L12: PIDs are UFDs and Polynomial Rings

Definition 12.1: Ascending Chains, Noetherian Ring

Let R be a commutative ring with $1 \neq 0$.
An **ascending chain** of ideals in R is a sequence

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset R$$

We say an ascending chain **stabilizes** if there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$, $I_n = I_m$.
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**.

Theorem 12.2: PID is Noetherian

If R is a PID, then R is Noetherian.

Proof. Let

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset R$$

be an ascending chain in a PID.
Consider

$$I := \bigcup_{n \in \mathbb{N}} I_n$$

which is an ideal. Then since R is a PID, $I = (a)$ for some $a \in R$.
Therefore

$$a \in I = \bigcup_{n \in \mathbb{N}} I_n \implies a \in I_N$$

for some $N \in \mathbb{N}$.
Hence $(a) \subset I_n$ implying $I \subset I_N$ and so we deduce

$$I = I_N = I_{N+1} = I_{N+2} = \ldots$$

■

Theorem 12.3: PID IS UFD

Every PID is a UFD.

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.

Lemma 12.4

R has **some** expression as a product of irreducibles

Proof. If r is irreducible, then $r = r$.
If not, then $r = r_1 \cdot r_2$, $r_1, r_2 \notin R^\times$. Then $r \in (r_1)$ but $(r) \neq (r_1)$, therefore $(r) \subsetneq (r_1)$.
If r_1, r_2 are irreducibles, then we are done.
If not,

$$r_1 = r_{11} \cdot r_{12}$$
$$r_2 = r_{21} \cdot r_{22}$$

where $r_{ij} \in R^\times$, $i, j \in \{1, 2\}$. Again, $r_1 \in (r_{11})$ but $(r_1) \neq (r_{11})$, therefore $(r) \subsetneq (r_1) \subsetneq (r_{11})$.
Since R is a PID, it is also Noetherian, and so this chain stabilizes eventually. Hence

$$r = (r_{111\ldots1} \cdot r_{111\ldots2}) \cdot \ldots \cdot (r_{222\ldots1} \cdot r_{222\ldots2})$$

where each term on the right is irreducible. ■

Lemma 12.5

The factorization into irreducibles is **unique** (up to reordering and associates).

Proof. Say $r = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Let's induct on n.
If $n = 1$, then $r = \underbrace{p_1}_{\text{irred.}}$ implies r is irreducible.
Suppose

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

But then $q_1, (q_2 \cdot \ldots \cdot q_n) \notin R^\times$ implying r is not irreducible, which is a contradiction.
Therefore $r = r$ is the unique way to write r as the product of irreducibles.
Now suppose if r admits a factorizaation into at most $n - 1$ irreducibles, then the factorization is unique. If

$$\begin{aligned} r &= p_1 \cdot p_2 \cdot \ldots \cdot p_n, \quad p_i\text{'s irreducible} \\ &= q_1 \cdot q_2 \cdot \ldots \cdot q_m, \quad q_j\text{'s irreducible for } m \geq n \end{aligned}$$

Then $p_1 | q_1 \cdot (q_2 \cdot \ldots \cdot q_m)$ and recall irreducibles are prime in a PID. Since p_1 is irreducible either $p_1 | q_1$ or $p_1 | (q_2 \cdot \ldots \cdot q_n)$, so w.l.og assume $p_1 | q_1$ i.e $q_1 = u \cdot p_1$, $u \in R$.
Since q_1 is irreducible, then $u \in R^\times$ or $p_1 \in R^\times$. But p_1 is irreducible, so it can be not an element of $R^\times$, therefore $u \in R^\times$ and so p_1 and q_1 associate.
So we write

$$\begin{aligned} r = p_1 \cdot p_2 \cdot \ldots \cdot p_n &= q_1 \cdot q_2 \cdot \ldots \cdot q_m \\ &= (u \cdot p_1) \cdot q_2 \cdot \ldots \cdot q_m \end{aligned}$$

