Debra Griffin
Section 3.4+
3.33, Corollary 3.34, Handout 3-8

1. Text #3.33
3.33. *Let k be a field, and let f (x), g(x) ∈ k[x] be relatively prime. If h(x) ∈ k[x], prove that f (x) | h(x) and g(x) | h(x) ⇒ f (x)g(x) | h(x).*
***Hint**: See Exercise 1.19 on p. 13.*

Proof:
Assume k is a field, $f(x), g(x) \in k[x]$ are relatively prime, and $f(x) \mid h(x)$ and $g(x) \mid h(x)$ for some $h(x) \in k[x]$. Then the gcd $(f(x), g(x)) = 1$.
Let a denote $a(x)$ $\forall$ $a(x) \in k[x]$.
By Thm 3.31 (If $f, g \in k[x]$, k a field, then gcd $(f, g) = sf + tg$ for some $s, t \in k[x]$.)
Then gcd $(f, g) = 1 \Rightarrow 1 = sf + tg$ for some $s, t \in k[x]$, and
$f \mid h$ and $g \mid h \Rightarrow h = fu = gv$ for some $u, v \in k[x]$.
So $h = hsf + htg = gvsf + futg = fg(vs + ut)$.
$\therefore f(x)g(x) \mid h(x)$. •

2. Corollary 3.34, p. 136
Let k be a field and let f (x) ∈ k[x] be a quadratic or cubic polynomial. Then f (x) is irreducible in k[x] if and only if f (x) does not have a root in k.

Proof:
Note that by Proposition 3.24 (If $f(x) \in k[x]$, then a is a root of $f(x)$ in k if and only if $x - a$ divides $f(x)$ in $k[x]$).
Assume $f(x) \in k[x]$ and deg $f(x) = n \in \{2, 3\}$.
We will show the forward implication by contraposition.
Suppose $f(x)$ does have a root, a, in k.
Then $(x - a) \mid f(x)$, or equivalently, $f(x) = g(x)(x - a)$ for some $g(x) \in k[x]$.
Since $k[x]$ is an integral domain, then deg $f(x)$ = deg $g(x)$ + deg $((x - a))$.
Thus deg $g(x)$ = 1 or 2 for deg $f(x)$ = 2 or 3 respectively, since degrees are nonnegative. $\therefore f(x)$ is reducible.
Or, equivalently, $f(x)$ is irreducible in $k[x] \Rightarrow f(x)$ does not have a root in k.

Conversely, suppose $f(x)$ does not have a root in k, then $(x - a) \nmid f(x)$ $\forall$ $a \in k$.
If $f(x) = g(x)h(x)$ for some $g(x), h(x) \in k[x]$, then neither g nor h has degree 1 (otherwise $(ab + c) \mid f(x)$, hence $-c/a$ is a root of $f(x)$ in k.)
And since deg $f(x)$ = deg $g(x)$ + deg $h(x)$, then at least one of the factors has degree 0, hence is a unit (that is 3 = deg $f(x)$ = deg $g(x)$ + deg $h(x)$ = 3 + 0 or 2 = deg $f(x)$ = deg $g(x)$ + deg $h(x)$ = 2 + 0).
$\therefore f(x)$ is irreducible. •

3. *Let R be a commutative ring with unity and let a, b $\in$ R.*
Prove (a, b) = {ar + bs|r, s $\in$ R}.

Proof:
Let $I = \{ar + bs\colon\ r, s \in R\}$. We first will show I is an ideal that contains a and b.
We have $0 = a \bullet 0 + b \bullet 0 \in I$.
Let $ar + bs$, $ar' + bs' \in I$, then since R is a commutative ring,
$(ar + bs) - (ar' + bs') = a(r - r') + b(s - s') \in I$, as $r - r' \in R$ and $s - s' \in R$.
Let $t \in R$. Then $(ar + bs)t = a(rt) + b(st) \in I$ as $rt, st \in R$.
Since $1, 0 \in R$, then $a = a \bullet 1 + b \bullet 0 \in I$ and $b = a \bullet 0 + b \bullet 1 \in I$.
$\therefore$ I is an ideal that contains a and b.
Since (a, b) is the smallest ideal that contains a and b, then $(a, b) \subseteq I$.
We now show the reverse containment.
Let $w \in I$. Then $w = ar + bs$ for some $r, s \in R$.
By definition of ideal, $ar \in (a, b)$ and $bs \in (a, b)$. And so $w = ar + bs \in (a, b)$.
$\therefore$ $(a, b) \subseteq I = \{ar + bs\colon\ r, s \in R\}$, hence $(a, b) = \{ar + bs\colon\ r, s \in R\}$. •

4. *Prove that every field is a PID.*

Proof:
Let k be a field. Let I be an ideal in k. If $I = \{0\}$, then $I = (0)$. If $I \neq \{0\}$, then $\exists\ a \in I$ such that $a \neq 0$. Since k is a field, then a is a unit, hence $\exists\ a^{-1} \in k$ such that $aa^{-1} = 1$.
$\therefore$ $aa^{-1} = 1 \in I$, hence $k = \{1 \bullet r\colon r \in k\} = I$.
Thus the only ideals in k are (0) and k.
That is, every ideal in k is a principal ideal, hence k is a PID. •

5. *Let R be an integral domain. Prove that for any a, b $\in$ R, the following are equivalent.*
(a) *a and b are associates*
(b) *a|b and b|a*
(c) *(a) = (b)*

Proof:
(a) ⇒ (b): Assume a and b are associates in R, an integral domain with unity.
Then $a = bu$ for some unit $u \in R$. Thus $\exists\ u^{-1} \in R$ such that $au^{-1} = buu^{-1} = b$.
Since $a = bu \Rightarrow a|b$ and $au^{-1} = b \Rightarrow b|a$, then we have $a|b$ and $b|a$, as desired.

