3. Divisibility & Factorization

* Throughout, R is an integral domain with 1.

<u>Def:</u> If $a, b \in R$, say that a <u>divides</u> b, or b is a <u>multiple</u> of a if $b = ac$ for some $c \in R$, and we write $a|b$.
If $a|b$ and $b|a$, then a & b are <u>associates</u>; write $a \sim b$.

<u>Note:</u> The only associate of 0 is 0, and the associates of 1 are the units of R.

<u>Prop 3.1:</u> $a, b \in R$ are associates iff $a = bu$ for some $u \in \mathcal{U}(R)$.

<u>Pf:</u> ($\Longrightarrow$) Assume $a \neq 0$. Since $a \sim b$, $a = bc$ and $b = ad$ for some $c, d \in R$. Now, $a = (ad)c = a(dc)$, so $dc = 1 \in \mathcal{U}(R)$. ✓
($\Longleftarrow$) If $a = bu$ and $u \in \mathcal{U}(R)$, then $b|a$, and $au^{-1} = b$, so $a|b$. $\square$

This defines an equivalence relation. The equiv. class containing $a \in R$ is $a\mathcal{U}(R)$.

<u>Note:</u> If $b \in R$ and $u \in \mathcal{U}(R)$, then $u|b$ since $b = u(u^{-1}b)$.

<u>Def:</u> If $b \in R$ is not a unit, and the only divisors of b are units & associates of b, then b is <u>irreducible</u>.

<u>Def:</u> If $0 \neq p \in R$, and $p \notin \mathcal{U}(R)$, and if $p|ab \Rightarrow p|a$ or $p|b$, then p is prime.

<u>Prop 3.2:</u> If $p \in R$ is prime, then p is irreducible

Pf: Suppose $p \in R$ is prime, but not irreducible. Then $p = ab$ with $a, b \notin U(R)$. Then (wlog) $p \mid a$, so $a = pc$, $c \in R$. But now, $p = ab = (pc)b = p(cb)$, so $cb = 1$, and thus $b \in U(R)$. $\lightning$ $\square$

Note: The converse of Prop 3.2 fails.

Example: Let $R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

Check: (HW): $3 \mid (2+\sqrt{-5})(2-\sqrt{-5}) = 9$, but $3 \nmid 2 \pm \sqrt{5}$.

Thus, 3 is prime, but not irreducible.

Def: If R is an integral domain with 1 in which every ideal is principal, then R is a principal ideal domain (PID).

Example: $R = \mathbb{Z}$ is a PID.

Claim: If $I \subseteq \mathbb{Z}$ is an ideal, and $a \in I$ is the smallest non-zero elt, then $I = (a)$.

Pf: Write $b = aq + r$, $q, r \in \mathbb{Z}$, $0 \leq r < a$. Then, $r = b - aq \in I$, so $r = 0 \Rightarrow b = qa \in \mathbb{Z}a = (a) \Rightarrow I = (a)$. $\square$

Def: A common divisor of elts a, b in an integral domain R is an elt $d \in R$ s.t. $d \mid a$ and $d \mid b$. Moreover, d is a greatest common divisor (GCD) if $c \mid d$ for all other common divisors c of a & b.

Prop 3.3: Suppose R is a PID, $a, b \in R$ are non-zero. Then a & b have a GCD, denoted $d = (a, b)$. It is unique up to associates, and $d = xa + yb$ for some $x, y \in R$.

Pf: Let $I = (a, b)$ (Ideal generated by a & b). Then $I = \{ua + vb : u, v \in R\}$. Since R is a PID, we may write $I = (d)$ for some $d \in I$, say $d = xa + yb$. ✓

Since $a, b \in (d)$, $d | a$ and $d | b$.

If c is a common divisor of a & b, then $c | xa + yb = d$, so d is a GCD for a & b. ✓ (Existence)

If d' is another GCD, then $d | d'$ and $d' | d$, so d & d' are associates ✓ (Uniqueness)

$\square$.

Cor: If R is a PID, then every irreducible element of R is prime.

Pf: Let $p \in R$ be irreducible and suppose $p | ab$ for some $a, b \in R$. If $p \nmid a$, then $(p, a) = 1$, so we may write $1 = xa + yp$ for some $x, y \in R$. Thus, $b = (xa + yp)b = x(ab) + (yb)p$.

