let x be of order n~~

Then $x^n - 1 = 0$ has exactly n distinct solutions over $\mathbb{C}$. In particular $(\mathbb{C}^*, \cdot)$ has a unique subgroup, say D, of order n, and such subgroup is generated by $e^{\frac{2\pi i}{n}}$ (since $|e^{\frac{2\pi i}{n}}| = n$). Let $a = e^{\frac{2\pi i}{n}}$.

0/4

Then $D = \{a, a^2, a^3, \dots, a^n = 1\}$.
We know $|a^k| = \frac{n}{\gcd(k,n)}$. Thus if $|b| = n$, then $b \in D$ because D is unique]. $b \in D$ and $|b| = n \Rightarrow b = a^i, 1 \le i \le n$ $\Rightarrow \gcd(i,n) = 1$. Hence there are exactly $\phi(n)$ elements of order n

Question 2: (Example of infinite group where each element has a finite order).

Consider the group $D = (\mathbb{Q}/\mathbb{Z}, \Delta)$ as usual for every $a, b \in \mathbb{Q}$ we have $(a+\mathbb{Z}) \Delta (b+\mathbb{Z}) = (a+b)+\mathbb{Z}$.

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

$$x = \frac{8}{12} + \mathbb{Z} = \frac{2}{3} + \mathbb{Z}$$

$\frac{8}{12}$ in reduced form is $\frac{2}{3}$, where $\gcd(2,3) = 1$.

$$\Rightarrow |x| = \left|\frac{8}{12} + \mathbb{Z}\right| = \left|\frac{2}{3} + \mathbb{Z}\right| = 3.$$

4/4

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

we have
$\gcd(1,12) = 1$
$\gcd(5,12) = 1$
$\gcd(7,12) = 1$
$\gcd(11,12) = 1$

$$\therefore F = \left\{ \left(\frac{1}{12} + \mathbb{Z}\right), \left(\frac{5}{12} + \mathbb{Z}\right), \left(\frac{7}{12} + \mathbb{Z}\right), \left(\frac{11}{12} + \mathbb{Z}\right) \right\} \Rightarrow |F| = 4.$$

$\therefore |F| = |U(12)|$, where $U(12) = \{a \in \mathbb{Z}_n^* \mid \gcd(a,n) = 1\}$.

$= \phi(12)$ since $12 = 2^2 \cdot 3$ we have $p_1 = 2$, $\alpha_1 = 2$, $p_2 = 3$, $\alpha_2 = 1$.

$= (p_1 - 1) p_1^{(\alpha_1 - 1)} \cdot (p_2 - 1) p_2^{(\alpha_2 - 1)}$

$= (2-1) 2^1 \cdot (3-1) \cdot 3^0$

$= 2 \cdot 2 = 4.$

4/4

$|F| = 4$ which can be seen above.

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

$$|F| = |U(m)| = \phi(m)$$

4/4

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

For each $n \in \mathbb{N}^+$, we have $a_n = \frac{1}{n} + \mathbb{Z} \in D$

where $|a_n| = n$.

we have $H_n = \{a_n, a_n^2, a_n^3, \dots, a_n^n = e\}$

is a subgroup of D.

$\therefore$ We can construct a subgroup H_n of D, where

$$H_n = \left\{\frac{1}{n} + \mathbb{Z}, \frac{2}{n} + \mathbb{Z}, \frac{3}{n} + \mathbb{Z}, \dots, \frac{n-1}{n} + \mathbb{Z}, \mathbb{Z}\right\}$$

where $|H_n| = n$.

<u>Question 3</u>: Let $D = (\mathbb{Z}_4, +) \times (\mathbb{Z}_5^*, \cdot)$ and $H = \{(a,b) \mid a \in \{0,2\}, b \in \{1,4\}\}$

Then $H \trianglelefteq D$ (you donot need to check this).

Let $F = D/H$. Find the elements of the group $(D/H, \triangle)$.

Find $|F|$. Construct Caley table of F and for each $a \in F$ find $|a|$.

