4. Rings

4.1. Definition and examples

A group is an algebraic system with one binary operation. The familiar examples of real numbers and 2×2 matrices are systems which involve two binary operations. In this chapter we study algebraic systems with two binary operations. We start considering the system $\mathbf{Z}$ of integers. $\mathbf{Z}$ has two binary operations "+" and "$\cdot$" $(\mathbf{Z}, +)$ is an abelian group. Multiplication is an associative binary operation in $\mathbf{Z}$. These two binary operations are connected by the two distributive laws given by $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$. A generalisation of these basic properties in $\mathbf{Z}$ leads us to the concept of a system called ***ring***.

Definition. A nonempty set R together with two binary operations denoted by "+" and "$\cdot$" and called addition and multiplication which satisfy the following axioms is called a ***ring***.

(i) $(R, +)$ is an abelian group.

(ii) "$\cdot$" is an associative binary operation on R.

(iii) $a\cdot(b+c) = a\cdot b+a\cdot c$ and $(a+b)\cdot c = a\cdot c+b\cdot c$ for all $a, b, c, \in R$.

Notation. The unique identity of the additive group $(R, +)$ is denoted by 0 and is called the ***zero element*** of the ring and the unique additive *inverse of a* is denoted by $-a$.

Examples

1. $(\mathbf{Z}, +, \cdot)$; $(\mathbf{Q}, +, \cdot)$; $(\mathbf{R}, +, \cdot)$; $(\mathbf{C}, +, .)$ are all rings.

2. $(2\mathbf{Z}, +, \cdot)$ is a ring.

3. Let $R = \{a + b\sqrt{2}/a, b \in \mathbf{Z}\}$.

   Clearly R is an abelian group under usual addition.

   Let $a + b\sqrt{2}$ and $c + d\sqrt{2} \in R$. Then

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \in R.$$

   Since the two binary operations are the usual addition and multiplication, the distributive laws and the associative law hold.
   Thus R is a ring with usual addition and multiplication.

4. Let $R = \{a + ib/a, b \in \mathbf{Z}\}$. Then R is a ring under usual addition and multiplication. This ring is called the ***ring of Gaussian integers***. In general, any subset of complex numbers which is a group under addition and is closed for multiplication is a ring (Verify).

5. $\{0\}$ with binary operations '+' and '$\cdot$' defined as $0 + 0 = 0$ and $0.0 = 0$ is a ring. This is called the ***null ring***.

6. In $\mathbf{R} \times \mathbf{R}$ we define $(a, b) + (c, d) = (a+c, b+d)$ and $(a, b)\cdot(c, d) = (ac, bd)$. Here $(\mathbf{R} \times \mathbf{R}, +)$ is an abelian group. The identity is $(0, 0)$ and the inverse of (a, b) is $(-a, -b)$.

   Further $(a, b)[(c, d) + (e, f)]$

$$= (a, b)(c + e, d + f)$$
$$= (ac + ae, bd + bf)$$
$$= (ac, bd) + (ae, bf)$$
$$= (a, b)(c, d) + (a, b)(e, f).$$

   Similarly $[(a, b) + (c, d)](e, f)$

$$= (a, b)(e, f) + (c, d)(e, f).$$

   Hence $(\mathbf{R} \times \mathbf{R}, +, \cdot)$ is a ring.

7. Let $(R, +)$ be any abelian group with identity 0.

   We define multiplication in R by $ab = 0$ for all $a, b \in R$. Clearly $a(bc) = 0 = (ab)c$ so that multiplication is associative.

Also $a(b+c) = 0 = ab + ac$ and

$$(a+b)c = 0 = ac + bc.$$

Hence R is a ring under these operations. This ring is called the ***zero ring***.

This example shows that any abelian group with identity 0 can be made into a ring by defining $ab = 0$.

8. $(\mathbf{Z}_n, \oplus, \odot)$ is a ring, for, we know that $(\mathbf{Z}_n, \oplus)$ is an abelian group and $\odot$ is an associative binary operation.

We now prove the distributive laws.

Let $a, b, c \in \mathbf{Z}_n$.

Then $b \oplus c \equiv (b+c) \pmod{n}$.

Hence $a \odot (b \oplus c) \equiv a(b+c) \pmod{n}$.

Also $a \odot b \equiv ab \pmod{n}$ and $a \odot c \equiv ac \pmod{n}$ so that

$(a \odot b) \oplus (a \odot b) \equiv (ab + ac) \pmod{n}$.

