ED's, PID's, UFD's, ID's:

- ID = Integral Domain = commutative ring w/ iden. $1 \neq 0$ and no zero-divs.
- UFD = Unique Factorization Domain

Defs: ① If R is an ID then a non-zero element $a \in R \setminus R^\times$ irreducible if a is not a product of non-units.

Otherwise a is called reducible.

② A nonzero element $a \in R$ is prime if (a) is a prime ideal.

Note: A prime element is always irreducible, but the converse is not true in general. (exercise)

③ For $a, b \in R$, we say that a and b are associates if $\exists u \in R^\times$ s.t. $a = ub$.

We say that an ID R is a UFD if every nonzero element $a \in R \setminus \{0\}$ can be written in the form

$a = u p_1 p_2 \cdots p_k$, where $u \in R^\times$, $p_1, \dots, p_k$ are irreducible elements, and this representation is unique up to associates and order of factors.

Ex: 1) These are some UFDs:

$\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$,

$\mathbb{Z}[\sqrt{-1}] = \{a+b\sqrt{-1} : a,b \in \mathbb{Z}\}$ (Gaussian integers)

2) $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b \in \mathbb{Z}\}$ is not a UFD.

To see this:

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Claim: i) $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are irreducible

ii) 2 is not an associate of $1+\sqrt{-5}$, $1+\sqrt{-5}$

To prove this, use the fact that the map

$N : \mathbb{Z}[-\sqrt{5}] \to \mathbb{Z}$ defined by

$$N(a+b\sqrt{-5}) = a^2+5b^2$$

satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$.

$N(2) = 4$, $N(3) = 9$

$N(1+\sqrt{-5}) = 6$, $N(1-\sqrt{-5}) = 6$

Also: multiplicativity $\Rightarrow N(u) = \pm 1$, if u is a unit.

These facts easily verify both parts of the claim.

• PID = principal ideal domain

an integral domain where every ideal is principal.

• ED = Euclidean domain

An integral domain R is called a Euclidean domain (ED) if there is a function $\phi : R \setminus \{0\} \to \mathbb{N}$ with the property that $\forall a, b \in R$ with $b \neq 0$, $\exists\, q, r \in R$ s.t.

$$a = bq + r \text{ and } (r = 0 \text{ or } \phi(r) < \phi(b)).$$

Thm: We have the following sequence of implications:

$$(ED) \Rightarrow (PID) \Rightarrow (UFD) \Rightarrow (ID).$$

Exs: 1) $R = \mathbb{Z}$ is an ED, with $\phi(n) = |n|$. (division algorithm)

2) $R = \mathbb{Z}[i]$ is an ED with $\phi(a+bi) = a^2 + b^2$. (needs proof)

3) $R = \mathbb{Z}[\sqrt{-5}]$ is not a UFD, so it's also not a PID or an ED.

(*) 4) Let F be a field. Then $R = F[x]$ is an ED, with $\phi(f) = \deg f$.

(*) Division algorithm for $F[x]$:

$\forall f, g \in F[x]$, $g(x) \neq 0$, $\exists\, q, r \in F[x]$ s.t.

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg g.$$

Idea of proof: Use induction on $\deg(f)$:

$f = a_n x^n + \cdots + a_0$, $a_n \neq 0$

$g = b_m x^m + \cdots + b_0$, $b_m \neq 0$

- If $\deg f < \deg g$ then $q(x) = 0$ and $r(x) = f(x)$.
- If $\deg f \geq \deg g$ then

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + h(x), \quad \deg h < \deg f.$$

By inductive hyp.,

$$h(x) = g(x) q_1(x) + r(x), \quad \deg r < \deg g. \quad \blacksquare$$

So if F is a field, $F[x]$ is an ED, PID, and UFD.

5) $\mathbb{Z}[x]$ is not a PID, because $(2, x)$ is not a principal ideal.

So: $\mathbb{Z}[x]$ is ~~an~~ ED.

However: $\mathbb{Z}[x]$ is a UFD. (Gauss's lemma, next time)

6) Example (without proof) of a PID which is not an ED:

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.