

## 7.1 Basic Definitions and Examples

Unless otherwise specified,  $R$  is a ring with 1.

**2)** If  $u$  is a unit in  $R$ , then so is  $-u$ .

*Proof:* Since  $u$  is a unit, there exists  $u^{-1} \in R$  where  $uu^{-1} = 1$ , but  $uu^{-1} = (-u)(-u^{-1}) = 1$ , showing that  $-u$  is also a unit.

**5)** (a) and (d) are rings. (b) fails closure, since  $1/12 + 1/4 = 1/3$ , and (c) lacks additive inverses.

**7)** Let  $Z(R)$  denote the center of  $R$ . Then  $Z(R)$  is a subring of  $R$ . Additionally, if  $R$  is a division ring, then  $Z(R)$  is a field.

*Proof:* For all  $a \in R$ , we have  $1 \cdot a = a = a \cdot 1$ , thus  $1 \in Z(R)$ . Now let  $r, s \in Z(R)$ , then

$$a(r + s) = ar + as = ra + sa = (r + s)a,$$

showing that  $r + s \in Z(R)$ . We also have that

$$a(-r) = -(ar) = -(ra) = (-r)a,$$

so  $-r \in Z(R)$ . Finally,

$$a(rs) = (ar)s = (ra)s = r(as) = r(sa) = (rs)a,$$

thus  $rs \in Z(R)$ , and  $Z(R)$  is a subring of  $R$ .

If  $R$  is a division ring, then every non-zero element of  $R$ , and thus every non-zero element of  $Z(R)$  is a unit. Additionally, if  $r \in Z(R)$ , then for all  $a \in R$ , we have

$$r^{-1}a = r^{-1}(ar)r^{-1} = r^{-1}(ra)r^{-1} = ar^{-1},$$

thus  $r^{-1} \in Z(R)$ , showing that  $Z(R)$  is a commutative division ring, and thus a field. ■

**11)** Let  $R$  be an integral domain and fix  $x \in R$ . If  $x^2 = 1$ , then  $x = \pm 1$ .

*Proof:* Suppose  $x^2 = 1$ , then  $x^2 - 1 = (x + 1)(x - 1) = 0$ . Since  $R$  is an integral domain, one of  $(x + 1)$  and  $(x - 1)$  must be 0, implying that  $x$  must be 1 or  $-1$ . ■

**15)** All boolean rings are commutative.

*Proof:* Let  $R$  be a boolean ring and fix  $a, b \in R$ . We have that

$$aabb = a^2b^2 = ab = (ab)^2 = abab,$$

and cancelling on both sides obtains  $ab = ba$ . ■

**21)** Fix an arbitrary set  $X$ , and denote  $\mathcal{P}(X)$  as its powerset. Also, for  $A, B \in \mathcal{P}(X)$ , define the operations  $+$  and  $\times$  as

$$A + B = A \Delta B = (A \setminus B) \cup (B \setminus A) \quad \text{and} \quad A \times B = A \cap B.$$

Then  $\mathcal{P}(X)$  forms a commutative boolean ring with 1 under these operations.

*Proof:* It is clear that  $\mathcal{P}(X)$  is closed under both operations. For any  $A \in \mathcal{P}(X)$ , we have  $A \Delta \emptyset = A$ , so  $\emptyset$  serves as our additive identity. Additionally,  $A \Delta A = \emptyset$ , so each element is its own additive inverse. It is left as an exercise for the reader to show that symmetric differences are associative. Thus,  $\mathcal{P}(X)$  forms an additive group under  $+$ .

We have that  $A \cap X = A$  for all  $A$ , thus  $X$  serves as our multiplicative identity. We also have that intersections distribute across symmetric differences, showing that  $\mathcal{P}(X)$  forms a ring. Finally, we have that  $A^2 = A \cap A = A$  and  $A \cap B = B \cap A$  for all  $A$  and  $B$ , so the ring is boolean and commutative. ■

## 7.2 Polynomial Rings, Matrix Rings, and Group Rings

**1)** Let  $p(x) = 2x^3 - 3x^2 + 4x - 5$  and  $q(x) = 7x^3 + 33x - 4$  be polynomials. If the coefficients exist in  $\mathbb{Z}$ , then we have

$$p(x) + q(x) = 9x^3 - 3x^2 + 37x - 9,$$

$$p(x)q(x) = 14x^6 - 21x^5 + 94x^4 - 142x^3 - 20x^2 - 181x + 20$$

In  $\mathbb{Z}/2\mathbb{Z}$ , we have

$$p(x) + q(x) = x^3 + x^2 + x + 1,$$

$$p(x)q(x) = x^5 + x.$$

In  $\mathbb{Z}/3\mathbb{Z}$ , we have

$$p(x) + q(x) = x,$$

$$p(x)q(x) = 2x^6 + x^4 + x^3 + x + 2$$

## 7.3 Ring Homomorphisms and Quotient Rings

4) There are six unique ring homomorphisms from  $\mathbb{Z}$  to  $\mathbb{Z}/30\mathbb{Z}$ .

*Proof:* Any ring homomorphism  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/30\mathbb{Z}$  is determined by where  $\phi(1)$  is sent. Fix  $n \in \mathbb{Z}/30\mathbb{Z}$  where  $\phi(1) = n$ , then  $n = \phi(1) = \phi(1)\phi(1) = n^2$ , so any value in  $\mathbb{Z}/30\mathbb{Z}$  that is equivalent to its square induces a unique homomorphism  $\phi$ . These values happen to be  $\overline{1}, \overline{6}, \overline{10}, \overline{15}, \overline{21}$ , and  $\overline{25}$ , thus there are six such homomorphisms. ■

6)  $\phi : M_2(\mathbb{Z}) \rightarrow \mathbb{Z}$  defined as the projection of the 1,1-th entry is not a homomorphism since the 1,1-th entry of the product of two matrices is not necessarily equal the product of the respective components.

$\phi : M_2(\mathbb{Z}) \rightarrow \mathbb{Z}$  defined as the trace of the matrix is not a homomorphism since the trace of the product of two matrices contains all entries of both matrices rather than just the diagonal entries.

$\phi : M_2(\mathbb{Z}) \rightarrow \mathbb{Z}$  defined as the determinant of the matrix is not a homomorphism the determinant of a sum is not necessarily equal to the sum of the determinants.

**Lemma 1:** If  $I$  and  $J$  are ideals in  $R$ , then  $I \times J$  is an ideal in  $R \times R$ .

*Proof:* Let  $(a, b) \in R \times R$  and  $(i, j) \in I \times J$ , then  $ai \in I$  and  $bj \in J$ , thus  $(a, b) \cdot (i, j) = (ai, bj) \in I \times J$ . ■

8) For (b) and (c), we can represent them as  $2\mathbb{Z} \times 2\mathbb{Z}$  and  $2\mathbb{Z} \times \{0\}$  respectively, and thus by **Lemma 1** they are ideals.

For (a) and (d), if  $m$  and  $n$  are distinct in  $\mathbb{Z}$ , then  $(m, n) \cdot (a, a)$  and  $(m, n) \cdot (a, -a)$  are not in their respective sets, and thus they are not ideals.