Since $a \odot (b \oplus c)$ and $(a \odot b) \oplus (a \odot c) \in \mathbf{Z}_n$, we have $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

Similarly $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

Hence $(\mathbf{Z}_n, \oplus, \odot)$ is a ring.

9. $(\wp(S), \Delta, \cap)$ is a ring. We know that $(\wp(S), \Delta)$ is an abelian group (refer example 12 of section 3.1).

Also $\cap$ is an associative binary operation on $\wp(S)$.

It can easily be verified that

$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$ and

$(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$.

Hence $(\wp(S), \Delta, \cap)$ is a rifg.

0. $M_2(\mathbf{R})$ under matrix addition and multiplication is a ring.

1. Let R be the set of all real functions. We define addition and multiplication by

$(f+g)(x) = f(x) + g(x)$ and

$(fg)(x) = f(x)g(x)$.

Then R is a ring.

Clearly addition of functions is associative and commutative.

The constant function $\mathbf{0}$ defined by $\mathbf{0}(x) = 0$, is the zero element of R and $-f$ is the additive inverse of f.

Hence R is an abelian group.

The associativity of multiplication and the distributative laws are consequences of the corresponding properties in $\mathbf{R}$. Hence R is a ring.

12. Let A be any abelian group. Let $Hom\,(A)$ be the set of all endomorphisms of A.

Let $f, g \in Hom(A)$. We define

$f + g$ by $(f+g)(x) = f(x) + g(x)$ and $fg = f \circ g$. Then $Hom\,(A)$ is a ring.

Proof. Let $f, g \in Hom(A)$.

Then
$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y)\\ &= f(x) + f(y) + g(x) + g(y)\\ &= f(x) + g(x) + f(y) + g(y)\\ &= (f+g)(x) + (f+g)(y).\end{aligned}$$

Hence $f + g \in Hom(A)$.

Obviously $+$ is associative.

Since A is an abelian group $f + g = g + f$.

If 0 is the identity element of the group A then the homomorphism $\mathbf{0}$ defined by $\mathbf{0}(a) = 0$, for all $a \in A$ is the zero element of $Hom(A)$.

Now, let $f \in Hom(A)$. The function $-f$ defined by $(-f)(x) = -[f(x)]$ is also a homomorphism, since

$$\begin{aligned}(-f)(x+y) &= -[f(x+y)]\\ &= -[f(x) + f(y)]\\ &= (-f)(x) + (-f)(y).\end{aligned}$$

Clearly $f + (-f) = 0$ and hence $-f$ is the additive inverse of f.

Thus $Hom(A)$ is an abelian group.

Now, $(f \circ g)(x+y)$

$= f[g(x+y)]$

$= f[g(x)+g(y)]$

$= f[g(x)] + f[g(y)]$

$= (f \circ g)(x) + (f \circ g)(y)$.

Hence $f \circ g \in Hom(A)$.

Similarly $(f+g) \circ h = f \circ h + g \circ h$.

Thus $Hom(A)$ is a ring.

13. Let Q be the set of all symbols of the form $a_0+a_1i+a_2j+a_3k$ where $a_0, a_1, a_2, a_3 \in \mathbf{R}$. Two such symbols $a_0 + a_1i + a_2j + a_3k$ and $b_0 + b_1i + b_2j + b_3k$ are defined to be equal iff $a_i = b_i, i = 0, 1, 2, 3$. We now make Q into a ring by defining $+$ and $\cdot$ as follows.

For any $x = a_0 + a_1i + a_2j + a_3k$ and $y = b_0 + b_1i + b_2j + b_3k$,

$$\begin{aligned} x+y &= (a_0 + a_1i + a_2j + a_3k) \\ &\quad + (b_0 + b_1i + b_2j + b_3k) \\ &= (a_0+b_0) + (a_1+b_1)i \\ &\quad + (a_2+b_2)j + (a_3+b_3)k \text{ and} \\ xy &= (a_0 + a_1i + a_2j + a_3k) \\ &\quad (b_0 + b_1i + b_2j + b_3k) \\ &= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) \\ &\quad + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i \\ &\quad + (a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3)j \\ &\quad + (a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1)k. \end{aligned}$$

The formula for the product comes from multiplying the two symbols formally and collecting the terms using the relations

$i^2 = j^2 = k^2 = ijk = -1, ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$.

Clearly $+$ is associative and commutative.

$0 = 0 + 0i + 0j + 0k$ is the zero element.

