Name————————————, ID —————

Webpage-MTH320-Course Portfolio-Fall 2020

Ayman Badawi

Table of contents

1 Section : Course Syllabus

AUS | الجـامـعـة الأمـيـركـيـة فـي الـشـارقـة
American University of Sharjah

COURSE SYLLABUS

Warning: During this difficult time, "trust" relationship between students and instructor will definitely facilitate our work, to ensure that this "trust" is not violated, suspicious Respondus reports (after exams) will be sent to the Associate Dean

<table>
<tr><td>A</td><td><b>Course Title & Number</b></td><td><b>MTH 320: Abstract Algebra</b></td></tr>
<tr><td>B</td><td><b>Pre/Co-requisite(s)</b></td><td>Prerequisite: MTH 221</td></tr>
<tr><td>C</td><td><b>Number of credits</b></td><td>3</td></tr>
<tr><td>D</td><td><b>Faculty Name</b></td><td>Ayman Badawi</td></tr>
<tr><td>E</td><td><b>Term/ Year</b></td><td>Fall 2020</td></tr>
<tr><td>G</td><td><b>Instructor Information</b></td><td>
<table>
<tr><th>Instructor</th><th>Office</th><th>Telephone</th><th>Email</th></tr>
<tr><td>Ayman Badawi</td><td>Nab 262 / Home</td><td></td><td>abadawi@aus.edu</td></tr>
</table>
<b><u>Office Hours</u></b>: UTR 15:00-16:00. Others by appointment, just email me .
.
</td></tr>
<tr><td>H</td><td><b>Course Description from Catalog</b></td><td>Covers semi-groups, monoids, groups, permutation groups, cyclic groups, Lagrange's Theorem, subgroups, normal subgroups, quotient groups, (external) direct product of groups, homomorphism and isomorphism theorems, Cayley's Theorem, and introduction to rings and fields (if times allowed).</td></tr>
<tr><td>I</td><td><b>Course Learning Outcomes</b></td><td>Upon completion of the course, students will be able to:
1. Demonstrate knowledge and understanding of groups, subgroups, order of an element in finite groups, Lagrange Theorem , and to construct proofs to groups. Exam I, final
2. Demonstrate knowledge and understanding of the concept of cosets of a subgroup of a group, normal subgroups, quotient groups, symmetric groups, cyclic groups and their properties. Exam I, Exam II, Final
3. Demonstrate knowledge and understanding of direct product of groups. Exam II, Final
4. Demonstrate knowledge and understanding of the concept of group homomorphism and isomorphism. Exam II, Final
5. Demonstrate knowledge and understanding of the method on classification of finite abelian groups. Final</td></tr>
<tr><td>J</td><td><b>Textbook and other Instructional Material and Resources</b></td><td><b><i>Class Notes (Very Crucial and it should be the main source for this course). Materials on I-Learn. Personal Webpage (for old HW's, Exam, Finals):</i></b>
<b><i>http://www.ayman-badawi.com/MTH%20320.htm</i></b>

<b><i>(Optional not required) Contemporary Abstract Algebra, Seventh Edition by Joseph A. Gallian</i></b></td></tr>
</table>

K Teaching and Learning Methodologies

All thoughts are popped out of the harmonic parts of my brain. To me I just enjoy listening to the musical abstract algebra tones. Students are expected to learn a new line of thinking.

L Grading Scale, Grading Distribution, and Due Dates

Grading Scale

85 – 100	4.0	A
82 – 84	3.7	A-
77 - 81	3.3	B+
72 - 76	3.0	B
68 – 71	2.7	B-
64 –67	2.3	C+
58– 63	2.0	C
50– 57	1.7	C-
40– 49	1.0	D
Less than 40	0	F

Note: Tests and other graded assignments due dates are set. No addendum, make-up exams, or extra assignments to improve grades will be given.

Grading Distribution

Assessment	Weight	Due Date
Homework	15%	TBA
Two exams	50%	TBA
Final	35%	TBA
Total	100%	

M Explanation of Assessments

The methods I used for assessments are very much standard methods that are used by most universities world-wide.

N Student Academic Integrity Code Statement

All students are expected to abide by the Student Academic Integrity Code as articulated in the AUS undergraduate catalog.

SCHEDULE

CHAPTER	NOTES
01: Introduction to groups, semi-groups and monoids	• Introduction to the Course
02: Groups	• Examples and that include the symmetric group
03: Finite groups, subgroups	• LaGrange theorem and its application
04: subgroups and cosets	• Definition and properties
06: Order of an element in a group	• Definition and its connection with LaGrange theorem
08: Cyclic groups	Definition and its properties
09: Cyclic groups	• More properties of cyclic groups
10: Review	• Over the above material
11: Permutation group	• Definition and examples
13: Permutation group	• Write an element as disjoint cycles and determine the order of an element, and discuss even permutations
14: Normal subgroups and quotient groups	• Definition and properties
16: Group homomorphism and isomorphism	Definition and examples
17: Group homomorphism and isomorphism	• First isomorphic Theorem and its uses
18: External and internal direct product of groups	• Definition, examples, and properties
22: External and internal direct product of groups	• More properties, determine the order of an element of a direct product of groups and determine when a direct product of groups is cyclic
• Classification of finite abelian groups	• Just explain the method without proofs
• **Presentations and Course Revision**	•
Final Exam	**COMPREHENSIVE**

2 Section : Academic Integrity Measures

Academic Integrity Measures in Online Exams

List the measures taken to ensure the academic integrity of the exam.

Homework's 1-6, each HW was posted on I-Learn. Students were given one week to ten days to solve the questions. All questions are essay.

Students used lockdown browser for exams one, two and final exam. All questions are essay. Students submitted their solution in a folder that I created on I-learn. The outcome (scores) was not significantly different from a normal in-class exams (see the scores of the students in the excel-sheet)

I am completely satisfied with the outcome of MTH320.

3 Section : Instructor Teaching Material-Handouts

3.1 2017 All HWs with Solution

Name TAHA AMEEN, ID @00066555

HW One: Abstract Algebra, MTH 320,Fall 2017

24/25

Ayman Badawi

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)

$\rightarrow \frac{4}{4}$

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

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

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

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

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

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

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

$\frac{8}{8}$

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

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

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

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 $a^n = e = 6$, $\quad \underline{\underline{|a| = 4}}.$

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

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 $D = \{f : \mathbb{R} \to \mathbb{R} \mid f$ 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 $b*a^2 = b*a*a = b*(a*a)$

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

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

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

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

?!

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

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

~~$a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ 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 @000 66555

HW One: Abstract Algebra, MTH 320,Fall 2017

4/4

Ayman Badawi

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 $0 \leq i, k \leq 3$. What is $H_0 \cup H_1 \cup H_2 \cup H_3$?] 5/5

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

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

(iii) Let $n \geq 2$ 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., $a^{\phi(n)} \equiv 1 \; (mod \; n)$) 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. 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. 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? 4/4

(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). 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]. 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 $\{b \; o \; R_1, b \; oR_2,$ 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] 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] 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 $R_i = R_1^i = R^{i-1} \; oR_1 = R_{i-1} \; o \; R_1$. 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] 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 $2 \leq i \leq 10$? 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 $e = H_0 = \{0,4\}$.

1/1

Finding d^{-1} ∀ $d \in D$:

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

4/4

→ Observation:

$H_i \cap H_k = \phi$ ∀ $0 \leq i,k \leq 3$.

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

∴ 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: $(a*b)*(b^{-1} * a^{-1})$

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

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

$= a * a^{-1}$

$= e$.

4/4

∴ Since the Inverse is Unique,

$(a*b)^{-1} = b^{-1} * a^{-1}$ ∎

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

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

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

Good

4/4

$$\left\{\begin{aligned} a * b &= (a * b)^{-1} && \text{[From (1) Above]} \\ &= b^{-1} * a^{-1} && \text{[From Q2(i)]} \\ &= b * a && \text{[From (1) Above]} \end{aligned}\right.$$

■

$\therefore$ 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: $3^1 = 3$. $3^2 = 3*3 = 1 \implies |3| = 2$.

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

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

$\therefore$ 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:

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

(ii) $(D_n, \circ)$ is the dihedral group of order '$2n$'.

<u>NOTE</u>: 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, $|R| = |Re| = n$. $\therefore \forall\ 1 \leq i, j \leq n,\ i \neq j \Rightarrow R_i \neq R_j$

★ 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 : $b = d * a^{-1}$.

Then, $\cancel{b} = \cancel{d} * \cancel{d}$.

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

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). ■

$\frac{4}{4}$

(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 $i \neq j$.

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 $R_i \neq R_j\ \forall\ i \neq j$ as $|R| = n$.

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

$\therefore |\{b * R_1, b * R_2, \ldots, b * R_n\}| = n$ 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, $b \in Re \Rightarrow |b| = 2 \Rightarrow b = b^{-1} \Rightarrow b^{-1} * c = b * c \in R$ ■

$\frac{4}{4}$ $\therefore b * c \in R \quad \forall\ b, c \in Re$.

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

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

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

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

$\frac{4}{4}$ $\therefore (Re)_k = (Re)_{k-1} * R_1$. We use this result as follows:

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

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

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

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

$\{(Re)_1, (Re)_2, (Re)_3, (Re)_4, (Re)_5\}$ 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): $(a^m)^k = e \Rightarrow a^{mk} = e$.

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

$\frac{4}{4}$

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

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

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

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

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

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

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 $a \neq e$ $b \neq e$ $a^{22} = a^{15}$, $b^{43} = b^{32}$, 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

Question 1: (i)

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

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

Proof:

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

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

Assume $|a| = k$. , since $k | n$ 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 $\Longrightarrow$ with $\underline{k}$ elements

Lagrange $\Longrightarrow$ $k | n$ $\Longrightarrow$ $a^n = e$

(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 $D = \{ c_1 , c_2 , ---- c^{q_1 q_2} = e \}$

let $C = a*b$.

$|c| = |a*b|$

$|c| = |a|*|b|$

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

~~the~~ $q_1 = 7$ & $q_2 = 11$.

$|c| = 7 \cdot 11 = 77$

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

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

prove $(F,*)$ is asubgroup.

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

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

we want to Find $(a^{-1} * b)^m = ?$.

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

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

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

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

$$= \boxed{e}$$

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

$\therefore$ F is asubgroup 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 tocheck to proof that F is asubgroup 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 asubgroup of C.

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

$a^n = e$.

let $a \& b \in D$.

$|a| = k$

$\boxed{a^k = e}$

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

$(\gcd(m,n) = k) \Rightarrow \boxed{k = wm + xn}$

$\boxed{k = 1}$.

$$1 = wm + xn$$

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

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

$$a = (a^w)^m * \underset{e}{\underset{\Downarrow}{(a^n)^x}}$$

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

let $b = a^w$

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

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

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

$f_1 = (35)$, $f_2 = (3142)$, $f_3 = (6453)$.

ⓐ $f_1 \circ f_3 = (35)\circ(6453)$

$= (364)$

ⓑ $f_2 \circ f_1 = (3142)\circ(35)$

(14235)

ⓒ $f_3 \circ f_2 = (6453)\circ(3142)$

$= (153)(264)$

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

ⓘ $L*H = ?$

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

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

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

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

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

(ii) ⇒ Question (5)

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

$|a| = 9$, $|b| = 8$.

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

So, $\boxed{|a^6| = 3}$ ✓

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

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 $|g| = 4. = |b^2| = \dfrac{|b|}{\gcd(2,|b|)} = \dfrac{8}{\gcd(2,8)} = \dfrac{8}{2} = \textcircled{4}$.

So, $|c| = |a*b^2|$ ✓
$(c = a*b^2)$.

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

$\therefore \exists\, q \in \mathbb{Z}$ 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 $|b| \,\big|\, n$. $\therefore 7 \mid n$ and $11 \mid n$.

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 $|L| = q_1 q_2$

$\therefore$ $\underline{L = D}$. $\underline{c = a * b}$.

✓

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

To Prove: $a^{-1} * b \in F$ ✓

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

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. $|c| = 36$.

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

→ $\gcd(|a|,|b^2|) = \gcd(9,4) = 1$

✓

→ The group is Abelian.

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

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 $F < D$. ■

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

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 $a = b^m$ ■

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

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

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

<u>ANSWER 5</u> (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):

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

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

(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, $F = \left\{ \frac{1}{12}+\mathbb{Z}, \frac{5}{12}+\mathbb{Z}, \frac{7}{12}+\mathbb{Z}, \frac{11}{12}+\mathbb{Z} \right\}$.
- The numerators are relatively prime. $\therefore \gcd = 1 \Rightarrow |y| = 12$.
- Although $\left|\frac{2}{24}+\mathbb{Z}\right| = 12$, etc. $\frac{2}{24}+\mathbb{Z} = \frac{1}{12}+\mathbb{Z}$ and we do not repeat elements in a set. $\therefore |F| = 4$.

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

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

(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 $\left|\frac{1}{n}+\mathbb{Z}\right| = n$ $\because \gcd(1,n) = 1 \; \forall n$.

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

- This reduces to :

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

(2) $D = \{a, a^2, a^3, \dots, a^{12} = e\}$

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

(i) Cayley's Table of H.

$\star$	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 $(D/H, \Delta)$

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

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

$H_2 = a_2 * H_0 = \{a^6, a^{10}, a^2\}$

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

→ we have 4 cosets. This is as Expected $\because \frac{|D|}{|H|} = \frac{12}{3} = 4$.

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

$$\begin{aligned} H_1 \Delta H_2 &= (a^1 * H_0) \Delta (a^2 * H_0) \\ &= (a^1 * a^2) * H_0 \\ &= a^3 * H_0 \\ &= H_3 \,// . \end{aligned}$$

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

- $H_0 = H = \{1,14\} \lhd D$
- $H_1 = 2 * H_0 = \{2,13\}$
- $H_2 = 4 * H_0 = \{4,11\}$
- $H_3 = 7 * H_0 = \{7,8\}$

Δ	H_0	H_1	H_2	H_3
H_a	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) $H \lhd D$. $|a| = n < \infty$. $x = a * H \in D/H$, $|x| = m$

To Prove: $m \mid n$.

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

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

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

Name TAHA AMEEN, ID @00066555

MTH 320 Abstract Algebra Fall 2017, 1–1

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

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

5

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)

5

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

[illegible] $\frac{54}{55}$

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

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

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

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

5/5 ✓

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

To Prove: (I) $NH < D$, (II) $H \triangleleft D \longrightarrow NH \triangleleft D$.

(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

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

$= n_k * h_m$ | ∵ 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 $a \in D$

$a * NH = \{a * n_a h_b \mid n_a \in N \wedge h_b \in H\}$

$= \{a * n_a * h_b\} = \{n_c * a * h_b\}$ | $\because N \lhd D$

5/5

$= \{n_c * h_d * a \mid n_c \in N \wedge h_d \in H\}$ | $\because H \lhd D$

$= NH * a$ (By Definition)

$\therefore NH \lhd D$ ■

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!

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

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

Deny. ∴ $\exists!\ a, a^{-1}$ 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 ∴ $(\mathbb{Q}^*, *)$ cannot be cyclic.

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

Deny. ∴ $\exists!\ a, a^{-1}$ st. $\mathbb{Q} = \langle a \rangle = \langle a^{-1} \rangle$. 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 $a^m = 0\ \forall\, m$. ∴ 0 cannot be a Generator (The Identity can never be the Generator).

∴ $(\mathbb{Q}, +)$ cannot be cyclic.

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

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

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

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

∴ $U(18) = \langle 11 \rangle$ 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 $\phi(16) = 8$.

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

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 $|15| = 2$. $\therefore \sim[\exists\, a \in U(16)$ s.t $|a| = \phi(16)]$

$\therefore U(16)$ cannot be Cyclic ■ ✓

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

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

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

$\therefore \exists\, H = \langle h \rangle < S_{17}$. $H = \{h, h^2, h^3, \ldots, h^{70} = e\}$. ✓ 5/5

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

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

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

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

$\therefore f$ is Odd $\Longrightarrow f \not\subset A_8$ ■ ✓ 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 $|f| = \text{LCM}(3, 5) = 15$.

→ 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.

$\therefore \underline{\underline{n = 15}}$. ✓

(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

HW SIX, Abstract Algebra, MTH 320, Fall 2017

Ayman Badawi

~~54~~ $\frac{49}{50}$

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 $f : (D, *) \rightarrow (D, *)$ 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 $f : (D, *) \rightarrow (D, *)$ 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 $f : (D, *) \rightarrow (D, *)$ 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 $D = \{f : (Z_{18}, +) \rightarrow (Z_{18}, +) \mid f \; is \; a \; group-isomorphism\}$. Hence $D \subset S_{18}$.

(i) Let $K : (Z_{18}, +) \rightarrow (Z_{18}, +)$ 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: $|D| = p^5$. $H \lhd D$; $|H| = p^4$; H is cyclic.
$F \lhd D$; $|F| = p$; $F \not\subseteq H$

To Prove: D is Abelian and Not cyclic.

Strategy: we show $D \cong \mathbb{Z}_{p^4} \times \mathbb{Z}_p$:

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

clearly, $F \cap H = \{e\}$ $\Big|$ $\because |F| = p$, $F \not\subseteq H$.

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

$\therefore D \cong H \times F$

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

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

✓ [illegible]/2

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

Step II: Equal Cardinality
Clear, As $|D| = |D|$ → that does not make f 1-1

Step III: ONTO : $\forall\ x\ (= m*a_i*m^{-1}) \in$ Range(f)
$\exists\ a_i \in$ 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 ⟺ 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 ∵ f is a homomorphism

∴ $a * b * a * b = a * a * b * b$

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

∴ D is Abelian.

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

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

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

∴ f is a Homomorphism. ■

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

4/4 To Show: f is a Group Isomorphism

Since $\langle a \rangle = \langle a^3 \rangle$, | ∵ $|a^3| = \frac{|a|}{\gcd(3,10)} = \frac{|a|}{1} = 10$

Both $\langle a \rangle = D$

AND $\langle a^3 \rangle = f(D)$ are Isomorphic to $\mathbb{Z}_{10}$ and Therefore Isomorphic to each other.

∵ $b = a^i \Rightarrow f(b) = a^{3i}$ $\forall b$,

$\therefore f$ is a Group Isomorphism.

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

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

Since $|\text{Range}(f)| = |D|/|\text{Ker}(f)|$ $\quad$ Range$(f) = D$ //

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

Since $d H d^{-1}$ is finite, it is sufficient to show closure.

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

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

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

4/5 $\quad = d * (h_k) * d^{-1}$, $h_k \in H$ $\because$ H is a group.

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

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

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

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

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

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

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

5/4

<u>(vi)</u> $|D| = 5^3 7^2$. $\quad |H| = 7^2$ (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) $|D| = pq$, $H \lhd D$, $|H| = p$, $F \lhd D$, $|F| = q$

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 $H \cap F = \{e\}$.

4/4 $\therefore D \cong F \times H \cong \mathbb{Z}_q \times \mathbb{Z}_p$ ($\because$ F and H are cyclic).

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

$\therefore$ D is cyclic ∎

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

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

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

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

3.2 2017 Exam One with Solution

Name Yousuf Abo Rahma, ID [illegible]

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

Exam I: Abstract Algebra, MTH 320,Fall 2017

Ayman Badawi

Excellent

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

1. Yousuf Abo Rahma

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

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

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

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

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

5/5

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

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

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

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

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

using (i)

next page shorter proof

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

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

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

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

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

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

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

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

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

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

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

$= y*x$

5/5

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

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

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

in Z_6 : $|5| = |1| = 6$
in Z_5^* : $|2| = 4$ $\Rightarrow$ $|(5,2)| = \text{lcm}(6,4) = 12$

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

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

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

$\Rightarrow$ $F_1 \times F_2$ is a sub group of order 4
$L_1 \times L_2$ is a subgroup of order 4

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

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

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

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

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

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

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

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

Since both are cyclic with 6 eliment we ~~th~~ they are isomorphic

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

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

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

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

$\Rightarrow$ they are not isomorphic

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

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

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

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

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

~~[illegible]~~

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

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

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

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

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

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

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

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

$\Rightarrow f$ is a homomorphism

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

Yes, there is.

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

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

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

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

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

First: observe $a \in a*H \xRightarrow{\text{by hypothesis}} a^4 \in a*H \Rightarrow a^4 = a*n$ (some $n \in H$)

$\Rightarrow a^3 = n \in H$. Hence $n^{-1} = a^{-3} \in H$.

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

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

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

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

Faculty information

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

Q1 (ii) continues here

To show $C \triangleleft D$ we show that $\forall a \in D$

$a * C = C * a$. ~~[illegible]~~

$\Rightarrow$ let $a \in D$, $c \in C$ show that $a * c * a^{-1} \in C$.

$a * c * a^{-1} = a * a^{-1} * c = c \in C$. $\Rightarrow C \triangleleft D$.

Exam I: Abstract Algebra, MTH 320,Fall 2017

Ayman Badawi

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

2. Taha Ameen

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

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

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

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

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

$\therefore b^{-1}*a = a*b^{-1}$ ■

5/5

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

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

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

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

$= x*(b^{-1}*a)$ ■ (By Part (i))

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

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

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

5/5 ✓

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

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

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

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

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

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

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

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

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

5/5

see Page 10/13

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

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

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

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

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

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

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

—— Constructing H_1:

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

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

$|H_1| = 2 * 2 = 4$ ✓.

—— Constructing H_2:

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

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

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

2/3 $\underline{|D| = 24}$. In other words we show D is NOT Cyclic.
($\therefore$ It cannot have element of ~~order~~ 24)

Maximum possible Order of an Element in D:

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

$\therefore |(a,b)| = LCM(|a|, |b|) = \frac{|a||b|}{gcd(|a|,|b|)}$ But $gcd(|a|,|b|) = gcd(6,4) = 2$

$\therefore |(a,b)| = 12$ at max $\Rightarrow$ NEVER Cyclic.

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

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

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

H must Contain Identity

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

Consider Subgroups ~~(non trivial)~~:

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

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

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

$\leftarrow$

See page 10/13

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

YES:

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

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

4/4

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

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

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

$\therefore (\mathbb{Z}_{41}^*, *)$ is cyclic.

4/4

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

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

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

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

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

Rewrite f:

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

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

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

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

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

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

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

6/6

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

$\because u | (\alpha u)$

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

Note: $m n = d u$

⟵ (Contd. on previous Page)

see page 13/13

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

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

6/6

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

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

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

Contd. on previous page - See page 11/13

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

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

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

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

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

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

see page 12/13

$\rightarrow$ (PTO)

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

see page 4/13

Faculty information

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

Q1(iii) Continues

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

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

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

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

$$= a_2 * a_1$$

■

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

D is Abelian.

If $L = N_1 \times N_2 \rightarrow N_2 = \mathbb{Z}_5^*$, and $|N_1| \geq 2$
$\Rightarrow |L| \geq 8$, Impossible since $|L| = 4$

Q2 (iv) → Let $x = (3,2) \Rightarrow |x| = 4$.

~~(3,2)~~ (0,4), (0,3)

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

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

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

But

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

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

not clear!

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

~~Makes it Cyclic~~

Q4(i) continues

∴ If such a homomorphism Exists:

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

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

we want to maintain that $|f(a)|\,|\,|a|$

and $f(a^{-1}) = [f(a)]^{-1}$

∴ Possible orders of remaining elements in $\mathbb{Z}_{18}$:

2, 3, 6, 9, 18

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

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

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

$$\therefore f(1) = 3$$

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

checking for homomorphism:

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

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

$$= 3^i * 3^j \text{ ~~mod~~}$$

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

Q4(ii) continues

$\therefore$ H is Unique.

Part II:

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

$|D| = 155$. Let $a \in D$.

$$|a| = \underbrace{1}_{\downarrow} \text{ (or) } \underbrace{5}_{\downarrow} \text{ (or) } \underbrace{31}_{\downarrow} \text{ (or) } 155$$

Identity

Elements in H (∵ H is Unique)

So we have 4 elements of order 5.

NONE

$\therefore \exists$ 150 Elements in D s.t their order is 155.

Pick any one, call it 'a'.

$$|a| = 155 = |D|$$

$$\Downarrow$$

D is Cyclic ■

Q3(iv) Continues

Strategy :

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

and an Element of Order m $(=b)$

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

a^m will do :

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

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

- $a * b = b * a \Rightarrow a^m * b = b * a^m$.
- $\gcd(\frac{n}{d}, m) = 1$.
- $\therefore |a^m * b| = |a^m||b| = (\frac{n}{d})(m) = u$.

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

i.e $\langle a^{|b|} * b \rangle$ and $|H| = 4$

3.3 2017 Exam II with Solution

Name Taha Ameen, ID 66555

MTH 320 Abstract Algebra Fall 2017, 1–3

Exam II, Abstract Algebra, MTH 320,Fall 2017

Ayman Badawi

Score = $\frac{}{63}$

$\frac{47}{47}$

QUESTION 1. Let $(D, *)$ be a finite group with 245 elements. Assume that D has a normal subgroup with 5 elements and it has also a subgroup with 49 elements. Prove that D is an abelian group. Up to isomorphism, find all possible structures of D.

$|D| = 245$. $\exists H_1 \lhd D$ st $|H_1| = 5$ and $\exists H_2 \lhd D$ s.t. $|H_2| = 49$.

WHY!

7/10

<u>To Prove</u>: D is Abelian.

$H_1 * H_2 \lhd D$. $|H_1 * H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|}$ | But $|H_1 \cap H_2| = 1$.

$\because H_1 \cap H_2 = \{e\}$ (or) H_1 ($\because |H_1|$ is prime). But $|H_1| \nmid 49$

$\therefore |H_1 * H_2| = \frac{|H_1||H_2|}{1} = \underline{\underline{245}}$. $\therefore \underline{\underline{H_1 * H_2 = D}}$.

So $H_1 \cap H_2 = \{e\}$

<u>Further</u>: $H_1 \cap H_2 = \{e\}$ (Explained $\nearrow$).

$\therefore D \cong H_1 \times H_2$. $|H_1| = 5 \Rightarrow$ Abelian. $|H_2| = 49 = p^2 (p = 7)$ $\therefore$ Abelian

$\therefore H_1 \times H_2$ is Abelian $\Rightarrow$ D is Abelian.

$H_1 \cong \mathbb{Z}_5$ and $H_2 \cong \mathbb{Z}_{49}$ (OR) $\mathbb{Z}_7 \times \mathbb{Z}_7$ [Classification of Abelian groups]

$\therefore D \cong \mathbb{Z}_5 \times \mathbb{Z}_{49}$ (OR) $D \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_7$

QUESTION 2. Let $(D, *)$ be a finite group with 125 elements. Prove that D is not simple.

$|D| = 125$ is a finite group

$\therefore |D| = p^3$. $\therefore |C(D)| \geq p$ (i.e. ≥ 5).

5/5

$\therefore \exists H = C(D) \lhd D$.

But the Centre is always a <u>Normal Group</u>.

$\therefore |C(D)| \geq p$ and $\underline{C(D) \lhd D}$.

If $|C(D)| = 5$ (or) 25, $\exists H$ st $|H| = 5$ (or) 25 s.t $H \lhd D$.

If $|C(D)| = 125$, the group is Abelian (PTO)

But

converse of Lagrange Theorem is True for Abelian groups.

$\therefore\ \exists\ H_1, H_2$ st $|H_1| = 5$, $|H_2| = 25$

and $H_1 \lhd D$, $H_2 \lhd D$

(All Subgroups of Abelian Groups are Normal)

$\therefore$ In All Cases,

we have normal Subgroups in D which

7 are non-trivial, and not Equal to D

$\therefore D$ is never Simple.

QUESTION 3. Does A_6 have a subgroup, say H, of order 72? if yes, then what is the maximal order of a cyclic subgroup of H. If No, then explain clearly.

~~$|A_6| = 360$ A has elements of order 2, 3, 5 by Cauchy.~~

~~'5' is the maximum possible Order~~

~~If H had a S.G of order 72,~~

~~the maximal Cyclic Subgroup of H would have~~

A_6 is Simple. If A_6 had S.G of order 72, then $[A_6 : H] = 5$.

$\therefore \exists f : A_6 \longrightarrow S_5$ which is a non-trivial homomorphism

$Ker(f) \neq A_6$. $Ker(f) \neq \{e\}$ $\because$ $A_6/Ker(f) \cong Range(f)$ and if $Ker(f) = \{e\}$ then $A_6/\{e\} \cong L$, where $L < S_5$

But $\frac{|A_6|}{|\{e\}|} = 360$ and $|S_5| = 120$ (Impossible for Subgroup to have more Elements than Group).

$\therefore$ $Ker(f) \neq \{e\} \neq A_6$ and $Ker(f) \lhd A_6$. But A_6 is Simple. Contradiction

6/6

QUESTION 4. (i) Is $Z_2 \times Z_4 \times Z_{12}$ isomorphic to $Z_8 \times Z_{12}$? EXPLAIN

NO. Deny. Then $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \cong \mathbb{Z}_8 \times \mathbb{Z}_{12}$

$\Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_8$.

But, $\exists$ $a \in \mathbb{Z}_8$ st $|a| = 8$ but not in $\mathbb{Z}_2 \times \mathbb{Z}_4$.

contradiction

5/5

(ii) Let $n = 2^7 \cdot 5^2 \cdot 7^3$. Write $U(n)$ in terms of products of its invariant factors.

