Lecture 11

26 February 2024 14:08

Isomorphism Theorems.

- **1st Iso Thm.**

If $f : R \to T$ is a homomorphism then

$$R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

- **2nd Iso Thm:**

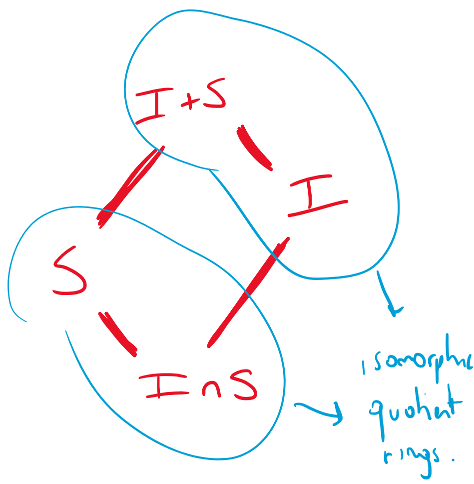
R ring and I ideal of R.

$$\left\{ \begin{array}{c} \text{subrings of } R \\ \text{containing } I \end{array} \right\} \xleftrightarrow[\text{bijection}]{1\text{-to-}1} \left\{ \begin{array}{c} \text{subrings} \\ \text{of } R/I \end{array} \right\}$$

- **3rd Iso Thm:**

I ideal, S subring of R. Then

$$S/I \cap S \cong I+S/I$$



Part II: Integral domains and factorisation

Definition: A **zero-divisor** in a ring R is a **non-zero** element $a \in R$ such that there exists a nonzero $b \in R$ satisfying

$$a \cdot b = 0 \, .$$

Example: In $\mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z}$ (integers modulo 6)

there are zero-divisors:

For instance $[2]_6 \neq 0$, $[3]_6 \neq 0$ but

$$[2]_6 \cdot [3]_6 = [0]_6 \leftarrow \text{zero of the ring.}$$

zero-divisors.

Example: In the ring $M_{2\times 2}(\mathbb{R})$, there are zero-divisors. For instance

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

zero-divisors.

Examples: In $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, there are no zero-divisors.

Definition: A domain is a commutative ring with identity.

An integral domain is a domain with no zero-divisors.

An <u>integral domain</u> is a domain with no zero-divisors.
$\underbrace{\text{integral}}_{\text{like the integers.}}$

Equivalently, a ring R is an integral domain if $a \cdot b = 0 \implies a = 0$ or $b = 0$.

<u>Example</u>: The ring of <u>Gaussian integers</u> is

$$\mathbb{Z}[i] = \{ a + bi \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{Z} \}.$$

This is a subring of $\mathbb{C}$.
We have $x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$ in $\mathbb{Z}[i]$ because it is true in general for any elements of $\mathbb{C}$.

- <u>Proposition</u>: A subring of an integral domain must be an integral domain.

<u>Rings of polynomials</u>:

If R is any ring, we can construct the ring $R[x]$ of polynomials in the variable x

ring $R[x]$ of polynomials in the variable x with coefficients in the ring R:

$$f(x) = r_0 + r_1 \cdot x + r_2 \cdot x^2 + r_3 x^3 + \dots + r_d x^d.$$

with $r_0, r_1 \dots, r_d \in R$.

The degree of a polynomial $f(x)$ is the largest d such that r_d is not zero.

Addition and multiplication in $R[x]$ are done as usual for polynomials.

This satisfies all the axioms of a ring.

- $R[x]$ has an identity if R has an identity
- $R[x]$ is commutative if R is commutative.

<u>Example</u>: $R = \mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$.

Consider $R[x] = \mathbb{Z}_4[x]$.

$$f = [1]_4 + [2]_4 x + [2]_4 x^2$$

$$g = \qquad [3]_4 x + [2]_4 x^2$$

$$f + g = [1]_4 + [1]_4 x$$

$$f+g = [1]_4 + [1]_4\, x$$

$$f \cdot g = \left([1]_4 + [2]_4\, x + [2]_4\, x^2\right) \cdot \left([3]_4\, x + [2]_4\, x^2\right)$$

$$= [3]_4\, x + [2]_4\, x^3 .$$

Note that $\deg(f \cdot g) < \deg(f) + \deg(g)$.

