

CHAPTER 3

Rings

§29

Basic Definitions

In the preceding chapter, we have examined groups. Groups are sets with one binary operation on them. In this chapter, we want to study sets with two binary operations defined on them. The most fundamental algebraic structure with two binary operations is called a ring.

29.1 Definition: Let R be a nonempty set and let $+$ and \cdot be two binary operations defined on R . The ordered triple $(R, +, \cdot)$ is called a *ring* if the following conditions (ring axioms) are satisfied.

(i) For all $a, b \in R$, $a + b \in R$.

(ii) For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$.

(iii) There is an element in R , denoted by 0 , such that

$$a + 0 = a \text{ for all } a \in R.$$

(iv) For each $a \in R$, there is an element in R , denoted by $-a$,

such that

$$a + (-a) = 0.$$

(v) For all $a, b \in R$, $a + b = b + a$.

(1) For all $a, b \in R$, $a \cdot b \in R$.

(2) For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(D) For all $a, b, c \in R$, there hold

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

The conditions (i) and (1) assert that two binary operations $+$ and \cdot are defined on R . We shall refer to $+$ as *addition* and to \cdot as *multiplication*. Further, we shall call the element $a + b$ the *sum of a and b* , and the element ab the *product of a and b* . The conditions (i)-(v) say that R forms a group with respect to addition. The identity element 0 of this group will be called the *zero element*, or simply the *zero of R* . So 0 is an element of the set R and not necessarily the number zero. The inverse element $-a$ of $a \in R$ is called the *opposite of a* .

The condition (2) states that the multiplication on R is associative. The condition (D) relates the two binary operations $+$ and \cdot . It is called the distributivity of multiplication over addition. Here it should be noted that $a \cdot b + a \cdot c$ stands for $(a \cdot b) + (a \cdot c)$ and similarly $b \cdot a + c \cdot a$ for $(b \cdot a) + (c \cdot a)$. Notice that there are two equations in (D), and we must check both of them when we want to show that a given ordered triple $(R, +, \cdot)$ is a ring. In general, neither of them implies the other, and it is not enough to check one of them. There are ordered triples $(R, +, \cdot)$ for which all the conditions above are satisfied, except for one of the equations in (D), and they fail to be a ring just for that reason.

For ease of notation, we shall frequently denote multiplication by juxtaposition and thus write ab in place of $a \cdot b$. Also, we shall write $a - b$ for $a + (-b)$. Since multiplication in a ring is associative, the products of elements in a ring are independent of the mode of inserting parentheses and the usual exponentiation rules are valid (see §8). We shall use the results of §8 without explicit mention.

29.2 Examples: (a) Let $(R, +)$ be any commutative group, whose identity element we shall denote as 0 . We define a multiplication on R by declaring

$$ab = 0 \quad \text{for all } a, b \in R.$$

It is easily seen that $(R, +, \cdot)$ is a ring.

(b) A more interesting ring is $(\mathbb{Z}, +, \cdot)$, where $+$ and \cdot are the usual addition and multiplication of integers.

(c) Let $2\mathbb{Z}$ denote the set of even integers. Then $(2\mathbb{Z}, +, \cdot)$, where $+$ and \cdot are the usual addition and multiplication of integers, is a ring. In the same way, if $n \in \mathbb{N}$ and $n\mathbb{Z}$ is the set of integers divisible by n , then $(n\mathbb{Z}, +, \cdot)$ is a ring.

(d) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ are rings under the usual addition and multiplication.

(e) Let $R := \{a/b \in \mathbb{Q} : (a, b) = 1 \text{ and } 5 \nmid b\}$. With respect to the usual addition and multiplication of rational numbers, $(R, +, \cdot)$ is a ring.

(f) Let $S := \{a/b \in \mathbb{Q} : (a, b) = 1 \text{ and } 6 \nmid b\}$. With respect to the usual addition and multiplication of rational numbers, $(S, +, \cdot)$ is a not ring. The very first property (i) is not satisfied. For example

$$\frac{1}{2} \in S, \quad \frac{1}{3} \in S, \quad \text{but } \frac{1}{2} + \frac{1}{3} = \frac{5}{6} \notin S.$$

(g) Let p be a prime number and put $T = \{a/b \in \mathbb{Q} : (a, b) = 1 \text{ and } p \nmid b\}$. With respect to the usual addition and multiplication of rational numbers, $(T, +, \cdot)$ is a ring.

