LECTURE 16

Homomorphisms and Isomorphisms of Rings

Having now seen a number of diverse examples of rings, it is appropriate at this point to see how two different sets might be endowed with essentially the same ring structure.

Consider a set R consisting of two elements a, b with the following addition and multiplication tables

$+$	a	b
a	a	b
b	b	a

$\times$	a	b
a	a	a
b	a	b

It is easy to verify that R has a structure of a commutative ring with identity if $0_R = a$ and $1_R = b$.

On the other hand, $\mathbb{Z}_2 = \{[0], [1]\}$ is another commutative ring with identity consisting of only two elements. If we write down the addition and multiplication tables for $\mathbb{Z}_2$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\times$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

we see that $\mathbb{Z}_2$ has about the same structure as that of R once we recognize the correspondences $a \leftrightarrow [0]$, $b \leftrightarrow [1]$. In such a case, when two sets R and S have a virtually identical ring structure, we shall say that R and S are *isomorphic*. Below we formalize this concept a little more precisely.

Recall that a map f from a set R to a set S is *injective* if

$$f(r) = f(r') \quad \Rightarrow \quad r = r' \quad .$$

$f : R \to S$ is *surjective* if every element in S can be expressed as $s = f(r)$ for some r in R. Finally, $f : R \to S$ is *bijective* if f is both injective and surjective. Finally, we recall that if f is bijective, then f has a inverse; i.e., there exists a (unique) function $f^{-1} : S \to R$ such that

$$f\left(f^{-1}(x)\right) = x = f^{-1}\left(f(x)\right) \quad \forall\, x \in R \quad .$$

DEFINITION 16.1. *A map $f : R \to S$ between two rings is a called a* ***homomorphism*** *if:*

(i) $f(r + r') = f(r) + f(r') \quad , \quad \forall\, r, r' \in R \quad ;$
(ii) $f(rr') = f(r)f(r') \quad , \quad \forall\, r, r' \in R \quad .$

f is said to be an ***isomorphism*** *if it is also bijective.*

Example 1. Consider the map $\sigma : \mathbb{C} \to \mathbb{C}$ where $\sigma(x + iy) = x - iy$ (i.e., σ is complex conjugation in $\mathbb{C}$). Then if $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$,

$$\begin{aligned} \sigma(z_1 + z_2) &= \sigma\left(x_1 + x_2 + i(y_1 + y_2)\right) \\ &= x_1 + x_2 - i(y_1 + y_2) \\ &= x_1 - iy_1 + x_2 - iy_2 \\ &= \sigma(z_1) + \sigma(z_2) \end{aligned} \tag{16.1}$$

$$\begin{aligned} \sigma(z_1z_2) &= \sigma\left(x_1x_2 - y_1y_2 + i(x_1y_2 + y_1x_2)\right) \\ &= x_1x_2 - y_1y_2 - i(x_1y_2 + y_1x_2) \\ &= (x_1 - iy_1)(x_2 - iy_2) \\ &= \sigma(z_1)\sigma(z_2) \end{aligned} \tag{16.2}$$

Thus, σ is a homomorphism of rings. Since

$$\sigma^2 = \sigma \circ \sigma = Identity \;\; map$$

it is clear that σ^{-1} exists, and so σ is a bijection. Thus, σ is a ring isomorphism.

THEOREM 16.2. *Let $f : R \to S$ be a homomorphism of rings. Then*

(i) $f(0_R) = 0_S$.
(ii) $f(-r) = -f(r)$ *for every* $r \in R$.

Moreover, if R and S have identities and f is an surjective homomorphism, then

(iii) $f(1_R) = 1_S$.
(iv) *Whenever $a \in R$ is a unit of R, then $f(a)$ is a unit of S and* $f(a)^{=1} = f\left(a^{-1}\right)$.

Proof.

(i) Since f is a homomorphism and $0_R + 0_R = 0_R$ in R,

$$f(0_R) + f(0_R) = f(0_R + 0_R) = f(0_R) \quad .$$

Adding $-f(0_R) \in S$ to both sides of this equation yields

$$f(0_R) = 0_S \quad .$$

(ii)

$$\begin{aligned} f(r) + f(-r) &= f\left(r + (-r)\right) \\ &= f(0_R) \\ &= 0_S \quad \text{by (i)} \end{aligned}$$

Hence f(-r) is the additive inverse of f(r) in S; i.e., $-f(r) = f(-r)$.

(iii) Since f is surjective, $1_S = f(r)$ for some $r \in R$. Therefore,

$$f(1_R) = f(1_R) \cdot 1_S = f(1_R) \cdot f(r) = f(1_R r) = f(r) \equiv 1_S \quad .$$

(iv) Suppose a is a unit in R with multiplicative inverse a^{-1}. Then by (iii)

$$1_S = f(1_R) = f\left(a^{-1}a\right) = f\left(a^{-1}\right) f(a)$$

and so $f(a)$ is a unit in S with multiplicative inverse $f\left(a^{-1}\right)$.

□

COROLLARY 16.3. *Let $f : R \to S$ be a ring homomorphism. Then the image of f in S*

$$image\,(f) = \{s \in S \mid s = f(r) \;\; \textit{for some}\; r \in R\}$$

is a subring of S.

Proof. From the fact that f is a ring homomorphism it follows that $image\,(f)$ is closed under addition and multiplication:

$$\begin{aligned} s, s' \in image\,(f) &\Rightarrow \exists\, r, r' \in R \quad s.t. \quad s = f(r) \;,\; s' = f(r') \\ &\Rightarrow s + s' = f(r) + f(r') = f(r + r') \in image\,(f) \end{aligned}$$

$$\begin{aligned} s, s' \quad &\in \quad image\,(f) \quad \Rightarrow \quad \exists\, r, r' \in R \quad s.t. \quad s = f\,(r)\ ,\ s' = f\,(r') \\ &\Rightarrow \qquad s \times s' = f\,(r) \times f\,(r') = f\,(r \times r') \in image\,(f) \end{aligned}$$

From part (ii) of the preceding theorem we have

$$s = f\,(r) \quad \text{for some } r \in R \quad \Rightarrow \quad -s = f\,(-r) \in image\,(f)$$

Since $image\,(f)$ is closed under addition, multiplication, and taking additive inverses, we have by Theorem 14.5, that $image(f)$ is a subring of S. $\square$