Example

Let $R = \mathbb{Z}$ and let I be the ideal $12\mathbb{Z}$. The quotient ring $\overline{R} = R/I = \mathbb{Z}/12\mathbb{Z}$ has ideals $\overline{R}$, $2\mathbb{Z}/12\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z}$, $6\mathbb{Z}/12\mathbb{Z}$, and $\overline{0} = 12\mathbb{Z}/12\mathbb{Z}$ corresponding to the ideals $R = \mathbb{Z}$, $2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, $6\mathbb{Z}$ and $12\mathbb{Z} = I$ of R containing I, respectively.

If I and J are ideals in the ring R then the set of sums $a + b$ with $a \in I$ and $b \in J$ is not only a subring of R (as in the Second Isomorphism Theorem for Rings), but is an *ideal* in R (the set is clearly closed under sums and $r(a + b) = ra + rb \in I + J$ since $ra \in I$ and $rb \in J$). We can also define the product of two ideals:

Definition. Let I and J be ideals of R.

(1) Define the *sum* of I and J by $I + J = \{a + b \mid a \in I,\ b \in J\}$.

(2) Define the *product* of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.

(3) For any $n \geq 1$, define the n^{th} *power* of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. Equivalently, I^n is defined inductively by defining $I^1 = I$, and $I^n = II^{n-1}$ for $n = 2, 3, \ldots$.

It is easy to see that the sum $I + J$ of the ideals I and J is the smallest ideal of R containing both I and J and that the product IJ is an ideal contained in $I \cap J$ (but may be strictly smaller, cf. the exercises). Note also that the elements of the product ideal IJ are *finite sums* of products of elements ab from I and J. The set $\{ab \mid a \in I,\ b \in J\}$ consisting just of products of elements from I and J is in general not closed under addition, hence is not in general an ideal.

Examples

(1) Let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$ in $\mathbb{Z}$. Then $I + J$ consists of all integers of the form $6x + 10y$ with $x, y \in \mathbb{Z}$. Since every such integer is divisible by 2, the ideal $I + J$ is contained in $2\mathbb{Z}$. On the other hand, $2 = 6(2) + 10(-1)$ shows that the ideal $I + J$ contains the ideal $2\mathbb{Z}$, so that $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$. In general, $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, where d is the greatest common divisor of m and n. The product IJ consists of all finite sums of elements of the form $(6x)(10y)$ with $x, y \in \mathbb{Z}$, which clearly gives the ideal $60\mathbb{Z}$.

(2) Let I be the ideal in $\mathbb{Z}[x]$ consisting of the polynomials with integer coefficients whose constant term is even (cf. Example 5). The two polynomials 2 and x are contained in I, so both $4 = 2 \cdot 2$ and $x^2 = x \cdot x$ are elements of the product ideal $I^2 = II$, as is their sum $x^2 + 4$. It is easy to check, however, that $x^2 + 4$ cannot be written as a single product $p(x)q(x)$ of two elements of I.

EXERCISES

Let R be a ring with identity $1 \neq 0$.

