Question 1

Show that two rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

Solution: There is no element in $\mathbb{Z}[x]$ such that $a + a = 1$. This is because for $a \in \mathbb{Z}[x]$, it follows that

$$a + a = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (a_i + a_i) x^i$$

If $a + a = 1$, then $a_0 + a_0 = 1$ for $a_0 \in \mathbb{Z}$. However, there is no such element in $\mathbb{Z}$.

But there is such an element in $\mathbb{Q}[x]$, which is $\frac{1}{2}x^0$.

Question 2

Let R and S be nonzero rings and let $\phi : R \to S$ be a nonzero ring homomorphism (so $\phi(1_R) = 1_S$, where 1_R and 1_S denote the identities of R and S, respectively).
Show that $\phi(u)$ is a unit in S and $\phi(u^{-1}) = \phi(u)^{-1}$ for each unit u of R.

Solution: Let u be a unit of R, then it follows that there is an element u^{-1} such that $uu^{-1} = u^{-1}u = 1_R$. Since ϕ is an homomorphism, then, $\phi(ab) = \phi(a)\phi(b)$ for any element $a, b \in R$ by definition. This means that $1_S = \phi(1_R) = \phi(uu^{-1}) = \phi(u)\phi(u^{-1})$, and similarly, $1_S = \phi(1_R) = \phi(u^{-1}u) = \phi(u^{-1})\phi(u)$.

As $\phi(u)\phi(u^{-1}) = 1_S = \phi(u^{-1})\phi(u)$, then $\phi(u^{-1}) = \phi(u)^{-1}$ by definition.

Question 3

In problem 2, prove that if $\phi(1_R) \neq 1_S$ then $\phi(1_R)$ is a zero divisor in S.

Solution: Since $1_S \in S$ and $\phi(1_R) \in S$, then

$$1_S\phi(1_R) = 1_S\phi(1_R \cdot 1_R) = 1_S\phi(1_R)\phi_(1_R) = \phi(1_R)\phi(1_R)$$

Which is that $1_S\phi(1_R) - \phi(1_R)\phi(1_R) = 0$, or $(1_S - \phi(1_R))\phi(1_R) = 0$. If $\phi(1_R) \neq 1_S$, then $1_S - \phi(1_R) \neq 0$. And $\phi(1_R) \neq 0$ since if $1_R = 0$, then $\phi(x) = \phi(1_R x) = 0\phi(x) = 0$ which means that ϕ is a zero homomorphism.

But as $\phi(1_R)(1_S - \phi(1_R)) = 0$ while both terms are non-zero, it must be the case that $\phi(1_R)$ is a zero-divisor.

Question 4

Let R be a ring. Prove that the center of the ring $M_n(R)$ is the set of all scalar matrices aI, where I is the identity matrix and a is an element of the center of R.

Solution: Consider if $a \in Z(R)$, then a commutes with every element in R, so

$$\begin{bmatrix} a & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a \end{bmatrix} \begin{bmatrix} b_{11} & \cdots & b_{n1} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix} = \begin{bmatrix} ab_{11} & \cdots & ab_{1n} \\ \vdots & \ddots & \vdots \\ ab_{n1} & \cdots & ab_{nn} \end{bmatrix} = \begin{bmatrix} b_{11}a & \cdots & b_{1n}a \\ \vdots & \ddots & \vdots \\ b_{n1}a & \cdots & b_{nn}a \end{bmatrix} = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix} \begin{bmatrix} a & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a \end{bmatrix}$$

Therefore, aI is an element of $Z(M_n(R))$.

