3.1.9 Let $\mathbb{Z}[\sqrt{2}]$ denote the set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

Note that $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$. We use Theorem 3.2 to show that $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$. We must check that conditions (i), (ii), (iii), (iv) are satisfied. We first verify that $\mathbb{Z}[\sqrt{2}]$ is closed under addition and multiplication. Let $x_1, x_2 \in \mathbb{Z}[\sqrt{2}]$; then $x_i = a_i + b_i\sqrt{2}$ for some $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2$. Hence,

$$x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \qquad \text{since} \quad a_1 + a_2, b_1 + b_2 \in \mathbb{Z}$$
$$x_1x_2 = (a_1b_1 + 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \qquad \text{since} \quad a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1 \in \mathbb{Z}.$$

Since $0_\mathbb{R} = 0 + 0\sqrt{2}$ and $0 \in \mathbb{Z}$, we have $0_\mathbb{R} \in \mathbb{Z}[\sqrt{2}]$. Now let $x \in \mathbb{Z}[\sqrt{2}]$ be given. Then $x = a + b\sqrt{2}$ for some $a, b \in \mathbb{Z}$. Then setting $y = -a + (-b)\sqrt{2}$, we have $y \in \mathbb{Z}[\sqrt{2}]$, since $-a, -b \in \mathbb{Z}$, and $x + y = 0_\mathbb{R}$. Hence, by Theorem 3.2, $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$. ◆

3.1.29a Prove or disprove: If R and S are integral domains, then $R \times S$ is an integral domain.

We will disprove the assertion. Let $R = S = \mathbb{Z}$. Then R and S are integral domains but $R \times S$ is not an integral domain. Indeed, set $a = (1, 0)$ and $b = (0, 1)$; then $ab = (0, 0) = 0_{R\times S}$ but $a \neq 0_{R\times S}$ and $b \neq 0_{R\times S}$. ◆

3.2.6 Let R be a ring and b a fixed element of R. Let $T = \{rb \mid r \in R\}$. Prove that T is a subring of R.

We use Theorem 3.6 to prove that T is a subring of R. First note that T is nonempty (since $b^2 \in T$) and $T \subseteq R$. We must now show that T is closed under multiplication and subtraction. Let $a_1, a_2 \in T$ be given. Then $a_1 = r_1b$ and $b = r_2b$ for some $r_1, r_2 \in R$. Then

$$a_1 - a_2 = r_1b - r_2b = (r_1 - r_2)b \in T \qquad \text{since} \quad r_1 - r_2 \in R$$
$$a_1a_2 = r_1br_2b = (r_1r_2b)b \in T \qquad \text{since} \quad r_1r_2b \in R.$$

Hence, T is a subring of R. ◆

3.2.12a Prove that $[a]$ is a unit in $\mathbb{Z}_n$ if and only if $(a, n) = 1$ in $\mathbb{Z}$.

Let $a, n \in \mathbb{Z}$ be given with $n > 1$. Suppose first that $(a, n) = 1$. Then by Theorem 1.3, there are $u, v \in \mathbb{Z}$ such that $au + nv = 1$. Hence $au - 1 = n(-v)$, so $n \mid au - 1$ and thus $au \equiv 1 \pmod{n}$. It follows that

$$[a][u] = [u][a] = 1$$

in $\mathbb{Z}_n$ and thus $[a]$ is a unit. (Note that this implication also follows directly from Corollary 2.10).

Now suppose that $[a]$ is a unit in $\mathbb{Z}_n$. Then there is $u \in \mathbb{Z}$ such that $[a][u] = 1$ and, hence, $au \equiv 1 \pmod{n}$. Therefore, $n \mid 1 - au$ and so $1 - au = nv$ for some $v \in \mathbb{Z}$. So $au + nv = 1$. It follows by Theorem 1.3 that $(a, n) = 1$, since 1 is the smallest positive integer which can be expressed as an integer linear combination of a and n. ◆

3.2.23 Let R be a commutative ring with identity. Prove that R is an integral domain if and only if cancellation holds in R (that is, $a \neq 0_R$ and $ab = ac$ in R imply $b = c$).

Suppose R is an integral domain; then by Theorem 3.10 cancellation holds in R. Conversely suppose that cancellation holds in R; let $a, b \in R$ be given such that $ab = 0_R$ and $a \neq 0_R$. Then by Theorem 3.5.1

$$ab = 0_R = a \cdot 0_R.$$

Since cancellation holds in R, $a \neq 0_R$ and $ab = a \cdot 0_R$, we conclude that $b = 0_R$. Hence, R is an integral domain. ◆