1. Prove that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

2. Prove that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

3. Find all homomorphic images of $\mathbb{Z}$.

4. Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. In each case describe the kernel and the image.
5. Describe all ring homomorphisms from the ring $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. In each case describe the kernel and the image.
6. Decide which of the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$:
   (a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$ (projection onto the 1,1 entry)
   (b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$ (the *trace* of the matrix)
   (c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$ (the *determinant* of the matrix).
7. Let $R = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{Z}\}$ be the subring of $M_2(\mathbb{Z})$ of upper triangular matrices. Prove that the map
$$\varphi : R \to \mathbb{Z} \times \mathbb{Z} \quad \text{defined by} \quad \varphi : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d)$$
is a surjective homomorphism and describe its kernel.
8. Decide which of the following are ideals of the ring $\mathbb{Z} \times \mathbb{Z}$:
   (a) $\{(a, a) \mid a \in \mathbb{Z}\}$
   (b) $\{(2a, 2b) \mid a, b \in \mathbb{Z}\}$
   (c) $\{(2a, 0) \mid a \in \mathbb{Z}\}$
   (d) $\{(a, -a) \mid a \in \mathbb{Z}\}$.
9. Decide which of the sets in Exercise 6 of Section 1 are ideals of the ring of all functions from [0,1] to $\mathbb{R}$.
10. Decide which of the following are ideals of the ring $\mathbb{Z}[x]$:
    (a) the set of all polynomials whose constant term is a multiple of 3
    (b) the set of all polynomials whose coefficient of x^2 is a multiple of 3
    (c) the set of all polynomials whose constant term, coefficient of x and coefficient of x^2 are zero
    (d) $\mathbb{Z}[x^2]$ (i.e., the polynomials in which only even powers of x appear)
    (e) the set of polynomials whose coefficients sum to zero
    (f) the set of polynomials $p(x)$ such that $p'(0) = 0$, where $p'(x)$ is the usual first derivative of $p(x)$ with respect to x.
11. Let R be the ring of all continuous real valued functions on the closed interval [0, 1]. Prove that the map $\varphi : R \to \mathbb{R}$ defined by $\varphi(f) = \int_0^1 f(t)dt$ is a homomorphism of additive groups but not a ring homomorphism.
12. Let D be an integer that is not a perfect square in $\mathbb{Z}$ and let $S = \{\begin{pmatrix} a & b \\ Db & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$.
    (a) Prove that S is a subring of $M_2(\mathbb{Z})$.
    (b) If D is not a perfect square in $\mathbb{Z}$ prove that the map $\varphi : \mathbb{Z}[\sqrt{D}] \to S$ defined by $\varphi(a + b\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix}$ is a ring isomorphism.
    (c) If $D \equiv 1 \bmod 4$ is squarefree, prove that the set $\{\begin{pmatrix} a & b \\ (D-1)b/4 & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ is a subring of $M_2(\mathbb{Z})$ and is isomorphic to the quadratic integer ring $\mathcal{O}$.

13. Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

14. Prove that the ring $M_4(\mathbb{R})$ contains a subring that is isomorphic to the real Hamilton Quaternions, $\mathbb{H}$.

15. Let X be a nonempty set and let $\mathcal{P}(X)$ be the Boolean ring of all subsets of X defined in Exercise 21 of Section 1. Let R be the ring of all functions from X into $\mathbb{Z}/2\mathbb{Z}$. For each $A \in \mathcal{P}(X)$ define the function

$$\chi_A : X \to \mathbb{Z}/2\mathbb{Z} \qquad \text{by} \qquad \chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

(χ_A is called the *characteristic function of* A with values in $\mathbb{Z}/2\mathbb{Z}$). Prove that the map $\mathcal{P}(X) \to R$ defined by $A \mapsto \chi_A$ is a ring isomorphism.

16. Let $\varphi : R \to S$ be a surjective homomorphism of rings. Prove that the image of the center of R is contained in the center of S (cf. Exercise 7 of Section 1).

17. Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.

(a) Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

(b) Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi(u^{-1}) = \varphi(u)^{-1}$ for each unit u of R.

18. **(a)** If I and J are ideals of R prove that their intersection $I \cap J$ is also an ideal of R.

(b) Prove that the intersection of an arbitrary nonempty collection of ideals is again an ideal (do not assume the collection is countable).

19. Prove that if $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of R then $\cup_{n=1}^{\infty} I_n$ is an ideal of R.

20. Let I be an ideal of R and let S be a subring of R. Prove that $I \cap S$ is an ideal of S. Show by example that not every ideal of a subring S of a ring R need be of the form $I \cap S$ for some ideal I of R.

21. Prove that every (two-sided) ideal of $M_n(R)$ is equal to $M_n(J)$ for some (two-sided) ideal J of R. [Use Exercise 6(c) of Section 2 to show first that the set of entries of matrices in an ideal of $M_n(R)$ form an ideal in R.]

