1. *Let R be a commutative ring with unity and $a, b \in R$.*

(a) *Prove that if $(a, b) = (d)$ for some $d \in R$, then d is a greatest common divisor of a and b.*

Proof:

Let $I = \{ar + bs | r, s \in R\}$. We have shown $I = (a, b)$.

Since $(a, b) = (d)$, then $a, b \in (d)$. Thus, $a = dj$ and $b = dk$ for some $j, k \in R$.

So d is a common divisor of a and b.

Let c be a common divisor of a and b. Then $a = cm$ and $b = cn$ for some $m, n \in R$.

Also $d \in I$, hence $d = ar + bs$ for some $r, s \in R$.

And so $d = cmr + cns = c(mr + ns)$, which implies $c \mid d$.

$\therefore$ d is a greatest common divisor of a and b. •

(b) *Prove that the converse of the above statement is false.*

Proof:

We know a gcd of 2 and x is 1, but $(1) \neq (2, x)$. •

2. *Prove that all euclidean rings are principal ideal domains.*

Proof:

Let R be a euclidean ring. Let I be an ideal in R.

If $I = \{0\}$, then I is a PID. Assume $I \neq \{0\}$.

Since R is a euclidean ring, we can find an element, a, in I that is of minimal degree.

Claim: $(a) = I$.

We have $(a) \subseteq I$ by definition.

Let $b \in I$.

Since R is a euclidean ring, $\exists\ q, r$ such that $b = aq + r$ where $r = 0$ or $\deg r < \deg a$.

Since $b \in I$ and $aq \in I$, then $r = b - aq \in I$.

Since a is of minimal degree, then $\deg r \not< \deg a$, hence $r = 0$.

And this implies that $b = aq$, hence $b \in (a)$.

$\therefore$ $I \subseteq (a)$. $\therefore$ $I = (a)$.

$\therefore$ Every ideal in R is a principal ideal.

$\therefore$ R is a PID. •

3. *Let R be an integral domain, $a \in R$ and $I = (a)$.*

(a) *Prove that if I is maximal, then a is irreducible.*

Proof:
Assume I is maximal. Let $a = bc$ be a factorization of a in R.
Then $a \in (b)$. Since I is maximal, then $I = (b)$ or $(b) = R$.
If $I = (b)$, then a and b are associates. Hence $a = bu$ for some unit u in R.
And so $bc = bu$, which gives us $c = u$ as R is an integral domain.
If $(b) = R$, then $1 = b \bullet b^{-1} \in R$. So then b is a unit.
$\therefore$ b or c is a unit, which implies a is irreducible. •

(b) *Prove that the converse of the above statement is false.*

Proof:
x is irreducible in $\mathbb{Z}[x]$, but (x) is not maximal as $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$. •

(c) *Prove that x is a prime element in R[x].*

Proof:
R is an integral domain $\Rightarrow R[x]$ is an integral domain.
$R[x]/(x) \cong R$ as $\varphi: R[x] \to R$ defined by $\varphi(a_0 + a_1x + \cdots + a_nx^n) = a_0$ for any
$a_0 + a_1x + \cdots + a_nx^n \in R[x]$ gives us that $\ker \varphi = (x)$.
Since R is an integral domain, then (x) is a prime ideal, hence x is a prime element. •

(d) *Prove that (x) is maximal in R[x] if and only if R is a field.*

Proof:
Assume (x) is maximal in $R[x]$.
Then $R[x]/(x)$ is a field. As argued in part (c), $R[x]/(x) \cong R$. Thus R is a field.

Conversely, assume R is a field. Then since $R[x]/(x) \cong R$, $R[x]/(x)$ is a field.
$\therefore$ (x) is maximal. •

4. *Let R be a commutative ring with unity and let I be a proper ideal in R. Recall that a ring is called local if it has a unique maximal ideal. (For this problem you may assume that a proper ideal is always contained in some maximal ideal.)*

(a) *Prove that if R is a local ring, then R/I is a local ring.*

Proof:
Assume R is a local ring and I is a proper ideal in R.

Then $\exists\ m$, a unique maximal ideal in R such that $I \subseteq m$, otherwise $I = R$.

Then by the correspondence theorem $\exists\ M \subsetneq R/I$ such that $M = m/I$.

Suppose $\exists\ M'$ an ideal in R/I such that M' is maximal but $M \neq M'$. Then $M' \not\subseteq M$, otherwise M' is not maximal.

And so by the correspondence theorem, $\exists\ m' \in R$ such that $M' = m'/I$ and $m \neq m'$ and $m' \not\subseteq m$. But since m is the unique maximal ideal in R and every proper ideal is always contained in some maximal ideal, then $m' \subseteq m$, a contradiction

$\therefore$ M is the unique maximal ideal of R/I.

$\therefore$ R/I is a local ring.

(b) *Let $M = \{r \in R | r \notin U(R)\}$. Prove that if M is an ideal in R, then R is a local ring.*

Proof:
Assume M is an ideal in R. Note that M is a proper ideal as R is a ring with unity.

So then $M \subseteq K$ where K is a maximal ideal of R as every proper ideal is contained in some maximal ideal.

Suppose K' is another maximal ideal of R such that $K' \neq K$.

Then $\exists\ b \in K'$ such that $b \notin K$, otherwise $K' \not\subseteq K$.

