Ex. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

**Pf.** In a UFD any irreducible element is prime. So it is enough to find an irreducible element which is not prime.

Claim 1. 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

**Pf of claim 1.** Suppose $3 = (a_1 + \sqrt{-5} b_1)(a_2 + \sqrt{-5} b_2)$ and $a_1, b_1 \in \mathbb{Z}$.

$$q = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$$

$\Rightarrow$ either $a_1^2 + 5b_1^2 = a_2^2 + 5b_2^2 = 3$ or $\exists i, a_i^2 + 5b_i^2 = 1$.

Notice that, if $b_i \neq 0$, then $a_i^2 + 5b_i^2 \geq 5$; and 3 is not a perfect square. Hence $\forall a_i, b_i \in \mathbb{Z}, a_i^2 + 5b_i^2 \neq 3$. Therefore $\exists i, a_i^2 + 5b_i^2 = 1$, which implies $(a_i + \sqrt{-5} b_i)(a_i - \sqrt{-5} b_i) = 1$.

$$\Rightarrow a_i + \sqrt{-5} b_i \in \mathbb{Z}[\sqrt{-5}]; \text{ and the claim follows.}$$

Claim 2. $3 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$; this is clear.

Claim 3. $3 \not| 1 \pm \sqrt{-5}$.

**Pf of claim 3.** If not, $\exists a, b \in \mathbb{Z}, 3(a + \sqrt{-5} b) = 1 \pm \sqrt{-5}$.

$$\Rightarrow 3a = 1 \text{ and } 3b = 1 \text{ (here we are using the fact that } \sqrt{-5} \notin \mathbb{Q}); \text{ which is a contradiction.}$$
Hence 3 is not prime. Therefore \( \mathbb{Z} [\sqrt{-5}] \) is not a UFD.

Next we would like to show \( \mathbb{Z} [x] \) is a UFD, but it is not a PID.

It will be done in many steps:

**Proposition.** \( \mathbb{R} [x] \) is a PID \( \iff \mathbb{R} \) is a field.

**Thm.** \( \mathbb{R} [x] \) is a UFD \( \iff \mathbb{R} \) is a UFD.

Clearly the above Prop. and Thm imply that \( \mathbb{Z} [x] \) is a UFD and it is not a PID.

To prove the above proposition we start with the following lemma:

**Lemma.** Suppose \( A \) is a unital commutative ring and \( \mathcal{A} \triangleleft A \).

Let \( \phi : A [x] \to (A / \mathcal{A}) [x] \), \( \phi (\sum a_i x^i) = \sum (a_i + \mathcal{A}) x^i \).

Then \( \phi \) is an onto ring homomorphism, and

\[
\ker \phi = \mathcal{A} [x] := \left\{ \sum a_i x^i \mid a_i \in \mathcal{A}, a_i = 0 \text{ except for finitely many } i \right\}.
\]

**Pf.** (Exercise)

**Cor.** In the above setting, \( A [x] / \mathcal{A} [x] \cong (A / \mathcal{A}) [x] \). (Pf. Use 1st iso. thm.)
Cor. \( \mathfrak{p} \in \text{Spec}(A) \iff \mathfrak{p}[x] \in \text{Spec}(A[x]) \).

\[ \begin{align*}
\mathfrak{p} \in \text{Spec}(A) & \iff A/\mathfrak{p} \text{ is an integral domain} \\
& \iff (A/\mathfrak{p})[x] \text{ is an integral domain} \\
& \iff A[x]/\mathfrak{p}[x] \text{ is an integral domain} \\
& \iff \mathfrak{p}[x] \in \text{Spec}(A).
\end{align*} \]

\[ \begin{align*}
\mathfrak{p} \text{ of proposition.} & \iff R: \text{field} \implies \text{we have long division in } R[x] \\
& \implies R[x] \text{ is a Euclidean domain} \implies R[x] \text{ is a PID.}
\end{align*} \]

\( \iff \) Suppose \( a \in R \setminus \{0\} \). We have to show \( a \in R^* \); this is equivalent to saying \( \langle a \rangle = R \). Suppose to the contrary that \( \langle a \rangle \) is a proper ideal. So there is a maximal ideal \( \mathfrak{m} \) s.t. \( \langle a \rangle \subseteq \mathfrak{m} \). Hence \( \mathfrak{m} \in \text{Spec}(R) \); and by the previous corollary \( \mathfrak{m}[x] \in \text{Spec}(R[x]) \).

Since \( R[x] \) is a PID, \( \text{Spec}(R[x]) = \text{Max}(R[x]) \cup \{0\} \).

As \( a \neq 0 \) and \( a \in \mathfrak{m}[x] \), we deduce that \( \mathfrak{m}[x] \in \text{Max}(R[x]) \).

Therefore \( R[x]/\mathfrak{m}[x] \) is a field. On the other hand,
\[ R/\mathfrak{m} \cong (R/\mathfrak{m})[x] ; \text{ and } (R/\mathfrak{m})[x] \cong (R/\mathfrak{m})^x \text{ as } R/\mathfrak{m} \text{ is a field. So } (R/\mathfrak{m})[x] \text{ cannot be a field, which gives us a contradiction.} \]

To prove the mentioned theorem, we start with the definition of greatest common divisor of elements of a ring.

\textbf{Def.} Suppose \( a, b \in \mathcal{D} \); we say \( a \mid b \) if \( \exists c \in \mathcal{D} \) s.t. \( b = ac \).

We say \( d \) is a greatest common divisor of \( a_1, \ldots, a_n \) if
\begin{enumerate}
  \item \( \forall i, \ d \mid a_i \); \text{ (2) if } d' \mid a_i \text{ for any } i; \text{ then } d' \mid d.
\end{enumerate}

\textbf{Lemma.} Suppose \( \mathcal{D} \) is an integral domain;

\begin{enumerate}
  \item \( d \) is a gcd of \( a_1, \ldots, a_n \) if and only if \( \langle d \rangle \) is the \underline{minimum} principal ideal which contains \( \langle a_1, \ldots, a_n \rangle \).
  \item If \( d_1 \) and \( d_2 \) are two gcd's of \( a_1, \ldots, a_n \), then \( \langle d_1 \rangle = \langle d_2 \rangle \) (and so \( d_1 \sim d_2 \)).
\end{enumerate}

\textbf{Proof.} (a) \( d \mid a_i \Rightarrow a_i \in \langle d \rangle \Rightarrow \langle a_1, \ldots, a_n \rangle \subseteq \langle d \rangle \).

- If \( \langle a_1, \ldots, a_n \rangle \subseteq \langle d' \rangle \), then \( d' \mid a_i \forall i \).

Hence \( d' \mid d \), which implies \( \langle d \rangle \subseteq \langle d' \rangle \).
(b) By part (a), \(<d_1>\) and \(<d_2>\) are the minimum principal ideal that contains \(<a_1, \ldots, a_n>\); and so \(<d_1> = <d_2>\). As \(D\) is an integral domain, we deduce that \(d_1 \sim d_2\). ■