- $\mathbb{Z}$ is a PID :

$I \subseteq \mathbb{Z}$ an ideal is a subgroup of $(\mathbb{Z},+)$. All subgroups of cyclic groups are cyclic $\Rightarrow I = (a)$.

- $K[x]$ is a PID : Same as the proof of

If $I=(0)$ we are done. If not, choose $f \in I$ of smallest degree. Then $I = (f)$. Indeed, if $g \in I$, then by division algorithm, $g = fq + r$. If $\deg r < \deg f$ then
$r = g - fq \in I$, contradicting minimality.
Thus $r = 0$.

Warning $(\bar{2}x^4+\bar{1})(\bar{2}x^4+\bar{1}) = \bar{4}x^8 + \bar{4}x^4 + \bar{1}$

$= \bar{1}$ in $(\mathbb{Z}/4\mathbb{Z})[x]$.

It's crucial that we are working in $K[x]$ with K a field.

- $\mathbb{C}[x,y]$ not a PID. Consider (x,y).

Defn Let R be a ring. A non-zero element $x \in R$ is called irreducible if it's not a unit and if $x = ab$ is ANY factorization, then a or b is a unit.

(Basically this means x is not "factorable")

Ex. $\mathbb{Z}$, $\mathbb{C}[x]$, $\mathbb{R}[x]$, $K[x]$

Defn An integral domain R is called a unique factorization domain (UFD) if every non-zero element that is not a unit can be written as a product of finitely many irreducible elements and this is unique i.e. if $a_1 \cdots a_k = b_1 \cdots b_m$ are two such products then $k = m$ and, after reordering, a_i is a unit times b_i

Ex. • $\mathbb{Z}$ is a UFD [This is unique prime factorization]
But we will give another proof of this

• $K[x]$ is a UFD
• $\mathbb{Z}[x]$ is a UFD (Hard: Follows from R UFD $\Rightarrow R[x]$ UFD)

• $\mathbb{Z}/6\mathbb{Z}$ is not a UFD because it's not a domain. But anyway notice $3 = 3 \cdot 3$

• $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ is a domain but not a UFD:
(Hwk) $6 = 2 \cdot 3$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. One needs to check $2, 3, 1 \pm \sqrt{-5}$ are irreducible and don't differ by a unit.

Thm PID is a UFD

Lemma Let R be a PID and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ an infinite chain of ideals. Then the chain is "stationary" i.e. $\exists\, n \in \mathbb{Z}_{\geq 1}$ s.t.
$$I_n = I_m \quad \forall\, m \geq n.$$
PF Let $I = \bigcup_i I_i$ be the union of all the ideals.

Note that this is an ideal. Indeed $0 \in I$ and if $x, y \in I \Rightarrow x \in I_k$ and $y \in I_\ell$. Wlog assume $\ell \geq k$, then by $I_k \subseteq I_\ell$

$\Rightarrow x, y \in I_\ell$

$\Rightarrow x + y \in I_\ell \subseteq I$. Thus I is closed under $+$

Similarly $\forall r \in R$, $rx \in I_k \subseteq I \Rightarrow I$ is an ideal.

Since R is a PID, $I = (b)$. But $b \in I_n$ for some $n \Rightarrow I = (b) \subseteq I_n \subseteq I$

$$\Rightarrow I = I_n$$

$$\Rightarrow I_n = I_m \quad \forall m \geq n \quad \blacksquare$$

We will now partially prove the theorem i.e. we will show every non unit / non-zero $x \in R$, a PID, can be factored into irreducible elements:

Pf (sketch) If x is irreducible we are done. If not $x = x_1 y_1$ with x_1, y_1 not units. Thus $(x) \subsetneq (x_1)$. If x_1 is not irreducible we write $x_1 = x_2 y_2$ and get $(x_1) \subsetneq (x_2)$. If x_2 is not irreducible we keep going and obtain $(x_1) \subsetneq (x_2) \subsetneq \cdots$. Since R is a PID this stops. Thus eventually we obtain an irreducible factor of x! So write $x = p_1 y$ with p_1 irreducible and now apply the same argument to y. Eventually we obtain $x = p_1 \cdots p_r$ with p_i irreducible (If not $(x) \subsetneq (p_2 \cdots) \subsetneq (p_3 \cdots) \subsetneq (p_4 \cdots)$ would be an infinite chain) $\blacksquare$