$n = 2^7 * 5^2 * 7^3$

$\therefore U(n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^5} \times \mathbb{Z}_{20} \times \mathbb{Z}_{294}$

i.e. $\mathbb{Z}_2 \times \mathbb{Z}_{32} \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{49}$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{23520}$

5/5

(iii) Let F be an abelian group with $3^4 \cdot 11^2$ elements. Up to isomorphism, find all possible structures of F. Partition:

4	2
4	2
3+1	1+1
2+2	
1+1+2	
1+1+1+1	

$\therefore F \cong \mathbb{Z}_{3^4} \times \mathbb{Z}_{11^2}$ (OR) $\mathbb{Z}_{3^4} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$

(OR) $\mathbb{Z}_{3^3} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{11^2}$ (OR) $\mathbb{Z}_{3^3} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$

(OR) $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{11^2}$ (OR) $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$

(OR) $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{11^2}$ (OR) $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$

(OR) $\mathbb{Z}_{3} \times \mathbb{Z}_{3} \times \mathbb{Z}_{3} \times \mathbb{Z}_{3} \times \mathbb{Z}_{11^2}$ (OR) $\mathbb{Z}_{3} \times \mathbb{Z}_{3} \times \mathbb{Z}_{3} \times \mathbb{Z}_{3} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$.

10/10

(iv) Let F be an abelian group with $5^3 \cdot 7$ elements. Assume F has a unique subgroup with 25 elements. Up to isomorphism, find all possible structures of F.

Partitions 3	1
3	1
2+1	
1+1+1	

Without Constraint: $\mathbb{Z}_{5^3} \times \mathbb{Z}_7$ (OR) $\mathbb{Z}_{5^2} \times \mathbb{Z}_5 \times \mathbb{Z}_7$ (OR) $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$

$\mathbb{Z}_{5^3} \times \mathbb{Z}_7$ has Unique Subgroup with 25 Elements.

but others have more than 1 Subgroup with 25 Elements

$\therefore F \cong \mathbb{Z}_{5^3} \times \mathbb{Z}_7$ ✓ //.

5/5

QUESTION 5. (Bonus) Assume that D is a group with $3^{2017} \cdot 5^2$ elements. Assume that D has a unique subgroup, say H with 3 elements and also assume that D/H is a cyclic group. Prove that D is a cyclic group. . Assume that H is a normal subgroup of D such that H has.

3/3

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

Ans) $D = 3^{2017} * 5^2$. Let $p = 3$, $i = 5^2$.

i.e. $D = p^n i$ and $\gcd(p, i) = \gcd(3, 5^2) = 1$.

D has Unique Subgroup, H st $|H| = 3$.

D/H is Cyclic.

$\therefore D/H = \langle a * H \rangle$ for some $a \in D$.

Consider: $f : D \longrightarrow D$ st $f(d) = d^p$.

This is clearly Homomorphism.

$Ker(f) = H$ ($\because d^p = e \Rightarrow |d| = p$ $\because p$ is prime).

$D/Ker \cong Range \Rightarrow |D/H| = \frac{|D|}{|H|} = \frac{p^n i}{p} = p^{(n-1)} i$.

$|Range(f)| \,\big|\, |D| \Rightarrow p^{(n-1)} i \,\big|\, p^n i$

(PTO)

$\therefore |D| = p^{(n-1)} i$ (OR) $|D| = p^{n} i$.

We show that $|D| = p^{n} i$.

In both cases $\Rightarrow \exists$ Unique Subgroup K in D of order p. $\therefore \underline{K = H}$.

But this K is made of powers of a

$\therefore \quad H = \{a^{i_1}, a^{i_2}, \ldots, a^{i_s}\}$.

For any $d \in D$

$$d * H = a^{m} * H$$
$$\Downarrow$$
$$d = a^{m} * h$$
$$= a^{m} * a^{i_k} \text{ for some } i_k$$
$$d = a^{m+i_k} \Rightarrow \underline{\underline{d = a^{x}}} \qquad (x = m + i_k)$$

$\therefore D$ is Cyclic.

3.4 2016 All HWs with Solution

HW one, MTH 320, Fall 2016

Ayman Badawi

$\frac{36}{40}$

QUESTION 1. (i) Let $(S, *)$ be a group. Fix $a, b \in S$. Show that if $a * b = a * c$ for some $c \in S$, then $b = c$. Also show that if $b * a = c * a$, then $b = c$.

(ii) Let $(S, *)$ be a group. Fix $a, b \in S$. Show that the equation $a * x = b$ has unique solution and find x. Note the $x * a = b$ has also unique solution, but only show it for $a * x = b$.

(iii) Let $(S, *)$ be a group and assume $|a| = 12$ for some $a \in S$. For what values of m $(1 \leq m \leq 12)$ do we have $|a^m| = 12$? For what values of m $(1 \leq m \leq 12)$ do we have $|a^m| = 4$?

(iv) Let $(S, *)$ be a group and assume $|a| = 6$ for some $a \in S$. Let $F = \{e, a, a^2, ..., a^5\}$. Construct the Caley's table of $(F, *)$. By staring at the table you should observe that F is a group and hence a subgroup of S.

(v) Convince me that if n is not prime, then (Z_n^*, X_n) is never a group.

(vi) Convince me that if n is prime, then (Z_n^*, X_n) is a group.[hint: recall Fermat little Theorem, if p is prime and $p \nmid m$ (meaning p is not a factor of m), then $m^{(p-1)}(mod p) = 1$.]

(vii) Let $F = \{3, 6, 9, 12\}$, and $* = multiplication \;\; module$ 15. Convince me that $(F, *)$ is a group by constructing the Caley's table. What is e in F? Find the inverse of each element of F. INTERESTING!!!!

(viii) Consider (D_5, o). We know that D_5 has 10 elements. Let s_1 be one of the reflections (we know that D_5 has 5 reflections). Let $a = R_{72}$. Convince me that $\{a \; o \; s_1, a^2 \; o \; s_1, a^3 \; o \; s_1, a^4 \; o \; s_1, a^5 \; o \; s_1\}$ = the set of all reflections in D_5[Hint: may be you need to use (i)]

Submit your solution on Tuesday September 20, 2016 at 2pm. 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 $(S, *)$ be a group. Fix $a, b \in S$. Show that if $a \times b = a$
for some $c \in S$, then $b = c$. Also show that if $b * a = c \times a$
then $b = c$

Proof : If $a * b = a * c$. Then,

$b = e * b = (a^{-1} * a) b$ (by Trivial result # 2)

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

$=$ ~~$a^{-1}(a*$~~ $(a^{-1} * a) c = e \times c = c$

Hence $b = c$

5/5

Proof: If $b * a = c * a$. Then

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

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

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

Hence $b = c$

ii) Let $(S, *)$ be a group. Fix $a, b \in S$. Show that the equation $a * x$
has a unique solution. Find x.

Proof:

$a * x = b$

$x = e * x$

$= (a^{-1} * a) x$

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

5/5

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

Proof of uniqueness:

Suppose m is also a solution to $a * x = b$. Then,

$a * m = b = a * x$

$m = x$

Hence the equation $a * x = b$ has a unique solution

iii) Let $(S,*)$ be a group and assume $|a| = 12$ for some $a \in S$.

$$|a^1| = \frac{12}{\gcd(1,12)} = 12$$

$$|a^2| = \frac{12}{\gcd(2,12)} = \frac{12}{2} = 6$$

$$|a^3| = \frac{12}{\gcd(3,12)} = \frac{12}{3} = 4$$

$$|a^4| = \frac{12}{\gcd(4,12)} = \frac{12}{4} = 3$$

$$|a^5| = \frac{12}{\gcd(5,12)} = 12$$

$$|a^6| = \frac{12}{\gcd(6,12)} = \frac{12}{6} = 2$$

$$|a^7| = \frac{12}{\gcd(7,12)} = 12$$

$$|a^8| = \frac{12}{\gcd(8,12)} = \frac{12}{4} = 3$$

$$|a^9| = \frac{12}{\gcd(9,12)} = \frac{12}{3} = 4$$

$$|a^{10}| = \frac{12}{\gcd(10,12)} = \frac{12}{2} = 6$$

$$|a^{11}| = \frac{12}{\gcd(11,12)} = 12$$

$$|a^{12}| = \frac{12}{\gcd(12,12)} = 1$$

For what values of m $(1 \leq m \leq 12)$ do we have $|a^m| = 12$?
$m = 1$, $m = 5$, $m = 7$, $m = 11$

5/5

For what values of m $(1 \leq m \leq 12)$ do we have $|a^m| = 4$?
$m = 3$ and $m = 9$

iv Let $(S,*)$ be a group and assume $|a| = 6$ for some $a \in S$. Let $F = \{e, a, a^2, \ldots a^5\}$. Construct the Caley's table of $(F,*)$.

Given $|a| = 6$

$\rightarrow |a| = n \Rightarrow a^n = e$ $\qquad F = \{e, a, a^1, a^2, \ldots a^5\}$

$|a| = 6 \Rightarrow a^6 = e$

Caley's Table of $(F,*)$

	e	a	a^2	a^3	a^4	a^5
e	e	a	a^2	a^3	a^4	a^5
a	a	a^2	a^3	a^4	a^5	e
a^2	a^2	a^3	a^4	a^5	e	a
a^3	a^3	a^4	a^5	e	a	a^2
a^4	a^4	a^5	e	a	a^2	a^3
a^5	a^5	e	a	a^2	a^3	a^4

(v) Convince me that if n is not prime, then (Z^*_n, X_n) is never a group.

$Z_n = \{0, 1, 2, 3, \dots n-1\}$
$Z^*_n = \{1, 2, 3, \dots n-1\}$

Suppose n is not prime, then

$n = pq$, where $1 < p < n$ and
$1 < q < n$

Hence $p \cdot_n q = 0 \longrightarrow \notin Z^*_n$.

Since $pq \equiv 0 \pmod{n}$
and 0 is not in Z_n^*
Hence (Z_n^*, X_n) is never a group.

OK

5/5

vi Convince me that if n is prime, then (Z^*_n, X_n) is a gr

$Z^*n = \{1, 2, 3, 4, \ldots p-1\}$

$e = 1$

$a^{p-1} \equiv 1 \quad (\bmod\ p)$

1) Closure: Let $a, b \in Z_n^*$. Show $a \cdot_n b \in Z_n^*$. Suppose $a \cdot_n b = 0$. Then $n | ab \Rightarrow n | a$ or $n | b$ (since n is prime). but $n \nmid a$ and $n \nmid b$, because $1 \le a, b \le n-1$.

Thus $a \cdot_n b \neq 0$. Hence $a \cdot_n b \in Z_n^*$.

2) Inverse: Let $a \in Z_n^*$. Since n

we Know $a^{n-1} (\bmod n) = 1$. Thus $a \cdot a^{n-2} (\bmod(n)) = 1$. Hence $a^{-1} = a^{n-2} (\bmod(n)) \in Z_n^*$.

1/5

vii Let F = {3, 6, 9, 12}, and * = multiplication module 15. Convi
me that (F, *.) is a group by constructing the Caley's Ta
What is e in F? Find the inverse of each element of F.

Given that F = {3, 6, 9, 12} and * = operation
(a*b) mod 15 = remainder of (axb)/15

*	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

- All elements in the table are the elements of F.

* → binary operator on F.

for any a, b, c in F it is clear. a*(b*c) = (a*b)*c

∴ identity = e = 6

ok

inverse of 3 is 12

inverse of 6 is 9

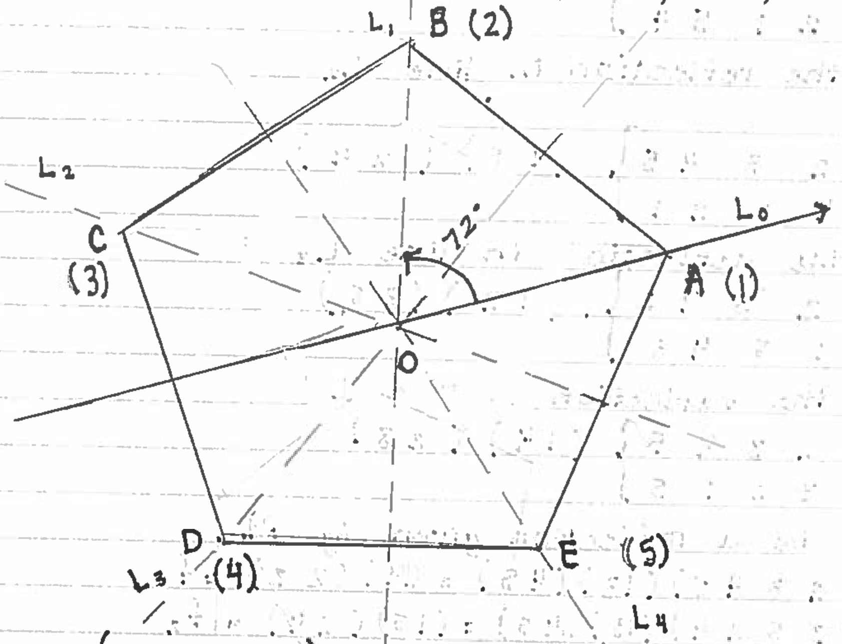
inverse of 9 is 6

inverse of 12 is 3

4/4

viii Consider $(D_5, \circ)$. We know D_5 has 10 elements. Let s_1 be one of the reflections. Let $a = R_{72}$. Convince me that $\{a \circ s_1, a^2 \circ s_1, a^3 \circ s_1, a^4 \circ s_1, a^5 \circ s_1\} =$ the set of all reflections in D_3.

If r is a rotation R_0 and s is any reflection then D_5 can b written as $\{1, r, r^2, r^3, r^4; a \cdot s_1, a^2 \cdot s_1, a^3 \cdot s_1, a^4 \cdot s_1; a^5 \cdot s_1\}$



$$a = R_{72} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5)$$

$$a^2 = R_{144} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = (1\ 3\ 5\ 2\ 4)$$

$$a^3 = R_{216} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 2\ 5\ 3)$$

$$a^4 = R_{288} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 5\ 4\ 3\ 2)$$

$$a^5 = R_{360} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1)$$
(R_0)

Let f_0 be the reflection between L_0

$f_0 = \left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{matrix}\right\} = (2\ 5)\cdot(3\ 4)$

f_1 be the reflection in line L_1

$f_1 = \left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{matrix}\right\} = (1\ 3)\ (4\ 5)$

f_2 be the reflection in line L_2

$f_2 . \left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{matrix}\right\}\ (1\ 5)\ (2\ 4)$

f_3 be the reflection in line L_3

$f_3 = \left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{matrix}\right\}\ (1\ 2)\ (3\ 5)$

f_4 be the reflection in line L_4

$f_4 = \left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{matrix}\right\}\ (1\ 4)\ (2\ 3)$

Let s be a reflection given by $f1$.

$a_s = (1\ 2\ 3\ 4\ 5)(1\ 3)(4\ 5) = (14)(2\ 3) = f_4$,

$a^2 s = (1\ 3\ 5\ 2\ 4)(13)(45) = (15)(24) = f_2$

$a^3 s = (1\ 4\ 2\ 5\ 3)(13)(45) = (25)(3\ 5) = f_0$

$a^4 s = (15432)(13)(45) = (12)(35) = f_3$

$a^5 s = (1)(13)(45) = (13)(45) = f_1$

$\Rightarrow \{a\cdot s, a^2\cdot s, a^3\cdot s, a^4 s, a^5 s\}$ is the set of Reflection of D_5

5/5

Very long!!

you can use mathematical argument !?

Name yumna omar, ID 52755

HW TWO, MTH 320, Fall 2016

Ayman Badawi

QUESTION 1. (i) Given $(S, *) = < a >$ for some $a \in S$ and S has exactly 24 elements. Let $F = \{b \in S \mid S = < b >\}$. Write the elements of F in terms of a. How many elements does F have?.

(ii) Let $S = \{(a, b) \mid a \in Z_3^*, b \in Z_3\}$. Define $*$ on S such that if$(x_1, x_2), (y_1, y_2) \in S$, then $(x_1, x_2) * (y_1, y_2) = (x_1 y_1 (mod 3),\ x_1 y_2 + x_2 y_1 (mod 3))$. Then $(S, *)$ satisfies the associative property (do not prove this). Construct the Caley's table of $(S, *)$. By staring at the table: Is S a group? if yes, what is e? what is the inverse of each element? Is S cyclic? If yes, find $a \in S$ such that $S = < a >$.

(iii) Let D be a group with 47 elements. Prove that D is abelian? Can you say more?

(iv) Let D be a group, H_1, H_2 be two subgroups of D such that $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$. Prove that $H_1 \cup H_2$ is never a subgroup of D.

(v) Let D be a group, and H_1, H_2 be two subgroups of D. Prove that $H_1 \cap H_2$ is a subgroup of D.

(vi) Let $(S, *)$ be a an abelian group with identity e. Fix an integer $n \geq 2$, and let $F = \{a \in S \mid a^n = e\}$. Prove that $(F, *)$ is a subgroup of S. Assume $n = 11$. Prove that either $F = \{e\}$ or F has at least 11 elements.

(vii) Construct the Caley's table for $(U(9), ._9)$. Is $U(9)$ is cyclic? If yes, then find $a \in U(9)$ such that $(U(9), ._9) = < a >$.

Submit your solution on Tuesday October 4, 2016 at 2pm. 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) GIVEN: $(S,*)=\langle a\rangle$ for some $a\in S$

$|S| = 24$ exactly

$F=\{b\in S \mid S=\langle b\rangle\}$

→ Elements of F in terms of a

$S=\{a,a^2,a^3,\dots,a^{24}=e\}$

Required to find: All elements in S that have an order of 24

Find all m such that $|a^m| = \frac{24}{\gcd(m,24)} = 24$

$\gcd(m,24)=1$

Hence, $m=\{1,5,7,11,13,17,19,23\}$

$$\boxed{F=\{a,a^5,a^7,a^{11},a^{13},a^{17},a^{19},a^{23}\}}$$

→ How many elements does F have?

$$\boxed{|F|=8}$$

(ii) GIVEN: $S = \{(a,b) \mid a \in \mathbb{Z}_3^*, b \in \mathbb{Z}_3\} = \{(1,0),(1,1),(1,2),(2,0),(2,1),$

$(x_1, x_2) * (y_1, y_2) = (x_1 y_1 \pmod 3, \; x_1 y_2 + x_2 y_1 \pmod 3))$

→ Construct the Caley's table

*	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
(1,0)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
(1,1)	(1,1)	(1,2)	(1,0)	(2,2)	(2,0)	(2,1)
(1,2)	(1,2)	(1,0)	(1,1)	(2,1)	(2,2)	(2,0)
(2,0)	(2,0)	(2,2)	(2,1)	(1,0)	(1,2)	(1,1)
(2,1)	(2,1)	(2,0)	(2,2)	(1,2)	(1,1)	(1,0)
(2,2)	(2,2)	(2,1)	(2,0)	(1,1)	(1,0)	(1,2)

→ Is S a group?

CLOSURE: By staring at the Caley's table, the closure axiom is satisfied

ASSOCIATIVE: Given in the question, and hence, satisfied

IDENTITY: clear that $\boxed{e = (1,0)}$ since $a * (1,0) = (1,0) * a = a \;\forall\, a \in S$

INVERSE: (1,0) with itself
(1,1) and (1,2)
(2,0) with itself
(2,1) and (2,2)

✓ 4/4

→ Is S cyclic?

$|(1,0)| = 1$
$|(1,1)| = 3$
$|(1,2)| = 3$
$|(2,0)| = 2$
$|(2,1)| = 6$ → could be the generators
$|(2,2)| = 6$ ↗

Check:

$S = \{(2,1), (2,1)^2 = (1,1), (2,1)^3 = (2,0),$
$(2,1)^4 = (1,2), (2,1)^5 = (2,2), (2,1)^6 = (1,0)\}$
$= \{(2,2), (2,2)^2 = (1,2), (2,2)^3 = (2,0),$
$(2,2)^4 = (1,1), (2,2)^5 = (2,1), (2,2)^6 = (1,0)$

$\boxed{\therefore\ S \text{ is cyclic} \Rightarrow S = \langle (2,1) \rangle = \langle (2,2) \rangle}$

(iiii) GIVEN: D is a group
$|D| = 47$

→ Show that D is an abelian group:

We notice that $|D|$ is a prime number

Let $a \in D$, such that a is not the identity ($a \neq e$).

We know that the cyclic group generated by a is a subgroup of D $\Rightarrow \langle a \rangle \leq D$

By Lagrange, the order of $\langle a \rangle$ divides $|D|$
$\Rightarrow |\langle a \rangle| \mid 47$

47 is prime $\Rightarrow$ the divors of 47 are 1 and itself

Since $a \neq e \Rightarrow |\langle a \rangle| > 1$, and hence, $|\langle a \rangle|$ must be 47

Hence $D = \langle a \rangle \Rightarrow$ $\boxed{\text{D is cyclic}}$ and generated by a

→ Can you say more?

We pr in our class notes that every cyclic oup is an abelian

Henc $\boxed{\text{is abelian}}$

(iv) GIVEN: D is a group.
$H_1 < D$ and $H_2 < D$
$H_1 \not\subset H_2$ and $H_2 \not\subset H_1$

→ Prove that $H_1 \cup H_2$ can never be a subgroup of D:

Let $a \in H_1$ and $a \notin H_2$
Let $b \in H_2$ and $b \notin H_1$

Hence, $a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$

Clear that $a * b \notin H_1$ and $a * b \notin H_2$

Therefore, $a * b \notin H_1 \cup H_2$

4/4

∴ Closure is not satisfied ⇒ $\boxed{H_1 \cup H_2 \text{ is not even a group to begin with}}$

→ EXAMPLE:

$(D_6, +_6)$ where $D_6 = \{0,1,2,3,4,5\}$

$H_1 = \{0,2,4\}$ and $H_2 = \{0,3\}$

$H_1 \cup H_2 = \{0,2,3,4\}$

$$\boxed{2 +_6 3 = 5 \notin H_1 \cup H_2}$$

you can make it shorter.

Let $a, b \in H_1 \cap H_2$. Show $a^{-1} * b \in H_1 \cap H_2$.

Since $a \in H_1 \cap H_2$, $a^{-1} \in H_1 \cap H_2$. Hence $a^{-1} * b \in H_1$ and $a^{-1} * b \in H_2$. Thus $a^{-1} * b \in H_1 \cap H_2$.

1(v) GIVEN: D is a group

$H_1 < D$ and $H_2 < D$

→ Show that $(H_1 \cap H_2) < D$:

CLOSURE: let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

then $a, b \in H_1$ and $a, b \in H_2$

Since H_1 is a subgroup, then $a * b \in H_1$

Similarly, $a * b \in H_2$

7/5

Hence, $a * b \in H_1 \cap H_2$ closure is satisfied ✓

ASSOCIATIVE: clear, since H_1 and H_2 are subgroups

Therefore, $H_2 \cap H_2$ satisfies the associative axiom ✓

IDENTITY: Since H_1 and H_2 are subgroups, the identity e is in both

$\Rightarrow e \in H_1$ and $e \in H_2$

Hence, $\boxed{e \in H_1 \cap H_2}$ ✓

INVERSE: if $a \in H_1 \cap H_2$, then $a \in H_1$ and $a \in H_2$

if $a \in H_1$, then $a^{-1} \in H_1$ because H_1 is a subgroup.

Similarly, $a \in H_2 \Rightarrow a^{-1} \in H_2$

Hence, $\boxed{a^{-1} \in H_1 \cap H_2}$ ✓

* $H_1 \cap H_2$ satisfies all group axioms and $H_1 \cap H_2 \subset D$

$\Rightarrow \boxed{H_1 \cap H_2 < D}$ *

Let $a,b \in F$. Show $a^{-1}*b \in F$. shorter-

~~Since $a^n = e$, $(a^n)^{-1} = (a^{-1})^n \in F$ Hence $a^{-1} \in F$.~~

(vi) GIVEN: $(S,*)$ is an abelian group with identity e

$F = \{a \in S \mid a^n = e\}$; $n \geq 2$

→ Prove that $(F,*)$ is a subgroup of S:

Since S is abelian $(a^{-1}*b)^n = (a^{-1})^n * b^n = (a^n)^{-1} * b^n = e*e=e$ Done

CLOSURE: Since $(S,*)$ is abelian, we know that

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

We also know that since $a*b=b*a$, then $(a*b)^n = a^n * b^n$

Let $a,b \in F \Rightarrow a^n = e$ & $b^n = e$

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

Since $(a*b)^n = e$, then $a*b \in F$ ✓ Closure satisfied

3/5

ASSOCIATIVE: Clear, since $F \subset S$ & S is a group

IDENTITY: Since $e^n = e \Rightarrow \boxed{e \in F}$ ✓

INVERSE: Let $a \in F \Rightarrow a^n = e$

We know that $|a| = |a^{-1}|$

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

if $n = m \Rightarrow (a^{-1})^n = e \Rightarrow \boxed{a^{-1} \in F}$

if $n \neq m \Rightarrow$ We know that $m \mid n$ and hence $(a^{-1})^n = e \Rightarrow \boxed{a^{-1} \in F}$ ✓

4/4

$*F$ is a group & $F \subset S \Rightarrow \boxed{F < S}*$

→ Assume $n = 11 \Rightarrow F = \{e\}$ or $|F|$ is at least 11

$F = \{a \in S \mid a^{11} = e\}$

11 is prime $\Rightarrow F = \{a \in S \mid |a| = 11\}$ since there cannot be any other m less than 11 such that $a^m = e$

In a group, we know that the order of any element in the group divides the order of the group $\Rightarrow |a| \mid |F| \ \forall \ a \in F$

Since $|a| = 11 \Rightarrow |F| = 11, 22, 33, 44, \ldots$

* F must have $\boxed{\text{at least 11 elements}}$ *

Assume that there exists no element in S whose order is 11, hence only e satisfies $e^{11} = e$

* $F = \boxed{\{e\}}$ *

↯

(vii) Given: $(U(9), \cdot_9)$

$$U(9) = \{a \in \{0,1,2,3,4,5,6,7,8\} \mid \gcd(a,9)=1\}$$

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

→ Construct the Caley's table:

$\cdot_9$	1	2	4	5	7	8
1	①	2	4	5	7	8
2	2	4	8	①	5	7
4	4	8	7	2	①	5
5	5	①	2	7	8	4
7	7	5	①	8	4	2
8	8	7	5	4	2	①

→ Is U(9) cyclic?

$|1| = 1$

$|2| = 6$ → could be the generators

$|4| = 3$

$|5| = 6$

$|7| = 3$

$|8| = 2$

Check: $U(9) = \{2, 2^2=4, 2^3=8, 2^4=7, 2^5=5, 2^6=1\}$

Hence, $\boxed{U(9) = \langle 2 \rangle}$ cyclic & generated by $a=2$

$U(9) = \{5, 5^2=7, 5^3=8, 5^4=4, 5^5=2, 5^6=1\}$

Hence, $\boxed{U(9) = \langle 5 \rangle}$ cyclic & generated by $a=5$

Name——————————, **ID** ——————

MTH 320 Abstract Algebra Fall 2016, 1–2

HW III, MTH 320, Fall 2016

Ayman Badawi

QUESTION 1. (i) We know that $6Z$, $8Z$ are infinite cyclic subgroups of $(Z, +)$. Hence $6Z \cap 8Z$ is also an infinite cyclic subgroup and thus $6Z \cap 8Z = aZ$ for some $a \in Z$. Find all possible values of a. Explain?

Sketch. Let a be the least positive integer that "lives" in 6Z and "lives" in 8Z. Hence $6|a$ and $8|a$. Since a is the least positive integer where $6|a$ and $8|a$, we conclude that $a = LCM[6, 8] = 24$. Thus $a = 24$. Thus $6Z \cap 8Z = 24Z$

(ii) In general fix $a, b \in (Z, +)$. Then $aZ \cap bZ = cZ$ for some $c \in Z$. Find all possible values c (of course write c in terms of a, b.

Sketch: Let $d \in (aZ \cap bZ)$. Then $a \mid d$ and $b \mid d$. Let $h = lcm[a, b]$. Then h is the least positive integer that lives in $aZ \cap bZ$. Since $aZ \cap bZ$ must be an infinite cyclic subgroup of Z, we conclude that $aZ \cap bZ = lcm[a, b]Z = hZ$. We know that if $H =< v >$ is an infinite cyclic group, then H has exactly two generators, namely: v and v^{-1}. Thus $aZ \cap bZ = lcm[a, b]Z = -lcm[a, b]Z$. Thus all possible values of c are : lcm[a,b] and -lcm[a, b]. .

(iii) Let $(S, *)$ be a group. Assume that $a * b = b * a$ for some $a, b \in S$. Prove that $a * b^{-1} = b^{-1} * a$.

Proof Since $a * b = b * a$, we have $b^{-1} * a * b * a^{-1} = b^{-1} * b * a * a^{-1} = e * e = e$. Since $b^{-1} * a * b * a^{-1} = e$ we conclude that $b^{-1} * a = e * a * b^{-1} = a * b^{-1}$.

(iv) Let $(D, *)$ be a group with 8 elements. Assume that D has a unique subgroup of order 2 and it has a unique abelian subgroup of order 4. Prove that D is an abelian group. In fact, you can prove that $(D, *)$ is cyclic.