Since $p | x(ab)$ and $p | (yb)p$, $p | x(ab) + (yb)p = b$. $\square$.

Example: Let $m \in \mathbb{Z}$, $m \neq 0, 1$. Consider the subring $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{C}$. If $m = k^2 n$, $k > 1$, then $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{n}]$, thus we may assume that m is square-free.

<u>Prop</u>: $\mathbb{Q}[\sqrt{m}] = \{r + s\sqrt{m} : r, s \in \mathbb{Q}\}$, and $\mathbb{Q}[\sqrt{m}]$ is a field; denote it by $\mathbb{Q}(\sqrt{m})$.

<u>Pf</u>: Exercise.

<u>Def</u>: If $m \neq 0, 1 \in \mathbb{Z}$ is square-free, define the ring R_m of <u>algebraic integers</u> in $\mathbb{Q}(\sqrt{m})$ as follows

* If $m \equiv 2$ or $3 \pmod 4$, then $R_m := \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$.
* If $m \equiv 1 \pmod 4$, then $R_m := \{\frac{1}{2}(a + b\sqrt{m}) : a, b \in \mathbb{Z},\ a \equiv b \pmod 2\}$

<u>Prop</u>: (HW)

(i) R_m is an integral domain with 1.
(ii) $\mathbb{Q}(\sqrt{m})$ is the field of fractions for R_m.
(iii) R_m is the set of $r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ that are roots of a monic quadratic polynomial. $x^2 + cx + d \in \mathbb{Z}[x]$.

<u>Def</u>: For $x = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, define the <u>norm</u> of x to be $N(x) = r^2 - ms^2$.

<u>Note</u>: $N(x) = (r + s\sqrt{m})(r - s\sqrt{m})$, thus $N(xy) = N(x)\,N(y)$.

<u>Exercise</u>: (i) $u \in U(R_m)$ iff $N(u) = \pm 1$.

(ii) If $m \in \mathbb{Z}$ is square-free, then $U(R_m)$ is infinite.

(iii) $U(R_{-1}) = \{\pm 1, \pm i\}$, $U(R_{-3}) = \{\pm 1, \pm \frac{1 \pm \sqrt{-3}}{2}\}$,
$U(R_m) = \{\pm 1\}$ all other square-free $m < 0$.

<u>Prop 3.4</u>: Let $m \neq 0, 1$ be square-free. Suppose for all non-zero $x, y \in R_m$ such that $y \nmid x$ and $|N(x)| \geq |N(y)|$ implies $\exists\, u, v \in R_m$ s.t. $xu \neq yv$ and $|N(xu - yv)| < |N(y)|$. Then R_m is a PID.

<u>Pf</u>: Let I be an ideal in R_m. Choose $y \in I$, $y \neq 0$ s.t. $|N(y)|$ is minimal. Given any $x \in I$, w.t.s. $y \mid x$.

Suppose not. Then $y \nmid x$ and $|N(x)| \geq |N(y)|$, so $\exists\, u, v \in R_m$ s.t. $xu - yv \neq 0$, but $|N(xu - yv)| < |N(y)|$, contradicting minimality of $|N(y)|$. Thus $y \mid x$, so $I = (y)$. $\square$

<u>Cor</u>: (i) R_{-1} is a PID.
(ii) R_{-19} is a PID.

<u>Pf</u>: (i) HW (Easy)
(ii) Long & hard!

<u>Def</u>: An integral domain R with 1 is <u>Euclidean</u> if $\exists\, d : R \setminus \{0\} \longrightarrow \mathbb{Z}$ with $d(r) \geq 0$ $\forall r \in R \setminus \{0\}$, s.t.
(i) $a, b \in R \setminus \{0\}$ and $a \mid b \Rightarrow d(a) \leq d(b)$, and
(ii) $a, b \in R$, $b \neq 0 \Rightarrow \exists\, q, r \in R$ s.t. $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

<u>Examples</u>: (1) $R = \mathbb{Z}$ (is Euclidean) Define $d(r) = |r|$.
(2) $R = F[x]$ (F a field). Define $d(f(x)) = \deg f(x)$.

