Debra Griffin
3.6 #58(ii), 60, 61, 64

3.58 (ii) *Show that 2 and x are relatively prime in $\mathbb{Z}[x]$, but that 1 is not a linear combination of them; that is, there do not exist $s(x), t(x) \in \mathbb{Z}[x]$ with $1 = 2s(x) + xt(x)$.*

Proof:
Let $d(x)$ be a gcd of 2 and x. Then $d(x)|2$ and $d(x)|x$.
So $2 = (d(x))(f(x))$ and $x = (d(x))(g(x))$ for some $f(x), g(x) \in \mathbb{Z}[x]$.
Since $\mathbb{Z}[x]$ is an integral domain, then $0 = \deg(2) = \deg(d(x)) + \deg(f(x))$.
And $\deg(d(x)) = 0$ as degrees are nonnegative. Hence $d(x)$ is a constant, which are integers in $\mathbb{Z}[x]$. Thus, $d(x) \in \{\pm 1, \pm 2\}$.
If $d(x) = \pm 2$, then $x = \pm 2g(x)$. But every coefficient on the right side is even, while the coefficient of x on the left side is 1. And so $d(x) = \pm 1$.
$\therefore$ 2 and x are relatively prime.
Suppose there exist $s(x), t(x) \in \mathbb{Z}[x]$ with $1 = 2s(x) + xt(x)$.
Then for $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n \in \mathbb{Z}$, $m, n \in \mathbb{Z}^+$, we have

$$1 = 2(a_0 + a_1x + \cdots a_mx^m) + x(b_0 + b_1x + \cdots + b_nx^n)$$
$$= 2a_0 + (2a_1 + b_0)x + (2a_2 + b_1)x^2 + \cdots$$

Thus, the constant term on the left side is 1, while the constant term on the right side is even, a contradiction to the integrity of the integers. ☺
$\therefore$ 1 is not a linear combination of 2 and x. •

3.60 *Prove that there are domains R containing a pair of elements having no gcd. (See the definition on page 147.)*
***Hint**: Let k be a field and let R be the subring of k[x] consisting of all polynomials having no linear term; that is, $f(x) \in R$ if and only if $f(x) = s_0 + s_2x^2 + s_3x^3 + \cdots$. Show that x^5 and x^6 have no gcd in R.*

Proof:
Let R be defined as in the hint above. Then the only factors of x^5 are x^3 and x^2. And the only factors of x^6 are x^4, x^3, x^2.
Suppose x^3 is the gcd of x^5 and x^6. Then $x^2 \mid x^5$ and $x^2 \mid x^6$ and implies $x^2 \mid x^3$, a contradiction to the fact that no polynomial of R has a linear term.
Then suppose x^2 is the gcd of x^5 and x^6. Since $x^3 \mid x^5$ and $x^3 \mid x^6$ and implies $x^3 \mid x^2$, then we have another contradiction.
$\therefore$ x^5 and x^6 have no gcd in R, hence R is a domain that contains a pair of elements having no gcd. •

3.61 *Prove that* $R = \mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ *is a euclidean ring with* $\partial(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Proof:
We first show that $\partial(\alpha) \le \partial(\alpha\beta)$.
Let $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$. Then

$$\begin{aligned}\partial(\alpha) = |a^2 - 2b^2| &\le |a^2 - 2b^2||c^2 - 2d^2| \\ &= |(a^2 - 2b^2)(c^2 - 2d^2)| \\ &= |a^2(c^2 - 2d^2) + 2b^2(c^2 - 2d^2)| \\ &= |(ac + 2bd)^2 - 2(ad + bc))^2| \\ &= \partial(\alpha\beta), \text{ as desired.}\end{aligned}$$

Next, we show that for any $\alpha, \beta \in R$, $\beta \neq 0$, $\alpha = \beta\gamma + \rho$ where $\gamma, \rho \in R$ and $\partial(\rho) < \partial(\beta)$.
Let $\alpha = q + r\sqrt{2}$ and $\beta = s + t\sqrt{2}$.
Note that $\partial(\alpha) \le \partial(\alpha\beta)$ is even true for all $\alpha, \beta \in \mathbb{Q}[x]$.
Regard α/β as an element of $\mathbb{R}$. Rationalizing the denominator gives
$\alpha/\beta = (q + r\sqrt{2})(s - t\sqrt{2})/\partial(\beta)$ so that $\alpha/\beta = x + y\sqrt{2}$ where $x, y \in \mathbb{Q}$.
Write $x = a + u$ and $y = b + v$ where $a, b \in \mathbb{Z}$ are integers closest to x and y, respectively; thus, $|u|, |v| \le \frac{1}{2}$. It follows that
$\alpha = \beta(x + y\sqrt{2}) = \beta(a + u + (b + v)\sqrt{2}) = \beta(a + b\sqrt{2}) + \beta(u + v\sqrt{2})$.
Notice that $\beta(u + v\sqrt{2}) \in \mathbb{Z}[\sqrt{2}\,]$, for it is equal to $\alpha - \beta(a + b\sqrt{2})$.
We have noted already that in $\mathbb{Q}[x]$, $\partial(\beta(u + v\sqrt{2})) = \partial(\beta)\,\partial(u + v\sqrt{2}))$.
And so ∂ will be a degree function if $\partial(\beta(u + v\sqrt{2})) = \partial(\beta)\,\partial(u + v\sqrt{2})) < \partial(\beta)$, or equivalently, if $\partial(u + v\sqrt{2}) < 1$.
And this is so, for the inequalities $|u| \le \frac{1}{2}$ and $|v| \le \frac{1}{2}$ give $u^2 \le \frac{1}{4}$ and $v^2 \le 1/4$, and hence $\partial(u + v\sqrt{2}) = |u^2 - 2v^2| \le |u^2| + |2v^2| \le \frac{1}{4} + \frac{1}{2} = \frac{3}{4} < 1$.
$\therefore$ $R = \mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a euclidean ring with $\partial(a + b\sqrt{2}) = |a^2 - 2b^2|$. •

3.64 *Let R be a Euclidean ring with degree function* ∂.
(i) *Prove that* $\partial(1) \le \partial(a)$ *for all nonzero* $a \in R$.

Proof:
Let $a \in R$, $a \neq 0$.
Then since R is a Euclidean ring, $\partial(1) \le \partial(1 \cdot a) = \partial(a)$.
$\therefore$ $\partial(1) \le \partial(a)$ for all nonzero $a \in R$.

3.64 (ii) *Prove that a nonzero $u \in R$ is a unit $\Leftrightarrow \partial(1) = \partial(u)$.*

Proof:
Let $u \in R$, $u \neq 0$.

Assume u is a unit.
Then $uu^{-1} = 1$. Since R is a Euclidean ring, $\partial(u) \leq \partial(uu^{-1}) = \partial(1)$.
By part (i), $\partial(1) \leq \partial(u)$.
$\therefore\ \partial(1) = \partial(u)$.

Conversely, assume $\partial(1) = \partial(u)$.
Since R is a euclidean ring, then $\exists\ q, r \in R$ such that
$1 = uq + r$ and $\partial(r) < \partial(u)$ or $r = 0$.
By part (i), $\partial(u) = \partial(1) \leq \partial(r)$, hence $r = 0$.
$\therefore\ 1 = uq$ which implies that u is a unit.

$\therefore$ A nonzero $u \in R$ is a unit $\Leftrightarrow \partial(1) = \partial(u)$.