

## Commutative rings, in general

The examples you should have in mind are these: the set of integers  $\mathbf{Z}$ ; the set  $\mathbf{Z}_n$  of integers modulo  $n$ ; any field  $F$  (in particular the set  $\mathbf{Q}$  of rational numbers and the set  $\mathbf{R}$  of real numbers); the set  $F[x]$  of all polynomials with coefficients in a field  $F$ ; the set  $F[x]/\langle p(x) \rangle$  of congruence classes of polynomials in  $F[x]$ , modulo the polynomial  $p(x)$ . The axioms we will use are the same as those for a field, with one crucial exception: we have dropped the requirement that each nonzero element has a multiplicative inverse, in order to include integers and polynomials in the class of objects we want to study.

**Example 5.1.1.** ( $\mathbf{Z}_n$ ) The rings  $\mathbf{Z}_n$  form a class of commutative rings that is a good source of examples and counterexamples.

**Definition 5.1.3.** Let  $S$  be a commutative ring. A nonempty subset  $R$  of  $S$  is called a **subring** of  $S$  if it is a commutative ring under the addition and multiplication of  $S$ .

**Proposition 5.1.4.** Let  $S$  be a commutative ring, and let  $R$  be a nonempty subset of  $S$ . Then  $R$  is a subring of  $S$  if and only if (i)  $R$  is closed under addition and multiplication; and (ii) if  $a \in R$ , then  $-a \in R$ .

**Definition 5.1.5.** Let  $R$  be a commutative ring. An element  $a \in R$  is **invertible** if there exists an element  $b \in R$  such that  $ab = 1$ . The element  $a$  is also called a **unit** of  $R$ , and its multiplicative inverse is usually denoted by  $a^{-1}$ .

**Proposition 5.1.6.** Let  $R$  be a commutative ring. Then the set  $R^\times$  of units of  $R$  is an abelian group under the multiplication of  $R$ .

An element  $e$  of a commutative ring  $R$  is said to be **idempotent** if  $e^2 = e$ . An element  $a$  is said to be **nilpotent** if there exists a positive integer  $n$  with  $a^n = 0$ . Note that exercises in Section 1.4 contain information about idempotent and nilpotent elements in  $\mathbf{Z}_n$ . The group  $\mathbf{Z}_n^\times$  of units of  $\mathbf{Z}_n$  is also studied in Section 1.4.

**Definition 5.2.1.** Let  $R$  and  $S$  be commutative rings. A function  $\phi : R \rightarrow S$  is called a **ring homomorphism** if  $\phi(a + b) = \phi(a) + \phi(b)$  and  $\phi(ab) = \phi(a)\phi(b)$  for all  $a, b \in R$ , and  $\phi(1) = 1$ .

A ring homomorphism that is one-to-one and onto is called an **isomorphism**. If there is an isomorphism from  $R$  onto  $S$ , we say that  $R$  is **isomorphic** to  $S$ , and write  $R \cong S$ . An isomorphism from the commutative ring  $R$  onto itself is called an **automorphism** of  $R$ .

**Proposition 5.2.2.** The inverse of a ring isomorphism is a ring isomorphism; the composition of two ring isomorphisms is a ring isomorphism.

**Proposition 5.2.3.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then (a)  $\phi(0) = 0$ ; (b)  $\phi(-a) = -\phi(a)$  for all  $a \in R$ ; (c)  $\phi(R)$  is a subring of  $S$ .

**Definition 5.2.4.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. The set  $\{a \in R \mid \phi(a) = 0\}$  is called the **kernel** of  $\phi$ , denoted by  $\ker(\phi)$ .

**Proposition 5.2.5.** Let  $\phi : R \rightarrow S$  be a ring homomorphism.

- (a) If  $a, b \in \ker(\phi)$  and  $r \in R$ , then  $a + b$ ,  $a - b$ , and  $ra$  belong to  $\ker(\phi)$ .
- (b) The homomorphism  $\phi$  is an isomorphism if and only if  $\ker(\phi) = \{0\}$  and  $\phi(R) = S$ .

**Proposition 5.2.7.** Let  $R$  and  $S$  be commutative rings, let  $\theta : R \rightarrow S$  be a ring homomorphism, and let  $s$  be any element of  $S$ . Then there exists a unique ring homomorphism  $\widehat{\theta}_s : R[x] \rightarrow S$  such that  $\widehat{\theta}_s(r) = \theta(r)$  for all  $r \in R$  and  $\widehat{\theta}_s(x) = s$ , defined by  $\widehat{\theta}_s(a_0 + a_1x + \dots + a_mx^m) = \theta(a_0) + \theta(a_1)s + \dots + \theta(a_m)s^m$ .

**Proposition 5.2.8.** Let  $R_1, R_2, \dots, R_n$  be commutative rings. The set of  $n$ -tuples  $(a_1, a_2, \dots, a_n)$  such that  $a_i \in R_i$  for each  $i$  is a commutative ring under componentwise addition and multiplication.