① Find the elements of the group $(D/H, \triangle)$.

$$D = (\mathbb{Z}_4, +) \times (\mathbb{Z}_5^*, \cdot) : \begin{Bmatrix} (0,1), (0,2), (0,3), (0,4), \\ (1,1), (1,2), (1,3), (1,4) \\ (2,1), (2,2), (2,3), (2,4) \\ (3,1), (3,2), (3,3), (3,4) \end{Bmatrix}$$

$$(0,1) * H = \{(0,1), (0,4), (2,1), (2,4)\} = H.$$

$$(0,2) * H = \{(0,2), (0,3), (2,2), (2,3)\}$$

$$(1,1) * H = \{(1,1), (1,4), (3,1), (3,4)\}$$

$$(1,2) * H = \{(1,2), (1,3), (3,2), (3,3)\}$$

$$D/H = F = \{H, (0,2)*H, (1,1)*H, (1,2)*H\}$$

② $|F| = 4$.

③ Construct Caley table of F:

Δ	H	$(0,2)*H$	$(1,1)*H$	$(1,2)*H$
H	H	$(0,2)*H$	$(1,1)*H$	$(1,2)*H$
$(0,2)*H$	$(0,2)*H$	$(0,4)*H = H$	$(1,2)*H$	$(1,4)*H = (1,1)*H$
$(1,1)*H$	$(1,1)*H$	$(1,2)*H$	$(2,1)*H = H$	$(2,2)*H = (0,2)*H$
$(1,2)*H$	$(1,2)*H$	$(1,4)*H = (1,1)*H$	$(2,2)*H = (0,2)*H$	$(2,4)*H = H$

For each $a \in F$, find $|a|$

④ $|H| = 1$

$|(0,2)*H| = 2$

$|(1,1)*H| = 2$

$|(1,2)*H| = 2$

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 $m|n$. (Max 2 lines. Note x^k mean $a*H \Delta a*H \Delta \cdots \Delta a*H = a^k * H$.)

Proof Let $|a| = n < \infty$ where $a \in D$.

Let $|x| = m$, where $x = a*H \in D/H$.

we want to show $m|n$

$\therefore x^n = (a*H)^n = a^n * H = e*H = H$.

$\Rightarrow m|n$.

MTH 530

Abstract Algebra I.

Ayman Badawi

HW5.

$\frac{58}{75}$

Name: Yasmine ElAshi

I.D.#: 7313.

Question 1: Let D, H be cyclic groups and $F = D \times H$

(a) If D is infinite and H is infinite, prove that F is never cyclic.

Let D be an infinite cyclic group, $\exists\, a \in D$ s.t.

$$D = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$$

Let H be a finite cyclic group, $\exists\, b \in H$; where $|b| = |H| = n$.

$$H = \langle b \rangle = \{b, b^2, b^3, \ldots, b^n = e\}$$

$$\{ \ldots 1 \leq j \leq n\}.$$

Then $F = D \times H = \{(a^i, b^j) \mid i \in \mathbb{Z} \text{ and } 1 \leq j \leq n\}$

Let $\langle (a,b) \rangle = \{ (a,b)^i = (a^i, b^i) \mid i \in \mathbb{Z}\}$

since $i \in \mathbb{Z}$, $i = mn + k$ $\quad 0 \leq k < n$

$b^i = b^{mn+k} = b^k$ since $|b| = n$

$\therefore \langle (a,b) \rangle = \{ (a^{mn+k}, b^k) \mid m, n \in \mathbb{Z},\ 0 \leq k < n\}$

By construction $\langle (a,b) \rangle \subseteq F$

Let $c = (a^i, b^j) \in F$ s.t. $i \neq j$

Then $i = mn + k \quad 0 \leq k < n$
$j = mn + r \quad 0 \leq r < n$ $\Big\}$ $k \neq r$ since $i \neq j$

$(a^i, b^j) = (a^{mn+k}, b^{mn+r}) = (a^{mn+k}, b^r)$

$(a^i, b^j) \notin \langle (a,b) \rangle$ since $k \neq r$

$\Rightarrow F \nsubseteq \langle (a,b) \rangle$

$\Rightarrow F \neq \langle (a,b) \rangle$

Hence F is never cyclic.

5/7

You are not using any Result!

Assume $F = D \times H$ is cyclic

Let $L = \{e_D\} \times H < F$, a contradiction since L is finite and F is infinite cyclic.

(b) If D is infinite and H is infinite, prove that F is never cyclic.

