

---

# Commutative Rings

---

## SOLUTIONS TO THE REVIEW PROBLEMS

1. Let  $R$  be the ring with 8 elements consisting of all  $3 \times 3$  matrices with entries in  $\mathbf{Z}_2$  which have the following form:

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix}$$

You may assume that the standard laws for addition and multiplication of matrices are valid.

- (a) Show that  $R$  is a commutative ring (you only need to check closure and commutativity of multiplication).

*Solution:* It is clear that the set is closed under addition, and the following computation checks closure under multiplication.

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix} \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ y & z & x \end{bmatrix} = \begin{bmatrix} ax & 0 & 0 \\ 0 & ax & 0 \\ bx + ay & cx + az & ax \end{bmatrix}$$

Because of the symmetry  $a \leftrightarrow x$ ,  $b \leftrightarrow y$ ,  $c \leftrightarrow z$ , the above computation also checks commutativity.

(b) Find all units of  $R$ , and all nilpotent elements of  $R$ .

*Solution:* Four of the matrices in  $R$  have 1's on the diagonal, and these are invertible since their determinant is nonzero. Squaring each of the other four matrices gives the zero matrix, and so they are nilpotent.

(c) Find all idempotent elements of  $R$ .

*Solution:* By part (b), an element in  $R$  is either a unit or nilpotent. The only unit that is idempotent is the identity matrix (in a group, the only idempotent element is the identity) and the only nilpotent element that is also idempotent is the zero matrix.

2. Let  $R$  be the ring  $\mathbf{Z}_2[x]/\langle x^2 + 1 \rangle$ . Show that although  $R$  has 4 elements, it is not isomorphic to either of the rings  $\mathbf{Z}_4$  or  $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ .

*Solution:* In  $R$  we have  $a + a = 0$ , for all  $a \in R$ , so  $R$  is not isomorphic to  $\mathbf{Z}_4$ . On the other hand, in  $R$  we have  $[x + 1] \neq [0]$  but  $[x + 1]^2 = [x^2 + 1] = [0]$ . Thus  $R$  cannot be isomorphic to  $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ , since in that ring  $(a, b)^2 = (0, 0)$  implies  $a^2 = 0$  and  $b^2 = 0$ , and this implies  $a = 0$  and  $b = 0$  since  $\mathbf{Z}_2$  is a field.

3. Find all ring homomorphisms from  $\mathbf{Z}_{120}$  into  $\mathbf{Z}_{42}$ .

*Solution:* Let  $\phi : \mathbf{Z}_{120} \rightarrow \mathbf{Z}_{42}$  be a ring homomorphism. The additive order of  $\phi(1)$  must be a divisor of  $\gcd(120, 42) = 6$ , so it must belong to the subgroup  $7\mathbf{Z}_{42} = \{0, 7, 14, 21, 28, 35\}$ . Furthermore,  $\phi(1)$  must be idempotent, and it can be checked that in  $7\mathbf{Z}_{42}$ , only 0, 7, 21, 28 are idempotent.

If  $\phi(1) = 7$ , then the image is  $7\mathbf{Z}_{42}$  and the kernel is  $6\mathbf{Z}_{120}$ . If  $\phi(1) = 21$ , then the image is  $21\mathbf{Z}_{42}$  and the kernel is  $2\mathbf{Z}_{120}$ . If  $\phi(1) = 28$ , then the image is  $14\mathbf{Z}_{42}$  and the kernel is  $3\mathbf{Z}_{120}$ .

4. Are  $\mathbf{Z}_9$  and  $\mathbf{Z}_3 \oplus \mathbf{Z}_3$  isomorphic as rings?

*Solution:* The answer is no. The argument can be given using either addition or multiplication. Addition in the two rings is different, since the additive group of  $\mathbf{Z}_9$  is cyclic, while that of  $\mathbf{Z}_3 \oplus \mathbf{Z}_3$  is not. Multiplication is also different, since in  $\mathbf{Z}_9$  there is a nonzero solution to the equation  $x^2 = 0$ , while in  $\mathbf{Z}_3 \oplus \mathbf{Z}_3$  there is not. (In  $\mathbf{Z}_9$  let  $x = 3$ , while in  $\mathbf{Z}_3 \oplus \mathbf{Z}_3$  the equation  $(a, b)^2 = (0, 0)$  implies  $a^2 = 0$  and  $b^2 = 0$ , and then  $a = 0$  and  $b = 0$ .)

