Chapter 3

Ideals, Homomorphisms and Factor Rings

3.1 Ring Homomorphisms and Ideals

In this section we develop some more of the abstract theory of rings. In particular we will describe those functions between rings that preserve the ring structure, and we will look at another way of forming new rings from existing ones.

Definition 3.1.1 *Let R be a ring. A non-empty subset S of R is a* subring *of R if it is itself a ring under the addition and multiplication of R.*

This means that S is closed under the addition and multiplication of R, that it contains the zero element of R, and that it contains the negative of each of its elements.

EXAMPLES

1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.
   $\mathbb{Q}$ is a subring of $\mathbb{R}$.
   $\mathbb{R}$ is a subring of $\mathbb{C}$.

2. The ring $M_n(F)$ of $n \times n$ matrices over a field F has the following subrings :

   - $D_n(F)$ - the ring of *diagonal* $n \times n$ matrices over F.
   - $U_n(F)$ - the ring of *upper triangular* $n \times n$ matrices over F.

3. For any field F, F is a subring of the polynomial ring $M_n(F)$. So also is $F[x^2]$, the subset of $F[x]$ consisting of those polynomials in which the coefficient of x^i is zero whenever i is odd.

4. Every (non-zero) ring R has at least two subrings - the full ring R and the zero subring $\{0_R\}$

QUESTIONS FOR THE SEMINAR:

1. Give two more examples of subrings of $M_n(\mathbb{Q})$.
2. Suppose that S is a subring of a ring R. Is it possible that S could have an identity element for multiplication that is different from the identity element of R?
   Could this happen if R is an integral domain?

Definition 3.1.2 *Let R and S be rings. A function $\phi : R \longrightarrow S$ is a* ring homomorphism *if for all $x, y \in R$ we have*

$$\phi(x+y) = \phi(x) + \phi(y)$$

and

$$\phi(xy) = \phi(x)\phi(y).$$

EXAMPLES

1. Choose a positive integer n and define $\phi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ to be the function that sends $k \in \mathbb{Z}$ to the congruence class modulo n to which k belongs. Then ϕ_n is a ring homomorphism.
2. Let F be a field. If $a \in F$ we can define a homomorphism

   $$\phi_a : F[x] \longrightarrow F$$

   given by $\phi_a(f(x)) = f(a)$ for $f(x) \in F[x]$.

QUESTION FOR THE SEMINAR: Determine whether each of the following is a ring homomorphism :

1. The function $\det : M_2(\mathbb{Q}) \longrightarrow \mathbb{Q}$ that associates to every matrix its determinant.
2. The function $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $g(n) = 2n$, for $n \in \mathbb{Z}$.
3. The function $\phi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}$ defined for $f(x) \in \mathbb{Q}[x]$ by

   $$\phi(f(x)) = \text{the sum of the coefficients of } f(x).$$

Definition 3.1.3 *Suppose that* $\phi : R \longrightarrow S$ *is a homomorphism of rings. The* kernel *of* ϕ *is the subset of* R *defined by*

$$\ker\phi = \{r \in R : \phi(r) = 0_S\}.$$

The image *of* ϕ *is the subset of* S *defined by*

$$\mathrm{Im}\phi = \{s \in S : s = \phi(r) \text{ for some } r \in R\}.$$

Lemma 3.1.4 $\mathrm{Im}\phi$ *is a subring of* S*.*

Proof: First we need to show that $\mathrm{Im}\phi$ is closed under the addition and multiplication of S. So suppose that $s_1,\ s_2$ are elements of $\mathrm{Im}\phi$ and let $r_1,\ r_2$ be elements of R for which $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$. Then

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = s_1 + s_2$$

and so $s_1 + s_2 \in \mathrm{Im}\phi$. Also

$$\phi(r_1 r_2) = \phi(r_1)\phi(r_2) = s_1 s_2$$

and so $s_1 s_2 \in \mathrm{Im}\phi$.
Next we show that $0_S \in \mathrm{Im}\phi$. To see this observe that

$$\phi(0_R) + \phi(0_r) = \phi(0_R + 0_R) = \phi(0_R).$$

Subtracting the element $\phi(0_R)$ of S from both sides gives

$$\phi(0_R) = 0_S.$$

Thus $0_S \in \mathrm{Im}\phi$ - in fact we have proved something more than this, namely that 0_S is the image of 0_R.
Finally we show that $\mathrm{Im}\phi$ contains the additive inverse in S of each of its elements. Let $s \in \mathrm{Im}\phi$ and let r be an element of R for which $\phi(r) = s$. Then

$$\phi(-r) + \phi(r) = \phi(0_R) = 0_S.$$

Thus $\phi(-r)$ is the additive inverse of s in S, i.e. $-s = \phi(-r)$ and $\mathrm{Im}\phi$ contains the negative of each of its elements. □

Lemma 3.1.5 $\ker\phi$ *is a subring of* R.