$-a_0 - a_1i - a_2j - a_3k$ is the additive inverse of $a_0 + a_1i + a_2j + a_3k$.

The associative law of multiplication and the two distributative laws can be easily verified.

Hence $(\mathbf{Q}, +, \cdot)$ is a ring.

This ring is called the ***ring of quaternions***.

14. The set R of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in \mathbf{R}$ is a ring under matrix addition and matrix multiplication.

Proof. Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in R$.

Then

$$A+B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R.$$

$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+ac) & ac-bd \end{pmatrix} \in R.$$

Clearly matrix addition is commutative and associative.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ is the zero element.

$\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$ is the inverse of the matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Further matrix multiplication is associative and the distributive laws are valid for 2×2 matrices.

Hence R is a ring.

Exercises

1. Prove that the set of all real numbers of the form $a + b\sqrt{3}$ where $a, b \in \mathbf{Q}$ under usual addition and multiplication is a ring.

2. Prove that the set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ where $a \in \mathbf{R}$ is a ring under matrix addition and multiplication.
3. Show that $(\mathbf{Z}, \oplus, \odot)$ is a ring where
$$a \oplus b = a + b - 1 \quad \text{and}$$
$$a \odot b = a + b - ab.$$
4. Shqw that $(n\mathbf{Z}, +, \cdot)$ is a ring.
5. Verify whether the sets $\{0, 1\}$ and $\{a, b\}$ are rings with operations defined by the following tables.

(a)

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

(b)

+	a	b
a	a	b
b	b	a

·	a	b
a	a	b
b	a	b

6. Construct the Cayley tables for the ring $(\wp(S), \Delta, \cap)$ when $S = \{1, 2\}$.
7. Show that $(2\mathbf{Z}, +, *)$ is a ring where $+$ is usual addition and $*$ is given by $a * b = \frac{1}{2}ab$.
8. In $\mathbf{R} \times \mathbf{R}$ define $(a, b)+(c, d) = (a+c, b+d)$ and $(a, b)(c, d) = (ac - bd, bc + ad)$. Show that $(\mathbf{R} \times \mathbf{R}, +, \cdot)$ is a ring.
9. Let $S = \{iy / y \in \mathbf{R}\}$. Is S a ring with usual addition and multiplication?
10. Is $(\wp(S), \cup, \cap)$ a ring?
11. Is $(\wp(S), \Delta, \cup)$ a ring?
12. In $\mathbf{Q}$ we define $a \oplus b = ab$ and $a \odot b = a + b$. Show that $(\mathbf{Q}, \oplus, \odot)$ is not a ring.
13. Determine which of the following statements are true and which are false.
    (a) The set of all even integers is a ring under usual addition and multiplication.
    (b) The set of all odd integers is a ring under usual addition and multiplication.
    (c) In any ring addition is commutative.
    (d) The non-zero elements of a ring form a group under multiplication.

Answers.

5. (a) Ring (b) Not a ring 9. No 10. No. 11. No.
13. (a) T (b) F (c) T (d) F

4.2. Elementary properties of rings

Theorem 4.1. Let R be a ring and $a, b \in R$. Then

(i) $0a = a0 = 0$ (ii) $a(-b) = (-a)b = -(ab)$

(iii) $(-a)(-b) = ab$ (iv) $a(b - c) = ab - ac$.

Proof. (i) $a0 = a(0 + 0) = a0 + a0$.

$\therefore a0 = 0$. (by cancellation law in $(R, +)$)

Similarly $0a = 0$.

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

$\therefore \quad a(-b) = -(ab)$.

Similarly, $(-a)b = -(ab)$.

(iii) By (ii), $(-a)(-b) = -[a(-b)] = -(-ab)$
$= ab$.

(iv) $a(b - c) = a[b + (-c)] = ab + a(-c)$
$= ab - ac$.

Solved problems

Problem 1. If R is a ring such that $a^2 = a$ for all $a \in R$, prove that

(i) $a + a = 0$ (ii) $a + b = 0 \Rightarrow a = b$ (iii) $ab = ba$

Proof. (i) $a + a = (a + a)(a + a)$

$= a(a + a) + a(a + a)$

$= aa + aa + aa + aa$

$= (a + a) + (a + a)$ (since $a^2 = a$)

Hence $a + a = 0$.

(ii) Let $a + b = 0$. By (i) $a + a = 0$.

$\therefore \quad a + b = a + a$ so that $a = b$.

