Theorem

\[ \text{R UFD } \Rightarrow \text{ R[x] UFD} \]

Proof

(i) Existence of factorization

Last time saw it suffices to show existence of factorization for \( p(x) \in \mathbb{F}[x] \) primitive.

Let \( \mathbb{Q} \) be the field of fractions of \( \mathbb{R} \).

If \( \mathbb{Q}[x] \) is a P.I.D. \( \Rightarrow \mathbb{Q}[x] \) is a U.F.D.

If \( p(x) = A(x)B(x) \), \( A(x), B(x) \in \mathbb{Q}[x] \) units

Then we showed (Gauss' Lemma)

\[ \exists a, b \in \mathbb{Q} \quad \text{s.t.} \quad a(x) = aA(x) \in \mathbb{R}[x] \]

\[ b(x) = bB(x) \in \mathbb{R}[x] \]
and $p(x) = a(x) b(x)$

Then if $p(x) = A_1(x) \ldots A_n(x)$ is a factorization into irreducibles in the UFD $R(x)$

Have $p(x) = a_1(x) \ldots a_n(x)$

$a_i(x) \in R_i(x) \subset R(x)$ for some

$k \in \mathbb{Q}$

Further $p(x)$ primitive $\Rightarrow a_i(x)$ primitive

Hence

$A_i(x) \in \mathbb{Q}[x]$ irreducible

$\Rightarrow a_i(x) \in \mathbb{Q}[x]$ irreducible (as $a_i(x)$ primitive)

So have factorized $p(x)$ as a product of irreducibles.

(Cii) Uniqueness of factorization

Notice that $a_i(x) \in \mathbb{Q}[x]$ irreducible and $\deg a_i(x) \geq 1$
$\Rightarrow a_i(x)$ primitive.

Suppose

$p(x) = r_1 \cdots r_n \; a_1(x) \cdots a_n(x)$ is a

factorization into irreducibles, $\deg r_i = 0$, $\deg a_i(x) \geq 1$

Then $r_1 \cdots r_n$ = gcd of coeffs of $p(x)$

($= \text{"content" of } p(x)$)

and $a_1(x) \cdots a_n(x)$ is primitive.

(else $f \mid p$ prime dividing each $a_i$

as $\mathbb{R} \text{ UFD } \Rightarrow d \mid a_i$ for some $d \in \mathbb{R}$)

$\mathbb{R}$ UFD, $r_i$'s are the essentially unique

prime factors of the content of $p(x)$ so

it suffices to show, if

$q(x) := a_1(x) \cdots a_n(x)$ primitive, $\deg q \geq 0$

then the factorization of the primitive poly $q(x)$

is unique,

let $q(x) = b_1(x) \cdots b_m(x)$, $b_i \in \mathbb{R}[x] \text{ irreduc}

poly$.  

As \( q \) is primitive, \( b_i(x) \) are all primitive.

By uniqueness of factorization in \( \mathbb{Q}(\sqrt{d}) \),

we can assume \( n = m \) and \( a_i(x) \) is

associated to \( b_i(x) \) in \( \mathbb{Q}(\sqrt{d}) \), i.e.,

\[
\exists \delta \in \mathbb{Q} \quad \text{s.t.} \quad a_i(x) = \delta \cdot b_i(x)
\]

\[
\text{for } x_i, y_i \in \mathbb{R}
\]

\[
y_i \cdot a_i(x) = x_i \cdot b_i(x)
\]

As \( a_i, b_i \) primitive, the gcd of the

coefficients ("content") of \( y_i \cdot a_i(x) \) is \( y_i \)

whereas the content of \( x_i \cdot b_i(x) \) is \( x_i \).

As the gcd is unique up to

associate,

\( x_i \) and \( y_i \) are associated

\( \Rightarrow \ x_i / y_i \in \mathbb{R}^* \) is a unit in \( \mathbb{R} \)
\[ a_i(x), b_i(x) \text{ are associates in } \mathbb{R}[x] \]

**Euclidean Domains**

**Definition**

An integral domain \( R \) is called an **integral domain** if there is a function \( N : R \to \mathbb{Z}_{\geq 0} \) with \( N(0) = 0 \) and \( N(x) > N(y) \) for all \( x, y \in R \) with \( x \neq y \). We can find \( q, r \in R \) such that

\[ a = qb + r \]

with \( r = 0 \) or \( N(r) < N(b) \).