Proof: Let $r_1, r_2 \in \ker\phi$. Then $\phi(r_1) = \phi(r_2) = 0_S$. We have

$$\begin{aligned} \phi(r_1 + r_2) &= \phi(r_1) + \phi(r_2) = 0_S + 0_S = 0_S, \\ \text{and } \phi(r_1 r_2) &= \phi(r_1)\phi(r_2) = 0_S 0_S = 0_S. \end{aligned}$$

Thus $\ker\phi$ is closed under addition and multiplication in R.
To see that $0_R \in \ker\phi$ we note that $\phi(0_R) = 0_S$ by the proof of Lemma 3.1.4 above. Finally if $r \in \ker\phi$ then

$$0_S = \phi(-r + r) = \phi(-r) + \phi(r) = \phi(-r) + 0_S$$

and so $\phi(-r) = 0$ and $-r \in \ker\phi$. Thus $\ker\phi$ is a subring of R. □

In fact $\ker\phi$ is not just a subring of R - it has an extra property. Suppose $r \in \ker\phi$ and let x be any element of R. Then xr and rx belong to $\ker\phi$, since

$$\begin{aligned} \phi(xr) &= \phi(x)\phi(r) = \phi(x)0_S = 0_S, \\ \phi(rx) &= \phi(r)\phi(x) = 0_S\phi(x) = 0_S. \end{aligned}$$

So not only is $\ker\phi$ closed under its own multiplication, it is also closed under the operation of multiplying an element of $\ker\phi$ by any element of R.

Definition 3.1.6 *Let* R *be a ring.*
A left ideal *of* R *is a subring* I_L *of* R *with the additional property that* $xa \in I_L$ *whenever* $a \in I_L$ *and* $x \in R$.
A right ideal *of* R *is a subring* I_R *of* R *with the additional property that* $ax \in I_R$ *whenever* $a \in I_R$ *and* $x \in R$.
A two-sided ideal *of* R *is a subring* I *of* R *with the additional property that both* xa *and* ax *are in* I *whenever* $a \in I$ *and* $x \in R$.

QUESTION FOR THE SEMINAR: Find some examples of left, right, or two-sided ideals in each of the following rings :

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{Q}[x],\ \mathbb{Z}[x],\ M_2(\mathbb{Q}).$$

NOTES

1. If R is commutative then every left or right ideal of R is a two-sided ideal. We do not talk about two-sided ideals in this case, just ideals.
2. (Two-sided) ideals play a role in ring theory similar to that played by normal subgroups in group theory.

EXAMPLES

1. Let R be a ring. We have already seen that the kernel of any ring homomorphism with domain R is a (two-sided) ideal of R.

2. The subrings

$$\begin{aligned} 2\mathbb{Z} &= \{\dots, -2, 0, 2, 4, \dots\} \\ 3\mathbb{Z} &= \{\dots, -3, 0, 3, 6, \dots\} \end{aligned}$$

   are ideals of $\mathbb{Z}$. In general if $n \in \mathbb{Z}$ we will denote by $n\mathbb{Z}$ or $\langle n \rangle$ the subring of $\mathbb{Z}$ consisting of all the integer multiples of n. In each case $\langle n \rangle$ is an ideal of $\mathbb{Z}$, since a multiple of n can be multiplied by *any* integer and the result is always a multiple of n.

   Note that $\langle n \rangle$ is the kernel of the homomorphism $\phi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ that sends $k \in \mathbb{Z}$ to the class of k modulo n.

3. Fix a polynomial $f(x) \in \mathbb{Q}[x]$. We denote by $\langle f(x) \rangle$ the subring of $\mathbb{Q}[x]$ consisting of all those polynomials of the form $g(x)f(x)$ for an element $g(x)$ of $\mathbb{Q}[x]$. Then $\langle f(x) \rangle$ is an ideal of $\mathbb{Q}[x]$, called the principal ideal generated by $f(x)$.

4. Let R be any ring and let $a \in R$. We define

$$Ra = \{ra : r \in R\}.$$

   Then Ra is a left ideal of R called the principal left ideal generated by a. Similarly $aR = \{ar : r \in R\}$ is the principal right ideal generated by a.
   If R is commutative then $aR = Ra$ for all $a \in R$, and this ideal is called the *principal ideal* generated by a. It is denoted by $\langle a \rangle$. In $\mathbb{Z}$, $n\mathbb{Z}$ is the principal ideal generated by n.
   In general an ideal in a commutative ring is called *principal* if it is the principal ideal generated by some element.

5. Every non-zero ring R has at least two ideals, namely the full ring R and the zero ideal $\{0_R\}$.

Lemma 3.1.7 *Let R be a ring, and let I be an ideal of R. If I contains a unit u of R, then $I = R$.*

Proof: Let u^{-1} denote the inverse of u in R. Then $u \in I$ implies $u^{-1}u = 1_R$ belongs to I. Now let $r \in R$. Then $r1_R = r$ belongs to I, so $R \subseteq I$ and $R = I$. □

Corollary 3.1.8 *If F is a field, then the only ideals in F are the zero ideal (consisting only of the zero element) and F itself.*