MTHSC 412 Section 3.3 – Isomorphisms and Homomorphisms

Kevin James

Example

Consider the set $S = \{0, 2, 4, 6, 8\} \subseteq \mathbb{Z}_{10}$. Its addition and multiplication tables are below.

$+$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

$\times$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

Note

1. S is a subring of $\mathbb{Z}_{10}$. It is commutative and has an identity.
2. In fact, S is even a field.
3. Have you seen this field before?
4. It "looks like" $\mathbb{Z}_5$.

Fact

We can define a map $\phi : S \to \mathbb{Z}_5$ *by* $\phi(x) = [x]_5$. *This map has the inverse map* $\psi : \mathbb{Z}_5 \to S$ *given by* $\psi(y) = [6y]_{10}$.

Note

1. ϕ is 1-1 and onto.
2. So, we can think of ϕ as a relabeling of the members of S provided that this relabeling preserves our addition and multiplication tables.
3. $\phi(a+b) = \phi(a) + \phi(b)$.
4. $\phi(ab) = \phi(a)\phi(b)$.

Definition

Suppose that R and S are rings. We say that a map $\phi : R \to S$ is an isomorphism of rings if the following hold.

1. ϕ is bijective (-i.e. 1-1 and onto).
2. $\phi(a + b) = \phi(a) + \phi(b)$.
3. $\phi(ab) = \phi(a)\phi(b)$.

In the case that there is an isomorphism $\phi : R \to S$, we say that R and S are isomorphic and write $R \cong S$.

Example

Show that complex conjugation is a ring isomorphism from $\mathbb{C}$ to itself.

Definition

Suppose that R and S are rings. We say that a map $\phi : R \to S$ is a ring homomorphism if the following hold.

1. $\phi(a+b) = \phi(a) + \phi(b)$.
2. $\phi(ab) = \phi(a)\phi(b)$.

Example

Define $f : \mathbb{Z} \to \mathbb{Z}_5$ by $f(x) = [x]$. Show that f is a homomorphism of rings.

Theorem

Suppose that $f : R \to S$ is a ring homomorphism. Then,

1. $f(0_R) = 0_S$.
2. $f(-a) = -f(a)$.
3. $f(a - b) = f(a) - f(b)$.
4. *If R is a ring with identity and f is surjective then S is a ring with identity and $f(1_R) = 1_S$.*
5. *If R, S and f are as above and $u \in R$ is a unit then $f(u)$ is a unit also and $f(u)^{-1} = f(u^{-1})$.*

Definition

Suppose that $f : R \to S$ is a function. We define the image of f as

$$\text{im}(f) = \{f(r) : r \in R\}.$$

Note

A function $f : R \to S$ is surjective (onto) if and only if $\text{im}(f) = S$.

Corollary

Suppose that $f : R \to S$ is a ring homomorphism. Then $im(f)$ is a subring of S.

Example

Are there isomorphisms from $\mathbb{Z}_{15}$ to $\mathbb{Z}_5 \times \mathbb{Z}_3$? Can you characterize all such maps?

Example

Show that there are no isomorphisms from R to S when R and S are chosen below.

1. $R = \mathbb{Z}$ and $S = \mathbb{Z}_6$.
2. $R = \mathbb{Z}_6$ and $S = \mathbb{Z}$.
3. $R = \mathbb{Z}_9$ and $S = \mathbb{Z}_3 \times \mathbb{Z}_3$.
4. $R = \mathbb{Q}$ and $S = \mathbb{Z}$.

Fact

Suppose that $R \cong S$. If R is commutative then so is S.