(h) Let R be a ring. A *matrix over R* is an array $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of four elements a, b, c, d of R , arranged in two rows and two columns and enclosed within parentheses. The set of all matrices over R will be denoted by $Mat_2(R)$. If $A, B \in Mat_2(R)$, we say A is equal to B provided the corresponding entries in A and B are equal and write $A = B$ in this case. This is clearly an equivalence relation on $Mat_2(R)$.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in Mat_2(R)$. The sum $A + B$ of A and B is defined to be the matrix $\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$ and the product AB of A and B is defined to be the matrix $\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$.

The proof of Theorem 17.4 remains valid and shows that $Mat_2(R)$ is a commutative group under addition. The proof of Theorem 17.6(1),(2),(4) is also valid and establishes the ring axioms (1),(2),(D). So $(Mat_2(R), +, \cdot)$ is a ring.

(i) Let K be the set of all real-valued functions defined on the closed interval $[0,1]$. We define operations $+$ and \cdot on K by

$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x)g(x) \quad \text{for all } x \in [0,1]$$

($f, g \in K$). So $f+g$ is that function that maps any $x \in [0,1]$ to the sum of the values $f(x)$ and $g(x)$ of the functions f and g at x ; and $f \cdot g$ is that function that maps any $x \in [0,1]$ to the product of the values $f(x)$ and $g(x)$. In " $f+g$ ", the sign "+" stands for the binary operation $+$ we just defined, and in " $f(x) + g(x)$ ", the sign "+" stands for the usual addition of real numbers. It is easily verified that $(K,+, \cdot)$ is a ring. The sum $f+g$ and the product $f \cdot g$ are said to be defined *pointwise*. The operations $+$ and \cdot are called *pointwise addition* and *pointwise multiplication*.

(j) Let S be any set and let $(R,+, \cdot)$ be any ring. Let L denote the set of all functions from S into R . For $f, g \in L$, we put

$$(f+g)(s) = f(s) + g(s), \quad (f \cdot g)(s) = f(s)g(s) \quad \text{for all } s \in S.$$

On the right, we have the sum (product) of elements $f(s), g(s)$ in R , on the left, we have the operations on L . The operations $+$ and \cdot on L are called *pointwise addition* and *pointwise multiplication*. With these operations, $(L,+, \cdot)$ is a ring.

Let us find the zero elements of the rings in Example 29.2. This is the identity element of the commutative group R in Example 29.2(a); the number zero in the Examples 29.2(b),(c),(d),(e),(f),(g) except in the case \mathbb{Z}_n of Example 29.2(d), where the zero element is the residue class $\bar{0} \in \mathbb{Z}_n$ of $0 \in \mathbb{Z}$; the so-called zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \text{Mat}_2(R)$, where 0 is the zero element of R in Example 29.2(h). In the ring of Example 29.2(i), the zero element is the function $\zeta: [0,1] \rightarrow \mathbb{R}$ for which $\zeta(x) = 0$ for all $x \in [0,1]$; and in the ring of Example 29.2(j), the zero element is the function $u: S \rightarrow R$ for which $u(s) = 0$ for all $s \in S$.

We make a convention. As in the case of groups, if $(R,+, \cdot)$ is a ring, and if it is clear from what the binary operations $+$ and \cdot are, we shall call the set R a ring. Hence we shall speak of the ring \mathbb{Z} instead of using the more correct but more cumbersome expression "the ring $(\mathbb{Z},+, \cdot)$ ", etc.

The addition in a ring has all the desirable properties one could wish for: it is associative, there is an identity element, all elements possess inverses, and it is also commutative. As for multiplication, only one of these properties, namely the associativity, is assumed to be satisfied. It may happen, of course, that multiplication in a ring has some of these properties. Then we make the following definitions.

29.3 Definition: A ring R is called a *commutative ring* if $ab = ba$ for all $a, b \in R$.

29.4 Definition: A ring R is called a *ring with identity* if there is an element e in R such that $ae = ea = a$ for all $a \in R$.

