UFD: I

Let \( R \) be an integral domain.

Define

(i) \( r \in R \) is said to be \underline{irreducible} if \( r \) is not a \( \text{unit} \) and \( ab = r \Rightarrow a \in R \) is a unit or \( b \in R \) is a unit.

(ii) \( p \in R \) is called a \underline{prime} if \( (p) \) is a prime ideal.

Lemma: \( R \) an integral domain. \( p \) prime

\[ \Rightarrow p \text{ irreducible.} \]

Proof: Suppose \( p = ab \). Then \( ab \in (p) \), which is a prime ideal so \( a \in (p) \) or \( b \in (p) \).

We can assume \( a \in (p) \) (so \( a = cp \), \( c \in R \)).

Let \( p = pcb \). By the cancellation law

\[ cb = 1 \Rightarrow b \text{ is a unit,} \]

\[ \Rightarrow p \text{ is irreducible.} \]
A Unique Factorization Domain (UFD) is an integral domain \( R \) s.t.

(i) each element \( r \in R \) has a factorization

\[ r = u \cdot p_1 \cdots p_n \]  

with \( n \geq 0 \)

\( u \in R \) a unit, \( p_i \in R \) irreducible

(ii) let \( r = v \cdot q_1 \cdots q_m \) with \( m \geq 0 \) be a 2nd factorization with \( v \) a unit.

Then \( M = N \) and there is a relabelling such that

\[ q_i = u_i \cdot p_i \]  

for some unit \( u_i \).

\[ q_i \sim p_i \]  

"associates"

Right now the only real example of a UFD we have is \( \mathbb{Z} \) which is a UFD by the Fundamental Theorem of Arithmetic.
Fields are trivial example of UFDs.
we will rectify this shortly.
But first we have a converse to the
previous lemma for UFDs.

Prop Let \( R \) be a UFD. Then irreducible
elements are prime.

PF Let \( r \to j \) not a unit be
irreducible. Let \( ab \in (r) \), i.e.
\( ab = sr \) for some \( s \)

Let \( a = u_1 p_1 \ldots p_i \) \( b = v_1 q_1 \ldots q_j \)
\( s = w t \) with the factorizations.

So \( u_1 v_1 p_1 q_1 \ldots q_j \) and
\( w t \ldots t \) in \( r \) are 2 factorizations
of \( ab \). By the uniqueness part of the
of a UFD, \( r \) must be canceled

to some \( p_n \) or \( q_m \) i.e.

\[
p_n = a \sqrt{r} \quad \text{or} \quad q_m = b \sqrt{s} \quad \text{such that} \quad a \in \mathbb{R} \quad \text{or} \quad b \in \mathbb{R}
\]

\[\Rightarrow \quad a \in \mathbb{R} \quad \text{or} \quad b \in \mathbb{R} \]

\[\Rightarrow \quad (\cdot) \quad \text{pure.} \]

\underline{Example}

\[\exists \sqrt{5} \quad \text{is not a UFD. First of all } \sqrt{5} \quad \text{is irreducible. To see this suppose} \]

\[3 = \alpha \beta \quad \Rightarrow \quad \alpha = a_1 + b_1 \sqrt{5} \quad \text{and} \quad \beta = a_2 + b_2 \sqrt{5} \]

Then taking absolute values (of complex nos.)

\[q = 3^2 = (a_1^2 - b_1^2)^2 = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2) \]

Suppose \( b_1 = 0 \). Then the integer \( \geq 5 \) clearly

\[q = 9, \quad \text{so} \quad q_1 = \pm 1, \quad a_1 = \pm 2 \]

would then necessarily have \( a_2 = \pm 1, \quad b_2 = 0 \)

i.e. \( 3 = \pm x, \quad x \in \mathbb{Q} \setminus \mathbb{Z} \) which is absurd.
So \( g_1 = 0 \) and by the same argument, \( b_2 = 0 \) so \( a_1 f \in \mathbb{Z} \). But \( 3 \in \mathbb{Z} \) is irreducible (its prime).

\[ 3 \in \mathbb{Z} \left[ \sqrt{-5} \right] \text{ irreducible} \]

So \( \mathbb{Z} \left[ \sqrt{-5} \right] \) is not principal.