Proof: Let F be the unique abelian subgroup of D with 2 elements and let M be the unique abelian subgroup of D with 4 elements. Since M is abelian with 4 elements, we know that M has an abelian subgroup K with 2 elements. Since K is also an abelian subgroup of D with 2 elements, we conclude that $K = F$. Now let $a \in D \setminus M$ and let $c = |a|$. Hence by Lagrange Theorem, $c = 1$ or 2 or 4 or 8. We know that $\{a, a^2, ..., a^c = e\} =< a >$ is an abelian (cyclic) subgroup of D with c elements. Since $a \in D \setminus M$ and $F \subset M$ are unique abelian subgroups of order 2 and 4 respectively, we conclude that $c \neq 2$ and $c \neq 4$. Clearly, $c \neq 1$. Hence $c = 8$. Thus $D =< a >$. ,

(v) Let $(D, *)$ be a group. Assume $a * b = b * a$ for some $a, b \in D$. Given $|a| = n$, $|b| = m$, and $gcd(n, m) = 1$. Prove that $|a * b| = nm$. [Hint: Since $gcd(n, m) = 1$, from class notes we know that if $n \mid mc$ for some $c \in Z$, then $n \mid c$. Also you need to use a trivial fact from number theory that if $gcd(n, m) = 1$ and $n \mid c$ and $m \mid c$ for some $c \in Z$, then $nm \mid c$]

Proof: Let $k = |a * b|$. Since $a * b = b * a$, $(a * b)^{nm} = (a^n)^m(b^m)^n = e * e = e$. Hence $k|nm$. Now $e = (a * b)^{km} = a^{km} * (b^m)^k = a^{km} * e = a^{km}$. Thus $n \mid km$. Since $gcd(n, m) = 1$, we conclude that $n \mid k$. Similarly, $e = (a * b)^{km} = (a^m)^k * b^{kn} = e * b^{kn} = b^{kn}$. Thus $m \mid kn$. Since $gcd(n, m) = 1$, we conclude that $m \mid K$. Since $n \mid k$ and $m \mid k$ and $gcd(n, m) = 1$, we conclude that $nm \mid k$. Since $k \mid nm$ and $nm \mid k$, we conclude that $k = nm$.

(vi) Let $(D, *)$ be a group. Assume $a * b = b * a$ for some $a, b \in D$. Given $|a| = 6$ and $|b| = 14$. Prove that $(D, *)$ has a cyclic subgroup of order 42. [hint: Some how show that D has an element of order 7, then you need to use (V)]

Proof. We know $|b^2| = 14/gcd(2, 14) = 7$. Since $a * b = b * a$, it is clear that $a * b^2 = b^2 * a$. Since gcd(6, 7) = 1, by part V $|a * b^2| = 42$. Hence $H =< a * b^2 >$ is a cyclic subgroup of D with 42 elements.

(vii) Let D be an abelian group with pq elements where p, q are distinct prime numbers. Prove that D is cyclic.

Proof. Since D is abelian, we have a subgroup H of order p and a subgroup K of order q. Let $a \in H$ such that $a \neq e$. By Lagrange Theorem we conclude $|a| = p$. Similarly, if $b \in K$ and $b \neq e$, then $|b| = q$. Thus $|a * b| = pq$ by part V. Hence $D =< a * b >$

(viii) Let D be a finite abelian group and H be a proper subgroup of D with 10 elements. Assume $a \in D \setminus H$ such that $|a| = 3$. Then

a. Show that $a * H$, $a^2 * H$, $a^3 * H$ are distinct left cosets of H[Hint: First note that $a^3 * H = e * H = H$. We know $a * H \cap H = \emptyset$. So show $a^2 * H \cap a * H = \emptyset$ and $a^2 * H \cap H = \emptyset$].

Proof: We show $a^2 \notin H$ and $a^2 \notin a * H$. Assume that $a^2 \in H$. Since $a^3 = e$, $a * a^2 = e$. Thus $e \in a * H$, impossible since $a * H \cap H = \emptyset$. Assume $a^2 \in a * H$. Thus $a^2 = a * h$ for some $h \in H$. Hence $a = h$, impossible. Thus $H, a * H, a^2 * H$ are all distinct left cosets of H.

b. Show that $F = a * H \cup a^2 * H \cup a^3 * H$ is a subgroup of D with 30 elements.

Proof: Note that $H = a^0 * H = e * H$and hence $F = a^0 * H \cup a * H \cup a^2 * H$. Let $x, y \in F$. Since F is finite, we only need show $x * y \in F$. Hence $x = a^i * h, y = a^k * g$ for some $i, k, 0 \leq i, k \leq 2$ and some $h, g \in H$. Since |a| = 3 and D is abelian, $x * y = (a^i * h) * (a^k * g) = a^{(i+k)mod3} * (h * g)$. Since $0 \leq (i + k)mod3 \leq 2$ and $h * g \in H$, we are done.

a. Find all distinct left cosets of H. Note there must be exactly 4 such left cosets

: This is my present to you... just straight forward calculations

b. Is $H \cup 5H$ a subgroup of $U(16)$? Is $H \cup 9H$ a subgroup of $U(16)$? explain

Note $K = H \cup 5H = \{1, 7, 3, 5\}$**. (5.3** $= 15 \notin K$**, so no) and** $L = H \cup 9H = \{1, 7, 9, 15\}$ **(by Caley's Table** L **is a subgroup)**

Submit your solution on Tuesday October 18, 2016 at 2pm. **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———————————, ID ————————

HW IV, MTH 320, Fall 2016

Ayman Badawi

QUESTION 1. (i) Let $\alpha = (1\ 4\ 5\ 2)o(2\ 6\ 5) \in S_6$. Find $|\alpha|$

Typical question

(ii) Let $\beta \in S_7$ and $x = \beta o(2\ 6\ 3\ 1)o\beta^{-1}$. Find $|x|$.

Typical question

(iii) Let $D = (Z_4, +) \times (Z_6, +)$. Give me a subgroup H of D such that there is no subgroup L_1 of Z_4 and there is no subgroup L_2 of Z_6 where $H = L_1 \times L_2$.

Solution: The element $(2, 3)$ in D is of order 2. Hence $H = \{(0, 0), (2, 3)\}$ is a subgroup of D but there is no subgroup L_1 of Z_4 and there is no subgroup L_2 of Z_6 where $H = L_1 \times L_2$.

(iv) Let $D = (S, *1) \times (F, *2)$ be a cyclic group (you may assume $|S| > 1, |F| > 1$). Let H be a subgroup of D. Prove that there exists a subgroup K of S and there exists a subgroup L of F such that $H = K \times L$. [Hint: You may use the fact that if $gcd(n, m) = 1$ and $i \mid nm$, then $i \mid n$ or $i \mid m$ or $i = ab$ $(a > 1$ and $b > 1)$ such that $a \mid n$ and $b \mid m$.) [**OBSERVE that the group in part III is not cyclic, interesting!**]

Solution: We know that F, S are cyclic and finite groups. Let $n = |S|$ and $m = |F|$. Hence $|D| = nm$. Since D is cyclic, we know $gcd(n, m) = 1$. Let H be a subgroup of D and $k = |H|$. Since D is cyclic, we know that H is the only subgroup of D that has k element. Since $k \mid nm$ and $gcd(n, m) = 1$, we conclude that $k = ab$ such that $a \mid n$, $b \mid m$, and $gcd(a, b) = 1$ (note it is possible that $a = 1$ or $b = 1$). Since $a \mid n$, S has a unique subgroup L_1 of order a. Since $b \mid m$, F has a unique subgroup L_2 of order b. Thus $L_1 \times L_2$ is the unique subgroup of D that has k elements. Hence $H = L_1 \times L_2$.

(v) Let $a \in S_n$ be a permutation (i.e $a = (a_1 \cdots a_k)$. Note that not every function in S_n is a permutation). Prove that $a \in A_n$ if and only if $|a|$ is an odd number.

Solution: Since $a = (a_1\ a_2 \cdots a_{k-1}\ a_k) = (a_1\ a_k)o(a_1\ a_{k-1})o \cdots o(a_1\ a_2)$, (k-1)-2-cycles, we conclude that $a \in A_n$ iff (k-1) is even. Hence k must be an odd positive integer. Thus $|a| = k$ is odd.

(vi) We know that D_4 is a subgroup of S_4 and hence $L = D_4 \cap A_4$ is a subgroup of S_4. Find L. Is $L \triangleleft A_4$? EXPLAIN

Solution: Let $L = D_4 \cap A_4 = \{(1), (1\ 3)(2\ 4), (1\ 3)(2\ 4), (2\ 3)(1\ 4)\}$. Now if we view L as a subgroup of A_4. Then $[A_4 : L] = 3$. Thus L has exactly 3 left cosets, say: L, aoL, and boL. Now do the calculation, show: $aoL = Loa$ and $boL = Lob$. Thus we conclude that $L \triangleleft A_4$.

(vii) Let D be a group with 15 elements. Assume $H \triangleleft D$ such that $|H| = 3$. Assume there exists $a \in S \setminus H$ such that $|a| \neq 5$. Prove that D is cyclic. [Hint: you may want to consider D/H !!]

Solution: We know D/H is a group with 5 element. Consider the natural group homomorphism from D onto D/H (given by $x \to x * H$). Let $k = |a|$, and $m = |a * H|$ (note that m is the order of the element $a * H$ in D/H). We know that $m \mid k$ and $m \mid 5$ (since $|D/H| = 5$). Since $a \notin H$, $m \neq 1$. Hence $m = 5$. Thus $5 \mid k$. Since $5 \mid k$ and $k \mid 15$ and $a^5 \neq 1$, we conclude that $k = 15$. Thud D is cyclic.

(viii) Let F be a nontrivial group-homomorphism from $(Z_6, +)$ into $(Z_8, +)$. Find $Ker(F)$ and find $Image(F)$ (i.e. $Range(F)$).

Solution: We know $Z_6/Ker(F) \approx Image(F)$ and $Image(F)$ is a subgroup of Z_8. Thus $|Image(F)|$ is a factor of 8. Let $a = |Image(F)|, b = |Z_6/Ker(F)|$. Hence $a = b$. Since $b \mid 6$ and $a = b$ and $a \mid 8$, we conclude that $a = b = 2$. Now Z_8 has exactly one subgroup of order 2. Thus $Image(F) = \{0, 4\}$. Since $b = 2$, we conclude $|Ker(F)| = 3$. Since Z_6 has exactly one subgroup of order 3, we conclude $Ker(F) = \{0, 2, 4\}$.

(ix) Is the group $(Z_4, +)$ isomorphic to $U(8)$? EXPLAIN.

Solution: No, Z_4 is cyclic but $U(8)$ is not cyclic

(x) Give me an example of a non-abelian group say D such that D has a normal subgroup H where D/H is abelian.

Solution: Let $D = S_3$ and $H = A_3$.

(xi) Give me an example of an abelian group say D that is not cyclic but D has a normal subgroup H where D/H is cyclic .

Solution: Let $D = U(8)$ and $H = \{1, 7\}$.

(xii) Give me an example of a group say D that has a normal subgroup H such that there is an $a \in D$ where $|a| = \infty$ but the order of the element $a * H$ in G/H is finite.

Solution: Let $D = (Z, +)$, $H = 5Z$, and $a = 1$. Then $|1| = \infty$. Since $Z/5Z \approx Z_5$, $|1 + 5Z| = 5$.

(xiii) Give me an example of a group say D such that for each integer $n \geq 2$, there is an element $a \in D$ with $|a| = n$. (note that such D must be infinite)

Solution: Let $D = (Q, +)$ and $H = Z$. Then $\frac{1}{n} + Z| = n$ in Q/Z.

(xiv) Let $n \geq 3$ and let $x \in S_n$. Prove that x^2 is always an even function.

Solution: Since $A_4 \lhd S_4$, we know that S_4/A_4 is a group with exactly 2 elements. Let $x \in S_4$. Then $(xoA_4)^2 = x^2oA = A$ in S_4/A_4. Thus $x^2 \in A_4$.

DUE DATE : Nov 18, 2016, Thursday at 2pm

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`

3.5 2016 Exam One with Solution

Name————————————, ID ——————

EXAM I, MTH 320, Fall 2016

Ayman Badawi

QUESTION 1. (i) We know that $(Z, +)$ is cyclic. Prove that $F = (Z, +) \times (Z, +)$ is not a cyclic (Some of you have the right idea but ...)

Proof. Deny. Then $F =< (a, b) >$ **for some** $a, b \in Z$**. It is clear that** $a \neq 0$**, and** $b \neq 0$**. Since** $(1, 0) \in F$**, there must exist** $k \in Z$ **such that** $(1, 0) = (a, b)^k = (ak, bk)$**. Hence** $bk = 0$ **and** $ak = 1$**. Since** $bk = 0$ **and** $b \neq 0$**, we conclude** $k = 0$**. But** $(a, b)^0 = (0, 0) \neq (1, 0)$**. A contradiction. Thus** F **is not cyclic.**

(ii) Give me an example of an abelian group with 16 elements, say D, such that D has a subgroup H with exactly 8 elements, but D has no elements of order 8.

Solution: Let $D = (Z_4, +) \times (Z_4, +)$**. We know that** $|(a, b)| = LCM[|a|, |b|]$**. Hence each element in D is of order 1, 2, or 4. Now** $H = \{0, 2\}$ **is a subgroup of** Z_4**. Thus** $Z_4 \times H$ **is a subgroup of** D **with 8 elements.**

(iii) Let D be an abelian group such that D has a subgroup H with 10 elements. Given that D has an element a of order 2 where $a \notin H$. Prove that D has a subgroup of order 20.

Proof. Let $F = H \cup a * H$**. We know** $H \cap a * H = \emptyset$ **and** $|F| = 20$**. Hence we show that** F **is closed. Let** $x, y \in F$**. Then** $x = a^i * h_1, y = a^k * h_2$ **where** $0 \leq i, k \leq 2, h_1, h_2 \in H$**. Thus** $x * y = a^{i+k(mod2)}h_1h_2 \in F$**.**

(iv) We know that if a, b are elements of a group $(D, *)$ such that $a * b = b * a$ and $gcd(|a|, |b|) = 1$, then $|a * b| = |a||b|$. Give me an example of a group D that has two elements, say a, b, such that $gcd(|a|, |b|) = 1$ but $|a * b| \neq |a||b|$.

Solution: Let $a = (1\ 2\ 3), b = (2\ 3) \in S_3$**. Then** $|a| = 3$ **and** $|b| = 2$**.** $aob = (1\ 2)$**. Thus** $|aob| = 2$**, where** $|a||b| = 6$

(v) Let $(D, *)$ be a group and $a, b \in D$ such that $a * b = b * a$. Prove that $a^{-1} * b^{-1} = b^{-1} * a^{-1}$.

Proof. Since $a*b = b*a$**, we have** $(a*b)^{-1} = (b*a)^{-1}$**. We know that** $(a*b)^{-1} = b^{-1}*a^{-1}$ **and** $(b*a)^{-1} = a^{-1}*b^{-1}$**. Thus** $a^{-1} * b^{-1} = b^{-1} * a^{-1}$**.**

(vi) Let $(D, *)$ be a group such that $a^2 = e$ for every $a \in D$. Prove that D is an abelian group.

Proof. Since $a^2 = e$ **for every** $a \in D$**, we conclude that** $a = a^{-1}$ **for every** $a \in D$**. Now let** $x, y \in D$**. Since** $x * y \in D$**, we have** $(x * y)^2 = (x * y) * (x * y) = e$**. Thus** $x * y = y^{-1} * x^{-1} = y * x$ **(since** $y^{-1} = y$ **and** $x^{-1} = x$

(vii) ((All of you - 2) got it right just straightforward class notes, see your notes)

Is $U(10) \times (Z_7, +)$ cyclic? Explain briefly.

b. Is $U(15) \times (Z_9, +)$ cyclic? Explain briefly.

c. Let $F = (Z_{12}, +)$ and $H = \{0, 3, 6, 9\}$. Find all left cosets of H

d. Let $V = (1\ 3\ 4)o(2\ 5\ 6)$ Find $|v|$

e. Let $V = (1\ 3\ 5)o(2\ 3\ 4\ 5)$. Find $|v|$.

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`

3.6 2016 Exam Two with Solution

Name—————————————, **ID** ————————

EXAM II, MTH 320, Fall 2016

Ayman Badawi

QUESTION 1. Let D be a group with 55 elements.

(i) **(6 points)**. Convince me that D is not simple.

Solution: We know that D has an element of order 11, and hence D has a subgroup, say H, with 11 elements. Since [D : H] = 5 and 5 is the smallest prime factor of 55, we know that H must be normal. Thus D is not simple.

(ii) **(8 points)**. Assume that D has a normal subgroup, say H, such that $|H| = 5$. Prove that D is cyclic.

Solution: Let K be a normal subgroup of D with 5 elements and let H as in (i). We know HK is a subgroup of D. Thus $|HK| = 5$ or 11 or 55. Since K and H are subgroups of HK, we conclude that $|HK| = 55$. Thus $HK = D$. It is clear that $H \cap K = \{e\}$. Hence by one of the results in class, we have $D/(H \cap K) \simeq D/H \times D/K$ and thus $D \simeq D/H \times D/K$. Since $|D/H| = 5$ and $|D/K| = 11$, we conclude that $D/H \simeq Z_5$ and $D/K \simeq Z_{11}$. Thus $D \simeq Z_5 \times Z_{11} \simeq Z_{55}$ is cyclic.

QUESTION 2. (8 points). Given that H is a normal subgroup of a group $(D, *)$ such that $|H| = 11$. Assume that $D/H =< a * H >$ (i.e., D/H is cyclic and generated by $a * H$) for some $a \in D \setminus H$ such that $a * h = h * a$ for every $h \in H$. Prove that D is abelian

Solution: I wrote this question to see how many of you read the proof I give in CLASS. Similar proof to if $D/C(D)$ is cyclic, then D is abelian. Here we go: Let $x, y \in D$. Show $x * y = y * x$. Hence $x = a^i * H, y = a^k * H$ in D/H. Thus $x = a^i * b, y = a^k * c$ for some $b, c \in H$. Now since $|H| = 11$, H is cyclic and hence abelian. Thus $b * c = c * b$. Also by hypothesis, we have $a * b = b * a$ and $a * c = c * a$. Hence $x * y = a^{i+k} * b * c = a^{i+k} * c * b = y * x$.

QUESTION 3. (6 points). Let $F : Z_{15} \rightarrow Z_{12}$ be a nontrivial group homomorphism. Find $Ker(F)$ and $Image(F)$.

Solution: We know $Z_{15}/Ker(F) \simeq Image(F)$. Hence by staring (and keep in mind that Image(F) is a subgroup of Z_{12} and $|image(F)|$ must be a factor of the two numbers 12 and 15), we conclude that $|Z_{15}/Ker(F)| = |Image(F)| = 3$. Thus $Image(F) = \{0, 4, 8\}$, and in order that $|Z_{15}/Ker(F)| = 3$ we must have $|Ker(F)| = 5$. Thus $Ker(F) = \{0, 3, 6, 9, 12\}$.

QUESTION 4. (6 points). Let $F : Z \rightarrow Z_{20}$ be a nontrivial group homomorphism. Given that F is not ONTO (not surjective) and $5 \in Image(F)$. Find $Ker(F)$ and $Image(F)$.

Solution: Since F is not onto and $5 \in Image(F)$, $< 5 >= \{0, 5, 10, 15\}$ is the only subgroup of Z_{20} that is not equal to Z_{20} and contains 5. Thus $Image(F) = \{0, 5, 10, 15\}$. We know every subgroup of Z is of the form kZ. Hence $Z/Ker(F) = Z/kZ \simeq Image(F) = \{0, 5, 10, 15\} \simeq Z_4$. Thus $K = 4$. Hence $Ker(F) = 4Z$.

QUESTION 5. (6 points). Let D be an abelian group with p^3 elements for some prime integer p. Assume that D has a unique subgroup of order p. Prove that D is cyclic.

Solution: We Know that (1) $D \simeq Z_{p^3}$ or (2) $D \simeq Z_p \times Z_{p^2}$ or (3) $D \simeq Z_p \times Z_p \times Z_p$. If D is isomorphic to the groups in (2) or (3), then clearly D has more than one subgroup with p elements. Thus $D \simeq Z_{p^3}$ is cyclic.

QUESTION 6. (6 points). Let D be a a noncyclic abelian group with 32 elements. Assume that $|a| = 16$ for some $a \in D$. Up to isomorphism, find all such groups.

Solution: We know (1) $D \simeq Z_{32}$ or (2) $D \simeq Z_2 \times Z_{16}$ or (3) $D \simeq Z_{k_1} \times \cdots Z_{k_m}$ where $k_1, ..., k_m \in \{2, 4, 8\}$. Now D is not isomorphic to Z_{32} since D is not cyclic. D is not isomorphic to a group as in (3) since all such groups have elements of order 8 or less. Thus $D \simeq Z_2 \times Z_{16}$.

QUESTION 7. (6 points). Assume that a group D has unique subgroup H where $|H| = 2016$. Prove that H is a normal subgroup of D.

Solution: Let $a \in D$. Show $a * H = H * a$. Since $C_a(H) = a * H * a^{-1}$ is a subgroup od D with cardinality equals to the cardinality of H, we conclude $a * H * a^{-1} = H$. Thus $a * H = H * a$.

QUESTION 8. (i) **(5 points)**. Is $U(27) \simeq Z_{18}$? explain

(ii) **(5 points)**. Is $(1\ 2\ 4)o(1\ 3) \in A_4$? explain

(iii) **(5 points)**. Is every abelian group with 45 elements isomorphic to $Z_{15} \times Z_3$? explain

(iv) **(5 points)**. Let $a = (1\ 3\ 4\ 5)o(2\ 4\ 1)$. Find $|a|$

(v) **(5 points)**. Let $a \in S_7$ and $m = |a|$. What is the maximum value of m. Explain briefly.

Solution: (i-iv): all of you got it right. For (v): just observe that a must be written as disjoint cycles say $a = a_1\ o\ a_2\ o \cdots o\ a_k$ and $|a|$ = LCM[length of a_1, length of a_2, ..., length a_k] = m = maximum. Now it should be clear that for m to be maximum $k = 2$, $|a_1| = 4$ and $|a_2| = 3$. Hence $m = 12$.

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

3.7 2016 Final Exam with Solution

Name——————————————, ID ————————

Final EXAM , MTH 320, Fall 2016

Ayman Badawi

QUESTION 1. (i) **(5 points)**. Is $(Q^*, .)$ isomorphic to $(Z, +)$? Explain

No. $(Q^*, .)$ **has a finite group, namely** $\{1, -1\}$**. So** $(Q*, .)$ **is not cyclic (since every subgroup of a cyclic infinite group is cyclic). However,** $(Z, +)$ **is cyclic. Thus** $(Q^*, .)$ **is not isomorphic to** $(Z, +)$**.**

(ii) **(5 points)**. Is $Z_3 \times Z_8$ isomorphic to $Z_6 \times Z_4$? Explain

$Z_3 \times Z_8$ **is isomorphic to** Z_{24} **and hence cyclic. Since** $gcd(6, 4) \neq 1$**,** $Z_6 \times Z_4$ **is not cyclic.**

(iii) **(5 points)** . Let $n = 5^2.7^3.11$, and let $D = \{a \in (Z_n, +) \mid |a| = 77\}$. Find the cardinality of D.

Since Z_n **is cyclic, we know** Z_n **has a unique subgroup of order 77, say** $H =< a >$**. Hence if** $b \in D$**, then** $< a >=< b >$**. Thus** $D = \{c \in H \mid |c| = 77\}$**. We know that** H **has exactly** $\phi(77) = \phi(7 \times 11) = 6 \times 10 = 60$ **elements of order 77. Thus** $|D| = 60$**.**

(iv) **(5 points)**. It is easy to see that A_8 has an elements of order 15. With at most two lines, convince me that A_8 must have at least two distinct subgroups each is of order 15.

Let H **be a subgroup of order 15. Since** A_5 **is simple, there exists** $a \in A_5$ **such that** $a * H \neq H * a$**. Thus** $a * H * a^{-1} \neq H$**. We know** $a * H * a^{-1}$ **is a subgroup of** A_8 **with 15 elements .**

(v) **(5 points)**. Is it possible to have infinitely many non-isomorphic groups such that each has 100 elements? Explain

It is clear that S_{100} **has finitely many subgroups, each is of order 100. By Caley's Theorem a group with 100 elements is isomorphic to a subgroup of** S_{100}**. Thus there are finitely many non-isomorphic groups such that each has 100 elements.**

(vi) **(5 points)**. Give me an example of a group D that has an element w of order 2 and an element f of order 3, but D has no elements of order 6.

S_3 **has no elements of order 6. However** $a = (1\ \ 2)$ **is of order 2 and** $b = (1\ \ 2\ \ 3)$ **is of order 3.**

(vii) **(8 points)**. Let $F : (Z, +) \to (Q^*, .)$ be a nontrivial group homomorphism such that F is not one-to-one. Find $F(1)$, then find $Image(F)$ and $Ker(F)$.

Since F **is not 1-1,** $Ker(f) \neq \{0\}$**. Hence** $Ker(F) = mZ$ **for some** $m \in Z^+$**. Thus** $Z/mZ = Z_m \simeq Image(F) < Q^*$**. Thus** $Image(F)$ **must be finite. However** $(Q^*, .)$ **has a unique finite subgroup** $H = \{1, -1\}$**. Thus** $Image(F) = H \simeq Z_2$**. Hence** $m = 2$ **and** $Ker(F) = 2Z$**. If** $F(1) = 1$**, then** $F(a) = 1$ **for every** $a \in Z$ **and thus** F **is the trivial group homomorphism, a contradiction. Hence** $F(1) = -1$**.**

(viii) **(8 points)**. Let F be a group with 21 elements such that F has a unique subgroup with 3 elements. Prove that F is isomorphic to Z_{21}.

We know F **has a subgroup with 7 elements, say** H**, and it has a subgroup with 3 elements, say** K**. Since** $[H : F] = 3$**, and** 3 **is the minimum prime divisor of** $|F| = 21$**, we conclude that** $H \lhd F$**. Since** K **is unique, we conclude** $K \lhd F$**. It is clear that** $|HK| = 21$ **and** $H \cap K = \{e\}$**. Hence** $HK = F$ **and F =** $F/(H \cap K) \simeq F/H \times F/K \simeq Z_3 \times Z_7 \simeq Z_{21}$ **is cyclic.**

(ix) **(8 points)**. Let D be a group with 77 elements. Prove that either $|C(D)| = 1$ or D is abelian.

$|C(D) = 1$ **or 7 or 11 or 77. If** $C(D) = 77$**, we are done. If** $C(D) = 7or11$**, then** $D/C(D)$ **is cyclic and hence** D **is abelian.**

(x) **(8 points)**. Let D be a finite group. Assume H is a normal subgroup. Given $|a * H| = n$ (the order of the element $a * H$ is n in G/H) for some $a \in D$. Prove that D has an element of order n.

Let $m = |a|$**. We know** $n \mid m$**. Thus** $m = nk$**. Let** $f = a^k \in D$**. We know** $|f| = |a^k| = \frac{m}{gcd(k,m)} = \frac{m}{k} = n$**.**

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

3.8 Notes on $U(n)$ and Invariant Factors

$U(n)$,

① $|U(n)| = \phi(n)$

② $(U(n), \cdot)$ is cyclic $\underline{\text{iff}}$

$n = 2, 4, p^m, 2p^m$, p is $\underline{\underline{\text{odd}}}$ prime $m \geq 1$.

