HW one, MTH 320, Fall 2016

Ayman Badawi

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)

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

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

Hence $b = c$

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 $b = c$

5/5

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

Proof:

$a * x = b$

$x = e * x$

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

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

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

5/5

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.

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

Suppose n is not prime, then

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

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

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

$Z^*_n = \{1, 2, 3, 4, \dots p-1\}$
$e = 1$
$a^{p-1} \equiv 1 \pmod{p}$

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 $1 \leq a, b \leq n-1$.
Thus $a \cdot_n b \neq 0$. Hence $a \cdot_n b \in Z^*_n$.

2) Inverse: Let $a \in Z^*_n$. Since n is prime we know $a^{n-1} \pmod{n} = 1$. Thus $a \cdot a^{n-2} \pmod{(n)} = 1$. Hence
$a^{-1} = a^{n-2} \pmod{(n)} \in Z^*_n$.

$\frac{\cancel{1}}{5}$

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
$(a * b) \bmod 15$ = remainder of $(a \times b) / 15$

*	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 $= e = 6$

inverse of 3 is 12

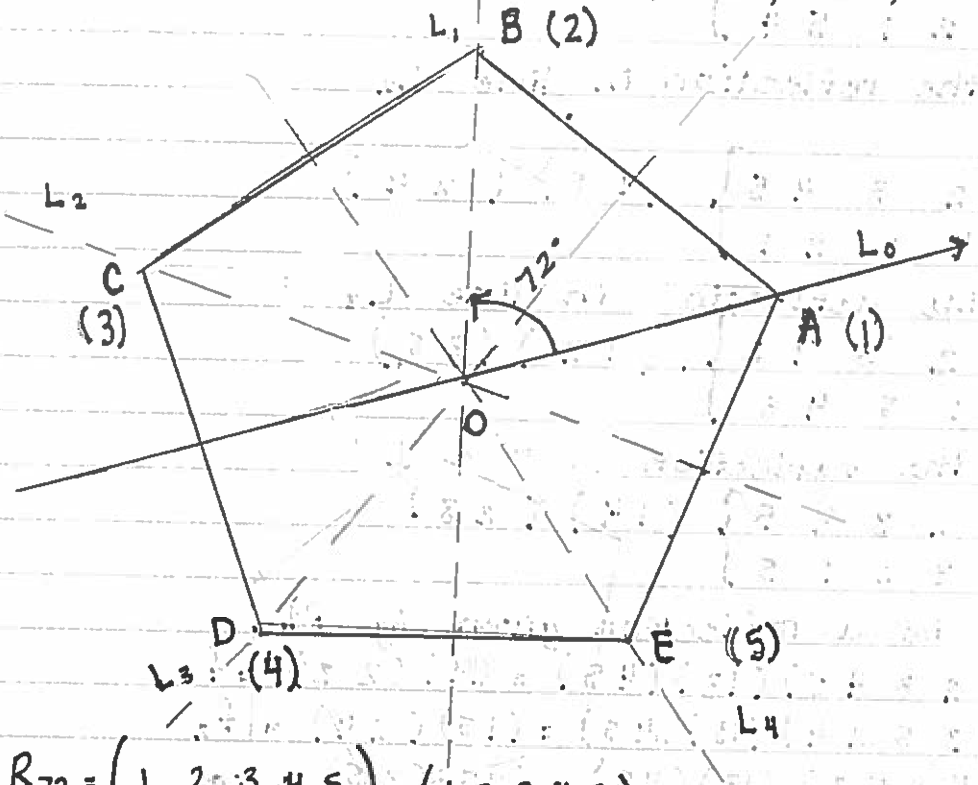
inverse of 6 is 9

inverse of 9 is 6

inverse of 12 is 3

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_5.

If r is a rotation R_0 and s is any reflection then D_5 can be 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

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

f_1 be the reflection in line L_1

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

f_2 be the reflection in line L_2

$$f_2 = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{Bmatrix} \quad (1\ 5)(2\ 4)$$

f_3 be the reflection in line L_3

$$f_3 = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{Bmatrix} \quad (1\ 2)(3\ 5)$$

f_4 be the reflection in line L_4

$$f_4 = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{Bmatrix} \quad (1\ 4)(2\ 3)$$

Let s be a reflection given by $f1$.

$a s = (1\ 2\ 3\ 4\ 5)(1\ 3)(4\ 5) = (1\ 4)(2\ 3) = f_4$

$a^2 s = (1\ 3\ 5\ 2\ 4)(1\ 3)(4\ 5) = (1\ 5)(2\ 4) = f_2$

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

$a^4 s = (1\ 5\ 4\ 3\ 2)(1\ 3)(4\ 5) = (1\ 2)(3\ 5) = f_3$

$a^5 s = (1)(1\ 3)(4\ 5) = (1\ 3)(4\ 5) = f_1$

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

Very long!! you can use mathematical argument?

Name yumna omar, ID b0735

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 $(x_1,x_2)*(y_1,y_2) = (x_1y_1(mod3),\ x_1y_2 + x_2y_1(mod3))$. 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 $(U(9), \cdot_9)$. Is $U(9)$ is cyclic? If yes, then find $a \in U(9)$ such that $(U(9), \cdot_9) =< a >$.

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

(ii) 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

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

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

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

→ 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
$a * (1,0) = (1,0) * a = a \quad \forall\, a \in S$

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

→ 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 [illegible]7

→ Can you say more?

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

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

Hence [illegible] $\boxed{\text{is abelian}}$

(iv) GIVEN: D is a group.

$H_1 < D$ and $H_2 < D$

$H_1 \notin H_2$ and $H_2 \notin H_1$

→ 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

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

→ EXAMPLE:

$(\cancel{D}\mathbb{Z}_6, +_6)$ where $\cancel{D}\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$H_1 = \{0, 2, 4\}$ 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 $a^{-1} * b \in H_1 \cap H_2$.

(v) GIVEN: D is a group
$H_1 < D$ and $H_2 < D$

$\longrightarrow$ 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, $a * b \in H_2$

2/5

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

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

(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
$a * b = b * a \;\; \forall \, a, b \in S$
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

3/3

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 $e^{11} = e$

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

$\lightning$

(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 $a=5$

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, $e = (a * b)^{kn} = (a^m)^k * b^{kn} = e * b^{kn} = b^{kn}$. 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, $x * y = (a^i * h) * (a^k * g) = a^{(i+k) mod 3} * (h * g)$. Since $0 \leq (i + k) mod 3 \leq 2$ 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

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 $L \lhd A_4$? 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 $L \lhd A_4$.

(vii) Let D be a group with 15 elements. Assume $H \lhd D$ 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`