(iii) $a+b=(a+b)(a+b)$
$=a(a+b)+b(a+b)$
$=aa+ab+ba+bb$
$=a+ab+ba+b.$

Hence $ab+ba=0$, so that by (ii), $ab=ba$.

Note. A ring R is called a ***Boolean ring*** if $a^2=a$ for all $a\in R$. For example $(\wp(S), \Delta, \cap)$ is a Boolean ring.

Problem 2. Complete the Cayley table for the ring $R=\{a,b,c,d\}$

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			a
d	a	b	c	

Solution. First we shall compute cb.

$cb=(b+d)b$ (from addition table)
$=bb+db$
$=b+b$ (from multiplication table)
$=a.$ (from addition table)

Now, $cc=c(b+d)=cb+cd=a+a=a.$
$bc=(b+d)c=cc+dc=a+c=c.$
$bd=b(b+c)=bb+bc=b+c=d.$
$dd=(b+c)d=bd+cd=d+a=d.$

Hence the completed table for multiplication is

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

Exercises

1. Given any positive integer n show that there exists a ring with n elements.
2. Let R be a ring and n any positive integer. Let $a_1, a_2, \ldots\ldots\ldots\ldots, a_n \in R$. Prove that
$$(-a_1)(-a_2)\ldots\ldots(-a_n) = \begin{cases} a_1a_2\ldots\ldots a_n & \text{if } n \text{ is even} \\ -a_1a_2\ldots\ldots a_n & \text{if } n \text{ is odd} \end{cases}$$
3. Complete the Cayley table for the ring $R=\{a,b,c,d\}$.

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			c
d	a	b	c	

Show that in this ring $xx=x$ for all $x\in R$.
4. Prove by induction that
$$a(b_1+b_2+\cdots+b_n)=ab_1+ab_2+\cdots+ab_n.$$

4.3. Isomorphism

In the study of any algebraic system, the idea of two systems being structurally the same is of basic importance. In algebra, this concept is always called ***isomorphism***. As in the case of groups, isomorphism between two rings can be defined as follows.

Definition. Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be two rings. A bijection $f: R\to R'$ is called an ***isomorphism*** if

(i) $f(a+b)=f(a)+f(b)$ and
(ii) $f(ab)=f(a)f(b)$ for all $a,b\in R$.

If $f: R\to R'$ is an isomorphism, we say that R is isomorphic to R' and we write $R\approx R'$.

Note. Let R and R' be two rings and $f: R\to R'$ be an isomorphism. Then clearly f is an isomorphism of the group $(R,+)$ to the group $(R',+)$.

Hence $f(0)=0'$ and $f(-a)=-f(a)$.

Examples

1. $f : \mathbf{C} \to \mathbf{C}$ defined by $f(z) = \bar{z}$ is an isomorphism. For, clearly f is a bijection.

   Also

   $$f(z_1 + z_2) = \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$$

   $$= f(z_1) + f(z_2), \text{ and}$$

   $$f(z_1 z_2) = \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} = f(z_1) f(z_2).$$

2. Let $\mathbf{C}$ be the ring of complex numbers. Let S be the set of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in \mathbf{R}$. Then S is a ring under matrix addition and matrix multiplication. Refer example 14 in 4.1. Now the mapping $f : \mathbf{C} \to S$ defined by $f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an isomorphism.

   Clearly f is a bijection. Now let $x = a + ib$ and $y = c + id$.

   $$f(x + y) = f[(a + c) + i(b + d)]$$

   $$= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

   $$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

   $$= f(x) + f(y).$$

   Similarly $f(xy) = f(x) f(y)$. (verify).

3. The groups $(\mathbf{Z}, +)$ and $(2\mathbf{Z}, +)$ are isomorphic under the map $f : \mathbf{Z} \to 2\mathbf{Z}$, given by $f(x) = 2x$.
   However f is not an isomorphism of the ring $(\mathbf{Z}, +)$ to $(2\mathbf{Z}, +, \cdot)$ since $f(xy) = 2xy$ and $f(x) f(y) = 2x2y = 4xy$ so that $f(xy) \neq f(x) f(y)$.
   In fact there is no isomorphism between the rings $(\mathbf{Z}, +, \cdot)$ and $(2\mathbf{Z}, +, \cdot)$(verify).

