MTH 4441 Subgroups and Cyclic Subgroups - Solutions

Fall 2017

Pat Rossi Name ____________________

1. Let $S(A) = \{e, \rho, \rho^2, \sigma, \gamma, \delta\}$. Decide whether each of the following subsets is a subgroup of $S(A)$. If a set is NOT a subgroup, give a reason why it is not (in addition to the fact that an element may appear more than once, or not at all, in a row or column).

Recall the group table for $(S(A), \cdot)$:

$\cdot$	e	ρ	ρ^2	σ	γ	δ
e	e	ρ	ρ^2	σ	γ	δ
ρ	ρ	ρ^2	e	γ	δ	σ
ρ^2	ρ^2	e	ρ	δ	σ	γ
σ	σ	δ	γ	e	ρ^2	ρ
γ	γ	σ	δ	ρ	e	ρ^2
δ	δ	γ	σ	ρ^2	ρ	e

a. $\{e, \sigma\}$

$\cdot$	e	σ
e	e	σ
σ	σ	e

It's a group.

Looking at the table, each element appears in each row and each column exactly once.

More specifically, $\cdot$ is closed on $\{e, \sigma\}$, e is the identity, and σ is its own inverse (because $\sigma \cdot \sigma = e$).

b. $\{e, \delta\}$

$\cdot$	e	δ
e	e	δ
δ	δ	e

It's a group.

Looking at the table, each element appears in each row and each column exactly once.

More specifically, $\cdot$ is closed on $\{e, \delta\}$, e is the identity, and δ is its own inverse (because $\delta \cdot \delta = e$).

c. $\{e, \rho\}$

$\cdot$	e	ρ
e	e	ρ
ρ	ρ	ρ^2

It's NOT a group.

Looking at the table, the identity e does not appear in either the row or the column headed by ρ.

More specifically, $\cdot$ is NOT closed on $\{e, \rho\}$, as $\rho \cdot \rho = \rho^2 \notin \{e, \rho\}$.

Also, since e does not appear in either the row or the column headed by ρ, this indicates that ρ does NOT have an inverse in $\{e, \rho\}$.

d. $\{e, \rho^2\}$

$\cdot$	e	ρ^2
e	e	ρ^2
ρ^2	ρ^2	ρ

It's NOT a group.

Looking at the table, the identity e does not appear in either the row or the column headed by ρ^2.

More specifically, $\cdot$ is NOT closed on $\{e, \rho^2\}$, as $\rho^2 \cdot \rho^2 = \rho \notin \{e, \rho^2\}$.

Also, since e does not appear in either the row or the column headed by ρ^2, this indicates that ρ^2 does NOT have an inverse in $\{e, \rho^2\}$.

e. $\{e, \rho, \rho^2\}$

$\cdot$	e	ρ	ρ^2
e	e	ρ	ρ^2
ρ	ρ	ρ^2	e
ρ^2	ρ^2	e	ρ

It's a group.

Looking at the table, each element appears in each row and each column exactly once.

More specifically, $\cdot$ is closed on $\{e, \rho, \rho^2\}$, e is the identity, and ρ and ρ^2 are inverses of one another (because $\rho \cdot \rho^2 = e = \rho^2 \cdot \rho$).

f. $\{e, \rho, \sigma\}$

$\cdot$	e	ρ	σ
e	e	ρ	σ
ρ	ρ	ρ^2	γ
σ	σ	δ	e

It's NOT a group.

We noted, in the previous exercise, that ρ and ρ^2 are inverses of one another. So neither ρ nor ρ^2 can be in a subgroup without the other being in the subgroup also.

More generally, when we look at the table, not every element in $\{e, \rho, \sigma\}$ appears Exactly once in every row and every column.

Also, the identity element e does not appear in either the row or the column headed by ρ. This is symptomatic of ρ not having an inverse in $\{e, \rho, \sigma\}$.

Furthermore, $\cdot$ is NOT closed on $\{e, \rho, \sigma\}$, as $\rho \cdot \rho = \rho^2 \notin \{e, \rho, \sigma\}$; $\rho \cdot \sigma = \gamma \notin \{e, \rho, \sigma\}$; and $\sigma \cdot \rho = \delta \notin \{e, \rho, \sigma\}$.

g. $\{e, \sigma, \gamma\}$

$\cdot$	e	σ	γ
e	e	σ	γ
σ	σ	e	ρ^2
γ	γ	ρ	e

It's NOT a group.

Looking at the table, γ does not appear in either the row or the column headed by σ, and σ does not appear in either the row or the column headed by γ.

More specifically, $\cdot$ is NOT closed on $\{e, \sigma, \gamma\}$, as $\sigma \cdot \gamma = \rho^2 \notin \{e, \sigma, \gamma\}$; and $\gamma \cdot \sigma = \rho \notin \{e, \sigma, \gamma\}$.

h. $\{e, \sigma, \gamma, \delta\}$

$\cdot$	e	σ	γ	δ
e	e	σ	γ	δ
σ	σ	e	ρ^2	ρ
γ	γ	ρ	e	ρ^2
δ	δ	ρ^2	ρ	e

It's NOT a group.

Looking at the table, σ does not appear in either the rows or the columns headed by γ and δ; γ does not appear in either the rows or the columns headed by σ and δ; and δ does not appear in either the rows or the columns headed by σ and γ.

