Lecture 14

15 March 2024 16:06

Last time:

- Units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$.
- We defined irreducible elements of an integral domain, and defined unique factorisation domains (UFD)
- Gauss' Lemma: If R is a UFD then $R[x]$ is also UFD.

Remark: The ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is not a UFD (Coursework 3).

Greatest common divisors and divisibility

If R is a commutative ring, $a, b \in R$ we say that a divides b if there exists $c \in R$ such that $b = a \cdot c$.

We also say that b is a multiple of a.

Proposition: Suppose a, a' are associate elements, and b, b' are associate elements in a domain R.

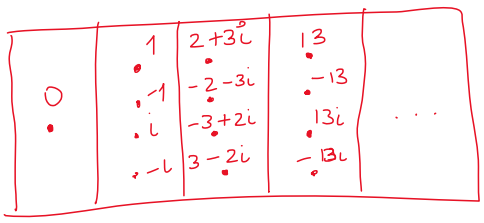
Then $a \mid b \iff a' \mid b'$

$a \mid b \iff a \mid b$

$a \mid b$: a divides b

$a \mid b$: a' divides b'.

Example. $\mathbb{Z}[i]$



→ associate classes (infinitely many)

Question.

Does $2+3i \mid 13$?

Yes because $13 = 4 + 9 = 2^2 + 3^2 = 2^2 - (3i)^2$

$= (2+3i)(2-3i)$

- Our proposition says that any associate of $2+3i$ divides any associate of 13.

Proof of proposition

Suppose a is associate to a' and b is associate to b'. This means $a = a' \cdot u$ and $b = b' \cdot v$ for u, v units of R.

If $a \mid b$, there exists $c \in R$ such that $b = a \cdot c$.

that $b = a \cdot c$.

Substituting, we get

$$b' \cdot v = a' \cdot u \cdot c$$

Multiplying by v^{-1}, we get

$$b' = a' \cdot (u \cdot c \cdot v^{-1})$$

showing that $a' \mid b'$.

Definition: Let R be a domain.

A greatest common divisor (g.c.d) between $a, b \in R$ is an element $d \in R$ such that

- $d \mid a$ and $d \mid b$.
- whenever $c \mid a$ and $c \mid b$, we have $c \mid d$.

Remark: Two elements $a, b \in R$ might have several g.c.d.s:

For instance, in $\mathbb{Z}$ 6 is a gcd of 18, 24

but also -6 is a gcd of 18, 24

Proposition:

- $1 \cdot R$

Proposition:

In a domain R

- a g.c.d between 0 and a is a.
- a g.c.d between 1 and a is 1.

Remark: In general integral domains, g.c.ds might not exist. (in not UFD).

Proposition: Suppose R is an integral domain.

- If $c \mid d$ and $d \mid c$ then c, d are associates
- "g.cds are unique up to associates", that is, if d, d' are g.c.ds of $a, b \in R$ then d and d' are associates.

Proof: Suppose $c \mid d$ and $d \mid c$. This means there exists $a \in R$ such that $d = c \cdot a$, and also there exists $b \in R$ such that $c = d \cdot b$.

Substituting, we get $c = c \cdot a \cdot b$.

- If $c \neq 0$, we can use the cancellative law (integral domain) to conclude $1 = a \cdot b$

to conclude $1 = a \cdot b$

So a, b are units, and therefore c, d are associates.

- If $c = 0$ then $d = 0$ so the proposition also holds.

- The second part follows directly from the first one, because if d and d' are g.cds of a, b then $d \mid d'$ and $d' \mid d$ so d and d' are associates by part a.

//

Common mistakes in CW1

- The "additive identity" of a ring does not need to be the element 0.

In Q1a, the multiplicative identity was the real number 0. (not the real number 1)

- In Q2a, many people used

"$(a+b)^2 = a^2 + 2ab + b^2$" ← not correct

$= a^2 + ab + ba + b^2$ ← correct.

Moreover 2 might not be an element of R so $2 \cdot a \cdot b$ does not make sense.

of R, so $\underline{2} \cdot a \cdot b$ does not make sense.

- In Q3b, many people said a symmetric matrix looks like $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ → not necessarily the same.

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} \leftarrow \text{correct.}$$

- In Q5d, people used

$$A \text{ is invertible} \iff \det(A) \neq 0$$

This is only true for matrices with entries in a field (like $\mathbb{R}$, $\mathbb{C}$), but not over any ring.

"

Questions about CW2:

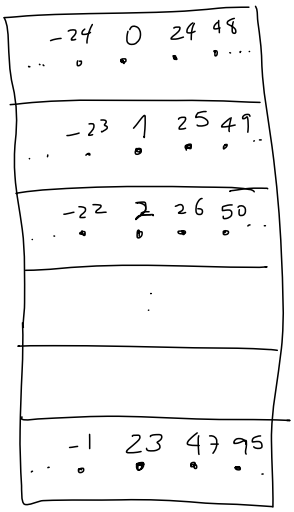
- In Q3a

$$f : \mathbb{Z}_{24} \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_6$$

$$[x]_{24} \longmapsto ([x]_4, [4x]_6)$$

Show this is well-defined.

$\mathbb{Z}_{24}$



$\longmapsto \left([\ ]_4 , [4\cdot]_6 \right)$

we should show that the answer here does not depend on the choice of x.

In other words we must show:

$$[x]_{24} = [y]_{24} \implies \left([x]_4 , [4x]_6 \right) = \left([y]_4 , [4y]_6 \right)$$

Q5c

Is the element $[2]_4 + [1]_4 x + [2]_4 x^2$ a zero-divisor in $\mathbb{Z}_4[x]$?

Zero-divisor means

$$\left([2]_4 + [1]_4 x + [2]_4 x^2 \right) \cdot \left([\ ]_4 + [\ ]_4 x + [2]_4 x^2 \right) = [0]_4$$

(0 or 2; has to be 2; might not be quadratic...)

Think about the x^3 term...