M E T U
Department of Mathematics

Group	BASIC ALGEBRAIC STRUCTURES MidTerm 2	List No.
Code : *Math 116* Acad. Year : *2017* Semester : *Spring* : Date : *May.11.2017* Time : *17:40* Duration : *100 minutes*	Last Name : Name : Student No. : Department : Section : Signature : 5 QUESTIONS ON 4 PAGES TOTAL 60 POINTS	

1	2	3	4	5	SHOW YOUR WORK	

Question 1. (16 points) Let G be the group of multiplicative invertible elements of $\mathbb{Z}_{28}$.

(a) (4 pts)List the elements of G and of its subgroup $\langle[3]\rangle$ spanned by $[3]$.

$G = \{[1],[3],[5],[9],[11],[13],[15],[17],[19],[23],[25],[27]\}$

$\langle[3]\rangle = \{[3],[9],[27],[25],[19],[1]\}$

(b) (4 pts)Find the cosets of $\langle[3]\rangle$ in G.

$o(G)=12$
$o([3])=6$ $\Rightarrow [G:\langle[3]\rangle]=2$

$\Rightarrow [5]\notin\langle[3]\rangle \quad [5]\langle[3]\rangle \neq \langle[3]\rangle$

$\Rightarrow \{\langle[3]\rangle, [5].\langle[3]\rangle\}$

(c) (4 pts)Find the multiplication table for the quotient group $G/\langle[3]\rangle$.

$G/\langle[3]\rangle$	$\langle[3]\rangle$	$[5]\langle[3]\rangle$
$\langle[3]\rangle$	$\langle[3]\rangle$	$[5]\langle[3]\rangle$
$[5]\langle[3]\rangle$	$[5]\langle[3]\rangle$	$\langle[3]\rangle$

(d) (4 pts) Is $G/\langle[3]\rangle$ cyclic? Explain your answer.

As $G/\langle[3]\rangle$ is of order 2, $G/\langle[3]\rangle \cong \mathbb{Z}_2$

So it is cyclic.

Question 2. **(12 points)** Let $R = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \text{ are real numbers} \right\}$

a)(4 pts) Is R a commutative ring? Explain your answer.

Hocam burada R'ın ring olduğunu söylememizi bekleyecek misiniz?

Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, B = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \in R$. Then

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

$$\begin{bmatrix} c & -d \\ d & c \end{bmatrix} \cdot \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} ca-db & -cb-da \\ da+cb & -db+ac \end{bmatrix}$$

As $AB = BA$ for all $A, B \in R$, R is a commutative ring.

b)(4 pts) Does R have a unity? If so identify the unity.

Consider $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. As it is of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ with $a=1$ & $b=0$, it is in R and $IA = AI$ for all $A \in M_2(\mathbb{R})$ hence in particular, for all $A \in R$. So R has a unity which is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

c)(4 pts) Is R an integral domain? Explain your answer.

Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, B = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \in R$ such that $AB = 0$.

$$AB = \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ iff } \begin{matrix} ac = bd \\ \& \\ ad = -bc \end{matrix}$$

$$\Rightarrow \begin{matrix} acd = bd^2 \\ acd = -bc^2 \end{matrix} \iff bd^2 = -bc^2 \iff bd^2 + bc^2 = 0 \iff b(d^2+c^2) = 0.$$

$\iff b = 0$ or $d^2+c^2 = 0$.

$d^2+c^2=0$ iff $d=c=0$ as $d, c \in \mathbb{R}$.

So R has no zero divisors.

As R is a comm ring with unity without zero divisors, it is an int. domain.

Question 3. (8 points) Prove that $\mathbb{Q}(i\sqrt{5}) = \{p + qi\sqrt{5} \mid p, q \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$.

① As $0 = 0 + 0.i\sqrt{2}$, $0 \in \mathbb{Q}(i\sqrt{5})$. So $\mathbb{Q}(i\sqrt{5}) \neq \emptyset$.

② Let $x, y \in \mathbb{Q}(i\sqrt{5})$. Then $x = p + qi\sqrt{5}$, $y = s + ti\sqrt{5}$, $p, q, s, t \in \mathbb{Q}$. Then $x - y = (p-s) + (q-s)i\sqrt{5}$ as $\mathbb{Q}$ is a ring.

$$x.y = (p + qi\sqrt{5}).(s + ti\sqrt{5})$$
$$= (ps - 5qt) + (pt + qs)i\sqrt{5} \in \mathbb{Q}(i\sqrt{5})$$

$\therefore$ $\mathbb{Q}(i\sqrt{5})$ is a subring of $\mathbb{C}$

Question 4. (12 points) Let R be a commutative ring and a be a fixed element of R. Let

$$I_a = \{x \in R \mid ax = 0\}.$$

(a) (6 pts) Show that I_a is a subring of R.

As $r.0 = 0$ for all $r \in R$, $a.0 = 0$. So $0 \in I_a \Rightarrow I_a \neq \emptyset$.

Let $x, y \in I_a$. Then $a.(x-y) = ax - ay = 0 - 0 = 0$

as $x \in I_a$, $ax = 0$ and $y \in I_a$, $ay = 0$

and hence $x - y \in I_a$. Also, $a(xy) = (ax).y = 0.y = 0$ which implies $xy \in I_a$. Hence I_a is a subring of R.

(b) (6 pts) Is I_a an ideal of R? Explain your answer.

I_a is an ideal iff I_a is a subring and for all $r \in R$ and $x \in I_a$, $rx, xr \in R$. As R is commutative, $rx = xr$ $\forall r \in R, x \in I_a$.

So enough to show $xr \in I_a$. For this,

$a(xr) = (ax).r = 0.r = 0$ Hence $xr = rx \in I_a$

As $x \in I_a$

$\therefore$ I_a is an ideal of R.

Question 5. (12 points) Let $[a]_n$ denote the congruence class of the integer a modulo n.

(a) (6 pts) Show that the map $f : \mathbb{Z}_{12} \to \mathbb{Z}_4$ that sends $[a]_{12}$ to $[a]_4$ is a surjective (onto) ring homomorphism.

Let $[x]_{12}, [y]_{12} \in \mathbb{Z}_{12}$. Then

$$\theta([x]_{12} \cdot [y]_{12}) = \theta([xy]_{12}) = [xy]_4 = [x]_4 [y]_4 = \theta([x]_{12})\,\theta([y]_{12}).$$

and

$$\theta([x]_{12} + [y]_{12}) = \theta([x+y]_{12}) = [x+y]_4 = [x]_4 + [y]_4 = \theta([x]_{12}) + \theta([y]_{12}).$$

Hence, θ is a ring homomorphism.

Let $[x]_4 \in \mathbb{Z}_4$. Then as $\theta([4x]_{12}) = [x]_4$,

θ is onto.

Hence, θ is a surjective ring homomorphism.

(b) (6 pts) Find the kernel of f.

$$\ker\theta = \{[x]_{12} \in \mathbb{Z}_{12} \mid \theta([x]_{12}) = [0]_4\}$$
$$= \{[x]_{12} \in \mathbb{Z}_{12} \mid [x]_4 = [0]_4\}.$$
$$= \{[0]_{12}, [4]_{12}, [8]_{12}\}$$