Lecture 8 Friday Feb 5

8.3 Unique factorization Domains.

In this section R denotes an integral domain

DEF 1 For $r \in R$, r is <u>irreducible</u>

whenever

(i) $r \neq 0$

(ii) r not a unit

(iii) there does not exist nonunits $a, b \in R$ such that

$$r = ab$$

DEF 2 For $p \in R$, p is <u>prime</u> whenever

(i) $p \neq 0$

(ii) the ideal Rp is prime

LEM 3 For $p \in R$, p is prime if and only if

(i) $p \neq 0$,

(ii) p not a unit,

(iii) For $a, b \in R$,

$p \mid ab$ implies $p \mid a$ or $p \mid b$

pf By the def of a prime ideal.

LEM 4 Given a prime $p \in R$.

Then p is irreducible.

pf Suppose $\exists$ nonunits $x, y \in R$ st

$$p = xy$$

So

$$p \mid xy$$

So

$$p \mid x \quad \text{or} \quad p \mid y$$

WLOG $p \mid x$

$\exists$ $r \in R$ st

$$pr = x$$

So

$$p = xy = pry$$

$$p(1 - ry) = 0$$

$$\overset{\#}{0} \quad 1 - ry = 0$$

y is unit cnt. $\square$

LEM 5 Assume R is a PID.

Given an irreducible $p \in R$.

Then p is prime.

pf By assumption $p \neq 0$, p not a unit.

Given $x, y \in R$ st

$$p \mid xy$$

Show $p \mid x$ or $p \mid y$

Write $pz = xy$ $\quad z \in R$

Ideal $Rp + Rx$ is principal

Write $Rp + Rx = Rd$ $\quad d \in R$

So $ap + bx = d$ $\quad a, b \in R$

$p = cd$ $\quad c \in R$

Since p is irred and $p = cd$,

c is unit or d is unit

Case: c is unit

$$Rd = Rp$$

$$\begin{matrix} \rotatebox{90}{$\in$} \\ x \end{matrix}$$

So $p \mid x$ ✓

Case: d is unit

WLOG $d = 1$

$$ap + bx = 1$$

$$(ap + bx)y = y$$

$$\|$$

$$apy + \underbrace{bxy}_{\overset{\shortparallel}{pz}}$$

$$p(ay + bz) = y$$

So $p \mid y$ ✓

$\square$

DEF 6 Fn nmo $x, y \in R$ TFAE

(i) $Rx = Ry$

(ii) $x \mid y$ and $y \mid x$

(iii) $\exists$ unit $u \in R$ such that

$$x = yu$$

Call x, y <u>associates</u> whenever (i) – (iii) hold.

DEF 7 R is a <u>Unique factorization Domain</u>. (UFD)

whenever:

For each nmo $x \in R$ that is not a unit,

(i) x is a product of irreducible elements of R;

(ii) above product is unique up to perm and associates.

Meaning of (ii):

Write

$$x = u_1 u_2 \cdots u_r \qquad r \geq 1 \qquad u_i \text{ irred} \qquad (1 \leq i \leq r)$$

$$x = v_1 v_2 \cdots v_s \qquad s \geq 1 \qquad v_i \text{ irred} \qquad (1 \leq i \leq s)$$

then $r = s$ and the sequence of ideals

$Ru_1, Ru_2, \cdots, Ru_r$

is a permutation of

$Rv_1, Rv_2, \cdots, Rv_s$

LEM 8 Assume R is a UFD

Given an irreducible $p \in R$.

Then p is prime.

pf By construction $p \neq 0$, p not a unit.

Given $a, b \in R$ st

$p \mid ab$

Show $p \mid a$ or $p \mid b$

Write $pc = ab$ $c \in R$ $\ast$

Write

$a = a_1 a_2 \cdots a_r$ $r \geq 1$ a_i irred $(1 \leq i \leq r)$

$b = b_1 b_2 \cdots b_s$ $s \geq 1$ b_i irred $(1 \leq i \leq s)$

$c = c_1 c_2 \cdots c_t C$ $t \geq 0$ c_i irred $(1 \leq i \leq t)$

C a unit

By $\ast$ and since C is unit, the sequence

$Rp, Rc_1, Rc_2, \ldots, Rc_t$

is a permutation of

$Ra_1, Ra_2, \ldots, Ra_r, Rb_1, Rb_2, \ldots, Rb_s$

So p is assoc some a_i or b_i

WLOG p assoc a_1

So $p \mid a_1$

But $a_1 \mid a$

So $p \mid a$

✓

$\square$

Assume R is a UFD

Given $0 \neq c \in R$

Write c as a product of primes and a unit:

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_t^{\gamma_t} C$$

$t \geq 0$

$p_1, p_2, \ldots, p_t$ mutually nonassoc primes in R

$\gamma_i \geq 0 \quad (1 \leq i \leq t)$

C a unit

LEM 9 With the above assumptions and notation

(i) For $a, b \in R$,

$$ab = c$$

if and only if

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} A$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} B$$

$0 \le \alpha_i$ $\quad$ $0 \le \beta_i$ $\quad$ $\alpha_i + \beta_i = \gamma_i$ $\quad$ $1 \le i \le t$

A, B units

$$AB = C$$

(ii) For $a \in R$,

$$a \mid c$$

if and only if

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} A$$

$0 \le \alpha_i \le \gamma_i$ $\quad$ $1 \le i \le t$

A a unit

Pf (i) By the definition of a UFD

(ii) By (i) above $\square$

Assume R is a UFD

Given nonzero $a, b \in R$

Write

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} A$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} B$$

$t \geq 0$

$p_1, p_2, \ldots, p_t$ mutually nonassoc primes in R

$0 \leq \alpha_i$ $\quad 0 \leq \beta_i$ $\quad (1 \leq i \leq t)$

A, B units in R

LEM 10 With above assumptions and notation,

$$d = \prod_{i=1}^{t} p_i^{\min(\alpha_i, \beta_i)}$$

is a GCD for a, b

pf By construction

$d \mid a$, $\quad d \mid b$

Given $e \in R$ st

$e \mid a$ and $e \mid b$

Show $e \mid d$

By LEM 9 and since e/a,

$$e = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} E$$

$$0 \le \varepsilon_i \le \alpha_i \qquad (1 \le i \le t)$$

$$E \text{ a unit}$$

Since e/b,

$$\varepsilon_i \le \beta_i \qquad (1 \le i \le t)$$

So

$$0 \le \varepsilon_i \le \min(\alpha_i, \beta_i)$$

Now e/d

$\square$