

Announcements

HW1 due Wednesday @ 9am via Gradescope

Don't be late! (see syllabus) (entry code: VB7EY2)

HW2 will be posted soon (due next Wed.)

Principal Ideal Domains

Recall: A Euclidean domain is an int. domain R w/ a norm

$N: R \rightarrow \mathbb{Z}_{\geq 0}$ s.t. $N(0) = 0$ and $\forall a, b \in R, b \neq 0,$

$\exists q, r \in R$ with $a = qb + r$ and $r = 0$ or $N(r) < N(b)$

Def: A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Last time: Euclidean domain \Rightarrow PID

Next time: PID \Rightarrow 'unique factorization domain' (UFD)

Def/recall:

$$R[a] = \{ r_0 + r_1 a + r_2 a^2 + \dots + r_n a^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0} \} / \text{equiv.}$$

Integral domain

HW1

$$\mathbb{Z}[\sqrt{-5}]$$

$$\mathbb{Z}[\sqrt{-3}]$$

$$\mathbb{Z}[\sqrt{-5}][x] \leftarrow \text{lecture 5}$$

UFD

$$F[x, y]$$

F: field

$$\mathbb{Z}[x]$$

lecture 3 & lecture 5
(not PID) (UFD)

PID

$$\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$$

DLF

P.282

ED

\mathbb{Z}

$$\mathbb{Z}[i]$$

lecture
2

F

$$F[x]$$

Prop: $R : \text{PID}$. Let $a, b \in R$, $(a, b) = (d)$.

Then

a) $d = sa + tb$ for some $s, t \in R$

b) d is a gcd of a and b

Pf: a) is a consequence of $d \in (d) \subseteq (a, b) = \{sa + tb\}$.

b) Since $a, b \in d$, d is a common divisor of a & b .

If $d' \mid a$, $d' \mid b$, then $d' \mid sa + tb = d$, so d is a gcd of a & b . \square

Remark: Consider $F[x, y]$: not a PID since (x, y) is not principal. We have $1 = \gcd(x, y)$, but can't have $1 = sx + ty$.

Recall/Def: Let R : integral domain

a) r is a unit if $\exists s \in R$ w/ $rs = sr = 1$

If r not unit, $r \neq 0$

b) r is irreducible if $r = ab \Rightarrow a$ or b is a unit

c) r is prime if $r \mid ab \Rightarrow r \mid a$ or $r \mid b$

Prop: r is prime $\Rightarrow r$ is irreducible

Pf: Let $r=ab$, and assume WLOG that $a=rt$.

Then $r=ab=rtb \Rightarrow r(1-tb)=0 \Rightarrow tb=1 \Rightarrow b$ is a unit.

□

Converse doesn't hold: 3 is irred. in $\mathbb{Z}[\sqrt{-5}]$, but

$3^2 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ and $3 \nmid 2 \pm \sqrt{-5}$, so
3 is not prime.

Recall/Def: Let I be an ideal in R

a) I is maximal if either/both:

- \nexists ideal J s.t. $I \subsetneq J \subsetneq R$
- R/I is a field

b) I is prime if either/both:

- $a, b \in I \Rightarrow a \in I$ or $b \in I$
- R/I is an integral domain

So maximal \Rightarrow prime

Lemma: (r) prime ideal $\Leftrightarrow r$ prime elt.

Pf: $a \in (r) \Leftrightarrow a$ is a multiple of r . So,

$$\left[\begin{array}{c} a, b \in (r) \\ \text{prime ideal} \end{array} \Rightarrow a \in (r) \text{ or } b \in (r) \right] \Leftrightarrow \left[\begin{array}{c} r | ab \Rightarrow r | a \text{ or } r | b \\ \text{prime elt.} \end{array} \right]$$

Prop: Every nonzero prime ideal in a PID is maximal

Pf: Let $0 \neq (p) \subseteq (m) \subsetneq R$, (p) : prime.

By the previous results, (p) prime $\Rightarrow p$ prime $\Rightarrow p$ irred.

Since $(p) \subseteq (m)$, $p = am$ for some a , so either

- a is a unit $\Rightarrow (m) = (p)$
- m is a unit $\Rightarrow (m) = R$

Therefore, (p) is maximal. □

Cor: If $r \in R$: PID, r prime $\Leftrightarrow r$ irred.

Pf: \Rightarrow holds in any int. dom. (see earlier)

\Leftarrow : By previous pf,

r irred. $\Rightarrow (r)$ maximal $\Rightarrow (r)$ prime $\Rightarrow r$ prime. □

Integral domain

HW 1

$$\mathbb{Z}[\sqrt{-5}]$$

$$\mathbb{Z}[\sqrt{-3}]$$

$$\mathbb{Z}[\sqrt{-5}][x] \leftarrow \text{lecture 5}$$

UFD

$$F[x, y]$$

F: field

$$\mathbb{Z}[x]$$

lecture 3 & lecture 5
(not PID) (UFD)

PID

$$\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$$

DLF

P. 282

ED

\mathbb{Z}

$$\mathbb{Z}[i]$$

lecture
2

F

$$F[x]$$

Ex: $\mathbb{Z}[x]$ is not a PID since $(2, x)$ is not principal

Prop: $R[x]: \text{PID} \Leftrightarrow R: \text{field}$

Pf: (\Leftarrow) If $R: \text{field}$, $R[x]$ is Euclidean (last time), hence a PID.

\Rightarrow

$R[x]$ integral domain $\Rightarrow R$ integral domain

$\Rightarrow (x)$ prime (since $R[x]/(x) \cong R$)

$\Rightarrow (x)$ maximal (since it is a prime ideal in a PID)

$\Rightarrow R \cong R[x]/(x)$ field

□