PIDs are UFDs.

Defn: Let R be a comm. ring w/ $1 \neq 0$

An ascending chain of ideals in R is a sequence

$$I_1 \subset I_2 \subset I_3 \subset \dots \subset R$$

We say an ascending chain stabilizes

if $\exists N \in \mathbb{N}$ s.t. $\forall n, m \geq N$, $I_n = I_m$

we say R satisfies the ascending chain condition (a.c.c.)

if every ascending chain stabilizes.

If R satisfies the a.c.c., we say it is a Noetherian ring.

Thm: If R is a PID, then R is Noetherian.

Pf: $I_1 \subset I_2 \subset I_3 \subset \dots \subset R$ an ascending chain in a PID.

Consider $I := \bigcup_{n \in \mathbb{N}} I_n$, which is an ideal

R a PID $\Longrightarrow I = (a)$

$\Longrightarrow a \in I = \bigcup_{n \in \mathbb{N}} I_n \Longrightarrow a \in I_N$ for some $N \in \mathbb{N}$.

$\Longrightarrow (a) \subset I_N \Longrightarrow I \subset I_N$

$\Longrightarrow I = I_N = I_{N+1} = I_{N+2} = \dots$ $\square$

Thm: Every PID is a UFD.

Pf: Let R be a PID.

we want to show if $r \in R \setminus \{0\}$, $r \notin R^\times$

Then r admits a unique expression as a product of irreducibles.

① we show r has some expression as a product of irreducibles.

Pf: If r is irred., then $r = r$ ✓

If not, then $r = r_1 \cdot r_2$, $r_1, r_2 \notin R^\times$

$\Longrightarrow r \in (r_1)$ but $(r) \neq (r_1)$

$\Longrightarrow (r) \subsetneq (r_1)$

If r_1, r_2 are irreducibles, we are done ✓

If not, $r_1 = r_{11} \cdot r_{12}$ $\quad r_{ij} \notin R^\times$, $i,j \in \{1,2\}$

$r_2 = r_{21} \cdot r_{22}$

$\Longrightarrow r_1 \in (r_{11})$ but $(r_1) \neq (r_{11})$

$\Longrightarrow (r) \subsetneq (r_1) \subsetneq (r_{11})$

Since R is a PID $\Longrightarrow R$ is Noetherian $\Longrightarrow$ This chain stabilizes.

$\Longrightarrow \quad r = (r_{111\cdots1} \cdot r_{11\cdots12}) \cdot \text{———} \cdots (r_{2222222\cdots1} \cdot r_{22\cdots2})$

where each term on the right is irreducible

□

(2) The factorization into irreducibles is <u>unique</u>

(up to reordering and associates)

Say $r = p_1 \cdot p_2 \cdots p_n$

We induct on n.

If $n=1$, then $r = \underbrace{p_1}_{\text{irred.}} \Longrightarrow r$ is irreducible.

Suppose $r = q_1 \cdot q_2 \cdots q_n$, $n \geq 2$, q_i irreducible $\forall i \in \{1, \dots, n\}$

But then $q_1, q_2 \dots q_n \notin R^{\times} \Longrightarrow r$ is not irreducible $\longrightarrow \Leftarrow$

$\Longrightarrow$ $r = r$ is the unique way to write r as the product of irreducibles.

Now suppose if r admits a factorization into at most $n-1$ irred.

Then the factorization is unique.

If $r = p_1 \cdot p_2 \cdots p_n$ $\quad$ p_i's irred.

$= q_1 \cdot q_2 \cdots q_m$ $\quad$ q_j's irred. $\quad m \geq n$

$\Longrightarrow p_1 \mid q_1 (q_2 \cdots q_m)$

Recall: Irreducible = prime in a PID.

p_1 irred. $\Longrightarrow p_1 \mid q_1$ or $p_1 \mid q_2 \dots q_m$

wlog, we may assume $p_1 \mid q_1$

i.e. $q_1 = u \cdot p_1$, $u \in R$

q_1 irred. $\Longrightarrow u \in R^\times$ or $p_1 \in R^\times$

p_1 irred. $\Longrightarrow p_1 \notin R^\times \Longrightarrow u \in R^\times \Longrightarrow p_1, q_1$ associate.

$$\Longrightarrow \quad r = p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m$$