5. In the group  $\mathbf{Z}_{180}^\times$  of units of the ring  $\mathbf{Z}_{180}$ , what is the largest possible order of an element?

*Solution:* Since  $180 = 2^2 3^2 5$ , it follows from Theorem 3.5.4 that the ring  $\mathbf{Z}_{180}$  is isomorphic to the ring  $\mathbf{Z}_4 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$ . Then Example 5.2.10 shows that

$$\mathbf{Z}_{180}^\times \cong \mathbf{Z}_4^\times \times \mathbf{Z}_9^\times \times \mathbf{Z}_5^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_4 .$$

In the latter additive group, the order of an element is the least common multiple of the orders of its components. It follows that the largest possible order of an element is  $\text{lcm}[2, 6, 4] = 12$ .

6. For the element  $a = (0, 2)$  of the ring  $R = \mathbf{Z}_{12} \oplus \mathbf{Z}_8$ , find  $\text{Ann}(a) = \{r \in R \mid ra = 0\}$ . Show that  $\text{Ann}(a)$  is an ideal of  $R$ .

*Solution:* We need to solve  $(x, y)(0, 2) = (0, 0)$  for  $(x, y) \in \mathbf{Z}_{12} \oplus \mathbf{Z}_8$ . We only need  $2y \equiv 0 \pmod{8}$ , so the first component  $x$  can be any element of  $\mathbf{Z}_{12}$ , while  $y = 0, 4$ . Thus  $\text{Ann}((0, 2)) = \mathbf{Z}_{12} \oplus 4\mathbf{Z}_8$ . This set is certainly closed under addition, and it is also closed under multiplication by any element of  $R$  since  $4\mathbf{Z}_8$  is an ideal of  $\mathbf{Z}_8$ .

7. Let  $R$  be the ring  $\mathbf{Z}_2[x]/\langle x^4 + 1 \rangle$ , and let  $I$  be the set of all congruence classes in  $R$  of the form  $[f(x)(x^2 + 1)]$ .

(a) Show that  $I$  is an ideal of  $R$ .

(b) Show that  $R/I \cong \mathbf{Z}_2[x]/\langle x^2 + 1 \rangle$ .

*Solution:* Define  $\phi : \mathbf{Z}_2[x]/\langle x^4 + 1 \rangle \rightarrow \mathbf{Z}_2[x]/\langle x^2 + 1 \rangle$  by

$\phi(f(x) + \langle x^4 + 1 \rangle) = (f(x) + \langle x^2 + 1 \rangle)$ . This mapping is well-defined since  $x^2 + 1$  is a factor of  $x^4 + 1$  over  $\mathbf{Z}_2$ . It is not difficult to show that  $\phi$  is an onto ring homomorphism, with kernel equal to  $I$ .

(c) Is  $I$  a prime ideal of  $R$ ?

*Solution:* No:  $(x + 1)(x + 1) \equiv 0 \pmod{x^2 + 1}$ .

*Hint:* If you use the fundamental homomorphism theorem, you can do the first two parts together.

8. Find all maximal ideals, and all prime ideals, of  $\mathbf{Z}_{36} = \mathbf{Z}/36\mathbf{Z}$ .

*Solution:* If  $P$  is a prime ideal of  $\mathbf{Z}_{36}$ , then  $\mathbf{Z}_{36}/P$  is a finite integral domain, so it is a field, and hence  $P$  is maximal. Thus we only need to find the maximal ideals of  $\mathbf{Z}_{36}$ . The lattice of ideals of  $\mathbf{Z}_{36}$  is exactly the same as the lattice of subgroups, so the maximal ideals of  $\mathbf{Z}_{36}$  correspond to the prime divisors of 36. The maximal ideals of  $\mathbf{Z}_{36}$  are thus  $2\mathbf{Z}_{36}$  and  $3\mathbf{Z}_{36}$ .