**Definition 5.2.9.** Let  $R_1, R_2, \dots, R_n$  be commutative rings. The set of  $n$ -tuples  $(a_1, a_2, \dots, a_n)$  such that  $a_i \in R_i$  for each  $i$  is called the **direct sum** of rings, and is denoted by  $R_1 \oplus R_2 \oplus \dots \oplus R_n$ .

**Example 5.2.13.** Let  $n$  be a positive integer with prime decomposition  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ . The mapping  $\phi$  defined by  $\phi([x]_n) = ([x]_{p_1^{\alpha_1}}, [x]_{p_2^{\alpha_2}}, \dots, [x]_{p_m^{\alpha_m}})$  for all  $[x]_n \in \mathbf{Z}_n$  is a ring isomorphism. That  $\phi$  is an additive isomorphism is shown by Theorem 3.5.4, and it is easy to show that  $\phi$  also preserves multiplication. The isomorphism  $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \oplus \mathbf{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbf{Z}_{p_m^{\alpha_m}}$  describes the structure of  $\mathbf{Z}_n$  in terms of simpler rings, and is the first example of what is usually called a “structure theorem.” This structure theorem can be used to determine the invertible, idempotent, and nilpotent elements of  $\mathbf{Z}_n$ , and provides an easy proof of our earlier formula for the Euler  $\varphi$ -function  $\varphi(n)$  in terms of the prime factors of  $n$ .

**Definition 5.2.10.** Let  $R$  be a commutative ring. The smallest positive integer  $n$  such that  $n \cdot 1 = 0$  is called the **characteristic** of  $R$ , denoted by  $\text{char}(R)$ . If no such positive integer exists, then  $R$  is said to have **characteristic zero**.

A more sophisticated way to view the characteristic is to define a ring homomorphism  $\phi : \mathbf{Z} \rightarrow R$  by  $\phi(n) = n \cdot 1$ . The characteristic of  $R$  is just the (nonnegative) generator of  $\ker(\phi)$ .

### Ideals and factor rings

**Definition 5.3.1.** Let  $R$  be a commutative ring. A nonempty subset  $I$  of  $R$  is called an **ideal** of  $R$  if (i)  $a \pm b \in I$  for all  $a, b \in I$ , and (ii)  $ra \in I$  for all  $a \in I$  and  $r \in R$ .

The set  $\{0\}$  is an ideal, which we will refer to as the **trivial** ideal, and the set  $R$  is also always an ideal. The kernel of any ring homomorphism is an ideal, and conversely, by Proposition 5.3.7, every ideal is the kernel of *some* ring homomorphism. Note that an ideal is a subgroup (under addition) with  $ra \in I$  for all  $a \in I$  and  $r \in R$ .

**Proposition 5.3.2.** Let  $R$  be a commutative ring. Then  $R$  is a field if and only if it has no proper nontrivial ideals.

**Definition 5.3.6.** (*modified*) Let  $I$  be an ideal of the commutative ring  $R$ . The set of all cosets of  $I$  (in  $R$  considered as an abelian group) will be denoted by  $R/I$ .

Let  $R$  be a commutative ring and let  $I$  be an ideal of  $R$ . The formulas for addition and multiplication in  $R/I$  have the form  $(a + I) + (b + I) = (a + b) + I$  and  $(a + I) \cdot (b + I) = ab + I$ , where  $a, b \in R$ .

**Theorem 5.3.5.** If  $I$  is an ideal of the commutative ring  $R$ , then  $R/I$  is a commutative ring.

**Proposition 5.3.7.** Let  $I$  be an ideal of the commutative ring  $R$ .

(a) The natural projection mapping  $\pi : R \rightarrow R/I$  defined by  $\pi(a) = a + I$  for all  $a \in R$  is a ring homomorphism, and  $\ker(\pi) = I$ .

(b) There is a one-to-one correspondence between the ideals of  $R/I$  and ideals of  $R$  that contain  $I$ .

**Theorem 5.2.6. [Fundamental Homomorphism Theorem for Rings]** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then  $R/\ker(\phi) \cong \phi(R)$ .

**Definition 5.1.7.** A commutative ring  $R$  is called an **integral domain** if for all  $a, b \in R$ ,  $ab = 0$  implies  $a = 0$  or  $b = 0$ .

The ring of integers  $\mathbf{Z}$  is the most fundamental example of an integral domain. The ring of all polynomials with real coefficients is also an integral domain, but the larger ring of all real valued functions is not an integral domain.

The cancellation law for multiplication holds in  $R$  if and only if  $R$  has no nonzero divisors of zero. One way in which the cancellation law holds in  $R$  is if nonzero elements have inverses in a larger ring; the next two results characterize integral domains as subrings of fields (that contain 1).

**Theorem 5.1.8.** Any subring of a field is an integral domain.

**Theorem 5.1.9.** Any finite integral domain must be a field.

**Proposition 5.2.11.** An integral domain has characteristic 0 or  $p$ , for some prime number  $p$ .

**Definition 5.3.8.** Let  $I$  be a proper ideal of the commutative ring  $R$ . Then  $I$  is said to be a **prime ideal** of  $R$  if for all  $a, b \in R$  it is true that  $ab \in I$  implies  $a \in I$  or  $b \in I$ .