Let D be an infinite cyclic group, then $\exists\, a \in D$ s.t.

$$D = \langle a \rangle = \{ a^i \mid i \in \mathbb{Z} \}$$

Let H be an infinite cyclic group, then $\exists\, b \in H$ s.t.

$$H = \langle b \rangle = \{ b^j \mid j \in \mathbb{Z} \}$$

Then $F = D \times H = \{ (a^i, b^j) \mid i, j \in \mathbb{Z} \}$

Let $\langle (a,b) \rangle = \{ (a,b)^i = (a^i, b^i) \mid i \in \mathbb{Z} \}$

By construction it is clear that $\langle (a,b) \rangle \subseteq F$

Let $c = (a^i, b^j) \in F$ s.t. $i \neq j$

then $c \notin \langle (a,b) \rangle \Rightarrow F \notin \langle (a,b) \rangle$

$\Rightarrow F \neq \langle (a,b) \rangle$, hence F is never cyclic.

5/

(c) Assume that D is finite and H is finite. Prove that F is cyclic if and only if $\gcd(|D|, |H|) = 1$.

Let D be a finite cyclic group, then $\exists\, a \in D$ where $|a| = |D| = n$

s.t. $D = \langle a \rangle = \{ a, a^2, a^3, \ldots, a^n = e \}$

Let H be a finite cyclic group, then $\exists\, b \in D$ where $|b| = |H| = m$

s.t. $H = \langle b \rangle = \{ b, b^2, b^3, \ldots, b^m = e \}$

$F = D \times H = \{ (a^i, b^j) \mid 1 \leq i \leq n,\ 1 \leq j \leq n \} \Rightarrow |F| = mn$

$\Rightarrow$ Suppose F is cyclic, then $\exists\, c \in F$ s.t. $|c| = mn$

Let $c = (a,b) \in F \Rightarrow |(a,b)| = mn$.

We know $|(a,b)| = \operatorname{lcm}(n,m) = \dfrac{mn}{\gcd(n,m)}$

since $|(a,b)| = mn$

$$\frac{mn}{\gcd(n,m)} = mn \Rightarrow \begin{array}{l} \gcd(n,m) = 1 \\ \gcd(|D|, |H|) = 1 \end{array}$$

5/

$\Leftarrow$ Suppose $\gcd(|D|, |H|) = \gcd(n,m) = 1$

We need to show F is cyclic

Let $c = (a,b) \in F$ then $|(a,b)| = \operatorname{lcm}(n,m) = \dfrac{nm}{\gcd(n,m)} = \dfrac{nm}{1} = nm$

we have found $c \in F$ s.t. $|c| = nm = |F|$, since F is finite

$F = \langle c \rangle = \langle (a,b) \rangle$

$\Rightarrow F$ is cyclic.

5

(d) In view of (c), we know that
$F = (\mathbb{Z}_{25}, +) \times (\mathbb{Z}_4, +)$ is a cyclic group.
Find all subgroups of F.

$(\mathbb{Z}_{25}, +) = \{0, 1, 2, 3, \ldots, 24\}$

$(\mathbb{Z}_4, +) = \{0, 1, 2, 3\}$

We have $\langle n \rangle = \mathbb{Z}_{25}$ when $\gcd(n, 25) = 1$

so for $\gcd(n, 25) \neq 1$, $n = 5, 10, 15, 20$

$\gcd(5, 25) = \gcd(10, 25) = \gcd(15, 25) = \gcd(20, 25) = 5$

$|5| = |1^5| = \frac{25}{\gcd(5,25)} = \frac{25}{5} = 5$

$\therefore |5| = |10| = |15| = |20| = 5$

$\Rightarrow \langle 5 \rangle = \langle 10 \rangle = \langle 15 \rangle = \langle 20 \rangle = \{0, 5, 10, 15, 20\}$ is a subgroup of $(\mathbb{Z}_{25}, +)$

We have $\langle n \rangle = \mathbb{Z}_4$ when $\gcd(n, 4) = 1$

so for $\gcd(n, 4) \neq 1$, we have $n = 2$

$\gcd(2, 4) = 2$

$|2| = |1^2| = \frac{4}{\gcd(2,4)} = \frac{4}{2} = 2$

$\langle 2 \rangle = \{0, 2\}$ is a subgroup of $(\mathbb{Z}_4, +)$

Subgroups of F:

$(\mathbb{Z}_{25}, +) \times \{0\}$ $\gcd(|\mathbb{Z}_{25}|, |\{0\}|) = \gcd(25, 1) = 1 \Rightarrow$ cyclic.

