me TAHA AMEEN, ID 66555 Taha + Muhannad + Reem

 © copyright Ayman Badawi 2017

HW IV: MTH 420, Spring 2018

27/30

Ayman Badawi

JESTION 1. Let A be a commutative ring such that $Char(A) = n \neq 0$.

) Prove that $na = 0$ for every $a \in A$. 5

) (Freshman Dream :)) Suppose that n is a prime number. Prove that $(a+b)^{n^m} = a^{n^m} + b^{n^m}$ for every $a, b \in A$ and for every positive integer $m \geq 1$. (Hint: Use math induction and (i)) 7

JESTION 2. Let P be a prime ideal of a commutative ring A, and let $L = \{f(x) \in A[x] \mid f(0) \in P\}$. Prove that L is rime ideal of $A[x]$. If P is a maximal ideal of A, prove that $A[x]/L$ is a field. 10

JESTION 3. (i) 5 Let $A = \begin{bmatrix} 2 & 2 & 3 \\ 3 & 1 & 2 \\ 3 & 3 & 4 \end{bmatrix} \in R^{3\times 3}(Z_5)$. Find A^{-1}. (hint: recall from class that 2/3, 1/4, ..., have meanings in Z_5. Also note that -2/3 has a meaning!. So, think of A as a matrix with entries from Q. Use MTH 220 (row operation) and find A^{-1} and then change the entries of A^{-1} to entries in Z_5)

) Find all solutions of the following system over Z_7 (again..solve it over Q as in MTH 220...then over Z_7) (Hint: we must have finitely many solutions)

$$x_1 + x_2 + 2x_3 = 4$$
$$6x_1 + 5x_3 = 2$$
$$6x_1 + x_2 + 5x_3 = 1$$

culty information

nan Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
iail: abadawi@aus.edu, www.ayman-badawi.com

ANSWER 1: Given char$(A) = n \neq 0$.

(i) To Prove: $na = 0 \quad \forall a \in A$.

Proof: Since char$(A) = n$, $n * 1 = 0$

$\therefore \quad na = n(1 * a) = (n * 1) * a = 0 * a = 0$ ■

(ii) Given: n is prime.

To Prove: $(a+b)^{n^m} = a^{n^m} + b^{n^m} \quad \forall m \geq 1 \in \mathbb{Z}$

Proof: By Mathematical Induction:

→ Let $P(m)$: $(a+b)^{n^m} = a^{n^m} + b^{n^m}$.

• $\underline{\underline{m = 1}}$ $\quad P(1)$: $(a+b)^n \overset{?}{=} a^n + b^n$.

$$(a+b)^n = a^n + \sum_{j=1}^{n-1} \frac{n!}{(n-j)!\, j!} a^{n-j} b^j + b^n$$

But: NONE of the Prime factors of $j!$ OR $(n-j)!$ divide n ($\because n$ is prime). ($\because$ 'n' is never cancelled in the sum)

$$\therefore \frac{n!}{(n-j)!\, j!} = n * k_j, \quad \text{where } k_j = \frac{(n-1)!}{(n-j)!\, j!}$$

$$\therefore (a+b)^n = a^n + \sum_{j=1}^{n-1} n * k_j * (a^{n-j} b^j) + b^n$$

$$= a^n + \sum_{\forall j} k_j * (n * c_j) + b^n \quad \text{where } c_j \in A.$$

$$= a^n + \sum_{\forall j} 0 + b^n = a^n + b^n \quad \Big| \because n c_j = 0 \ \forall j$$

- Assume $P(m)$ is true

$$\therefore (a+b)^{n^m} = a^{n^m} + b^{n^m}$$

- $P(m+1)$: To show: $(a+b)^{n^{m+1}} = a^{n^{m+1}} + b^{n^{m+1}}$

$$(a+b)^{n^{m+1}} = (a+b)^{n^m * n} = \left[(a+b)^{(n^m)}\right]^n = \left[a^{n^m} + b^{n^m}\right]^n$$

But: Since $(x+y)^n = x^n + y^n$, let $x = a^{n^m}$ and $y = b^{n^m}$

$$\therefore \left(a^{n^m} + b^{n^m}\right)^n = \left(a^{(n^m)}\right)^n + \left(b^{(n^m)}\right)^n = a^{n^m n} + b^{n^m n}$$
$$= a^{n^{m+1}} + b^{n^{m+1}} \blacksquare$$

ANSWER 2: Given: P is a Prime Ideal of A.

$$L = \{f(x) \in A[x] \mid f(0) \in P\}$$

(i) To Prove: L is a prime Ideal of $A[x]$

Proof: Let $f(x) * g(x) \in L$.