Since R is an integral domain, we can cancel p_1 from both sides to get

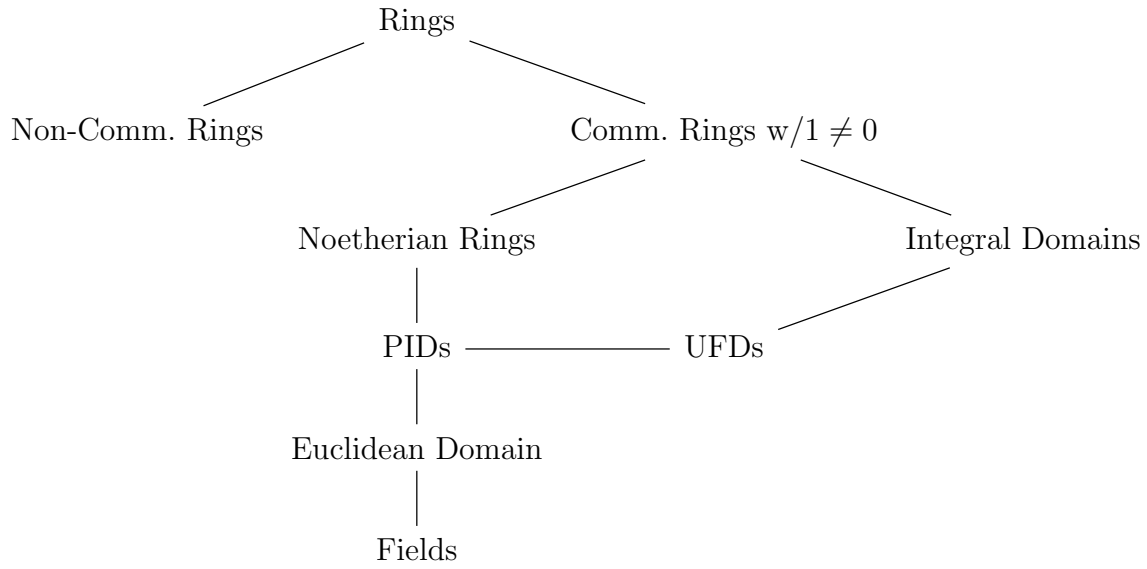
$$\underbrace{p_2 \cdot \ldots \cdot p_n}_{\text{product of (n-1) irred.}} = (u \cdot q_2) \cdot q_3 \cdot \ldots \cdot q_m$$

Now by our induction hypothesis, r admits a factorization into at most $(n-1)$ irreducibles, which implies

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

and so $m = n$ and the p_i's are unique. ■

We can now see a hierarchy for the specific structures we have discussed thus far



Polynomial Rings (Again)

Let R be an commutative integral domain with $1 \neq 0$. **Recall** some facts we've already proven (1) $R[X]$ is an integral domain.
(2) $R[X]^\times = R^\times$ e.g $\mathbb{Z}[X]$, the only units are $\{\pm 1\}$.
(3) $\deg[p(X) \cdot q(X)] = \deg p(X) + \deg q(X)$
(4) The field of fractions of $R[X]$ is the field of rational functions

$$R(X) := \left\{ \frac{p(X)}{q(X)} \middle| \, p, q \in R[X],\, q \neq 0 \right\}$$

(5) If F is a field, then $F[X]$ is a Euclidean Domain.

Corollary 12.6: $F[X]$ is PID, UFD, and Noetherian

If F is a field, $F[X]$ is a PID, UFD, and Noetherian.

(6) Let $I \subset R$ be an ideal, and define

$$(I) \coloneqq I[X] \coloneqq \{p(X) \in R[X] \mid \text{coeffs. are in } I\}$$

Then

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

Proof.
Consider the map

$$\phi \colon R[X] \to (R/I)[X]$$
$$a_0 + a_1X + \cdots + a_nX^n \mapsto \overline{a} + \overline{a_1}X + \overline{a_2}X^2 + \cdots + \overline{a_n}X^n$$

for example

$$\phi \colon \mathbb{Z}[X] \to (\mathbb{Z}/3\mathbb{Z})[X]$$
$$1 + 2X + 4X^3 \mapsto \overline{1} + \overline{2}X + \overline{4}X^3 = \overline{1} + \overline{2}X + X^3$$

"Clearly" ϕ is a surjective ring homomorphism, so

$$(R/I)[X] \cong R[X]/\operatorname{Ker}\phi$$

But $\operatorname{Ker}\phi \coloneqq \{a_0 + a_1X + \cdots + a_nX^n \mid a_i \in I\} = (I)$. ■

Corollary 12.7

If $I \subset R$ is prime, then $(I) \subset R[X]$ is prime.

