Proof ② ⇒ ③. Since $d \in (a,b)$, $d = ax + by$ for some $x, y \in R$.
We also have $\forall\, s,t$

$$as + bt \in (a,b) = (d)$$

so $\exists\ y \in R$ s.t $as + bt = dy$
Hence $d \mid as + bt$.

③ ⇒ ④ First statement is immediate
Taking $s = 1$, $t = 0$ gives $d \mid a$
$s = 0$, $t = 1$ gives $d \mid b$

④ ⇒ ② $d = ax + by \Rightarrow d \in (a,b)$ hence $(d) \subseteq (a,b)$. Since $d \mid a$, $a \in (d)$ similarly $b \in (d)$. so $(a,b) \subseteq (d)$

Hence $(a,b) = (d)$ as wanted.

④ ⇒ ① By assumption $d \mid a$, $d \mid b$ hence d is a common divisor of a, b.
If c is a common divisor of a, b then $c \mid ax$, and $c \mid by$
hence $c \mid ax + by = d$

Thus d is gcd of a, b ∎

lemma 1.2 says prime $\Rightarrow$ irreducible in an I.D. We have that in $\mathbb{Z}$, prime = irreducible.

In fact this is true for any PID.

More precisely we have

Prop 1.5 In a PID every irreducible element is also a prime element

Proof (Exercise sheet 1)

Rmk. Every PID satisfies Ascending chain condition on principal ideals. (ACCP)

Every ascending chain of principal ideals $I_1 \subseteq I_2 \subseteq \cdots$ eventually become stationary

ie $\exists n \in \mathbb{N}$ s.t $I_k = I_n \ \forall k \geq n$.

Proof of this is also an exercise

Prop 1.5 says that in a PID
irreducible $\Rightarrow$ prime elt.
Since in any I.D prime $\Rightarrow$ irred,
in a PID prime = irreducible.
(Note 0 is neither prime nor irreducible.

For a $p \neq 0$ prime, (p) is a prime ideal
in fact in a PID, (p) is also a maximal
ideal (Recall I maximal $\Rightarrow$ I prime always
hold)
To see this: suppose $(p) \subseteq (m)$

Then $p = am$ for some $a \in R$
Now p is also irreducible (every prime is irred.)
Hence $a \in R^{\times}$ or $m \in R^{\times}$. If $m \in R^{\times}$ then
$(m) = R$ and if $a \in R^{\times}$ then $(p) = (m)$

Hence we have

$\boxed{\text{Prop 1.5}' \quad R \text{ a PID. Then every non-zero prime ideal is maximal.}}$

We have seen in Thm 1.4 that if R
is a PID, then $\gcd(a,b)$ always exist
and is equal to d where
$(a,b) = (d)$ (or an associate of d)

Since every ED is a PID, gcd's always
exist in E.Domains and the Euclidean alg.

allows us to compute the greatest common divisor of a, b algorithmically, by successive divisions.

We can write

$$a = q_0 b + r_0 \quad (0)$$

$$b = q_1 r_0 + r_1 \quad (1)$$

$$r_0 = q_2 r_1 + r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad (n)$$

$$r_{n-1} = q_{n+1} r_n \quad (n+1)$$

where r_n is the last non-zero remainder. Such an r_n exists since $N(b) > N(r_0) > \ldots > N(r_n)$ is a decreasing sequence of non-negative integers if the remainders are non-zero and such a sequence cannot continue indefinitely.

We then have

Thm 1.6 Let R be a E.D, a, b non-zero elts of R. Let $d = r_n$ the last non-zero remainder in the Euc. algorithm for a and b. Then ① $d = \gcd(a,b)$

② $(d) = (a,b)$ and in particular $d = ax + by$ for some $x, y \in R$.

