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:

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

Note that the roles of a and c are flipped in the two equations. It is important to note that the indices of a, b, and c add up to n and the starting and ending indices for the sums are the same. Because of this we can shift indices and end up with the coefficients in both products being the same. That is, we could define $m = n - j - k$ and carry out the necessary shifts and see that we have a sum over $a_m b_j c_{n-j-m}$ with the same starting and terminating indices.

From this it is clear that the distributive laws hold since they hold in R.

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 $M_2(\mathbb{Z})$.

Proof
Consider the following:

$$\begin{pmatrix} a & b \\ Db & a \end{pmatrix} - \begin{pmatrix} a' & b' \\ Db' & a' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ D(b - b') & a - a' \end{pmatrix} \in M_2(\mathbb{Z})$$

and

$$\begin{pmatrix} a & b \\ Db & a \end{pmatrix}\begin{pmatrix} a' & b' \\ Db' & a' \end{pmatrix} = \begin{pmatrix} aa' + Dbb' & ab' + ba' \\ D(ba' + ab') & Dbb' + aa' \end{pmatrix} = \begin{pmatrix} c & d \\ Dd & c \end{pmatrix} \in M_2(\mathbb{Z}).$$

Thus, S is a subring of $M_2(\mathbb{Z})$.

■

b) If D is not 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.

Proof
It is clear that this is a group homomorphism under addition:

$$\begin{aligned}\varphi([a + b\sqrt{D}] + [a' + b'\sqrt{D}]) &= \begin{pmatrix} a + a' & b + b' \\ D(b + b') & a + a' \end{pmatrix} = \begin{pmatrix} a & b \\ Db & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ Db' & +a' \end{pmatrix} \\ &= \varphi(a + b\sqrt{D}) + \varphi(a' + b'\sqrt{D}).\end{aligned}$$

Under multiplication, we have

$$\varphi([a + b\sqrt{D}] \times [a' + b'\sqrt{D}]) = \varphi(aa' + bb'D + [ab' + ba']\sqrt{D}) = \begin{pmatrix} aa' + bb'D & ab' + ba' \\ D(ab' + ba') & aa' + bb'D \end{pmatrix}$$

$$\varphi(a + b\sqrt{D}) \times \varphi(a' + b'\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix} \begin{pmatrix} a' & b' \\ Db' & a' \end{pmatrix} = \begin{pmatrix} aa' + Dbb' & ab' + ba' \\ a'bD + ab'D & bb'D + aa' \end{pmatrix}.$$

Thus, this is a ring homomorphism.

■

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 isomorphic to the quadratic integer ring $\mathcal{O}$.

Proof
Since this is a subset of matrices, it is clear that it inherits the basic properties of matrix operations. Thus, it is an abelian additive group, associative under multiplication, and follows the necessary distribution laws.

Consider the map $\phi : \mathcal{O} \to S$, where S is the set of matrices defined above, defined by $\phi : a + b\omega \mapsto \begin{pmatrix} a & b \\ (D-1)b/4 & a + b \end{pmatrix}$, where $\omega = (1 + \sqrt{D})/2$. We prove that this is an

isomorphism:

$$\begin{aligned}
\phi([a+b\omega]+[a'+b'\omega]) &= \begin{pmatrix} a+a' & b+b' \\ (D-1)\frac{b+b'}{4} & (a+a')+(b+b') \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ (D-1)\frac{b}{4} & a+b \end{pmatrix} + \begin{pmatrix} a' & b' \\ (D-1)\frac{b'}{4} & a'+b' \end{pmatrix} \\
&= \phi(a+b\omega)+\phi(a'+b'\omega) \\
\phi([a+b\omega]\times[a'+b'\omega]) &= \phi(aa'+bb'\omega^2+[ab'+ba']\omega) \\
&= \phi(aa'+bb'\frac{D-1}{4}+[ab'+ba'+bb']\omega) \\
&= \begin{pmatrix} aa'+bb'\frac{D-1}{4} & ab'+ba'+bb' \\ (D-1)\frac{ab'+ba'+bb'}{4} & aa'+bb'\frac{D-1}{4}+ab'+ba'+bb' \end{pmatrix} \\
\phi(a+b\omega)\phi(a'+b'\omega) &= \begin{pmatrix} a & b \\ (D-1)\frac{b}{4} & a+b \end{pmatrix}\begin{pmatrix} a' & b' \\ (D-1)\frac{b'}{4} & a'+b' \end{pmatrix} \\
&= \begin{pmatrix} aa'+b(D-1)\frac{b'}{4} & ab'+b(a'+b') \\ \frac{D-1}{4}[ba'+b'(a+b)] & (D-1)\frac{b}{4}b'+(a+b)(a'+b') \end{pmatrix}.
\end{aligned}$$

Hence, this is a ring homomorphism. Proving that this is a bijection is fairly simple. We could define the function $\psi : S \to \mathcal{O}$ defined by $\psi : \begin{pmatrix} a & b \\ (D-1)b/4 & a+b \end{pmatrix} \mapsto a+b\omega$. Since this is a two sided inverse of ϕ, it is clear that ϕ is a bijection.

