MATH321 Tutorial 2

Emma Hogan

53837798

March 12, 2020

Question 1

Show that char($\mathbb{Z}_m \oplus \mathbb{Z}_n$) is the least common multiple of m and n.

First we show that $n = char(\mathbb{Z}_n)$:

n is the lowest positive integer such that $n * 1 = 0$ in $\mathbb{Z}_n$. Also, $\forall a \in \mathbb{Z}_n$, $n * a = 0$.

Therefore $char(\mathbb{Z}_n) = n$.

We want the lowest possible k so that $\forall a \in \mathbb{Z}_m, \subsetneq \mathbb{Z}_n$:

$$\begin{aligned} char(\mathbb{Z}_m \oplus \mathbb{Z}_n) &= k \\ k(a,b) = (ka, kb) &= (0,0) \\ \implies ka &= 0 \\ \implies kb &= 0 \end{aligned}$$

k must be a multiple of m and a multiple of n so that

$$\begin{aligned} k * 1 = 0 \in \mathbb{Z}_m \\ k * 1 = 0 \in \mathbb{Z}_n \end{aligned}$$

So the lowest value k could possible hold is $lcm(m,n)$. Let $k = lcm(m,n)$, with $k = xn$ and $k = ym$. We now show this is sufficient.

$$(ka, kb) = (x * n * a, y * m * b) = (x * 0, y * 0) = (0,0)$$

So $char(\mathbb{Z}_m \oplus \mathbb{Z}_n) = lcm(m,n)$.

Question 2

Determine whether $3x^2 + 6x - 6$ is irreducible over $\mathbb{Z}$; over $\mathbb{Q}$; over $\mathbb{Z}_5$; over $\mathbb{Z}_{11}$.

Let $f(x) = 3x^2 + 6x - 6$.

Over $\mathbb{Z}$:

3 is not a unit in $\mathbb{Z}$ so $f(x)$ is reducible because a factor of 3 can be taken out.

Over $\mathbb{Q}$:

$\mathbb{Q}$ is a field, so since $f(x)$ has no zeroes in $\mathbb{Q}$, it is irreducible.

Over $\mathbb{Z}_5$:

$\mathbb{Z}_5$ is a field, so since $f(x)$ has no zeroes in $\mathbb{Z}_5$, it is irreducible.

Over $\mathbb{Z}_{11}$:

$f(x)$ has zeroes $x = 4$ and $x = 5$ in $\mathbb{Z}_{11}$, so $f(x)$ is reducible over $\mathbb{Z}_{11}$.

Question 3

Consider the map $\varphi : \mathbb{Z}[\sqrt{(5)}] \to M_2(\mathbb{Z})$ given by $\varphi(m + n\sqrt{(5)} = \begin{bmatrix} m & 5n \\ n & m \end{bmatrix}$.

(a) Verify that φ is a ring homomorphism.

Checking φ is additive:

$$\begin{aligned}
\varphi(m_1 + n_1\sqrt{5}) + \varphi(m_2 + n_2\sqrt{5}) &= \begin{bmatrix} m_1 & 5n_1 \\ n_1 & m_1 \end{bmatrix} + \begin{bmatrix} m_2 & 5n_2 \\ n_2 & m_2 \end{bmatrix} \\
&= \begin{bmatrix} m_1 + m_2 & 5n_1 + 5n_2 \\ n_1 + n_2 & m_1 + m_2 \end{bmatrix} \\
&= \begin{bmatrix} m_1 + m_2 & 5(n_1 + n_2) \\ n_1 + n_2 & m_1 + m_2 \end{bmatrix} \\
&= \varphi(m_1 + m_2 + (n_1 + n_2)\sqrt{5}) \\
&= \varphi((m_1 + n_1\sqrt{5}) + (m_2 + n_2\sqrt{5}))
\end{aligned}$$

So φ is additive. Checking φ is multiplicative:

$$\begin{aligned}
\varphi(m_1 + n_1\sqrt{5}) * \varphi(m_2 + n_2\sqrt{5}) &= \begin{bmatrix} m_1 & 5n_1 \\ n_1 & m_1 \end{bmatrix} * \begin{bmatrix} m_2 & 5n_2 \\ n_2 & m_2 \end{bmatrix} \\
&= \begin{bmatrix} m_1m_2 + 5n_1n_2 & 5m_15n_2 + 5m_2n_1 \\ m_2n_1 + m_1n_2 & 5n_1n_2 + m_1m_2 \end{bmatrix} \\
&= \begin{bmatrix} m_1m_2 + 5n_1n_2 & 5(m_1n_2 + n_1m_2) \\ m_1n_2 + n_1m_2 & m_1m_2 + 5n_1n_2 \end{bmatrix} \\
&= \varphi((m_1m_2 + 5n_1n_2) + (m_1n_2 + n_1m_2)\sqrt{5}) \\
&= \varphi((m_1 + n_1\sqrt{5}) * (m_2 + n_2\sqrt{5}))
\end{aligned}$$

So φ is multiplicative. Therefore, φ is a homomorphism.

(b) $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} | a, b, c \in \mathbb{Z} \right\}$ is a subring of $M_2(\mathbb{Z})$. Find $\varphi^{-1}(S)$.

I don't understand how to do this question. φ only maps onto elements of S that have $b = 0$, so how can I take φ^{-1} over all S?

Question 4

Let R and S be rings. Show that $R \oplus S$ and $S \oplus R$ are isomorphic.

Define $\varphi : R \oplus S \to S \oplus R$ by

$$\varphi((a, b)) = (b, a)$$

φ is additive because:

$$\begin{aligned}\varphi((a_1, b_1) + (a_2, b_2)) &= \varphi((a_1 + a_2, b_1 + b_2)) \\ &= (b_1 + b_2, a_1 + a_2) \\ &= (b_1, a_1) + (b_2, a_2) \\ &= \varphi(a_1, b_2) + varphi(a_2, b_2)\end{aligned}$$

φ is multiplicative because:

$$\begin{aligned}\varphi((a_1, b_1) * (a_2, b_2)) &= \varphi((a_1a_2, b_1b_2)) \\ &= (b_1b_2, a_1a_2) \\ &= (b_1, a_1) * (b_2, a_2) \\ &= \varphi(a_1, b_1) * \varphi(a_2, b_2)\end{aligned}$$

Therefore, φ is a homomorphism. Clearly it is also both one-to-one and onto, so φ is an isomorphism. Since there exists an isomorphis between $R \oplus S$ and $S \oplus R$, they are isomorphic.