

30.12 Definition Let a map $\phi : R \rightarrow R'$ be a homomorphism of rings. The subring

$$\phi^{-1}[0'] = \{r \in R \mid \phi(r) = 0'\}$$

is the **kernel** of ϕ , denoted by $\text{Ker}(\phi)$. ■

If we forget about the multiplicative part of a ring, we see that the kernel of a ring homomorphism is the same as the kernel of the underlying group homomorphism. Any property of a group homomorphism must also hold for a ring homomorphism.

30.13 Theorem **Analogue of Theorem 10.17** Let $\phi : R_1 \rightarrow R_2$ be a ring homomorphism. The elements $a, b \in R_1$ are in the same additive coset of $\text{Ker}(\phi)$ if and only if $\phi(a) = \phi(b)$. ◆

30.14 Theorem **Analogue of Corollary 10.19** A ring homomorphism $\phi : R_1 \rightarrow R_2$ is one-to-one if and only if $\text{Ker}(\phi) = \{0\}$. ◆

The kernel of a group homomorphism $\phi : G_1 \rightarrow G_2$ is a normal subgroup of G_1 and normality is what is needed in order to construct a factor group from a subgroup. The situation is similar in rings. We need a subring to be an ideal in order to construct a factor ring. The following theorem states that in fact the kernel of a ring homomorphism is an ideal.

30.15 Theorem Let $\phi : R_1 \rightarrow R_2$ be a ring homomorphism. Then $\text{Ker}(\phi)$ is an ideal in R_1 .

Proof Since $\{0\} \subset R_2$ is an ideal in R_2 , $\text{Ker}(\phi) = \phi^{-1}[\{0\}]$ is an ideal in R_1 by Property 7 of Theorem 30.11. ◆

Fundamental Homomorphism Theorem

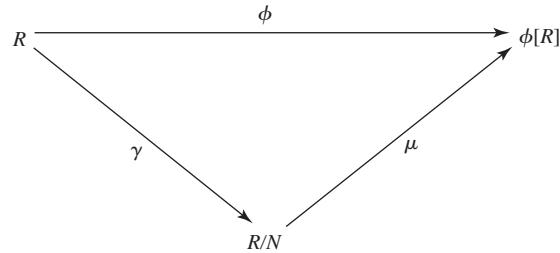
To complete our analogy with groups, we give the analogues of Theorems 12.12 and 12.14.

30.16 Theorem **(Analogue of Theorem 12.12)** Let N be an ideal of a ring R . Then $\gamma : R \rightarrow R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with kernel N .

Proof The additive part is done in Theorem 12.12. Turning to the multiplicative question, we see that

$$\gamma(xy) = (xy) + N = (x + N)(y + N) = \gamma(x)\gamma(y). \quad \diamond$$

30.17 Theorem **(Fundamental Homomorphism Theorem; Analogue of Theorem 12.14)** Let $\phi : R \rightarrow R'$ be a ring homomorphism with kernel N . Then $\phi[R]$ is a ring, and the map $\mu : R/N \rightarrow \phi[R]$ given by $\mu(x + N) = \phi(x)$ is an isomorphism. If $\gamma : R \rightarrow R/N$ is the homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$, we have $\phi(x) = \mu \circ \gamma(x)$.



30.18 Figure

Proof This follows at once from Theorems 30.15 and 30.16. Figure 30.18 is the analogue of Fig. 12.15. \blacklozenge

30.19 Example Example 30.3 shows that $n\mathbb{Z}$ is an ideal of \mathbb{Z} , so we can form the factor ring $\mathbb{Z}/n\mathbb{Z}$. Example 22.11 shows that $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ where $\phi(m)$ is the remainder of m modulo n is a homomorphism, and we see that $\text{Ker}(\phi) = n\mathbb{Z}$. Theorem 30.17 then shows that the map $\mu : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$ where $\mu(m + n\mathbb{Z})$ is the remainder of m modulo n is well defined and is an isomorphism. \blacktriangle

30.20 Example Continuing Example 30.5, let F be the ring of all functions mapping \mathbb{R} into \mathbb{R} and let N be the subset of F consisting of all functions f with $f(2) = 0$. The set N is an ideal in F , so F/N is a ring. Furthermore, N is the kernel of the evaluation homomorphism $\phi_2 : F \rightarrow \mathbb{R}$ defined by $\phi_2(f) = f(2)$. Since ϕ_2 maps onto \mathbb{R} , F/N is isomorphic with \mathbb{R} by Theorem 30.17. The function $\mu : F/N \rightarrow \mathbb{R}$ given by $\mu(f) = f(2)$ is an isomorphism. \blacktriangle

In summary, every ring homomorphism with domain R gives rise to a factor ring R/N , and every factor ring R/N gives rise to a homomorphism mapping R into R/N . An *ideal* in ring theory is analogous to a *normal subgroup* in the group theory. Both are the type of substructure needed to form a factor structure.