Thus $b \notin M$ (as $M \subseteq K$), hence b is a unit.

So then $K' = R$. And this gives us that K' is not maximal.

$\therefore$ K is the unique maximal ideal of R. $\therefore$ R is a local ring.

5. *Let R be a unique factorization domain and a, b, c ∈ R. Prove that if a and b are relatively prime and a|bc, then a|c.*

Proof:

Let $a, b, c \in R$ such that a and b are relatively prime and $a \mid bc$.

Then $bc = ar$ for some $r \in R$ and the gcd of a and b is a unit.

If $b \in U(R)$, then $bc = ar \Rightarrow c = b^{-1}ar$, hence $a \mid c$.

If $a \in U(R)$, then $c = aa^{-1}c$, hence $a \mid c$.

Assume $a, b \notin U(R)$.

Since R is a UFD, we can write

$a = up_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$,

$b = vp_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$, and

$c = wp_1^{g_1} p_2^{g_2} \cdots p_t^{g_t}$ where $u, v, w \in U(R)$, $p_1, p_2, \cdots, p_t$ are distinct irreducibles,

$e_i \geq 0$, $f_i \geq 0$, and $g_i \geq 0$ for all i.

Since the gcd, of a and b is a unit, then $\min\{e_i, f_i\} = 0$ for all i.

And since $a \mid bc$, then $e_i \leq f_i + g_i$ for all i.

Let $M_i = \max\{e_i, f_i\}$. Then, by reindexing, we have

$a = up_1^{M_1} p_2^{M_2} \cdots p_s^{M_s} p_{s+1}^0 p_{s+2}^0 \cdots p_t^0$ and

$b = vp_1^0 p_2^0 \cdots p_s^0 p_{s+1}^{M_{s+1}} p_{s+2}^{M_{s+2}} \cdots p_t^{M_t}$ for some positive integer $s \leq t$.

So $bc = vp_{s+1}^{M_{s+1}} p_{s+2}^{M_{s+2}} \cdots p_t^{M_t} \bullet wp_1^{g_1} p_2^{g_2} \cdots p_t^{g_t} = up_1^{M_1} p_2^{M_2} \cdots p_s^{M_s} r = ar$.

Since $e_i \leq f_i + g_i$, and for each $i \in \{1, 2, \ldots, s\}$ $f_i = 0$, then $M_i \leq g_i$.

Thus we can write

$c = wp_1^{M_1} p_1^{g_1 - M_1} p_2^{M_2} p_2^{g_2 - M_2} \cdots p_s^{M_s} p_s^{g_s - M_s} \cdots p_t^{g_t} = wp_1^{M_1} p_2^{M_2} \cdots p_s^{M_s} p_1^{g_1 - M_1} p_2^{g_2 - M_2} \cdots p_s^{g_s - M_s} p_{s+1}^{g_{s+1}} p_{s+2}^{g_{s+2}} \cdots p_t^{g_t}$

$\therefore$ $a \mid c$.

6. *Let R be an integral domain, Q = Frac(R) and f (x) ∈ R[x] such that deg f (x) > 0.*

(a) *Prove that if f (x) is irreducible in R[x], then f (x) is primitive.*

Proof:
Assume $f(x)$ is irreducible in $R[x]$. Then $f(x) \neq 0$ and $f(x)$ is not a unit.
Let d = gcd of the coefficients of $f(x)$.
Then $f(x) = d \bullet g(x)$ for some $g(x)$ in $R[x]$.
Since $f(x)$ is irreducible, then d is a unit or $g(x)$ is a unit.
Since $R[x]$ is an integral domain, $\deg f(x) = \deg d + \deg g(x) = 0 + \deg g(x)$.
$\therefore$ $g(x)$ is not a unit, otherwise $\deg g(x) = 0$.
$\therefore$ d is a unit.
$\therefore$ $f(x)$ is primitive.

(b) Prove that the converse of the above statement is false.

Proof:
$x^2 + 2x + 1$ is primitive in $\mathbb{Z}[x]$, but $x^2 + 2x + 1 = (x + 1)(x + 1)$.

(c) *Prove that if f (x) is primitive and irreducible in Q[x], then f (x) is irreducible over R[x].*

Proof:
Assume $f(x)$ is primitive and irreducible in $Q[x]$.
Let $f(x) = g(x)h(x)$ be any factorization of $f(x)$ in $R[x]$.
Then $f(x) = g(x)h(x)$ is also a factorization of $f(x)$ in $Q[x]$.
Since $f(x)$ is irreducible in $Q[x]$, then $g(x)$ is a unit or $h(x)$ is a unit in $Q[x]$.
Say it's $g(x)$. Then $\deg g(x) = 0$. So $\deg g(x) = 0$ in $R[x]$ also.
Thus $g(x)$ is a constant polynomial in $R[x]$, call it r.
Then r divides the coefficients of $f(x)$.
Since $f(x)$ is primitive, then the gcd of its coefficients is a unit, call it d.
So $r \mid d$. Thus $d = rs$ for some $s \in R$.
And since d is a unit, then $1 = d^{-1}rs$, hence r is a unit.
$\therefore$ $g(x)$ is a unit in $R[x]$. $\therefore$ $f(x)$ is irreducible in $R[x]$.