■

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.

Proof
Notice that $\varphi(1_R) = \varphi(1_R)\varphi(1_R)$, so by the distributive laws, $\varphi(1_R)[1_S - \varphi(1_R)] = 0$. That is, since $\varphi(1_R) \neq 1_S$, it is clear that $1_S - \varphi(1_R) \neq 0$ and that $\varphi(1_R)$ is a zero divisor in S.

Notice an equivalent statement of the theorem above is the following:

$$\text{If } \varphi(1_R) \text{ is not a zero divisor in } S, \text{ then } \varphi(1_R) = 1_S.$$

Hence, it follows that if S is an integral field, meaning that it contains no zero divisors, then $\varphi(1_R) = 1_S$.

■

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.

Proof
Let u be a unit of R. Observe that $\varphi(u^{-1}u) = \varphi(u^{-1})\varphi(u) = 1_S$. That is, $\varphi(u)$ is a unit in 1_S, with inverse $\varphi(u)^{-1} = \varphi(u^{-1})$.

■

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.

Proof
Let $x \in I \cap J$. Then $x \in I$ and $x \in J$. It follows then that $rx \in I$ and $rx \in J$ for any $r \in R$, implying that $rx \in I \cap J$. Thus, $r(I \cap J) \subset I \cap J$. Following a similar logic with right multiplication gives that $(I \cap J)r \subset I \cap J$. Hence, $I \cap J$ is ideal.

■

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

Proof
Consider a set of ideals: $\{J_\alpha | \alpha \in I\}$. It is clear then that $rJ_\alpha \subset J_\alpha$ and $J_\alpha r \subset J_\alpha$ for each $r \in R$. Hence $r\bigcap_{\alpha\in I} J_\alpha \subset \bigcap_{\alpha\in I} J_\alpha$ and $\left(\bigcap_{\alpha\in I} J_\alpha\right) r \subset \bigcap_{\alpha\in I} J_\alpha$, implying that the intersection of ideals is ideal.

■

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.

Proof
Notice that for $n = 0$ we have $(a+b)^0 = 1 = \binom{0}{0}$, which is true. Now suppose this is true for some integer n. We show that the binomial theorem holds for the $n+1$ case. Observe

that

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\ &= a^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} + b^{n+1}.\end{aligned}$$

We now shift the index of the first sum $k+1 \mapsto k$, giving

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]a^k b^{n+1-k} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k} + b^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}.\end{aligned}$$

■

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 $\mathcal{N}(\mathcal{R})$.

Proof
We have previously shown that if $x \in R$ is nilpotent then if r is any element of R that rx and xr are nilpotent. This means that $r\mathcal{N}(R) \subset \mathcal{N}(R)$ and $\mathcal{N}(R)r \subset \mathcal{N}(R)$, and since the nilradical of R is left and right ideal it is ideal.

■

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.

Proof
First, we show that $I + J$ is ideal. It is simple to show that this is a subring of R since if $a, c \in I$ and $b, d \in J$, then $(a+b) - (c+d) = (a-c) + (b-d) \in I + J$. Additionally, $(a+b)(c+d) = \underbrace{ac}_{\in I} + \underbrace{ad}_{\in I\cap J} + \underbrace{bc}_{\in I\cap J} + \underbrace{bd}_{\in J} \in I + J$. Now $r(a+b) = \underbrace{ra}_{\in I} + \underbrace{rb}_{\in J} \in I + J$, and by a similar argument $(a+b)r \in I + J$.

Next, we show that $I, J \subset I + J$. Consider $a \in I$. It is clear that $a + 0 \in I + J$, meaning $a \in I + J$, and similarly $b \in J$ implies that $b \in I + J$.

Finally, we show that if K is ideal and $I, J \subset K$ that $I + J \subset K$. Let $x, y \in K$. Then, $x + y \in K$. If we let $x = a \in I$ and $y = b \in J$, then $x + y = a + b \in I + J$. Thus, $I + J \subset K$.

■

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

Proof
Recall that $IJ = \{a_1b_1 + \ldots + a_nb_n | a_i \in I \text{ and } b_i \in J\}$. Notice that $rab = rab \in IJ$ and $abr = abr \in IJ$. It has been proven that IJ is a subring of R.

Now, we show that $IJ \subset I + J$. Let $x \in IJ$. Then $x = a_1b_1 + \ldots + a_nb_n$. Since $I + J$ is an abelian additive group and $a_ib_i \in I \cap J$ since I and J are ideal, it follows that $x \in I + J$.

■

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

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

Proof
It has already been shown that $IJ \subset I \cap J$, so it remains to be shown that $I \cap J \subset IJ$. Let $x \in I$ and $y \in J$ such that $x + y = 1$. Now, let $z \in I \cap J$, then $z = z(x + y) = zx + zy \in IJ$.

■