Exercises

1. In $2\mathbf{Z}$ we define $a * b = \frac{1}{2}ab$. Show that $(2\mathbf{Z}, +, *)$ is a ring isomorphic to $(\mathbf{Z}, +, \cdot)$.
2. Let S be the set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ where $a \in \mathbf{R}$. Show that $f : \mathbf{R} \to S$ given by $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is an isomorphism.
3. Verify whether $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = -x$ is an isomorphism.
4. Let $A = \{(a, b, c) / a, b, c \in \mathbf{R}\}$. Define $(a, b, c) + (x, y, z) = (a + x, b + y, c + z)$ and $(a, b, c) \cdot (x, y, z) = (ax, ay + bz, cz)$. Show that $(A, +, \cdot)$ is a ring.
5. Let S be the set of all matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. Show that S is a ring under matrix addition and matrix multiplication.
6. Show that the rings given in exercises 4 and 5 are isomorphic.

4.4. Types of rings

Compared with addition in R, the multiplication in R is relatively unknown to us. For example the definition of a ring does not guarantee the existence of an identity with respect to multiplication. The ring $(2\mathbf{Z}, +, \cdot)$ has no multiplicative identity. Even if a ring has a multiplicative identity some elements of the ring may not have multiplicative inverses. For example, the ring $(\mathbf{Z}, +, \cdot)$ has 1 as a multiplicative identity and all the elements of $\mathbf{Z}$ except 1 and -1 do not have multiplicative inverses.

Again in a ring R, the multiplication need not be commutative. For example, in the ring of 2×2 matrices matrix multiplication is not commutative. Hence we get several special classes of rings by imposing conditions on the multiplicative structure.

Definition. A ring R is said to be ***commutative*** if $ab = ba$ for all $a, b \in R$.

Examples

1. The familiar rings $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ are all commutative. The following are examples of non-commutative rings.

2. Let F denote the set of all functions from $\mathbf{R}$ to $\mathbf{R}$. We define $(f+g)(x) = f(x) + g(x)$ and $f \cdot g = f \circ g$. Then $(F, +, \cdot)$ is non-commutative ring.

3. The ring of quaternions given in example 13 of 4.1 is a non- commutative ring since $ij = k$ and $ji = -k$.

4. $M_2(\mathbf{R})$ is a non-commutative ring.

Exercises Determine which of the rings given in section 4.1 are commutative.

Answers. 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14 are commutative rings.

Definition. Let R be a ring. We say that R is a ***ring with identity*** if there exists an element $1 \in R$ such $a1 = 1a = a$ for all $a \in R$.

Examples

1. The familiar rings $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ are all rings with identity.

2. $(n\mathbf{Z}, +, \cdot)$ when $n > 1$ is a ring which has no identity.

3. $M_2(\mathbf{R})$ is a ring with identity.

Exercises Determine which of the rings given in section 4.1 are rings with identity.

Answers. 1, 3, 4, 6, 8, 9, 10, 11, 12, 13 and 14 are rings with identity.

Note. Consider the null ring $\{0\}$. In this case 0 is both additive identity and multiplicative identity. This is the only case where 0 can act as the multiplicative identity, for if 0 is the multiplicative identity in a ring R, then $0a = a$ for all $a \in R$. But in any ring $0a = 0$. Hence $a = 0$, so that $R = \{0\}$. In what follows we will exclude this trivial case when speaking of the multiplicative identity. Hence whenever we speak of a multiplicative identity in a ring, we assume that the multiplicative identity is not 0.

Theorem 4.2. In a ring with identity the identity element is unique.

Proof. Let $1, 1'$ be multiplicative identities.

Then $1 \cdot 1' = 1$ (considering $1'$ as identity)

and $1 \cdot 1' = 1'$ (considering 1 as identity)

$\therefore \quad 1 = 1'$. Hence the identity element is unique.

Definition. Let R be a ring with identity. An element $u \in R$ is called a ***unit*** in R if it has a multiplicative inverse in R. The multiplicative inverse of u is denoted by u^{-1}.

For example, in $(\mathbf{Z}, +, \cdot)$, 1 and -1 are units.

In $M_2(\mathbf{R})$, all the non-singular matrices are units.

In $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ every non-zero element is a unit.

Theorem 4.3. Let R be a ring with identity. The set of all units in R is a group under multiplication.

Proof. Let U denote the set of all units in R.

Clearly $1 \in U$. Let $a, b \in U$.

Hence a^{-1}, b^{-1} exists in R.

Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1}$

$= aa^{-1} = 1$.

Similarly $(b^{-1}a^{-1})(ab) = 1$.

Hence $ab \in U$.

