7.4.1) Let L_j be the left ideal of $M_n(R)$ consisting of arbitrary entries in the j^{th} column and zero in all other entries and let E_{ij} be the element of $M_n(R)$ whose i, j entry is 1 and whose other entries are all 0. Prove that $L_j = M_n(R)E_{ij}$ for any i.

Proof
Let

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

be the kronecker delta symbol. This is just notation that will simplify the matrix multiplication visually. Thus, if $M \in M_n(R)$, then

$$\begin{aligned}(ME_{ij})_{lm} = \sum_{k=1}^{n} M_{lk}(E_{ij})_{km} &= \sum_{k=1}^{n} M_{lk}\delta_{ik}\delta_{jm} \\ &= M_{li}\delta_{jm}..\end{aligned}$$

This tells us that the entries are only nonzero if $m = j$, meaning that only the j^{th} column on ME_{ij} is nonzero, with entries M_{li}, where l is the row label. Hence, $ME_{ij} \in L_j$ for all $M \in M$.

Now, we must prove that $L_j \subset M_n(R)E_{ij}$. This is easy to do by construction: we translate from L_j to $M_n(R)$ by taking the j^{th} column of the element of L_j and making it the j^{th} row of some element in $M_n(R)$. Since we know then that multiplying this element in $M_n(R)$ by E_{ij} gives L_j, it is clear that $L_j \subset M_n(R)E_{ij}$.

■

7.4.4) Assume R is commutative. Prove that R is a field iff 0 is a maximal ideal.

Proof
($\implies$) Suppose that 0 is a maximal ideal of R. Then $R/\{0\}$ is a field. We can construct a trivial isomorphism between this quotient ring and R as follows:

$$\begin{aligned}\varphi &: R/\{0\} \to R \\ \varphi &: \overline{r} \mapsto r.\end{aligned}$$

Since $R \cong R/\{0\}$, we know that R is a field too.

($\implies$) We know that a field only has $\{0\}$ and itself as maximal ideals, so this direction of the proof is trivial.

■

7.4.7) Let R be a commutative ring with 1. Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal iff R is an integral domain. Prove that (x) is a maximal ideal iff R is a field.

Proof
Consider the ring homomorphism $\varphi : R[x] \to R$ defined by $\varphi : p(x) \mapsto p(0)$. Then, the $\ker \varphi = (x)$ since $p(0)$ if and only if $a_0 = 0$, where a_0 is the constant term of $p(x)$. If the constant term is zero, then by the division algorithm, we can write $p(x) = xq(x) \in (x)$. By the first isomorphism theorem for rings, we know that $R[x]/(x) \cong R$.

It is known that R/P is an integral domain if and only if P is a prime ideal in R. Hence, the proposition in the problem statement follows immediately from the above isomorphism.

$\blacksquare$

7.4.8) Let R be an integral domain. Prove that $(a) = (b)$ for some elements $a, b \in R$ iff $a = ub$ for some unit $u \in R$.

Proof
($\implies$) If $(a) = (b)$, $a \in (b)$ and $b \in (a)$. That is, $a = ub$ and $b = va$ for some $u, v \in R$. Thus, $ab = (ub)(va) = (uv)ab$, or $ab(1 - uv) = 0$. Hence, $uv = 1$, meaning that $u \in R$ is a unit.

($\impliedby$) Notice that $ca \in (a)$ can be written $c(ub) = (cu)b \in (b)$. Next, notice that $db = d(u^{-1}a) = (du^{-1})a \in (a)$.

$\blacksquare$

7.4.9) Let R be the ring of all continuous functions on $[0, 1]$ and let I be the collection of functions $f(x)$ in R with $f(\frac{1}{3}) = f(\frac{1}{2}) = 0$. Prove that I is an ideal of R but it is not a prime ideal.

Proof
We know that the ring of functions is commutative, so we need only show that I is left ideal to show that it is ideal. This is easy to do since if $f \in I$ and $g \in R$, then

$$gf\left(\frac{1}{3}\right) = g\left(\frac{1}{3}\right)f\left(\frac{1}{3}\right) = g\left(\frac{1}{3}\right) \times 0 = 0$$
$$gf\left(\frac{1}{2}\right) = g\left(\frac{1}{2}\right)f\left(\frac{1}{2}\right) = g\left(\frac{1}{2}\right) \times 0 = 0.$$

Hence, I is an ideal in R.

It is easy to see that I is not a prime ideal. Consider the linear functions $f(x) = x - \frac{1}{3}$ and $g(x) = x - \frac{1}{2}$. Clearly, fg is identically zero at $\frac{1}{3}$ and $\frac{1}{2}$, but neither is zero at both. That, is $fg \in I$ but $f, g \notin I$.

$\blacksquare$

7.4.17) Let $x^3 - 2x + 1$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^3 - 2x + 1)$. Let $p(x) = 2x^7 - 7x^5 + 4x^3 - 9x + 1$ and let $q(x) = (x - 1)^4$.

a) Express each of the following elements of $\overline{E}$ in the form $\overline{f(x)}$ for some polynomial $f(x)$ of degree ≤ 2: $\overline{p(x)}$, $\overline{q(x)}$, $\overline{p(x) + q(x)}$, and $\overline{p(x)q(x)}$.

$\rightarrow$ We define $\overline{p(x)}$ as the remainder when $p(x)$ is divided by $x^3 - 2x + 1$. This gives us that

$$\begin{aligned}
\overline{p(x)} &= -x^2 - 11x + 3 \\
\overline{q(x)} &= 8x^2 - 13x + 5 \\
\overline{p(x) + q(x)} &= \overline{\overline{p(x)} + \overline{q(x)}} = 7x^2 - 24x + 8 \\
\overline{p(x)q(x)} &= \overline{\overline{p(x)}\,\overline{q(x)}} = 146x^2 - 236x + 90.
\end{aligned}$$

b) Prove that $\overline{E}$ is not an integral domain.

c) Prove that $\overline{x}$ is a unit in $\overline{E}$.

7.4.27) Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.

Proof
Suppose that $a^m = 0$. Then,

$$\begin{aligned}
(1 - ab)(1 + ab + \ldots + (ab)^{m-1}) &= (1 + ab + \ldots + (ab)^{m-1}) - ab(1 + ab + \ldots + (ab)^{m-1}) \\
&= (1 + ab + \ldots + (ab)^{m-1}) - (ab + (ab)^2 + \ldots + (ab)^m) \\
&= 1.
\end{aligned}$$

This is true regardless of our choice of b.

$\blacksquare$

7.5.1) Fill in all the details in the proof of Theorem 15.

7.5.2) Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R.

Proof
Suppose that F is the quotient field of R. Then we define $\varphi : D^{-1}R \to F$ such that $\varphi(d^{-1}r) = \frac{r}{d}$.

$\blacksquare$

7.5.4) Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

Proof

Any subfield of $\mathbb{R}$ must be contained in $\mathbb{R}$ and be a field itself under the same operations. Hence, it must contain the integers since $1 \in \mathbb{R}$, implying $(1) = \mathbb{Z} \subset \mathbb{R}$. We also must have the multiplicative inverse of each element. That is, if $n \in \mathbb{Z} \backslash \{0\}$ is also in the subfield, then $\frac{1}{n} \in \mathbb{Q}$ is also in the subfield, and $\left(\frac{1}{n}\right)$ must be contained in the subfield. Since any rational number can be generated by some principal ideal $\left(\frac{1}{n}\right)$, implying that $\mathbb{Q}$ is contained in every subfield of $\mathbb{R}$.

$\blacksquare$