So 3 elements which are irreducible but not prime in \( \mathbb{Z} \left[ \sqrt{-5} \right] \) and hence it can't be a UFD.

We are still lacking good examples of UFDs. We will show \( \mathbb{R} \) UFD which will start to give \( \mathbb{R} \times \mathbb{R} \) UFD which will start to give good examples of them (like \( \mathbb{Z} \)), \( \mathbb{Z} \left[ x, y \right] \) etc. To begin.

Thus (Polynomial Division)

Let \( F \) be a field and \( a(x), b(x) \in F[x] \)
\[ b(x) \to 0, \]
Then \( q(x), r(x) \in F[x] \)

\[ q(x) = q(x)b(x) + r(x) \quad \text{with} \]
\[ \gamma(x) = 0 \quad \text{or} \quad \deg r(x) < \deg b(x) \]

The theorem is obvious if \( a = 0 \) so

Assume \( a(x) \) is not the zero poly.

Let \( n = \deg a(x), m = \deg b(x) \).

If \( m > n \) take \( q = 0, r(x) = a(x) \).

So may assume \( n \leq m \). We proceed by induction on \( n \).
If \( n = 0 \) then \( a(x), b(x) \) are constants \( \in F \).

Now let \( a(x) = a_0 + a_1x + \ldots + a_mx^m \)
\( b(x) = b_0 + b_1x + \ldots + b_mx^m \).
Consider
\[ \phi(x) = a(x) - \frac{a_n x^{n-m} b(x)}{b_m} \]

(assume that \( n \geq m \) and \( F \) a field)

Then we have eliminated the term of highest degree \( a_n x^n - \frac{a_n x^{n-m} b_m x^m}{b_m} = 0 \)

so \( \deg \phi(x) < n \).

By induction
\[ \phi(x) = q'(x) b(x) + r(x) \]
with \( r(x) = 0 \) or \( \deg r'(x) < \deg b(x) \)

So
\[ a(x) = q'(x) b(x) + r(x) + a_n x^{n-m} \]
\[ a(x) = (q'(x) + \frac{a_n x^{n-m}}{b_m}) b(x) + r(x) \]

Take \( q(x) \) giving the claim.
Our first step will be to use the Polynomial Division Theorem to show that \( \mathbb{F}[x] \) is a Principal Ideal Domain (PID) for \( \mathbb{F} \) a field.

**Definition** A integral domain \( R \) is called a Principal Ideal Domain (PID) if every ideal \( I \) is principal (i.e., \( I = (x) \) for some \( x \in R \)).

Suppose \( \mathbb{F} \) a field. Then \( \mathbb{F}[x] \) is a PID.

If let \( I \subseteq \mathbb{F}[x] \) be an ideal.

(0) is a principal ideal, so assume \( I \neq (0) \). Let \( f \) be an element of \( I \) of least degree. We claim \( (f) = I \). Obviously \( (f) \subseteq I \). Now
let \( g \in \mathcal{I} \). Then write
\[
g = qf + r \quad \text{for} \quad q, r \in \mathcal{F} \mathcal{G} \mathcal{A}
\]
with \( r = 0 \) or \( \deg r < f \).

So \( r = g - qf \in \mathcal{I} \). As \( f \) is the least degree, we must have \( r = 0 \).

\[
\Rightarrow g = qf + (I)
\]

Our immediate goal is to prove
\[
\text{PID } \Rightarrow \text{UPD}
\]

So in particular \( \mathbb{Z}[x] \) is a UPD.

**Def.** (Noetherian Rings)

A ring \( R \) is called Noetherian if it satisfies the ascending chain condition, i.e.,

any chain of ideals

\[
I_1 \subseteq I_2 \subseteq \ldots \subseteq I_{k-1} \subseteq I_k \subseteq \ldots
\]
Then $I \neq n \cdot t$,

$I_n = I_{n+1} = \ldots$

(i.e., $I_k = I_n \cup k \cdot t$ or the claims stabilize.)