$\therefore f(0) * g(0) \in P$ (by definition)

But P is prime $\Longrightarrow f(0) \in P$ (or) $g(0) \in P$.

$\therefore f(x) \in L$ (or) $g(x) \in L$

$\therefore L$ is prime $\blacksquare$

(ii) To Prove: If P is a Maximal Ideal of A, then $A[x]/L$ is a field.

Proof: Since P is Maximal in A, $\frac{A}{P}$ is a field —(i)

Consider the ring homomorphism:

$$\phi : A[x] \longrightarrow A/P \quad \text{s.t. } \phi(f(x)) = f(0) + P$$

This is a homomorphism.

$\because \phi(f(x)+g(x)) = f(0)+g(0)+P = (f(0)+P)+(g(0)+P) = \phi(f(x))+\phi(g(x))$

and $\phi(f(x)*g(x)) = f(0)*g(0)+P = (f(0)+P)*(g(0)+P) = \phi(f(x))*\phi(g(x))$

$\rightarrow$ Image$(f) = A/P$

$\because \forall\ a+P \in A/P$, $\exists\ g(x) = x\,l(x)+a$ s.t. $\phi(g(x)) = a+P$

$\rightarrow$ Ker$(f) = L$ $\quad \Big| \because L = \{f(x)\in A[x] \mid f(0)\in P\}$.

$\therefore \phi(f(x)) = f(0)+P = P$.

$\therefore \dfrac{A[x]}{L} \cong A/P$ by first Isomorphism Theorem.

$\therefore \dfrac{A[x]}{L}$ is a field $\blacksquare$

ANSWER 3 (i) $A = \begin{pmatrix} 2 & 2 & 3 \\ 3 & 1 & 2 \\ 3 & 3 & 4 \end{pmatrix}$. To Find: A^{-1}!

$$\left(\begin{array}{ccc|ccc} 2 & 2 & 3 & 1 & 0 & 0 \\ 3 & 1 & 2 & 0 & 1 & 0 \\ 3 & 3 & 4 & 0 & 0 & 1 \end{array}\right) \xrightarrow{R_2 - R_1 \to R_2} \left(\begin{array}{ccc|ccc} 2 & 2 & 3 & 1 & 0 & 0 \\ 1 & -1 & -1 & -1 & 1 & 0 \\ 3 & 3 & 4 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_1 \leftrightarrow R_2} \left(\begin{array}{ccc|ccc} 1 & -1 & -1 & -1 & 1 & 0 \\ 2 & 2 & 3 & 1 & 0 & 0 \\ 3 & 3 & 4 & 0 & 0 & 1 \end{array}\right) \xrightarrow[3R_1 - R_3 \to R_3]{2R_1 - R_2 \to R_2} \left(\begin{array}{ccc|ccc} 1 & -1 & -1 & -1 & 1 & 0 \\ 0 & -4 & -5 & -3 & 2 & 0 \\ 0 & -6 & -7 & -3 & 3 & -1 \end{array}\right)$$

$$\xrightarrow{-\frac{1}{4}R_2 \to R_2} \left(\begin{array}{ccc|ccc} 1 & -1 & -1 & -1 & 1 & 0 \\ 0 & 1 & 5/4 & 3/4 & -1/2 & 0 \\ 0 & -6 & -7 & -3 & 3 & -1 \end{array}\right) \xrightarrow[6R_2 + R_3 \to R_3]{R_1 + R_2 \to R_1} \left(\begin{array}{ccc|ccc} 1 & 0 & 1/4 & -1/4 & 1/2 & 0 \\ 0 & 1 & 5/4 & 3/4 & -1/2 & 0 \\ 0 & 0 & 1/2 & 3/2 & 0 & -1 \end{array}\right)$$

$$\xrightarrow{\frac{4}{2}R_3 \to R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 1/4 & -1/4 & 1/2 & 0 \\ 0 & 1 & 5/4 & 3/4 & -1/2 & 0 \\ 0 & 0 & 1 & 3 & 0 & -2 \end{array}\right) \xrightarrow[-\frac{1}{4}R_3 + R_1 \to R_1]{-\frac{5}{4}R_3 + R_2 \to R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 1/2 & 1/2 \\ 0 & 1 & 0 & -3 & -1/2 & 5/2 \\ 0 & 0 & 1 & 3 & 0 & -2 \end{array}\right)$$