22. Let a be an element of the ring R.

(a) Prove that $\{x \in R \mid ax = 0\}$ is a right ideal and $\{y \in R \mid ya = 0\}$ is a left ideal (called respectively the right and left *annihilators* of a in R).

(b) Prove that if L is a left ideal of R then $\{x \in R \mid xa = 0 \text{ for all } a \in L\}$ is a two-sided ideal (called the left *annihilator* of L in R).

23. Let S be a subring of R and let I be an ideal of R. Prove that if $S \cap I = 0$ then $\overline{S} \cong S$, where the bar denotes passage to R/I.

24. Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that if J is an ideal of S then $\varphi^{-1}(J)$ is an ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if J is an ideal of S then $J \cap R$ is an ideal of R.

(b) Prove that if φ is surjective and I is an ideal of R then $\varphi(I)$ is an ideal of S. Give an example where this fails if φ is not surjective.

25. Assume R is a commutative ring with 1. Prove that the Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

holds in R, where the binomial coefficient $\binom{n}{k}$ is interpreted in R as the sum $1+1+\cdots+1$ of the identity 1 in R taken $\binom{n}{k}$ times.

26. The *characteristic* of a ring R is the smallest positive integer n such that $1+1+\cdots+1=0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0. For example, $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n for each positive integer n and $\mathbb{Z}$ is a ring of characteristic 0.

(a) Prove that the map $\mathbb{Z} \to R$ defined by

$$k \mapsto \begin{cases} 1+1+\cdots+1 \ (k \text{ times}) & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1-1-\cdots-1 \ (-k \text{ times}) & \text{if } k < 0 \end{cases}$$

is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of the terminology "characteristic 0" instead of the archaic phrase "characteristic ∞" for rings in which no sum of 1's is zero).

(b) Determine the characteristics of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}/n\mathbb{Z}[x]$.

(c) Prove that if p is a prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

27. Prove that a nonzero Boolean ring has characteristic 2 (cf. Exercise 15, Section 1).

28. Prove that an integral domain has characteristic p, where p is either a prime or 0 (cf. Exercise 26).

29. Let R be a commutative ring. Recall (cf. Exercise 13, Section 1) that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements form an ideal — called the *nilradical* of R and denoted by $\mathfrak{N}(R)$. [Use the Binomial Theorem to show $\mathfrak{N}(R)$ is closed under addition.]

30. Prove that if R is a commutative ring and $\mathfrak{N}(R)$ is its nilradical (cf. the preceding exercise) then zero is the only nilpotent element of $R/\mathfrak{N}(R)$ i.e., prove that $\mathfrak{N}(R/\mathfrak{N}(R)) = 0$.

31. Prove that the elements $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent elements of $M_2(\mathbb{Z})$ whose sum is not nilpotent (note that these two matrices do not commute). Deduce that the set of nilpotent elements in the noncommutative ring $M_2(\mathbb{Z})$ is not an ideal.

32. Let $\varphi : R \to S$ be a homomorphism of rings. Prove that if x is a nilpotent element of R then $\varphi(x)$ is nilpotent in S.

33. Assume R is commutative. 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 $R[x]$.

(a) Prove that $p(x)$ is a unit in $R[x]$ if and only if a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent in R. [See Exercise 14 of Section 1.]

(b) Prove that $p(x)$ is nilpotent in $R[x]$ if and only if $a_0, a_1, \ldots, a_n$ are nilpotent elements of R.

34. Let I and J be ideals of R.

(a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

(b) Prove that IJ is an ideal contained in $I \cap J$.

(c) Give an example where $IJ \neq I \cap J$.

(d) Prove that if R is commutative and if $I + J = R$ then $IJ = I \cap J$.

35. Let I, J, K be ideals of R.

(a) Prove that $I(J+K) = IJ + IK$ and $(I+J)K = IK + JK$.

(b) Prove that if $J \subseteq I$ then $I \cap (J+K) = J + (I \cap K)$.