(b) ⇒ (c): Assume $a|b$ and $b|a$. Then $b = au$ and $a = bv$ for some $u, v \in R$.
Let $w \in (a)$. Then $w = ar$ for some $r \in R$. So $w = bvr \in (b)$, as $vr \in R$. Thus $(a) \subseteq (b)$.
To show the reverse containment, let $y \in (b)$, Then $y = bs$ for some $s \in R$.
And $y = aus \in (a)$, as $us \in R$, hence $(b) \subseteq (a)$. $\therefore$ $(a) = (b)$.

(c) ⇒ (a): Assume $(a) = (b)$.
Since $a \in (a)$ and $b \in (b)$, then $a \in (b)$ and $b \in (a)$,
hence $b = au$ and $a = bv$ for some $u, v \in R$.
Thus, $a = auv$ which implies that $1 = uv$, since R is an integral domain.
And so u and v are units, which implies a and b are associates. •

6. (a) *Let R be an integral domain and $p \in R$. Prove that if p is a prime element, then p is irreducible.*

Proof:
Assume p is prime. Then $p \neq 0$ and p is not a unit.
Let $p = ab$ be a factorization of p. Note that this implies $a|p$.
Since $p = p \bullet 1 = ab$, then $p|ab$. And since p is prime then $p|a$ or $p|b$.
If $p|a$ then we have $p|a$ and $a|p$, so by #5 above, we have that p and a are associates.
Thus $p = au$ for some unit u. So then $p = au = ab$. And since R is an integral domain, we have that $u = b$ by cancellation.
Hence b is a unit.
Similarly, if $p|b$, then p and b are associates, which implies a is a unit.
$\therefore$ p is irreducible. •

6. (b) *Let R be a PID and $p \in R$. Prove that if p is irreducible, the p is a prime element.*

Proof:
Assume p is irreducible. Then $p \neq 0$ and p is not a unit.
Suppose $p \mid ab$ for some $a, b \in R$. So $pq = ab$ for some $q \in R$.
Since R is a PID, then $\exists\, c \in R$ such that $(a, p) = (c)$.
This gives us 3 results:
(1) By #3 above, $\exists\, x, y \in R$ such that $ax + py = c$; (2) $p \in (c)$; and (3) $a \in (c)$.
$p \in (c) \Rightarrow p = cm$ and $a \in (c) \Rightarrow a = cn$ for some $m, n \in R$
Since p is irreducible, then c is a unit or m is a unit.
If m is a unit, then $c = pm^{-1}$, hence $a = pm^{-1}n$. So $p|a$.
If c is a unit, then $1 = cc^{-1} = axc^{-1} + pyc^{-1}$.
So $b = baxc^{-1} + bpyc^{-1} = pqxc^{-1} + pbyc^{-1} = p(qxc^{-1} + byc^{-1})$, as R is commutative.
This gives us that $p|b$.
$\therefore$ $p|b$ or $p|a$, hence p is a prime element. •

7. *Let R be a commutative ring with unity. Let $a, b \in R$ and let d be a GCD of a and b. Prove that ud is also a GCD of a and b for every $u \in U(R)$.*

Proof:
Let R be a commutative ring with unity.
Let $a, b \in R$ and let d be a gcd of a and b. Thus, $a = dr$ and $b = ds$ for some $r, s \in R$.
Since $1 \in R$, then $U(R) \neq \emptyset$, and we can let $u \in U(R)$.
So $ua = udr$ and $ub = uds$. Since R is commutative, then
$a = u^{-1}udr = ud(ru^{-1})$ and $b = u^{-1}uds = ud(su^{-1})$.
Thus $ud|a$ and $ud|b$.
Moreover, since d is a gcd of a and b, then $c|a$ and $c|b$, $\Rightarrow c|d$, hence $c|ud$.
$\therefore$ ud is a gcd of a and b $\forall\, u \in U(R)$. •

8. *Let R be a PID and a, b ∈R. Prove (a, b) = (d) where d is a GCD of a and b.*

Proof:
Let R be a PID. Let $a, b \in R$. Let $I = (a, b)$.
By #3 above, $(a, b) = \{ar + bs | r, s \in R\}$.
Since R is a PID, then $\exists\, d \in R$ such that $(a, b) = (d)$.
We will show d is a gcd of a and b.
Since $a \bullet 1 + b \bullet 0 = a \in I$, then $a = dk$ for some $k \in R$. So $d|a$.
Similarly $d|b$.
Assume $c|a$ and $c|b$, then $a = cm$ and $b = cn$ for some $m, n \in R$.
And since $d \in I$, then $\exists\, x, y \in R$ such that
$d = ax + by = cmx + cny = c(mx + ny)$.
$\therefore$ $c|d$, hence d is a gcd of a and b. •