Now, consider an element A of $Z(M_n(R))$, then $AB = BA$ for all $B \in M_n(R)$.

$$\text{Let consider arbitrary } A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \text{ and } B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix}$$

Then, $(AB)_{ik} = \sum_{j=0}^{n} a_{ij}b_{jk}$ and $(BA)_{ik} = \sum_{j=0}^{n} b_{ij}a_{jk}$. Therefore, if $A \in Z(M_n(R))$, then it must follow that

$$\sum_{j=0}^{n} a_{ij}b_{jk} = \sum_{j=0}^{n} b_{ij}a_{jk} \text{ for any } B \in Z(R)$$

Since b is arbitrary, consider if $B = bI$, for any $b \in R$ and $b \notin Z(R)$, then this yields

$$\begin{bmatrix} a_{11}b & \cdots & a_{1n}b \\ \vdots & \ddots & \vdots \\ a_{n1}b & \cdots & a_{nn}b \end{bmatrix} = \begin{bmatrix} ba_{11} & \cdots & ba_{1n} \\ \vdots & \ddots & \vdots \\ ba_{n1} & \cdots & ba_{nn} \end{bmatrix}$$

So, $a_{ij}b = ba_{ij}$, but since b is arbitrary, then $a_{ij} \in Z(R)$ for any i, j.

Therefore it must follow that $\sum_{j=0}^{n} a_{ij}b_{jk} = \sum_{j=0}^{n} b_{ij}a_{jk} = \sum_{j=0}^{n} a_{jk}b_{ij}$.

Now, if B were chosen so that $b_{jk} = b_{ij} = 0$ except for $b_{ij'} \neq b_{j'k}$ only at certain j', then

$$a_{ij'}b_{j'k} = \sum_{j \neq j'} a_{ij}b_{ij} + a_{ij'}b_{j'k} = \sum_{j=0}^{n} a_{ij}b_{ij} = \sum_{j=0}^{n} a_{jk}b_{ij} = \sum_{j \neq j'} a_{jk}b_{ij} + a_{j'k}b_{ij'} = a_{j'k}b_{ij'}$$

If $i = j' = k$, then $a_{j'j'}b_{j'j'} = a_{j'j'}b_{j'j'}$ trivially, But otherwise, since $b_{ij'} \neq b_{j'k}$, it must be the case that $a_{ij'} = a_{j'k} = 0$ Thus, A must be diagonal.

Then consider $b_{ij} = 1$ for all entries. So,

$$\begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{bmatrix} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_1 \\ \vdots & \ddots & \vdots \\ a_n & \cdots & a_n \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_n \\ \vdots & \ddots & \vdots \\ a_1 & \cdots & a_n \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{bmatrix}$$

Which, by considering the element in the i^{th} row and j^{th} column, yeilds $a_i = a_j$. Which means that $a_1 = a_2 = \cdots = a_n$. So, $A = aI$ for some $a \in Z(R)$

Question 5

Let R be a commutative ring. Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $f(x)$ is nilpotent in $R[x]$ if and only if $a_0, a_1, \ldots, a_n$ are nilpotent elements of R.

Solution:

$(\Longrightarrow)$:

> **Claim 1**
>
> If a and b are nilpotent, then $a - b$ is nilpotent.
>
> ***Proof:*** If a and b are nilpotent, then let m be an integer such that $a^m = b^m = 0$, Then $(a-b)^{2m} = a^{2m} - \binom{2m-1}{1} a^{2m-1}b + \cdots + b^{2m}$. And since each term contain either a^m or b^m. Therefore, all the terms are zero. Thus, $(a-b)^{2m} = 0$. So, $a - b$ is nilpotent. □

Assume that $f_k(x)$ be a degree k nilpotent polynomial such that $f_k(x)^m = 0$. For induction, assume that $f_{k-1}(x)$ is nilpotent implies $a_{k-1}, \ldots, a_0$ are all nilpotent, then

$$f_k(x)^m = (a_kx^k + f_{k-1}(x))^m = (a_k^m x^k m + f_{k-1}(x)^m)$$

Therefore, $a_k^m x^k m = 0$ follows, so, a_k must be nilpotent. This means that $f_k(x)$ is nilpotent implies a_k is nilpotent and $f_k(x) - a_kx^k$ is nilpotent by claim. So, by the induction hypothesis, $a_k, a_{k-1}, \ldots a_0$ are all nilpotent. Note that if $f_0(k) = a_0$ is nilpotent, then a_0 is nilpotent trivially.