Proof. By thm 1.1 since R is also a P.I.D, $(a,b) = (d)$. So the thm is proved if we can show $d = r_n$

We need to show (i) $r_n | a$ and $r_n | b$ hence $(a,b) \subseteq (r_n)$
and that (ii) $(r_n) \subseteq (a,b)$
Ie r_n is a lin. comb. of a, and b.
Both parts can be proved by induction.
(i) to prove $r_n | a$, $r_n | b$
we start with $(n+1)$st eqn
$r_{n-1} = q_{n+1} r_n$ to see

$r_n | r_{n-1}$. Clearly $r_n | r_n$
By induction (going from index n to index 0) assuming r_n divides r_{k+1} and r_k, By the
$(k+1)^{st}$ eqn $r_{k-1} = q_k r_k + r_{k+1}$ we get $r_n | r_{k-1}$
From 1st eqn we get $r_n | b$
and from 0 th eqn $r_n | a$.
(ii) To prove $(r_n) \subseteq (a,b)$ proceed again by induction from eqn (0) to eqn (n)
From eqn (0) $\Rightarrow r_0 \in (a,b)$
eqn (1) $\Rightarrow r_1 = b - q_1 r_0 \in (a,b)$
By induction assume $r_{k-1}, r_k \in (a,b)$
then $(k+1)^{st}$ eqn gives
$r_{k+1} = r_{k-1} - q_{k+1} r_k \in (r_{k-1}, r_k) \subseteq (a,b)$

Hence $(r_n) \subset (a,b)$

$\boxtimes$

Example: $R=\mathbb{Z}[i]$, $a=50-50i$, $b=43-i$

$$50-50i=(1-i)(43-i)+(8-6i)$$
$$(43-i)=(3+2i)(8-6i)+(7+i)$$
$$8-6i=(1-i)(7+i)$$

last non-zero remainder is $(7+i)$
to find the lin. combination we go backwards from the one before the last eqn

$$(7+i)=43-i-(3+2i)(8-6i)$$
$$=(43-i)-(3+2i)[(50-50i)-(1-i)(43-i)]$$

$$d=\underbrace{(-3-2i)}_{x}\underbrace{(50-50i)}_{a}+\underbrace{(6-i)}_{y}\underbrace{(43-i)}_{b}$$

In $\mathbb{Z}$, there is another way to find the gcd of 2 integers $a, b \in \mathbb{Z}$, other than the Euc. alg.
Namely we write $a = \pm p_1^{e_1} \cdots p_r^{e_r}$, $b = \pm p_1^{f_1} \cdots p_r^{f_r}$ in terms its factorization into prime factors then $\gcd(a,b) = \prod_{i=1}^{r} p_i^{\min(e_i, f_i)}$

Since $\mathbb{Z}$ is a PID, prime $\equiv$ irreducible
In general IDs, we saw this is not the case. (We always have prime $\Rightarrow$ irred.)
In $R = \mathbb{Z}[\sqrt{-5}]$ irred $\not\Rightarrow$ prime.
Rings which has the unique factorization into irreducibles are special.

Defn: Let R be an I.D. R is called a unique factorization Domain (UFD) if every $r \in R$, $r \neq 0$, $r \notin R^\times$ has the following properties
(1) r can be written as a finite product of irreducibles (not necess distinct), $r = s_1 \cdots s_n$, s_i irred.
(2) The decomposition in (1) is unique up to associates and renumbering
i.e if $r = s_1 \cdots s_n = t_1 \cdots t_m$ then $n = m$ and there is renumbering so that $s_i \sim t_i$ $i = 1, \ldots n$.

Prop 1.7 Let R be a UFD, $r \neq 0$, $r \in R$, $r \notin R^\times$.
Then r is irreducible $\Leftrightarrow$ r is prime

Proof: prime $\Rightarrow$ irred is true for any ID.

Let q be an irred elt of R. Assume $q \mid ab$ for some $a, b \in R$.
w.t.s: $q \mid a$ or $q \mid b$.
$q \mid ab \Rightarrow qc = ab$ for some $c \in R$

Since R is a UFD, $a = p_1 \cdots p_r$, $b = \tilde{p}_1 \cdots \tilde{p}_s$

and $c = p_1' \cdots p_t'$ w/ $p_i, \tilde{p}_i, p_i'$ irreducibles
Since q is irreducible, and R is a UFD

$q\, p_1' \cdots p_t' = p_1 \cdots p_r\, \tilde{p}_1 \cdots \tilde{p}_s$ is
2 factorizations of ab into irreducibles
Hence q must be associate to one of p_i's or one of $\tilde{p}_i$'s. Thus
either $q \mid a$ or $q \mid b$ (Uniqueness of factorization)
$\boxtimes$

Thm 1.8 Every PID is a UFD.

