M E T U
Department of Mathematics

	Basic Algebraic Structures MIDTERM II	
Code : *Math 116* Acad. Year : *2018 Spring* Instructor : *A.Beyaz, G.Ercan, M.Kuzucuoğlu, Ö.Küçüksakallı F.Özbudak.* Date : *April 26, 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) Let $G = \langle a \rangle$ be a cyclic group generated by an element of order 28.

(a) Find all elements which generate G.

Solution: The generators of G are of the form a^k with $\gcd(28, k) = 1$ and $1 \leq k \leq 28$. All elements which generate G are

$$a^1, a^3, a^5, a^9, a^{11}, a^{13}, a^{15}, a^{17}, a^{19}, a^{23}, a^{25}, a^{27}.$$

(b) List all elements of the subgroup $\langle a^4 \rangle$ and determine their orders.

Solution: We have $\langle a^4 \rangle = \{a^0, a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24}\}$. Note that $|\langle a^4 \rangle| = 7$. An element of $\langle a^4 \rangle$ must have order dividing 7. Recall that the identity is the unique element with order 1. It follows that each element that is not identity must have order 7.

(c) What are the generators of the subgroup $\langle a^4 \rangle$?

Solution: The set of generators of $\langle a^4 \rangle$ consists of all the elements of $\langle a^4 \rangle$ except the identity element. More precisely, we have

$$\langle a^4 \rangle - \{a^0\} = \{a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24}\}.$$

There are 6 elements that generate $\langle a^4 \rangle$.

(d) Find all subgroups of G and determine their orders.

Solution: A subgroup of a cyclic group must be cyclic as well. So there is one-to-one correspondence between the positive divisors of 28 and the subgroups of G with the corresponding order. The positive divisors of 28 are $1, 2, 4, 7, 14$ and 28. The corresponding subgroups are $\langle a^{28} \rangle$, $\langle a^{14} \rangle$, $\langle a^7 \rangle$, $\langle a^4 \rangle$, $\langle a^2 \rangle$ and $\langle a^1 \rangle$, respectively.

2. (25pts) Let $\sigma = (1923)(1965)(1487)$ in S_9

(a) Express σ as a product of disjoint cycles .

Solution: We have $\sigma = (148723)(596)$

(b) Find the order of σ.

Solution: The permutation σ is a product of two disjoint cycles of lenghts 6 and 3. It follows that the order of σ is 6, the least common multiple of 6 and 3. Alternatively, note that $(148723)^k \neq (1)$ for $k = 1, 2, 3, 4, 5$ but $(148723)^6 = (1)$. It follows that the order of σ is at least 6. On the other hand $(596)^6 = (1)$, too. It follows that the order of σ is 6.

(c) Find σ^{183}.

Solution: From the previous part, we know that $\sigma^6 = (1)$. By using the division algorithm, we obtain $183 = 6 \cdot 30 + 3$. It follows that

$$\sigma^{183} = \sigma^{6\cdot 30+3} = (\sigma^6)^{30}\sigma^3 = \sigma^3.$$

By using the representation of σ in terms of disjoint cycles, we easily find that

$$\sigma^{183} = \sigma^3 = (17)(42)(83).$$

(d) Write σ as a product of transpositions. Is σ odd or even?

Solution: We have

$$\sigma = (1923) \cdot (1965) \cdot (1487) = [(13)(12)(19)] \cdot [(15)(16)(19)] \cdot [(17)(18)(14)]$$

or

$$\sigma = (148723) \cdot (596) = [(13)(12)(17)(18)(14)] \cdot [(56)(59)].$$

The element σ is odd since it can be written as a product of odd number of transpositions.

(e) If $\alpha = (1524) \in S_9$, then find the conjugate $\alpha\sigma\alpha^{-1}$.

We have

$$\begin{aligned}\alpha\sigma\alpha^{-1} &= [\alpha(1)\ \alpha(9)\ \alpha(2)\ \alpha(3)] \cdot [\alpha(1)\ \alpha(9)\ \alpha(6)\ \alpha(5)] \cdot [\alpha(1)\ \alpha(4)\ \alpha(8)\ \alpha(7)] \\ &= (5943) \cdot (5962) \cdot (5187) \\ &= (187435)(296).\end{aligned}$$

3. **(25pts)** Let G be the subset of $\mathbb{Z}_{16}$ which consists of elements with multiplicative inverses. You are given that G is a group under multiplication. Let H be the subgroup of G generated by $[7]$.

(a) Find the multiplication table of the quotient group G/H.

Solution: The elements of G can be represented by odd integers in between 1 and 16. More precisely, we have

$$G = \{[1], [3], [5], [7], [9], [11], [13], [15]\}.$$

Moreover $H = \langle [7] \rangle = \{[1], [7]\}$. There are 4 (left) cosets of H, namely:

$$[1]H = [7]H, \quad [3]H = [5]H, \quad [9]H = [15]H \quad \text{and} \quad [11]H = [13]H.$$

The multiplication table of the quotient group G/H is as follows:

$*$	$[1]H$	$[3]H$	$[9]H$	$[11]H$
$[1]H$	$[1]H$	$[3]H$	$[9]H$	$[11]H$
$[3]H$	$[3]H$	$[9]H$	$[11]H$	$[1]H$
$[9]H$	$[9]H$	$[11]H$	$[1]H$	$[3]H$
$[11]H$	$[11]H$	$[1]H$	$[3]H$	$[9]H$

(b) Determine whether G/H is isomorphic to $\mathbb{Z}_4$. Justify your answer.

Solution: The quotient group G/H is cyclic of order 4 and generated by $[3]H$ (or by $[11]H$). The group $\mathbb{Z}_4$ is also cyclic and generated by $[1]$ (or by $[3]$).

We can construct an isomorphism by sending the generator $[3]H \in G/H$ to the generator $[1] \in \mathbb{Z}_4$.

Consider the map $f : G/H \to \mathbb{Z}_4$ given by $([3]H)^k \mapsto k[1]$ for any integer k. The map $f : G/H \to \mathbb{Z}_4$ is easily verified to be a homomorphism since

$$f(([3]H)^{k+\ell}) = (k + \ell)[1] = k[1] + \ell[1].$$

Moreover this map is bijective since

$$[3]H \mapsto [1], \quad [9]H \mapsto [2], \quad [11]H \mapsto [3] \quad \text{and} \quad [1]H \mapsto [0].$$

We have proved that G/H is isomorphic to $\mathbb{Z}_4$ by the isomorphism $f : G/H \to \mathbb{Z}_4$.

4. (25pts) You are given that

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

is a ring with respect to the matrix addition and multiplication.

(a) Is R a commutative ring?

Solution: The ring R is commutative because

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} = \begin{bmatrix} ac & ad+bc \\ 0 & ac \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}.$$

(b) Does R have a unity?

Solution: The element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R$ satisfies

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

We conclude that the ring R has a unity .

(c) Is R an integral domain?

Solution: The R is not an integral domain because it has zero divisors. For example

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

even though

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

(d) Is R a field?

Solution: We claim that the element $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in R$ does not have a multiplicative inverse. Assume otherwise, then

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

for some real numbers a and b. On the other hand

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

This is a contradiction. The ring R has a nonzero element which does not have a multiplicative inverse. Thus R is not a field.