Ring Homomorphisms

In analogy with group homomorphisms, we define a map $\varphi: R \rightarrow S$ between two rings $R$ and $S$ to be a **ring homomorphism** if it is operation-preserving with respect to both of the ring operations, i.e.,

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{and} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

A ring homomorphism which is also a bijection between the two rings is a **ring isomorphism**.

**Examples:**
The complex conjugation map $a + bi \mapsto a - bi$ is a ring isomorphism between $\mathbb{C}$ and itself (indeed, it is a **ring automorphism**)
The map from $\mathbb{Z}$ to $\mathbb{Z}_n$ given by $k \mapsto k \mod n$ is the natural homomorphism between these rings
Given some fixed real number $a$, the map from $\mathbb{R}[x]$ to $\mathbb{R}$ given by $p(x) \mapsto p(a)$ is a ring homomorphism
If $R$ is a commutative ring of characteristic 2, then the map $x \mapsto x^2$ is a ring homomorphism between $R$ and itself
Since every ring homomorphism $\varphi: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{30}$ is also an additive group homomorphism, we know it completely determined by the value of $\varphi(1)$; that is, $\varphi(x) = x \cdot \varphi(1)$, and as $0 = \varphi(0) = \varphi(12) = 12\varphi(1)$, $\varphi(1)$ must be a multiple of 5. But $\varphi(1) = \varphi(1^2) = \varphi(1)^2$ in
$\mathbb{Z}_{30}$, so this means $\varphi(1)$ can equal 0, 10, 15 or 25. Therefore, there are four such homomorphisms: the maps $\varphi(x) = 0$, $\varphi(x) = 10x$, $\varphi(x) = 15x$, and $\varphi(x) = 25x$.

**Theorem** Let $\varphi: R \to S$ be a ring homomorphism, and let $A$ be a subring of $R$ and $B$ an ideal of $S$.
1. For any $r \in R$ and positive integer $n$,
   \[ \varphi(nr) = n\varphi(r) \text{ and } \varphi(r^n) = \varphi(r)^n; \]
2. $\varphi(A)$ is a subring of $S$;
3. if $A$ is an ideal and $\varphi$ is onto, then $\varphi(A)$ is an ideal of $S$;
4. the pullback $\varphi^{-1}(B)$ is an ideal of $R$;
5. if $R$ is commutative, then $\varphi(R)$ is commutative;
6. if $R$ has unity element 1, $S$ is not trivial and $\varphi$ is onto, then $\varphi(1)$ is the unity element of $S$;
7. $\varphi$ is an isomorphism $\iff$ $\varphi$ is onto and $\text{Ker} \varphi$ is the trivial subring of $R$;
8. if $\varphi: R \to S$ is an isomorphism, then $\varphi^{-1}: S \to R$ is an isomorphism.

**Proof** Straightforward. //

**Theorem** Let $\varphi: R \to S$ be a ring homomorphism. Then $\text{Ker} \varphi$ is an ideal of $R$.

**Proof** Left as an exercise. //
The Fund Thm of Ring Homomorphisms

Let $\varphi: R \rightarrow S$ be a ring homomorphism. Then $R/\ker \varphi \cong \varphi(R)$ via the natural isomorphism $r \cdot \ker \varphi \mapsto \varphi(r)$.

Proof Also left as an exercise. //

Theorem Every ideal $A$ of the ring $R$ can be represented as the kernel of some homomorphism of $R$, namely the natural map $r \mapsto r + A$ from $R$ to $R/A$.

Proof Obvious. //

Theorem Let $R$ be a ring with unity element 1. Then the map $\varphi: \mathbb{Z} \rightarrow R$ given by $\varphi(n) = n \cdot 1$ is a ring homomorphism.

Proof Suppose first that $m$ and $n$ are nonnegative integers. Then

$$\varphi(m + n) = (m + n) \cdot 1 = \underbrace{(1 + 1 + \cdots + 1)}_{m + n \text{ terms}} =$$

$$\underbrace{(1 + 1 + \cdots + 1)}_{m \text{ terms}} + \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ terms}} = m \cdot 1 + n \cdot 1 = \varphi(m) + \varphi(n)$$
if \( m \) and \( n \) are both negative,

\[
\varphi(m + n) = (m + n) \cdot 1 \\
= (-m - n)(-1) \\
= (-m)(-1) + (-n)(-1) \\
= m \cdot 1 + n \cdot 1 \\
= \varphi(m) + \varphi(n)
\]

and if \( m \) is nonnegative and \( n \) is negative, then

\[
\varphi(m + n) = (m + n) \cdot 1 \\
= (m - |n|) \cdot 1 \\
= \overbrace{(1+1+\cdots+1)}^{m \text{ terms}} - \overbrace{(1+1+\cdots+1)}^{\text{|n| terms}} \\
= m \cdot 1 - |n| \cdot 1 \\
= m \cdot 1 + n \cdot 1 \\
= \varphi(m) + \varphi(n)
\]

So \( \varphi \) is addition-preserving.