More specifically, $\cdot$ is NOT closed on $\{e, \sigma, \gamma, \delta\}$, as:

$\sigma \cdot \gamma = \rho^2 \notin \{e, \sigma, \gamma, \delta\}$; $\quad \sigma \cdot \delta = \rho \notin \{e, \sigma, \gamma, \delta\}$;

$\gamma \cdot \sigma = \rho \notin \{e, \sigma, \gamma, \delta\}$; $\quad \gamma \cdot \delta = \rho^2 \notin \{e, \sigma, \gamma, \delta\}$;

$\delta \cdot \sigma = \rho^2 \notin \{e, \sigma, \gamma, \delta\}$; $\quad \delta \cdot \gamma = \rho \notin \{e, \sigma, \gamma, \delta\}$

2. Determine whether each of the following sets is a subgroup of $G = \{1, -1, i, -i\}$ under multiplication. If a set is NOT a subgroup, give a reason why.

a. $\{1, -1\}$

$\cdot$	1	-1
1	1	-1
-1	-1	1

It's a group.

Looking at the table, each element appears in each row and each column exactly once.

More specifically, $\cdot$ is closed on $\{1, -1\}$, 1 is the identity, and -1 is its own inverse (because $(-1) \cdot (-1) = 1$).

b. $\{1, i\}$

$\cdot$	1	i
1	1	i
i	i	-1

It's NOT a group.

Looking at the table, the identity 1 does not appear in either the row or the column headed by i.

More specifically, $\cdot$ is NOT closed on $\{1, i\}$, as $i \cdot i = -1 \notin \{1, i\}$.

Also, since 1 does not appear in either the row or the column headed by i, this indicates that i does NOT have an inverse in $\{1, i\}$.

c. $\{i, -i\}$

It's NOT a group.

We KNOW that 1 is the identity, and $1 \notin \{i, -i\}$. (i.e., There is NO IDENTITY - this can't be a group.)

d. $\{1, -i\}$

$\cdot$	1	$-i$
1	1	$-i$
$-i$	$-i$	-1

It's NOT a group.

Looking at the table, the identity 1 does not appear in either the row or the column headed by $-i$.

More specifically, $\cdot$ is NOT closed on $\{1, -i\}$, as $(-i) \cdot (-i) = -1 \notin \{1, -i\}$.

Also, since 1 does not appear in either the row or the column headed by $-i$, this indicates that $-i$ does NOT have an inverse in $\{1, -i\}$.

3. Consider the group $(\mathbb{Z}_{16}, +)$. List all the elements of the subgroup $\langle 6 \rangle$, and state its order.

   In the **additive** subgroup generated by 6, the representative elements of $\langle 6 \rangle$ are of the form $6n$ for $n = 0, 1, 2, \ldots, 15$

   $6 \cdot 0 = 0$

   $6 \cdot 1 = 6$

   $6 \cdot [2] = 12$

   $6 \cdot [3] = 2$

   $6 \cdot [4] = 8$

   $6 \cdot [5] = 14$

   $6 \cdot 6 = 4$

   $6 \cdot 7 = 10$

   $6 \cdot 8 = 0$ (repeat element)

   $\langle 6 \rangle = (\{0, 2, 4, 6, 8, 10, 12, 14\}, +)$

   The **order** of $\langle 6 \rangle = 8$ (the number of elements in $\langle 6 \rangle$)

4. Consider the group $(\mathbb{Z}_{18}, +)$. List all the elements of the subgroup $\langle 8 \rangle$, and state its order.

   In the **additive** subgroup generated by 8, the representative elements of $\langle 8 \rangle$ are of the form $8n$ for $n = 0, 1, 2, \ldots, 17$

   $8 \cdot 0 = 0$

   $8 \cdot 1 = 8$

   $8 \cdot 2 = 16$

   $8 \cdot 3 = 6$

   $8 \cdot 4 = 14$

   $8 \cdot 5 = 4$

   $8 \cdot 6 = 12$

   $8 \cdot 7 = 2$

   $8 \cdot 8 = 10$

   $8 \cdot 9 = 0$ (repeat element)

   $\langle 8 \rangle = (\{0, 2, 4, 6, 8, 10, 12, 14, 16\}, +)$

   The **order** of $\langle 8 \rangle = 9$ (the number of elements in $\langle 8 \rangle$)

5. $(U_{13}, \cdot)$ is a group. (Where $U_{13} = \{1, 2, 3, \ldots, 12\}$.)

a. List the elements of the subgroup $\langle 4 \rangle$ of $(U_{13}, \cdot)$, and state its order.

In the **multiplicative** subgroup generated by 4, the representative elements of $\langle 4 \rangle$ are of the form 4^n for $n = 0, 1, 2, \ldots, 12$

Recall: The **order** of the subgroup $\langle 4 \rangle$ is two equivalent things:

i. It's the number of elements in $\langle 4 \rangle$

ii. It's the least natural number k such that $4^k = 1$

$4^1 = 4$

$4^2 = 3$

$4^3 = 12$

$4^4 = 9$

$4^5 = 10$

$4^6 = 1$

The **order** of $\langle 4 \rangle$ is 6

$\langle 4 \rangle = (\{1, 3, 4, 9, 10, 12\}, \cdot)$

b. List the elements of the subgroup $\langle 8 \rangle$ of $(U_{13}, \cdot)$, and state its order.

In the **multiplicative** subgroup generated by 8, the representative elements of $\langle 8 \rangle$ are of the form 8^n for $n = 0, 1, 2, \ldots, 12$

$8^1 = 8$

$8^2 = 12$

$8^3 = 5$

$8^4 = 1$

The **order** of $\langle 8 \rangle$ is 4

$\langle 8 \rangle = (\{1, 5, 8, 12\}, \cdot)$