7.2.2) Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $p(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ such that $bp(x) = 0$.

Proof
($\implies$) Suppose $p(x)$ be a zero divisor in $R[x]$. That is, $\exists 0 \neq g(x) \in R[x]$ such that $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ and $g(x)p(x) = 0$. Further suppose that the degree m of $g(x)$ is the least positive integer such that this is true. It is clear then that $\sum_{i=0}^{k} a_i b_{k-i} = 0$, which is the coefficient of the term x^k. This implies that for the term x^{n+m} we have that $b_m a_n = 0$. Thus, the polynomial $a_n g(x)$ is a polynomial of degree less than m which gives $a_n g(x)p(x) = 0$, but this cannot be the case, meaning that $a_n g(x)$ is identically zero. That is, $a_n b_i = 0$ for all $i = 0, 1, \ldots, m$. Since $g(x)$ is the smallest degree polynomial such that $g(x)p(x) = 0$, it must follow that $a_k g(x) = 0$ for each $0 \leqslant k \leqslant n$. Hence, it follows that $a_k b_i = 0$ for each $i = 0, 1, \ldots$, implying that $b_i p(x) = 0$.

($\impliedby$) We know that R is a subring of $R[x]$, so if $\exists 0 \neq b \in R$ such that $bp(x) = 0$, then we can take any polynomial with coefficients equal to b. For simplicity, we choose the polynomial with $g(x) = b$. It is clear then that $g(x) \neq 0$ and $g(x)p(x) = 0$, meaning that $p(x)$ is a zero divisor.

■

7.2.3) Define the set $R[[x]]$ of *formal power series* in the indeterminate x with coefficients from R to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots.$$

Define addition and multiplication of power series in the same way as for power series with real or complex coefficients i.e., extend polynomial addition and multiplication to power series as though they were "polynomials of infinite degree":

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$
$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n.$$

a) Prove that $R[[x]]$ is a commutative ring with 1.

Proof
It is clear that $R[[x]]$ is an abelian group under addition since R is abelian. That is, the inverse of $\sum_{n=0}^{\infty} a_n x^n \in R[[x]]$ is just $(-\sum_{n=0}^{\infty} a_n x^n)$, and the identity is zero. Additionally, addition is associative since it is defined in powers of x, and addition is also commutative since R is an abelian additive group.

Now, we show that multiplication is associative. Consider the following:

$$\begin{aligned}\sum_{n=0}^{\infty} a_n x^n \left(\sum_{n=0}^{\infty} b_n x^n \times \sum_{n=0}^{\infty} c_n x^n \right) &= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k c_{n-k} \right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_n \left(\sum_{k=0}^{n} b_k c_{n-k} \right) \right) x^n.\end{aligned}$$

From this it is simple to show that the distribution laws hold:

Now, we see that the identity is just 1, the identity of R, and that it is commutative since R is commutative.

■

b) Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \ldots$.

Proof
This is a fairly simple execise since

$$(1 - x)\left(1 + x + x^2 + \ldots\right) = \left(1 + x + x^2 + \ldots\right) - \left(x + x^2 + \ldots\right) = 1.$$

■

c) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ iff a_0 is a unit in R.

Proof
($\Longrightarrow$) Suppose that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ such that $\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = 0$. It is clear then that the constant term has coefficient $a_0 b_0 = 0$. Thus, we have that a_0 is a unit in R.

($\Longleftarrow$) Suppose that a_0 is a unit in R. That is, $\exists b \in R$ such that $a_0 b = 0$. Now, define $b_n = -b \sum_{k=1}^{n} a_k b_{n-k}$ with $b_0 = b$. By induction then $\sum_{n=0}^{\infty} b_n x^n \times \sum_{n=-}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_n b_{n-k} \right) x^n = 1$

■

7.2.6) Let S be a ring with identity $1 \neq 0$. Let $n \in \mathbb{Z}^+$ and let A be an $n \times n$ matrix with entries from S whose i, j entry is a_{ij}. Let E_{ij} be the element of $M_n(S)$ whose i, j entry is 1 and whose other entries are all 0.

a) Prove that $E_{ij}A$ is the matrix whose i^{th} row equals the j^{th} row of A and all other rows are zero.

Proof
We see that

$$(E_{ij}A)_{lm} = \sum_{k=1}^{n} e_{lk}a_{km}.$$

Now, $e_{ik} = 1$ if $k = j$ but is zero otherwise. Thus,

$$(E_{ij}A)_{lm} = \begin{cases} a_{jm} & l = i \\ 0 & \text{otherwise} \end{cases}.$$

This means that the i^{th} row of $E_{ij}A$ is the j^{th} column of A.

