(3) Let $R = \mathbb{Z}[x]$ be the ring of polynomials in x with integer coefficients. Let I be the collection of polynomials whose terms are of degree at least 2 (i.e., having no terms of degree 0 or degree 1) together with the zero polynomial. Then I is an ideal: the sum of two such polynomials again has terms of degree at least 2 and the product of a polynomial whose terms are of degree at least 2 with *any* polynomial again only has terms of degree at least 2. Two polynomials $p(x), q(x)$ are in the same coset of I if and only if they differ by a polynomial whose terms are of degree at least 2, i.e., if and only if $p(x)$ and $q(x)$ have the same constant and first degree terms. For example, the polynomials $3 + 5x + x^3 + x^5$ and $3 + 5x - x^4$ are in the same coset of I. It follows easily that a complete set of representatives for the quotient R/I is given by the polynomials $a + bx$ of degree at most 1.

Addition and multiplication in the quotient are again performed by representatives. For example,

$$(\overline{1+3x}) + (\overline{-4+5x}) = \overline{-3+8x}$$

and

$$(\overline{1+3x})(\overline{-4+5x}) = \overline{(-4-7x+15x^2)} = \overline{-4-7x}\,.$$

Note that in this quotient ring R/I we have $\overline{x}\,\overline{x} = \overline{x^2} = \overline{0}$, for example, so that R/I has zero divisors, even though $R = \mathbb{Z}[x]$ does not.

(4) Let A be a ring, let X be any nonempty set and let R be the ring of all functions from X to A. For each fixed $c \in X$ the map

$$E_c : R \to A \quad \text{defined by} \quad E_c(f) = f(c)$$

(called *evaluation at c*) is a ring homomorphism because the operations in R are pointwise addition and multiplication of functions. The kernel of E_c is given by $\{f \in R \mid f(c) = 0\}$ (the set of functions from X to A that vanish at c). Also, E_c is surjective: given any $a \in A$ the constant function $f(x) = a$ maps to a under evaluation at c. Thus $R/\ker E_c \cong A$.

Similarly, let X be the closed interval [0,1] in $\mathbb{R}$ and let R be the ring of all continuous real valued functions on [0,1]. For each $c \in [0, 1]$, evaluation at c is a surjective ring homomorphism (since R contains the constant functions) and so $R/\ker E_c \cong \mathbb{R}$. The kernel of E_c is the ideal of all continuous functions whose graph crosses the x-axis at c. More generally, the fiber of E_c above the real number y_0 is the set of all continuous functions that pass through the point (c, y_0).

(5) The map from the polynomial ring $R[x]$ to R defined by $p(x) \mapsto p(0)$ (evaluation at 0) is a ring homomorphism whose kernel is the set of all polynomials whose constant term is zero, i.e., $p(0) = 0$. We can compose this homomorphism with any homomorphism from R to another ring S to obtain a ring homomorphism from $R[x]$ to S. For example, let $R = \mathbb{Z}$ and consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ defined by the composition $p(x) \mapsto p(0) \mapsto p(0) \bmod 2 \in \mathbb{Z}/2\mathbb{Z}$. The kernel of this composite map is given by $\{p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$, i.e., the set of all polynomials with integer coefficients whose constant term is even. The other fiber of this homomorphism is the coset of polynomials whose constant term is odd, as we determined earlier. Since the homomorphism is clearly surjective, the quotient ring is $\mathbb{Z}/2\mathbb{Z}$.

(6) Fix some $n \in \mathbb{Z}$ with $n \geq 2$ and consider the noncommutative ring $M_n(R)$. If J is any ideal of R then $M_n(J)$, the $n \times n$ matrices whose entries come from J, is a two-sided ideal of $M_n(R)$. This ideal is the kernel of the surjective homomorphism $M_n(R) \to M_n(R/J)$ which reduces each entry of a matrix mod J, i.e., which maps each entry a_{ij} to $\overline{a_{ij}}$ (here bar denotes passage to R/J). For instance, when $n = 3$ and $R = \mathbb{Z}$, the 3×3 matrices whose entries are all even is the two-sided ideal $M_3(2\mathbb{Z})$

of $M_3(\mathbb{Z})$ and the quotient $M_3(\mathbb{Z})/M_3(2\mathbb{Z})$ is isomorphic to $M_3(\mathbb{Z}/2\mathbb{Z})$. If the ring R has an identity then the exercises below show that every two-sided ideal of $M_n(R)$ is of the form $M_n(J)$ for some two-sided ideal J of R.

(7) Let R be a commutative ring with 1 and let $G = \{g_1, \ldots, g_n\}$ be a finite group. The map from the group ring RG to R defined by $\sum_{i=1}^n a_i g_i \mapsto \sum_{i=1}^n a_i$ is easily seen to be a homomorphism, called the *augmentation map* . The kernel of the augmentation map, the *augmentation ideal*, is the set of elements of RG whose coefficients sum to 0. For example, $g_i - g_j$ is an element of the augmentation ideal for all i, j. Since the augmentation map is surjective, the quotient ring is isomorphic to R.

Another ideal in RG is $\{\sum_{i=1}^n ag_i \mid a \in R\}$, i.e., the formal sums whose coefficients are all equal (equivalently, all R-multiples of the element $g_1 + \cdots + g_n$).