The function \( N \) is called the **norm**.

**Examples**

(i) \( \mathbb{Z} \) with \( N(a) = |a| \)

(ii) \( F[x] \) with \( F \) a field and
\[ N(p(x)) = \deg p(x). \]

Two main facts we will prove:
(i) Every Euclidean domain is a PID
(ii) Have an algorithm (the Euclidean algorithm) to compute the gcd in a Euclidean Domain

**THEM R Euclidean Domain**

\[ \Rightarrow R \text{ P.I. D} \]

If let \( I \neq (0) \) CR be an ideal.
Let \( d \in I \) be an nonzero element with minimum norm \( N(d) \).
We claim \((d) = I\). Let \( a \in I \).
Then \( r \leq r \) with \( a = qd + r \) and \( r = 0 \) or \( N(r) < N(d) \). As \( r = a - qd \in I \)
and if the minimum norm, we must have \( r = 0 \Rightarrow a \in \mathfrak{c}(d) \).

As \( R \neq \mathfrak{d} \Rightarrow R \neq \mathfrak{u} \neq \mathfrak{d} \)
we may talk about the gcd of two elements \( a, b \in R \setminus \{0\} \) (gcd is defined up to associates).

**Proposition:** Let \( R \) be E.D. and \( a, b \) nonzero elements of \( R \). Then any generator of \( (a, b) \) is a gcd of \( a, b \).

**Proof:** Suppose \( (a, b) = (d) \).

Then \( a \in (d), \ b \in (d) \Rightarrow d \mid a \) and \( d \mid b \).

Suppose \( e \mid a \) and \( e \mid b \)

i.e. \( a = xe, b = ye \) so \( (a, b) \leq (e) \).

Then \( (d) \leq (e) \Rightarrow d = ye \)

\[ \Rightarrow e(d). \]
The Euclidean Algorithm is as such:

Let \( a, b \in \mathbb{R} \) an E.D. / 6 to 1

Then we can write:

\[
\begin{align*}
\qquad a &= q_0 b + r_0 \quad (0) \\
\qquad b &= q_1 r_0 + r_1 \quad (1) \\
\qquad r_0 &= q_2 r_1 + r_2 \quad (2) \\
\qquad r_1 &= q_3 r_2 + r_3 \quad (3) \\
\vdots & \quad \qquad \vdots \\
\qquad r_{n-2} &= q_n r_{n-1} + r_n \quad (n) \\
\qquad r_{n-1} &= q_{n+1} r_n \quad (n+1)
\end{align*}
\]

where \( r_n \) is the last nonzero remainder.

This algorithm always terminates after finitely many steps because

\[ N(b) \geq N(r_0) > N(r_2) > N(r_3) \mathrel{\ldots} \]

and any sequence of integers \( \geq 20 \)
eventually reaches 0.

Thus let \( r_n \) be the last nonzero remainder in the Euclidean Algorithm above. Then \( r_n \) is a gcd of \( a, b \).

From (n+1) we see

\[ r_{n-1} \in (r_n). \]

But then (n) shows

\[ r_{n-2} = q_n r_{n-1} + r_n \in (r_n) \]

Then (n-1):

\[ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \in (r_n) \]

\[ \Rightarrow r_{n-3} \in (r_n) \]

and so (in general \( r_{n-k} = q_{n-1} r_{n-2} + r_{n-1} \in (r_n) \))

on

and the terms \( r_{n-k+1}, r_{n-k+2} \in (r_n) \) by
induction on $\Gamma_{n+2}$, \( c = 9 \), \( \ldots, n+2 \\
\Gamma_1 = 5, \quad \Gamma_2 = 9 \)

Thus \( a, b \in (\Gamma_n) \) and \( \Gamma_n \) is a common divisor, i.e., \( (9, 5) \leq (\Gamma_n) \)

It suffices to show \( m \in (9, 5) \)

(0) shows \( m \in (9, 5) \). Then (1) shows \( m \in (9, 5) \). Continuing in this way (by induction) \( m \in (9, 5) \)

\[ \square \]