This happened because there are zero-divisors.

- If R is an integral domain,

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Proposition: (Cancellative law for multiplication)

If R is an integral domain then

$$a \cdot b = a \cdot c \quad \text{and} \quad a \neq 0 \implies b = c.$$

(you can cancel out the a on both sides).

Proof: Assume $a \cdot b = a \cdot c$ and $a \neq 0$.

$$\implies ab - ac = 0$$

$$\implies a(b-c) = 0$$

Since R has no zero-divisors, this means that $a = 0$ or $b - c = 0$

But we are assuming $a \neq 0$, so

$$b - c = 0$$

$$\Rightarrow \quad b = c. \qquad \blacksquare$$

<u>Definition</u>: Let R be a ring with identity. An element $u \in R$ is called a <u>unit</u> (or <u>invertible</u>) if there exists $v \in R$ such that

$$u \cdot v = 1$$

$$v \cdot u = 1.$$

<u>Examples</u>:

- In $\mathbb{Z}$, the units are 1 and -1.
- In fact, 1 and -1 are always units in any ring with identity (but it might be that $1 = -1$).

- In $\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$ we have:

$[0]_{12}$ ← neither unit nor zero-divisor
$[1]_{12}$ ← unit
$[2]_{12}$ ← zero-div
$[3]_{12}$ ← zero-div
$[4]_{12}$ ← zero-div
$[5]_{12}$ ← unit $[5]_{12} \cdot [5]_{12} = [1]_{12}$
$[6]_{12}$ ← zero-div
$[7]_{12}$ ← unit $[7]_{12} \cdot [7]_{12} = [1]_{12}$
$[8]_{12}$ ← zero-div
$[9]_{12}$ ← zero-div
$[10]_{12}$ ← zero-div.
$[11]_{12}$ ← unit $[11]_{12} \cdot [11]_{12} = [1]_{12}$

- A division ring is a ring in which every nonzero is a unit.

- Proposition: If R ring with "identity". If U is a unit then its inverse is unique.

Proof: Assume V_1 and V_2 are elements of R such that

$$U \cdot V_1 = 1 \qquad U \cdot V_2 = 1$$
$$V_1 \cdot U = 1 \qquad V_2 \cdot U = 1$$

Subtracting both equations we get:

$$U \cdot V_1 - U \cdot V_2 = 1 - 1 = 0$$

$$\Rightarrow \quad U(V_1 - V_2) = 0$$

$$\Rightarrow \quad V_1 \underbrace{U}_{1} (V_1 - V_2) = \underbrace{V_1 \cdot 0}_{0}$$

$$\Rightarrow \quad \overset{1}{\cancel{v_1 \cdot u}} \cdot (v_1 - v_2) = \cancel{v_1 \cdot} \, 0$$

$$\Rightarrow \quad 1 \cdot (v_1 - v_2) = 0$$

$$\Rightarrow \quad v_1 - v_2 = 0$$

$$\Rightarrow \quad v_1 = v_2 \qquad \blacksquare$$

<u>Remark</u>: <u>The</u> inverse of u is denoted u^{-1}.

<u>Example</u>: $R = \mathbb{Z}_{12}$

- Is it true that

$$[3]_{12} \cdot x = [3]_{12} \cdot y \Rightarrow x = y \ ?$$

<u>No</u>, for instance $x = [4]_{12}$ $y = [8]_{12}$.

Reason: $[3]_{12} \cdot \underbrace{(x - y)}_{\text{does not need to be zero.}} = 0$.

as $[3]_{12}$ is a zero-divisor

- Is it true that

$$[5]_{12}\, x = [5]_{12}\, y \Rightarrow x = y \ ?$$

Yes, because you can multiply by $[5]_{12}^{-1} = [5]_{12}$

to get

So get

$$\cancel{[5]_{12}^{-1}[5]_{12}}\, x = \cancel{[5]_{12}^{-1}[5]_{12}}\, y$$

$$x = y.$$