

2. Let  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  be an element of the polynomial ring  $R[x]$ . Prove that  $p(x)$  is a zero divisor in  $R[x]$  if and only if there is a nonzero  $b \in R$  such that  $bp(x) = 0$ . [Let  $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$  be a nonzero polynomial of minimal degree such that  $g(x)p(x) = 0$ . Show that  $b_m a_n = 0$  and so  $a_n g(x)$  is a polynomial of degree less than  $m$  that also gives 0 when multiplied by  $p(x)$ . Conclude that  $a_n g(x) = 0$ . Apply a similar argument to show by induction on  $i$  that  $a_{n-i} g(x) = 0$  for  $i = 0, 1, \dots, n$ , and show that this implies  $b_m p(x) = 0$ .]
3. Define the set  $R[[x]]$  of *formal power series* in the indeterminate  $x$  with coefficients from  $R$  to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

Define addition and multiplication of power series in the same way as for power series with real or complex coefficients i.e., extend polynomial addition and multiplication to power series as though they were “polynomials of infinite degree”:

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n \\ \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k b_{n-k} \right) x^n. \end{aligned}$$

(The term “formal” is used here to indicate that convergence is not considered, so that formal power series need not represent functions on  $R$ .)

- (a) Prove that  $R[[x]]$  is a commutative ring with 1.  
 (b) Show that  $1 - x$  is a unit in  $R[[x]]$  with inverse  $1 + x + x^2 + \cdots$ .  
 (c) Prove that  $\sum_{n=0}^{\infty} a_n x^n$  is a unit in  $R[[x]]$  if and only if  $a_0$  is a unit in  $R$ .
4. Prove that if  $R$  is an integral domain then the ring of formal power series  $R[[x]]$  is also an integral domain.
5. Let  $F$  be a field and define the ring  $F((x))$  of *formal Laurent series* with coefficients from  $F$  by

$$F((x)) = \left\{ \sum_{n \geq N}^{\infty} a_n x^n \mid a_n \in F \text{ and } N \in \mathbb{Z} \right\}.$$

(Every element of  $F((x))$  is a power series in  $x$  plus a polynomial in  $1/x$ , i.e., each element of  $F((x))$  has only a finite number of terms with negative powers of  $x$ .)

- (a) Prove that  $F((x))$  is a field.  
 (b) Define the map

$$v : F((x))^{\times} \rightarrow \mathbb{Z} \quad \text{by} \quad v\left(\sum_{n \geq N}^{\infty} a_n x^n\right) = N$$

where  $a_N$  is the first nonzero coefficient of the series (i.e.,  $N$  is the “order of zero or pole of the series at 0”). Prove that  $v$  is a discrete valuation on  $F((x))$  whose discrete valuation ring is  $F[[x]]$ , the ring of formal power series (cf. Exercise 26, Section 1).

6. Let  $S$  be a ring with identity  $1 \neq 0$ . Let  $n \in \mathbb{Z}^+$  and let  $A$  be an  $n \times n$  matrix with entries from  $S$  whose  $i, j$  entry is  $a_{ij}$ . Let  $E_{ij}$  be the element of  $M_n(S)$  whose  $i, j$  entry is 1 and whose other entries are all 0.