Thus a ring is a commutative ring if the multiplication on it is commutative. This is a natural definition: since addition is commutative in any ring, commutativity can refer only to multiplication. \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , $2\mathbb{Z}$ and \mathbb{Z}_n are examples of commutative rings. $Mat_2(\mathbb{Z})$ is not a commutative ring because, for instance,

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Likewise, a ring with identity is a ring with a multiplicative identity. The additive identity exists in any ring anyway. Notice that e in Definition 29.4 must be both a right identity and a left identity. Since multiplication in a ring is not necessarily commutative, we cannot conclude, say, from

$$ae = a \quad \text{for all } a \in R$$

that the other condition

$$ea = a \quad \text{for all } a \in R$$

also holds. In the case of groups, we proved that a right identity is also a left identity, but in the proof we made use of the existence of inverse elements. We cannot use the same argument in the case of rings, for we do not know anything about the existence of inverse elements. They may or may not exist for all $a \in R$. It is possible that a ring R has an element f such that

$$af = a \quad \text{for all } a \in R$$

but

$$fb \neq b \quad \text{for some } b \in R.$$

In short, R may have a multiplicative right identity which is not a left identity. If each right identity in a ring fails to be a left identity, then the ring is not a ring with identity.

These remarks make sense only for noncommutative rings. Of course, in a commutative ring, any right (left) identity is also a left (right) identity.

A ring may be commutative without having an identity: $2\mathbb{Z}$ is an example. A ring may have an identity without being commutative: $Mat_2(\mathbb{Z})$ is an example. An identity of this ring is the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. More generally, if R is a ring with an identity e , then $Mat_2(R)$ is a ring with an identity $\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}$. The proof of Theorem 17.6(3) works here without change.

29.5 Lemma: *Let R be a ring with identity. Then its multiplicative identity is unique (i.e., there is one and only one element e such that $ea = ae = a$ for all $a \in R$).*

Proof: If e and f are identity elements of R , then $e = ef$ since f is a right identity and $ef = f$ since e is a left identity, so $e = ef = f$. \square

In view of this lemma, we can speak of *the* identity. We shall follow the convention of writing 1 for the multiplicative identity of a ring with identity. 1 is therefore an element of the ring under study, and not necessarily the number one. For instance, in the ring $Mat_2(\mathbb{Z})$, the element 1 is the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the identity matrix. The ring K of Example 29.2(i) is a ring with identity, and one checks easily that 1 here is the function $h: [0,1] \rightarrow \mathbb{R}$ such that $h(x) = 1$ (real number one) for all $x \in [0,1]$.

What about the existence of multiplicative inverses? Of course the ring must be a ring with identity if we are to speak about multiplicative inverses. We will see presently that the additive identity 0 of a ring cannot have a multiplicative inverse unless the ring is idiosyncratic.

29.6 Lemma: *Let R be a ring and 0 its zero element.*

- (1) $a0 = 0$ for all $a \in R$.
- (2) $0a = 0$ for all $a \in R$.
- (3) $a(-b) = -(ab)$ for all $a, b \in R$.
- (4) $(-a)b = -(ab)$ for all $a, b \in R$.
- (5) $(-a)b = a(-b)$ for all $a, b \in R$.
- (6) $(-a)(-b) = ab$ for all $a, b \in R$.

Proof: (1) Since 0 is the additive identity of R , we have $0 + 0 = 0$. Thus

$$\begin{aligned} a(0 + 0) &= a0 \quad \text{for all } a \in R, \\ a0 + a0 &= a0 \quad \text{for all } a \in R. \end{aligned}$$

By Lemma 7.3(1), $a0$ must be the identity of the group $(R, +)$. Thus $a0 = 0$.

(2) This is proved by the same argument, using $0a + 0a = (0 + 0)a = 0a$.

(3) For any $a, b \in R$, we have

$$0 = a0 = a(b + (-b)) = ab + a(-b).$$

So $a(-b)$ is the additive inverse of ab . The additive inverse of ab is $-(ab)$ by definition. Hence $a(-b) = -(ab)$.

(4) For any $a, b \in R$, we have

$$0 = 0b = (a + (-a))b = ab + (-a)b.$$

So $(-a)b$ is the additive inverse of ab . The additive inverse of ab is $-(ab)$. Hence $(-a)b = -(ab)$.

(5) This follows from (3) and (4).

(6) This follows from (5) on writing $-b$ for b and observing $-(-b) = b$. \square

29.7 Lemma: *Let R be a ring with identity 1. If the zero element 0 of R has an inverse (i.e., if there is an element $t \in R$ such that $0t = t0 = 1$), then R has only one element.*

Proof: If $r \in R$, then $r = r1 = r(0t) = (r0)t = 0t = 0$, so $R \subseteq \{0\}$, so $R = \{0\}$. \square

The set $\{0\}$ can be made into a ring if we define $+$ and \cdot in the only possible way: $0 + 0 = 0$ and $0 \cdot 0 = 0$. This is a commutative ring with

identity, the multiplicative identity being the additive identity 0. This ring is called the *null ring*.

