Lecture 7
12 February 2024 14:08

Last time:

- All cosets of a subring S in a ring R have all the same cardinality, equal to $|S|$.

- Defined homomorphism of rings

A function $f : R \longrightarrow T$

satisfying
$$f(a+b) = f(a) + f(b)$$
$$f(a \cdot b) = f(a) \cdot f(b).$$

Properties of homomorphisms

Proposition: If $f : R \longrightarrow T$ is a ring homomorphism

(a) $f(0_R) = 0_T$

(b) $f(-a) = -f(a)$

negative in R — negative in T

(c) $f(a-b) = f(a) - f(b)$.

Proof:

(a) $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$

Using the cancellative law (in T) we get

$$0_T = f(0_R)$$

(b) We want to show that $f(-a)$ is the negative of $f(a)$. In other words:

$$f(-a) +_T f(a) \stackrel{?}{=} 0_T$$

$$f(-a + a) \stackrel{?}{=} 0_T$$

$$f(0_R) \stackrel{?}{=} 0_T \quad \checkmark \text{ Part (a)}$$

(c) $f(a-b) = f(a + (-b))$

$$= f(a) + f(-b)$$

$$= f(a) + (-f(b))$$

$$= f(a) - f(b)$$

Images and kernels of homomorphisms

Suppose $f: R \longrightarrow T$ is a homomorphism of rings.

The <u>image</u> of f is

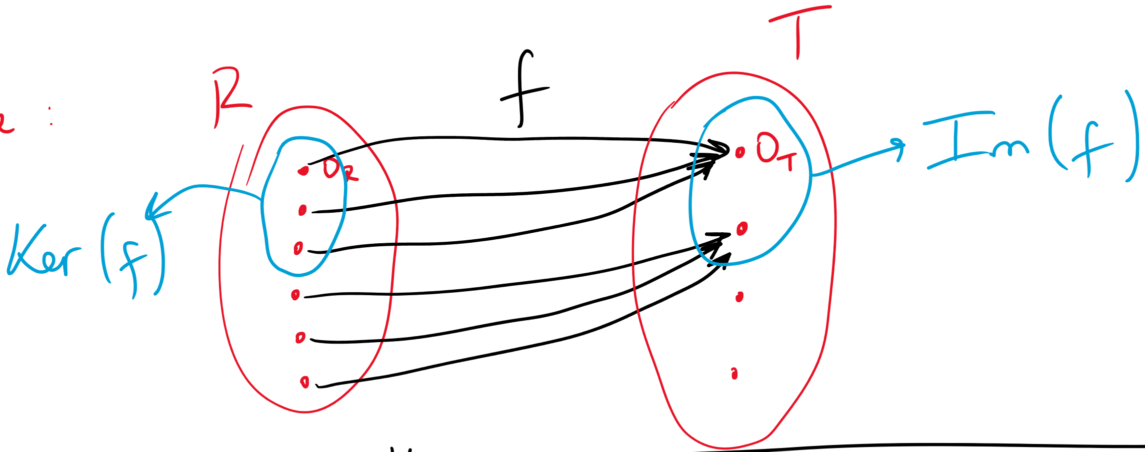
$$\mathrm{Im}(f) = \{ b \in T \mid \text{there exists } a \in R \text{ satisfying } f(a) = b \}$$

$$= \{ f(a) \in T \mid a \in R \}$$

The <u>kernel</u> of f is

$$\mathrm{Ker}(f) = \{ a \in R \mid f(a) = 0_T \}$$

Picture:



<u>Ex</u>: Consider $f : \mathbb{Z} \longrightarrow \mathbb{Z}_6$ defined as

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

$$f(n) = [3n]_6 .$$

(For instance:

$$f(3) = [9]_6 = [3]_6$$

$$f(14) = [42]_6 = [0]_6$$

$$f(5) = [15]_6 = [3]_6 \quad)$$

It's [illegible] that f is a homomorphism:

$$f(5) = [15]_6 = [3]_6$$

Let's prove that f is a homomorphism:

$$f(a+b) = [3(a+b)]_6 = [3a+3b]_6$$
$$= [3a]_6 + [3b]_6$$
$$= f(a) + f(b).$$

$$f(a \cdot b) = [3(a \cdot b)]_6 = [3ab + 6ab]_6$$
$$= [9ab]_6 = [3a]_6 \cdot [3b]_6$$
$$= f(a) \cdot f(b). \blacksquare$$

