Math 521A

3.3 – Isomorphisms and Homomorphisms

Consider the ring $R = \{0, 2, 4\}$ (subring of $\mathbb{Z}_6$) and $S = \mathbb{Z}_3$. Let us write down the respective addition tables:

R:

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

S:

+	0	2	1
0	0	2	1
2	2	1	0
1	1	0	2

and now the multiplication tables:

R:

·	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

S:

·	0	2	1
0	0	0	0
2	0	1	2
1	0	2	1

Note that the addition (respectively, multiplication) table for S can be obtained from the addition (respectively, multiplication) table for R if we relabel 4 as 1, while not relabeling the other elements (or relabeling each other element as itself).

Formally, what we have done was to define a bijective mapping $f : R \to S$ given by $f(0) = 0, f(2) = 2, f(4) = 1$, and satisfying:

(i) $f(a + b) = f(a) + f(b)$, i.e., the label of $a + b$ equals the label of a plus the label of b;

(ii) $f(a \cdot b) = f(a) \cdot f(b)$, i.e., the label of ab equals the label of a times the label of b

for all $a, b \in R$. Note that the $+$ and the $\cdot$ on the LHS take place in the ring R whereas the $+$ and the $\cdot$ on the RHS take place in the ring S.

Definition

A ring R is isomorphic to a ring S (notation: $R \cong S$) if $\exists f : R \to S$ such that

(i) f is bijective;

(ii) $f(a + b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)\ \forall\ a, b \in R$.

In this case, f is called an isomorphism.

Remark: Notice that in our original example, the mapping $f : R \to S$ given by

$$0 \mapsto 0, \quad 2 \mapsto 1, \quad 4 \mapsto 2,$$

is **not** an isomorphism from R into S: Compare $f(2 \cdot 2)$ and $f(2) \cdot f(2)$.

Example

The mapping $f : M_2(\mathbb{R}) \to \mathbb{C}$ given by

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + bi \quad \forall a, b \in \mathbb{R}$$

is an isomorphism.

Example

Is $\begin{array}{cccc} f: & \mathbb{Z} & \to & 2\mathbb{Z} \\ & x & \mapsto & 2x \end{array}$ an isomorphism?

$\cong$ is an equivalence relation on the set of all rings:

- $R \cong R$;
- $R \cong S \Rightarrow S \cong R$;
- $R \cong S,\ S \cong T \Rightarrow R \cong T$.

Definition

Let R, S be rings. A function $f : R \to S$ is said to be a homomorphism if

$$f(a+b) = f(a) + f(b) \quad \text{and} \quad f(a \cdot b) = f(a) \cdot f(b)$$

$\forall\ a, b \in R$.

Remark: Every isomorphism is a homomorphism, but not conversely.

Example (Trivial homomorphism)

$$\begin{array}{rccc} f: & R & \to & S \\ & x & \mapsto & 0_S \end{array}.$$

Example (Projection)

$$\begin{array}{rccc} \pi_1: & R_1 \times R_2 & \to & R_1 \\ & (x,y) & \mapsto & x \end{array}, \quad \begin{array}{rccc} \pi_2: & R_1 \times R_2 & \to & R_2 \\ & (x,y) & \mapsto & y \end{array}$$

Example

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & x & \mapsto & [x]_n \end{array}$$

Theorem

Let $f : R \to S$ be a homomorphism. Then:

(1) $f(0_R) = 0_S$;

(2) $f(-a) = -f(a), \quad \forall a \in R$.

(3) $f(a-b) = f(a) - f(b), \quad \forall a, b \in R$.

If R is a ring with identity and f is surjective then:

(4) *S is a ring with identity and $f(1_R) = 1_S$;*

(5) *a is a unit in $R \Rightarrow f(a)$ is a unit and $f(a)^{-1} = f(a^{-1})$.*

The proof of the last theorem is on the board.

In preparation for the next result, here is a definition: Let $f : A \to B$ be any mapping. The image of f, denoted by $f(A)$, is defined as

$$f(A) := \{f(x) \mid x \in A\}.$$

Note that $f(A)$ is contained in B, or $f(A)$ is a subset of B.

Corollary

If $f : R \to S$ is a homomorphism then $f(R)$ is a subring of S.

Example

$\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$ because units must be mapped into units. Note that $f(1) = 1$ (by Part (4) of the theorem), so $f(2) = f(1+1) = f(1) + f(1) = 2$. In conclusion, $2 \in \mathbb{Q}$ is a unit, but $f(2) \in \mathbb{Z}$ is not. This contradicts Part (5) of the theorem.

Example

Show that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Hint: Let $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be an isomorphism. Calculate $f(0), f(1)$, and $f(1+1) = f(1) + f(1)$.

Example

Determine all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

Example

Is $\begin{array}{cccc} f: & \mathbb{Z}_5 & \to & \mathbb{Z}_2 \\ & [x]_5 & \mapsto & [x]_2 \end{array}$ a ring homomorphism? Hint: f is not well-defined.

Example

Is $\begin{array}{cccc} f: & \mathbb{Z}_6 & \to & \mathbb{Z}_2 \\ & [x]_6 & \mapsto & [x]_2 \end{array}$ a ring homomorphism?

Example

Is $\begin{array}{rccc} f: & \mathbb{Z}_{12} & \to & \mathbb{Z}_5 \\ & [x]_{12} & \mapsto & [x]_5 \end{array}$ a ring homomorphism?

Example

Is $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$?