Lecture 17

22 March 2024 16:11

Last time:

- In every PID, gcds always exist and if d is a gcd of a, b then you can write

$$d = xa + yb$$

- Theorem: Every PID is a UFD.

Euclidean Domains:

Think of these as integral domains where you can use "division algorithm" and "Euclid's Algorithm".

Definition: Let R be an integral domain. A Euclidean function on R is a function

$$d : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

satisfying: (a) $d(a \cdot b) \geq d(a)$ for any non-zero $a, b \in R$

(b) If $a, b \in R$ and $b \neq 0$ then there is a $q \in R$ and $r \in R$ such that $a = b \cdot q + r$ with $d(r) < d(b)$.

A Euclidean domain is an integral domain that admits a Euclidean function.

Examples.

- $R = \mathbb{Z}$ is a Euclidean domain, with Euclidean function

$$d : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

$$d(a) = |a| \leftarrow \text{absolute value}$$

This function d satisfies the two properties:

(a) $$|a \cdot b| = |a| \cdot \underbrace{|b|}_{\geq 1} \geq |a|$$

(b) Follows from the division algorithm for $\mathbb{Z}$.

Example:

Let F be a field (like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$)

Take R to be $R = F[x]$.

R is a Euclidean domain, with Euclidean function

$$d : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

$$d(f) := \text{degree of } f.$$

It satisfies the two properties because:

(a) $$\deg(f \cdot g) = \deg(f) + \underbrace{\deg(g)}_{\geq 0} \geq \deg(f)$$

(b) Division algorithm for polynomials.

If $f, g \in R$ and $g \neq 0$ then there is $q \in R$ and $r \in R$ such that

$$f = g \cdot q + r \quad \text{with} \quad \deg(r) < \deg(g).$$
or $r = 0$.

Example:
The ring $R = \mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, with Euclidean function

$$d : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

$$d(a+bi) = a^2 + b^2.$$

This satisfies the two properties:

(a) $d\big((a+bi)(c+di)\big) = d(a+bi) \cdot \underbrace{d(c+di)}_{\geq 1} \geq d(a+bi)$

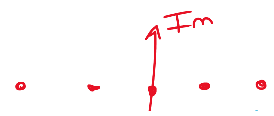
(b) Note that division of Gaussian integers might not be a Gassian integer

$$\frac{2+3i}{1+2i} = \frac{(2+3i)}{(1+2i)} \cdot \frac{(1-2i)}{(1-2i)} = \frac{2-6i^2-4i+3i}{1^2+2^2}$$

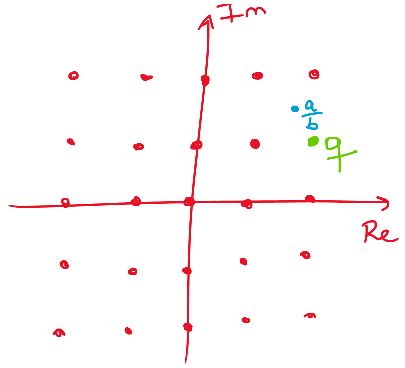
$$= \frac{8-i}{5} = \frac{8}{5} - \frac{1}{5} i.$$

Suppose $a = x + yi$ and $b = z + wi$

... number a



Consider the complex number $\frac{a}{b}$.



Let q be a closest Gaussian integer to $\frac{a}{b}$.

$$\left| q - \frac{a}{b} \right| \leq \frac{\sqrt{2}}{2} \quad \text{so} \quad \left| q - \frac{a}{b} \right|^2 \leq \frac{1}{2}.$$

Let r be $r = a - b \cdot q$.

$$(a = b \cdot q + r)$$

We have

$$d(r) = |a - bq|^2 = \left| b \cdot \left(\frac{a}{b} - q \right) \right|^2$$

$$= |b|^2 \cdot \left| \frac{a}{b} - q \right|^2 \leq \frac{|b|^2}{2} < |b|^2 = d(b) \quad \blacksquare$$

Theorem: Every Euclidean domain is a PID.

Exercises:

1. Perform the division algorithm in $\mathbb{Z}_5[x]$ to divide $f = x^3 - [3]_5 x + [4]_5$ by $g = [3]_5 x - [2]_5$.

2. Use the extended Euclid Algorithm to compute a gcd between $a = 2$ and $b = 3 + i$ in $\mathbb{Z}[i]$.

(3) Let F be a field. Show that the function

$$d: F \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$
$$d(a) = 1$$

is a Euclidean function.

(so every field is a Euclidean domain)

Answers:

(1)
$$q = [2]_5 x^2 + [3]_5 x + [1]_5$$
$$r = [1]_5$$

(2) Euclid's Algorithm

$$\underbrace{3+i}_{a} = \underbrace{2}_{b} \cdot 1 + \underbrace{(1+i)}_{r_1}$$

$$\underbrace{2}_{b} = \underbrace{(1+i)}_{r_2}(1-i) + \underbrace{0}_{r_2}$$

A gcd is $1+i$.

Other valid answers: $-1-i$, $-1+i$, $1-i$.

(3) Hint: The division algorithm holds.

easily as we can always get $r=0$.