③ $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$$U(n) \cong U(p_1^{\alpha_1}) \oplus U(p_2^{\alpha_2}) \oplus \cdots \oplus U(p_k^{\alpha_k})$$

$U(2^m), m \geq 3 \longrightarrow \cong Z_2 \oplus Z_{m-2}$

$U(p^m), P \neq 2 \longrightarrow \cong Z_{p-1} \oplus Z_{p^{m-1}}$

Ex. $\rightarrow$ $n = 2^6 5^3 7^2$

$$U(n) \cong \underline{U(2^6)} \oplus U(5^3) \oplus U(7^2)$$

$$U(n) \approx Z_2 \oplus Z_{2^4} \oplus Z_4 \oplus \cancel{Z_{5^2}} + Z_6 \oplus \cancel{Z_7}$$

$m_1, \ldots, m_w$ (invariant factors)

$$U(n) \approx Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_w \quad (Z_2 \oplus \cancel{Z_3})$$

start with W_K, and go backward (if you wish

$$W_K = CM[2, 2^4, 4, 5^2, 6, 7]$$

$$W_K = 2^4 \cdot 5^2 \cdot 3 \cdot 7$$

$$Z_2 \oplus Z_2 \oplus Z_4 \oplus Z_{2^4 \cdot 5^2 \cdot 3 \cdot 7}$$

$m_1 = 2,\ m_2 = 2,\ m_3 = 4,\ m_5 =$

$$U(2^5 \cdot 7^3 \cdot 11) \approx U(2^5) \oplus U(7^3) \oplus U(11)$$

$$\approx Z_2 \oplus Z_{2^3} \oplus Z_6 \oplus Z_{7^2} \oplus Z_{10}$$

$$\approx Z_{m_1} \oplus \cdots \oplus Z_{m_w} \quad \text{s.t.}$$

$$m_1 \mid m_2 \cdots \mid m_w$$

$$m_w = LCM[10, 7^2, 6, 2^3, 2] = \underbrace{5 \cdot 7^2 \cdot 3 \cdot 2^3}_{\text{in view of this}}$$

so $\approx Z_2 \oplus \cancel{Z_{2^3}} \oplus Z_2 \oplus \cancel{Z_3} \oplus \cancel{Z_{7^2}} \oplus Z_2 \oplus \cancel{Z_5}$

so $m_w = 5 \cdot 7^2 \cdot 3 \cdot 2^3 \Rightarrow$ cross $Z_5, Z_{7^2}, Z_3, Z_{2^3}$

so

$$U(n) \approx \underset{m_1}{Z_2} \oplus \underset{m_2}{Z_2} \oplus \underset{m_3}{Z_2} \oplus \underset{m_4}{Z_{5 \cdot 7^2 \cdot 3 \cdot 2^3}}$$

$n = 2^5 \cdot 3^2 \cdot 7^2$

write $U(n)$ in terms of invariant factors

$U(n) \approx U(2^5) \oplus U(3^2) \oplus U(7^2)$

$\approx Z_2 \oplus \overset{x}{Z_{2^3}} \oplus \underbrace{Z_2 \oplus Z_3} \oplus \overset{x}{Z_6} \oplus \overset{x}{Z_7}$

We need $U(n) \approx Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_w}$

$m_w = 7 \cdot 6 \cdot 8 =$

$Z_2 \oplus Z_6 \oplus Z_{7\cdot 6\cdot 8}$

Invariant factors

$m_1 = 2,\ m_2 = 6,\ m_3 = 7\cdot 6\cdot 8$
$= 608$

$\to U(2^5 \cdot 3 \cdot 5^2) \approx U(2^5) \oplus U(3) \oplus U(5^2)$

$\approx Z_2 \oplus \overset{x}{Z_8} \oplus Z_2 \oplus Z_4 \oplus \overset{x}{Z_5}$

$m_w \to LCM[2, 8, 2, 4, 5] = 5 \cdot 8$

$Z_2 \oplus Z_2 \oplus Z_4 \oplus Z_8 \oplus Z_{5\cdot 8}$

$m_1 = 2, m_2 = 2, m_3 = 4, m_4 = 40$

1 classify all finite abelian groups (up to isomorphic) of ord $\boxed{2^3}\cdot\boxed{3^2}\cdot\boxed{5^3}$

Partion of 3	Partion of 2	all possible groups of order 2^3	Possible groups of order 3^2	Possible groups order 5^3
$0+3$ ✓	$0+2$ ✓	Z_8	Z_9	Z_{125}
$1+2$	$1+1$	$Z_2 \oplus Z_4$	$Z_3 \oplus Z_3$	$Z_5 \oplus Z_{25}$
$1+1+1$		$Z_2 \oplus Z_2 \oplus Z_2$	—	$Z_5 \oplus Z_5 \oplus Z_5$

$\downarrow 3$ $\downarrow 2$ $\times 3$

We will have exactly $\overset{18}{3 \times 2 \times 3}$ non-isomphic groups of order $2^3\cdot3^2\cdot5^3$

any group of order $2^3\cdot3^2\cdot5^3$ ~~[illegible]~~ will isomorphic to

(group in colum 3) $\oplus$ (group colum 4) $\oplus$ (group from column 5)

Introduction to rings

not on the final

Def. $(R, \underset{+}{+}, \underset{\text{mut.}}{\cdot})$, set R with 2 binary operations $+, \cdot$ s.t.

① $(R, +)$ is abelian group

② $(R, \cdot)$ is semigroup. (closure, associative)

③ $\forall a, b, c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$

distributive

and $(b+c) \cdot a = b \cdot a + c \cdot a$

any set $(R, +, \cdot)$ satisfies (1) + (2) + (3), called ring

If $(R^*, \cdot)$ [$R^* = R -$ additive identity of R] is abelian group,

we say R is a field.

$(\mathbb{Z}, +, \cdot)$ is a ring — $(R, \cdot)$ is abelian semigroup.

commutative ring

$(R^{2\times 2}, +, \cdot) \rightarrow$ ring

noncommutative

$\left(\text{cont. function}, +, \circ\right)$

4 Section : Worked out Solutions for all Assessment Tools

4.1 HW1-Solution

MTH320 - Abstract Algebra I

HW #1

September 14th, 2020

Question 1:
Let H be the set of all symmetries on an equilateral triangle. Construct the Caley's Table of $(H,\circ)$ and conclude that $(H,\circ)$ is a group.

From class notes, we have the following 6 functions:

$$\left\{f_1\colon\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, f_2\colon\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, f_3=e\colon\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, f_4\colon\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, f_5\colon\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, f_6\colon\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\right\}$$

We further know that the binary operator is the composition of the functions. We define the binary operator as per the following example:

$$f_1\circ f_2=f_1(f_2)$$

By this, we say for each $a,b,c\in f_n$, we approach it by doing the following. Let us take a for this case and see what happens to a.

1. We first see what a corresponds to in f_2. In this case, it is c
2. Now, we return to f_1 and see what c corresponds to after the rotation, and in this case, it is a

Therefore, if we proceed with the same logic, we go by each of the columns:

$$\begin{gathered} a\to c\to a \\ b\to a\to b \\ c\to b\to c \end{gathered}$$

So:

$$f_1\circ f_2\colon\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}=f_3=e$$

Now, let us see the case for all 6 functions and their compositions with each other.

$$f_1\circ f_1\colon\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}=f_2$$

$$f_1\circ f_2\colon\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}=e$$

$$f_1\circ e\colon\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}=f_1$$

$$f_1\circ f_4\colon\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}=f_6$$

$$f_1\circ f_5\colon\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}=f_4$$

$$f_1\circ f_6\colon\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}=f_5$$

We can do the same for all the rows of the Caley table, but they are trivial. So we will no longer work out each individual composition and instead put all the results as per the same standards of the aforementioned technique.

Therefore, we can come up with the following Caley's Table:

$\circ$	f_1	f_2	e	f_4	f_5	f_6
f_1	f_2	e	f_1	f_6	f_4	f_5
f_2	e	f_1	f_2	f_5	f_6	f_4
e	f_1	f_2	e	f_4	f_5	f_6
f_4	f_5	f_6	f_4	e	f_1	f_2
f_5	f_6	f_4	f_5	f_2	e	f_1
f_6	f_4	f_5	f_6	f_1	f_2	e

Table 1.

We have thus constructed the Caley's table for the set of symmetries for an equilateral triangle. Now, what are some things we can conclude from this? We conclude that $(H, \circ)$ is a group because it has closure (all compositions result in elements of the set, H), it has an identity, e, and we will now look for the inverse of each element.

By definition, the inverse of an element is defined as follows: $a \cdot a^{-1} = e$. In this set, all we need to do is look at the Caley table to see what elements composed with each other give us the identity, e.

(i)

$$\begin{array}{ll} f_1^{-1} = f_2 & \text{since } f_1 \circ f_2 = e \\ f_2^{-1} = f_1 & \text{since } f_2 \circ f_1 = e \\ f_3^{-1} = f_3 & \text{since } f_3 = e \text{ and } e \circ e = e \\ f_4^{-1} = f_4 & \text{since } f_4 \circ f_4 = e \\ f_5^{-1} = f_5 & \text{since } f_5 \circ f_5 = e \\ f_6^{-1} = f_6 & \text{since } f_6 \circ f_6 = e \end{array}$$

Hence, we have found all the inverses, and these inverses are clearly also in the set H. Furhtermore, by observation from the Caley's table, we can see that it is also associative. So, since this is the case, we conclude that $(H, \circ)$ is a group (closure, inverse, identity, associative).

(ii) For all $f \in H$, find $|f|$. Note that $|f|$, or the order of f, is the minimum number of times the binary operation has to be repeated on the f before we obtain the identity, e. We will do one example to show the process and put the final answers for the rest.

$$\begin{array}{r} \text{To find } |f_1|, \text{ first we do:} \\ f_1 \circ f_1 \colon \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = f_2 \\ \text{Now we do } f_2 \circ f_1 \\ f_2 \circ f_1 \colon \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = f_3 \\ \text{Since } f_2 \circ f_1 = (f_1 \circ f_1) \circ f_1 = f_3 = e; \\ \text{we conclude that } |f_1| = 3 \\ \text{(Since it took 3 binary operations to get } e) \end{array}$$

$$\begin{array}{ll} |f_1| = 3 & \text{Since } f_1 \circ f_1 \circ f_1 = e \\ |f_2| = 3 & \text{Since } f_2 \circ f_2 \circ f_2 = e \\ |f_3| = 1 & \text{Since } f_3 = e \end{array}$$

$$
\begin{aligned}
|f_4| &= 2 \quad \text{Since } f_4 \circ f_4 = e\\
|f_5| &= 2 \quad \text{Since } f_5 \circ f_5 = e\\
|f_6| &= 2 \quad \text{Since } f_6 \circ f_6 = e
\end{aligned}
$$

We have thus found the order of each of the six elements in the group.

(iii) Show that $(H, \circ)$ is a non-Abelian group.

The definition of an Abelian group is that for all Takeelements in a group, the binary operator acting on the elements results in the same outcome, which is another element in the group, regardless of the order the operator is acted.

Mathematically, Let $(D, \cdot)$ be a group. Then: $\forall a, b \in D,\ a \cdot b = b \cdot a \in D$.

To prove that this group is non-Abelian, we need to find just one example where this commutivity does not hold. We can simply refer to the Caley's table to see this.

$$f_1 \circ f_4 = f_6$$

$$f_4 \circ f_1 = f_5$$

Clearly we have shown that $f_4 \circ f_1 \neq f_1 \circ f_4$, and thus the commutative property does not hold for all elements in this group. Therefore, the group is safely concluded to be non-Abelian.

Question 2:

Let C be the set of complex numbers. We know that $(C^*, \times)$ is a group under multiplication. Let n be some fixed positive integer, $n \geqslant 2$, and let H be the set of all the roots of the polynomial $x^n - 1$. i.e.

$$H = \{x \in C^* |\, x^n - 1 = 0\}$$

Prove that $(H, \times)$ is a subgroup of $(C^*, \times)$.

Firstly, we take advantage of the fact that H is a finite subset of C. If we take this into consideration, then we can use a result introduced in the lectures that tells us that if we have a finite subset of a "larger" set, if the larger set is a group, then the subset, under the same binary operator, will also be a group iff it is closed.

In our case, we know that $(C^*, \times)$ is a group, and $H \subset C^*$. Then we need to show that $(H, \times)$ is closed for it to be a subgroup. We proceed as follows:

$$
\begin{aligned}
\text{Let } a, b \in H & \quad a \text{ and } b \text{ are chosen randomly}\\
a \text{ satisfies: } a^n - 1 = 0 &\\
b \text{ satisfies: } b^n - 1 = 0 &\\
a^n = b^n = 1 &\\
\text{We want to show that } a \cdot b \in H &\\
(a \cdot b)^n - 1 = (a^n) \times (b^n) - 1 &\\
= (1 \times 1) - 1 &\\
= 0 &
\end{aligned}
$$

$$
\begin{aligned}
\text{Therefore:} \quad (a \times b)^n - 1 = 0 &\\
\text{And thus } a \cdot b \in H &\\
H \text{ is closed.} &
\end{aligned}
$$

We have shown that H is closed under the binary operation $\times$. Since it is a finite subset, it is then concluded that $(H, \times)$ is a subgroup of $(C^*, \times)$.

Question 3:

Consider the group $(\mathbb{Z}_{20}, +)$. Find $|1|, |6|, |14|, |15|, |17|, |12|$.

We first find $|1|$ and observe the fact that $k = 1^k$. Then we can proceed and find the rest.

$$\begin{aligned} 1 + 1 + 1 + \text{....} + 1\,(20\,\text{times}) &= 20 \\ 20\text{mod}20 &= 0 \\ \text{Therefore, } |1| &= 20 \end{aligned}$$

Note that by a result introduced in the lectures, if we have some a in a group where the order of a is finite, then $|a^k| = \frac{m}{\gcd(k, m)}$. We also know that for some $k \in \mathbb{Z}_{20}$, $1^k = k$ (As per the instructions of the question, but we can also observe this fact very easily).

Using these results, we can go on to find the orders of the remaining five elements.

$$\begin{aligned} |6| = |1^6| &= \frac{|1|}{\gcd(|1|, 6)} \\ &= \frac{20}{\gcd(20, 6)} \\ &= \frac{20}{2} = 10 \\ \text{Therefore, } |6| &= 10 \end{aligned}$$

$$\begin{aligned} |14| = |1^{14}| &= \frac{20}{\gcd(20, 14)} \\ &= \frac{20}{2} = 10 \end{aligned}$$

$$\begin{aligned} |15| = |1^{15}| &= \frac{20}{\gcd(20, 15)} \\ &= \frac{20}{5} = 4 \end{aligned}$$

$$\begin{aligned} |17| = |1^{17}| &= \frac{20}{\gcd(20, 17)} \\ &= \frac{20}{1} = 20 \end{aligned}$$

$$\begin{aligned} |12| = |1^{12}| &= \frac{20}{\gcd(20, 12)} \\ &= \frac{20}{4} = 5 \end{aligned}$$

Question 4:

Let $H = \{2, 4, 6, 8, 10, 12\}$. Let $\cdot$ be the binary operation: multiplication modulo 14. Construct the Caley's table for $(H, \cdot)$

$\boxed{\cdot_{14}}$	2	4	6	8	10	12
2	4	8	12	2	6	10
4	8	2	10	4	12	6
6	12	10	8	6	4	2
8	2	4	6	8	10	12
10	6	12	4	10	2	8
12	10	6	2	12	8	4

Table 2.

Obviously, this is an Abelian group because $\forall a, b \in H$, $a \cdot b = b \cdot a$.

(i) What is e?

for some $d, e \in H$, we have that $d \cdot e = e \cdot d = d$. What element do we have in H such that

$(d \cdot e)(\mathrm{mod} 14) = d$?

This element is 8. Notice that, as an example, $(2 \cdot 8)\mathrm{mod}14 = 16\mathrm{mod}14 = 2$. Another example would be $(12 \cdot 8)\mathrm{mod}14 = 96\mathrm{mod}14 = 12$.

$$\text{Obviously}, e = 8$$

(ii) For each $a \in H$, find a^{-1}.

$$\begin{aligned} 2^{-1} &= 4 && \text{Since } (2 \cdot)\mathrm{mod}14 = 8 \\ 4^{-1} &= 2 && \text{Since } (4 \cdot 2)\mathrm{mod}14 = 8 \\ 6^{-1} &= 6 && \text{Since } (6 \cdot 6)\mathrm{mod}14 = 8 \\ 8^{-1} &= 8 && \text{Since } (8 \cdot 8)\mathrm{mod}14 = 8 \\ 10^{-1} &= 12 && \text{Since } (10 \cdot 12)\mathrm{mod}14 = 8 \\ 12^{-1} &= 10 && \text{Since } (12 \cdot 10)\mathrm{mod}14 = 8 \end{aligned}$$

(iii) Find $|6|$ and $|10|$

$$(6 \cdot 6)\mathrm{mod}14 = 8, \text{therefore } |6| = 2$$

Using a calculator, we can see that

$$1{,}000{,}000\mathrm{mod}14 = 8$$

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 1000000$$

$$\text{Therefore, } |10| = 6$$

Question 5:

Part 1:

Let a, b be elements in a group, $(D, \cdot)$ such that $a \cdot b = b \cdot a$. Given that $|a| = n$, $|b| = m$, where n, $m \neq \infty$ and $\gcd(n, m) = 1$, let $x = a \cdot b$. Prove that $|x| = n m$.

Hints:

$$\text{if } a \cdot b = b \cdot a, \text{then } (a \cdot b)^n = a^n \cdot b^n$$

$$\text{if } a \cdot b \neq b \cdot a, \text{we CANNOT conclude } (a \cdot b)^n = a^n \cdot b^n$$

Let k, n, m be positive integers

1. If $n|km$ and $\gcd(n,m) = 1$, then $n|k$.
2. If $n|k$ and $m|k$ and $\gcd(n,m) = 1$, then we conclude that $nm|k$

In the question, we are given the following facts: $\gcd(n,m) = 1$, $|a| = n$, $|b| = m$.

$$\begin{aligned} x &= a \cdot b \\ \text{Let us take } k = |x| & \quad (i.e. x^k = e), k \in \mathbb{Z}^+ \\ \text{Assume } k \text{ to be the smallest positive integer} & \\ \text{such that } x^k = e & \end{aligned}$$

$$\begin{aligned} (a \cdot b)^k = (a)^k \cdot (b)^k &= e \\ \text{We know } a^n = e \text{ and } b^m &= e \end{aligned}$$

By some result introduced in the lectures, we know that if $|a| = n$, and $a^k = e$, then $n|k$. So we can conclude the following:

$$\begin{aligned} n|k, k \text{ is divisible by } n & \\ \frac{k}{n} = \alpha & \quad \alpha \in \mathbb{Z}^+ \\ \text{In other words, } k = \alpha n & \end{aligned}$$

$$\begin{aligned} \text{Furthermore, } m|k & \\ \frac{k}{m} = & \quad \quad \in \mathbb{Z}^+ \\ \text{In other words, } k = \beta m & \end{aligned}$$

By the hint given to us in the question, we know that if $n|k$ and $m|k$, then $nm|k$ (Given that $\gcd(n,m) = 1$). In other words, $k = \gamma nm$, for some $\gamma \in \mathbb{Z}^+$.

$$\begin{aligned} (a \cdot b)^{mn} &= a^{mn} \cdot b^{mn} \\ &= (a^n)^m \cdot (b^n)^m \\ a^n &= b^n = e \\ \text{Therefore:} \quad e^m \cdot e^m &= e \cdot e = e \end{aligned}$$

$$\text{Hence } k|mn$$

Since $k\ |mn$ and $mn|k$, we can logically conclude that $k = mn$. In this case, we can easily see the following:

$$|x| = k = nm$$

$$x^k = x^{mn} = e$$

Part 2:

Find two elements in **Question 1**, f and k in $(H, \circ)$ s.t. $|f| = 2$ and $|k| = 3$, but $|f \circ k| \neq 6$.

Let us take $f = f_4, |f_4| = 2$, and $k = f_1, |f_1| = 3$.

$$f_4 \circ f_1 = f_5$$

$$|f_5| = 2 \neq 6$$

Hence we can clearly see that despite the fact that $\gcd(2, 3) = 1$, we cannot claim that $|f_4 \circ f_1| = 6$, in fact we have proven for it to be 2. This is because the group in **Question 1** is NON-Abelian and we cannot say that $a \cdot b = b \cdot a \quad \forall a, b \in H$.

4.2 HW2-Solution

MTH320 - Abstract Algebra I

HW #2 (Solutions)

September 29th, 2020

Question 1:

Let $A=\{1,2,3\}$ and D be the power set of A, i.e., D is the set of all subsets A (note that $|D|=2^3=8$). Define "·" on D to mean $a\cdot b=(a\ \cancel{b})\cup(b\ \cancel{a})\,\forall a,b\in D$. Then $(D,\cdot)$ is an Abelian group.
Since D is the set of all subsets of A, then:

$$D=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$$

The Caley's Table:

$a\cdot b$	$\varnothing$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{1,3\}$	$\{2\}$	$\{3\}$	$\{1,2,3\}$	$\{2,3\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{2,3\}$	$\{1\}$	$\{1,2,3\}$	$\{3\}$	$\{1,3\}$
$\{3\}$	$\{3\}$	$\{1,3\}$	$\{2,3\}$	$\varnothing$	$\{1,2,3\}$	$\{1\}$	$\{2\}$	$\{1,2\}$
{1,2}	$\{1,2\}$	$\{2\}$	$\{1\}$	$\{1,2,3\}$	$\varnothing$	$\{2,3\}$	$\{1,3\}$	$\{3\}$
{1,3}	$\{1,3\}$	$\{3\}$	$\{1,2,3\}$	$\{1\}$	$\{2,3\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
{2,3}	$\{2,3\}$	$\{1,2,3\}$	$\{3\}$	$\{2\}$	$\{1,3\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2,3\}$	$\{1,2,3\}$	$\{2,3\}$	$\{1,3\}$	$\{1,2\}$	$\{3\}$	$\{2\}$	$\{1\}$	$\varnothing$

Table 1.

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

Obviously e is the element where for some $a\in D$, $a\cdot e=a$. In other words, $(a-e)\cup(e-a)=a$. The only element with this property is $\varnothing$. For any a, $a\cdot\varnothing=a$. As an example:

$$\{1,2,3\}\cdot\varnothing=[\{1,2,3\}-\varnothing]\cup[\varnothing-\{1,2,3\}]=\{1,2,3\}$$

(ii) For each $a\in D$, find a^{-1}

Again, we will simply use the Caley's table to find the inverse of each of the 8 elements in D. We proceed as follows:

$$\begin{aligned}
\{1\}^{-1}&=\{1\} \quad \text{Since } \{1\}\cdot\{1\}=\varnothing,\text{same argument for all}\\
\{2\}^{-1}&=\{2\}\\
\{3\}^{-1}&=\{3\}\\
\{1,2\}^{-1}&=\{1,2\}\\
\{1,3\}^{-1}&=\{1,3\}\\
\{2,3\}^{-1}&=\{2,3\}\\
\{1,2,3\}^{-1}&=\{1,2,3\}\\
\varnothing^{-1}&=\varnothing
\end{aligned}$$

As a matter of fact, each element is its own inverse (Again visible from the Caley's table).

(iii) For each $a \in D$, find $|a|$

A sample calculation is provided below as to how we get the order of each element. The rest is self explanatory.

$$\begin{aligned} &\{1\}: \\ \{1\} \cdot \{1\} &= \varnothing \\ \{1\}^2 &= \varnothing \\ \text{Therefore } |\{1\}| &= 2 \end{aligned}$$

$$\begin{aligned} |\{2\}| &= 2 \\ |\{3\}| &= 2 \\ |\{1,2\}| &= 2 \\ |\{1,3\}| &= 2 \\ |\{2,3\}| &= 2 \\ |\{1,2,3\}| &= 2 \\ |\varnothing| &= 1 \qquad \text{Since } \varnothing \text{ is the identity} \end{aligned}$$

(iv) The converse of the Lagrange theorem is correct when a group is finite and Abelian, i.e. if D is an Abelian group, $|D| = n$, and $m|n$, Then D has at least one subgroup with m elements. Now the above group is Abelian and $|D| = 8$. Give a subgroup, say H, of D with 4 elements. Verify that H is a subgroup by doing the Caley's table. Does D have an element of order 4?

(If $m|n$, then we must have a subgroup with m elements, but not necessarily an element of order m)

Let us take $H = \{\varnothing, \{1,2\}, \{1,3\}, \{2,3\}\}$. This subset of D is clearly a subgroup of $(D, \cdot)$. The Caley's table is shown below:

$a \cdot b$	$\varnothing$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$
$\varnothing$	$\varnothing$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$
$\{1,2\}$	$\{1,2\}$	$\varnothing$	$\{2,3\}$	$\{1,3\}$
$\{1,3\}$	$\{1,3\}$	$\{2,3\}$	$\varnothing$	$\{1,2\}$
$\{2,3\}$	$\{2,3\}$	$\{1,3\}$	$\{1,2\}$	$\varnothing$

Table 2.

From the table we can see that H is indeed a group. In fact, $H < D$. It satisfies all the properties of a group (Identity $e = \varnothing$, each element has an inverse, it is closed and associative). Furthermore, H is an Abelian group since $\forall a, b \in H, b \cdot a = a \cdot b$.

Now we can see that $|H| = 4$, and $4|8$. However, it is evident that $\forall a \in H, |a| = 2$, except for the case of $a = \varnothing$, in which case $|\varnothing| = 1$. Therefore, we can conclude that if we have $m|n$, that does not necessarily imply that we can find a subgroup with m elements that also has elements of order m.

Question 2:

Let $D = \{2, 4, 6, 8, 10, 12\}$. From HW1, we know that D under multiplication modulo 14 is an Abelian group. Now $H = \{6, 8\}$ is a subgroup of D. Find all the left cosets of H. Since D is Abelian, H is a normal subgroup of D. Construct the Caley's table for the group $(D/H, *)$.

From HW1, we know that $e = 8$. We will take the binary operator to be $\cdot_{14}$. All the left cosets of of H are as follows:

$$a \cdot H = \{a \cdot h \mid a \in D, h \in H\}$$

$$\begin{aligned}
2 \cdot H &= \{2 \cdot 6, 2 \cdot 8\} = \{12, 2\} \\
4 \cdot H &= \{4 \cdot 6, 4 \cdot 8\} = \{10, 4\} \\
6 \cdot H &= \{6 \cdot 6, 6 \cdot 8\} = \{8, 6\} = H \\
8 \cdot H &= \{8 \cdot 6, 8 \cdot 8\} = \{6, 8\} = H \\
10 \cdot H &= \{10 \cdot 6, 10 \cdot 8\} = \{4, 10\} \\
12 \cdot H &= \{12 \cdot 6, 12 \cdot 8\} = \{2, 12\}
\end{aligned}$$

Note that the identity here is:

$$e = 6 \cdot H = 8 \cdot H = H$$

We have 3 distinct left cosets of H. These are $2 \cdot H = \{2, 12\}, 4 \cdot H = \{4, 10\}$ and $6 \cdot H = \{6, 8\}$.

These are the elements of the set D/H.

$$D/H = \{2H, 4H, 6H\}$$

We define $*$, the binary operator on the set D/H as the following:

$$\forall x, y \in D/H, x * y = (a \cdot b) \cdot H$$

a, b are two left cosets of H.

Therefore, the Caley's table for $(D/H, *)$ would be:

$x * y$	$2H$	$4H$	$6H$
$2H$	$4H$	$6H$	$2H$
$4H$	$6H$	$2H$	$4H$
$6H$	$2H$	$4H$	$6H$

Table 3.

What is the identity of $(D/H, *)$? $6H$, since $\forall x \in D/H, x * 6H = x$. We can see from the Caley's Table that $(D/H, *)$ is closed, associative, each element has an inverse and it is closed. Furthermore, we can see that this group is Abelian because $\forall x, y \in D/H, x * y = y * x$.

Question 3:

Let $(D, \cdot)$ be a group, and H, K are distinct subgroups of D (i.e. $H \neq K$).

(i) Prove that $F = H \cap K$ is a subgroup of D [Hint: Let $a, b \in F$. By class result, you only need to show that $a^{-1} \cdot b \in F$ for every $a, b \in F$].

$$\begin{aligned}
F &= H \cap K \\
\\
\text{Firstly, since } H < D, \text{we know that } \{e\} &\in H \\
\text{Similarly, since } K < D, \{e\} &\in K \\
\text{Therefore } H \cap K \text{ contains AT LEAST the identity} \\
\text{Or, in other words, } H \cap K &\neq \varnothing \\
\\
\text{Let } a, b &\in F \\
\text{This means that } a, b \in H \text{ and } a, b &\in K \\
\\
\text{Since } H \text{ and } K \text{ are both subgroups,} \\
\text{then } a^{-1} \cdot b \in H \text{ and } a^{-1} \cdot b &\in K \\
\text{and since } a^{-1} \cdot b \text{ is in both } H \text{ and } K, \\
\text{by definition of the intersection,} \\
a^{-1} \cdot b &\in F \\
\\
\text{Therefore } F = H \cap K \text{ is a subgroup of } D
\end{aligned}$$

Since F is a subgroup of D, and $F \subseteq H, F \subseteq K$, then we can also directly say that $F < H$ and $F < K$. Therefore F is also a subgroup of both H and K.

(ii) Assume that neither $K \subset H$ nor $H \subset K$. Prove that $H \cup K$ is never a subgroup of D.

We proceed by contradiction, i.e. we assume $F = H \cup K$ is a subgroup of D.

$$\begin{aligned}
H \not\subset K \text{ and } K \not\subset H \\
\text{we choose } a \in H \text{ and } b \in K, \text{but } a \notin K \text{ and } b \notin H \\
\\
\text{but since } F \text{ is a subgroup,} \\
a \cdot b \in F \\
\text{Meaning that } a \cdot b \in H \text{ or } a \cdot b \in K & \quad \text{By definition of the union} \\
\\
a^{-1} \cdot a \cdot b \in H \rightarrow b \in H & \quad \text{Contradiction} \\
\text{OR} \\
a \cdot b \cdot b^{-1} \in K \rightarrow a \in K & \quad \text{Also a contradiction}
\end{aligned}$$

In other words, if we assume the union to be a subgroup, then we would have that an element that cannot be in one of the subgroups H and K would be in them, which is a contradiction of the fact that $H \not\subset K$ and $K \not\subset H$.

Therefore, $H \cup K$ is never a subgroup of D.

(iii) Assume $|H| = |K| = m$, where m is a prime positive integer. Prove that $H \cap K = \{e\}$

The intersection between $H \text{ and} K$ must be a subgroup, by the result proven in 3(i). This means that $H \cap K < D$. We can also say that $H \cap K < H \text{ and} H \cap K < K$. Now,

$$\begin{array}{r}
\text{Since } |H| = |K| = m \\
\text{and } H \cap K < H \\
\\
\text{Therefore, by Langrange}'s\text{ theorem:} \\
|H \cap K|\,|m \\
\text{The cardinality of } H \cap K \text{ divides } m, \\
\text{which is the cardinality of } H \\
\\
\text{But we know that } m \text{ is prime, meaning that:} \\
\text{the only numbers that divide it are 1 and } m \\
\text{So:} \\
|H \cap K| = m \text{ or } |H \cap K| = 1 \\
\\
\text{However:} \\
\text{Since } H \text{ is not the same as } K \text{ and } m \text{ is prime,} \\
|H \cap K| \neq m \\
\text{So:} \\
\\
|H \cap K| = 1 \\
\\
\text{Since } H \cap K \text{ is a group with one element,} \\
\text{then the only element it can contain is } e \\
\\
\text{Therefore } H \cap K = \{e\}
\end{array}$$

We have proven that the intersection of two subgroups (which is itself a subgroup) of D contains only the identity of D.