Proof: Exercise

Rmk In a PID, we've seen (Prop 1.5') prime ideal $\Rightarrow$ maximal ideal
In a UFD this is not the case
$\mathbb{Z}[X]$ is a UFD, (2) prime ideal but not maximal
$(2) \subset (2, x)$

In an UFD Prop 1.7 shows that for $0 \neq r \in R \setminus R^\times$
r is irred $\Leftrightarrow$ r is prime.

In $\mathbb{Z}$ other than Euclidean algorithm
we also use unique factorization into primes
to find gcds.

We have the analog result.

Prop Let R be a UFD, $a, b \in R$, $a \neq 0$, $b \neq 0$
Suppose $a = u p_1^{e_1} \dots p_n^{e_n}$
$b = v p_1^{f_1} \dots p_n^{f_n}$
are factorizations of a, b into irreducibles
with $e_i, f_i \geq 0$. Then

$d = p_1^{\min(e_1, f_1)} \dots p_n^{\min(e_n, f_n)}$ is a gcd of
a and b.

Pf. Obviously $d | a$, $d | b$
If $c | a$, $c | b$ then by unique factorization
$c = \tilde{u} p_1^{k_1} \dots p_n^{k_n}$ with $\tilde{u}$ a unit
and $k_i \leq \min(e_i, f_i)$ $\forall i$

Thus $c | d$.

$\square$

Rmk

We've seen

fields $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ ID.

Each inclusion is proper.

① $\mathbb{Z}$ is an ED which is not a field

② $R = \{a + b(\frac{1+\sqrt{-19}}{2}) \mid a, b \in \mathbb{Z}\}$ is a PID

but not ED. (The proof is not trivial)

See eg. J.C. Wilson "A principal ideal ring that is not a Euclidean ring" Math Mag 46 (1973) p. 34-38

or

K. Williams: Note on non Euclidean PID's. Math Mag 48 (1975)

③ $\mathbb{Z}[X]$ is a UFD but not a PID.

$(2, x)$ is not principal hence $\mathbb{Z}[x]$ not a PID

$\mathbb{Z}[x]$ is a UFD follows from

R UFD $\Longrightarrow$ $R[X]$ UFD which follows from Gauss' lemma which we'll see

④ $\mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$, $i^2 = -1$

is an ID but not UFD.

$2, 2i$ are both irreducibles and they are not associates in $\mathbb{Z}[2i]$. $i \notin \mathbb{Z}[2i]$

i is not a unit in $\mathbb{Z}[2i]$, even though it is in $\mathbb{Z}[i]$.

$4 = 2.2 = (-2i)(2i)$ are 2 distinct factorizations of 4 into irreducibles

We have seen that in an ID R, a non-zero non unit element $p \in R$ is prime $\iff$ (p) is a prime ideal.

What about the ideals generated by irreducible elements?

Prop 1.9 Let R be an I.D, $r \in R \setminus \{0\}$. Then r is irreducible $\iff$ (r) is maximal amongst all proper principal ideals of R.

i.e. if $(s) \subsetneq R$ is a proper principal ideal w/ $(r) \subseteq (s)$ then $(r) = (s)$

Proof: $(\Rightarrow)$ Suppose r is irreducible. Assume $(r) \subset (s) \subsetneq R$. Then for some $x \in R$, $r = xs$. Since r is irreducible, either $x \in R^\times$ or $s \in R^\times$. Since $(s) \neq R$, s is not a unit so $x \in R^\times$ and hence $(r) = (s)$. Hence (r) is maximal amongst proper principal ideals of R.

$(\Leftarrow)$ Suppose (r) is max'l amongst proper principal ideals and suppose $r = xs$ with x, s, non-zero non-unit elts of R

Then

$(r) = (xs) \subsetneq (x) \subsetneq R$, since neither s nor x are units

($(x) = (xs) \Rightarrow x \in (xs) \Rightarrow x = xst$ for some $t \in R$

$\Rightarrow x(1 - st) = 0 \Rightarrow st = 1 \Rightarrow s \in R^\times$)

(Since ~~s~~ x is not a unit $(x) \neq R$)

$\boxtimes$

Cor 1.10 If R is a PID, $0 \neq r \in R$, $r \notin R^\times$. Then r is irreducible $\Leftrightarrow (r)$ is a maximal ideal

This gives another way to see that in a PID every non-zero prime ideal is maximal

Rmk. We always have that PID $\Rightarrow$ UFD but UFD $\not\Rightarrow$ PID. In fact if R is a UFD. Then R is a PID $\Leftrightarrow$ every non-zero prime ideal is maximal.