An alternate approach we can use Proposition 5.3.7, which shows that there is a one-to-one correspondence between the ideals of  $\mathbf{Z}/36\mathbf{Z}$  and the ideals of  $\mathbf{Z}$  that contain  $36\mathbf{Z}$ . In  $\mathbf{Z}$  every ideal is principal, so the relevant ideals correspond to the divisors of 36. Again, the maximal ideals that contain  $36\mathbf{Z}$  are  $2\mathbf{Z}$  and  $3\mathbf{Z}$ , and these correspond to  $2\mathbf{Z}_{36}$  and  $3\mathbf{Z}_{36}$ .

9. Give an example to show that the set of all zero divisors of a ring need not be an ideal of the ring.

*Solution:* The elements  $(1, 0)$  and  $(0, 1)$  of  $\mathbf{Z} \times \mathbf{Z}$  are zero divisors, but if the set of zero divisors were closed under addition it would include  $(1, 1)$ , an obvious contradiction.

10. Let  $I$  be the subset of  $\mathbf{Z}[x]$  consisting of all polynomials with even coefficients. Prove that  $I$  is a prime ideal; prove that  $I$  is not maximal.

*Solution:* Define  $\phi : \mathbf{Z}[x] \rightarrow \mathbf{Z}_2[x]$  by reducing coefficients modulo 2. This is an onto ring homomorphism with kernel  $I$ . Then  $R/I$  is isomorphic to  $\mathbf{Z}_2[x]$ , which is not a field, so  $I$  is not maximal.

11. Let  $R$  be any commutative ring with identity 1.

(a) Show that if  $e$  is an idempotent element of  $R$ , then  $1-e$  is also idempotent.

*Solution:* We have  $(1-e)^2 = (1-e)(1-e) = 1-e-e+e^2 = 1-e-e+e = 1-e$ .

(b) Show that if  $e$  is idempotent, then  $R \cong Re \oplus R(1-e)$ .

*Solution:* Note that  $e(1-e) = e-e^2 = e-e = 0$ . Define  $\phi : R \rightarrow Re \oplus R(1-e)$  by  $\phi(r) = (re, r(1-e))$ , for all  $r \in R$ . Then  $\phi$  is one-to-one since if  $\phi(r) = \phi(s)$ , then  $re = se$  and  $r(1-e) = s(1-e)$ , and adding the two equations gives  $r = s$ . Furthermore,  $\phi$  is onto, since for any element  $(ae, b(1-e))$  we have  $(ae, b(1-e)) = \phi(r)$  for  $r = ae + b(1-e)$ . Finally, it is easy to check that  $\phi$  preserves addition, and for any  $r, s \in R$  we have  $\phi(rs) = (rse, rs(1-e))$  and  $\phi(r)\phi(s) = (re, r(1-e))(se, s(1-e)) = (rse^2, rs(1-e)^2) = (rse, rs(1-e))$ .

12. Let  $R$  be the ring  $\mathbf{Z}_2[x]/\langle x^3 + 1 \rangle$ .

*Solution:* Note: Table 5.0.1 gives the multiplication table. It is not necessary