<u>Prop 3.5</u>: If R is Euclidean, then $U(R) = \{x \in R \setminus \{0\} : d(x) = d(1)\}$.

<u>Pf</u>: If $a \sim b$ in $R \setminus \{0\}$, then $a \mid b \Rightarrow d(a) \leq d(b)$ and $b \mid a \Rightarrow d(b) \leq d(a)$ $\Rightarrow d(a) = d(b)$ ✓

If $u \in U(R)$, then $u \sim 1$ so $d(u) = d(1)$.

Now, suppose $x \in R \setminus \{0\}$ and $d(x) = d(1)$.

Then $1 = qx + r$, $q \in R$, $r = 0$ or $d(r) < d(x) = d(1)$.

If $r \neq 0$, then $d(1) \leq d(r)$ since $1 \mid r$.

Thus, $r = 0 \Rightarrow qx = 1 \Rightarrow x \in U(R)$. □

<u>Prop 3.6</u>: If R is Euclidean, then R is a PID.

<u>Pf</u>: Let $I \neq 0$ be an ideal. Choose $b \in I \setminus \{0\}$ with $d(b)$ minimal.

If $a \in I$, write $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

<u>Note</u>: $r = a - bq \in I$, so $d(r) \geq d(b)$ by minimality.

Therefore, $a = qb \in (b) \Rightarrow I = (b)$. □.

<u>Exercise</u>: (i) $I = (3, 2+\sqrt{-5})$ is not principal in R_{-5}

(ii) If R is an integral domain, then $I = (x, y)$ is not principal in $R[x, y]$.

Therefore, R_{-5} & $R[x, y]$ are not Euclidean.

<u>Prop 3.7</u>: If $m = -2, -1, 2$ or 3, then R_m is Euclidean with $d(r) = |N(r)|$ for all nonzero $r \in R_m$.

Pf: Take $a, b \in R_m$ with $b \neq 0$. Then $a/b \in \mathbb{Q}(\sqrt{m})$, i.e.,

$a/b = s + t\sqrt{m}$ with $s, t \in \mathbb{Q}$.

Pick $c, d \in \mathbb{Z}$ so that $|s-c| \leq \frac{1}{2}$ and $|t-d| \leq \frac{1}{2}$.

Set $q = c + d\sqrt{m}$ and $r = a - bq$.

Check: $a = bq + r$. ✓ We must show $r = 0$ or $d(r) < d(b)$.

* To show $d(r) < d(b)$, it suffices to show that $|N(r/b)| < 1$.

$$N(r/b) = (s-c)^2 - (t-d)^2 m$$

Case 1: $m = -2$ or -1:

$$0 \leq N(r/b) \leq \frac{1}{4} + \frac{1}{4} \cdot 3 = \frac{3}{4} < 1 \quad ✓$$

Case 2: $m = 2$ or 3.

$$\left.\begin{array}{l} (s-c)^2 - (t-d)^2 m \geq 0 - \frac{1}{4} \cdot 3 = -\frac{3}{4} \\ (s-c)^2 - (t-d)^2 m \leq \frac{1}{4} + 0 = \frac{1}{4} \end{array}\right\} \Rightarrow -\frac{3}{4} \leq N(r/b) \leq \frac{1}{4} \quad ✓$$

Exercise (HW): Show that Prop 3.7 holds if $m = -3, -7$, or -11.

Hint: Choose $d \in \mathbb{Z}$ nearest to $2t$ and $c \in \mathbb{Z}$ s.t. c is as near to $2s$ as possible with $c \equiv d \pmod 2$. Then set $q = (c + d\sqrt{m})/2$.

Prop 3.8: Suppose $m \in \mathbb{Z}$ is negative & square-free, but $m \neq -1, -2, -3, -7$, or -11. Then R_m is not Euclidean.

Pf: Suppose for sake of contradiction that R_m is Euclidean. Since R_5 is not a PID, $m = -6, -10$, or ≤ -13.

8

Choose a nonzero $b \in R_m \setminus U(R_m)$ s.t. $d(b)$ is minimal.

Now, for any $a \in R_m$, $\exists\, q, r \in R_m$ s.t. $a = bq + r$, $r = 0$ or $d(r) < d(b)$.