Also $(a^{-1})^{-1} = a$ and hence $a \in U \Rightarrow a^{-1} \in U$.

Hence U is a group under multiplication.

Exercises Find all the units in the rings given in section 4.1

Answers. 1. In $\mathbf{Z}$, 1 and -1 are units; $\mathbf{Q}^*$, $\mathbf{R}^*$ and $\mathbf{C}^*$ are the units in $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ respectively. 2. Nil 3. 1 and -1, 4. $1, i, -1, -i$. 5. Nil 6. $\mathbf{R}^* \times \mathbf{R}^*$. 7. Nil. 8. $\{a/a \in \mathbf{Z}_n$ and $(a, n) = 1\}$. 9. S. 10. All non-singular matrices. 11. All bijections. 12. All automorphisms 13. $\mathbf{Q}^*$ 14. $\mathbf{R}^*$.

Definition. Let R be a ring with identity element. R is called a ***skew field*** or a ***division ring*** if every non-zero element in R is a unit.

(ie) For every non-zero element $a \in R$, there exists a multiplicative inverse $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Thus in a skew field the non-zero elements form a group under multiplication.

Definition. A commutative skew field is called a *field*.

In other words a field is a system $(F, +, \cdot)$ satisfying the following conditions.

(i) $(F, +)$ is an abelian group.
(ii) $(F - \{0\}, \cdot)$ is an abelian group.
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Examples

1. **Q**, **R** and **C** are fields under usual addition and multiplication.

2. Let p be a prime. Then $(\mathbf{Z}_p, \oplus, \odot)$ is field.

   Proof. $(\mathbf{Z}_p, \oplus, \odot)$ is a ring (by example 8 of 4.1)
   Also since p is prime $(\mathbf{Z}_p - \{0\}, \odot)$ is an abelian group. (refer example 23 of 3.1).
   Hence $(\mathbf{Z}_p, \oplus, \odot)$ is a field.

3. Let M be the set of all matrices of the form $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ where $a, b, \in \mathbf{C}$. Then M is a skew field under matrix addition and matrix multiplication.

   Proof. Let $A, B \in M$.

   Let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ and

   $B = \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$. Then

   $$A + B = \begin{pmatrix} a + b & b + d \\ -\bar{b} - \bar{d} & \bar{a} + \bar{c} \end{pmatrix}$$
   $$= \begin{pmatrix} a+c & b+d \\ -\overline{(b+d)} & \overline{a+c} \end{pmatrix} \in M.$$

   Hence M is closed under matrix addition.
   Obviously matrix addition is associative and commutative.
   $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element of M.
   $\begin{pmatrix} -a & -b \\ \bar{b} & -\bar{a} \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$.
   Hence M is an abelian group under matrix addition.
   Now,

   $$AB = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$$
   $$= \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \overline{ac} \end{pmatrix}$$

   which is of the form $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$.
   Hence M is closed under matrix multiplication.
   Further matrix multiplication is associative and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ is the multiplicative identity.
   Now, let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ be a non-zero matrix in M.
   Then either $a \neq 0$ or $b \neq 0$ so that either $|a| > 0$ or $|b| > 0$.
   Hence $|A| = a\bar{a} + b\bar{b} = |a|^2 + |b|^2 > 0$.
   Thus A is a non-singular matrix and hence has an inverse and $A^{-1} \in M$. Thus M is a skew field. Also since matrix multiplication is not commutative, M is not a field.

4. Let Q be the ring of quarternions given in example 13 of section 4.1. Q is a skew field but not a field.

   Proof. We have proved that $(Q, +, \cdot)$ is a ring.
   $1 = 1 + 0i + 0j + 0k$ is the identity element.
   Let $x = a_0 + a_1 i + a_2 j + a_3 k$ be a non-zero element in Q.
   Then not all of a_0, a_1, a_2, a_3 are zero.
   Let $\alpha = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Clearly $\alpha \neq 0$.

Let

$y = (a_0/\alpha) - (a_1/\alpha)i - (a_2/\alpha)j - (a_3/\alpha)k$.

Now, $y \in Q$ and $xy = yx = 1$. (verify).

Thus Q is a skew field.

In Q, multiplication is not commutative since $ij = k$ and $ji = -k$. Hence Q is not a field.

5. $(\mathbf{Z}, +, \cdot)$ is a commutative ring with identity but not a field since 1 and -1 are the only non-zero elements which have inverses.

