date: monday, march 18, 2024

Principal Ideal Domains

Recall: An integral domain is a principal ideal domain (PID) if every ideal in the domain is principal.

eg. $\mathbb{Z}$, $F[x]$

Goal: To show all PIDs are UFDs

Lemma: Let D be a PID. Let $I_1, I_2, I_3, \dots$ be a collection of ideals such that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Then there exists an N such that

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

Proof

Let $I = \bigcup_{i=1}^{\infty} I_i$. We claim that I is an ideal.

- $I \neq \emptyset$ since $0 \in I_1 \subseteq I$.
- Let $a, b \in I$. So we have $a \in I_i$ and $b \in I_j$ for some i, j. If $i \leq j$, $a \in I_i \subseteq I_j$. So $a, b \in I_j$. Thus, $a - b \in I_j \subseteq I$ (similar argument if $j < i$).
- Let $a \in I$. So $a \in I_i$. For any $r \in D$, $ra \in I_i \subseteq I$.

Since D is a PID, there exists $d \in D$ such that $I = \langle d \rangle$. Since $d \in I = \bigcup_{i=1}^{\infty} I_i$, there exists a N such that $d \in I_N$. So

$$\langle d \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I = \langle d \rangle.$$

So $\langle d \rangle = I_N = I_{N+1} = \cdots$.

$\square$

Def^n: A ring R is a Noetherian ring if it has the ascending chain condition, ie. for any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists N such that

$$I_N = I_{N+1} = \cdots.$$

Corollary: Any PID is Noetherian.

Lemma: Let S be a nonempty set of ideals in a PID. Then S has a maximal element, ie. a $J \in S$ such that for all $I \in S$

with $J \subseteq I$, $J = I$.

Proof

Suppose S did not have a maximal element. Let $I_1 \in S$. Since I_1 is not maximal, there exists $I_2 \in S$ such that

$$I_1 \subsetneq I_2.$$

Again, I_2 is not maximal, so exists $I_3 \in S$ such that $I_1 \subsetneq I_2 \subsetneq I_3$. We can continue this process forever to get

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

But this contradicts the fact that a PID is Noetherian.

$\square$

Lemma: Let R be a PID. If a is not a unit, then a can be written as a product of irreducibles.

Proof

Let $S = \{\langle a \rangle \mid a \text{ cannot be written as a product of irreducibles}\}$ (a is not a unit). Goal is to show $S = \emptyset$.

Suppose $S \neq \emptyset$. Then by previous theorem, there exists $\langle a \rangle \in S$ such that $\langle a \rangle$ is maximal in S. But we also know $a = bc$ with a not reducible, so b and c not units. But then,

$$\langle a \rangle \subset \langle b \rangle \text{ and } \langle a \rangle \subset \langle c \rangle.$$

So $\langle b \rangle, \langle c \rangle \notin S$. So $b = p_1 \cdots p_r$ and $c = q_1 \cdots q_s$ can be factored into irreducibles. But then $a = bc = p_1 \cdots p_r q_1 \cdots q_s$ is a product of irreducibles. So $\langle a \rangle \notin S$, a contradiction. So $S = \emptyset$.

$\square$

Theorem: Every PID is also a UFD.

Proof

Given an $a \in D$ that is not a unit, we saw a can be written as a product of irreducibles,

$$a = p_1 \cdots p_r.$$

Suppose $a = p_1 \cdots p_r$ and $a = q_1 \cdots q_s$ are two ways to write a as a product of irreducibles.

Assume $r \leq s$. So $p_1 \cdots p_r = q_1 \cdots q_j$. Since D is a PID, p_1 is also prime. Since $p_1 \mid q_1 \cdots q_s$, we have $p_1 \mid q_i$ for some i. Relabel so

$p_1 | q_1$, ie. $q_1 = u_1 p_1$. Since q_1 is irreducible, u_1 is a unit. Thus,

$$p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s.$$

If $r<s$, would end with

$$1 = u_1 \cdots u_r q_{r+1} \cdots q_s.$$

But this can't happen since q_is are not units.
So $r=s$ and $p_i = u_i q_i$ for all i.

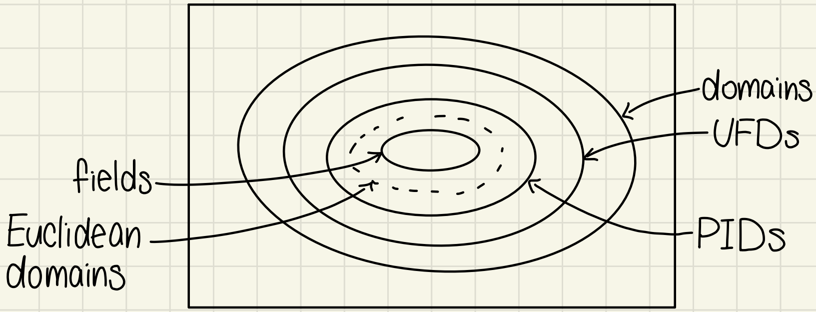
$\square$

Corollary: If F is a field, $F[x]$ is an UFD.

eg. $\mathbb{Z}$ is an UFD

Note: Converse is false, there are UFDs that are not PIDs.

eg. $F[x_1,\dots,x_n]$ is a UFD but not a PID.



Def^n: Let D be an integral domain. Suppose that there is a function $v: D\setminus\{0\} \to \mathbb{N}$ that satisfies:

1. If $a,b \in D$, then $v(a) \leq v(ab)$.
2. Let $a,b \in D$ with $b \neq 0$, then there exists $q,r \in D$ such that
$$a = bq + r \text{ with } r=0 \text{ or } v(r) < v(b).$$

Then D is called an Euclidean domain and v is a Euclidean valuation.

v puts a "size" on elements of D.

eg. For $D = \mathbb{Z}$, we use
$$v: \mathbb{Z}\setminus\{0\} \to \mathbb{N}$$
$$a \mapsto |a|.$$

eg. For $D = F[x]$, we use $v : D \setminus \{0\} \to \mathbb{N}$

$$p(x) \mapsto \deg p(x).$$

So $\mathbb{Z}$ and $F[x]$ are Euclidean domains.

Goal: If D is Euclidean, then D is a PID.