$\{0\} \times (\mathbb{Z}_4, +)$ $\gcd(|\{0\}|, |\mathbb{Z}_4|) = \gcd(1, 4) = 1 \Rightarrow$ cyclic.

$\langle 5 \rangle \times \{0\}$ $\gcd(|\langle 5 \rangle|, |\{0\}|) = \gcd(5, 1) = 1 \Rightarrow$ cyclic

$\{0\} \times \langle 2 \rangle$ $\gcd(|\{0\}|, |\langle 2 \rangle|) = \gcd(1, 2) = 1 \Rightarrow$ cyclic

$\langle 5 \rangle \times \langle 2 \rangle$ $\gcd(|\langle 5 \rangle|, |\langle 2 \rangle|) = \gcd(5, 2) = 1 \Rightarrow$ cyclic

$(\mathbb{Z}_{25}, +) \times (\mathbb{Z}_4, +)$ $\Rightarrow$ cyclic.

7/3

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

Proof: (1) show $NH = \{nh \mid n \in N \text{ and } h \in H\}$ is a subgroup of D

Let $a \in NH$, s.t. $a = n_1 h_1$, where $n_1 \in N$ and $h_1 \in H$
$b \in NH$, s.t. $b = n_2 h_2$, where $n_2 \in N$ and $h_2 \in H$

we need to show $a^{-1} b \in NH$

$a^{-1} = (n_1 h_1)^{-1} = \cancel{(h_1 n_1)^{-1}} = \cancel{\underbrace{n_1^{-1}}_{\in N} \underbrace{h_1^{-1}}_{\in H}} \Rightarrow$ ~~$a \in$~~ $\rightarrow h_1^{-1} n_1^{-1}$

since $N \trianglelefteq D$

$a^{-1}b = (n_1^{-1} h_1^{-1})(n_2 h_2)$
$= n_1^{-1}(h_1^{-1} n_2) h_2$ NO NO

since $N \trianglelefteq D$ $\longrightarrow = \underbrace{(h_1^{-1} n_2)}_{\in N} \underbrace{(h_1^{-1} h_2)}_{\in H} = n_3 h_3$

$a^{-1}b = h_1^{-1} n_1^{-1} n_2 h_2$
Let $n_3 = n_1^{-1} n_2 \Rightarrow$
$a^{-1}b = h_1^{-1} n_3 h_2 \Rightarrow$
$a^{-1}b = n_4 h_1^{-1} h_2$ (since $N \trianglelefteq D$) $\Rightarrow$ $a^{-1}b \in ND$

$a^{-1}b = n_3 h_3$ where $n_3 = n_1^{-1} n_2 \in N$
$h_3 = h_1^{-1} h_2 \in H \Rightarrow a^{-1} b \in NH$.
Thus NH is a subgroup of D.

(2) Suppose $H \trianglelefteq D$, that is $aH = Ha$ for some $a \in D$.
we need to show $NH \trianglelefteq D$
Let $nh \in NH$. Let $a \in D$
show $a(nh) = (nh)a$

$a(nh) = (an)h = \overset{n_1}{(na)} h = n_1(ah) = n_1(h_1 a) = (n_1 h_1)a$

$N \trianglelefteq D$ NO NO $H \trianglelefteq D$

$\therefore NH \trianglelefteq D$.

6/10

Question 3:

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

Proof: We have $|D| = 25$, and assume D has a unique subgroup H, s.t. $|H| = 5$.

Suppose D is NOT cyclic.

Let $b \in D$ s.t. $b \neq e$ and $|b| = m$

since $m \mid 25 \Rightarrow m = 1, 5$ or 25

$m \neq 1$, since $b \neq e$

$m \neq 25$, since D is not cyclic (there doesnot exist an element in D with order 25)

$\therefore m = 5$

Let $\langle b \rangle = \{b, b^2, b^3, b^4, b^5 = e\}$

where $\langle b \rangle$ is a subgroup of D and $|\langle b \rangle| = 5$.