Theorem 4.4. In a skew field R,

(i) $ax = ay, a \neq 0 \Rightarrow x = y$
(ii) $xa = ya, a \neq 0 \Rightarrow x = y$
} (cancellation laws in ring)
(iii) $ax = 0 \Leftrightarrow a = 0$ or $x = 0$.

Proof. (i) Let $ax = ay$ and $a \neq 0$.

Since R is a skew field there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Hence $ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay)$
$\Rightarrow x = y$.

(ii) can be proved similarly.

(iii) If $a = 0$ or $x = 0$, then clearly $ax = 0$.

Conversely let $ax = 0$ and $a \neq 0$.

$\therefore \quad ax = a0$.

$\therefore \quad x = 0$ by (i).

Note. Thus in a skew field the product of two non-zero elements is again a non-zero element. However this is not true in an arbitrary ring. For example,

1. Consider the ring $(\mathbf{R} \times \mathbf{R}, +, \cdot)$ where '+' and '$\cdot$' are defined by

$$(a, b) + (c, d) = (a + c, b + d) \text{ and}$$
$$(a, b) \cdot (c, d) = (ac, bd).$$

$\mathbf{R} \times \mathbf{R}$ is a commutative ring with identity. Here $(1, 0)(0, 1) = (0, 0)$.

2. The product of two non-zero matrices can be equal to the zero matrix. For example, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Definition. Let R be a ring. A non-zero element $a \in R$ is said to be a **zero-divisor** if there exists a non-zero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Examples

1. In the ring $\mathbf{R} \times \mathbf{R}$, $(1, 0)$ and $(0, 1)$ are zero divisors, since $(1, 0)(0, 1) = (0, 0)$. In fact all the elements of the form $(a, 0)$ and $(0, a)$ where $a \neq 0$ are zero divisors.

2. In the ring of matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ are zero-divisors, since $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

3. In the ring $\mathbf{Z}_{12}$, 3 is a zero-divisor, since $3 \odot 4 = 0$. Also 2, 4, 6 are zero-divisors.

4. In the ring of integers, no element is a zero-divisor.

5. No skew field has any zero-divisor.

Theorem 4.5. A ring R has no zero-divisors iff cancellation law is valid in R.

Proof. Let R be a ring without zero-divisors.

Let $ax = ay$ and $a \neq 0$.

$\therefore \quad ax - ay = 0$. Hence $a(x - y) = 0$ and $a \neq 0$.

$\therefore \quad x - y = 0$ (since R has no zero-divisors).

$\therefore \quad x = y$. Thus cancellation laws is valid in R.

Conversely let the cancellation law be valid in R.

Let $ab = 0$ and $a \neq 0$. Then $ab = 0 = a0$.

Hence by cancellation law $b = 0$.

Hence R has no zero-divisors.

Theorem 4.6. Any unit in R cannot be a zero-divisor.

Proof. Let $a \in R$ be a unit.

Then $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow b = 0$.

Similarly $ba = 0 \Rightarrow b = 0$.

Hence a cannot be a zero-divisor.

Note. The converse of the above result is not true. (ie.,) a is not a zero-divisor does not imply a is a unit.

For example, in $\mathbf{Z}$, 2 is not a zero-divisor and 2 is not a unit.

Definition. A commutative ring with identity having no zero-divisors is called in ***integral domain***.

Thus in an integral domain $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

Or equivalently $ab = 0$ and $a \neq 0 \Rightarrow b = 0$; or $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Examples

1. $\mathbf{Z}$ is an integral domain.
2. $n\mathbf{Z}$ where $n > 1$ is not an integral domain since the ring $n\mathbf{Z}$ does not have an identity.
3. $\mathbf{Z}_{12}$ is not an integral domain since 4 is a zero-divisor in $\mathbf{Z}_{12}$.
4. $\mathbf{Z}_7$ is an integral domain.

Theorem 4.7. $\mathbf{Z}_n$ is an integral domain iff n is prime.

Proof. Let $\mathbf{Z}_n$ be an integral domain.

We claim that n is prime. Suppose n is not prime.

Then $n = pq$ where $1 < p < n$ and $1 < q < n$.

Clearly $p \odot q = 0$.

Hence p and q are zero-divisors.

$\therefore$ $\mathbf{Z}_n$ is not an integral domain which is a contradiction. Hence n is prime.

Conversely, suppose n is prime. Let $a, b \in \mathbf{Z}_n$.