Question 4:

(a) **[CORRECTED]** Let $(D, \cdot)$ be a group, H is a normal subgroup of D, and K is a subgroup of D. Prove that $H \cdot K = \{h \cdot k | h \in H, k \in K\}$ is a subgroup of D. Note that H is a subgroup of $H \cdot K$ and $K$is a subgroup of $H \cdot K$ since $H \cdot e = H \text{ and} e \cdot K = K$ [Hint: Let $a, b \in H \cdot K$, by a class result, you only need to show that $a^{-1} \cdot b \in H \cdot K$ for every $a, b \in H \cdot K$].

$$\begin{aligned}
\text{Let } a, b &\in H \cdot K \\
a = h_1 \cdot k_1, b &= h_2 \cdot k_2 && h_1, h_2 \in H, k_1, k_2 \in K \\
a^{-1} \cdot b &= (h_1 \cdot k_1)^{-1} \cdot (h_2 \cdot k_2) \\
k_1^{-1} &\cdot h_1^{-1} \cdot h_2 \cdot k_2 \\
h_1^{-1} \cdot h_2 &\in H && \text{Since } H \text{ is a subgroup} \\
\text{Let } h_3 = h_1^{-1} \cdot h_2 &\in H \\
\text{Hence } a^{-1} \cdot b &= k_1^{-1} \cdot h_3 \cdot k_2
\end{aligned}$$

$$\begin{aligned}
&\text{Since } H \text{ is normal, we have:}\\
k_1^{-1}\cdot h_3\cdot k_2 &= h_4\cdot k_1^{-1}\cdot k_2\\
&\text{For some } h_4\in H\\
\\
\text{Let } k_3 &= k_1^{-1}\cdot k_2\\
&\text{meaning that } k_3\in K\\
\\
&\text{Therefore:}\\
a^{-1}\cdot b &= h_4\cdot k_3\in H\cdot K
\end{aligned}$$

Therefore, we have proven that for every $a, b\in H\cdot K$, $a^{-1}\cdot b\in H\cdot K$. This condition is enough to satisfy the condition for subgroups, and therefore $H\cdot K$ is a subgroup of D.

(b) **[CORRECTED]** Consider S_3, the symmetric group of an equilateral triangle (As in HW1). Give a subgroup, say H of S_3, that is not a normal subgroup of S_3.

$$\left\{ f_1{:}\begin{pmatrix} a & b & c\\ b & c & a \end{pmatrix}, f_2{:}\begin{pmatrix} a & b & c\\ c & a & b \end{pmatrix}, f_3 = e{:}\begin{pmatrix} a & b & c\\ a & b & c \end{pmatrix}, f_4{:}\begin{pmatrix} a & b & c\\ a & c & b \end{pmatrix}, f_5{:}\begin{pmatrix} a & b & c\\ c & b & a \end{pmatrix}, f_6{:}\begin{pmatrix} a & b & c\\ b & a & c \end{pmatrix} \right\}$$

This is the symmetric group of an equilateral triangle. Out of these 6 elements, we can form a subgroup, H that is NOT a normal subgroup of S_3. This means that for some $a\in S_3, a\cdot H\neq H\cdot a$.

We need to note here that we mustn't fall into this trap: The condition for a normal subgroup is that we can find some $h, k\in H$ st $\forall a\in S_3$, $a\cdot h = k\cdot a$. k and h do not necessarily need to equal each other for the subgroup to be normal. With that in mind, let us take $H = \{e, f_4\}$:

$$H = \left\{ e{:}\begin{pmatrix} a & b & c\\ a & b & c \end{pmatrix}, f_4{:}\begin{pmatrix} a & b & c\\ a & c & b \end{pmatrix} \right\}$$

The Caley's table for this subset is:

$\circ$	e	f_4
e	e	f_4
f_4	f_4	e

Table 4.

Clearly, from this Caley's table, we can see that the subset is a subgroup of S_3. Now, let us see if the subgroup is normal. Since being a normal subgroup means: $\forall a\in S_3, a\cdot H = H\cdot a$, the negation of the statement means that $\exists a\in D$ (at least one) where $a\cdot H\neq H\cdot a$.

Let us take some random element in S_3, which will serve as our a. Take $a = f_1$. Then:

$$\begin{aligned}
\text{We check to see if } a\cdot h &= k\cdot a && h, k\in H\\
f_1\circ f_4 &= f_6 && \text{From Caley's Table in } \mathbf{HW1}\\
f_4\circ f_1 &= f_5\\
f_4\circ f_1 &\neq f_1\circ f_4
\end{aligned}$$

Note that H only has two elements, making it easy to see the other possibilities. Hence:

$$f_4\cdot H\neq H\cdot f_4$$

And this shows that H is NOT a normal subgroup of S_3.

4.3 HW3-Solution

MTH 320 - Abstract Algebra

HW #3 Solutions

October 14th, 2020

Question 1: Let $(D,\cdot)$ be a group with 130 elements. Given $a,b \in D$ such that $a \cdot b = b \cdot a$, $|a| = 10$ and $|b| = 13$, prove that D is an Abelian group. What more can we say about this group?

We are given some $a,b \in D$ such that $|a| = 10$ and $|b| = 13$. By previous result shown in HW1, we know that since $(D,\cdot)$ is a group and we have two elements in D, say a and b, then $|a \cdot b| = |a| \cdot |b|$ if $\gcd(|a|,|b|) = 1$ and $a \cdot b = b \cdot a$.

In our case, we know that $\gcd(10,13) = 1$, meaning that for some $c = a \cdot b \in D$, $|c| = |a| \cdot |b| = 10 \cdot 13 = 130$. This means that the order of the element c is 130, or in other words, there exists an element inside D such that the order of the element is equal to the cardinality of D itself. Mathematically:

$$\exists c \in D \,\text{st}\, |c| = 130 = |D|$$

With this knowledge, we know that c forms up the entirety of the group, D. In other words, $D = <c>$. Every other element in the group, $(D,\cdot)$ can be made by taking c to some power, where the power represents the repitition of the binary operation, $(\cdot)$.

This means that D is indeed not only a group, but a *cyclic* group. Automatically, through the discussion introduced in class, we know that if a group is cyclic, then it is also Abelian. Therefore we have proven that $(D,\cdot)$ is Abelian, and went an extra step to show that it is alo cyclic.

Question 2:

i. Assume $(D,\cdot)$ is an infinite cyclic group and $a \in D \,\text{st}\, a \neq e$. Prove that $|a| = \infty$.

   Since $(D,\cdot)$ is an infinite cyclic group, $D = <a>$ for some $a \in D$. Let $b \in D$ and assume that $|b| = m$. Since we know that $b \in D = <a>$, then we conclude that $b = a^k$ for some $k \in \mathbb{Z}$.

   Since $|b| = m$, we have that $b^m = e$, which means that $(a^k)^m = e$. However, this is a contradiction because we are saying that a^{km}, where km is a finite number gives us the identity, e. Since $(D,\cdot)$ is an infinite cyclic group, we conclude that $|a| = \infty$.

ii. We know that $(\mathbb{Z}_8,+)$ is cyclic and $(\mathbb{Z},+)$ is cyclic. Prove that $\mathbb{Z}_8 \oplus \mathbb{Z}$ is not a cyclic group. Use the above proof from (i).

   Let $x = (1,0) \in \mathbb{Z}_8 \oplus \mathbb{Z}$. Then we know that $|x| = \text{lcm}(|1|,|0|) = \text{lcm}(8,1) = 8$. Since x is not the identity of $\mathbb{Z}_8 \oplus \mathbb{Z}$ by our choice, and it is of finite order, we can conclude using (i) that D is NOT cyclic.

iii. Let $(H,\cdot)$ and $(K,*)$ be cyclic groups st $|H|=m$ and $|K|=n$. Let $D=H\oplus K$. Prove that D is cyclic iff $\gcd(m,n)=1$.

$$\Longrightarrow$$

$$\text{Assume } D \text{ is cyclic, show } \gcd(m,n)=1$$

$$\text{let } h\in H, k\in K$$

$$\text{We know that since } D=H\oplus K\text{, then } |D|=|H|\times|K|$$

$$\text{ie } |D|=m\,n$$

$$\text{Since } H \text{ is cyclic, it has exactly } \varphi(m) \text{ elements of order } m$$

$$\text{Similarly, } K \text{ has exactly } \varphi(n) \text{ elements of order } n$$

$$\text{(From class result)}$$

$$\text{We are assuming that } D \text{ is cyclic, ie } \exists a\in D \text{ st } |a|=|D| \qquad a=(h,k)$$

$$|a|=|(h,k)|=m\times n$$

We know that the concept of order suggests the LEAST positive number st $a^{m\times n}=e$, leading us to the fact that:

$$\operatorname{lcm}(m,n)=m\times n$$

$$\gcd(m,n)=\frac{m\times n}{\operatorname{lcm}(m,n)}=\frac{m\,n}{m\,n}=1$$

$$\Longleftarrow$$

$$\text{Assume } \gcd(m,n)=1\text{, show that } D \text{ is cyclic}$$

$$\gcd(m,n)=\frac{m\,n}{\operatorname{lcd}(m,n)}\Rightarrow \operatorname{lcd}(m,n)=m\,n$$

$$\text{Let } h\in H \text{ and } k\in K$$

$$\text{Since } H \text{ and } K \text{ are both cyclic groups, then } \exists h\in H \text{ st } |h|=m=|H|$$

$$\text{and similarly, } \exists k\in K \text{ st } |k|=n=|K|$$

$$|D|=m\,n \text{ (By previous proof)}$$

$$\text{Let } a=(h,k)\in D$$

$$|a|=\operatorname{lcm}(m,n) \qquad \text{By definition of } D$$

$$|a|=n\,m$$

$$\text{Therefore, } \exists a\in D \text{ st } |a|=|D|=|H|\times|K|=m\,n$$

$$\text{And hence } D \text{ is cyclic, } D=<a>$$

iv. Let $D=(\mathbb{Z}_8,+)\oplus(\mathbb{Z}_{15},+)$. Then, by (iii), D is cyclic. How many generators does D have? Find all subgroups of D with 20 elements. How many elements of order 40 does D have?

Since $\gcd(8,15)=1$, D is cyclic and $|D|=|\mathbb{Z}_8|\times|\mathbb{Z}_{15}|$. We know that $\mathbb{Z}_8$ has $\varphi(8)=4$ generators and similarly, $\mathbb{Z}_{15}$ has $\varphi(15)=8$ generators. This means that the number of generators for D is exactly $4\times 8=32$, since each pair of two generators from $\mathbb{Z}_8$ and $\mathbb{Z}_{15}$ can form a generator for D.

We know that $|D| = 15 \times 8 = 120$. This means that the total number of elements in D is 120. By a class result, we know that since $20|120$, then there exists a unique subgroup of D where the cardinality is 20. In other words, this subgroup contains exactly 20 elements, and it is the only one that does.

There is exactly one subgroup, H, of D with 20 elements. Choose one element in D with order 20. For example, choose $x = (2, 3)$. $|x| = 20$. Thus $H = <(2, 3)> = F \oplus K$, where $F = \{0, 2, 4, 6\} < \mathbb{Z}_8$ (subgroup of $\mathbb{Z}_8$) and $K = \{0, 3, 6, 9, 12\} < \mathbb{Z}_{15}$ (subgroup of $\mathbb{Z}_{15}$).

To find the number of elements in D that have order 40, we consider the following:

$$\begin{aligned} \text{Let } d = (h, k) \in D \\ h \in \mathbb{Z}_8, k \in \mathbb{Z}_{15} \\ \text{st lcm } (|h|, |k|) = 40 \quad \forall d \in D \\ \\ |h| = 8, |k| = 5 \text{ or } |h| = 5, |k| = 8 \\ \text{In either case,} \\ \text{the number of elements with order 5: } \varphi(5) \\ \text{the number of elements with order 8: } \varphi(8) \\ \\ \text{Therefore:} \\ \text{the number of elements with order 40: } \varphi(5) \times \varphi(8) \\ = 4 \times 4 \\ = 16 \end{aligned}$$

v. Let $(D, \cdot)$ be a group. Given that D has exactly 10 distinct subgroups, each with 13 elements, how many elements of order 13 does D have?

We know that we have 10 distinct subgroups with 13 elements in each. Let us consider the following:

$$\begin{aligned} \text{Consider } H < D \ (H \text{ is a random subgroup of } D) \\ |H| = 13 \\ \text{We want to find an element, } h \in H \text{ st } |h| = 13 \\ \forall h \in H, |h| = 13 \text{ because } |H| \text{ is prime} \\ \text{and } |h| \text{ divides } |H| \\ \\ \text{Therefore, we conclude that } H = <h> \text{ (Cyclic)} \\ \text{and thus } H \text{ has } \varphi(13) \text{ elements with 13 elements} \\ \varphi(13) = 12 \\ \\ \text{We know from a previous HW that the intersection} \\ \text{of two subgroups that both have prime order is } \{e\}. \\ \text{Hence } D \text{ has exactly 10 subgroups,} \\ \text{and so it has } 10 \times 12 \text{ elements of order 13} \\ = 120 \text{ elements} \end{aligned}$$

Question 3:

a) Let $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 6 & 8 & 9 & 2 & 3 & 1 & 5 \end{smallmatrix}\right) \in S_9$. Find $|f|$.

We have an element in the symmetric group of size 9, such that $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 6 & 8 & 9 & 2 & 3 & 1 & 5 \end{smallmatrix} \right)$. In order to find the order of f, we need to consider the following:

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

And so we know that $|f| = \text{lcm}\,(3, 4, 2) = 12$.

$$\text{Therefore: } |f| = 12$$

b) Let $f = (\ 1\ \ 3\ \ 7\ ) \circ (\ 1\ \ 2\ \ 4\ \ 5\ ) \circ (\ 2\ \ 3\ \ 1\ \ 6\ ) \in S_7$. Find $|f|$.

Similar to part (a), we can simply proceed as follows:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

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

Since we have now written f is the composition of disjoint cycles, we can use the result used in part (a):

$$|f| = 7$$

Question 4: Let $(D, \cdot)$ be a group st $|D| = 77$. Given that H is a normal subgroup of D st $|H| = 7$, suppose that D has exactly one subgroup with 11 elements. Prove that D is a cyclic group. Think about D/H.

Let $a \in D, a \neq e$. By Lagrange's theorem, $|a| = 7, 11\,\text{or}\,77$. Let F be the unique subgroup of D with 11 elements. Choose $b \notin F\,\text{and}\,b \notin H$. Since F is a unique subgroup with 11 elements, then $|b| \neq 11$. Therefore, $|b| = 7\,\text{or}\,77$. We say that $|b| = 7$ because there is no uniqueness for the subgroup H, implying that even if $b \notin H$, it could still belong to another subgroup with 7 elements.

Let us assume that $|b| = 7$. $b \cdot H$ is an element of the group D/H ($H \lhd D$, and thus D/H is a group), and $b \cdot H \neq H$ (Because $b \notin H$). Furthermore, because $|b| = 7$, we have that $b^7 = e \in D$.

We conclude that $(b \cdot H)^7 = e \cdot H = H \in D/H$. Thus $|b \cdot H| = 7$. However, we have that $|D/H| = 11$, and by Lagrange's theorem, that means that $7|11$. This is not possible since 7 does not divide 11. This leaves us with one option, and that is $|b| = 77$.

Since we have found an element in D that has the same order as the number of elements in the group, we can conclude the following:

$$D = <b>$$

Therefore, D is a cyclic group.

4.4 HW4

Name————————————, ID ——————

Homework Four, MTH 320 , Fall 2020, Due date: October 29, 2020, by MIDNIGHT, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

QUESTION 1. Let D_n ($n \geq 3$) be the set of all symmetries on $n - gon$ (see class notes). We know from class notes that (D_n, o) is a group with exactly 2n elements (exactly n elements are rotations and exactly n elements are reflections, note $e = R_{360}$ and $R_a^{-1} = R_a$ for every reflection $R_a \in D_n$.). It is clear that the composition of two rotations is a rotation in D_n.

(i) (give a short proof, but clear-cut). Prove that the composition of a rotation with a reflection is a reflection in D_n (nice!) (i.e, assume that R is a rotation and R_a is a reflection, prove that $R\ o\ R_a = R_b$ for some reflection R_b in D_n.)

Proof. Let R be a rotation and E be a reflection. Assume that $R\ o\ E = R_1$ for some rotation R_1. Hence $E = R_1\ oR^{-1}$, a contradiction since the composition of two rotations is a rotation. Thus $R\ o\ E = F$ for some reflection F. (note, similarly $EoR = H$ for some reflection H.)

(ii) (give a short proof, but clear-cut).Prove that the composition of two reflections is a rotation in D_n (i.e, assume that R_a, R_b are reflections in D_n, prove that $R_a\ o\ R_b = R$ for some rotation R in D_n.).

Proof Assume that $F_1\ F_2 = F_3$, where F_1, F_2, F_3 are some reflections. Since number of rotations = number of reflections, by (i) we conclude $\{F_1\ o\ R_1, F_1\ o\ R_2, ..., F_1\ o\ R_n\}$ = set of all reflections. Thus $F_1\ o\ R_i = F_3$ for some rotation R_i. Since $F_1\ o\ F_2 = F_3$ and $F_1\ o\ R_i = F_3$, we conclude that $R_i = F_2$, impossible. Thus $F_1\ o\ F_2$ is a rotation.

QUESTION 2. (a) Assume $(D, .)$ is a group such that $a^2 = e$ for every $a \in D$. Prove that D is an abelian group.

Proof. Let $a \in D$. Since $a^2 = e$, we conclude that $a^{-1} = a$. Let $a, b \in D$. Since, $a.b \in D$, we have $(a.b)^2 = e$. Thus

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

Hence

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

. Thus (1) and (2) implies $a.b = b.a$.

(b) Assume that $(D, .)$ is a group such that $(ab)^2 = a^2b^2$ for every $a, b \in D$. Prove that D is an abelian group.

Proof. $(a.b)^2 = a.b.a.b = a.a.b.b$. Hence $a^{-1}.(a.b.a.b).b^{-1} = a^{-1}.(a.a.b.b).b^{-1}$. Thus $b.a = a.b$.

QUESTION 3. a) Let (D, .) be a group and $a \in D$ such that $|a| = n < \infty$. Prove that $|b.a.b^{-1}| = |a| = n$ for every $b \in D$.

Proof. Let $m = |b.a.b^{-1}|$. Note that $(b.a.b^{-1})^n = b.a.b^{-1}.b.a.b^{-1}. \cdots .b.a.b^{-1}$ (n times) = $b.a^n.b^{-1} = b.e.b^{-1} = e$. Hence $m \mid n$. Since $|b.a.b^{-1}| = m$, we have $(b.a.b^{-1})^m = b.a.b^{-1}b.a.b^{-1}. \cdots .b.a.b^{-1} = b.a^m.b^{-1} = e$. ($m$ times). Thus $a^m = b.b^{-1} = e$. Thus $n \mid m$. Since $m \mid n$ and $n \mid m$, we conclude that $n = m$.

b) Let (D, .) be a group and H be a subgroup of D such that $|H| = m < \infty$.

i) Prove that $|a.H.a^{-1}| = |H| = m$ for every $a \in D$. [Hint : Let $a \in D$ and construct a function $f : H \rightarrow a.H.a^{-1}$ such that $f(b) = a.b.a^{-1}$. Show that f is 1-1 and onto , (easy)]

Proof. Let $a \in H$. Define $f : H \rightarrow a.H.a^{-1}$ such that $f(h) = a.h.a^{-1}$. We show f is ONTO. Let $d \in a.H.a^{-1}$. Then $d = a.h_1.a^{-1}$ for some $h_1 \in H$. Thus $f(h_1) = a.h_1.a^{-1}$. We show f is one-to-one. Assume $f(h_1) = f(h_2)$. Thus $a.h_1.a^{-1} = a.h_2.a^{-1}$. Hence $h_1 = h_2$.

ii) Let $a \in (D, .)$. Prove that $a.H.a^{-1}$ is a subgroup of D [Hint: Let $x, y \in a.H.a^{-1}$, show that $x.y \in a.H.a^{-1}$].

Proof. Let $x, y \in a.H.a^{-1}$. Since $a.H.a^{-1}$ is a finite set, by a class-notes result, we show $x.y \in a.H.a^{-1}$. Thus $x = a.h_1.a^{-1}$ and $y = a.h_2.a^{-1}$. Hence $x.y = a.h_1.a^{-1}.a.h_2.a^{-1} = a.h_1.h_2.a^{-1} \in a.H.a^{-1}$. Thus $a.H.a^{-1}$ is a subgroup of D.

iii) Assume H is unique (i.e., H is the only subgroup of D with m elements). Prove that H is a normal subgroup of D (nice! and easy, make use of (i) and (ii))

Proof. Let $a \in D$. Hence by (i) and (ii), $a.H.a^{-1} = H$. Thus $a.H = H.a$. Since $a.H = H.a$ for every $a \in D$, we conclude that H is a normal subgroup of D.

QUESTION 4. Let $f = (1\ 2\ 6)\ o\ (6\ 3\ 2\ 5)\ o\ (1\ 6\ 2\ 4\ 5) \in S_6$.

a) Find |f|.

Solution We must write f as disjoint cycles. Hence $f = (1\ 3\ 6\ 5\ 2\ 4)$. Thus $|f| = 6$.

b) Find f^{-1}

$f^{-1} = (4\ 2\ 5\ 6\ 3\ 1)$

c) Is $f \in A_n$? explain.

Since f is a 6-cycle, clearly f is an odd permutation (function). Thus $f \notin A_n$.

e) Let $h \in A_9$ such that $|h|$ is maximum. What is $|h|$? (think, not difficult) (i.e., if $|h| = m$, then $|b| <= m$ for every $b \in A_9$)

IDEA: Imagine that we Write h as disjoint cycles, by try and error and staring , we conclude that h is a composition of a 5-cycle with a 3-cycle. Hence $|h| = 15$.

QUESTION 5 (Nice, good exercise, see class notes). . Let $f : (Z_{12}, +) \to (Z_9, +)$ be a non-trivial group homomorphism.

a) Find Range(f) and Ker(f).

By class notes, |Range(f)| must be a factor of 9 and 12 (i.e., |Range(f)| must be a factor of |co-domain| and |domain|). Thus $|Range(f)| = 3$.

Since $(Z_9, +)$ is cyclic, Z_9 has exactly one subgroup with 3 elements. Since $|3|$ is 3, we have $Range(f) =< 3 >= \{0, 3, 6\}$.

By class-notes (First-Isomorphism Theorem), we have $Z_{12}/Ker(f) \equiv Range(f)$. Hence $|Z_{12}|/|Ker(f)| = |Range(f)|$ Thus $|Ker(f)| = 4$.

Since $(Z_{12}, +)$ is cyclic, it has a unique subgroup K of Z_{12} with 4 elements. To find k choose an element in Z_{12} of order 4 (for example $1^3 = 3$) Hence $K = \{0, 3, 6, 9\}$.

b) What are all possibilities of $f(1)$? For each possibility of $f(1)$, find $f(a)$ for every $a \in Z_{12}$. [Hint: Note if we know f(1), then we know $f(a)$ for every $a \in Z_{12}$. Since $Z_{12} =< 1 >$ and f is a group homomorphism, $f(a) = f(1^a) = (f(1))^a$. By the first isomorphism theorem , we know $Z_{12}/Ker(f)$ is group-isomorphic to Range(f) (see class notes: $K(b + Ker(f)) = f(b)$. Hence if $i + Ker(f)$ is a left coset of Ker(f). Then $K(i + Ker(f)) = f(i)$. Observe that each element in a left coset can be chosen as a representative, Thus for every $b \in i + Ker(f)$ (we know b + Ker(f) = i + Ker(f)), we have $K(i + Ker(f)) = K(b + Ker(f)) = f(i) = f(b)$ (i,e., if W is a left coset of Ker(f), then all elements of W must map to the same number in Z_9). Now since 1 is a generator of Z_{12}, $f(1)$ must be a generator of Range(f) (note that Range(f) is a cyclic subgroup of Z_9).

Now since $Z_{12} =< 1 >$, we conclude that $Range(f) =< f(1) >$. Hence $f(1) = 3$ or $f(1) = 6$ since $< 3 >=< 6 >= Range(f)$. So assume $f(1) = 3 = 1^3$.(if you choose, then you can find f(a) for every $a \in Z_{12}$ Note $f(a) = f(1^a) = (f(1))^a = (1^3)^a = 3.a(mod\, 9$)

But, here is a different approach :

Now recall from class notes the map $K : Z_{12}/Ker(f) \to Range(f) = \{0, 3, 6\}$, where $K(a + Ker(f)) = f(a)$. (Note that this map is well-defined, K is group-homomorphism, 1-1, and onto). For assume that $h \in a + Ker(f)$. We know (class notes) that $h + Ker(f) = a + Ker(f)$. Hence $K(a + Ker(f)) = K(h + Ker(f)) = f(h) = f(a)$). Since K is 1-1, each left coset of $Z_{12}/Ker(f)$ maps to one and only one number in RANGE(F).

Now we find the left cosets of Ker(f) (note that Ker(f) has exactly 3 left cosets)

(1) Ker(f), and hence $f(a) = 0$ for every a in Ker(f).

(2) $1 + Ker(f) = \{1, 4, 7, 10\}$. Thus $f(a) = f(1) = 3$ for every $a \in 1 + Ker(f)$.

(3) $2 + Ker(f) = \{2, 5, 8, 11\}$. Thus $f(a) = f(2) = f(1^2) = (f(1))^2 = (1^3)^2 = 6$ for every a in 2 + Ker(f).

Similarly, assume $f(1) = 6 = 1^6$....YOU DO IT.

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

WARNING: Title too long for running head.
PLEASE supply a shorter form with \headlinetitle

4.5 HW5-Solution

Name————————————, **ID** ——————

Solution-MTH 320, Exam II, Fall 2020

Ayman Badawi

——————
47

QUESTION 1. (6 points) Let $(D, .)$ be a group with 39 elements. Assume that D has a normal subgroup with 3 elements. Prove that D is cyclic.

Proof.(very similar to a HW-problem) Since $39 = 3.13$, we know by HW and by class-result that D has an element a of order 13. Let $H =< a >$. Hence $|H| = 13$. Since $[H : D] = 3$ is the smallest prime factor of $|D|$, we conclude that H is a normal subgroup of D. Let F be the given normal subgroup of D with 3 elements. It is clear that $H \cap F = \{e\}$. Thus $D = H \cdot F$. Hence $D \approx H \oplus F$ by a class result. It is clear that $F \approx Z_{13}$ and $F \approx Z_3$. Hence $D \approx Z_{13} \oplus Z_3$. Since Z_{13}, Z_3 are cyclic groups and $gcd(13, 3) = 1$, we conclude that $D \approx Z_{13} \oplus Z_3 \approx Z_{39}$ is a cyclic group.

QUESTION 2. Let $(D, .)$ be an abelian group with 245 = $5 \cdot 7^2$ elements. Assume that D is non-cyclic.

i) **(6 points)** Find $m_1, .., m_k$ such that $D \approx (Z_{m_1}, +) \oplus \cdots \oplus (Z_{m_k}, +)$. SHOW THE WORK.

(similar to a HW-problem) Since D is abelian, D has a normal subgroup, H, with $7^2 = 49$ elements and it has a normal subgroup F with 5 elements. Since $gcd(5, 49) = 1$, we conclude that $H \cap F = \{e\}$. Thus $D = H \cdot F$. Hence, we know that $D \approx H \oplus F$. It is clear that $F \approx Z_5$. Since $|H| = 7^2$, By a HW-problem we know that either $F \approx Z_{49}$ OR $H \approx Z_7 \oplus Z_7$. Hence either $D \approx H \oplus F \approx Z_{49} \oplus Z_5$ OR $D \approx H \oplus F \approx Z_7 \oplus Z_7 \oplus Z_5$. Assume that $D \approx Z_{49} \oplus Z_5$. Since $gcd(49, 5) = 1$, we conclude that $D \approx Z_{49} \oplus Z_5 \approx Z_{245}$ is cyclic, a contradiction (since it is given that D is non-cyclic). Thus $D \approx Z_7 \oplus Z_7 \oplus Z_5 \approx Z_7 \oplus Z_{35}$. Thus you may choose either ($m_1 = m_2 = 7$ and $m_3 = 5$) OR ($m_1 = 7$ and $m_2 = 35$).

ii) **(3 points)** How many elements of order 35 does D have?

