Definition 20.1

A *homomorphism* from a ring R to a ring S is a function $f\colon R \to S$ such that for any $a, b \in R$ we have

- $f(a+b) = f(a) + f(b)$
- $f(ab) = f(a) \cdot f(b)$

Note. Since a homomorphism of rings $f\colon R \to S$ is a homomorphism of their additive groups, thus we have $f(0) = 0$ and $f(-a) = -f(a)$ for any $a \in R$.

On the other hand if R and S are rings with unity, then it need not be true in general that $f(1) = 1$. Take for example $R = \mathbb{Z}$, $S = \mathbb{Z} \times \mathbb{Z}$, and let $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be given by $f(n) = (n, 0)$. Then f is a ring homomorphism, but $f(1) = (1, 0)$ which is not the unity in $\mathbb{Z} \times \mathbb{Z}$.

To avoid such situations, usually, when working with rings with unity, it is additionally assumed that homomorphisms preserve the unity, $f(1) = 1$.

Example. For $n > 1$ the function $f\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $f(k) = k \mod n$ is a ring homomorphism.

Example. Let R be a ring and let $a \in R$. The function $f\colon R[x] \to R$ defined by $f(p(x)) = p(a)$ is a homomorphism of rings.

Example. If R is a ring and $I \triangleright R$ then the function $q\colon R \to R/I$ given by $q(a) = a + I$ is a homomorphism of rings.

Definition 20.2

A *isomorphism* of rings is a homomorphism $f\colon R \to S$ which is a bijection.

If there exists an isomorphism between rings R and S then we say that these rings are *isomorphic* and we write $R \cong S$.

Theorem 20.3

If $f\colon R \to S$ is an isomorphism of rings then the inverse function $f^{-1}\colon S \to R$ is also an isomorphism of rings.

Proof. Exercise. □

Definition 20.4

Let $f\colon R \to S$ be a homomorphism of rings. The *image* of f is the set $\mathrm{Im}(f) \subseteq S$ defined by

$$\mathrm{Im}(f) = \{f(r) \mid r \in R\}$$

The *kernel* of f is the set $\mathrm{Ker}(f) \subseteq R$ given by

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

Theorem 20.5

Let $f\colon R \to S$ be homomorphism of rings. Then

1) $\mathrm{Im}(f)$ is a subring of S

2) $\mathrm{Ker}(f)$ is an ideal of R.

Proof.

1) Exercise.

2) One can check that $\mathrm{Ker}(f)$ is a subring of R (exercise). Also, if $a \in \mathrm{Ker}(f)$ and $r \in R$ then

$$f(ra) = f(r) \cdot f(a) = f(r) \cdot 0 = 0$$

so $ra \in \mathrm{Ker}(f)$. Similarly, $ar \in \mathrm{Ker}(f)$. This show that $Ker(f) \triangleleft R$. □

Theorem 20.6 (First Isomorphism Theorem for Rings)

Let $f\colon R \to S$ be a ring which is onto. Then $S \cong R/\mathrm{Ker}(f)$.

Proof. Define $g\colon R/\mathrm{Ker}(f) \to S$ by $g(a + \mathrm{Ker}(f)) = f(a)$. One can check that this is a well defined function, which gives an isomorphism of rings. □

Example. Recall that for $n > 1$ we have an onto homomorphism $f\colon \mathbb{Z} \to \mathbb{Z}_n$, $f(k) = k \bmod n$. Notice that

$$\mathrm{Ker}(f) = \{nk \mid k \in \mathbb{Z}\} = n\mathbb{Z}$$

This gives $\mathbb{Z}/n\mathbb{Z} \overset{\sim}{=} \mathbb{Z}_n$.

Example. Take the homomorphism $f\colon R[x] \to R$ defined by $f(p(x)) = p(0)$. This homomorphism of onto, since if $a \in R$ then $r = f(p(x))$ for the polynomial $p(x) = a$. We have

$$\begin{aligned}\mathrm{Ker}(f) &= \{p(x) \mid p(x) = 0\} \\ &= \{a_1x + \ldots + a_nx^n \mid a_i \in R, n \geq 0\} \\ &= xR[x]\end{aligned}$$

This shows that $R[x]/xR[x] \overset{\sim}{=} R$.

Theorem 20.7

If R is a ring and $I \triangleleft R$ then there exists a ring homomorphism $f\colon R \to S$ such that $\mathrm{Ker}(f) = I$.

Proof. Take $S = R/I$ and $f\colon R \to R/I$ defined by $f(a) = a + I$. □