By minimality of $d(b)$, $d(r) < d(b) \Rightarrow r \in U(R_m) \Rightarrow r = \pm 1$.

(Note: It's a HW exercise to show that $U(R_m) = \{\pm 1\}$ for $m < -3$)

Thus, $r = 0, -1$, or $1 \Rightarrow a = bq,\ bq - 1$ or $bq + 1$

$\Rightarrow bq = a,\ a+1$ or $a - 1$

$\Rightarrow b \mid a,\ a+1$ or $a-1$,

Since this holds for any $a \in R$, we can pick $a = 2$.

Then $b \mid 2$ or $b \mid 3$. We'll show this can't happen.

Claim: 2 & 3 are irreducible in R_m.

(This would imply that $b = \pm 2$ or ± 3)

Note: This isn't obvious; 2 is reducible in R_{-7} and 3 is reducible in R_{-11}.

We must check several cases:

* Show 3 is irreducible if $m \equiv 1 \pmod 4$.

If it were, then $3 = (u + v\sqrt{m})/2 \cdot (x + y\sqrt{m})/2$ $\quad u, v, x, y \in \mathbb{Z}$ are nonunits.

Thus, $N(3) = 3^2 = \underbrace{(u^2 - mv^2)/4}_{=3} \cdot \underbrace{(x^2 - my^2)/4}_{=3}$

But $u^2 - mv^2 = 12$ has no integer solutions if $m = -6, -10, \le -13$.

The other cases are similar but easier.

Thus, $b = \pm 2$ or ± 3.

We've shown that $\forall a \in R_m$, $b \mid a, a-1$ or $a+1$.

- If $m \equiv 2$ or $3 \pmod 4$, take $a = 1+\sqrt{m}$.

  Clearly, neither 2 nor 3 divides a, $a-1$, or $a+1$.

- If $m \equiv 1 \pmod 4$, take $a = (1+\sqrt{m})/2$.

  Similarly, neither 2 nor 3 divides a, $a-1$, or $a+1$

Thus, $m \not\equiv 1, 2$ or $3 \pmod 4$ $\lightning$. $\square$

Cor: R_{-19} is a PID that is not Euclidean.

Def: An ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ of ideals of R terminates if it is finite, or if for some index k, $I_j = I_k$ for all $j \geq k$.

Def: A commutative ring R is Noetherian if every ascending chain of ideals terminates.

Prop 3.9: If R is a PID, then R is Noetherian.

Pf: Let $I_1 \subseteq I_2 \subseteq \ldots$ be a chain of ideals.

Note that $I := \bigcup_{k=1}^{\infty} I_k$ is an ideal, so $I = (a)$ for some $a \in R$.

Then, $a \in I_k$ for some $k \Rightarrow I_j = I_k$ for $j > k$, & thus the chain terminates. $\square$

Def: An integral domain is a unique factorization domain (UFD) if:

(i) Every nonzero element is a product of irreducible elements

(ii) Every irreducible element is prime.

<u>Prop 3.10</u>: If R is a PID, then R is a UFD.

<u>Pf</u>: Let $X = \{\text{nonzero } a \in R \setminus U(R) \text{ that can't be written as a product of irreducibles}\}$.

<u>Goal</u>: Show $X = \emptyset$.

If $X \neq \emptyset$, then pick $a_1 \in X$.
If possible, pick $a_2 \in X \setminus (a_1)$, $a_3 \in X \setminus (a_2)$, and so on.
We have an ascending chain $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$ of ideals.
Since R is a PID, it is Noetherian, so this process terminates, with some $a_n \in X$ such that $\nexists\, x \in X$ s.t. $(a_n) \subsetneq (x)$.
By construction, a_n is not irreducible or a product of irreducibles, so we may write $a_n = a_{n+1} b$, where neither are units, and $a_{n+1} \in X$ or $b \in X$.
Say wlog that $a_{n+1} \in X$. Since $b \notin U(R)$, $(a_n) \subsetneq (a_{n+1})$, a contradiction.
Therefore, $X = \emptyset$. $\square$

<u>Thm 3.11</u>: (Unique Factorization) If R is a UFD, $a \in R$ a non-zero non-unit, then $a = p_1 p_2 \cdots p_k$, where p_i is prime. This is unique, i.e, if $a = q_1 q_2 \cdots q_m$ with q_i prime, then $m = k$ and for some relabeling, $p_i \sim q_i$ for all i.