29.8 Lemma: *Let R be a ring with identity 1. If R is not the null ring, then $1 \neq 0$.*

Proof: If R is not the null ring, then there is an $r \in R$, $r \neq 0$. Then the assumption $1 = 0$ leads to the contradiction $r = r1 = r0 = 0$. So $1 \neq 0$.

□

Lemma 29.7 states that 0 in a ring cannot possess a multiplicative inverse unless the ring is the null ring. We now want to show that divisors of 0 cannot possess a multiplicative inverses, either.

29.9 Definition: Let R be a ring. If $a \neq 0$, $b \neq 0$ are elements of R such that $ab = 0$, then a is called a *left zero divisor* and b is called a *right zero divisor*.

It may very well happen that $a \neq 0$, $b \neq 0$, but $ab = 0$ in a ring. For example, in the ring $Mat_2(\mathbb{Q})$ of matrices over \mathbb{Q} ,

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 0, \text{ but } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

As a second example, consider the ring K of real-valued functions on $[0,1]$ with respect to pointwise addition and multiplication (Example 29.2(i)). The zero element in this ring is the function ζ , where $\zeta(x) = 0 \in \mathbb{R}$ for all $x \in [0,1]$. The functions a and b , where

$$a(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq 1/2 \\ 1 & \text{if } 1/2 < x \leq 1 \end{cases}, \quad b(x) = \begin{cases} 1 & \text{if } 0 \leq x \leq 1/2 \\ 0 & \text{if } 1/2 < x \leq 1 \end{cases}$$

are thus distinct from ζ , but their pointwise product is ζ , as $a(x)b(x) = 0$ for all $x \in [0,1]$.

In a commutative ring, there is no distinction between right and left zero divisors. But in a non commutative ring, an element $a \neq 0$ may be a right zero divisor without being a left zero divisor, and vice versa.

29.10 Lemma: *Let R be a ring with identity. If a is a left zero divisor, then a does not have a multiplicative left inverse. If a is a right zero divisor, then a does not have a multiplicative right inverse.*

Proof: Let 1 be the identity of R . If a is left zero divisor, then $a \neq 0$ and there is a $b \neq 0$ in R such that $ab = 0$. Now if a had a left inverse x , so that $xa = 1$, we would obtain $b = 1b = (xa)b = x(ab) = x0 = 0$, a contradiction. So a has no left inverse. The second statement is proved analogously. \square

We know that the zero element in a ring distinct from the null ring cannot have an inverse and we understand from Lemma 29.10 that being a zero divisor is the very opposite of having an inverse. So if we want a ring to have the property that every nonzero element in it has a multiplicative inverse, the ring has to be free from zero divisors.

29.11 Definition: A commutative ring with identity, which is distinct from the null ring, and which has no zero divisors, is called an *integral domain*.

29.12 Definition: A ring with identity, which is distinct from the null ring, and in which every nonzero element has a right inverse, is called a *division ring*.

An integral domain is therefore a ring in which we may expect that nonzero elements have inverses, but nothing is said about the actual existence of inverses. The necessary condition that zero divisors be absent is satisfied in an integral domain, plus commutativity. Whether the nonzero elements do in fact have inverses is not relevant in the definition of integral domains.

In a division ring, every nonzero element does have a right inverse; more precisely, a right inverse. But this means that the nonzero elements in a division ring form a group under multiplication. We know

that, in any group, right inverses are also left inverses and that they are unique (Lemma 7.3). Hence, in a division ring, every nonzero element has a left inverse as well, and the right and left inverse of an arbitrary element coincide. This will be called *the* inverse of that element.

\mathbb{Z} is an integral domain. In fact, \mathbb{Z} is the prototype of all integral domains. $2\mathbb{Z}$ is not an integral domain, because $2\mathbb{Z}$ is not a ring with identity, although $2\mathbb{Z}$ is commutative and has no zero divisors. An example of division rings is given in Ex. 9.

A ring which is both an integral domain and a division ring deserves a name.

29.13 Definition: A commutative ring with identity, which is distinct from the null ring, and in which every nonzero element has a multiplicative inverse, is called a *field*.