- (a) Prove that  $E_{ij}A$  is the matrix whose  $i^{\text{th}}$  row equals the  $j^{\text{th}}$  row of  $A$  and all other rows are zero.
- (b) Prove that  $AE_{ij}$  is the matrix whose  $j^{\text{th}}$  column equals the  $i^{\text{th}}$  column of  $A$  and all other columns are zero.
- (c) Deduce that  $E_{pq}AE_{rs}$  is the matrix whose  $p, s$  entry is  $a_{qr}$  and all other entries are zero.
7. Prove that the center of the ring  $M_n(R)$  is the set of scalar matrices (cf. Exercise 7, Section 1). [Use the preceding exercise.]
8. Let  $S$  be any ring and let  $n \geq 2$  be an integer. Prove that if  $A$  is any strictly upper triangular matrix in  $M_n(S)$  then  $A^n = 0$  (a strictly upper triangular matrix is one whose entries on and below the main diagonal are all zero).
9. Let  $\alpha = r + r^2 - 2s$  and  $\beta = -3r^2 + rs$  be the two elements of the integral group ring  $\mathbb{Z}D_8$  described in this section. Compute the following elements of  $\mathbb{Z}D_8$ :
- (a)  $\beta\alpha$ , (b)  $\alpha^2$ , (c)  $\alpha\beta - \beta\alpha$ , (d)  $\beta\alpha\beta$ .
10. Consider the following elements of the integral group ring  $\mathbb{Z}S_3$ :

$$\alpha = 3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3) \quad \text{and} \quad \beta = 6(1) + 2(2\ 3) - 7(1\ 3\ 2)$$

(where  $(1)$  is the identity of  $S_3$ ). Compute the following elements:

- (a)  $\alpha + \beta$ , (b)  $2\alpha - 3\beta$ , (c)  $\alpha\beta$ , (d)  $\beta\alpha$ , (e)  $\alpha^2$ .
11. Repeat the preceding exercise under the assumption that the coefficients of  $\alpha$  and  $\beta$  are in  $\mathbb{Z}/3\mathbb{Z}$  (i.e.,  $\alpha, \beta \in \mathbb{Z}/3\mathbb{Z}S_3$ ).
12. Let  $G = \{g_1, \dots, g_n\}$  be a finite group. Prove that the element  $N = g_1 + g_2 + \dots + g_n$  is in the center of the group ring  $RG$  (cf. Exercise 7, Section 1).
13. Let  $\mathcal{K} = \{k_1, \dots, k_m\}$  be a conjugacy class in the finite group  $G$ .
- (a) Prove that the element  $K = k_1 + \dots + k_m$  is in the center of the group ring  $RG$  (cf. Exercise 7, Section 1). [Check that  $g^{-1}Kg = K$  for all  $g \in G$ .]
- (b) Let  $\mathcal{K}_1, \dots, \mathcal{K}_r$  be the conjugacy classes of  $G$  and for each  $\mathcal{K}_i$  let  $K_i$  be the element of  $RG$  that is the sum of the members of  $\mathcal{K}_i$ . Prove that an element  $\alpha \in RG$  is in the center of  $RG$  if and only if  $\alpha = a_1K_1 + a_2K_2 + \dots + a_rK_r$  for some  $a_1, a_2, \dots, a_r \in R$ .

## 7.3 RING HOMOMORPHISMS AND QUOTIENT RINGS

A ring homomorphism is a map from one ring to another that respects the additive and multiplicative structures:

**Definition.** Let  $R$  and  $S$  be rings.

- (1) A *ring homomorphism* is a map  $\varphi : R \rightarrow S$  satisfying
- (i)  $\varphi(a + b) = \varphi(a) + \varphi(b)$  for all  $a, b \in R$  (so  $\varphi$  is a group homomorphism on the additive groups) and
- (ii)  $\varphi(ab) = \varphi(a)\varphi(b)$  for all  $a, b \in R$ .
- (2) The *kernel* of the ring homomorphism  $\varphi$ , denoted  $\ker \varphi$ , is the set of elements of  $R$  that map to 0 in  $S$  (i.e., the kernel of  $\varphi$  viewed as a homomorphism of additive groups).
- (3) A bijective ring homomorphism is called an *isomorphism*.

If the context is clear we shall simply use the term “homomorphism” instead of “ring homomorphism.” Similarly, if  $A$  and  $B$  are rings,  $A \cong B$  will always mean an isomorphism of rings unless otherwise stated.