To show that \( \varphi \) is multiplication-preserving, suppose that \( m \) is nonnegative. Then
\[ \varphi(mn) = (mn) \cdot 1 \]
\[ = \left( n + n + \cdots + n \right) \cdot 1 \]
\[ = n \cdot 1 + n \cdot 1 + \cdots + n \cdot 1 \]
\[ = \varphi(n) + \varphi(n) + \cdots + \varphi(n) \]
\[ = (m \cdot 1)\varphi(n) \]
\[ = \varphi(m)\varphi(n) \]

and if both \( m \) and \( n \) are negative, then
\[ \varphi(|m|) + \varphi(m) = \varphi(|m| + m) = \varphi(0) = 0 \]
\[ \Rightarrow \varphi(|m|) = -\varphi(m) \]

so
\[ \varphi(mn) = \varphi(|m| \cdot |n|) \]
\[ = \varphi(|m|)\varphi(|n|) \]
\[ = -\varphi(m) \cdot -\varphi(n) \]
\[ = (-1)^2 \varphi(m)\varphi(n) \]
\[ = \varphi(m)\varphi(n) \]

This completes the proof.  //
**Corollary** Every ring $R$ with unity element 1 contains a subring isomorphic to $\mathbb{Z}$ if char $R = 0$, and contains a subring isomorphic to $\mathbb{Z}_n$ if char $R = n > 0$.

**Proof** Let $S = \{k \cdot 1 \mid k \in \mathbb{Z}\}$. Then $S$ is the subring of $R$ equal to the image of $\mathbb{Z}$ under the homomorphism $\varphi: \mathbb{Z} \to R$ given by $\varphi(k) = k \cdot 1$. By the First Isomorphism Theorem then, $S \approx \mathbb{Z} / \ker \varphi$.

But if char $R = 0$, then $\ker \varphi$ is trivial, so $S \approx \mathbb{Z} / \ker \varphi = \mathbb{Z} / \{0\} \approx \mathbb{Z}$; if char $R = n$, then $\ker \varphi = n\mathbb{Z}$, so $S \approx \mathbb{Z} / \ker \varphi = \mathbb{Z} / n\mathbb{Z} \approx \mathbb{Z}_n$. //

**Corollary** For any positive integer $m$, the map $\varphi: \mathbb{Z} \to \mathbb{Z}_m$ given by $\varphi(n) = n \mod m$ is a ring homomorphism.

**Proof** In $\mathbb{Z}_m$, $n \cdot 1 = n \mod m$. //

**Corollary** If $F$ is a field of characteristic 0, then $F$ contains a field isomorphic to $\mathbb{Q}$, and if char $F = p$ is positive, then $F$ contains a field isomorphic to $\mathbb{Z}_p$.

**Proof** The case of positive characteristic has already been handled, so suppose char $F = 0$. Then $F$ contains a subring $S$ isomorphic to $\mathbb{Z}$. If
$T = \{ rs^{-1} \mid r, s \in S \text{ with } s \neq 0 \}$, then $T$ is also a subring of $F$ all of whose nonzero elements are units (why?) and which is isomorphic to $\mathbb{Q}$ (why?). //

These results can be viewed as indicating the primary importance of the rings $\mathbb{Z}$, $\mathbb{Z}_n$, and the fields $\mathbb{Z}_p$, and $\mathbb{Q}$. In particular, note that amongst these, $\mathbb{Z}$ is a subring of $\mathbb{Q}$. Indeed, $\mathbb{Q}$ is the set of all quotients of elements of $\mathbb{Z}$. This relationship can be generalized to any integral domain, as follows.

Let $D$ be an integral domain; then define the set $S = \{(a,b) \mid a, b \in D \text{ with } b \neq 0\}$ and consider the relation $\equiv$ on the set $S$ defined by

$$(a,b) \equiv (c,d) \iff ad = bc.$$ 

Then $\equiv$ is an equivalence relation (why?). Denote the equivalence class containing the pair $(a,b)$ by the symbol $a/b$ and let $F$ be the set of these equivalence classes.

We make $F$ into a ring by putting

$$a/b + c/d = (ad + bc)/bd \quad \text{and} \quad (a/b)(c/d) = ac/bd.$$ 

Why are these well-defined operations? First, note that if $b$ and $d$ are nonzero, then so is $bd$; that is,
these definitions, $F$ is closed under both operations. Now, if $a' / b' = a/b$ and $c' / d' = c/d$, then $a'b = ab'$ and $c'd = cd'$, so

$$(ad + bc)b'd' = (ab')dd' + bb'(cd')$$
$$= (a'b)dd' + bb'(c'd)$$
$$= (a'd' + b'c')bd$$

whence $(a' / b') + (c' / d') = (a / b) + (c / d)$; similarly, $(a'c')(bd) = (a'b)(c'd) = (ab')(cd') = (ac)(b'd')$ implies that $(a' / b')(c' / d') = (a / b)(c / d)$.

Note that $0/1 (= 0/b$ for any nonzero $b$ in $D$) is the zero element of $F$ and the additive inverse of $a/b$ is $-a/b$. If $D$ has unity element 1, then $1/1 (= b/b$ for any nonzero $b$ in $D$) is the unity element of $F$ and if $a/b$ is nonzero in $F$, then $a \neq 0$ in $D$, and the multiplicative inverse of $a/b$ is $b/a$. Thus, $F$ is a field, called the fraction field (or quotient field) of $D$.

**Theorem** Every integral domain $D$ has a fraction field $F$ containing a subring isomorphic to $D$.

**Proof** The map $\varphi: D \rightarrow F$ given by $\varphi(a) = a / 1$ is an isomorphism between $D$ and its image in $F$. //

**Example:** The integral domain $\mathbb{Q}[x]$ has as fraction field the set of rational expressions $p(x)/q(x)$ with nonzero denominator, which we denote by $\mathbb{Q}(x)$.