Lecture 12

PIDs are UFDs

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 12.1

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 12.2

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 12.1: Existence

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

$$r = (r_{111\dots1} \cdot r_{111\dots2}) \cdot \dots \cdot (r_{222\dots1} \cdot r_{222\dots2})$$

where each term on the right is irreducible. ■

Lemma 12.2: Uniqueness

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

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

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

But then $q_1, (q_2 \cdot \dots \cdot q_n) \notin R^\times$ 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

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

Then $p_1 | q_1 \cdot (q_2 \cdot \dots \cdot q_m)$ and recall irreducibles are prime in a PID. Since p_1 is irreducible either $p_1 | q_1$ or $p_1 | (q_2 \cdot \dots \cdot q_n)$, 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

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

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

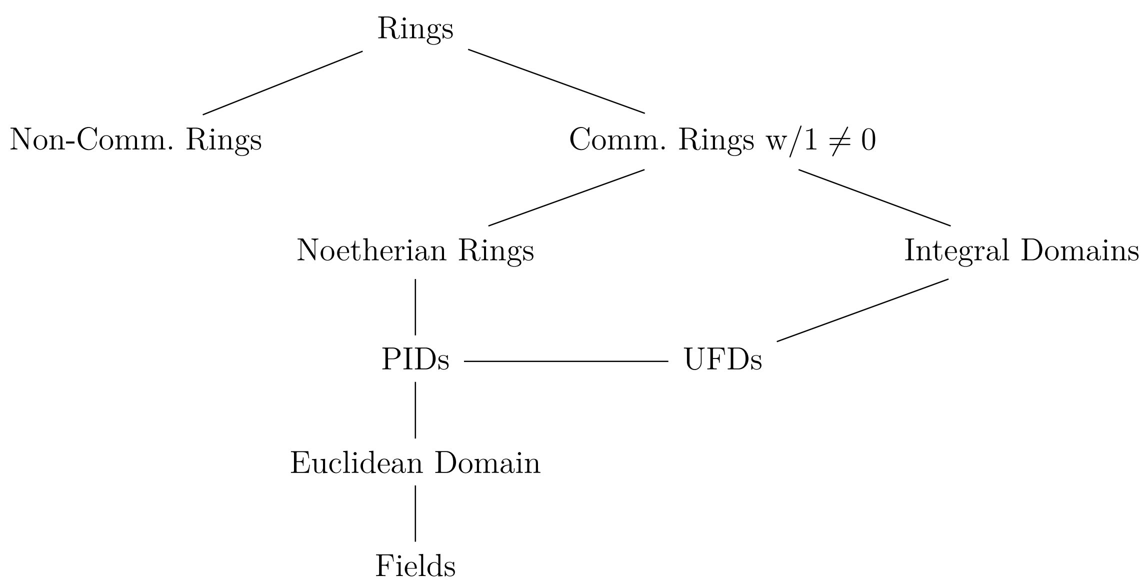
$$\underbrace{p_2 \bullet \ldots \bullet p_n}_{\text{product of (n-1) irred.}} = (u \bullet q_2) \bullet q_3 \bullet \ldots \bullet q_m$$

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

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

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 12.1

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

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

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

Then

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

Proof.
Consider the map

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

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 $\operatorname{Ker}\phi := \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in I\} = (I)$. ■

Corollary 12.2

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

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

$$(3\mathbb{Z}) := \{a_0 + a_1 x + a_2 x + \cdots + a_n x^n \mid a_i \in 3\mathbb{Z}\} \implies \mathbb{Z}[x]/(3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})[x]$$

e.g

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

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 12.3

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

$$\begin{aligned}\deg[(q'-q) \cdot b] &= \deg(q'-q) + \deg(b)\\ &= \deg[r - r'] < \deg b\end{aligned}$$

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

Corollary 12.3

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 12.4

$b(x)|a(x)$ 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 $\mathbb{R}[x]$.

PIDs are UFDs

Definition 12.2

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 12.3

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 12.1

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) $\deg[p \bullet q] = \deg p + \deg q$