From (i), we know that $D \approx Z_7 \oplus Z_{35}$. Let $(a, b) \in Z_7 \oplus Z_{35}$ such that $|(a, b)| = LCM[|a|, |b|] = 35$. Since $gcd(35, 7) = 7$, we conclude that $|(a, b)| = 35$ if and only $|b| = 35$ OR $|a| = 7$ and $|b| = 5$. Hence a can be any element in Z_7 and we know that Z_{35} has exactly $\phi(35) = 24$ elements of order 35 OR a can be any nonzero element of Z_7 and $b \in Z_{35}$ such that $|b| = 5$. We know that Z_{35} has exactly $\phi(5) = 4$ elements of order 5. Thus D has exactly $7 \cdot 24 + 6 \cdot 4 = 168 + 24 = 192$ elements of order 35.

iii) **(3 points)** How many elements of order 7 does D have? **For this part, maybe it is easier to use the other version of D, i.e., $D \approx Z_7 \oplus Z_7 \oplus Z_5$. Let $(a, b, c) \in Z_7 \oplus Z_7 \oplus Z_5$ such that $|(a, b, c)| = LCM[|a|, |b|, |c|] = 7$. Hence either ($a$ is a nonzero element of Z_7 and $b \in Z_7$ and $c = 0$) OR ($a = 0$ and b is a nonzero element of Z_7 and $c = 0$). Thus D has exactly $6 \cdot 7 \cdot 1$ + $1 \cdot 6 \cdot 1 = 48$ elements of order 7.**

QUESTION 3. (5 points) Let $(D, .)$ be a non-cyclic-group with 2020 elements. Prove that there are finitely many groups, say $D_1, ..., D_m$, each with 2020 elements such that $D \not\approx D_i$ (i.e., D is not group-isomorphic to D_i) for every i, where $1 \leq i \leq m$.

The idea is in Caley's Theorem: We know that every group with 2020 elements is isomorphic to a subgroup of S_{2020} by Caley's Theorem. Since S_{2020} is a FINITE group, S_{2020} has FINITELY many subgroups of order 2020. In particular, S_{2020} has FINITELY many NON-ISOMORPHIC subgroups of order 2020, say $M_1, ..., M_k$, where $k < \infty$. Thus each group of order 2020 is isomorphic to one and only one M_i for some i, $1 \leq i \leq k$. We may assume that $D \approx M_1$. Then $D \not\approx M_i$ for every i, $2 \leq i \leq k$. Thus if L a group with 2020 elements and $L \not\approx D$, then $L \approx M_i$ for some i, $2 \leq i \leq k$. Hence D is not isomorphic to exactly $k - 1$ groups of order 2020.

QUESTION 4. Let $f : (Z_6, +) \oplus (Z_6, +) \to (Z_6, +)$ such that $f((a, b)) = 2 \cdot (a + b^{-1})$ (note that b^{-1} means the inverse of b under addition mod 6, and in $2 \cdot (a + b^{-1})$, the "+" means addition mod 6 and "$\cdot$" means multiplication mod 6 .

i) **(3 points)** Show that f is a group-homomorphism.

Trivial: Let $(a, b), (c, d) \in (Z_6, +) \oplus (Z_6, +)$. We show $f((a, b) \oplus (c, d)) = f(a, b) + f(c, d)$. (note that in general $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, here "$\cdot$" is + mod 6, and Z_6 is abelian. Hence $(a + b)^{-1} = b^{-1} + a^{-1} = a^{-1} + b^{-1}$)

Now $f((a, b) \oplus (c, d)) = f(a + c, b + d) = 2(a + c + (b + d)^{-1}) = 2a + 2c + 2b^{-1} + 2d^{-1} = 2(a + b^{-1}) + 2(c + d^{-1}) = f(a, b) + f(c, d)$.

ii) **(3 points)** Find the range of f.

We know $|Range(f)|$ is a factor of 6. Since Z_6 is cyclic, we know that Z_6 has unique subgroup of order 2 and it has unique subgroup of order 3. It is clear that $1 \notin Range(f)$. Hence $Range(f) \neq Z_6$. Since $f(1, 0) = 2 \in Range(f)$, we conclude that $Range(f) = \{0, 2, 4\}$ is the unique subgroup of Z_6 with 3 elements.

iii)**(5 points)** Find $ker(f)$.

We know that $(Z_6 \oplus Z_6)/Ker(f) \approx Range(f)$. Hence 36/|Ker(f) = 3. Thus $|Ker(f)| = 12$. So we need to find 12 elements in $Z_6 \oplus Z_6$, say (a, b), such that $2(a + b^{-1}) = 0$ in Z_6. So if we set $a + b^{-1} = 0$, we get that $b = a$. Thus $(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5) \in Ker(f)$, but we still need to find 6 more elements. By staring at $2(a + b^{-1}) = 0$ in Z_6, we see that if $a + b^{-1} = 3$ in Z_6, then $2(a + b^{-1}) = 0$ in Z_6. By Setting $a + b^{-1} = 3$ and solving for b, we get $b^{-1} = 3 + a^{-1}$. Hence $b = (3 + a^{-1})^{-1} = 3^{-1} + a = 3 + a$ in Z_6. Thus $(0, 3), (1, 4), (2, 5), (3, 0), (4, 1), (5, 2) \in Ker(f)$.

Hence $Ker(f) = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (0, 3), (1, 4), (2, 5), (3, 0), (4, 1), (5, 2)\}$

QUESTION 5. Let $D = (Aut(Z_{20}), o)$. [Recall: $Aut(Z_{20})$ is the group of all group-isomorphism from $(Z_{20}, +)$ onto $(Z_{20}, +)$ under composition.]

i) **(3 points)** Is D cyclic? explain?

One lecture (1 hours and 15 minutes) was only on $Aut(Z_n)$. We know $Aut(Z_{20}) \approx U(20)$. Since $20 = 2^2 \cdot 5$, we conclude that $U(20)$ is not cyclic by class-result. Thus $(Aut(Z_{20}), o)$ is not cyclic.

ii) **(4 points)** Construct a non-cyclic subgroup of D, say (H, o), of D such that $|H| = 4$.

See my lecture on $Aut(Z_n)$. We constructed a group-isomorphism $K : ((U(20), .)$ (note "." is multiplication module 20) $\rightarrow (Aut(Z_{20}), o)$ such that $k(a) = f_a$ for every $a \in U(20)$, where $f_a \in Aut(Z_{20})$ and $f_a : (Z_{20}, +) \rightarrow (Z_{20}, +)$ such that $f_a(b) = ab$ in Z_{20} for every $b \in Z_{20}$. Since $U(n)$ is abelian, we conclude that $Aut(Z_n)$ is abelian. Hence one way to construct a noncyclic-subgroup of $Aut(Z_{20})$ with 4 elements: Construct two subgroups H, F of $Aut(Z_{20})$ such that $|H| = |F| = 2$. Then $L = H\ o\ K$ will be a noncyclic subgroup with 4 elements since $H \cap F = \{e\}$.

Hence choose $a = 9 \in U(20)$. Then $|a| = 2$. Since $K(9) = f_9 : Z_{20} \rightarrow Z_{20}$, where $f_9(b) = 9b$ in Z_{20} for every $b \in Z_{20}$, we conclude $|f_9| = 2$. Note that the identity, e, in $Aut(Z_{20})$ is the identity map $I : Z_{20} \rightarrow Z_{20}$ such that $I(b) = b$ for every $b \in Z_{20}$. Thus $H = \{I, f_9\}$ is a subgroup of $Aut(Z_{20})$ with 2 elements.

Choose $a = 11 \in U(20)$. Then $|11| = 2$. Thus (similar to the case above), $K = \{I, f_{11}\}$ is a subgroup of $Aut(Z_{20})$ with 2 elements. Thus $H\ o\ K = \{I, f_9, f_{11}, f_{19}\}$ is a non-cyclic subgroup of $Aut(Z_{20})$ with 4 elements (note that $(f_9\ o\ f_{11})(b) = f_9(11b) = 99b = 19b$ for every $b \in Z_{20}$.

QUESTION 6. Let $n = 16 \cdot 9$ and $D = U(n)$.

(i)**(4 points)** Find $m_1, .., m_k$ such that $D \approx (Z_{m_1}, +) \oplus \cdots \oplus (Z_{m_k}, +)$. SHOW THE WORK.

By the last lecture (before the exam), we know that $U(2^4 \cdot 3^2) \approx U(2^4) \oplus U(3^2)$. Also we know that $U(2^m)$ $(m \geq 3) \approx Z_2 \oplus Z_{2^{(m-2)}}$ and $U(p^n)$ (p is prime, $p \neq 2$ and $n \geq 1$) $\approx Z_{p-1} \oplus Z_{p^{(n-1)}} \approx Z_{p^n - p^{(n-1)}}$.

Hence $U(2^4 \cdot 3^2) \approx U(2^4) \oplus U(3^2) \approx Z_2 \oplus Z_4 \oplus Z_2 \oplus Z_3 \approx Z_2 \oplus Z_2 \oplus Z_{12}$.

So you may choose either ($m_1 = 2, m_2 = 4, m_3 = 2$ and $m_4 = 3$) OR ($m_1 = m_2 = 2$ and $m_3 = 12$)

(ii) **(2 points)** Let $a \in D$ such that $|a|$ is maximum. Find $|a|$.

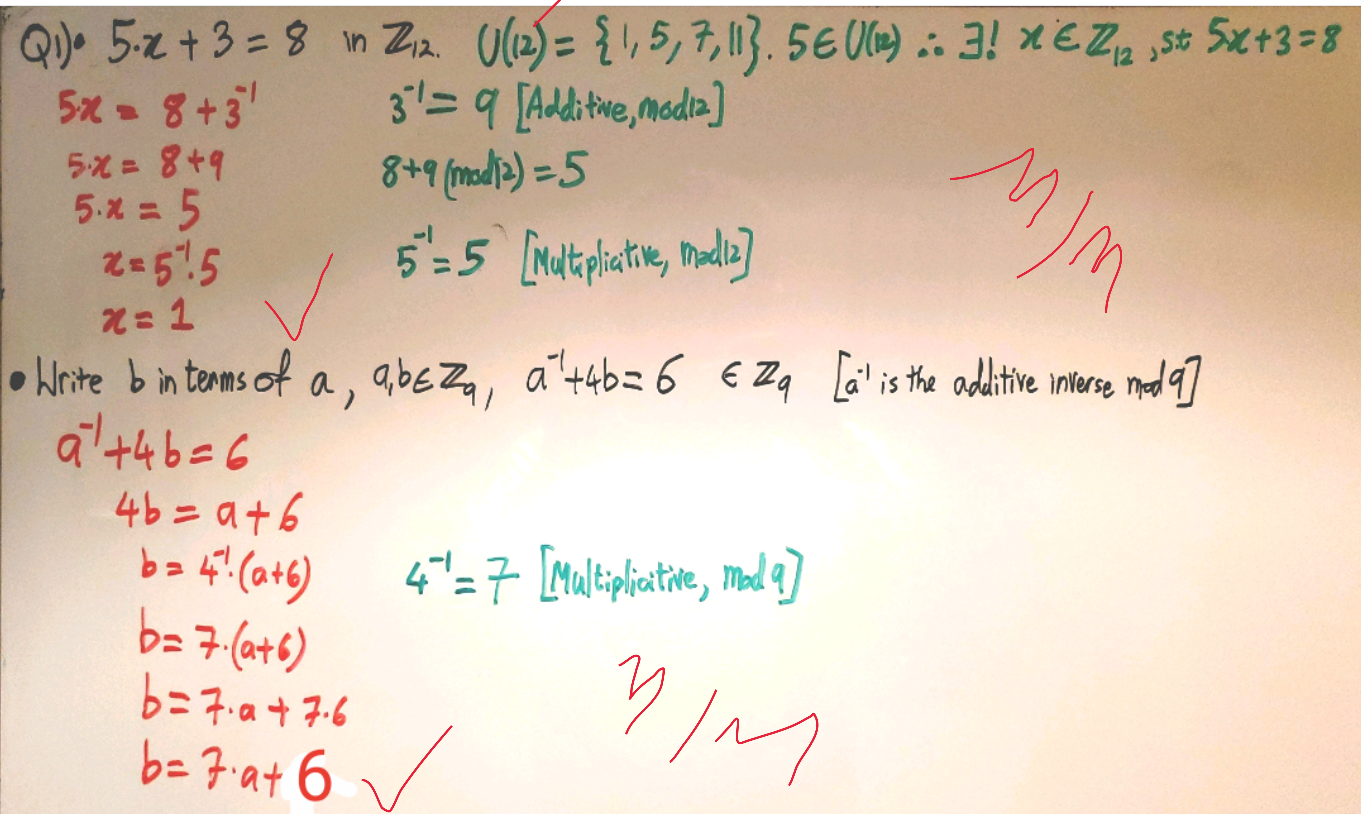
Let $(b, c, d) \in Z_2 \oplus Z_2 \oplus Z_{12}$ such that $|(b, c, d)| = LCM[|b|, |c|, |d|] = k$ such that k is maximum. By staring $k = 12$. Since $U(2^4 \cdot 3^2) \approx Z_2 \oplus Z_2 \oplus Z_{12}$. we conclude that $|a| = k = 12$.

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

4.6 HW6-Solution

24/24



Q1)• $5 \cdot x + 3 = 8$ in $\mathbb{Z}_{12}$. $U(12) = \{1, 5, 7, 11\}$. $5 \in U(12) \therefore \exists!\, x \in \mathbb{Z}_{12}$, s.t $5x + 3 = 8$

$5 \cdot x = 8 + 3^{-1}$ $\quad$ $3^{-1} = 9$ [Additive, mod12]

$5 \cdot x = 8 + 9$ $\quad$ $8 + 9 \pmod{12} = 5$

$5 \cdot x = 5$

$x = 5^{-1} \cdot 5$ $\quad$ $5^{-1} = 5$ [Multipliative, mod12]

$x = 1$ ✓

3/3

• Write b in terms of a, $a, b \in \mathbb{Z}_9$, $a^{-1} + 4b = 6 \in \mathbb{Z}_9$ [a^{-1} is the additive inverse mod 9]

$a^{-1} + 4b = 6$

$4b = a + 6$

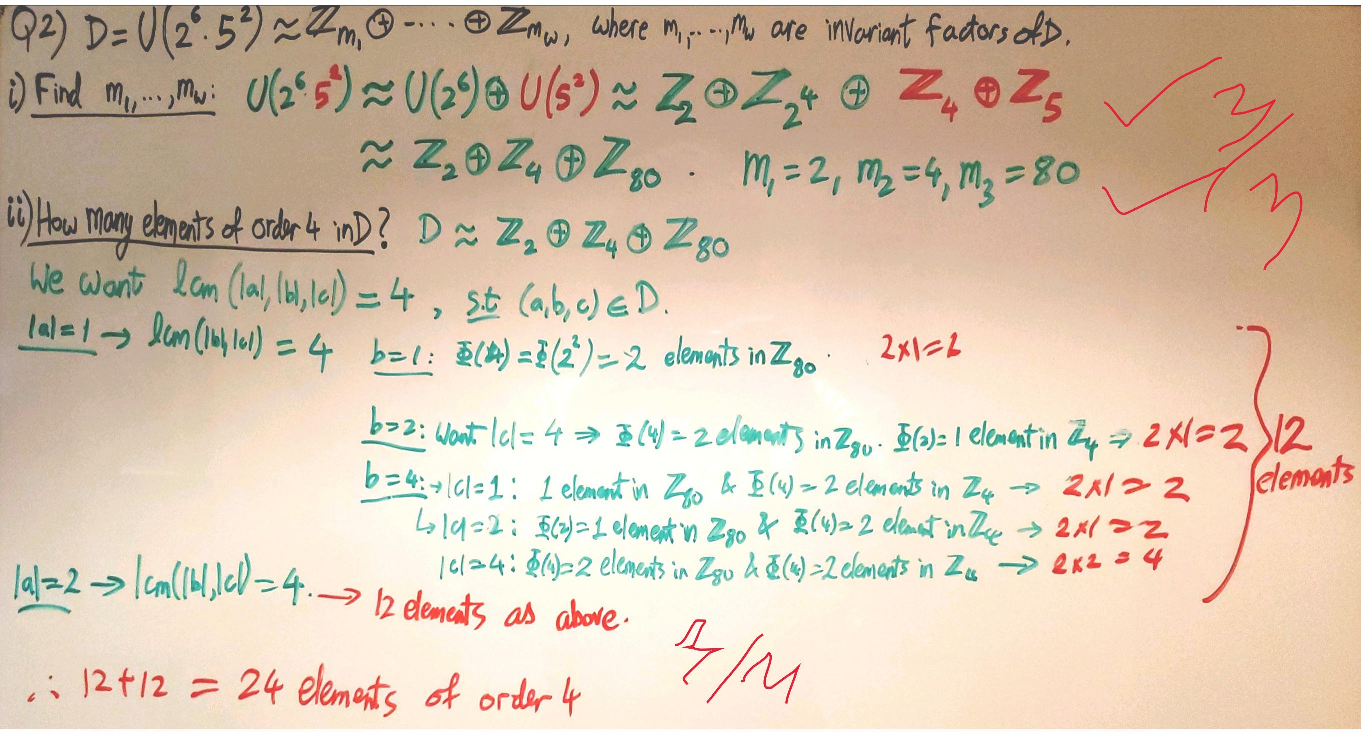
$b = 4^{-1} \cdot (a + 6)$ $\quad$ $4^{-1} = 7$ [Multiplicative, mod 9]

$b = 7 \cdot (a + 6)$

$b = 7 \cdot a + 7 \cdot 6$

$b = 7 \cdot a + 6$ ✓

3/3



Q2) $D = U(2^6 \cdot 5^2) \approx \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_w}$, where $m_1, \ldots, m_w$ are invariant factors of D.

i) Find $m_1, \ldots, m_w$: $U(2^6 5^2) \approx U(2^6) \oplus U(5^2) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^4} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$ ✓ 3/3

$\approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{80}$. $m_1 = 2$, $m_2 = 4$, $m_3 = 80$ ✓ 3/3

ii) How many elements of order 4 in D? $D \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{80}$

We want $lcm(|a|, |b|, |c|) = 4$, s.t $(a, b, c) \in D$.

$|a| = 1 \rightarrow lcm(|b|, |c|) = 4$ $\quad$ $b=1$: $\Phi(4) = \Phi(2^2) = 2$ elements in $\mathbb{Z}_{80}$. $\quad 2 \times 1 = 2$

$b=2$: Want $|c| = 4 \Rightarrow \Phi(4) = 2$ elements in $\mathbb{Z}_{80}$. $\Phi(2) = 1$ element in $\mathbb{Z}_4 \Rightarrow 2 \times 1 = 2$

$b=4$: $\rightarrow |c| = 1$: 1 element in $\mathbb{Z}_{80}$ & $\Phi(4) = 2$ elements in $\mathbb{Z}_4 \rightarrow 2 \times 1 = 2$

$\hookrightarrow |c| = 2$: $\Phi(2) = 1$ element in $\mathbb{Z}_{80}$ & $\Phi(4) = 2$ element in $\mathbb{Z}_4 \rightarrow 2 \times 1 = 2$

$|c| = 4$: $\Phi(4) = 2$ elements in $\mathbb{Z}_{80}$ & $\Phi(4) = 2$ elements in $\mathbb{Z}_4 \rightarrow 2 \times 2 = 4$

} 12 elements

$|a| = 2 \rightarrow lcm(|b|, |c|) = 4. \rightarrow$ 12 elements as above.

$\therefore 12 + 12 = 24$ elements of order 4 $\quad$ 4/4

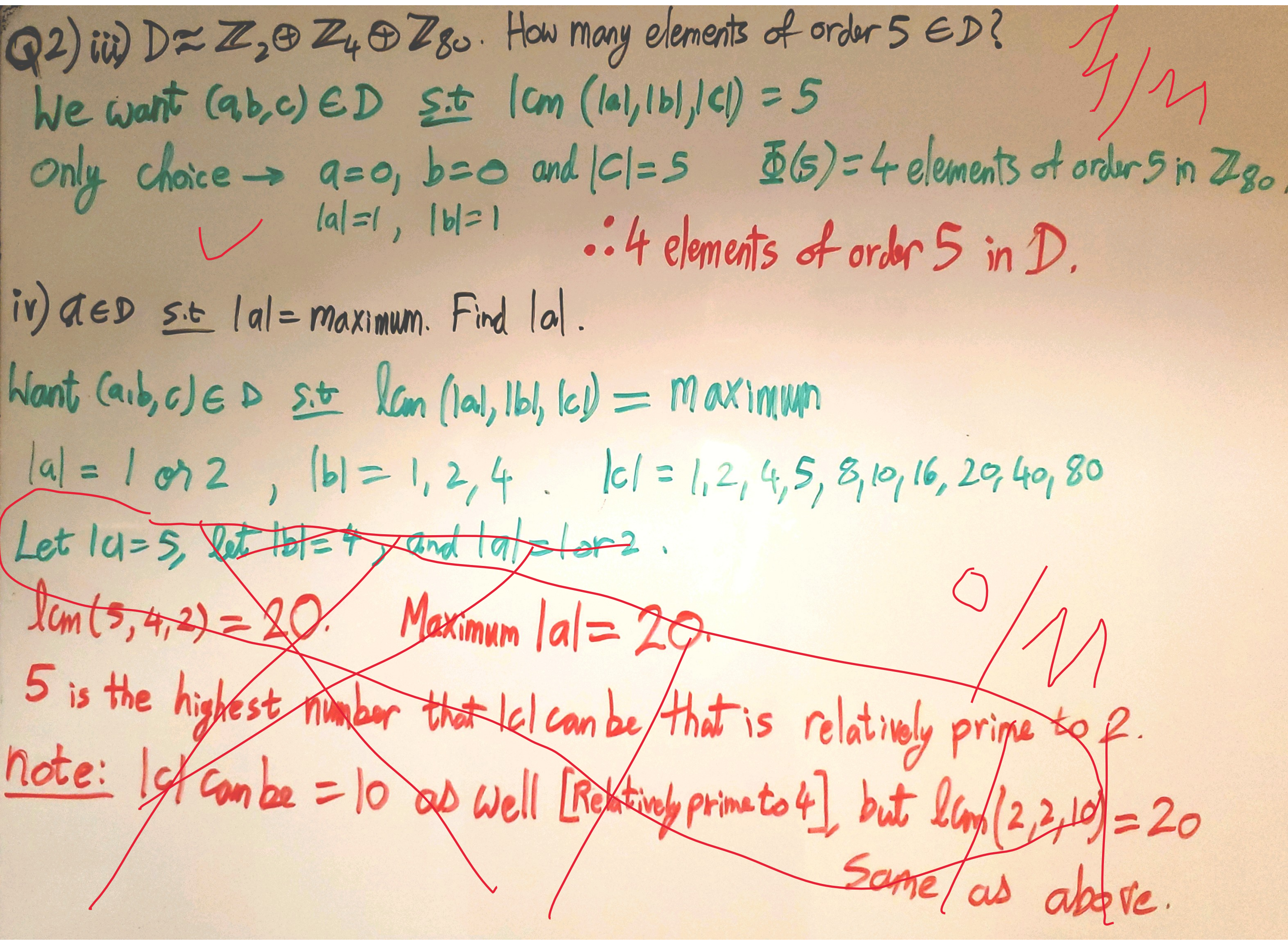
Here is one way to do it (algorithm)

D = Z_2 (oplus) Z_4 (oplus) Z_{80}

|(a, b, c)| = LCM[|a|, |b|, |c|] = 4.

LCM[1, 4, 1] = 4. There are exactly 1 X phi(4)X 1 = 2 of these elements
LCM[1, 4, 2] = 4 . There are exactly 1 X phi(4)X phi(2) = 2 of these elements
LCM[1, 4, 4] = 4 . There are exactly 1 X phi(4)X phi(4) = 4 of these elements
LCM[1, 1, 4] = 4. There are exactly 1 X 1X phi(4) = 2 of these elements
LCM[1, 2, 4] = 4. There are exactly 1 X phi(2)X phi(4) = 2 of these elements
LCM[2, 1, 4] = 4. There are exactly phi(2)X1Xphi(4) = 2 of these elements
LCM[2, 2, 4] = 4. There are exactly phi(2)Xphi(2)Xphi(4) = 2 of these elements
LCM[2, 4, 1] = 4. There are exactly phi(2)Xphi(4)X1 = 2 of these elements
LCM[2, 4, 2] = 4. There are exactly phi(2)Xphi(4)Xphi(2) = 2 of these elements
LCM[2, 4, 4] = 4 There are exactly phi(2)X phi(4)X phi(4) = 4 of these elements

Total of elements of order 4 is 24 elements



Q2) iii) $D \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{80}$. How many elements of order 5 $\in D$? 4/4

We want $(a,b,c) \in D$ s.t $\text{lcm}(|a|,|b|,|c|) = 5$

only choice → $a=0,\ b=0$ and $|c|=5$ $\Phi(5) = 4$ elements of order 5 in $\mathbb{Z}_{80}$.

$|a|=1,\ |b|=1$ ✓

∴ 4 elements of order 5 in D.

iv) $a \in D$ s.t $|a| = $ maximum. Find $|a|$.

Want $(a,b,c) \in D$ s.t $\text{lcm}(|a|,|b|,|c|) = $ maximum

$|a| = 1$ or 2 , $|b| = 1,2,4$. $|c| = 1,2,4,5,8,10,16,20,40,80$

Let $|c|=5$, ~~let $|b|=4$, and $|a|=1$ or 2~~ .

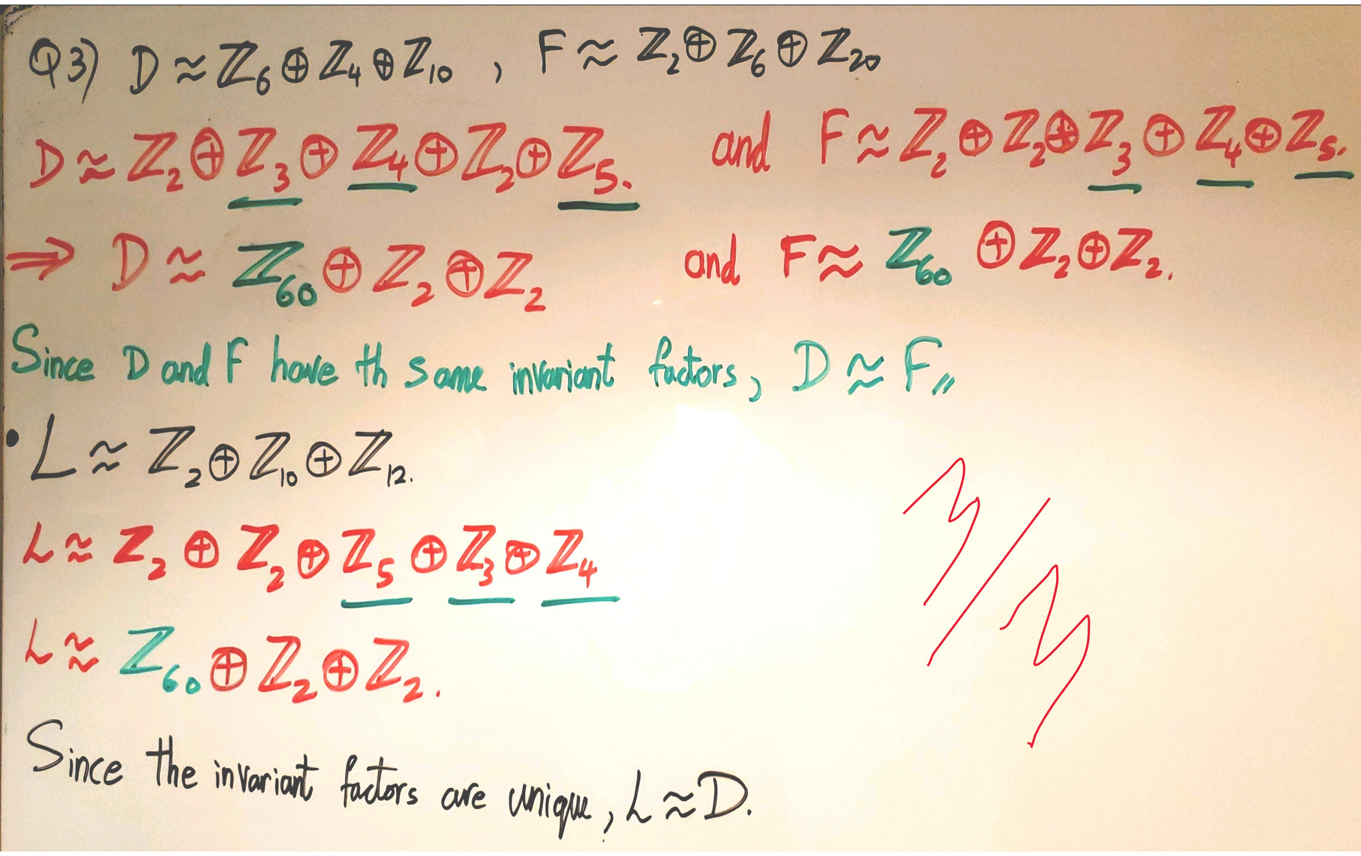
$\text{lcm}(5,4,2) = 20$. Maximum $|a| = 20$. 0/4

5 is the highest number that $|c|$ can be that is relatively prime to 2.

note: $|c|$ can be $= 10$ as well [Relatively prime to 4], but $\text{lcm}(2,2,10) = 20$

Same as above.

