Lecture 6 Monday Feb 1

Euclidean domains, cont.

Until further notice R is a commutative ring

DEF 9 Given nonO $a, b \in R$.

An element $d \in R$ is called a "GCD"

greatest commm divisor of a, b

whenever

(i) $d \neq 0$

(ii) d / a and d / b

(iii) $\forall\ 0 \neq e \in R$.

e / a and e / b implies e / d

— o —

Note
Referring to DEF 9, a GCD of a, b might not exist.

If it exists it might not be unique.

Prop 10 Given nonzero $a, b \in R$ such that the ideal

$$Ra + Rb \text{ is principal.}$$

Then for $d \in R$ TFAE:

(i) $Ra + Rb = Rd$

(ii) d is a GCD for a, b

pf (i) $\to$ (ii)

$d \neq 0$ since $a \neq 0$

d/a and d/b since $a, b \in Rd$

Given $0 \neq e \in R$ st

e/a and e/b

Then $a, b \in Re$

So $d \in Rd = Ra + Rb \subseteq Re$

So e/d

$(ii) \to (i)$ Since $Ra + Rb$ is principal

$\exists\ D \in R$ s.t. $Ra + Rb = RD$

We saw D is a GCD for a, b

Each of d, D is a GCD for a, b

$d \mid D$ and $D \mid d$

So $Rd = RD$

Now $Ra + Rb = RD = Rd$ ✓ $\square$

Prop 11 Given integer $n \geq 1$

Given nmo $$r_0, r_1, \dots, r_n \in R$$

Given $$x_1, x_2, \dots, x_n \in R$$

Assume

$$r_{i-1} = x_i r_i + r_{i+1} \qquad 1 \leq i \leq n-1 \qquad *$$

$$r_{n-1} = x_n r_n \qquad **$$

Then

$$R r_0 + R r_1 = R r_n \qquad ☆$$

Moreover

r_n is a GCD of r_0, r_1

pf Show ☆

$\subseteq$: Using $*$, $**$ find each of

$$r_n, r_{n-1}, r_{n-2}, \dots, r_1, r_0$$

is in $R r_n$

$\supseteq$: Using $*$ find each of

$$r_0, r_1, \dots, r_n$$

is in $R r_0 + R r_1$

we have ☆. Last assertion follows by Prop 10 $\square$

We now consider the uniqueness of the GCD.

Prop 12 Assume R is an integral domain.

Given nonzero $a, b \in R$.

Assume a, b has a GCD d.

Then for $d' \in R$ TFAE:

(i) d' is a GCD of a, b

(ii) $\exists$ unit $u \in R$ s.t. $d' = du$

pf (i) $\to$ (ii) By assumption

$d | a$ $\quad d | b$ $\quad d' | a$ $\quad d' | b$

So $d | d'$ $\quad d' | d$

So $\exists$ $u, v \in R$ st

$d' = ud$ $\quad d = vd'$

So $d = vd' = uvd$

$d(uv - 1) = 0$

$\stackrel{\neq}{0}$

$uv = 1$

u, v are units

(ii) $\to$ (i) Since $Rd = Rd'$

$\square$

DEF 13 Assume R is an integral domain.

An element $\theta \in R$ is called a

<u>universal side-divisor</u>

whenever

(i) $\theta \neq 0$

(ii) θ not a unit

(iii) $\forall x \in R, \quad \exists q, r \in R$ st

$$x = q\theta + r$$

and

$r = 0$ or r is unit

Prop 14 Assume R is Euclidean domain but not a field. Then R contains a universal side-divisor.

pf Since R is not a field,

$\exists\ x \in R$ such that

$x \neq 0$ and x not a unit

Define

$$m = \min\{ N(x) \mid x \in R,\ x \neq 0,\ x \text{ not unit} \}$$

$\exists\ \theta \in R$ such that

$\theta \neq 0$, θ not a unit, $N(\theta) = m$

Show θ is a univ side-divisor.

Since R is Euclidean, for $x \in R$ $\exists\ q, r \in R$

st

$$x = q\theta + r$$

and

$r = 0$ or $N(r) < \underset{m}{\underset{\shortparallel}{N(\theta)}}$

$\uparrow$

r must be 0 or unit

So

$r = 0$ or r is unit

$\square$

Ex 15 Consider ring

$$R = \mathbb{Z}\left[\underbrace{\frac{1+\sqrt{-19}}{2}}_{\sigma}\right]$$

$$= \{a + b\sigma \mid a, b \in \mathbb{Z}\}$$

$$= \left\{\frac{A + B\sqrt{-19}}{2} \;\middle|\; A, B \in \mathbb{Z},\ A - B \text{ even}\right\}$$

Show R is not a Euclidean domain with respect to any norm.

pf Show R has no universal side-divisor.

For $x \in \mathbb{C}$ write

$x = \alpha + \beta i \qquad \alpha, \beta \in \mathbb{R} \qquad i^2 = -1$

Define $N(x) = \alpha^2 + \beta^2$

So $N(x) \in \mathbb{R}$

$N(x) \geq 0$

$N(xy) = N(x)\,N(y) \qquad \forall\, x, y \in \mathbb{C}$

For $x = \dfrac{A + B\sqrt{-19}}{2} \in R$

$N(x) = \dfrac{A^2 + 19B^2}{4} \in \mathbb{Z}$

<u>claim</u> The units in R are $1, -1$.

<u>pf cl</u> Given unit $x \in R$

$\exists y \in R$ st $xy = 1$

Apply Norm N:

$1 = N(1) = N(xy) = \underset{\in \mathbb{Z}}{N(x)}\ \underset{\in \mathbb{Z}}{N(y)}$

$N(x)$ is positive unit in $\mathbb{Z}$

$N(x) = 1$

Write $x = \dfrac{A + B\sqrt{-19}}{2}$ $A, B \in \mathbb{Z}$
$A - B$ even

$1 = N(x) = \dfrac{A^2 + 19B^2}{4}$

$4 = A^2 + 19B^2$

Require $A = \pm 2$ $B = 0$

So $x = \pm 1$ ✓

claim proved

We assume R has a univ side-divisor θ and get a contradiction.

Obs $\theta \neq 0$, $\theta \neq 1$, $\theta \neq -1$

So $N(\theta) \neq 0$ $N(\theta) \neq 1$

So $N(\theta)$ is integer ≥ 2

Factor $N(\theta)$ over $\mathbb{Z}$

$N(\theta)$ has a prime factor p (>0)

Consider poss values of p

$\forall x \in R$

θ divides x or $x-1$ or $x+1$

So $N(\theta)$ divides $N(x)$ or $N(x-1)$ or $N(x+1)$

So p divides $N(x)$ or $N(x-1)$ or $N(x+1)$

Take $x = 2$

$N(x-1) = N(1) = 1$

$N(x) = N(2) = 4$

$N(x+1) = N(3) = 9$

p divides 1 or 4 or 9

$p = 2$ or $p = 3$

Take $x = \dfrac{1 + \sqrt{-19}}{2}$

Find

$N(x-1) = 5$

$N(x) = 5$

$N(x+1) = 7$

p divides 5 or 7

$p = 5$ or $p = 7$

Contradiction.

R has no univ side-divisor.

$\square$