Table 5.0.1 Multiplication in  $\mathbf{Z}_2[x]/\langle x^3 + 1 \rangle$

$\times$	1	$x$	$x^2$	$x^2 + x + 1$	$x^2 + x$	$x + 1$	$x^2 + 1$
1	1	$x$	$x^2$	$x^2 + x + 1$	$x^2 + x$	$x + 1$	$x^2 + 1$
$x$	$x$	$x^2$	1	$x^2 + x + 1$	$x^2 + 1$	$x^2 + x$	$x + 1$
$x^2$	$x^2$	1	$x$	$x^2 + x + 1$	$x + 1$	$x^2 + 1$	$x^2 + x$
$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x + 1$	0	0	0
$x^2 + x$	$x^2 + x$	$x^2 + 1$	$x + 1$	0	$x^2 + x$	$x + 1$	$x^2 + 1$
$x + 1$	$x + 1$	$x^2 + x$	$x^2 + 1$	0	$x + 1$	$x^2 + 1$	$x^2 + x$
$x^2 + 1$	$x^2 + 1$	$x + 1$	$x^2 + x$	0	$x^2 + 1$	$x^2 + x$	$x + 1$

to compute the multiplication table in order to solve the problem.

(a) Find all ideals of  $R$ .

*Solution:* By Proposition 5.3.7, the ideals of  $R$  correspond to the ideals of  $\mathbf{Z}_2[x]$  that contain  $\langle x^3 + 1 \rangle$ . We have the factorization  $x^3 + 1 = x^3 - 1 = (x-1)(x^2 + x + 1)$ , so the only proper, nonzero ideals are the principal ideals generated by  $[x + 1]$  and  $[x^2 + x + 1]$ .

(b) Find the units of  $R$ .

*Solution:* We have  $[x]^3 = [1]$ , so  $[x]$  and  $[x^2]$  are units. On the other hand,  $[x + 1][x^2 + x + 1] = [x^3 + 1] = [0]$ , so  $[x + 1]$  and  $[x^2 + x + 1]$  cannot be units.

This also excludes  $[x^2 + x] = [x][x + 1]$  and  $[x^2 + 1] = [x^2][1 + x]$ . Thus the only units are 1,  $[x]$ , and  $[x^2]$ .

(c) Find the idempotent elements of  $R$ .

*Solution:* Using the general fact that  $(a + b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$  (since  $\mathbf{Z}_2[x]$  has characteristic 2) and the identities  $[x^3] = [1]$  and  $[x^4] = [x]$ , it is easy to see that the idempotent elements of  $R$  are  $[0]$ ,  $[1]$ ,  $[x^2 + x + 1]$ , and  $[x^2 + x]$ .

13. Let  $S$  be the ring  $\mathbf{Z}_2[x]/\langle x^3 + x \rangle$ .

*Solution:* Note: Table 5.0.2 gives the multiplication table. It is not necessary

Table 5.0.2 Multiplication in  $\mathbf{Z}_2[x]/\langle x^3 + x \rangle$

$\times$	1	$x^2 + x + 1$	$x^2$	$x$	$x^2 + x$	$x + 1$	$x^2 + 1$
1	1	$x^2 + x + 1$	$x^2$	$x$	$x^2 + x$	$x + 1$	$x^2 + 1$
$x^2 + x + 1$	$x^2 + x + 1$	1	$x^2$	$x$	$x^2 + x$	$x + 1$	$x^2 + 1$
$x^2$	$x^2$	$x^2$	$x^2$	$x$	$x^2 + x$	$x^2 + x$	0
$x$	$x$	$x$	$x$	$x^2$	$x^2 + x$	$x^2 + x$	0
$x^2 + x$	$x^2 + x$	$x^2 + x$	$x^2 + x$	$x^2 + x$	0	0	0
$x + 1$	$x + 1$	$x + 1$	$x^2 + x$	$x^2 + x$	0	$x^2 + 1$	$x^2 + 1$
$x^2 + 1$	$x^2 + 1$	$x^2 + 1$	0	0	0	$x^2 + 1$	$x^2 + 1$

to compute the multiplication table in order to solve the problem.

(a) Find all ideals of  $S$ .