Let x = (a, b, c) of maximum order. Since U(2^6.5^2) = Z_2 (olpus) Z_4 (oplus) Z_80 and 2 |4|80, we know Max Order of x = Max LCM[|a|, |b|, |c|] = 80



Q3) $D \approx \mathbb{Z}_6 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}$, $F \approx \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{20}$

$D \approx \mathbb{Z}_2 \oplus \underline{\mathbb{Z}_3} \oplus \underline{\mathbb{Z}_4} \oplus \mathbb{Z}_2 \oplus \underline{\mathbb{Z}_5}.$ and $F \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \underline{\mathbb{Z}_3} \oplus \underline{\mathbb{Z}_4} \oplus \underline{\mathbb{Z}_5}.$

$\Rightarrow D \approx \mathbb{Z}_{60} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $F \approx \mathbb{Z}_{60} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$

Since D and F have th same invariant factors, $D \approx F$ //

• $L \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{12}.$

$L \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \underline{\mathbb{Z}_5} \oplus \underline{\mathbb{Z}_3} \oplus \underline{\mathbb{Z}_4}$

$L \approx \mathbb{Z}_{60} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$

Since the invariant factors are unique, $L \approx D.$

3/3

Q4) i) Upto isomorphic, Classify all finite Abelian groups with $2^5 \cdot 5^3$ elements.

Partitions of 5	Partitions of 3	$\lvert H\rvert = 2^n$	$\lvert K\rvert = 5^k$
5 + 0	0 + 3	$\mathbb{Z}_{32}$	$\mathbb{Z}_{125}$
4 + 1	1 + 2	$\mathbb{Z}_{16} \oplus \mathbb{Z}_2$	$\mathbb{Z}_5 \oplus \mathbb{Z}_{25}$
3 + 2	1 + 1 + 1	$\mathbb{Z}_8 \oplus \mathbb{Z}_4$	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.
3 + 1 + 1		$\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	
2 + 2 + 1		$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$	
2 + 1 + 1 + 1		$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	
1 + 1 + 1 + 1 + 1		$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	

We have exactly $7 \times 3 = 21$ possible isomorphisms.

Any Abelian group order $2^5 \cdot 5^3$ $\approx$ group from col H $\oplus$ group from col K.

✓ 3/M

ii) Non-cyclic. has element order $200 = \boxed{2^3 5^2}$. Write in terms of invariant factors. ✓

- $\mathbb{Z}_{32} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \approx \mathbb{Z}_5 \oplus \mathbb{Z}_{800}$
- $\mathbb{Z}_{16} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{125} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2000}$
- $\mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{125} \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{1000}$
- $\mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \approx \mathbb{Z}_{20} \oplus \mathbb{Z}_{200}$
- $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{125} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{1000}$
- $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{200}$

3/M

4.7 Exam One Solution

ABSTRACT ALGEBRA - MIDTERM I

ROHAN MITRA
85023

Q1) i) $|H| = 33$. H is Abelian. Prove H is cyclic

~~Consider~~ ~~$a \neq$~~ $a \in H$, $a \neq e$.

$|a| = 3, 11,$ ~~33 only~~

The converse of Lagrange is true for Abelian groups.

$\therefore \exists$ atleast one subgroup of H, of order 3, ~~one~~ of order 11, and of order 33.

Let $F < H$ s.t $|F| = 3$ and $L < H$ s.t $|L| = 11$.

Both F and L are cyclic as their cardinality is prime.

This implies, $\exists f \in F$ and $\exists l \in L$ s.t $|f| = 3$ and $|l| = 11$.

Consider $f \cdot l$. Since $f, l \in H$, $f \cdot l \in A$. ~~$|f.l| = lcm(3,11)$~~.

$|f.l| = |f| \cdot |l|$ as $gcd(|f|, |l|) = 1$. $|fl| = 3 \times 11 = 33$.

$\therefore \exists h \in H$ s.t $|h| = 33$. $\therefore$ H is cyclic.

Q2(ii) Let F be the unique subgroup of D with 5 elements and M = D/H. Let a in D - (F U H). Then a*H not equal to H. Since |M| = 5, |a*H| = 5. Thus 5 must divide |a|. Since a is not in F and F is unique, |a| = 13 or 65. Since 5 does not divide 13, |a| is not 13. Thus |a| = 65. Hence D is cyclic.

Q2) i) $\langle 4 \rangle = \{4, 8, 12, 16, 0\} = H$, $H < D$ & $|H| = 5$

ii) Left cosets of H

We know number of all left cosets of H is |D|/|H| = 20/5 = 4.

So we have

H

1+ H = {5, 9, 13, 17, 1}, 2 + H = {6, 10, 14, 18, 2}, 3 + H = {7, 11, 15, 19, 3}

tinct left cosets of H:

H, 1+H, 2+H, 3+H.

Q3) $D = \mathbb{Z}_6 \oplus \mathbb{Z}_{35}$.

i) $\gcd(6,35) = 1$ $\therefore$ By HW, Since $\mathbb{Z}_6$ and $\mathbb{Z}_{35}$ are cyclic and $\gcd(6,35)=1$, $D = \mathbb{Z}_6 \oplus \mathbb{Z}_{35}$ is cyclic.

ii) $D = \langle (1,1) \rangle$

iii) if $a \in \mathbb{Z}_6$, $b \in \mathbb{Z}_{35}$, $(a,b) \in D$. $|(a,b)| = \operatorname{lcm}(|a|,|b|)$ want $= 15$.

$|a|$ must be 3 Since $\mathbb{Z}_6$ is cyclic, there are $\Phi(3)$ elements of order 3 $\Phi(3) = (3-1)\cdot 3^0 = 2$

$|b|$ must be 5. Since $\mathbb{Z}_{35}$ is cyclic, there are $\Phi(5)$ elements of order 5. $\Phi(5) = (5-1)5^0 = 4$.

There are 2 possible choices for a, and 4 possible choices for b. $\therefore$ $4 \times 2 = 8$ elements of order 15.

iv) $\{0,3\} \oplus \{5,10,15,20,25,30,0\}$. = {(0, 5), (0, 10), (0, 15), ..., (3, 5), (3, 10),... (3, 30)}

Q4) $A = (1\,2\,5) \circ (6\,5\,2) \circ (3\,8\,6\,10)$

i) $\underline{|A|}$: $A = (1\,2\,6\,10\,3\,8)$ all other elements map to themselves.

$|A| = 6$

ii) A is an odd permutation, as $|A|$ is even. $A = (1\,8) \circ (1\,3) \circ (1\,10) \circ (1\,6) \circ (1\,2)$

iii) ~~Aof~~ ~~Ao(10~~ $A \circ (10\,2\,3) = (1\,2\,6\,10\,3\,8) \circ (10\,2\,3)$

$= (1\,2\,8) \circ (6\,10)$

$|A \circ (10\,2\,3)| = \operatorname{lcm}(3,2) = 6$.

Q5) i) $|\text{Range}(f)| = 2$ or 4 $\text{Range}(f) = \{0,6\}$ or $\{0,3,6,9\}$

ii) $|\text{Ker}(f)| = \dfrac{|\mathbb{Z}_{16}|}{|\text{Range}(f)|}$ If $|\text{Range}(f)| = 2 \Rightarrow |\text{Ker}(f)| = \frac{16}{2} = 8 \Rightarrow \text{Ker}(f) = \{0,2,4,6,8,10,12,14\}$

If $|\text{Range}(f)| = 4 \Rightarrow |\text{Ker}(f)| = \frac{16}{4} = 4 \Rightarrow \text{Ker}(f) = \{0,4,8,12\}$.

iii) If $\text{Ker}(f) = \{0,4,8,12\}$

and $\text{Range}(f) =$ ~~$\{0,6\}$~~ $\{0,3,6,9\}$.

$f(0) = f(4) = f(8) = f(12) = 0$

Since $\mathbb{Z}_{16} = \langle 1 \rangle$, and f is a Group homomorphism,

$f(1^K) = (f(1))^K = b^K$.

$\therefore$ By HW, we know: $(a + \text{Ker}(f) \longrightarrow f(a))$

$f(1) = f(5) = f(9) = f(13) = b$

$f(1^2) = f(2) = f(6) = f(10) = f(14) = b^2$

$f(1^3) = f(3) = f(7) = f(11) = f(15) = b^3$.

continued..

Similarly, If $\text{Ker}(f) = \{0,2,4,6,8,10,12,14\}$,

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

$f(0) = f(2) = f(4) = f(6) = f(8) = f(10) = f(12) = f(14) = 0$

Since $\mathbb{Z}_{16} = \langle 1 \rangle$, & f is a G.H, $f(1^K) = (f(1))^K = b$.

$\therefore$ We Know $1^K + \text{Ker}(f) \longrightarrow [f(1)]^K$.

~~f(1)~~ Consider $1 + \text{Ker}(f)$, We have:

$f(1) = f(3) = f(5) = f(7) = f(9) = f(11) = f(13) = f(15) = b$.

4.8 Exam Two Solution

Name——————————, ID ——————

Solution-MTH 320, Exam II, Fall 2020

Ayman Badawi

47

QUESTION 1. (6 points) Let $(D, .)$ be a group with 39 elements. Assume that D has a normal subgroup with 3 elements. Prove that D is cyclic.

Proof.(very similar to a HW-problem) Since $39 = 3.13$, we know by HW and by class-result that D has an element a of order 13. Let $H =< a >$. Hence $|H| = 13$. Since $[H : D] = 3$ is the smallest prime factor of $|D|$, we conclude that H is a normal subgroup of D. Let F be the given normal subgroup of D with 3 elements. It is clear that $H \cap F = \{e\}$. Thus $D = H \cdot F$. Hence $D \approx H \oplus F$ by a class result. It is clear that $F \approx Z_{13}$ and $F \approx Z_3$. Hence $D \approx Z_{13} \oplus Z_3$. Since Z_{13}, Z_3 are cyclic groups and $gcd(13, 3) = 1$, we conclude that $D \approx Z_{13} \oplus Z_3 \approx Z_{39}$ is a cyclic group.

QUESTION 2. Let $(D, .)$ be an abelian group with 245 = $5 \cdot 7^2$ elements. Assume that D is non-cyclic.

i) **(6 points)** Find $m_1, .., m_k$ such that $D \approx (Z_{m_1}, +) \oplus \cdots \oplus (Z_{m_k}, +)$. SHOW THE WORK.

(similar to a HW-problem) Since D is abelian, D has a normal subgroup, H, with $7^2 = 49$ elements and it has a normal subgroup F with 5 elements. Since $gcd(5, 49) = 1$, we conclude that $H \cap F = \{e\}$. Thus $D = H \cdot F$. Hence, we know that $D \approx H \oplus F$. It is clear that $F \approx Z_5$. Since $|H| = 7^2$, By a HW-problem we know that either $F \approx Z_{49}$ OR $H \approx Z_7 \oplus Z_7$. Hence either $D \approx H \oplus F \approx Z_{49} \oplus Z_5$ OR $D \approx H \oplus F \approx Z_7 \oplus Z_7 \oplus Z_5$. Assume that $D \approx Z_{49} \oplus Z_5$. Since $gcd(49, 5) = 1$, we conclude that $D \approx Z_{49} \oplus Z_5 \approx Z_{245}$ is cyclic, a contradiction (since it is given that D is non-cyclic). Thus $D \approx Z_7 \oplus Z_7 \oplus Z_5 \approx Z_7 \oplus Z_{35}$. Thus you may choose either ($m_1 = m_2 = 7$ and $m_3 = 5$) OR ($m_1 = 7$ and $m_2 = 35$).

ii) **(3 points)** How many elements of order 35 does D have?

From (i), we know that $D \approx Z_7 \oplus Z_{35}$. Let $(a, b) \in Z_7 \oplus Z_{35}$ such that $|(a, b)| = LCM[|a|, |b|] = 35$. Since $gcd(35, 7) = 7$, we conclude that $|(a, b)| = 35$ if and only $|b| = 35$ OR $|a| = 7$ and $|b| = 5$. Hence a can be any element in Z_7 and we know that Z_{35} has exactly $\phi(35) = 24$ elements of order 35 OR a can be any nonzero element of Z_7 and $b \in Z_{35}$ such that $|b| = 5$. We know that Z_{35} has exactly $\phi(5) = 4$ elements of order 5. Thus D has exactly $7 \cdot 24 + 6 \cdot 4 = 168 + 24 = 192$ elements of order 35.

iii) **(3 points)** How many elements of order 7 does D have? **For this part, maybe it is easier to use the other version of D, i.e., $D \approx Z_7 \oplus Z_7 \oplus Z_5$. Let $(a, b, c) \in Z_7 \oplus Z_7 \oplus Z_5$ such that $|(a, b, c)| = LCM[|a|, |b|, |c|] = 7$. Hence either ($a$ is a nonzero element of Z_7 and $b \in Z_7$ and $c = 0$) OR ($a = 0$ and b is a nonzero element of Z_7 and $c = 0$). Thus D has exactly $6 \cdot 7 \cdot 1$ + $1 \cdot 6 \cdot 1 = 48$ elements of order 7.**

QUESTION 3. (5 points) Let $(D, .)$ be a non-cyclic-group with 2020 elements. Prove that there are finitely many groups, say $D_1, ..., D_m$, each with 2020 elements such that $D \not\approx D_i$ (i.e., D is not group-isomorphic to D_i) for every i, where $1 \leq i \leq m$.

The idea is in Caley's Theorem: We know that every group with 2020 elements is isomorphic to a subgroup of S_{2020} by Caley's Theorem. Since S_{2020} is a FINITE group, S_{2020} has FINITELY many subgroups of order 2020. In particular, S_{2020} has FINITELY many NON-ISOMORPHIC subgroups of order 2020, say $M_1, ..., M_k$, where $k < \infty$. Thus each group of order 2020 is isomorphic to one and only one M_i for some i, $1 \leq i \leq k$. We may assume that $D \approx M_1$. Then $D \not\approx M_i$ for every i, $2 \leq i \leq k$. Thus if L a group with 2020 elements and $L \not\approx D$, then $L \approx M_i$ for some i, $2 \leq i \leq k$. Hence D is not isomorphic to exactly $k - 1$ groups of order 2020.

QUESTION 4. Let $f : (Z_6, +) \oplus (Z_6, +) \to (Z_6, +)$ such that $f((a, b)) = 2 \cdot (a + b^{-1})$ (note that b^{-1} means the inverse of b under addition mod 6, and in $2 \cdot (a + b^{-1})$, the "+" means addition mod 6 and "$\cdot$" means multiplication mod 6 .

i) **(3 points)** Show that f is a group-homomorphism.

Trivial: Let $(a, b), (c, d) \in (Z_6, +) \oplus (Z_6, +)$. We show $f((a, b) \oplus (c, d)) = f(a, b) + f(c, d)$. (note that in general $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, here "$\cdot$" is + mod 6, and Z_6 is abelian. Hence $(a + b)^{-1} = b^{-1} + a^{-1} = a^{-1} + b^{-1}$)

Now $f((a, b) \oplus (c, d)) = f(a + c, b + d) = 2(a + c + (b + d)^{-1}) = 2a + 2c + 2b^{-1} + 2d^{-1} = 2(a + b^{-1}) + 2(c + d^{-1}) = f(a, b) + f(c, d)$.

ii) **(3 points)** Find the range of f.

We know $|Range(f)|$ is a factor of 6. Since Z_6 is cyclic, we know that Z_6 has unique subgroup of order 2 and it has unique subgroup of order 3. It is clear that $1 \notin Range(f)$. Hence $Range(f) \neq Z_6$. Since $f(1, 0) = 2 \in Range(f)$, we conclude that $Range(f) = \{0, 2, 4\}$ is the unique subgroup of Z_6 with 3 elements.

iii)**(5 points)** Find $ker(f)$.

We know that $(Z_6 \oplus Z_6)/Ker(f) \approx Range(f)$. Hence 36/|Ker(f) = 3. Thus $|Ker(f)| = 12$. So we need to find 12 elements in $Z_6 \oplus Z_6$, say (a, b), such that $2(a + b^{-1}) = 0$ in Z_6. So if we set $a + b^{-1} = 0$, we get that $b = a$. Thus $(0,0),(1,1),(2,2),(3,3),(4,4),(5,5) \in Ker(f)$, but we still need to find 6 more elements. By staring at $2(a + b^{-1}) = 0$ in Z_6, we see that if $a + b^{-1} = 3$ in Z_6, then $2(a + b^{-1}) = 0$ in Z_6. By Setting $a + b^{-1} = 3$ and solving for b, we get $b^{-1} = 3 + a^{-1}$. Hence $b = (3 + a^{-1})^{-1} = 3^{-1} + a = 3 + a$ in Z_6. Thus $(0,3),(1,4),(2,5),(3,0),(4,1),(5,2) \in Ker(f)$.

Hence $Ker(f) = \{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5),(0,3),(1,4),(2,5),(3,0),(4,1),(5,2)\}$

QUESTION 5. Let $D = (Aut(Z_{20}), o)$. [Recall: $Aut(Z_{20})$ is the group of all group-isomorphism from $(Z_{20}, +)$ onto $(Z_{20}, +)$ under composition.]

i) **(3 points)** Is D cyclic? explain?

One lecture (1 hours and 15 minutes) was only on $Aut(Z_n)$. We know $Aut(Z_{20}) \approx U(20)$. Since $20 = 2^2 \cdot 5$, we conclude that $U(20)$ is not cyclic by class-result. Thus $(Aut(Z_{20}), o)$ is not cyclic.

ii) **(4 points)** Construct a non-cyclic subgroup of D, say (H, o), of D such that $|H| = 4$.

See my lecture on $Aut(Z_n)$. We constructed a group-isomorphism $K : ((U(20), .)$ (note "." is multiplication module 20) $\rightarrow (Aut(Z_{20}), o)$ such that $k(a) = f_a$ for every $a \in U(20)$, where $f_a \in Aut(Z_{20})$ and $f_a : (Z_{20}, +) \rightarrow (Z_{20}, +)$ such that $f_a(b) = ab$ in Z_{20} for every $b \in Z_{20}$. Since $U(n)$ is abelian, we conclude that $Aut(Z_n)$ is abelian. Hence one way to construct a noncyclic-subgroup of $Aut(Z_{20})$ with 4 elements: Construct two subgroups H, F of $Aut(Z_{20})$ such that $|H| = |F| = 2$. Then $L = H\ o\ K$ will be a noncyclic subgroup with 4 elements since $H \cap F = \{e\}$.

Hence choose $a = 9 \in U(20)$. Then $|a| = 2$. Since $K(9) = f_9 : Z_{20} \rightarrow Z_{20}$, where $f_9(b) = 9b$ in Z_{20} for every $b \in Z_{20}$, we conclude $|f_9| = 2$. Note that the identity, e, in $Aut(Z_{20})$ is the identity map $I : Z_{20} \rightarrow Z_{20}$ such that $I(b) = b$ for every $b \in Z_{20}$. Thus $H = \{I, f_9\}$ is a subgroup of $Aut(Z_{20})$ with 2 elements.

Choose $a = 11 \in U(20)$. Then $|11| = 2$. Thus (similar to the case above), $K = \{I, f_{11}\}$ is a subgroup of $Aut(Z_{20})$ with 2 elements. Thus $H\ o\ K = \{I, f_9, f_{11}, f_{19}\}$ is a non-cyclic subgroup of $Aut(Z_{20})$ with 4 elements (note that $(f_9\ o\ f_{11})(b) = f_9(11b) = 99b = 19b$ for every $b \in Z_{20}$.

QUESTION 6. Let $n = 16 \cdot 9$ and $D = U(n)$.

(i)**(4 points)** Find $m_1, .., m_k$ such that $D \approx (Z_{m_1}, +) \oplus \cdots \oplus (Z_{m_k}, +)$. SHOW THE WORK.

By the last lecture (before the exam), we know that $U(2^4 \cdot 3^2) \approx U(2^4) \oplus U(3^2)$. Also we know that $U(2^m)$ ($m \geq 3$) $\approx Z_2 \oplus Z_{2^{(m-2)}}$ and $U(p^n)$ (p is prime, $p \neq 2$ and $n \geq 1$) $\approx Z_{p-1} \oplus Z_{p^{(n-1)}} \approx Z_{p^n - p^{(n-1)}}$.

Hence $U(2^4 \cdot 3^2) \approx U(2^4) \oplus U(3^2) \approx Z_2 \oplus Z_4 \oplus Z_2 \oplus Z_3 \approx Z_2 \oplus Z_2 \oplus Z_{12}$.

So you may choose either ($m_1 = 2, m_2 = 4, m_3 = 2$ and $m_4 = 3$) OR ($m_1 = m_2 = 2$ and $m_3 = 12$)

(ii) **(2 points)** Let $a \in D$ such that $|a|$ is maximum. Find $|a|$.

Let $(b, c, d) \in Z_2 \oplus Z_2 \oplus Z_{12}$ such that $|(b, c, d)| = LCM[|b|, |c|, |d|] = k$ such that k is maximum. By staring $k = 12$. Since $U(2^4 \cdot 3^2) \approx Z_2 \oplus Z_2 \oplus Z_{12}$. we conclude that $|a| = k = 12$.

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

4.9 Final Exam Solution

Question 1: $f = (1\ 3\ 2\ 4) \circ (1\ 2\ 3) \circ (4\ 5)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$$

(i) Is $f \in A_5$? $f = (1\ 4\ 5) = (1\ 4) \circ (1\ 5)$

We have an even number of 2-cycles, thus f is an even permutati

$\therefore$ $f \in A_5$.

(ii) $|f|$: Since $f = (1\ 4\ 5) \rightarrow |f| = 3$.

(iii) Determine f^{-1}: $f^{-1} = (5\ 4\ 1)$

Question 2: All non-cyclic Abelian, 36 elements = $2^2 \cdot 3^2$ elements.

Partition of 2:	Order 2^2	Order 3^2	
0 + 2	$\mathbb{Z}_4$	$\mathbb{Z}_9$	4 groups total.
1 + 1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	

We want non-cyclic, with order 9 element (unique).

All: $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{36}$ since $\gcd(4,9)=1$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

Since there is a unique subgroup of order 9;

$\mathbb{Z}_2 \oplus \mathbb{Z}_{18}$ is none cyclic
$\mathbb{Z}_3 \oplus \mathbb{Z}_{12}$ is non-cyclic
$\mathbb{Z}_6 \oplus \mathbb{Z}_6$ is non-cyclic
} Of these, they each have order 9

element. $\Longrightarrow$ $\operatorname{lcm}(|a|,|b|) = 9$

Since they are Abelian & non-cyclic, converse of Lagrange implies uniqueness for all three structures.

Question 3: $F: \mathbb{Z}_5 \oplus \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$; $f(a,b) = a^{-1} + 2\cdot b$.

(i) Let $a,b,c,d \in \mathbb{Z}_5 \oplus \mathbb{Z}_5$. Then: $f(a+b, c+d) =$

$$= (a+b)^{-1} + 2(c+d)$$
$$= b^{-1} + a^{-1} + 2\cdot c + 2\cdot d$$
$$= [a^{-1} + 2\cdot c] + [b^{-1} + 2\cdot d]$$
$$= f(a,c) + f(b,d).$$

$\therefore f$ is a group homomorphism.

(ii) Ker(f): a, b s.t. $f(a,b) = e$ in $\mathbb{Z}_5 = 0$.

By observation: consider $a^{-1} + 2\cdot b$ where $a \in \mathbb{Z}_5$, $b \in \mathbb{Z}_5$

$f(0,0) \longrightarrow 0$

b

a	0	1	2	3	4
0	0	2	4	1	3
1	2				
2					
3					
4					

$2^{-1} + 2(1) = 3 + 2 = 5 \mod 5 \equiv 0$

$\therefore (2,1)$.

$4^{-1} = 1$; $2(2) = 4$; $\Rightarrow (4,2)$ works.

$(1)^{-1} = 4$; $2(3) = 6$; $4 + 6 = 0 \mod 5$; $\Longrightarrow (1,3)$ works.

$3^{-1} = 2$, $2(4) = 8$; $2 + 8 = 0 \mod 5$.

$\therefore$ ker$(f) = \{(0,0), (4,2), (1,3), (2,1), (3,4)\}$.

Question 5: $a^{-1} + 2b = f(a, b)$

(iii) Union of all left cosets make up $(\mathbb{Z}_5, +) \oplus (\mathbb{Z}_5, +)$

$\mathrm{Ker}(f) = \{(0,0), (4,2), (1,3), (2,1), (3,4)\}$

$1 + \ker(f) = \{(1,1), (0,2), (2,3), (3,2), (4,0)\}$

$2 + \ker(f) = \{(2,2), (1,3), (3,4), (4,3), (0,1)\}$

$3 + \ker(f) = \{(3,3), (2,4), (4,0), (0,4) (1,2)\}$

$4 + \ker(f) = \{(4,4) (3,0) (0,1) (1,0) (2,3\}$

$$\left.\begin{array}{l}
f(0,0) = f(4,2) = f(1,3) = f(2,1) = f(3,4) = e. \\
f(1,1) = f(0,2) = F(2,3) = f(3,2) = f(4,0) = 1 \\
f(2,2) = \ldots = 2 \\
f(3,3) = \ldots = 3 \\
f(4,4) = \ldots = 4
\end{array}\right\}$$

__Question 4:__ $(\mathrm{Aut}(\mathbb{Z}_{24}), \circ) \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$.

(i) We know by class result: $(\mathrm{Aut}(\mathbb{Z}_{24}), \circ) \cong (U(24), \times)$

$$U(24) = U(2^3 \cdot 3) \cong U(2^3) \oplus U(3).$$

$$\Rightarrow \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

$$\therefore (\mathrm{Aut}(\mathbb{Z}_{24}), \circ) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2; \quad \left\{ \begin{array}{l} m_1 = 2 \\ m_2 = 2 \\ m_3 = 2 \end{array} \right\}$$

(ii) Subgroup, H, with $|H| = 4$. Can H be cyclic?

Construct ~~$F: (\mathbb{Z}_{24}) \to (\mathbb{Z}_{24}, +)$~~

Construct $K : (U(24), \cdot) \to (\mathrm{Aut}(\mathbb{Z}_{24}), \circ)$

$K(a) = f_a$ for every $a \in U(24)$ & $f_a \in \mathrm{Aut}(\mathbb{Z}_{24})$.

Let $f_a : (\mathbb{Z}_{24}, +) \to (\mathbb{Z}_{24}, +)$, $f_a(b) = ab \pmod{24}$.

$$U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

~~$H \le U(24)$ s.t. $H = \{1, 5\}$ is a subgroup of order~~

Take $\{1, 5, 7, 11\}$

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$$\therefore H \le U(24) \Rightarrow \{f_5, f_7, f_{11}, e\} < \mathrm{Aut}(\mathbb{Z}_{24}).$$

However, H cannot be cyclic because we cannot find elements that could form subgroups L, M s.t. $|L| \neq 2$ & $|M| \neq 2$.

All subgroups are of order 2 and thus H would never ~~be~~ be cyclic.

Question 5: $(D, \cdot)$ group, $H \lhd D$ s.t. D/H cyclic but D is not Abelian.

Take some $n \in \mathbb{Z} \geq 5$. We know by class result that $A_n \lhd S_n$. We have a group, S_n, and a normal subgroup, A_n.

Now: $|S_n/A_n| = \dfrac{|S_n|}{|A_n|} = \dfrac{n!}{\frac{n!}{2}} = 2$, 2 is a prime.

$\therefore$ since every group of prime order is cyclic (by result),

S_n/A_n cyclic.

But we know that S_n is not Abelian. Refer to HW1 problem for counter example.

Question 6: All Abelian with 72 elements:

$72 = 2^3 \times 3^2$

Partition of 3	Partition of 2	Order 2^3	Order 3^2
$0+3$	$0+2$	$\mathbb{Z}_8$	$\mathbb{Z}_9$
$1+2$	$1+1$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$.
$1+1+1$		$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	
		$\underbrace{\quad}_{3}$	$\underbrace{\quad}_{2}$

We have $3 \cdot 2 = 6$ total

i.e. There are 6 Abelian groups with 72 elements.

Question 7: $U(360) = U(2^3 \cdot 3^2 \cdot 5)$

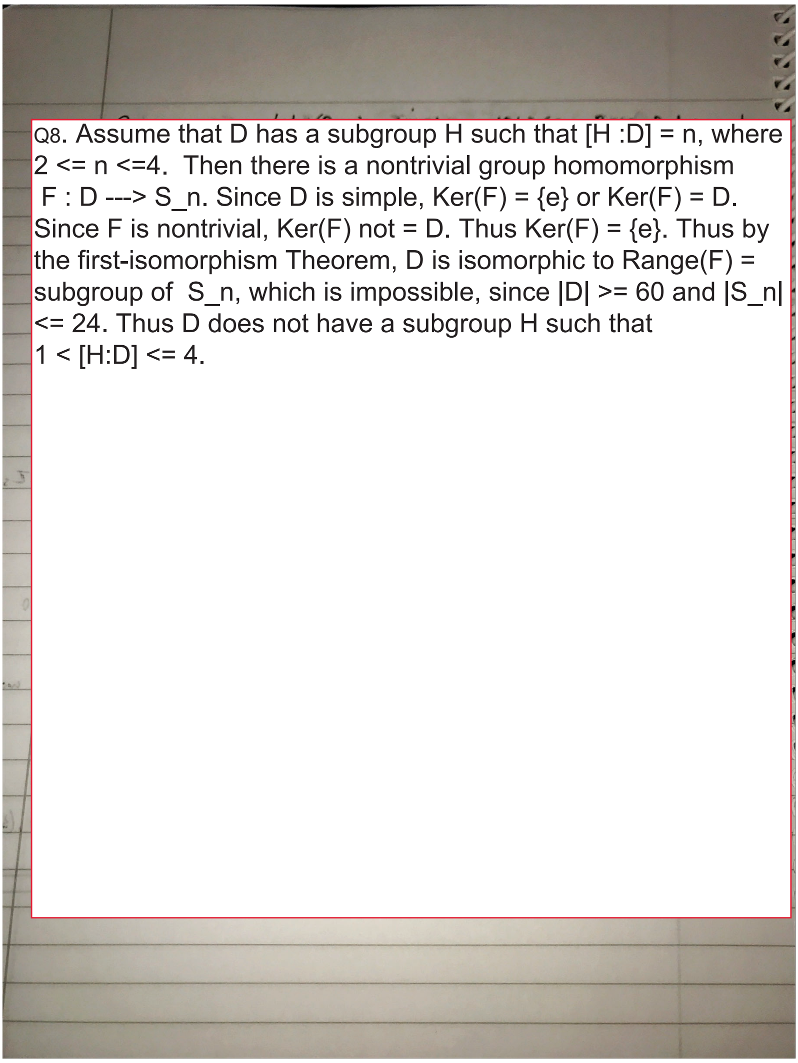
$$\cong U(2^3) \oplus U(3^2) \oplus U(5)$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$$

since $\gcd(3,4) = 1 \Rightarrow$ combine $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{12}$.