■

b) Prove that AE_{ij} is the matrix whose j^{th} column equals the i^{th} column of A and all other columns are zeros.

Proof
This proof is similar to the last problem, except that now

$$(AE_{ij})_{lm} = \sum_{k=1}^{n} a_{lk}e_{km} = \begin{cases} a_{li} & m = j \\ 0 & \text{otherwise} \end{cases}.$$

That is, the j^{th} column of AE_{ij} is equal to the i^{th} row of A.

■

c) Deduce that $E_{pq}AE_{rs}$ is the matrix whose p, s entry is a_{qr} and all other entries are zero.

Proof
We have that

$$(E_{pq}A)_{ij} = \begin{cases} a_{qj} & i = p \\ 0 & \text{otherwise} \end{cases}.$$

Thus

$$(E_{pq}AE_{rs})_{ij} = \begin{cases} (E_{pq}A)_{ir} & j = s \\ 0 & \text{otherwise} \end{cases}.$$

Notice that if $i = p$ and $j = s$ then the p, s entry of $E_{pq}AE_{rs}$ is a_{qr} and if $i \neq p$ that the corresponding entries are $E_{pq}A$ is identically zero, meaning that $(E_{pq}AE_{rs})_{ij} = 0$.

■

7.2.7) Prove that the center of the ring $M_n(R)$ is the set of scalar matrices.

Proof
Recall that the center of a ring is the set of elements which commute with all other elements in the ring. Thus, the center of $M_n(R)$ is the set of matrices A such that $AB = BA$, where B is some matrix in $M_n(R)$. Let E_{ij} be defined as in the last problem. Observe that $E_{ij}E_{lm} = E_{im}$ if $j = l$ and is the zero matrix otherwise. This allows us to consider $E_{ij}AE_{lm}$, where A is in the center of the matrix ring. It is clear that the i, m entry of $E_{ij}AE_{lm}$ is a_{jl}. First, suppose that $j \neq l$, then $a_{jl} = 0$, meaning that A is diagonal. Now, observe that $E_{ij}A = AE_{ji}$. This tells us that the i^{th} row of A is the same as the j^{th} column of A. Since the off diagonal components of A are identically zero, it is only the diagonal components that are of interest. The diagonal element in the i^{th} row of A is a_{ii}, which is equal to the diagonal component in the j^{th} column of A. That is $a_{ii} = a_{jj}$, implying that the diagonal elements are all the same. Hence, we have shown that A must be a scalar matrix if it is in the center of $M_n(R)$.

■

7.3.12) Let D be an integer that is not a perfect square in $\mathbb{Z}$ and let $S = \begin{pmatrix} a & b \\ Db & a \end{pmatrix} | a, b \in \mathbb{Z}$.

a) Prove that S is a subring of $M_2(\mathbb{Z})$

b) If D is no a perfect square in $\mathbb{Z}$ prove that the map $\varphi : \mathbb{Z}[\sqrt{D}] \to S$ defined by $\varphi\left(a + b\sqrt{D}\right) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix}$ is a ring isomorphism.

c) If $D \equiv 1 \mod 4$ is squarefree, prove that the set $\begin{pmatrix} a & b \\ (D-1)\frac{b}{4} & a+b \end{pmatrix} | a, b \in \mathbb{Z}$ is a subring of $M_2(\mathbb{Z})$ and is isomorphi to the quadratic integer ring $\mathcal{O}$.

7.3.17) Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.

a) Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

b) Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi\left(u^{-1}\right) = \varphi\left(u\right)^{-1}$ for each unit u of R.

7.3.18)

a) If I and J are ideals of R prove that their intersection $I \cap J$ is also an ideal of R.

b) Prove that the intersection of an arbitrary nonempty collection of ideals is again an ideal (do not assume the collection is countable).

7.3.25) Assume R is a commutative ring with 1. Prove that the Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

holds in R, where the binomial coefficient $\binom{n}{k}$ is interpreted in R as the sum $1+1+\ldots+1$ of the identity 1 in R taken $\binom{n}{k}$ times.

7.3.29) Let R be a commutative ring. Recall that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements form an ideal – called the *nilradical* of R and denoted $\mathcal{N}(\mathcal{R})$.

7.3.34) Let I and J be ideals of R.

a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

b) Prove that IJ is an ideal contained in $I \cap J$.

c) Give an example where $IJ \neq I \cap J$.

d) Prove that if R is commutative and if $I + J = R$ then $IJ = I \cap J$.