Thus a field is a commutative division ring. Also, a field is an integral domain in which every nonzero element does have an inverse. A field is a ring in which the nonzero elements form a commutative group under multiplication.

\mathbb{Z} is not a field, since $2 \in \mathbb{Z}$, for instance, does not have an inverse in \mathbb{Z} (there is no $z \in \mathbb{Z}$ such that $2z = 1$). Thus \mathbb{Z} is an integral domain which is not a field. The rings \mathbb{Q} , \mathbb{R} , \mathbb{C} , and \mathbb{Z}_p (where p is a prime number) are example of fields, so Definition 17.1 is consistent with Definition 29.13. There are fields with finitely many elements as well as with infinitely many elements.

29.14 Definition: Let R be a ring with identity. An element $a \in R$ of R is said to be a *unit of R* if a has both a right inverse and a left inverse in R . The set of all units in R will be denoted by R^\times .

For example, the units of \mathbb{Z} are 1 and -1, so $\mathbb{Z}^\times = \{1, -1\}$. The units in \mathbb{Z}_n are the residue classes \bar{a} for which there is a $\bar{b} \in \mathbb{Z}_n$ such that $\bar{a}\bar{b} = \bar{1}$, and this holds if and only if $(a, n) = 1$. Hence $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n : (a, n) = 1\}$, as in §11. We know that $\mathbb{Z}^\times = \{1, -1\}$ and \mathbb{Z}_n^\times are groups under multiplication (Theorem 12.4). These are special cases of the following theorem.

29.15 Theorem: *Let R be a ring with identity. Then R^\times is a group under multiplication.*

Proof: We denote the identity of R by 1. Since $1 \cdot 1 = 1$, we have $1 \in R^\times$ and so $R^\times \neq \emptyset$. We now show that any unit of R has a unique right inverse, which is also the unique left inverse of that unit. Let $a \in R^\times$, let x be any right inverse of a and let y be any left inverse of a . Then $ax = 1 = ya$ and

$$y = y1 = y(ax) = (ya)x = 1x = x.$$

Thus any right inverse of a is equal to y . Hence there is only one right inverse of a , namely x . Then any left inverse of a is also equal to x . Hence there is a unique left inverse of a , namely the unique right inverse x of a .

We check the group axioms.

(i) If $a, b \in R^\times$, then there are uniquely determined elements x, z in R with $ax = 1 = xa$ and $bz = 1 = zb$. From

$$(ab)(zx) = a(bz)x = a1x = ax = 1, \quad (zx)(ab) = z(xa)b = z1b = zb = 1,$$

we see that zx is both a right inverse and a left inverse of ab . Hence $ab \in R^\times$ and R^\times is closed under multiplication.

(ii) The multiplication on R^\times is associative since R is a ring.

(iii) Since $a1 = a = 1a$ for all $a \in R$, and since $1 \in R^\times$, we see that 1 is the identity element of R^\times .

(iv) If $a \in R^\times$, then there is an $x \in R$ with $ax = 1 = xa$. This x is in fact an element of R^\times : it follows from $ax = 1 = xa$ that a is a left and right inverse of x , so $x \in R^\times$. So any $a \in R^\times$ has an inverse in R^\times .

Thus R^\times is a group under multiplication. □

The reader will check easily that, if R is a ring with identity, distinct from the null ring, then R is a division ring if and only if $R^\times = R \setminus \{0\}$. Likewise, if K is a commutative ring with identity, distinct from the null ring, then K is a field if and only if $K^\times = K \setminus \{0\}$.

From now on we will write $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ for the multiplicative groups $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ of nonzero rational, real, complex numbers, respectively.

We conclude this paragraph with the binomial theorem.

29.16 Theorem (Binomial Theorem) : *Let R be a ring and $a, b \in R$. If*

$$ab = ba, \text{ then } (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$

Proof: First we remark that $a^n b^0$ and $a^0 b^n$ are to be interpreted as a^n and b^n respectively, even if R has no identity. As usual, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ and $0! = 1$. We use the formula $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ for $1 \leq k \leq n-1$.