*Solution:* Over  $\mathbf{Z}_2$  we have the factorization  $x^3 + x = x(x^2 + 1) = x(x + 1)^2$ , so by Proposition 5.3.7 the proper nonzero ideals of  $S$  are the principal ideals generated by  $[x]$ ,  $[x + 1]$ ,  $[x^2 + 1] = [x + 1]^2$ , and  $[x^2 + x] = [x][x + 1]$ .

$$\langle [x^2 + x] \rangle = \{[0], [x^2 + x]\} \quad \langle [x^2 + 1] \rangle = \{[0], [x^2 + 1]\}$$

$$\langle [x] \rangle = \{[0], [x], [x^2], [x^2 + x]\} \quad \langle [x + 1] \rangle = \{[0], [x + 1], [x^2 + 1], [x^2 + x]\}$$

(b) Find the units of  $R$ .

*Solution:* Since no unit can belong to a proper ideal, it follows from part (a) that we only need to check  $[x^2 + x + 1]$ . This is a unit since  $[x^2 + x + 1]^2 = [1]$ .

(c) Find the idempotent elements of  $R$ .

*Solution:* Since  $[x^3] = [1]$ , we have  $[x^2]^2 = [x^2]$ , and then  $[x^2 + 1]^2 = [x^2 + 1]$ . These, together with  $[0]$  and  $[1]$ , are the only idempotents.

14. Show that the rings  $R$  and  $S$  in the two previous problems are isomorphic as abelian groups, but not as rings.

*Solution:* Both  $R$  and  $S$  are isomorphic to  $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ , as abelian groups. They cannot be isomorphic as rings since  $R$  has 3 units, while  $S$  has only 2.

15. Let  $\mathbf{Z}[i]$  be the subring of the field of complex numbers given by

$$\mathbf{Z}[i] = \{m + ni \in \mathbf{C} \mid m, n \in \mathbf{Z}\}.$$

- (a) Define  $\phi : \mathbf{Z}[i] \rightarrow \mathbf{Z}_2$  by  $\phi(m + ni) = [m + n]_2$ . Prove that  $\phi$  is a ring homomorphism. Find  $\ker(\phi)$  and show that it is a principal ideal of  $\mathbf{Z}[i]$ .

*Solution:* We have the following computations, which show that  $\phi$  is a ring homomorphism.

$$\begin{aligned}\phi((a + bi) + (c + di)) &= \phi((a + c) + (b + d)i) = [a + c + b + d]_2 \\ \phi((a + bi)) + \phi((c + di)) &= [a + b]_2 + [c + d]_2 = [a + b + c + d]_2\end{aligned}$$

$$\begin{aligned}\phi((a + bi)(c + di)) &= \phi((ac - bd) + (ad + bc)i) = [ac - bd + ad + bc]_2 \\ \phi((a + bi))\phi((c + di)) &= [a + b]_2 \cdot [c + d]_2 = [ac + ad + bc + bd]_2.\end{aligned}$$

We claim that  $\ker(\phi)$  is generated by  $1 + i$ . It is clear that  $1 + i$  is in the kernel, and we note that  $(1 - i)(1 + i) = 2$ . Let  $m + ni \in \ker(\phi) = \{m + ni \mid m + n \equiv 0 \pmod{2}\}$ . Then  $m$  and  $n$  are either both even or both odd, and so it follows that  $m - n$  is always even. Therefore

$$\begin{aligned}m + ni &= (m - n) + n + ni = (m - n) + n(1 + i) \\ &= \left(\frac{m - n}{2}\right)(1 - i)(1 + i) + n(1 + i) \\ &= \left[\frac{1}{2}(m - n)(1 - i) + n\right](1 + i),\end{aligned}$$

and so  $m + ni$  belongs to the principal ideal generated by  $1 + i$ .

- (b) For any prime number  $p$ , define  $\theta : \mathbf{Z}[i] \rightarrow \mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$  by  $\theta(m + ni) = [m + nx]$ . Prove that  $\theta$  is an onto ring homomorphism.

