# Announcements

HW1 due Wednesday @ 9am via Gradescope

Don't be late! (see syllabus) (entry code: 2BZDK7)

HW2 posted (due next Wed.)

Problem session tomorrow (3:00pm-4:20pm, Loomis Lab. 143)

Fill out midterm conflict survey

**Integral domain**

HW1 $\mathbb{Z}[\sqrt{-5}]$ $\mathbb{Z}[\sqrt{-3}]$

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

**UFD**

$F[x,y]$ ($F$: field) lecture 6

$\mathbb{Z}[x]$ lecture 3 (not PID) & lecture 5 (UFD)

**PID**

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ D&F p.277, 282

**ED**

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

$F$ $F[x]$

lecture 2

# Principal Ideal Domains

Recall: A <u>Euclidean domain</u> is an int. domain $R$ w/ a norm

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

Prop: $R$ : 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 $d' | a$, $d' | b$, then $d' | sa + tb = d$, so $d$ is a gcd of $a$ & $b$. $\square$

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

Def: Let $r \in R$: 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 $r \mid a$, $a = rt$.
Then $r = ab = rtb \Rightarrow r(1-tb) = 0 \Rightarrow tb = 1 \Rightarrow b$ is a unit.

$\square$

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.

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:

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

So maximal $\Rightarrow$ prime

Lemma: If $r \neq 0$, $(r)$ prime ideal $\Leftrightarrow$ $r$ prime elt.

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

$$\underbrace{\left[ab \in (r) \Rightarrow a \in (r) \text{ or } b \in (r)\right]}_{\text{prime ideal}} \Leftrightarrow \underbrace{\left[r \mid ab \Rightarrow r \mid a \text{ or } r \mid b\right]}_{\text{prime elt.}}$$

$\square$

Prop: Every nonzero prime ideal in a PID is maximal

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

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

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

$\Leftarrow$) By previous pf,

$$r \text{ irred.} \Rightarrow (r) \text{ maximal} \Rightarrow (r) \text{ prime} \Rightarrow r \text{ prime}.$$ $\square$

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

Prop: $R[x]$: PID $\Leftrightarrow$ $R$: field

Pf: $\Leftarrow$) If $R$: 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 $\square$