<u>Pf</u>: Existance holds because R is a UFD.

We'll show uniqueness by induction.

Base case: $k=1$ ✓

Assume it's true for $k-1$ primes, and that $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$.

Then $p_1 \mid q_1 q_2 \cdots q_m \Rightarrow p_1 \mid q_i$ for some i (since q_i's are prime).

WLOG, assume $p_1 \mid q_1$ (otherwise relabel).

Since p_1, q_1 irreducible, $p_1 \sim q_1 \Rightarrow q_1 = p_1 u$ for some $u \in U(R)$.

Thus $p_1 p_2 \cdots p_k = (p_1 u) q_2 \cdots q_m = p_1 q_2' q_3 \cdots q_m$ $\quad (q_2' = u q_2)$

$\Rightarrow p_2 \cdots p_k = q_2' \cdots q_m$. Now apply IHOP. $\square$

Cor: If R is a UFD, then if $a \in R$ is a non-zero non-unit,

$a = u p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where $n, e_1, \ldots, e_n \in \mathbb{Z}^+$ unique, $u \in U(R)$

$p_1, \ldots, p_n$ distinct primes, unique up to assoc.

Cor. (Fundamental theorem of arithmetic): Unique factorization holds in $\mathbb{Z}$.

Also holds in any field F, $F[x]$, R_{-19}, R_{-2}, R_{-1}, R_2, R_3.

Unique factorization does not hold in R_{-5}: $(2+\sqrt{-5})(2-\sqrt{-5}) = 3 \cdot 3 = 9$.

Fact: If $m<0$, then R_m is a PID iff $m = -1, -2, -3, -7, -11, -19, -43, -67$ or -163.

Fact: If $m>0$, then R_m is Euclidean (with $d(r) = |N(r)|$) iff $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57,$ or 73.

Open problem: For $m>0$, when is R_m a PID?

<u>Prop 3.12</u>: If R is a UFD, $a, b \in R$ not both zero, then a & b have a GCD, unique up to associates.

(Recall that Prop 3.3 said the same, but for a PID.

<u>Pf</u>: If $a = 0$, then b is a GCD.
If $a \in U(R)$, then 1 is a GCD.

If neither are zero, write $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $b = u p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$,
p_i distinct primes, $0 \leq e_i, f_i \in \mathbb{Z}$, $u \in U(R)$.

Set $g_i = \min\{e_i, f_i\}$ and $d = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$.

<u>Claim</u>: d is a GCD. (easy to check).

<u>Uniqueness</u>: If d, d' are GCDs, then $d \mid d'$, $d' \mid d \Rightarrow d \sim d'$. $\square$

Let I be an ideal of a comm. ring R with 1.

Let $\eta : R \longrightarrow R/I$ be the canonical quotient map.

By Thm 2.4 (substitution), $\exists$ homom $R[x] \longrightarrow (R/I)[x]$,
given by $f(x) = r_0 + r_1 x + \cdots + r_n x^n = \hat{f}(x)$.
$= \eta(r_0) + \eta(r_1) + \cdots + \eta(r_n)x^n$,

called the <u>reduction of coefficients</u> modulo I.

$$\begin{tikzcd} R \arrow[r, hook, "\phi"] \arrow[dr, "\eta"'] & R[x] \arrow[d, dashed] \\ & (R/I)[x] \end{tikzcd}$$

<u>Def:</u> Let R be a UFD. If $0 \neq f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, then define the <u>content</u> of $f(x)$ to be $d = GCD(a_0, a_1, \ldots, a_n)$ (unique up to associates).

If $f(x) = R[x]$, then we may write $f(x) = d\, f_1(x)$, where d is the content & $f_1(x)$ primitive.

In particular, if $f(x)$ is irreducible & non-const, then $f(x)$ is primitive.

<u>Thm 3.13:</u> (Gauss' lemma). Suppose R is a UFD and $f(x), g(x) \in R[x]$ primitive. Then $f(x)g(x)$ is primitive.