$$= (u \cdot p_1) \cdot q_2 \cdots q_m$$

R is int. dom, we can cancel p_1 from both sides

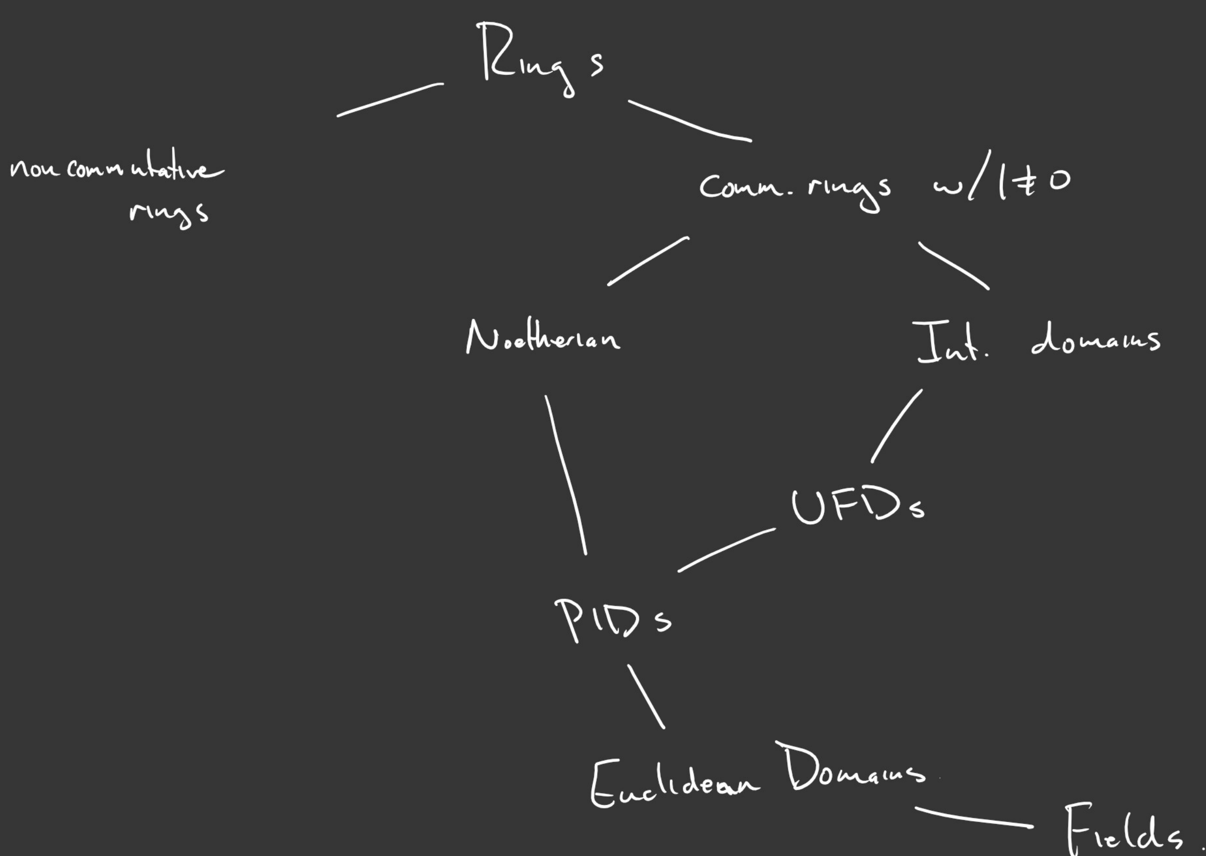
$$\Longrightarrow \quad \underbrace{p_2 \cdot p_3 \cdots p_n}_{\text{product of } (n-1) \text{ irreducibles}} = \underbrace{(u \cdot q_2) \cdot q_3 \cdots q_m}$$

Induction $\Longrightarrow \{(u \cdot q_2), q_3, q_4, \ldots q_m\} = \{p_2, p_3, \ldots, p_n\}$

(up to associates)

$\Longrightarrow m = n$, p_i's are unique

$\square$



Polynomial Rings: (we assume that rings are comm., w/ $1 \neq 0$)

Recall some facts we've already proven.

Let R be an int. dom.

Fact 1: $R[x]$ is an int. domain.

Fact 2: $R[X]^\times = R^\times$

e.g. $\mathbb{Z}[x]$, the only units are $\{\pm 1\}$.

Fact 3: $\deg[p(x) \cdot q(x)] = \deg p(x) + \deg q(x)$.

Fact 4: The field of fractions of $R[x]$ is the field of rational functions:

$$R(x) := \left\{ \frac{p(x)}{q(x)} \;\middle|\; p, q \in R[x],\ q \not\equiv 0 \right\}$$

Fact 5: If F is a field, then $F[x]$ is a Euclidean Domain.

Cor: If F is a field, $F[x]$ is a PID, UFD, and Noetherian.

Fact 6: Let $I \subset R$ is an ideal

$$(I) := I[X] := \{ p(x) \in R[x] \mid \text{coeffs are in } I \}$$

Then $$R[x]/(I) \cong (R/I)[X]$$

Cor: If $I \subset R$ is prime, then $(I) \subset R[x]$ is prime.

Example: Consider $3\mathbb{Z} := \{0, 3, -3, 6, -6, \dots\}$

$$(3\mathbb{Z}) := \{a_0 + a_1 x + a_2 x + \dots + a_n x^n \mid a_i \in 3\mathbb{Z}\}$$

$$\implies \mathbb{Z}[x] / (3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})[x]$$

e.g. $1 + 2x + 4x^3 = 1 + 2x + x^3 + 3x^3 \in (3\mathbb{Z})$

$\implies$ we can think about the coefficents

$$\underset{\text{in } \mathbb{Z}.}{1, 2, 4} \rightsquigarrow \bar{1}, \bar{2}, \bar{1} \in \mathbb{Z}/3\mathbb{Z}$$

Pf: of Fact 6.

