Lecture 9 Monday Feb 8

We continue to discuss unique factorization domains.

Assume R is a UFD.

Given nonzero $a, b \in R$

Write

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} A \qquad t \geq 0$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} B$$

$p_1, p_2, \ldots, p_t$ 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 notation and assumptions,

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

is a GCD for a, b.

pf By constr

$$d \mid a, \qquad d \mid b$$

Given $e \in R$ such that

$$e \mid a, \qquad e \mid b$$

Show

$$e/d$$

By LEM 9 and since e/a,

$$e = \rho_1^{\varepsilon_1} \rho_2^{\varepsilon_2} \cdots \rho_t^{\varepsilon_t} E$$

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

E unit

Since e/b,

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

So

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

Now e/d. □

Thm 11 Assume R is a PID.

Then R is a UFD.

pf For $i \in \mathbb{N}$ define a subset $R_i \subseteq R$ as follows:

R_0 = set of units in R

Fix $i \geq 1$

$$R_i = \left\{ x \in R \;\middle|\; \exists \text{ irred } u_1, u_2, \ldots, u_i \in R \text{ st } x = u_1 u_2 \cdots u_i \right\}$$

Note that for $x, y \in R$,

$x \in R_i$ and $y \in R_j$ implies $xy \in R_{i+j}$

Define

$$\tilde{R} = \bigcup_{i \in \mathbb{N}} R_i$$

So for $x, y \in \tilde{R}$,

$$xy \in \tilde{R}$$

Going to show

$$\tilde{R} = R \setminus 0$$

claim 1 Given $0 \neq r \in R \setminus \tilde{R}$,

$\exists \quad 0 \neq s \in R \setminus \tilde{R}$ s.t. $R_r \subsetneq R_s$

pf cl 1

r not a unit, else $r \in R_0 \subseteq \tilde{R}$

r not irred, else $r \in R_1 \subseteq \tilde{R}$

$\exists$ nonunits $s, t \in R$ s.t.

$$r = st$$

So $s \neq 0, \quad t \neq 0$

obs

$$s \notin \tilde{R} \quad \text{or} \quad t \notin \tilde{R}$$

else $r = st \in \tilde{R}$, cnt.

WLOG $s \notin \tilde{R}$

We have

$$r = st \in R_s$$

So $R_r \subseteq R_s$

Also

$R_2 \nsubseteq R_r$

since t is not a unit

So $R_r \subsetneq R_2$ claim proved ✓

claim 2 $\quad \tilde{R} = R \setminus 0$

pf cl 2 Suppose not.

Pick

$$0 \neq r_0 \in R \setminus \tilde{R}$$

Applying claim 1 repeatedly, $\exists$ ∞ sequence

$r_1, r_2, r_3, \ldots$

of elements in $R \setminus \tilde{R}$ st

$$Rr_0 \subsetneq Rr_1 \subsetneq Rr_2 \subsetneq \cdots$$

Define

$$I = \bigcup_{i \in \mathbb{N}} Rr_i$$

I is an ideal in R, hence principal.

Write $\quad I = Rd \qquad d \in R$

So $\quad d \in I$

So $\exists \; i \in \mathbb{N}$ st

$$d \in Rr_i$$

Now

$$Rr_{i+1} \subseteq I = Rd \subseteq Rr_i \subsetneq Rr_{i+1}$$

Contr. claim 2 proved ✓

Given $x \in R$ that is nonzero and not a unit.

By Claim 2. x is a product of irreducibles:

$$x = u_1 u_2 \cdots u_s \qquad s \geq 1$$

We show this product is unique up to perm and assoc.

Use induction on s

Suppose

$$x = v_1 v_2 \cdots v_t \qquad t \geq 1$$

v_i irred $\quad (1 \leq i \leq t)$

Show $s = t$ and

$Ru_1, Ru_2, \ldots, Ru_s$ is perm of $Rv_1, Rv_2, \ldots, Rv_t$ *

Recall u_1 irred $\Rightarrow$ u_1 prime.

We have

$$u_1 \mid v_1 v_2 \cdots v_t$$

So

$u_1 \mid v_1$ or $u_1 \mid v_2 \cdots v_t$

$\downarrow$

$u_1 \mid v_2$ or $u_1 \mid v_3 \cdots v_t$

etc

$\exists\ i\ (1 \leq i \leq t)$ st

$$u_1 \mid v_i$$

WLOG $i = 1$

Write

$$u_1 y = v_1 \qquad y \in R$$

v_1 is irred $\Leftrightarrow$ y is unit

So

$$Ru_1 = Rv_1$$

We have

$$u_1 u_2 \cdots u_s = v_1 v_2 \cdots v_t$$
$$\| \\ u_1 y$$

Cancel u_1

$$u_2 \cdots u_s = y v_2 \cdots v_t \qquad Ry v_2 = Ry v_2$$

By induction $s = t$

and

$Ru_2, \ldots, Ru_s$ perm of $Rv_2, \ldots, Rv_t$

$*$ follows.

□

Recall the Gaussian integers

$$\mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \} \qquad i^2 = -1$$

We saw that $\mathbb{Z}[i]$ is a Euclidean domain

with norm

$$N(a+bi) = a^2 + b^2$$

So $\mathbb{Z}[i]$ is a PID and UFD.

Next goal: For $\mathbb{Z}[i]$ describe the units

and primes (= irreducibles).

LEM 12 For $x \in \mathbb{Z}[i]$ TFAE

(i) x is unit

(ii) $N(x) = 1$

(iii) $x \in \{1, -1, i, -i\}$

pf (i) $\rightarrow$ (ii) $\exists\ y \in \mathbb{Z}[i]$ st

$$xy = 1$$

$$1 = N(1) = N(xy) = N(x)N(y)$$

$\uparrow$ $\uparrow$ pos integers

(ii) $\rightarrow$ (iii) write $x = a + bi$

$$1 = a^2 + b^2 \qquad a, b \in \mathbb{Z}$$

(iii) $\rightarrow$ (i) clear $\square$

A technical lemma

LEM 13 Given a prime integer $p \geq 3$ such that

$$p \equiv 1 \pmod 4$$

then $\exists \; x \in \mathbb{Z}$ such that

$$x^2 + 1 \equiv 0 \pmod p$$

pf Consider ring

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$$

Group of units

$$\mathbb{Z}_p^{\times} \text{ has size } p-1$$

Each non 0 element of $\mathbb{Z}_p$ is a unit

$\mathbb{Z}_p$ is a field

Let λ = indeterminate

Consider ring of polynomials

$$\mathbb{Z}_p[\lambda]$$

This is Eucl domain. PID, UFD.

Given $a \in \mathbb{Z}_p^{\times}$

$\exists$ integer $n \geq 1$ st

$$a^n = 1$$

n divides $|\mathbb{Z}_p^{\times}| = p-1$ by Lagrange thm

So $$a^{p-1} = (a^n)^{\frac{p-1}{n}} = 1^{\frac{p-1}{n}} = 1$$

Note $$\frac{p-1}{2} \in \mathbb{Z}$$

and

$$0 = a^{p-1} - 1$$

$$= \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$$

so

$$a^{\frac{p-1}{2}} \in \{1, -1\}$$

<u>claim</u> $\exists\ a \in \mathbb{Z}_p^{\times}$ st $a^{\frac{p-1}{2}} = -1$