We make induction on n . The formula $(a + b)^1 = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1$ is clearly true. We suppose that the formula is proved when the exponent of $a + b$ is n . Then

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n = (a + b) \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \\ &= \sum_{k=0}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1} \\ &= \binom{n}{0} a^{n+1} b^0 + \sum_{k=1}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} + \binom{n}{n} a^0 b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} b^0 + \sum_{k=1}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^n \binom{n}{k-1} a^{n-(k-1)} b^k + \binom{n+1}{n+1} a^0 b^{n+1} \end{aligned}$$

$$\begin{aligned}
&= \binom{n+1}{0} a^{n+1} b^0 + \sum_{k=1}^n \left(\binom{n}{k} + \binom{n}{k-1} \right) a^{n+1-k} b^k + \binom{n+1}{n+1} a^0 b^{n+1} \\
&= \binom{n+1}{0} a^{n+1} b^0 + \sum_{k=1}^n \binom{n+1}{k} a^{n+1-k} b^k + \binom{n+1}{n+1} a^0 b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k
\end{aligned}$$

and the formula is true when the exponent of $a + b$ is $n + 1$. This completes the proof. \square

Exercises

1. Let $X = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ and $Y = \{a + b\sqrt[3]{2} : a, b \in \mathbb{Z}\}$. Determine whether X and Y are rings under the usual addition and multiplication of real numbers.

2. Let $(R, +, \cdot)$ be a ring. On the group $(R, +)$, we define an operation \circ by declaring $a \circ b = ba$ for all $a, b \in R$. Show that $(R, +, \circ)$ is a ring (called the *opposite ring* of $(R, +, \cdot)$).

3. On the group $\mathbb{Z} \oplus \mathbb{Z}$, we define a multiplication by

$$(a, b) \cdot (c, d) = (ac, b)$$

for all $(a, b), (c, d) \in \mathbb{Z} \oplus \mathbb{Z}$. Does $\mathbb{Z} \oplus \mathbb{Z}$ become a ring with this multiplication?

4. Show that the set $A = \{a/b \in \mathbb{Q} : (a, b) = 1, n \nmid b\}$ is not a ring (under the usual addition and multiplication of rational numbers) if n is a composite number.

5. Prove that \mathbb{Z}_n has zero divisors if n is composite, and that \mathbb{Z}_n is a field if n is prime.

6. On the group $R = \mathbb{Z} \oplus \mathbb{Z}$, we define a multiplication by

$$(a,b) \cdot (c,d) = (ac, ad)$$

for all $(a,b), (c,d) \in \mathbb{Z} \oplus \mathbb{Z}$. Prove that, with this multiplication, R becomes a ring. Show that $(1,0)$ is a left identity in R , but not a right identity; and that $(1,0)$ is a right zero divisor, but not a left zero divisor. Is R a ring with identity?

7. Let R be a ring without identity, and let $S = R \oplus \mathbb{Z}$. On the commutative group S , we define a multiplication by

$$(r,a) \cdot (r',b) = (rr' + ar' + br, ab)$$

for all $(r,a), (r',b) \in S$. Prove that S is a ring with identity.

8. On the group $R = \mathbb{Z}_n \oplus \mathbb{Z}_n$, we define a multiplication by

$$(\bar{a}, \bar{b}) \cdot (\bar{c}, \bar{d}) = (\overline{ac - bd}, \overline{ad + bc})$$

for all $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}) \in R$. Show that R is a commutative ring with identity. Prove that R is a field when $n = 3, 7, 11$ and that R is not an integral domain if $n = 5, 13, 17$.

9. Let $H = \left\{ \begin{pmatrix} a & -b \\ \bar{b} & a \end{pmatrix} : a, b \in \mathbb{C} \right\} \subseteq \text{Mat}_2(\mathbb{C})$. Prove that, under the usual matrix addition and multiplication, H is a division ring (cf. §17, Ex. 14).

10. Let R_1, R_2, \dots, R_n be rings. Prove that the group $R_1 \oplus R_2 \oplus \dots \oplus R_n$ becomes a ring if multiplication is defined by

$$(r_1, r_2, \dots, r_n)(s_1, s_2, \dots, s_n) = (r_1 s_1, r_2 s_2, \dots, r_n s_n)$$

for all $(r_1, r_2, \dots, r_n), (s_1, s_2, \dots, s_n) \in R_1 \oplus R_2 \oplus \dots \oplus R_n$. Moreover, prove that $R_1 \oplus R_2 \oplus \dots \oplus R_n$ is a commutative ring if and only if each R_k is; and that $R_1 \oplus R_2 \oplus \dots \oplus R_n$ is a ring with identity if and only if each R_k is. The ring $R_1 \oplus R_2 \oplus \dots \oplus R_n$ is called the *direct sum of* R_1, R_2, \dots, R_n .