15 Chapter

Definition 15.1. *Ring Homomorphism, Ring Isomorphism*
A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

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

A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

EXAMPLE 1 For any positive integer n, the mapping $k \to k \mod n$ is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$ (see Exercise 9 in Chapter 0). This mapping is called the *natural homomorphism* from $\mathbb{Z}$ to $\mathbb{Z}_n$.
EXAMPLE 2 The mapping $a + bi \to a - bi$ is a ring isomorphism from the complex numbers onto the complex numbers (see Exercise 37 in Chapter 6).
EXAMPLE 4 The correspondence $\phi : x \to 5x$ from $\mathbb{Z}_4$ to $\mathbb{Z}_{10}$ is a ring homomorphism. Although showing that $\phi(x+y) = \phi(x) + \phi(y)$ appears to be accomplished by the simple statement that $5(x+y) = 5x + 5y$, we must bear in mind that the addition on the left is done modulo 4, whereas the addition on the right and the multiplication on both sides are done modulo 10. An analogous difficulty arises in showing that ϕ preserves multiplication. So, to verify that ϕ preserves both operations, we write $x + y = 4q_1 + r_1$ and $xy = 4q_2 + r_2$, where $0 \le r_1 < 4$ and $0 \le r_2 < 4$. Then $\phi(x+y) = \phi(r_1) = 5r_1 = 5(x + y|4q_1) = 5x + 5y - 20q_1 = 5x + 5y = \phi(x) + \phi(y)$ in $\mathbb{Z}_{10}$ Similarly, using the fact that $5 \cdot 5 = 5$ in $\mathbb{Z}_10$, we have $\phi(xy) = \phi(r_2) = 5r_2 = 5(xy - 4q_2) = 5xy - 20q_2 = (5 \cdot 5)xy = 5x5y = \phi(x)\phi(y)$ in $\mathbb{Z}_{10}$.
EXAMPLE 5 We determine all ring homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_30$. By Example 10 in Chapter 10, the only group homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$ are $x \to ax$, where $a = 0, 15, 10, 20, 5,$ or 25. But, since $1 \cdot 1 = 1$ in $\mathbb{Z}_{12}$ we must have $a \cdot a = a$ in $\mathbb{Z}_{30}$. This requirement rules out 20 and 5 as possibilities for a. Finally, simple calculations show that each of the remaining four choices does yield a ring homomorphism.
EXAMPLE 6 Let R be a commutative ring of characteristic 2. Then the mapping $a \to a^2$ is a ring homomorphism from R to R.
EXAMPLE 7 Although $2\mathbb{Z}$, the group of even integers under addition, is group-isomorphic to the group $\mathbb{Z}$ under addition, the ring $2\mathbb{Z}$ is not ring- isomorphic to the ring $\mathbb{Z}$. (Quick! What does $\mathbb{Z}$ have that $2\mathbb{Z}$ doesn't?) I
EXAMPLE 8 Test for Divisibility by 9 An integer n with decimal representation akakil - - - a0 is divisible by 9 if and only if ak + ak71 + - - - + a0 is divisible by 9. To verify this, observe that n = aklOk + akillOk'1 + - - - + a0. Then, letting a denote the natural homomorphism from to Z9 [in particular, a(10) = l], we note that n is divisible by 9 if and only if
0 = a(n) = a(ak)(a(10))k + a(ak71)(oz(10))k'1 + - - ' + a(a0) = a(ak) + a(ak71) + - - - + oz(ao) = (1(ka + ak71+ - - - + do).
But a(ak + ak71+ - - - + a0) = 0is equivalent to ak + ak71+- - - + a0 being divisible by 9. I
EXAMPLE 9 Theorem of Gersonides
In 1844 Eugene Charles Catalan conjectured that 2^3 and 3^2 is the only instance of two consecutive powers greater than 1 of natural numbers. That is, they are the only solution in the natural numbers of $x^m - y^n = 1$ where $m, n, x, y > 1$. This conjecture was proved in 2002 by Preda Mihailescu. The special case where x and y are restricted to 2 and 3 was first proved by the Rabbi Gersonides in the fourteenth century who proved for $m, n > 1$ the only case when $2^m = 3^n \pm 1$ is for $(m, n) = (3, 2)$. To verify this is so for $2^m = 3^n + 1$, observe that for all n we have $3^n \mod 8 = 3$ or 1. Thus, $3^n + 1 \mod 8 = 4$ or 2. On the other hand, for $m > 2$, we have $2^m \mod 8 = 0$. To handle the case where $2^m = 3^n - 1$, we first note that for all n, $3^n \mod 16 = 3, 9, 11,$ or 1, depending on the value of $n \mod 4$. Thus, $(3^n - 1) \mod 16 = 2, 8, 10,$ or 0. Since $2^m \mod 16 = 0$ for $m \ge 4$, we have ruled out the cases Where $n \mod 4 = 1, 2,$ or 3. Because $3^{4k} \mod 5 = (3^4)^k \mod 5 = 1^k \mod 5 = 1$, we know that $(3^{4k} - 1) \mod 5 = 0$. But the only values for $2^m \mod 5$ are $2, 4, 3,$ and 1. This contradiction completes the proof.

Theorem 15.1. *Properties of Ring Homomorphisms*
Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.

1. *For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.*

2. *$\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.*

3. *If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.*

4. *$\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.*

5. *If R is commutative, then $\phi(R)$ is commutative.*

6. *If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.*

7. *ϕ is an isomorphism if and only if ϕ is onto and $\ker \phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.*

8. *If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.*

Theorem 15.2. *Kernels Are Ideals*
Let ϕ be a ring homomorphism from a ring R to a ring S. Then $\ker \phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem 15.3. *First Isomorphism Theorem for Rings*
Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\ker \phi$ to $\phi(R)$, given by $r + \ker \phi \to \phi(r)$, is an isomorphism. In symbols, $R/\ker \phi \approx \phi(R)$.

Theorem 15.4. *Ideals Are Kernels*
Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A.

EXAMPLE 10 Since the mapping ϕ from $\mathbb{Z}[x]$ onto $\mathbb{Z}$ given by $\phi(f(x)) = f(0)$ is a ring homomorphism with $\ker \phi = (x)$ (see Exercise 31 in Chapter 14), we have, by Theorem 15.3, $\mathbb{Z}[x]/\langle x \rangle \approx \mathbb{Z}$. And because $\mathbb{Z}$ is an integral domain but not a field, we know by Theorems 14.3 and 14.4 that the ideal $\langle x \rangle$ is prime but not maximal in $\mathbb{Z}[x]$.

Theorem 15.5. *Homomorphism from $\mathbb{Z}$ to a Ring with Unity*
Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

Corollary 15.6. *A Ring with Unity Contains $\mathbb{Z}_n$ or $\mathbb{Z}$*
If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 15.7. *$\mathbb{Z}_m$ Is a Homomorphic Image of $\mathbb{Z}$*
For any positive integer m, the mapping of $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \mod m$ is a ring homomorphism.

Corollary 15.8. *A Field Contains $\mathbb{Z}_p$ or $\mathbb{Q}$ (Steinitz, 1910)*
If F is a field of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$. If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers.

Theorem 15.9. *Field of Quotients*
Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.

EXAMPLE 11 Let $D = \mathbb{Z}[x]$. Then the field of quotients of D is $\{f(x)/g(x) \mid f(x), g(x) \in D\}$, where $g(x)$ is not the zero polynomial.
EXAMPLE 12 Let p be a prime. Then $\mathbb{Z}_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0\}$ is an infinite field of characteristic p.