$\therefore$ In $\mathbb{Q}$, $A^{-1} = \begin{pmatrix} -1 & 1/2 & 1/2 \\ -3 & -1/2 & 5/2 \\ 3 & 0 & -2 \end{pmatrix}$

$\therefore$ In $R^{3\times3}(\mathbb{Z}_5)$ $\quad A^{-1} = \begin{pmatrix} 4 & 3 & 3 \\ 2 & 2 & 0 \\ 3 & 0 & 3 \end{pmatrix}$

Verify: $A * A^{-1} = \begin{pmatrix} 2 & 2 & 3 \\ 3 & 1 & 2 \\ 3 & 3 & 4 \end{pmatrix}\begin{pmatrix} 4 & 3 & 3 \\ 2 & 2 & 0 \\ 3 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 21 & 10 & 15 \\ 20 & 11 & 15 \\ 30 & 15 & 21 \end{pmatrix}$ in $R^{3\times3}(\mathbb{Q})$

$= I_{3\times3}$ in $R^{3\times3}(\mathbb{Z}_5)$

(iii) Matrix Representation in $\mathbb{Q}$:

$\begin{pmatrix} 1 & 1 & 2 \\ 6 & 0 & 5 \\ 6 & 1 & 5 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 6 & 0 & 5 \\ 6 & 1 & 5 \end{pmatrix}^{-1}\begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix}$

(See next page)

$\therefore \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 6 & 0 & 5 & 0 & 1 & 0 \\ 6 & 1 & 5 & 0 & 0 & 1 \end{array}\right) \xrightarrow[6R_1 - R_3 \to R_3]{6R_1 - R_2 \to R_2} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 6 & 7 & 6 & -1 & 0 \\ 0 & 5 & 7 & 6 & 0 & -1 \end{array}\right) \xrightarrow{R_2 - R_3 \to R_2} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 5 & 7 & 6 & 0 & -1 \end{array}\right)$

$\xrightarrow[-5R_2 + R_3 \to R_3]{-R_2 + R_1 \to R_1} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 1 & -1 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 7 & 6 & 5 & -6 \end{array}\right) \xrightarrow{\frac{R_3}{7} \to R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 1 & -1 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & \frac{6}{7} & \frac{5}{7} & \frac{-6}{7} \end{array}\right)$

$\xrightarrow{-2R_3 + R_1 \to R_1} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -5/7 & -3/7 & 5/7 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 6/7 & 5/7 & -6/7 \end{array}\right)$ $\quad \therefore \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \frac{-5}{7} & \frac{-3}{7} & \frac{5}{7} \\ 0 & -1 & 1 \\ \frac{6}{7} & \frac{5}{7} & \frac{-6}{7} \end{pmatrix}\begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix}$

$\therefore \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -3 \\ -1 \\ 4 \end{pmatrix}$ in $\mathbb{Q}$

$\therefore \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \\ 4 \end{pmatrix}$ in $R^{3\times3}(\mathbb{Z}_7)$

Question 3.

$2^{-1} = 4 \qquad -2 = 5$
$3^{-1} = 5 \qquad -3 = 4$
$6^{-1} = 6 \qquad -6 = 1$

(ii) $x_1 + x_2 + 2x_3 = 4$
$6x_1 \quad + 5x_3 = 2$
$6x_1 + x_2 + 5x_3 = 1$

$$\left[\begin{array}{ccc|c} 1 & 1 & 2 & 4 \\ 6 & 0 & 5 & 2 \\ 6 & 1 & 5 & 1 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 1 & 2 & 4 \\ 0 & 1 & 0 & 6 \\ 0 & 2 & 0 & 5 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 1 & 2 & 4 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$$\to \left[\begin{array}{ccc|c} 1 & 0 & 2 & 5 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 0 \end{array}\right] \qquad \left.\begin{array}{l} x_3 = x_3 \\ x_2 = 6 \\ x_1 = 5 - 2x_3 \end{array}\right\} \text{for } x_3 \in \mathbb{Z}_7$$

we get $(5, 6, 0)$, $(3, 6, 1)$, $(1, 6, 2)$,
$(6, 6, 3)$, $(4, 6, 4)$, $(2, 6, 5)$,
$(0, 6, 6)$

✓ Good