The image of f is:

$$\text{Im}(f) = \{[0]_6, [3]_6\}$$

The kernel of f is:

$$\text{Ker}(f) = \text{even numbers} = 2\mathbb{Z} = \{0, 2, 4, \ldots, -2, -4, \ldots\}.$$

<u>Remark</u>: Any homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_m$ has to be of the form

$$f(n) = [\underbrace{k}_{\text{some constant}} \cdot n]_m.$$

This is because:

$$f(0) = [0]_m$$

$$f(1) = [k]_m$$

some integer.

$$f(2) = [k\cdot 2]_m$$

$$f(3) = [k\cdot 3]_m$$

$$f(4) = [k\cdot 4]_m$$

$$\vdots$$

$$f(-1) = [k(-1)]_m$$

$$f(-2) = [k(-2)]_m$$

$$\vdots$$

In general $f(n) = [k\cdot n]_m$.

⚠ Not every k will satisfy $f(a\cdot b) = f(a)\cdot f(b)$.

only some special values, depending on m.

- Challenge exercise: Find the exact condition on m and k that makes this a homomorphism.

//

Proposition: Suppose $f: R \to T$ is a homomorphism.

(a) $Im(f)$ is a subring of T.

(b) $Ker(f)$ is a subring of R.

(c) In fact, $Ker(f)$ satisfies:

$$a \in Ker(f) \text{ and } b \in R \Rightarrow a \cdot b \in Ker(f).$$

Proof:

(a). let's use the subring test for $Im(f)$:

(S0) $Im(f) \neq \phi$ because $0_T \in Im(f)$.
(because $f(0) = 0_T$)

(S1) Suppose $a, b \in Im(f)$. This means

$$a = f(x) \text{ and } b = f(y).$$

Then $f(x-y) = f(x) - f(y) = a - b$

so $a - b \in Im(f)$.

(S2) Suppose $a, b \in Im(f)$. This means that

$$a = f(x) \text{ and } b = f(y)$$

Then $f(x \cdot y) = f(x) \cdot f(y) = a \cdot b$, so $a \cdot b \in Im(f)$.

(b) Using the subring test for $Ker(f)$:

(S0) $Ker(f) \neq \phi$ because $0_R \in Ker(f)$
(because $f(0_R) = 0$).

(S1) Suppose $a, b \in Ker(f)$. This means that

$$f(a) = 0 \text{ and } f(b) = 0.$$

Then $f(a-b) = f(a) - f(b) = 0 - 0 = 0$,

so $a-b \in Ker(f)$.

(S2) We want to show that if $a, b \in Ker(f)$

then $a \cdot b \in Ker(f)$.

Instead, let's prove the stronger statement

(C). If $a \in Ker(f)$ and $b \in R$ then $a \cdot b \in Ker(f)$.

Take $a \in Ker(f)$ and $b \in R$. This means that

$f(a) = 0$.

need not be 0.

Then $f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot f(b) = 0$

and so $a \cdot b \in Ker(f)$. ∎

<u>Definition</u>: A subring S of a ring R

is called an <u>ideal</u> if

$$a \in S \text{ and } b \in R \implies a \cdot b \in S.$$

<u>Ex</u>: We just proved that kernels of homomorphisms are always ideals.

<u>Ex</u>: If $R = \mathbb{Z}$ and $S = m \cdot \mathbb{Z}$ then

S is an ideal of R.

[Proof: If $a \in S$ then $a = m \cdot k$, and then $a \cdot b = m \cdot k \cdot b \in m\mathbb{Z} = S$]

Ex: A subring that is not an ideal:

If $R = \mathbb{Q}$ and $S = \mathbb{Z}$ then S is not an ideal: for instance $2 \in \mathbb{Z}$ $\frac{1}{3} \in \mathbb{Q}$ but $2 \cdot \frac{1}{3} = \frac{2}{3} \notin \mathbb{Z}$.

Exercise: $R = M_{2\times 2}(\mathbb{R})$ and S = upper triangular matrices

Explain why S is not an ideal.

Proposition. (The ideal test).

A subset I of a ring R is an ideal of R if and only if it satisfies

(I0) $I \neq \emptyset$

(I1) $a, b \in I \Rightarrow a - b \in I$

(I2) $a \in I$, $b \in R \Rightarrow a \cdot b \in I$.