*Solution:* We have the following computations, which show that  $\theta$  is a ring homomorphism. We need to use the fact that  $[x^2] = [-1]$  in  $\mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$ .

$$\begin{aligned}\theta((a + bi) + (c + di)) &= \theta((a + c) + (b + d)i) = [(a + c) + (b + d)x] \\ \theta((a + bi)) + \theta((c + di)) &= [a + bx] + [c + dx] = [(a + c) + (b + d)x]\end{aligned}$$

$$\begin{aligned}\theta((a + bi)(c + di)) &= \theta((ac - bd) + (ad + bc)i) = [(ac - bd) + (ad + bc)x] \\ \theta((a + bi))\theta((c + di)) &= [a + bx][c + dx] = [ac + (ad + bc)x + bdx^2].\end{aligned}$$

Since the elements of  $\mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$  all have the form  $[a + bx]$ , for some congruence classes  $a$  and  $b$  in  $\mathbf{Z}_p$ , it is clear the  $\theta$  is an onto function.

16. Let  $I$  and  $J$  be ideals in the commutative ring  $R$ , and define the function  $\phi : R \rightarrow R/I \oplus R/J$  by  $\phi(r) = (r + I, r + J)$ , for all  $r \in R$ .

(a) Show that  $\phi$  is a ring homomorphism, with  $\ker(\phi) = I \cap J$ .

*Solution:* The fact that  $\phi$  is a ring homomorphism follows immediately from the definitions of the operations in a direct sum and in a factor ring. Since the zero element of  $R/I \oplus R/J$  is  $(0 + I, 0 + J)$ , we have  $r \in \ker(\phi)$  if and only if  $r \in I$  and  $r \in J$ , so  $\ker(\phi) = I \cap J$ .

(b) Show that if  $I + J = R$ , then  $\phi$  is onto, and thus  $R/(I \cap J) \cong R/I \oplus R/J$ .

*Solution:* If  $I + J = R$ , then we can write  $1 = x + y$ , for some  $x \in I$  and  $y \in J$ . Given any element  $(a + I, b + J) \in R/I \oplus R/J$ , consider  $r = bx + ay$ , noting that  $a - r = a - bx - ay = ax - bx \in I$ , and  $b - r = b - bx - ay = by - ay \in J$ . Thus  $\phi(r) = (a + I, b + J)$ , and  $\phi$  is onto. The isomorphism follows from the fundamental homomorphism theorem.

17. Considering  $\mathbf{Z}[x]$  to be a subring of  $\mathbf{Q}[x]$ , show that these two integral domains have the same quotient field.

*Solution:* An element of the quotient field of  $\mathbf{Q}[x]$  has the form  $\frac{f(x)}{g(x)}$ , for polynomials  $f(x)$  and  $g(x)$  with rational coefficients. If  $m$  is the lcm of the denominators of the coefficients of  $f(x)$  and  $n$  is the lcm of the denominators of the coefficients of  $g(x)$ , then we have  $\frac{f(x)}{g(x)} = \frac{n}{m} \frac{h(x)}{k(x)}$  for  $h(x), k(x) \in \mathbf{Z}[x]$ , and this shows that  $\frac{f(x)}{g(x)}$  belongs to the quotient field of  $\mathbf{Z}[x]$ .

18. Let  $p$  be an odd prime number that is not congruent to 1 modulo 4. Prove that the ring  $\mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$  is a field.

*Hint:* Show that a root of  $x^2 = -1$  leads to an element of order 4 in the multiplicative group  $\mathbf{Z}_p^\times$ .

*Solution:* We must show that  $x^2 + 1$  is irreducible over  $\mathbf{Z}_p$ , or, equivalently, that  $x^2 + 1$  has no root in  $\mathbf{Z}_p$ .

Suppose that  $a$  is a root of  $x^2 + 1$  in  $\mathbf{Z}_p$ . Then  $a^2 \equiv -1 \pmod{p}$ , and so  $a^4 \equiv 1 \pmod{p}$ . The element  $a$  cannot be a root of  $x^2 - 1$ , so it does not have order 2, and thus it must have order 4. By Lagrange's theorem, this means that 4 is a divisor of the order of  $\mathbf{Z}_p^\times$ , which is  $p - 1$ . Therefore  $p = 4q + 1$  for some  $q \in \mathbf{Z}$ , contradicting the assumption.