Since H is a unique subgroup of order 5,

we must have $\langle b \rangle = H$

$\Rightarrow b \in H$

$\Rightarrow D \subseteq H$ which is impossible

We reach a contradiction,

$\therefore$ we conclude that D must be cyclic.

ok

6/

Question 4:

(a) Convince me that $(\mathbb{C}^*, \cdot)$ is not cyclic

Suppose $(\mathbb{C}^*, \cdot)$ is cyclic

Then $\mathbb{C}^* = \langle (a+bj) \rangle$ for some $a, b \in \mathbb{R}$ s.t. $a \neq 0$, $b \neq 0$

Since $1 \in \mathbb{C}^*$, then $\exists\, n \in \mathbb{Z}, n \neq 0$ s.t. $(a+bj)^n = 1$

$a + bj = Re^{j\theta}$ $\quad R = \sqrt{a^2+b^2}$ $\quad \theta = \tan^{-1}\left(\frac{b}{a}\right) \neq 0$

$(Re^{j\theta})^n = 1$

$\Rightarrow R^n = 1 \Rightarrow R = 1$

$\theta n = 0 \Rightarrow$ either $n = 0$ or $\theta = 0$ or both are zero, which is a contradiction to our assumption.

$\therefore (\mathbb{C}^*, \cdot)$ is never cyclic

9/4

I do not like it

$i^4 = 1$ so $(\mathbb{C}^*, \cdot)$ not cyclic

(b) Convince me that $(\mathbb{Q}^*, \cdot)$ is not cyclic

Suppose $(\mathbb{Q}^*, \cdot)$ is cyclic

Then $\mathbb{Q}^* = \langle \frac{p}{q} \rangle$ for some $\frac{p}{q} \in \mathbb{Q}$ where $\gcd(p,q) = 1$, $p, q \in \mathbb{Z}$ and $p \neq 0$ and $q \neq 0$

Since $\frac{1}{2} \in \mathbb{Q}$, then $\exists\, n \in \mathbb{Z}, n \neq 0$, s.t. $\frac{1}{2} = \left(\frac{p}{q}\right)^n$

$\Rightarrow p^n = 1 \Rightarrow p = 1 \in \mathbb{Z}$

$\Rightarrow q^n = 2 \Rightarrow q = \sqrt[n]{2} \in \mathbb{R}$ (irrational), but this is a contradiction since $q \in \mathbb{Z}$

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

I do not like it

$|-1| = 2$ so $(\mathbb{Q}^*, \cdot)$ not cyclic

5/0K

Convince me that $(\mathbb{Q}, +)$ is not cyclic.

Suppose $(\mathbb{Q}, +)$ is cyclic

Then $\mathbb{Q} = \langle \frac{p}{q} \rangle$ for some $\frac{p}{q} \in \mathbb{Q}$ where $\gcd(p,q) = 1$, $p, q \in \mathbb{Z}$ and $q \neq 0$

Since $\frac{p}{2q} \in \mathbb{Q}$, then $\exists\, n \in \mathbb{Z}, n \neq 0$, s.t. $\frac{p}{2q} = \left(\frac{p}{q}\right)^n = n\left(\frac{p}{q}\right)$

since binary operation is + (normal addition)

$\Rightarrow n = \frac{1}{2} \in \mathbb{Q}$

which is a contradiction, since $n \in \mathbb{Z}$

$\Rightarrow (\mathbb{Q}, +)$ is not cyclic.

5/5 OK

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

$|U(18)| = \phi(18) = 6$

$18 = 3^2 \cdot 2^1$

$\phi(18) = (3-1)3^1 \cdot (2-1)2^0 = 2 \cdot 3 = 6$

If $U(18)$ is cyclic, there must be $\phi(6) = 2$ generators

$U(18) = \{1, 5, 7, 11, 13, 17\}$

$5^1 = 5$

$5^2 = 25 \equiv_{18} 7$

$5^3 = 5^2 \cdot 5 \equiv_{18} 7 \cdot 5 = 35 \equiv_{18} 17$

$5^4 = 5^3 \cdot 5 \equiv_{18} 17 \cdot 5 = 85 \equiv_{18} 13$

$5^5 = 5^4 \cdot 5 \equiv_{18} 13 \cdot 5 = 65 \equiv_{18} 11$

$5^6 = 5^5 \cdot 5 \equiv_{18} 11 \cdot 5 = 55 \equiv_{18} 1$

$\therefore |5| = 6 = |U(18)|$

We have found an element $5 \in U(18)$ s.t. $|5| = 6 \Rightarrow U(18)$ is cyclic