<u>Pf:</u> If not, then $\exists$ prime $p \in R$ dividing all coeffs of $f(x)g(x)$.

$$\begin{tikzcd} R \arrow[rr, hook, "\phi"] \arrow[dr, "\eta"'] & & R[x] \arrow[dl, dashed] \\ & R/(p)[x] & \end{tikzcd}$$

Reduce coeffs mod (p) in each polynomial to get a homom $R[x] \twoheadrightarrow R/(p)[x]$

$$h(x) \longmapsto \hat{h}(x).$$

But $\widehat{f(x)g(x)} = \hat{f}(x)\hat{g}(x) = 0$, so $\hat{f}(x) = 0$ or $\hat{g}(x) = 0$, (b/c $R/(p)$, and $R/(p)[x]$, are integral domains).

Thus, p divides all coefficients of $f(x)$ or $g(x)$. $\lightning$ $\square$

Let F_R be the field of fractions of R.

Clearly, if $f(x) \sim g(x)$ in $F_R[x]$ then $f(x) \sim g(x)$ in $R[x]$.

<u>Question:</u> When does the converse hold?
<u>Answer:</u> When $f(x)$ & $g(x)$ are <u>primitive</u>.

Prop 3.14: Let R be a UFD, $F = F_R$ the field of fractions. Suppose $f(x)$ & $g(x)$ are primitive in $R[x]$ and $f(x) \sim g(x)$ in $F[x]$. Then $f(x) \sim g(x)$ in $R[x]$.

Pf: Since $U(F[x]) = F \setminus \{0\}$, we may write $f(x) = a\, g(x)$ for some $a \in F$.

Write $a = b/c$ $(b, c \in R) \Rightarrow c\, f(x) = b\, g(x) \in R[x]$.

Note: $\text{content}(c\, f(x)) = c$, $\text{content}(b\, g(x)) = b \Rightarrow b \sim c$ in $R[x]$.

Thus, $b = cu$ $u \in U(R) \Rightarrow b/c$ is a unit in R
$\Rightarrow f(x) \sim g(x)$ in $R[x]$. $\square$

Clearly, if $f(x)$ is irreducible in $F_R[x]$, it is irreducible in $R[x]$.

Question: When does the converse hold?

Answer: Always!

Prop 3.15: Let R be a UFD, F the field of fractions, and $f(x) \in R[x]$ irreducible. Then $f(x)$ is irreducible in $F[x]$.

Pf: Since $f(x)$ is irreducible in $R[x]$, it is primitive.

Suppose $f(x) = f_1(x) f_2(x)$, both non-const elts in $F[x]$.

Write
$$f_1(x) = a_1 g_1(x), \quad f_2(x) = a_2 g_2(x) \qquad a_i \in F,\ g_i(x) \in R[x] \text{ primitive.}$$

Now, $f(x) = a_1 a_2 g_1(x) g_2(x) \overset{(\text{Prop } 3.14)}{\Longrightarrow} f(x) \sim g_1(x) g_2(x)$ in $R[x]$.

Thus, $f(x) = u\, g_1(x) g_2(x)$ for some $u \in U(R)$. $\lightning$ $\square$

Thm 3.16: If R is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD.

Pf: Since $R[x_1, \ldots, x_n] \cong (R[x_1, \ldots, x_{n-1}])[x_n]$, we may assume that $n=1$.

Let $f(x) \in R[x]$ be a nonzero element.

Claim 1: $f(x)$ is a product of irreducibles.

Use induction on $m = \deg f(x)$

Base case: $m=0$ ✓ (R is a UFD).

Now, suppose it holds true for $\deg < m$.

Write $f(x) = a f_1(x)$ where $f_1(x)$ is primitive, $a \in R$ is a unit or product of irreducibles.

If $f_1(x)$ is irreducible, we're done.

If not, then write $f_1(x) = f_2(x) f_3(x)$ with $f_i(x) < \deg f(x)$.

By IHOP, $f_i(x)$ is a product of irreducibles, so we're done. ✓

Claim 2: Every irreducible is prime.

Suppose $f(x)$ is irreducible (& thus primitive), and $f(x) \mid g(x)h(x)$ in $R[x]$. Let F be the field of fractions for R.

Prop 3.15 $\Longrightarrow$ $f(x)$ is irreducible in $F[x]$.