$\therefore$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$. $\Longrightarrow$ invariant factors.

$\therefore m_1 = 2, m_2 = 2, m_3 = 2, m_4 = 12$



Q8. Assume that D has a subgroup H such that [H :D] = n, where 2 <= n <=4. Then there is a nontrivial group homomorphism F : D ---> S_n. Since D is simple, Ker(F) = {e} or Ker(F) = D. Since F is nontrivial, Ker(F) not = D. Thus Ker(F) = {e}. Thus by the first-isomorphism Theorem, D is isomorphic to Range(F) = subgroup of S_n, which is impossible, since |D| >= 60 and |S_n| <= 24. Thus D does not have a subgroup H such that 1 < [H:D] <= 4.

Question 9. $f: D \to L$ group homomorphism, $H < \text{range}(F)$.

$$K = \{ a \in D \mid f(a) \in H \} < D, \quad \ker(f) \subseteq K.$$

Since $H < \text{range}(F)$, $\longrightarrow$ $|H| \mid |\text{range}(F)|$

Let $a, b \in K$. Show that $a^{-1} \cdot b \in K$.

$$\left.\begin{array}{l} a \in D \text{ s.t. } f(a) \in H \\ b \in D \text{ s.t. } f(b) \in H \end{array}\right\}$$

We know H group, so: $[f(a)]^{-1} \in H$ ~~st.~~ $\to f(a^{-1}) \in H$.

$$f(a^{-1} \cdot b) = [f(a)]^{-1} \times [f(b)] \implies f(a^{-1}) \times f(b)$$

$f(a^{-1}) \in H$, $f(b) \in H$; $\implies$ closed, $\therefore K < D$.

Since $H <$ range(f); $\longrightarrow$ the identity element is in H.

Since K consists of all the elements that map to $f(a) \in H$, this means K maps to some elements in the range of F, and e is in the range of F.

$\therefore$ The elements that map to e must be in K, and thus $\text{Ker}(F) \subseteq K$.

Done.

Question 10: $(D, \cdot)$ group with $|D| = 65$. Let $K \trianglelefteq D$ s.t. $|K| = 5$. Prove D is cyclic.

Since $|D| = 65 = 5 \times 13$, we know D has an element of order 13. let $a \in D$ st. $|a| = 13$.

Let $H = \langle a \rangle \Longrightarrow |H| = 13$.

Consider D/H. $|D/H| = \frac{|D|}{|H|} = \frac{65}{13} = 5 \longrightarrow$ smallest prime factor of D. $\Longrightarrow$ H normal subgroup of D.

~~Also~~ Clearly $H \trianglelefteq D$ and $K \trianglelefteq D \longrightarrow$ We know $H \cap K = \{e\}$ since $\gcd(13, 5) = 1$.

Thus $D = H \cdot K$ and hence $D \cong H \oplus K$.

$$\left.\begin{aligned} H &\cong \mathbb{Z}_{13} \\ K &\cong \mathbb{Z}_5 \end{aligned}\right\} \text{ since } \gcd(13,5) = 1; \text{ then:}$$

$D \cong \mathbb{Z}_{13 \cdot 5} = \mathbb{Z}_{65}$. $\mathbb{Z}_{65}$ is cyclic. Thus D is cyclic.

5 Section 5: Assessment Tools-Home Work’s (unanswered)

5.1 HW I

Name——————————————, ID ——————

Homework One, MTH 320 , Fall 2020, Due date: Sept 14 by MIDNIGHT, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

QUESTION 1. Let H be the set of all symmetries on an equilateral triangle (see class notes). Construst the Caley's table of (H, o). By staring at the table, you should conclude that (H, o) is a group.

(i) For each $f \in H$, find f^{-1}

(ii) For each $f \in H$, find $|f|$ (note f^m here means $f\ o\ f\ o\ f\ o \cdots\ of$ (m times))

(iii) Show that (H, o) is a non-abelian group (i.e., show that $f\ o\ k \neq k\ o\ f$ for some $f, k \in H$)

QUESTION 2. Let C be the set of all complex numbers. It is clear that (C^*, X) is group under multiplication. Fix a positive integer $n \geq 2$ and let H be the set of all roots of the polynomial $x^n - 1$ (i.e., $H = \{x \in C^* \mid x^n - 1 = 0\}$). Prove that (H, X) is a subgroup of (C^*, X). [Hint : note that H is a finite subset of C^*.]

QUESTION 3. Consider the group $(Z_{20}, +)$ Find $|1|, |6|, |14|, |15|, |17|, |12|$ [Hint: first find $|1|$, then observe that $k = 1^k$ (for example $8 = 1^8$)], then use a class-result to find the order of the remaining elements]

QUESTION 4. Let $H = \{2, 4, 6, 8, 10, 12\}$ and "." be the multiplication modulo 14. Construct the Caley's Table of $(H, .)$. By staring at the table you will observe that $(H, .)$ is an abelian group.

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

(ii) For each $a \in H$, find a^{-1}.

(iii) Find $|6|, |10|$.

QUESTION 5. (1) Let a, b be elements in a group $(D, .)$ such that $a \cdot b = b \cdot a$. Given $|a| = n, |b| = m$, where $n, m \neq \infty$ and $gcd(n, m) = 1$. Let $x = a \cdot b$. Prove $|x| = nm$. [Hint: (you need to know these facts, you might need them later on in the course) (1) If $a \cdot b = b \cdot a$, then $(a \cdot b)^n = a^n \cdot b^n$, if $a \cdot b \neq b \cdot a$, then we cannot CLAIM that $(a \cdot b)^n = a^n \cdot b^n$. (2) Let k, n, m be positive integers: (a) if $n \mid km$ and $gcd(n, m) = 1$, then $n \mid k$. (b) if $n \mid k$ and $m \mid k$ and $gcd(n, m) = 1$, then $nm \mid k$].

(2) In Question 1 (above), find two elements f, k in (H, o) such that $|f| = 2$ and $|k| = 3$, but $|f\ o\ k| \neq 6$ (note that $gcd(2, 3) = 1$). So the hypothesis $a \cdot b = b \cdot a$ in (1) is very crucial.

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

WARNING: Title too long for running head.
PLEASE supply a shorter form with \headlinetitle

5.2 HW II

Homework Two, MTH 320 , Fall 2020, Due date: Sept 29 (Tuesday) by MIDNIGHT, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

QUESTION 1. Let $A = \{1, 2, 3\}$ and D be the power set of A, i.e., D is the set of all subsets of A (note that $|D| = 2^3 = 8$). Define "." on D to mean $a \cdot b = (a - b) \cup (b - a)$ for every $a, b \in D$. Then $(D, .)$ is an abelian group (optional, you may verify this by doing the Caley's Table, but it is not a must)

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

(ii) For each $a \in D$, find a^{-1}

(iii) For each $a \in D$, find $|a|$.

(iv) (nice), I told you that the converse of Lagrange Theorem is correct when a group is finite and abelian (I allow you to use this fact), i.e., if D is abelian group, $|D| = n$, and $m \mid n$. Then D has at least one subgroup with m elements. Now the above group is abalian and $|D| = 8$. Give me a subgroup, say H, of D with 4 elements. Verify that H is a subgroup by doing the Caley's table. Does D have an element of order 4? so what do you learn from this question? Answer: if $m|n$, then we must have a subgroup with m elements, but not necessarily an element of order m.

QUESTION 2. Let $D = \{2, 4, 6, 8, 10, 12\}$. From HW-One, we know that D under multiplication modulo 14 is an abelian group (see HW-One (Question 4)). Now $H = \{8, 6\}$ is a subgroup of D. Find all left cosets of H. Since D is abelian, H is a normal subgroup of D. Construct the Caley's Table of the group $(D/H, *)$.

QUESTION 3. Let $(D, .)$ be a group, H, K are distinct subgroups of D, i.e., $H \neq K$

(i) Prove that $F = H \cap K$ is a subgroup of D [Hint: Let $a, b \in F$, by a class result, you only need to show that $a^{-1} \cdot b \in F$ for every $a, b \in F$.]

(ii) Assume that neither $K \subset H$ nor $H \subset K$. Prove that $H \cup K$ is never a subgroup of D.

(iii) Assume $|H| = |K| = m$, where m is a prime positive integer. Prove that $H \cap K = \{e\}$.

QUESTION 4. (a) Let $(D, .)$ be a group, H is a normal subgroup of D, and K is a subgroup of D. Prove that $H \cdot K = \{h \cdot k \mid h \in H, k \in K\}$ is a subgroup of D. Note that H is a subgroup of $H \cdot K$ and K is a subgroup of $H \cdot K$ since $H \cdot e = H$ and $e \cdot K = K$ [Hint: Let $a, b \in H \cdot K$, by a class result, you only need to show that $a^{-1} \cdot b \in H \cdot K$ for every $a, b \in H \cdot K$.]

(b)Conside S_3 the symmetric group of an equilateral triangle as in HW-one. Give me a subgroup, say H, of S_3 that is not a normal subgroup of S_3.

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

WARNING: Title too long for running head.
PLEASE supply a shorter form with \headlinetitle

5.3 HW III

Name——————————————, **ID** ————————

Homework Three, MTH 320 , Fall 2020, Due date: October 14 (Wednesday) by MIDNIGHT, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

QUESTION 1. Let $(D, .)$ be a group with 130 elements. Given, $a, b \in D$ such that $a \cdot b = b \cdot a$, $|a| = 10$ and $|b| = 13$. Prove that D is an abelian group. Can you say more about D?

QUESTION 2. (i) Assume $(D, .)$ is an infinite cyclic group and $a \in D$ such that $a \neq e$. Prove that $|a| = \infty$.

(ii) We know $(Z_8, +)$ is cyclic and $(Z, +)$ is cyclic. Prove that $Z_8 \oplus Z$ is not a cyclic group. [Hint: use (i) above!].

(iii) Let $(H, .)$, $(K, *)$ be cyclic groups such that $|H| = m$ and $|K| = n$. Let $D = H \oplus K$. Prove that D is cyclic if and $gcd(m, n) = 1$[Hint: First assume that D is cyclic. Show $gcd(m, n) = 1$. Second direction: Assume $gcd(m, n) = 1$. Show that D is cyclic.]

(iv) Let $D = (Z_8, +) \oplus (Z_{15}, +)$. Then by (iii), D is cyclic. How many generators does D have? Find all subgroups of D with 20 elements. How many elements of order 40 does D have?

(v) Let $(D, .)$ be a group. Given that D has exactly 10 distinct subgroups, each has 13 elements. How many elements of order 13 does D have?

QUESTION 3. (a) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 6 & 8 & 9 & 2 & 3 & 1 & 5 \end{pmatrix} \in S_9$. Find $|f|$.

(b) Let $f = (1\ 3\ 7)\ o\ (1\ 2\ 4\ 5)\ o\ (2\ 3\ 1\ 6) \in S_7$. Find $|f|$.

QUESTION 4. Let $(D, .)$ be a group such that $|D| = 77$. Given that H is a normal subgroup of D such that $|H| = 7$. Suppose that D has exactly one subgroup with 11 elements. Prove that D is a cyclic group. [Hint : Think about D/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

WARNING: Title too long for running head.
PLEASE supply a shorter form with \headlinetitle

5.4 HW IV

Homework Four, MTH 320 , Fall 2020, Due date: October 29, 2020, by MIDNIGHT, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

QUESTION 1. Let D_n ($n \geq 3$) be the set of all symmetries on $n - gon$ (see class notes). We know from class notes that (D_n, o) is a group with exactly 2n elements (exactly n elements are rotations and exactly n elements are reflections, note $e = R_{360}$ and $R_a^{-1} = R_a$ for every reflection $R_a \in D_n$.). It is clear that the composition of two rotations is a rotation in D_n.

(i) (give a short proof, but clear-cut). Prove that the composition of a rotation with a reflection is a reflection in D_n (nice!) (i.e, assume that R is a rotation and R_a is a reflection, prove that $R\ o\ R_a = R_b$ for some reflection R_b in D_n.)

(ii) (give a short proof, but clear-cut).Prove that the composition of two reflections is a rotation in D_n (i.e, assume that R_a, R_b are reflections in D_n, prove that $R_a\ o\ R_b = R$ for some rotation R in D_n.)

QUESTION 2. (a) Assume $(D, .)$ is a group such that $a^2 = e$ for every $a \in D$. Prove that D is an abelian group.

(b) Assume that $(D, .)$ is a group such that $(ab)^2 = a^2b^2$ for every $a, b \in D$. Prove that D is an abelian group.

QUESTION 3. a) Let (D, .) be a group and $a \in D$ such that $|a| = n < \infty$. Prove that $|b.a.b^{-1}| = |a| = n$ for every $b \in D$.

b) Let (D, .) be a group and H be a subgroup of D such that $|H| = m < \infty$.

i) Prove that $|a.H.a^{-1}| = |H| = m$ for every $a \in D$. [Hint : Let $a \in D$ and construct a function $f : H \to a.H.a^{-1}$ such that $f(b) = a.b.a^{-1}$. Show that f is 1-1 and onto , (easy)]

ii) Let $a \in (D, .)$. Prove that $a.H.a^{-1}$ is a subgroup of D [Hint: Let $x, y \in a.H.a^{-1}$, show that $x.y \in a.H.a^{-1}$].

iii) Assume H is unique (i.e., H is the only subgroup of D with m elements). Prove that H is a normal subgroup of D (nice! and easy, make use of (i) and (ii))

QUESTION 4. Let $f = (1\ 2\ 6)\ o\ (6\ 3\ 2\ 5)\ o\ (1\ 6\ 2\ 4\ 5) \in S_6$.

a) Find |f|.

b) Find f^{-1}

c) Is $f \in A_n$? explain.

e) Let $h \in A_9$ such that $|h|$ is maximum. What is $|h|$? (think, not difficult) (i.e., if $|h| = m$, then $|b| <= m$ for every $b \in A_9$)

QUESTION 5 (Nice, good exercise, see class notes). . Let $f : (Z_{12}, +) \to (Z_9, +)$ be a non-trivial group homomorphism.

a) Find Range(f) and Ker(f).

b) What are all possibilities of $f(1)$? For each possibility of $f(1)$, find $f(a)$ for every $a \in Z_{12}$. [Hint: Note if we know f(1), then we know $f(a)$ for every $a \in Z_{12}$. Since $Z_{12} =< 1 >$ and f is a group homomorphism, $f(a) = f(1^a) = (f(1))^a$. By the first isomorphism theorem , we know $Z_{12}/Ker(f)$ is group-isomorphic to Range(f) (see class notes: $K(b + Ker(f)) = f(b)$. Hence if $i + Ker(f)$ is a left coset of Ker(f). Then $K(i + Ker(f)) = f(i)$. Observe that each element in a left coset can be chosen as a representative, Thus for every $b \in i + Ker(f)$ (we know b + Ker(f) = i + Ker(f)), we have $K(i + Ker(f)) = K(b + Ker(f)) = f(i) = f(b)$ (i,e., if W is a left coset of Ker(f), then all elements of W must map to the same number in Z_9). Now since 1 is a generator of Z_{12}, $f(1)$ must be a generator of Range(f) (note that Range(f) is a cyclic subgroup of Z_9).

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

WARNING: Title too long for running head.
PLEASE supply a shorter form with \headlinetitle

5.5 HW V

Name——————————————, ID ————————

HW5, MTH 320, Due date: November 26, Thursday by MIDNIGHT + 4 more hours, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

PLEASE when you write something /make it brief/ clear/ try to avoid writing something that you do not understand

QUESTION 1. Let D be the set of all functions with continuous 4th derivative, a_1, a_2 be some nonzero fixed real numbers. We know that $(D, +)$ is an abelian group. Define $K : (D, +) \rightarrow (D, +)$ such that $k(y(x)) = a_1 y^{(4)} + a_2 y^{(2)}$.

(i) Convince me that K is a group-homomorphism,

(ii) Given $f(x) = cos(2x)e^{3x} \in Range(K)$. Given $h(x) \in D$ such that $K(h(x)) = f(x)$. Let $m(x) \in D$ such that $K(m(x)) = f(x)$. Prove that $m(x) = h(x) + g(x)$, for some $g(x) \in Ker(K)$. i.e., by doing this question, you will understand why the general solution, y_g, to a linear diff. equation with constant coefficients is $y_h + y_p$ (where y_h is the homogeneous part and y_p is the particular part.) [hint: Use $D/Ker(k)$ is group-isomorphic to $Range(K)$]

QUESTION 2. Let $(D, .)$ be an abelian group with 125 elements, $m \geq 2$ be a fixed positive integer. Set $F = \{a^m \mid a \in D\}$. Find all possibilities of $|F|$ [Hint: Can you say something about F?]. Do we need abelian here? explain.

QUESTION 3. Let D be a group with $3^2.5^2$ elements. Given $|C(D)| \geq 15$. Prove that D is an abelian group[Hint: Straight forward if you use two theorems that I told you about in the lectures]

QUESTION 4. Given $(D, .)$ is a group with 60 elements, $a \in D$ such that $|C(a)| = 15$. Find $|Conjugate(a)|$.

QUESTION 5. (NICE)

(1) Let D be a group with p^2 elements. Prove that $D \approx Z_{p^2}$ or $D \approx Z_p \oplus Z_p$. [Hint: What do you know about a group with p^2 elements? Use the result if H, K are normal subgroups of D, where $D = H.K$ and $H \cap K = \{e\}$, then $D \approx H \oplus K$.]

(2) Let D be an abelian group with p^3 elements such that D has a unique subgroup with p^2 elements. Prove that D is cyclic. [Hint: Assume not, use the hint as in (1), find H, K such that $D \approx H \oplus K$, then prove that $H \oplus K$ has more than one subgroup with p^2 elements, a contradiction]

QUESTION 6. Let p_1, p_2 be distinct prime integers and D be a group such that $|D| = p_1 p_2$. Prove that D is not a simple group [Recall that D is simple if and only if $\{e\}$ is the only proper normal subgroup of D, then use a class result (straight forward)]

QUESTION 7. Let D be a group with 75 elements. Given D has a subgroup with 25 elements and a normal subgroup with 3 elements. Prove that D is abelian

QUESTION 8. Let $f : (Q, +) \rightarrow (Q, +)$ be a group-homomorphism such that $f(3) = -3$.

1) Prove that $f(1/m) = -1/m$ for every $m \in Z \setminus \{0\}$

2) Prove that $f(x) = -x$ for every $x \in Q$.[Note that Q is the set of all rational numbers and Z is the set of all integers]

QUESTION 9. Let $f : (Z_{15}, +) \rightarrow (Z_{10}, +)$ be a group homomorphism such that $f(2) = 2$. For each left coset of $Ker(f)$, say H, find $f(h)$ for each $h \in H$.

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

WARNING: Title too long for running head.
PLEASE supply a shorter form with \headlinetitle

5.6 HW VI

Name———————————————, **ID** ——————————

HW 6, MTH 320, Due date: Any time before or at Dec 13, Sunday by MIDNIGHT + 4 more hours, email your Solution as a PDF to abadawi@aus.edu

Ayman Badawi

PLEASE when you write something /make it brief/ clear/ try to avoid writing something that you do not understand

Remark 1. We know $U(n)$ is group under multiplication mod n and Z_n is group under addition mod n. So now we can solve linear equations over Z_n.

Example: Solve for x :

$$3x + 7 = 4 \ \ in\ Z_8$$

.

$$3x = 4 + 7^{-1}\ in\ Z_8\ (7^{-1}\ means\ inverse\ of\ 7\ under\ addition\ mod\ 8)$$

$$3x = 4 + 1 = 5$$

$$note\ 3 \in U(8),\ hence\ x = 3^{-1} \cdot 5\ in\ Z_8\ (3^{-1}\ means\ inverse\ of\ 3\ under\ multiplication\ mod\ 8)$$

$$x = 3 \cdot 5 = 7\ in\ Z_8 (since\ 3^{-1} = 3\ in\ U(8))$$

Note that if $a \in U(n), b \in Z_n$, and $c \in Z_n$, then $ax + b = c$ has only one solution in Z_n.

Note that if $a \notin U(n)$, then $ax + b = c$ might have more than one solution or no solutions.

For example: $2x + 1 = 3$ has two solutions in Z_8, x = 1, and x = 5.

For example $2x + 1 = 4$ has no solutions in Z_8.

I expect that you know how to solve $ax + b = c$, when $a \in U(n)$.

QUESTION 1. Solve for x: $5x + 3 = 8$ in Z_{12}.

Write b in terms of a, where $a, b \in Z_9$: $a^{-1} + 4b = 6$ in Z_9. (a^{-1} is the inverse of a under addition mod 9)

QUESTION 2. We know $D = U(2^6 \cdot 5^2) \approx Z_{m_1} \oplus \cdots \oplus Z_{m_w}$, where $m_1, m_2, ..., m_w$ are the invariant factors of D.

(i) Find $m_1, ..., m_w$.

(ii) How many elements of order 4 does D have?

(iii) How many elements of order 5 does D have?

iv) Let $a \in D$ such that $|a|$ is maximum. Find $|a|$.

QUESTION 3. Given $D \approx Z_6 \oplus Z_4 \oplus Z_{10}$ and $F \approx Z_2 \oplus Z_6 \oplus Z_{20}$. Convince me that $D \approx F$.

Let $L = Z_2 \oplus Z_{10} \oplus Z_{12}$. Then $|L| = |D| = |F| = 240$. Convince me that $L \approx D \approx F$.

QUESTION 4. (i) Up to isomorphic, classify all finite abelian groups with $2^5 \cdot 5^3$ elements.

(ii) up to isomorphic, classify all non-cyclic finite abelian groups with $2^5 \cdot 5^3$ elements such that each has an element of order $200 = 2^3 \cdot 5^2$. Write each group in terms of its invariant factors.

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 Section 5: Assessment Tools-Exams (unanswered)

6.1 Exam I

Name——————————————, **ID** ——————

Exam-One, MTH 320

Ayman Badawi

QUESTION 1. i) Let H be an abelian group with 33 elements. Prove that H is cyclic.
ii) Let D be a group with 65 elements. Suppose that D has a normal subgroup with 13 elements and a unique subgroup with 5 elements. Prove that D is cyclic.

QUESTION 2. Consider the group $(Z_{20}, +)$

(i) Construct a subgroup H of Z_{20} that contains exactly 5 elements.

(ii) Find all distinct left cosets of H.

QUESTION 3. Let $D = Z_6 \times Z_{35}$
i) Is D cyclic? explain.
ii) Find a generator of D.
ii) How many elements of order 15 does D have?
iii) construct a subgroup of D that has exactly 14 elements.

QUESTION 4. Let $A = (1\ 2\ 5)\ o\ (6\ 5\ 2)\ o\ (3\ 8\ 6\ 10)$
i) Find $|A|$
ii) Is A even or odd? explain.
ii) Find $|A\ o\ (10\ 2\ 3)|$.

QUESTION 5. Let $f : (Z_{16}, +) \to (Z_{12}, +)$ be a non-trivial group homomorphism.
i) Find $Range(f)$.
ii) Find $Ker(f)$.
iii) Give me one possibility for $f(1)$, let us call it b. Using $f(1) = b$, find f(a) for every $a \in Z_{16}$.

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`

6.2 Exam II

Name———————————————, ID ————————

MTH 320, Exam II, Fall 2020

Ayman Badawi

————
47

QUESTION 1. (6 points) Let $(D, .)$ be a group with 39 elements. Assume that D has a normal subgroup with 3 elements. Prove that D is cyclic.

QUESTION 2. Let $(D, .)$ be an abelian group with 245 = $5 \cdot 7^2$ elements. Assume that D is non-cyclic.

i) **(6 points)** Find $m_1, .., m_k$ such that $D \approx (Z_{m_1}, +) \oplus \cdots \oplus (Z_{m_k}, +)$. SHOW THE WORK.

ii) **(3 points)** How many elements of order 35 does D have?

iii) **(3 points)** How many elements of order 7 does D have?

QUESTION 3. (5 points) Let $(D, .)$ be a non-cyclic-group with 2020 elements. Prove that there are finitely many groups, say $D_1, ..., D_m$, each with 2020 elements such that $D \not\approx D_i$ (i.e., D is not group-isomorphic to D_i) for every i, where $1 \leq i \leq m$.

QUESTION 4. Let $f : (Z_6, +) \oplus (Z_6, +) \to (Z_6, +)$ such that $f((a, b)) = 2 \cdot (a + b^{-1})$ (note that b^{-1} means the inverse of b under addition mod 6, and in $2 \cdot (a + b^{-1})$, the "+" means addition mod 6 and "$\cdot$" means multiplication mod 6 .

i) **(3 points)** Show that f is a group-homomorphism.

ii) **(3 points)** Find the range of f.

iii)**(5 points)** Find $ker(f)$.

QUESTION 5. Let $D = (Aut(Z_{20}), o)$. [Recall: $Aut(Z_{20})$ is the group of all group-isomorphism from $(Z_{20}, +)$ onto $(Z_{20}, +)$ under composition.]

i) **(3 points)** Is D cyclic? explain?

ii) **(4 points)** Construct a non-cyclic subgroup of D, say (H, o), of D such that $|H| = 4$.

QUESTION 6. Let $n = 16 \cdot 9$ and $D = U(n)$.

(i)**(4 points)** Find $m_1, .., m_k$ such that $D \approx (Z_{m_1}, +) \oplus \cdots \oplus (Z_{m_k}, +)$. SHOW THE WORK.

(ii) **(2 points)** Let $a \in D$ such that $|a|$ is maximum. Find $|a|$.

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`

6.3 Final Exam

Name——————————————, ID ————————

Final-Exam, MTH 320, Fall 2020

Ayman Badawi

$$\text{Score} = \frac{\qquad}{48}$$

QUESTION 1. (6 points) Let $F = (1\ 3\ 2\ 4)\ o\ (1\ 2\ 3)\ o\ (4\ 5)$

(i) Is $F \in A_5$? Explain

(ii) Find $|F|$

(iii) Find F^{-1}

QUESTION 2. (6 points) (up to isomorphic) classify all noncyclic abelian group with 36 elements, such that each has unique subgroup with 9 elements. Write down the invariant factors of each group.

QUESTION 3. (6 points) Let $F : Z_5 \oplus Z_5 \to Z_5$ such that $F(a, b) = a^{-1} + 2b$ (note that a^{-1} means inverse of a under addition mod 5 and 2b means 2 times b mod 5)

(i) Show that F is a group homomorphism.

(ii) Find $Ker(F)$

(iii) For each left cosets, say L, of $Ker(f)$, find $F(w)$ for every $w \in L$.

QUESTION 4. (6 points)

(i) We know that $(Aut(Z_{24}),\ o) \approx Z_{m_1} \oplus \cdots \oplus Z_{m_w}$, where $m_1, ..., m_w$ are the invariant factors of $Aut(Z_{24})$. Find $m_1, ..., m_w$.

(ii) Construct a subgroup, H, of $Aut(Z_{24})$ such that $|H| = 4$. Is it possible that H is cyclic? Explain.

QUESTION 5. (4 points) Give me an example of a group $(D, .)$ such that D has a normal subgroup H such that D/H is cyclic, but D is not abelian.

QUESTION 6. (4 points) (up to isomorphic) classify all abelian group with 72 elements.

QUESTION 7. (4 points) We know $U(360) \approx Z_{m_1} \oplus \cdots \oplus Z_{m_w}$, where $m_1, ..., m_w$ are the invariant factors of $U(360)$. Find $m_1, ..., m_w$. [Note $360 = 2^3 \cdot 3^2 \cdot 5$]

QUESTION 8. (4 points) Let D be a simple group such that $|D| \geq 60$. Prove that D does not have a subgroup H such that $1 < [H : D] \leq 4$ (Recall that $[H : D] = |D|/|H|$)

QUESTION 9. (4 points) Let $F : D \to L$ be a group homomorphism and H be a subgroup of $Range(F)$. Prove that $K = \{a \in D \mid F(a) \in H\}$ is a subgroup of D and $Ker(F) \subseteq K$.

QUESTION 10. (4 points) Let D be a group such that $|D| = 65$. Assume that D has a normal subgroup with 5 elements. Prove that D is cyclic.

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

Faculty information

Ayman Badawi, American University of Sharjah, UAE.
E-mail: abadawi@aus.edu