M E T U
Department of Mathematics

	Basic Algebraic Structures MIDTERM I	
Code : *Math 116* Acad. Year : *2018 Spring* Instructor : *A.Beyaz, G.Ercan, M.Kuzucuoğlu, Ö.Küçüksakallı F.Özbudak.* Date : *March 22, 2018* Time : *17:40* Duration : *120 minutes*	Last Name : Name : Student No. : Department : Section : Signature :	
	4 QUESTIONS ON 4 PAGES 100 TOTAL POINTS	

1	2	3	4		

1. (25pts) Consider the binary operation $\bigstar$ on $S = \{a, b, c, d\}$ given by the table:

$\bigstar$	a	b	c	d
a	c	a	b	d
b	a	b	c	d
c	c	c	a	b
d	d	d	b	a

(a) Is $\bigstar$ associative?

Solution: No! For example $(a\bigstar c)\bigstar d = b\bigstar d = d$. On the other hand $a\bigstar(c\bigstar d) = a\bigstar b = a$.

(b) Is $\bigstar$ commutative?

Solution: No! For example $a\bigstar c = b \neq c = c\bigstar a$

(c) Does there exist an identity element?

Solution: Yes! The element b is an identity element with respect to $\bigstar$ because $b\bigstar x = x\bigstar b = x$ for each $x \in S$.

(d) Does each element have an inverse?

Solution: No! Observe that $x\bigstar a \neq b$ for all $x \in S$. Thus the element a does not have a left inverse so it does not have an inverse.

2. (25pts) This question has two **independent** parts.

(a) Find all integers x such that $6x \equiv 14 \pmod{55}$.

Solution: We have $\gcd(2, 55) = 1$. Cancelling 2 from both sides, we obtain that $3x \equiv 7 \pmod{55}$. In order to cancel 3 in a similar fashion, we add $55 \cdot 2$ to the right hand side. More precisely, we have

$$3x \equiv 7 + 55 \cdot 2 \equiv 117 \equiv 3 \cdot 39 \pmod{55}.$$

Since $\gcd(3, 55) = 1$, we find that $x \equiv 39 \pmod{55}$. We conclude $x = 39 + 55 \cdot k$ for some integer $k \in \mathbb{Z}$.

(b) Find the greatest common divisor $d = \gcd(602, 252)$ by using the Euclidean algorithm. Express d in the form $m \cdot 602 + n \cdot 252$ for some integers m and n.

Solution: Applying the Euclidean algorithm, we find that

$$\begin{aligned}
602 &= 252 \cdot 2 + 98 \\
252 &= 98 \cdot 2 + 56 \\
98 &= 56 \cdot 1 + 42 \\
56 &= 42 \cdot 1 + 14 \\
42 &= 14 \cdot 3 + 0
\end{aligned}$$

Thus $\gcd(602, 252) = 14$. Aplying this algorithm in the reverse order, we find that

$$\begin{aligned}
14 &= 56 - 42 \\
&= 56 - (98 - 56) \\
&= 2 \cdot 56 - 98 \\
&= 2 \cdot (252 - 98 \cdot 2) - 98 \\
&= 2 \cdot 252 - 5 \cdot 98 \\
&= 2 \cdot 252 - 5(602 - 252 \cdot 2) \\
&= 12 \cdot 252 - 5 \cdot 602.
\end{aligned}$$

We can pick $m = -5$ and $n = 12$.

3. (25pts) Consider the following sets of 3×3 matrices with entries from real numbers

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \quad \text{and} \quad H = \left\{ \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : d \in \mathbb{R} \right\}.$$

(a) Show that G is a group under the matrix multiplication.

Solution: We start with verifying the fact that the set G is closed under the matrix multiplication:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \tilde{a} & \tilde{b} \\ 0 & 1 & \tilde{c} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+\tilde{a} & b+\tilde{b}+a\tilde{c} \\ 0 & 1 & c+\tilde{c} \\ 0 & 0 & 1 \end{bmatrix}$$

Secondly, the matrix multiplication restricted to G is associative because the matrix multiplication has this property in general. Consider the element

$$I_3 = [\delta_{ij}]_{3\times 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in G.$$

Obviously $I_3 M = M I_3$ for each matrix $M \in G$. Thus there exists an identity element in G. Moreover each element of G has an inverse because

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} = I_3 = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

We conlude that G is a group with respect to the matrix multiplication.

(b) Is H a subgroup of G?

Solution: By picking $d = 0$, we find that $I_3 \in H$. We have

$$\begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & \tilde{d} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & d+\tilde{d} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore, the subset H is closed under the binary operation of G. Moreover for each element in G, we have

$$\begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & -d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in H.$$

We conclude that H is a subgroup of G.

4. (25pts) Consider the following set of 2×2 matrices

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_2 \text{ and } ad - bc \neq [0] \right\}$$

with entries from $\mathbb{Z}_2$, the set of congruence classes modulo 2. You are given that G is a group under the matrix multiplication. (Don't show that G is a group.)

(a) Write the elements of G and show that G has order six.

Solution: For simplicity, we use the notation $0 = [0]$ and $1 = [1]$. We have

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

(b) Is G an abelian group?

Solution: No! For example

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(c) Is G a cyclic group?

Solution: No! To see this, we note that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

There is no element generating the group G.