date: thursday, march 14, 2024

Special Domains: UFDs

During the next few lectures, learn about special classes of domains.

Assumptions: R is a commutative ring with identity 1_R and D is an integral domain

- a divides b, written $a|b$ if $b=ac$ for some c
- $a\in R$ is a unit if exists $u\in R$ such that $au=1$
- a and b are associates if exists a unit u such that $a=ub$
- p is irreducible if whenever $p=ab$, a or b is a unit
- p is a prime if whenever $p|ab$, then $p|a$ or $p|b$

Lemma: If $p\in D$ is prime, then p is irreducible.

Proof

Suppose $p=ab$. So $p|ab$. Because p is prime, $p|a$ or $p|b$. If $p|a$, $a=pc$. Thus $p=pcb$. Can cancel p since D a domain. So $1=cb$. So b is a unit. Same result if $p|b$.

$\square$

eg. If $p\in D$ is irreducible, may not be prime.
In $\mathbb{Q}[x^2,xy,y^2]$ $\leftarrow$ all polynomials in x^2, xy, y^2. We have xy is irreducible (can't factor into two degree 1 terms). But xy is not prime since $(xy)|(x^2)(y^2)$, but $xy\nmid x^2$ and $xy\nmid x^2$.

Def^{n}: An integral domain D is a unique factorization domain (UFD) if

① every $0\neq a\in D$ that is not a unit can be written as
$$a=p_1p_2\cdots p_r$$
with p_i irreducible.

② if $a=p_1\cdots p_r$ and $a=q_1\cdots q_s$ with p_i,q_i irreducible, then $r=s$ and p_i,q_i are associates (after relabelling) eg. $\mathbb{Z}$ is an UFD since every $a \in \mathbb{Z}$ can be written uniquely as

$$a = \underbrace{(-1)^t}_{\text{unit in } \mathbb{Z}} p_1^{b_1} \cdots p_s^{b_s} \text{ with } p_i \text{ prime}$$

eg. $20 = 2 \times 2 \times 5 = (-2) \times (2) \times (-5)$

eg. Not all integral domains are UFDs.
Set $S = \{f \in \mathbb{R}[x] \mid f = a_0 + \underbrace{0x}_{\text{coefficient of } x = 0} + a_2x^2 + \cdots + a_nx^n\}$

This is a subring of $\mathbb{R}[x]$ that is an integral domain. In this ring, x^2 is irreducible (can't factor as a product of two degree 1 polynomials). Also, x^3 is irreducible.
Consider $x^6 = (x^2)(x^2)(x^2) = (x^3)(x^3)$ <- two factorizations!

$\boxed{\text{PIDs}}$

Def^n: A domain is a principal ideal domain (PID) if every ideal of D is principal.

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

Goal: All PIDs are UFDs.

Lemma: Let $a, b \in D$. Then
1. $a \mid b$ iff $\langle b \rangle \subseteq \langle a \rangle$ (to divide is to contain)
2. a and b are associates iff $\langle a \rangle = \langle b \rangle$
3. a is a unit iff $\langle a \rangle = D$

<u>Proof</u>

① "=>" Given $a \mid b$, so $b = ac$ and $b \in \langle a \rangle$. Then $\langle b \rangle \subseteq \langle a \rangle$.
"<=" Since $b \in \langle b \rangle \subseteq \langle a \rangle$, $b = ac$ for some c. So $a \mid b$.

② "=>" If a and b are associates, $a = ub$ and $u^{-1}a = b$. So $b \mid a$ and $a \mid b$. By ①, $\langle b \rangle \subseteq \langle a \rangle \subseteq \langle b \rangle$. So $\langle a \rangle = \langle b \rangle$.
"<=" Given $\langle a \rangle = \langle b \rangle$, so $\langle a \rangle \subseteq \langle b \rangle$ and $\langle b \rangle \subseteq \langle a \rangle$. So $b \mid a$ and $a \mid b$. So $a = bc$ and $b = at$. So $a = atc$. So $1 = tc$. So c is a

unit. So a and b are associates.

③ "=>" a is a unit so $au = 1 \iff a = 1 \cdot u^{-1}$. So $a \mid 1$ and $1 \mid a$. Thus, $\langle a \rangle = \langle 1 \rangle = D$.

"<=" Exercise.

$\square$

Theorem: Let D be a PID. Then p is irreducible iff $\langle p \rangle$ is a maximal ideal.

<u>Proof</u>

"=>" Suppose p irreducible and $\langle p \rangle \subseteq \langle a \rangle$. So $a \mid p$. Since p is irreducible, a is an associate of p or a unit. If it is an associate $\langle p \rangle = \langle a \rangle$. If a a unit, $\langle a \rangle = D$. So $\langle p \rangle$ is maximal.

"<=" Suppose $p = ab$. We have $\langle p \rangle \subseteq \langle a \rangle$. Since $\langle p \rangle$ is maximal, $\langle p \rangle = \langle a \rangle$ or $\langle a \rangle = D$. If $\langle a \rangle = D$, a is a unit. If $\langle p \rangle = \langle a \rangle$, a is an associate of p, so b is a unit. So p is irreducible.

$\square$

Corrollary: Let D be a PID. Then p is prime iff p is irreducible.

<u>Proof</u>

"=>" Always true.

"<=" Suppose p is irreducible. So $\langle p \rangle$ is a maximal ideal and thus a prime ideal. If $ab \in \langle p \rangle$ (ie. $p \mid ab$), then $a \in \langle p \rangle$ or $b \in \langle p \rangle$. So $p \mid a$ or $p \mid b$.

$\square$

Note: In $\mathbb{Z}$ and $F[x]$, prime = irreducible.