■ EXERCISES 30

Computations

1. Describe all ring homomorphisms of $\mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$. [Hint: Note that if ϕ is such a homomorphism, then $\phi((1, 0)) = \phi((1, 0))\phi((1, 0))$ and $\phi((0, 1)) = \phi((0, 1))\phi((0, 1))$. Consider also $\phi((1, 0)(0, 1))$.]
2. Find all positive integers n such that \mathbb{Z}_n contains a subring isomorphic to \mathbb{Z}_2 .
3. Find all ideals N of \mathbb{Z}_{12} . In each case compute \mathbb{Z}_{12}/N ; that is, find a known ring to which the quotient ring is isomorphic.
4. Give addition and multiplication tables for $2\mathbb{Z}/8\mathbb{Z}$. Are $2\mathbb{Z}/8\mathbb{Z}$ and \mathbb{Z}_4 isomorphic rings?

Concepts

In Exercises 5 through 7, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

5. An *isomorphism* of a ring R with a ring R' is a homomorphism $\phi : R \rightarrow R'$ such that $\text{Ker}(\phi) = \{0\}$.
6. An *ideal* N of a ring R is an additive subgroup of $\langle R, + \rangle$ such that for all $r \in R$ and all $n \in N$, we have $rn \in N$ and $nr \in N$.
7. The *kernel* of a homomorphism ϕ mapping a ring R into a ring R' is $\{\phi(r) = 0' \mid r \in R\}$.
8. Let F be the ring of all functions mapping \mathbb{R} into \mathbb{R} and having derivatives of all orders. Differentiation gives a map $\delta : F \rightarrow F$ where $\delta(f(x)) = f'(x)$. Is δ a homomorphism? Why? Give the connection between this exercise and Example 30.4.
9. Give an example of a ring homomorphism $\phi : R \rightarrow R'$ where R has unity 1 and $\phi(1) \neq 0'$, but $\phi(1)$ is not unity for R' .
10. Determine whether each of the following is true or false.
 - a. The concept of a ring homomorphism is closely connected with the idea of a factor ring.
 - b. A ring homomorphism $\phi : R \rightarrow R'$ carries ideals of R into ideals of R' .
 - c. A ring homomorphism is one-to-one if and only if the kernel is $\{0\}$.
 - d. \mathbb{Q} is an ideal in \mathbb{R} .

- e. Every ideal in a ring is a subring of the ring.
 - f. Every subring of every ring is an ideal of the ring.
 - g. Every quotient ring of every commutative ring is again a commutative ring.
 - h. The rings $\mathbb{Z}/4\mathbb{Z}$ and \mathbb{Z}_4 are isomorphic.
 - i. An ideal N in a ring R with unity 1 is all of R if and only if $1 \in N$.
 - j. The concept of an ideal is to the concept of a ring as the concept of a normal subgroup is to the concept of a group.
11. Let R be a ring. Observe that $\{0\}$ and R are both ideals of R . Are the factor rings R/R and $R/\{0\}$ of real interest? Why?
12. Give an example to show that a factor ring of an integral domain may be a field.
13. Give an example to show that a factor ring of an integral domain may have divisors of 0.
14. Give an example to show that a factor ring of a ring with divisors of 0 may be an integral domain.
15. Find a subring of the ring $\mathbb{Z} \times \mathbb{Z}$ that is not an ideal of $\mathbb{Z} \times \mathbb{Z}$.
16. A student is asked to prove that a quotient ring of a ring R modulo an ideal N is commutative if and only if $(rs - sr) \in N$ for all $r, s \in R$. The student starts out:
Assume R/N is commutative. Then $rs = sr$ for all $r, s \in R/N$.
- a. Why does the instructor reading this expect an incorrect proof?
 - b. What should the student have written?
 - c. Prove the assertion. (Note the “if and only if.”)