Therefore, if $f(x)$ is nilpotent, then $a_0, a_1, \ldots a_n$ are all nilpotent.

$(\Longleftarrow)$:

If $a_0, \ldots, a_n$ are all nilpotent, then there is an integer m such that $a_0^m = a_1^m = \cdots = a_n^m$. Now, consider $(a_nx^n + \cdots + a_0)^{nm}$. The coefficients of x^k is a summation of all product that contains $a_n^{i_n} \cdots a_0^{i_0}$ for which $\sum_{j=0}^{n} ji_j = k$ and $\sum_{j=0}^{n} i_j = nm$

But since $\sum_{j=0}^{n} i_j = nm$ then by pigeon hole principle, there must be at least one j such that $i_j \geq m$ Therefore, the product

$$a_n^{i_n} \cdots a_0^{i_0} = a_n^{i_n} \cdots a_j^{i_j} \cdots a_0^{i_0} = a_n^{i_n} \cdots 0 \cdots a_n^{i_n} = 0$$

So the coefficient of x^k is a summation of all products, which are all zeros, so the coefficient of x^k is zero, for any k.

Therefore, $(a_n x^n + \cdots + a_0)^{nm} = 0$, so $a_n x^n + \cdots + a_0$ is nilpotent.

Question 6

Let R be a commutative ring. Let $g(x)$ be a nonzero polynomial in $R[x]$. Prove that $g(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ such that $b \cdot g(x) = 0$.

Solution:

($\Longrightarrow$):

Let $g(x)$ be a nonzero polynomial, written $g(x) = g_0 + \cdots + g_n x^n$ and $g(x)f(x) = 0$ for f with smallest degree. Assume that degree of f is greater than 0. Let that degree of f be m. Then consider $f(x) = f_0 + f_1 x + \cdots + f_m x^m$.

If, for every i, $g_i x^i \cdot f(x) = 0$, then $g_i x^i \cdot f_m x^m = 0$, so $g(x) \cdot f_m = 0$. So, the statement was proved. Otherwise, let i be the highest degree such that $g_i x^i \cdot f(x) \neq 0$. So,

$$g(x)f(x) = (g_0 + \cdots + g_i x^i + \cdots + g_n x^n)(f_0 + \cdots + f_m x^m) = (g_0 + \cdots + g_i x^i)(f_0 + \cdots + f_m x^m)$$

But then, $g(x)f(x) = 0$ implies that $g_i f_m = 0$. So, $g_i f(x) = g_i f_0 + \cdots + g_i f_m x^m = g_i f_0 + \cdots + g_i f_{m-1} x^{m-1}$ is a degree $m-1$ polynomial.

This means that $g(x) g_i f(x) = 0$, but $g_i f(x)$ is a degree $m-1$ polynomial, contradicting that f is the smallest degree. Therefore, f must be a degree 0 polynomial, or simply $g(x) f_0 = 0$ for some $f_0 \in R$.

($\Longleftarrow$):

if $b \in R$, then $b = bx^0 \in R[x]$. So, if $b \cdot g(x) = 0$, then $g(x)$ is a zero-divisor.

Question 7

Let R be a commutative ring. Let $R[[x]$ be formal power series in the indeterminate x with coefficients in R. Show that $1 - x$ is a unit in $R[[x]]$.

Solution: Consider an element $p = \sum_{i=0}^{\infty} x^i = 1 + x + x^2 + \cdots$. Then

$$p(1-x) = (1-x)p = 1 - x + x - x^2 + x^2 - \cdots = 1 - (0) - (0) - \cdots = 1$$

So, p is the inverse of $1 - x$. Thus, $1 - x$ is a unit.