($\Rightarrow$) is Cor. 1.10

($\Leftarrow$) Can be proved using

Claim 1: If R is a UFD, and p an irred elt, then (p) is a prime ideal

Claim 2 If R is a UFD s.t every non-zero prime ideal is maximal. Then every non-zero prime ideal is principal

<u>Claim 3</u> If every prime ideal in R is principal then all ideals are principal.

(Proof of Claim 3 needs Zorn's lemma)

[Zorn's lemma: Let S be a partially ordered set. If every totally ordered sset of S has an upper bound, then S has a maximal elt.]

We know that for R a comm ring an ideal I is maximal $\Leftrightarrow$ R/I is a field.

On the other hand Cor 1.10 says for a PID, $r \notin R^\times$ non zero r is irred $\Leftrightarrow$ (r) is maximal

Putting these together gives a method to construct fields K containg a copy of a field F.

- More precisely: Let F be a field, then $F[x]$ is a ED, hence a PID. Take an irred poly f in $F[x]$. Then $F[x]/(f)$ is a field containg an isom. copy of F as a subfield i.e. the image of constant polynomials

Hence to construct fields contay F, we need to find ways to decide when a given poly $f \in F[x]$ is irreducible.

Next we study polynomial rings in a bit more detail.

To summarize:

- Fields $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ ID

$$\text{Fields} \subset \underset{\mathbb{Z}}{\text{ED}} \subset \underset{\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]}{\text{PID}} \subset \underset{\mathbb{Z}[x]}{\text{UFD}} \subset \underset{\mathbb{Z}[2i],\ \mathbb{Z}[\sqrt{-5}]}{\text{ID}}$$

$R \neq I$ an ideal in a I.D. R.

I is prime $\iff$ R/I an I.D.

$\iff$ $\forall a, b \in R$ with $ab \in I$, either $a \in I$ or $b \in I$

I is maximal $\iff$ R/I is a field

$\iff$ $\forall$ ideals J s.t. $I \subset J$ we have $J = I$ or $J = R$.

- I maximal $\implies$ I prime always.

Thm R a PID, $0 \neq I = (p)$. TFAE

1. p is prime
2. p is irreducible
3. (p) prime ideal
4. (p) max'l ideal

(1) $\iff$ (2): true in any ID, lemma 1.2; Prop 1.7 since any PID also a UFD

(3) $\iff$ (4): Rmk after Cor 1.10

(2) $\iff$ (4): Cor 1.10

Thm R UFD, $0 \neq p \in R$. TFAE

1. p is irreducible
2. p is prime
3. (p) is a prime ideal

(1) $\iff$ (2): Prop 1.7

(2) $\iff$ (3): Lemma 1.2.

Note in a UFD, there are prime ideals $\neq 0$ which are not maximal

eg $R = \mathbb{Z}[x]$. (x) is a prime ideal, not maximal $\quad (x) \subset (2, x)$

$\left(\varphi : \begin{array}{l} R \to \mathbb{Z} \\ f(x) \to f(0) \end{array} \quad \ker \varphi = (x) \quad R/\ker\varphi \cong \mathbb{Z} \text{ I.D.} \right)$

In UFD, PID, ED's $\gcd(a,b)$ always exists

In a PID $d = \gcd(a,b) \Leftrightarrow (d) = (a,b)$

In this case $\exists$ x, y s.t $ax + by = d$.

- In a ED Euclidean alg. can be used to find $\gcd(a,b) = d$
  d is the last non-zero remainder
  We can again find x, y s.t $ax + by = d$.
- In a UFD, we write $a = p_1^{e_1} \cdots p_n^{e_n}$
  $b = p_1^{f_1} \cdots p_n^{f_n}$

then $\gcd(a,b) = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$

- ! It is not in general the case that

$d = ax + by$ for some x, y

eg. let $R = F[X, Y]$ which is a UFD

X, Y are relatively prime
But no lin combination of X, Y is 1

Indeed if $cX + dY = f$ for some $f \in F[X,Y]$
then $\varphi_{(0,0)} : F[X,Y] \to F$ is a hom
$g \to g(0,0)$

$\varphi(f) = \varphi(cX + dY) = 0$
$\varphi(1) = 1 \neq 0$.