Lecture 5 Friday Jan 29

8.1 Euclidean domains

Until further notice

R is a commutative ring

Recall the natural numbers

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

DEF 1 Assume R is an integral domain

A <u>norm</u> on R is a function

$$N : R \longrightarrow \mathbb{N}$$

such that

$$N(0) = 0$$

The norm N is <u>positive</u> whenever

$$N(r) > 0 \quad \text{for } 0 \neq r \in R$$

DEF 2 Assume R is an integral domain.

Then R is called Euclidean whenever it

has a norm N with this property:

$\forall\ a, b \in R$ with $b \neq 0$,

$\exists\ q, r \in R$ such that

$a = bq + r$

and

$r = 0$ or $N(r) < N(b)$

Ex Integers $\mathbb{Z}$ form a Eucl Domain

with $N(x) = |x|$ $\forall x \in \mathbb{Z}$

Ex 3 let F denote a field

So F is an integral domain.

Let N denote any norm on F.

Then N turns F into a Euclidean domain:

$\forall$ $a, b \in F$ with $b \neq 0$,

define $q = ab^{-1}$, $r = 0$.

then $a = bq + r$.

Ex 4 let F denote a field

let x = indeterminate

let $F[x]$ = ring of polynomials in x that have all coefs in F

Recall $F[x]$ is integral domain.

Define $N(f)$ = the degree of f $\quad f \in F[x]$

Then N is a norm on $F[x]$.

N turns $F[x]$ into Eucl domain.

Ex 5 Recall the Gaussian integers

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

$\quad \shortparallel$
$\quad R$

R is integral domain

For $r = a+bi \in R$ define

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

N is positive norm on R

Show N turns R into a Euclidean domain.

pf Note that

$$N(rs) = N(r)\,N(s) \qquad r,s \in R$$

Given $x,y \in R$ with $y \neq 0$

Display $q,r \in R$ s.t.

$$x = qy + r, \qquad N(r) < N(y)$$

Write

$$x = a+bi \qquad y = c+di$$

In $\mathbb{C}$,

$$y^{-1} = \frac{c-di}{c^2+d^2}$$

In $\mathbb{C}$,

$$xy^{-1} = \frac{(a+bi)(c-di)}{c^2+d^2}$$

$$= A + Bi.$$

where

$$A = \frac{ac+bd}{c^2+d^2}, \qquad B = \frac{bc-ad}{c^2+d^2}$$

$\exists\ \alpha, \beta \in \mathbb{Z}$ st

$$|A - \alpha| \le 1/2, \qquad |B - \beta| \le 1/2$$

Define $q = \alpha + \beta i$

Define $r = x - qy$

Show $N(r) < N(y)$

Show $\frac{N(r)}{N(y)} < 1$

$$\frac{N(r)}{N(y)} = \frac{N(\overbrace{x - qy}^{= (xy^{-1} - q)y})}{N(y)}$$

$$= \frac{N(xy^{-1} - q)\, N(y)}{N(y)}$$

$$= N(xy^{-1} - q)$$

$$= N\left(A - \alpha + (B - \beta)i\right)$$

$$= (A - \alpha)^2 + (B - \beta)^2$$

$$\leq \frac{1}{4} + \frac{1}{4}$$

$$= \frac{1}{2}$$

$$< 1 \qquad \checkmark$$

$\square$

<u>Recall</u> $\forall\ a \in R$,

$$Ra = \{ ra \mid r \in R \}$$

is the ideal of R generated by a.

Given any ideal $I \subseteq R$,

I is <u>principal</u> whenever

$\exists\ a \in R$ s.t.

$$I = Ra.$$

Prop 6 Assume R is a Euclidean domain with norm N.

Let A denote a nonO ideal of R

Define

$$m = \min\{ N(a) \mid a \in A,\ a \neq 0 \}$$

Pick

$$d \in A, \qquad N(d) = m$$

Then

$$A = Rd$$

In particular A is principal.

pf $A \supseteq Rd$ ✓

$A \subseteq Rd$:

Given $a \in A$ show $a \in Rd$

Since R is Euclidean,

$$\exists \; q, r \in R$$

st

$$a = qd + r$$

and

$$r = 0 \quad \text{or} \quad N(r) < N(d)$$

Obs

$$r = \underset{A}{\overset{}{\underset{\cap}{a}}} - q\underset{A}{\underset{\cap}{d}}$$

$$\in A$$

So

$$r = 0 \quad \text{or} \quad N(r) \geq m = N(d)$$

So

$$r = 0$$

Now

$$a = qd \in Rd$$

$\square$

Ex 7 Recall the ring

$$\underset{\substack{\parallel \\ R}}{\mathbb{Z}[\sqrt{-5}]} = \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$$

R is an integral domain

this ring is not a Eucl domain

pf We display an ideal **A** of R that is not principal

For $r = a + b\sqrt{-5}$ define

$$N(r) = a^2 + 5b^2$$

N is a positive norm on R

$$N(rs) = N(r)\,N(s) \qquad \forall\, r, s \in R$$

For $r \in R$

$$N(r) \in \{ 0, 1, 4, 5, 6, \dots \}$$

Define

$$x = 1 + \sqrt{-5} \qquad y = 2$$

So

$$N(x) = 1 + 5 = 6 \qquad N(y) = 4$$

Define ideal

$$A = Rx + Ry$$

Show A is not principal

Suppose A is principal, Write

$$A = Rd \qquad d \in R$$

$\exists$ $a, b \in R$ st

$$x = ad, \qquad y = bd$$

$$\underset{6}{\overset{\shortparallel}{N(x)}} = N(a)N(d) \qquad \underset{4}{\overset{\shortparallel}{N(y)}} = N(b)N(d)$$

$N(d)$ divides 4 and 6

$$N(d) \in \{1, 2\}$$

$$N(d) \neq 2 \qquad \text{so}$$

$$N(d) = 1$$

$$d = \mp 1$$

WLOG $d = 1$

$\exists \; r, s \in R$ st

$$rx + sy = 1$$

Write

$$r = a + b\sqrt{-5}, \qquad s = A + B\sqrt{-5}$$

$$a, b, A, B \in \mathbb{Z}$$

$$1 = (a + b\sqrt{-5})(1 + \sqrt{-5}) + (A + B\sqrt{-5})2$$

$$= \underbrace{a - 5b + 2A}_{\overset{\shortparallel}{1}} + \underbrace{(a + b + 2B)}_{\overset{\shortparallel}{0}}\sqrt{-5}$$

Mod 2,

$$1 \equiv a - 5b + 2A \equiv a + b$$

$$0 \equiv a + b + 2B \equiv a + b$$

Cont.

So A is not principal. $\square$

Recall our commutative ring R

DEF 8 Given $a, b \in R$ with $b \neq 0$

Write

$$b \mid a \quad \text{whenever} \quad a \in Rb$$

"b divides a"