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 norm on $R$ is a function

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

such that

$N(0) = 0$

The norm $N$ is positive whenever

$N(r) > 0 \quad \text{for all} \quad r \in R$
DEF 2 Assume $R$ is an integral domain.

Then $R$ is called Euclidean whenever it has a norm $N$ with the property:

$orall 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 $N(x) = |x|$ for $\forall x \in \mathbb{Z}$
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 \( a = bq + r \).
Example 9: Let $F$ denote a field.

Let $x$ be indeterminate.

Let $F[x] = \text{ring of polynomials in } x \text{ that have all coefficients in } F$.

Recall $F[x]$ is integral domain.

Define $N(f) = \text{degree of } f \quad f \in F[x]$.

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

$N$ turns $F[x]$ into Euclidian domain.
Ex 5  Recall the Gaussian integers

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

In \[ R \]

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

\[ N(rs) = N(r)N(s) \quad r, s \in R \]

Given \[ x, y \in R \] with \[ y \neq 0 \]

Display \[ q, r \in R \] s.t.

\[ x = qy + r \quad N(r) < N(y) \]

Write

\[ x = a + bi \]

\[ y = c + di \]

In \[ \mathbb{C} \]

\[ y^{-1} = \frac{c - di}{c^2 + d^2} \]
In \( \mathbb{C} \),

\[
x y^{-1} = \frac{(a + bi)(c - di)}{c^2 + d^2} = A + B i
\]

where

\[
A = \frac{ac + bd}{c^2 + d^2}, \quad B = \frac{bc - ad}{c^2 + d^2}
\]

\[
\exists \quad \alpha, \beta \in \mathbb{Z} \text{ such that } |A - \alpha| \leq \frac{1}{2}, \quad |B - \beta| \leq \frac{1}{2}
\]

Define

\[
t = \alpha + \beta i
\]

Define

\[
r = x - ty
\]

Show

\[
N(r) < N(t)
\]

Show

\[
\frac{N(r)}{N(t)} < 1
\]
\[
\frac{N(r)}{N(\gamma)} = \frac{N(\sqrt{x^2 - \gamma^2})}{N(\gamma)}
\]

\[
= \frac{N(x\gamma^2 - \gamma)}{N(\gamma)}
\]

\[
= N(x\gamma - \gamma)
\]

\[
= N\left(A - \alpha + (B - \beta)\right)
\]

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

\[
\leq \frac{1}{4} + \frac{1}{4}
\]

\[
= \frac{1}{2}
\]

\[
< 1
\]

\[\square\]
Recall \( \forall a \in R \)

\[ Ra = \{ ra \mid r \in R \} \]

is the ideal of \( R \) generated by \( a \).

Given any ideal \( I \subseteq R \),

\( I \) is principal whenever

\[ \exists a \in R \text{ s.t.} \]

\[ I = Ra. \]
Prop 6 Assume \( R \) is a Euclidean domain with norm \( N \).

Let \( A \) denote a nonzero ideal of \( R \).

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

Pick \( d \in A \), \( N(d) = m \).

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,

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

set

$$a = qd + r$$

and

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

Obs

$$r = a - qd$$

$$\in A \quad \exists A$$

So

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

So

$$r = 0$$

Now

$$a = qd \in R$$
Recall the ring
\[ \mathbb{Z}[\sqrt{-5}] = \left\{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \right\} \]

is an integral domain.

This ring is not a Eucl domain.

If 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 \( R \).

\[ N(rs) = N(r)N(s) \quad \forall r, s \in R \]

For \( r \in R \)
\[ N(r) \in \{0, 1, 4, 5, 6, \ldots \} \]

Define
\[ x = 1 + \sqrt{-5} \quad y = 2 \]

So
\[ N(x) = 1 + 5 = 6 \quad N(y) = 4 \]
Define ideal

\[ A = Rx + Ry \]

Show \( A \) is not principal.

Suppose \( A \) is principal. Write

\[ A = Rd \quad d \in \mathbb{R} \]

\[ \exists \ a, b \in \mathbb{R} \text{ s.t. } \]

\[ x = ad, \quad y = bd \]

\[ N(x) = N(a)N(d) \quad N(y) = N(b)N(d) \]

\[ \frac{11}{6} \]

\[ N(d) \text{ divides } 4 \text{ and } 6 \]

\[ N(d) \in \{1, 2, 3\} \]

\[ N(d) \neq 2 \quad \text{so} \]

\[ N(d) = 1 \]

\[ d = \pm 1 \]

Hence \( d = 1 \)

\[ \text{Hence } d = 1 \]
If \( r, a \in \mathbb{R} \) then
\[
r + ay = 1
\]
Write
\[
r = a + b \sqrt{-5}, \quad a = A + \beta \sqrt{-5}
\]
\[
a, b, A, \beta \in \mathbb{Z}
\]

\[
1 = \left( a + b \sqrt{-5} \right) \left( 1 + \sqrt{-5} \right) + \left( A + \beta \sqrt{-5} \right) \cdot 2
\]

\[
= a - 5b + 2A + \frac{1}{2} \cdot \left( a + b + 2\beta \right) \cdot \sqrt{-5}
\]

\[
\mod 2,
\]

\[
1 \equiv a - 5b + 2A \equiv a + b
\]

\[
0 \equiv a + b + 2\beta \equiv a + b
\]

\[\square\]

So, \( a \) is not principal.
Recall our commutative ring $R$.

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

$$b \mid a$$

whenever $a \in Rb$.

"b divides a"