$F[x]$ Euclidean $\Longrightarrow$ $F[x]$ UFD $\Longrightarrow$ $f(x)$ is prime in $F[x]$.

Thus $f(x) \mid g(x)$ or $f(x) \mid h(x)$ in $F[x]$ (say wlog $f(x) \mid g(x)$).

Then for some $k(x) \in F[x]$, $g(x) = f(x) k(x)$.

Factor out contents: $g(x) = a g_1(x) = (b/c) f(x) k_1(x)$

$g_1(x)$, $k_1(x)$ primitive in $R[x]$.

Thus, $g_1(x) \sim \overbrace{f(x)k_1(x)}^{\text{Primitive by Gauss' Lemma}}$ in $F[x]$.

$\Rightarrow g_1(x) \sim f(x)k_1(x)$ in $R[x]$ (by Prop 3.14)

$\Rightarrow g_1(x) = u\, f(x)k_1(x)$ for some $u \in U(R)$.

$\Rightarrow f(x) \mid g_1(x) \mid g(x)$ in $R[x]$. ✓

$\square$

Cor: If R is a UFD, then $R[x,y]$ is a UFD that is not a PID. (e.g., (x,y) is not principal).

Summary of ring types:

$\mathbb{Z}[x]$ $\downarrow$ (PID's $\subsetneq$ Noetherian)

$$\text{Fields} \underset{\mathbb{Z},\ F[x]}{\subsetneq} \text{Euclidean domains} \underset{R_{-19}}{\subsetneq} \text{PID's} \underset{\mathbb{Z}[x]}{\subsetneq} \text{UFD's} \underset{R_{-5}}{\subsetneq} \text{Int domains} \underset{\mathbb{Z}_{2n}}{\subsetneq} \text{Comm. rings}$$

Prop 3.17: If R is a PID, every nonzero prime ideal P is maximal

Pf: Let $P \subseteq I \subseteq R$ be a chain of ideals, $P = (p)$, $I = (a)$.

Then $p \in (a) \Rightarrow p = ab$ for some $b \in R$.

Since p is prime, $p \mid a$ or $p \mid b$.

If $p \mid a$, then $a \in (p) \Rightarrow I = P$

If $p \mid b$, then $b = cp$, $c \in R$

now, $p = ab = acp \Rightarrow ac = 1 \Rightarrow a \in U(R) \Rightarrow I = R$. $\square$

Cor: If R is a PID & $p \in R$ prime, then $R/(p)$ is a field.

<u>Thm 3.18:</u> (Eisenstein Criterion): Suppose R is a PID, & $f(x) = a_0 + a_1 x + \dots + a_n x^n$ is primitive in $R[x]$.

Suppose $\exists$ prime $p \in R$ s.t.: (i) $p \mid a_i$ for $i \neq n$
(ii) $p \nmid a_n$
(iii) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible.

<u>Pf:</u> Let $K = R/(p)$, which is a field.

Then $K[x]$ is Euclidean $\Rightarrow$ $K[x]$ is a UFD.

Reduce coeffs mod (p), via homom
$$\eta : R[x] \longrightarrow K[x]$$
$$k(x) \longmapsto \hat{k}(x).$$

Suppose that $f(x) = g(x)h(x)$, where
$g(x) = b_0 + b_1 x + \dots + b_k x^k$, $h(x) = c_0 + c_1 x + \dots + c_m x^m$ are nonunits.

Both have positive degree, so $\hat{f}(x) = \hat{g}(x)\hat{h}(x) = \eta(a_n)x^n$.

Therefore, $x \mid \hat{g}(x)$ and $x \mid \hat{h}(x)$ in $K[x]$.

$\Rightarrow \eta(b_0) = 0$ & $\eta(c_0) = 0 \Rightarrow p \mid b_0$ & $p \mid c_0$
$\Rightarrow p^2 \mid b_0 c_0 = a_0$. $\lightning$ $\square$

<u>Note:</u> The converse fails, just take $f(x) = x + 1 \in \mathbb{Z}[x]$.
Actually, Eisenstein's criterion holds more generally, where R is a UFD.

<u>Example:</u> $f(x) = 6 + 2x + 4x^3 + 7x^5$ is irreducible in $\mathbb{Z}[x]$ (and in $\mathbb{Q}[x]$, by Prop 3.15).