Theory

17. Let $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and let R' consist of all 2×2 matrices of the form $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{Z}$. Show that R is a subring of \mathbb{R} and that R' is a subring of $M_2(\mathbb{Z})$. Then show that $\phi : R \rightarrow R'$, where $\phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ is an isomorphism.
18. Show that each homomorphism from a field to a ring is either one-to-one or maps everything onto 0.
19. Show that if R, R' , and R'' are rings, and if $\phi : R \rightarrow R'$ and $\psi : R' \rightarrow R''$ are homomorphisms, then the composite function $\psi\phi : R \rightarrow R''$ is a homomorphism. (See Exercise 39 of Section 8.)
20. Let R be a commutative ring with unity of prime characteristic p . Show that the map $\phi_p : R \rightarrow R$ given by $\phi_p(a) = a^p$ is a homomorphism (the **Frobenius homomorphism**).
21. Let R and R' be rings and let $\phi : R \rightarrow R'$ be a ring homomorphism such that $\phi[R] \neq \{0'\}$. Show that if R has unity 1 and R' has no 0 divisors, then $\phi(1)$ is unity for R' .
22. Let $\phi : R \rightarrow R'$ be a ring homomorphism and let N be an ideal of R .
- a. Show that $\phi[N]$ is an ideal of $\phi[R]$.
 - b. Give an example to show that $\phi[N]$ need not be an ideal of R' .
 - c. Let N' be an ideal either of $\phi[R]$ or of R' . Show that $\phi^{-1}[N']$ is an ideal of R .
23. Let F be a field, and let S be any subset of $F \times F \times \cdots \times F$ for n factors. Show that the set N_S of all $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ that have every element (a_1, \dots, a_n) of S as a zero (see Exercise 28 of Section 27) is an ideal in $F[x_1, \dots, x_n]$. This is of importance in algebraic geometry.
24. Show that a factor ring of a field is either the trivial (zero) ring of one element or is isomorphic to the field.
25. Show that if R is a ring with unity and N is an ideal of R such that $N \neq R$, then R/N is a ring with unity.
26. Let R be a commutative ring and let $a \in R$. Show that $I_a = \{x \in R \mid ax = 0\}$ is an ideal of R .
27. Show that an intersection of ideals of a ring R is again an ideal of R .
28. Let R and R' be rings and let N and N' be ideals of R and R' , respectively. Let ϕ be a homomorphism of R into R' . Show that ϕ induces a natural homomorphism $\phi_* : R/N \rightarrow R'/N'$ if $\phi[N] \subseteq N'$. (Use Exercise 41 of Section 12.)

29. Let ϕ be a homomorphism of a ring R with unity onto a nonzero ring R' . Let u be a unit in R . Show that $\phi(u)$ is a unit in R' .
30. An element a of a ring R is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that the collection of all nilpotent elements in a commutative ring R is an ideal, the **nilradical of R** .
31. Referring to the definition given in Exercise 30, find the nilradical of the ring \mathbb{Z}_{12} and observe that it is one of the ideals of \mathbb{Z}_{12} found in Exercise 3. What is the nilradical of \mathbb{Z} ? of \mathbb{Z}_{32} ?
32. Referring to Exercise 30, show that if N is the nilradical of a commutative ring R , then R/N has as nilradical the trivial ideal $\{0 + N\}$.
33. Let R be a commutative ring and N an ideal of R . Referring to Exercise 30, show that if every element of N is nilpotent and the nilradical of R/N is R/N , then the nilradical of R is R .
34. Let R be a commutative ring and N an ideal of R . Show that the set \sqrt{N} of all $a \in R$, such that $a^n \in N$ for some $n \in \mathbb{Z}^+$, is an ideal of R , the **radical of N** .
35. Referring to Exercise 34, show by examples that for proper ideals N of a commutative ring R ,
- a. \sqrt{N} need not equal N
 - b. \sqrt{N} may equal N .
36. What is the relationship of the ideal \sqrt{N} of Exercise 34 to the nilradical of R/N (see Exercise 30)? Word your answer carefully.
37. Show that $\phi : \mathbb{C} \rightarrow M_2(\mathbb{R})$ given by

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

for $a, b \in \mathbb{R}$ gives an isomorphism of \mathbb{C} with the subring $\phi[\mathbb{C}]$ of $M_2(\mathbb{R})$.

SECTION 31

PRIME AND MAXIMAL IDEALS

Exercises 12 through 14 of the preceding section asked us to provide examples of factor rings R/N where R and R/N have very different structural properties. We start with some examples of this situation, and in the process, provide solutions to those exercises.

31.1 Example As was shown in Corollary 23.5, the ring \mathbb{Z}_p , which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, is a field for p a prime. *Thus a factor ring of an integral domain may be a field.* ▲

31.2 Example The ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain, for

$$(0, 1)(1, 0) = (0, 0),$$

showing that $(0, 1)$ and $(1, 0)$ are 0 divisors. Let $N = \{(0, n) \mid n \in \mathbb{Z}\}$. Now N is an ideal of $\mathbb{Z} \times \mathbb{Z}$, and $(\mathbb{Z} \times \mathbb{Z})/N$ is isomorphic to \mathbb{Z} under the correspondence $[(m, 0) + N] \leftrightarrow m$, where $m \in \mathbb{Z}$. Thus a factor ring of a ring may be an integral domain, even though the original ring is not. ▲

31.3 Example The subset $N = \{0, 3\}$ of \mathbb{Z}_6 is easily seen to be an ideal of \mathbb{Z}_6 , and \mathbb{Z}_6/N has three elements, $0 + N$, $1 + N$, and $2 + N$. These add and multiply in such a fashion as to show that $\mathbb{Z}_6/N \cong \mathbb{Z}_3$ under the correspondence

$$(0 + N) \leftrightarrow 0, \quad (1 + N) \leftrightarrow 1, \quad (2 + N) \leftrightarrow 2.$$

This example shows that *if R is not even an integral domain, that is, if R has zero divisors, it is still possible for R/N to be a field.* ▲

31.4 Example Note that \mathbb{Z} is an integral domain, but $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$ is not. The preceding examples showed that a factor ring may have a structure that seems *better* than the original ring.