Consider the map

$$\phi : R[x] \longrightarrow (R/I)[x]$$

$$a_0 + a_1 x + \_\_ + a_n x^n \longmapsto \bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + \dots + \bar{a}_n x^n$$

e.g. $\phi : \mathbb{Z}[x] \longrightarrow (\mathbb{Z}/3\mathbb{Z})[x]$

$$1 + 2x + 4x^3 \longmapsto \bar{1} + \bar{2}x + \bar{4}x^3 = \bar{1} + \bar{2}x + x^3$$

"Clearly" ϕ is a surjective ring homomorphism.

$$\implies (R/I)[x] \cong R[x]/\mathrm{Ker}\,\phi$$

But $\mathrm{Ker}\,\phi := \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in I\} = (I)$ $\square$

Thm: If $a(x), b(x) \in F[x]$, F a field

then $\exists!\ q(x), r(x) \in F[x]$ s.t. $\deg(r(x)) < \deg(b(x))$ (or $r(x) = 0$)

for which $a(x) = q(x) \cdot b(x) + r(x)$.

Note: Recall $\mathbb{Z}$ are a Euclidean Domain w/ $N(n) = |n|$

e.g. $7 = 3 \cdot 2 + 1$ $\quad N(1) = 1 < N(2)$

$7 = 4 \cdot 2 - 1$ $\quad N(-1) = 1 < N(2)$

Pf: Suppose $a(x) = q(x) \cdot b(x) + r(x)$

$= q'(x)\, b(x) + r'(x)$

$\Longrightarrow$ $r(x) = a(x) - q(x) \cdot b(x)$

$r'(x) = a(x) - q'(x)\, b(x)$

$\deg(r), \deg(r') < \deg(b)$ [or they're both assume]

Consider $r(x) - r'(x) = q'(x) \cdot b(x) - q(x) \cdot b(x)$

$= [q'(x) - q(x)] \cdot b(x)$

If $q' - q, b \neq 0$, then $\deg[(q' - q) \cdot b] = \deg(q' - q) + \deg(b)$

$\deg[r - r'] < \deg b$

$\Longrightarrow q' - q = 0 \Rightarrow q' = q \Longrightarrow r = r'$

$\square$

Cor: Suppose F, K are fields, $F \subset K$

and $a(x), b(x) \in F[x]$

Then the quotient and remainder polynomials of a by b

are independent of field.

Pf: $\exists\, q(x), r(x) \in F[x]$, $\exists\, Q(x), R(x) \in K[x]$

$\deg r < \deg b$ $\qquad$ $\deg R < \deg b$

s.t. $a(x) = q(x) \cdot b(x) + r(x)$ $\qquad$ $a(x) = Q(x) \cdot b(x) + R(x)$.

uniqueness, since $q, r \in K[x]$, $q(x) = Q(x)$

$r(x) = R(x)$ $\square$

Cor: $b(x) \mid a(x)$ in $K[x]$ iff $b(x) \mid a(x)$ $F[x]$.

e.g. $(x-1) \mid x^2 - 1$ in $\mathbb{R}[x]$, $\mathbb{C}[x]$

However, $(x-i) \mid x^2+1$ in $\mathbb{C}[x]$ but not $\mathbb{R}[x]$

$\Longrightarrow$ x^2+1 has no nontrivial factors in $\mathbb{R}[x]$

Polynomial rings with multiple variables

Defn: Let R be a comm. ring w/ $1 \neq 0$

The <u>polynomial ring in the variables $x_1, \ldots, x_n$ with coefficients in R</u>

is defined inductively as

$$R[x_1, x_2, \ldots, x_n] := R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

Concretely, think of $R[x_1, \ldots, x_n]$ as finite sums of

<u>monomials</u>, i.e. $a x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ $\quad d_i \in \mathbb{Z},\ d_i \geq 0$

e.g. $\mathbb{Z}[x,y] \ni 1 + 2xy + y^2,$

$$2x - 7x^3y + 2xy^4 + 1$$

Defn: The <u>degree</u> of a monomial

$$a x_1^{d_1} x_2^{d_2} x_3^{d_3} \cdots x_n^{d_n}$$

is $d = d_1 + d_2 + \cdots + d_n$

The <u>multi-degree</u> is $(d_1, d_2, d_3, \ldots, d_n)$

The <u>degree</u> of a polynomial is the highest degree of any monomial in it.

<u>Prop:</u> Let R be an int. dom.,

$$p(x_1, \ldots, x_n),\ q(x_1, \ldots, x_n) \in R[X_1, X_2, \ldots, X_n] \setminus \{0\}$$

1. $R[X_1, X_2, \ldots, X_n]$ is an int. dom.

2. $R[X_1, X_2, \ldots, X_n]^\times = R^\times$

3. $\deg[p \cdot q] = \deg p + \deg q$.