Lecture 15

18 March 2024 14:00

Last time:

We talked about greatest common divisors.

g.c.d. might not always exist, but if it does then it is unique up to associate class. (in integral domains).

Theorem: If R is a unique factorisation domain then any two elements have a g.c.d. (an it is unique up to associate class)

Idea of the proof:

Suppose $a, b \in R$.

- If one of them is zero, say $a = 0$, then b is a g.c.d. of 0 and b.
- If one of them is a unit, say a is a unit, then 1 is a g.c.d of a and b.
- If neither a nor b are 0 or units, we can factor them (uniquely up to associates) into irreducibles

$$a = p_1 \cdot p_2 \cdots p_k$$

$$b = q_1 \cdot q_2 \cdots q_l$$

where p_i and q_j are all irreducible elements.

Pick representatives $r_1, r_2, \dots, r_m$ for every associate

Pick representatives $r_1, r_2, \dots, r_m$ for

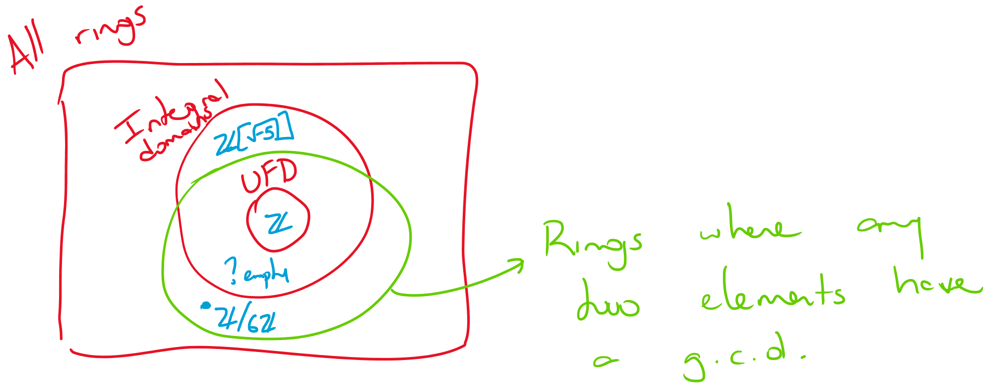
class among $\{p_1, \dots, p_k, q_1, \dots, q_e\}$

Define k_i to be the largest integer such that

$$r_i^{k_i} \mid a \quad \text{and} \quad r_i^{k_i} \mid b.$$

Let $d = r_1^{k_1} \cdot r_2^{k_2} \cdots r_m^{k_m}$. Because factorisations into irreducibles are "unique", one can show that this is a g.c.d of a and b. ■

Picture



$\mathbb{Z}/6\mathbb{Z}$: Do any two elements have a g.c.d?

$\{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$

Do $[2]_6$ and $[3]_6$ have a g.c.d?

Divisors of $[2]_6$: $[1]_6, [2]_6, [4]_6, [5]_6$

Divisors of $[3]_6$: $[1]_6, [3]_6, [5]_6$

Common divisors: $[1]_6, [5]_6$

Both of them are g.c.ds.

Do g.c.ds always exist in the ring $\mathbb{Z}/m\mathbb{Z}$?

- Do g.c.ds always exist in the ring $\mathbb{Z}/m\mathbb{Z}$?

Generating ideals in a domain

$\rightarrow$ Comm. ring with identity.

Let R be a domain, and $a_1, a_2, \dots, a_m \in R$.

Define

$$\underbrace{\langle a_1, a_2, \dots, a_m \rangle}_{\text{the ideal of } R \text{ generated by } a_1, \dots, a_m} := \left\{ r_1 a_1 + r_2 a_2 + \dots + r_m a_m : \begin{matrix} r_1, r_2, \dots, r_m \\ \text{are} \\ \text{any} \\ \text{elements} \\ \text{of } R \end{matrix} \right\}$$

Ex: $R = \mathbb{Z}$. What is $\langle 6, 8 \rangle$?

$$\langle 6, 8 \rangle = \{ m \cdot 6 + n 8 : m, n \in \mathbb{Z} \}$$
$$= 2\mathbb{Z}.$$

$R = \mathbb{Z}[x]$. What is $\langle 2, x \rangle$?

$$\langle 2, x \rangle = \{ p(x) \cdot 2 + q(x) \cdot x : p(x), q(x) \in \mathbb{Z}[x] \}$$

Is $2 + 3x^2 \in \langle 2, x \rangle$? Yes: $2 + 3x^2 = (1) \cdot 2 + (3x) \cdot x$

Is $3 + 3x^2 \in \langle 2, x \rangle$? No, because the constant term is odd.

Is $4 + x + 2x^3 \in \langle 2, x \rangle$? Yes: $(2) 2 + (2x^2 + 1) \cdot x$

Conclusion: $\langle 2, x\rangle = \{$ polynomials in $\mathbb{Z}[x]$ with even constant term $\}$.