The other generator is $5^5 = 11 \in U(18)$ since $\gcd(5,6) = 1$

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

$|U(16)| = \phi(16) = (2-1)2^3 = 8$

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

If $U(16)$ is cyclic there must be $\phi(8) = 4$ generators

$3^1 = 3$

$3^2 = 9$

$3^3 = 27 \equiv_{16} 11$

$3^4 = 3^3 \cdot 3 = 11 \cdot 3 = 33 \equiv_{16} 1$

$|3| = 4 \neq 8$

$5^1 = 5$

$5^2 = 25 \equiv_{16} 9$

$5^3 = 5^2 \cdot 5 \equiv_{16} 9 \cdot 5 = 45 \equiv_{16} 13$

$5^4 = 5^3 \cdot 5 \equiv_{16} 13 \cdot 5 = 65 \equiv_{16} 1$

$|5| = 4 \neq 8$

$7^1 = 7$

$7^2 = 49 \equiv_{16} 1$

$|7| = 2 \neq 8$

$9^1 = 9$

$9^2 = 81 \equiv_{16} 1$

$|9| = 2 \neq 8$

Since we have only 3 elements remaining 11, 13, 15, then we don't have to search further, and we conclude that $U(16)$ is not cyclic, since it must have 4 generators, and we have only three remaining, so none of the elements in $U(16)$ have order 8.

Question 5:

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

Proof: Let $\alpha = (a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7) \in S_{17}$

$\beta = (a_8\ a_9\ a_{10}\ a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15}\ a_{16}\ a_{17}) \in S_{17}$

s.t. $|\alpha| = 7$, $|\beta| = 10$

and α, β are disjoint.

$\Rightarrow \alpha \circ \beta = \beta \circ \alpha$ since disjoint

we also have $|\alpha \circ \beta| = \operatorname{lcm}[|\alpha|, |\beta|] = \operatorname{lcm}[7, 10] = 70$

Let $H = \langle \alpha \circ \beta \rangle \Rightarrow$ subgroup of S_{17}

$\Rightarrow H$ is cyclic $\Rightarrow H$ is abelian.

$\therefore H = \langle \alpha \circ \beta \rangle$ is an abelian, cyclic subgroup of S_{17}

where $|H| = 70$.

5/5

(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 $|f|$

$f = \underbrace{(1\,3\,4)}_{\alpha} \circ \overbrace{(2\,5\,8)}^{\beta} \circ \overbrace{(6\,7)}^{\gamma} \in S_8$

$|f| = \text{Lcm}(3, 3, 2) = 6$

Is $f \in A_8$?

$f = \alpha \circ \beta \circ \gamma$

$\alpha \to$ even fcn

$\beta \to$ even fcn

$\gamma \to$ odd fcn

$(\beta \circ \gamma) \to$ odd fcn

$\alpha \circ (\beta \circ \gamma) \to$ odd fcn

$\Rightarrow$ f is an odd fcn.

$f \notin A_8$.

$\alpha = (1\,3\,4) = (1\,4) \circ (1\,3)$

$\beta = (2\,5\,8) = (2\,8) \circ (2\,5)$

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

5 (2-cycle)s

$\Rightarrow f$ is odd fcn.

(c) Let $n = \max\{|f|, \text{ where } f \in A_9\}$

$n = 9$ since $f = (a_1\, a_2 \cdots a_9) \in A_9$ where $|f| = 9$ is the maximum order of f, s.t. $f \in A_9$

0/4

$\alpha = (1\,2\,3\,4\,5)(6\,7\,8)$ $\in A_9$

$|\alpha| = 15$

(d) Let $f \in S_n$ $(n \geq 3)$ be an odd fcn. Prove that $|f|$ is an even number.

Proof: $f = (a_1\, a_2 \cdots a_k)$

$|f| = k$

$f = (a_1\, a_k) \circ (a_1\, a_{k-1}) \circ \cdots \circ (a_1\, a_2)$

$(k-1)$ 2-cycles

Since f is an odd fcn

$k - 1 = 2m + 1$ for some positive integer m

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

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

$\Rightarrow k$ is an even number

Since $|f| = k$

$|f|$ is even number

WAW

If $k-1$ is odd

k is even

Let $n = |f|$.

We know

$A_n \triangleleft S_n$.

Let $m = |f \circ A_n|$.

$|m| = 2$. Hence, we know

$m \mid n \Rightarrow 2 \mid n \Rightarrow n$ is even

0/5