Question 8

In problem 7, prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Solution:

($\Longrightarrow$):

If $\sum_{n=0}^{\infty} a_n x^n$ have an inverse, then $(\sum_{n=0}^{\infty} a_n x^n)(\sum_{n=0}^{\infty} b_n x^n) = 1$. Then the constant term of the equality is $a_0 \times b_0 = 1$ Therefore, a_0 must be a unit in R

($\Longleftarrow$):

If a_0 is a unit, then there exists b such that $a_0 b = 1$. Then assume that a degree n polynomial with the constant term being a_0 is a unit for induction. This holds for $n = 0$. Let that degree n polynomial be $f(x)$, and $b \in R[[x]]$ such that $b \cdot f(x) = 1$ then

$$\begin{aligned}
(f(x) + a_{n+1}x^{n+1}) \cdot (b - b^2 a_{n+1} x^{n+1} + b^3 a_{n+1}^2 x^{(n+1)2} + \cdots) \\
&= bf(x) \ + \ ba_{n+1}x^{n+1} \ - \ bba_{n+1}f(x)x^{n+1} \ - \ bba_{n+1}^2 x^{(n+1)2} \ + \ \cdots \\
&= 1 \ + \ ba_{n+1}x^{n+1} \ - \ ba_{n+1}x^{n+1} \ - \ b^2 a_{n+1}^2 x^{(n+1)2} \ + \ \cdots \\
&= 1 \ + \ 0 + \cdots \ 0 \ \cdots \\
&= 1
\end{aligned}$$

Now, as $b - b^2 a_{n+1} x^{n+1} + b^3 a_{n+1}^2 x^{(n+1)2} + \cdots$ is an element of $R[[x]]$, then the argument holds for a polynomial of degree $n+1$. Thus, the argument holds for any element of $R[[x]]$ by induction.

Question 9

Prove that if R is an integral domain, then the ring of formal power series $R[[x]]$ is also an integral domain.

Solution: If $R[[x]]$ is not an integral domain, then there is a zero-divisor. Let there be nonzero elements A, B such that $A = \sum_{i=0}^{\infty} a_n x^n$ and $B = \sum_{i=0}^{\infty} b_n x^n$ and $AB = 0$

As A and B are nonzero, let $A = A' x^{k_a}$ and $B = B' x^{k_b}$ for which k_a and k_b is the smallest non-zero term of A and B. There exist this number by the well-ordering principle.

So,

$$0 = (\sum_{i=0}^{\infty} a_n x^n)(\sum_{i=0}^{\infty} b_n x^n) = (a_{k_a} b_{k_b} + a_{k_a+1} b_{k_b} x + b_{k_b+1} a_{k_a} x + \cdots) x^{k_a + k_b}$$

Hence, $a_{k_a} \cdot b_{k_b} = 0$, which means that $a_{k_a} \in R$ is a zero-divisor since $a_{k_a} \neq 0$, and $b_{k_b} \neq 0$ by construction, thus R is not an integral domain. So, the argument is proved by contraposition.

Question 10

Let R be a commutative ring. Let $G = \{ g_1, \ldots g_n \}$ be a finite group. Prove that the element $N = g_1 + g_2 + \cdots + g_n$ is in the center of the group ring RG

Solution: As $RG = \left\{ \sum_g r_g \cdot g \mid \forall r \right\}$, then let $N = g_1 + g_2 + \cdots + g_n$. Consider an arbitrary element $a = \sum_g r_g \cdot g = r_1 g_1 + \cdots + r_n g_n$. Then,

$$\begin{aligned}
Na &= N(r_1 g_1 + \cdots + r_n g_n) \\
&= (g_1 + \cdots g_n)(r_1 g_1 + \cdots + r_n g_n) \\
&= r_1 g_1 g_1 + \cdots + r_1 g_1 g_n + r_2 g_2 g_1 + \cdots + r_2 g_2 g_n + \cdots + r_n g_n g_n \\
&= r_1 g_1 g_1 + r_2 g_2 g_1 + \cdots + r_n g_n g_1 + \cdots + r_n g_n g_n \\
&= (r_1 g_1 + \cdots + r_n g_n)(g_1 + \cdots + g_n) \\
&= aN
\end{aligned}$$

So, $N \in Z(RG)$