Note that this ideal is not equal to the multiples of one single polynomial.

Proposition:

$\langle a_1, \dots, a_m\rangle$ is an ideal of R. In fact, it the smallest ideal of R containing the elemets $a_1, \dots, a_m$.

Proof:

To prove that $\langle a_1, \dots, a_m\rangle$ is an ideal, we use the ideal test:

(I0) $\langle a_1, \dots, a_m\rangle$ is nonempty because $0 \in \langle a_1, \dots, a_m\rangle$

$$0 = 0 \cdot a_1 + 0 \cdot a_2 + \dots + 0 \cdot a_m$$

(I1) If $x_1 a_1 + x_2 a_2 + \dots + x_m a_m \in \langle a_1, \dots, a_m\rangle$

and $y_1 a_1 + y_2 a_2 + \dots + y_m a_m \in \langle a_1, \dots, a_m\rangle$

then their difference is

$$(x_1 - y_1) \cdot a_1 + (x_2 - y_2) \cdot a_2 + \dots + (x_m - y_m) a_m$$

which is an element of $\langle a_1, \dots, a_m\rangle$.

(I2) If $x_1 a_1 + x_2 a_2 + \dots + x_m a_m \in \langle a_1, \dots, a_m\rangle$

and $r \in R$, their product is

$$(r x_1) a_1 + (r x_2) a_2 + \dots + (r x_m) a_m$$

which is an element of $\langle a_1, \dots, a_m\rangle$.

$(r x_1)a_1 + (r x_2)a_2 + \cdots + (r x_m) \ldots$

which is an element of $\langle a_1, \ldots, a_m \rangle$.

This shows $\langle a_1, \ldots, a_m \rangle$ is an ideal of R.

It contains $a_1, \ldots, a_m$ because

$$a_1 = 1 \cdot a_1 + 0\, a_2 + 0\, a_3 + \cdots + 0\, a_m \in \langle a_1, \ldots, a_m \rangle$$

$$a_2 = 0 \cdot a_1 + 1 \cdot a_2 + 0 \cdot a_3 + \cdots + 0 \cdot a_m \in \langle a_1, \ldots, a_m \rangle$$

$$\vdots$$

$$a_m = 0 \cdot a_1 + 0\, a_2 + \cdots + 1 \cdot a_m \in \langle a_1, \ldots, a_m \rangle.$$

It is the smallest ideal containing $a_1, \ldots, a_m$

because if some ideal I contains $a_1, a_2, \ldots, a_m$,

I must contain $x_1 a_1$ for any $x_1 \in R$

I " " $x_2 a_2$ for any $x_2 \in R$

$\vdots$

I must contain $x_m a_m$ for any $x_m \in R$

Since I is closed under addition, I must contain $x_1 a_2 + x_2 a_2 + \cdots + x_m a_m$. ■

- In other words, if I ideal such that $a_1, \ldots, a_m \in I$ then $\langle a_1, \ldots, a_m \rangle \subseteq I$.

Ex: In $R = \mathbb{Z}$ $\quad \langle 12, 18, 36 \rangle = \{ n \cdot 12 + m \cdot 18 + p \cdot 36 : n, m, p \in \mathbb{Z} \}$

$= 6\mathbb{Z}$.

This is the smallest ideal that contains 12, 18, 36.

There are other ideals containing 12, 18, 36,

e.g. $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \underline{6\mathbb{Z}}$.

this one is contained in all four of them.

<u>Def</u>: An ideal I of a domain R is called <u>principal</u> if $I = \langle a \rangle$ for some $a \in R$.

$$= \{x \cdot a : x \in R\}$$

$$= \{\text{all multiples of } a\}.$$

<u>Def</u>: An integral domain R is called a <u>principal ideal domain</u> PID if all ideals of R are principal.

<u>Ex</u>: $\mathbb{Z}$ is a PID because any ideal I of $\mathbb{Z}$ has the form $I = m \cdot \mathbb{Z} = \langle m \rangle$.

<u>Ex</u>: $\mathbb{Z}[x]$ is not a PID because $\langle 2, x \rangle$ is not principal, as it cannot be generated by just one polynomial.

<u>Ex</u>: $\mathbb{Z}/7\mathbb{Z}$ is a field because all nonzero elements are units. The ideals of $\mathbb{Z}/7\mathbb{Z}$

elements are units. The ideals of $\mathbb{Z}/7\mathbb{Z}$

are $$1\cdot\mathbb{Z}/7\mathbb{Z} = \{[0]_7, \dots, [6]_7\} = \langle [1]_6 \rangle$$

$$7\cdot\mathbb{Z}/7\mathbb{Z} = \{[0]_7\}. = \langle [0]_7 \rangle$$

These ideals are both principal, so $\mathbb{Z}/7\mathbb{Z}$ is a PID.