## Examples

- (1) The map  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  defined by sending an even integer to 0 and an odd integer to 1 is a ring homomorphism. The map is additive since the sum of two even or odd integers is even and the sum of an even integer and an odd integer is odd. The map is multiplicative since the product of two odd integers is odd and the product of an even integer with any integer is even. The kernel of  $\varphi$  (the fiber of  $\varphi$  above  $0 \in \mathbb{Z}/2\mathbb{Z}$ ) is the set of even integers. The fiber of  $\varphi$  above  $1 \in \mathbb{Z}/2\mathbb{Z}$  is the set of odd integers.
- (2) For  $n \in \mathbb{Z}$  the maps  $\varphi_n : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $\varphi_n(x) = nx$  are *not* in general ring homomorphisms because  $\varphi_n(xy) = nxy$  whereas  $\varphi_n(x)\varphi_n(y) = nxy = n^2xy$ . Hence  $\varphi_n$  is a ring homomorphism only when  $n^2 = n$ , i.e.,  $n = 0, 1$ . Note however that  $\varphi_n$  is always a *group homomorphism* on the additive groups. Thus care should be exercised when dealing with rings to be sure to check that *both* ring operations are preserved. Note that  $\varphi_0$  is the zero homomorphism and  $\varphi_1$  is the identity homomorphism.
- (3) Let  $\varphi : \mathbb{Q}[x] \rightarrow \mathbb{Q}$  be the map from the ring of polynomials in  $x$  with rational coefficients to the rationals defined by  $\varphi(p(x)) = p(0)$  (i.e., mapping the polynomial to its constant term). Then  $\varphi$  is a ring homomorphism since the constant term of the sum of two polynomials is the sum of their constant terms and the constant term of the product of two polynomials is the product of their constant terms. The fiber above  $a \in \mathbb{Q}$  consists of the set of polynomials with  $a$  as constant term. In particular, the kernel of  $\varphi$  consists of the polynomials with constant term 0.

**Proposition 5.** Let  $R$  and  $S$  be rings and let  $\varphi : R \rightarrow S$  be a homomorphism.

- (1) The image of  $\varphi$  is a subring of  $S$ .
- (2) The kernel of  $\varphi$  is a subring of  $R$ . Furthermore, if  $\alpha \in \ker \varphi$  then  $r\alpha$  and  $\alpha r \in \ker \varphi$  for every  $r \in R$ , i.e.,  $\ker \varphi$  is closed under multiplication by elements from  $R$ .

*Proof:* (1) If  $s_1, s_2 \in \text{im } \varphi$  then  $s_1 = \varphi(r_1)$  and  $s_2 = \varphi(r_2)$  for some  $r_1, r_2 \in R$ . Then  $\varphi(r_1 - r_2) = s_1 - s_2$  and  $\varphi(r_1 r_2) = s_1 s_2$ . This shows  $s_1 - s_2, s_1 s_2 \in \text{im } \varphi$ , so the image of  $\varphi$  is closed under subtraction and under multiplication, hence is a subring of  $S$ .

(2) If  $\alpha, \beta \in \ker \varphi$  then  $\varphi(\alpha) = \varphi(\beta) = 0$ . Hence  $\varphi(\alpha - \beta) = 0$  and  $\varphi(\alpha\beta) = 0$ , so  $\ker \varphi$  is closed under subtraction and under multiplication, so is a subring of  $R$ . Similarly, for any  $r \in R$  we have  $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r) 0 = 0$ , and also  $\varphi(\alpha r) = \varphi(\alpha)\varphi(r) = 0 \varphi(r) = 0$ , so  $r\alpha, \alpha r \in \ker \varphi$ .

In the case of a homomorphism  $\varphi$  of groups we saw that the fibers of the homomorphism have the structure of a group naturally isomorphic to the image of  $\varphi$ , which led to the notion of a quotient group by a normal subgroup. An analogous result is true for a homomorphism of rings.

Let  $\varphi : R \rightarrow S$  be a ring homomorphism with kernel  $I$ . Since  $R$  and  $S$  are in particular additive abelian groups,  $\varphi$  is in particular a homomorphism of abelian groups