(8) Let R be a commutative ring with identity $1 \neq 0$ and let $n \in \mathbb{Z}$ with $n \geq 2$. We exhibit some one-sided ideals in the ring $M_n(R)$. For each $j \in \{1, 2, \ldots, n\}$ let L_j be the set of all $n \times n$ matrices in $M_n(R)$ with arbitrary entries in the j^{th} column and zeros in all other columns. It is clear that L_j is closed under subtraction. It follows directly from the definition of matrix multiplication that for any matrix $T \in M_n(R)$ and any $A \in L_j$ the product TA has zero entries in the i^{th} column for all $i \neq j$. This shows L_j is a *left ideal* of $M_n(R)$. Moreover, L_j is *not* a *right* ideal (hence is not a two-sided ideal). To see this, let E_{pq} be the matrix with 1 in the p^{th} row and q^{th} column and zeros elsewhere $(p, q \in \{1, \ldots, n\})$. Then $E_{1j} \in L_j$ but $E_{1j}E_{ji} = E_{1i} \notin L_j$ if $i \neq j$, so L_j is not closed under right multiplication by arbitrary ring elements. An analogous argument shows that if R_j is the set of all $n \times n$ matrices in $M_n(R)$ with arbitrary entries in the j^{th} row and zeros in all other rows, then R_j is a *right* ideal which is not a *left* ideal. These one-sided ideals will play an important role in Part VI.

Example: (The Reduction Homomorphism)

The canonical projection map from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ obtained by factoring out by the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is usually referred to as "reducing modulo n." The fact that this is a *ring homomorphism* has important consequences for elementary number theory. For example, suppose we are trying to solve the equation

$$x^2 + y^2 = 3z^2$$

in *integers* x, y and z (such problems are frequently referred to as *Diophantine equations* after Diophantus, who was one of the first to systematically examine the existence of *integer* solutions of equations). Suppose such integers exist. Observe first that we may assume x, y and z have no factors in common, since otherwise we could divide through this equation by the square of this common factor and obtain another set of integer solutions smaller than the initial ones. This equation simply states a relation between these elements in the *ring* $\mathbb{Z}$. As such, the same relation must also hold in any *quotient* ring as well. In particular, this relation must hold in $\mathbb{Z}/n\mathbb{Z}$ for any integer n. The choice $n = 4$ is particularly efficacious, for the following reason: the squares mod 4 are just $0^2, 1^2, 2^2, 3^2$, i.e., 0, 1 (mod 4). Reading the above equation mod 4 (that is, considering this equation in the quotient ring $\mathbb{Z}/4\mathbb{Z}$), we must have

$$\begin{Bmatrix} 0 \\ 1 \end{Bmatrix} + \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \equiv 3 \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \equiv \begin{Bmatrix} 0 \\ 3 \end{Bmatrix} \pmod 4$$

where the $\begin{Bmatrix} 0 \\ 1 \end{Bmatrix}$, for example, indicates that either a 0 or a 1 may be taken. Checking the few possibilities shows that we must take the 0 each time. This means that each

of x, y and z must be even integers (squares of the odd integers gave us 1 mod 4). But this contradicts the assumption of no common factors for these integers, and shows that this equation has *no solutions in nonzero integers.*

Note that even had solutions existed, this technique gives information about the possible residues of the solutions mod n (since we could just as well have examined the possibilities mod n as mod 4) and note that for each choice of n we have only a *finite* problem to solve because there are only finitely many residue classes mod n. Together with the Chinese Remainder Theorem (described in Section 6), we can then determine the possible solutions modulo very large integers, which greatly assists in finding them numerically (when they exist). We also observe that this technique has a number of limitations — for example, there are equations which have solutions modulo every integer, but which do not have integer solutions. An easy example (but extremely hard to verify that it does indeed have this property) is the equation

$$3x^3 + 4y^3 + 5z^3 = 0.$$

As a final example of this technique, we mention that the map from the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients to the ring $\mathbb{Z}/p\mathbb{Z}[x]$ of polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$ for a prime p given by *reducing the coefficients modulo p* is a ring homomorphism. This example of reduction will be used in Chapter 9 in trying to determine whether polynomials can be factored.

The following theorem gives the remaining Isomorphism Theorems for rings. Each of these may be proved as follows: first use the corresponding theorem from group theory to obtain an isomorphism of *additive groups* (or correspondence of groups, in the case of the Fourth Isomorphism Theorem) and then check that this group isomorphism (or correspondence, respectively) is a multiplicative map, and so defines a *ring* isomorphism. In each case the verification is immediate from the definition of multiplication in quotient rings. For example, the map that gives the isomorphism in (2) below is defined by $\varphi : r + I \mapsto r + J$. This map is multiplicative since $(r_1 + I)(r_2 + I) = r_1r_2 + I$ by the definition of the multiplication in the quotient ring R/I, and $r_1r_2 + I \mapsto r_1r_2 + J = (r_1 + J)(r_2 + J)$ by the definition of the multiplication in the quotient ring R/J, i.e., $\varphi(r_1r_2) = \varphi(r_1)\varphi(r_2)$. The proofs for the other parts of the theorem are similar.

Theorem 8. Let R be a ring.

(1) *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A,\ b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

(2) *(The Third Isomorphism Theorem for Rings)* Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(3) *(The Fourth or Lattice Isomorphism Theorem for Rings)* Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.