Example 12.1. Consider $3\mathbb{Z} \coloneqq \{0, 3, -3, 6, -6, \dots\}$ and

$$(3\mathbb{Z}) \coloneqq \{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \mid a_i \in 3\mathbb{Z}\} \implies \mathbb{Z}[X]/(3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})[x]$$

e.g

$$1 + 2X + 4X^3 = 1 + 2X + X^3 + \underbrace{3X^3}_{\in 3\mathbb{Z}}$$

we can think about the coefficients

$$\underbrace{1, 2, 4}_{\in \mathbb{Z}} \to \underbrace{\overline{1}, \overline{2}, \overline{1}}_{\in \mathbb{Z}/3\mathbb{Z}}$$

Theorem 12.8: $F[X]$ satisfies euclidean condition

If $a(X), b(X) \in F[X]$ where F is a field. Then there exist unique $q(X), r(X) \in F[X]$ such that $\deg(r(X)) < \deg(b(X))$ (or $r(X) = 0$) for which

$$a(X) = q(X) \cdot b(X) + r(X)$$

Note: Recall $\mathbb{Z}$ are a Euclidean Domain with $N(n) = |n|$, e.g

$$7 = 3 \cdot 2 + 1 \quad N(1) = 1 < N(2)$$
$$7 = 4 \cdot 2 - 1 \quad N(-1) = 1 < N(2)$$

Proof. Suppose $a(X) = q(X) \cdot b(X) + r(X) = q'(X)b(X) + r'(X)$, then

$$r(X) = a(X) - q(X) \cdot b(X)$$
$$r'(X) = a(X) - q'(X) \cdot b(X)$$

and $\deg(r), \deg(r') < \deg(b)$.
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

$$\deg[(q' - q) \cdot b] = \deg(q' - q) + \deg(b)$$
$$= \deg[r - r'] < \deg b$$

Then $\deg q - q'$ must be 0 and so $q' - q = 0 \implies q' = q \implies r = r'$. ■

Corollary 12.9

Suppose F, K are fields with $F \subset K$ and $a(X), b(X) \in F[X]$.
Then the quotient and remainder polynomials of a by b are independent of of field.

Proof. There exist $q(X), r(X) \in F[X]$ and $Q(X), R(X) \in K[X]$ with $\deg r < \deg b$ and $\deg R < \deg b$, such that

$$a(X) = q(X) \cdot b(X) + r(X) \quad a(X) = Q(X) \cdot b(X) + R(X)$$

But there is uniqueness since $q, r \in K[X]$ it must mean that

$$q(X) = Q(X) \quad r(X) = R(X)$$

■

Corollary 12.10

$b(X)|a(X)$ in $K[X]$ *iff* $b(X)|a(X)$ in $F[X]$

Example 12.2.

$$(X - 1)|X^2 - 1 \text{ in } \mathbb{R}[X], \mathbb{C}[X]$$

However,

$$(X - i)|X^2 + 1 \text{ in } \mathbb{C}[X] \text{ but not } \mathbb{R}[X]$$

Since $X^2 + 1$ has no nontrivial factors in $\mathbb{R}[X]$.

Polynomial Rings with Multiple Variables

Definition 12.11: Multivariable Polynoimal Ring

Let R be a commutative ring with $1 \neq 0$.
The **polynomial ring in the variables $X_1, \ldots, X_n$ with coefficients in R** is defined inductively as

$$R[X_1, X_2, \ldots, X_n] \coloneqq R[X_1, X_2, \ldots, X_{n-1}][X_n]$$

Concretely, think of $R[X_1, \ldots, X_n]$ as finite sums of **monomials**, i.e

$$aX_1^{d_1} X_2^{d_1} \ldots X_n^{d_n}, \quad d_i \in \mathbb{Z},\ d_i \geq 0$$

e.g

$$1 + 2XY + Y^2, 2X - 7X^3y + 2XY^4 + 1 \in \mathbb{Z}[X, Y]$$

Definition 12.12: Multi-Degree

The **degree** of a monomial

$$aX_1^{d_1} X_2^{d_1} \ldots X_n^{d_n}$$

is $d = d_1 + d_2 + \cdots + d_n$.
The **multi-degree** is $(d_1, d_2, d_3, \ldots, d_n)$.
The **degree** of a polynomial is the highest degree of any monomial in it.

Proposition 12.13

Let R be an integral domain and

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

then

(1) $R[X_1, X_2, \ldots, X_n]$ is an integral domain.
(2) $R[X_1, X_2, \ldots, X_n]^\times = R^\times$
(3) $\deg[p \cdot q] = \deg p + \deg q$