The ideal  $I$  is said to be a **maximal ideal** of  $R$  if for all ideals  $J$  of  $R$  such that  $I \subseteq J \subseteq R$ , either  $J = I$  or  $J = R$ .

**Proposition 5.3.9.** Let  $I$  be a proper ideal of the commutative ring  $R$ .

- (a) The factor ring  $R/I$  is a field if and only if  $I$  is a maximal ideal of  $R$ .
- (b) The factor ring  $R/I$  is an integral domain if and only if  $I$  is a prime ideal of  $R$ .
- (c) If  $I$  is maximal, then it is a prime ideal.

**Definition 5.3.3.** Let  $R$  be a commutative ring, and let  $a \in R$ . The ideal

$$aR = \{x \in R \mid x = ar \text{ for some } r \in R\}$$

is called the **principal ideal** generated by  $a$ . The notation  $\langle a \rangle$  will also be used.

An integral domain in which every ideal is a principal ideal is called a **principal ideal domain**.

**Theorem 5.3.10.** Every nonzero prime ideal of a principal ideal domain is maximal.

**Example 5.3.1. ( $\mathbf{Z}$  is a principal ideal domain)** Theorem 1.1.4 shows that the ring of integers  $\mathbf{Z}$  is a principal ideal domain. Moreover, given any nonzero ideal  $I$  of  $\mathbf{Z}$ , the smallest positive integer in  $I$  is a generator for the ideal.

**Example 5.3.7. (Ideals of  $F[x]$ )** Let  $F$  be any field. Then  $F[x]$  is a principal ideal domain, since the ideals of  $F[x]$  have the form  $I = \langle f(x) \rangle$ , where  $f(x)$  is the unique monic polynomial of minimal degree in the ideal. The ideal  $I$  is prime (and hence maximal) if and only if  $f(x)$  is irreducible. If  $p(x)$  is irreducible, then the factor ring  $F[x]/\langle p(x) \rangle$  is a field.

**Example 5.3.9. (Evaluation mapping)** Let  $F$  be a subfield of  $E$ , and for any element  $u \in E$  define the evaluation mapping  $\phi_u : F[x] \rightarrow E$  by  $\phi_u(f(x)) = f(u)$ , for all  $f(x) \in F[x]$ . Since  $\phi_u(F[x])$  is a subring of  $E$  that contains 1, it is an integral domain, and so  $\ker(\phi_u)$  is a prime ideal. Thus if  $\ker(\phi_u)$  is nonzero, then it is a maximal ideal, so  $F[x]/\ker(\phi_u)$  is a field, and the image of  $\phi_u$  is a subfield of  $E$ .

## A COMPARISON OF GROUPS AND RINGS

### GROUPS

$S_n$ ;  $GL_n(F)$ ,  $F$  a field

One binary operation  $\cdot$   
 associative, identity  $e$ , inverses  $g^{-1}$

Group homomorphisms

$$\phi(g)\phi(h) = \phi(gh), \forall g, h \in G$$

Kernels of group homomorphisms

Normal subgroups:  
 $gNg^{-1} \subseteq N, \forall g \in G$

Factor groups

cosets  $gN$ , where  $N$  is normal  
 $gN \cdot hN = ghN$

Some classes of groups

Abelian groups  
 $gh = hg, \forall g, h \in G$

Cyclic groups  
 $\mathbf{Z}$ ;  $\mathbf{Z}_n$

Simple abelian groups  
 $\mathbf{Z}_p$  (if  $p$  is prime)

### COMMUTATIVE RINGS

(the analog of  $GL_n(F)$  is  $M_n(F)$ ,  $F$  a field,  
 but this is not a *commutative* ring)

Two binary operations  $+$ ,  $\cdot$   
 abelian group under  $+$ , identity  $0$ , inverses  $-r$   
 multiplication is associative, with identity  $1$   
 distributive laws connect  $+$  and  $\cdot$

Ring homomorphisms

$$\begin{aligned} \phi(r) + \phi(s) &= \phi(r + s), \forall r, s \in R \\ \phi(r)\phi(s) &= \phi(rs), \forall r, s \in R \\ \phi(1) &= 1 \end{aligned}$$

Kernels of ring homomorphisms

Ideals:  
 subgroups with  $rI \subseteq I, \forall r \in R$

Factor rings

cosets  $r + I$ , where  $I$  is an ideal  
 $(r + I) + (s + I) = (r + s) + I$   
 $(r + I) \cdot (s + I) = rs + I$

Some classes of commutative rings

Integral domains  
 $rs \neq 0$  if  $r \neq 0$  and  $s \neq 0$

Principal ideal domains  
 $\mathbf{Z}$ ;  $F[x]$

Fields  
 $\mathbf{Q}$ ;  $\mathbf{R}$ ;  $\mathbf{C}$ ;  $\mathbf{Z}_p$  (if  $p$  is prime)  
 $F[x]/\langle p(x) \rangle$  (if  $p(x)$  is irreducible)