Then $a \odot b = 0 \Rightarrow ab = qn$ where $q \in \mathbf{Z}_n$.

$\Rightarrow n|ab$

$\Rightarrow n|a$ or $n|b$ (since n is prime)

$\Rightarrow a = 0$ or $b = 0$.

$\therefore$ $\mathbf{Z}_n$ has no zero-divisors.

Also $\mathbf{Z}_n$ is a commutative ring with identity.

Hence $\mathbf{Z}_n$ is an integral domain.

Theorem 4.8. Any field F is an integral domain.

Proof. It is enough if we prove that F has no zero-divisors.

Let $a, b \in F, ab = 0$ and $a \neq 0$.

Since F is a field a^{-1} exists.

Now, $ab = 0 \Rightarrow a^{-1}(ab) = 0$

$\Rightarrow b = 0$.

$\therefore$ F has no zero-divisors.

Hence F is an integral domain.

Note. The converse of the above theorem is not true. (ie) An integral domain need not be a field.

For example $\mathbf{Z}$ is an integral domain but not a field.

Theorem 4.9. Let R be a commutative ring with identity 1. Then R is an integral domain iff the set of non-zero elements in R is closed under multiplication.

Proof. Let R be an integral domain.

Let $a, b \in R - \{0\}$.

Since R has no zero-divisors $ab \neq 0$ so that $R - \{0\}$ is closed under multiplication.

Conversely, suppose $R - \{0\}$ is closed under multiplication. Then the product of any two non-zero elements is a non-zero element. Hence R has no zero-divisors so that R is an integral domain.

Theorem 4.10. Let R be a commutative ring with identity. Then R is an integral domain iff cancellation law is valid in R.

Proof. The result is an immediate consequence of Theorem 4.5.

Theorem 4.11. Any finite integral domain is a field.

Proof. Let R be a finite integral domain. We need only to prove that every non-zero element in R has a multiplicative inverse.

Let $a \in R$ and $a \neq 0$.

Let $R = \{0, 1, a_1, a_2, \ldots\ldots, a_n\}$.

Consider $\{a1, aa_1, aa_2, \ldots\ldots, aa_n\}$.

By Theorem 4.9 all these elements are non-zero and all these elements are distinct by Theorem 4.10.

Hence $aa_i = 1$ for some $a_i \in R$

Since R is commutative, $aa_i = a_i a = 1$ so that $a_i = a^{-1}$.

Hence R is a field.

Remark. The above result is not true for an infinite integral domain. For example consider the ring of integers. It is an integral domain but not a field.

Theorem 4.12. $\mathbf{Z}_n$ is a field iff n is prime.

Proof. By theorem 4.7, $\mathbf{Z}_n$ is an integral domain iff n is prime.

Further $\mathbf{Z}_n$ is finite. Hence the result follows from Theorem 4.11.

Theorem 4.13. A finite commutative ring R without zero-divisors is a field.

Proof. If we prove that R has an identity element then R becomes an integral domain and hence by Theorem 4.11 it is a field. So we prove the existence of identity.

Let $R = \{0, a_1, \ldots\ldots\ldots, a_n\}$.

Let $a \in R$ and $a \neq 0$.

Then the elements $aa_1, aa_2, \ldots\ldots\ldots, aa_n$, are distinct and non-zero.

$\therefore$ $aa_i = a$ for some i.

Since R is commutative we have $aa_i = a_i a = a$.

We now prove that a_i is the identity element of R.

Let $b \in R$. Then $b = aa_j$ for some j.

$\therefore$ $a_i b = a_i(aa_j) = (a_i a)a_j = aa_j = b$.

Thus $a_i b = ba_i = b$.

Since $b \in R$ is arbitrary, a_i is the identity of R.

Hence the theorem.

Solved problems

Problem 1. Prove that the set F of all real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbf{Q}$ is a field under the usual addition and multiplication of real numbers.

Solution. Obviously, $(F, +)$ is an abelian group with 0 as the zero element.

Now, let $a + b\sqrt{2}$ and $c + d\sqrt{2} \in F$. Then

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in F.$$

Since the two binary operations are the usual addition and multiplication of real numbers, multiplication is associative and commutative and the two distributive laws are true.

$1 = 1+0\sqrt{2} \in F$ and is the multiplicative identity.

Now, let $a + b\sqrt{2} \in F - \{0\}$.

Then a and b are not simultaneously 0.

$$\text{Also } \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}.$$

We claim that $a^2 - 2b^2 \neq 0$.

Case (i) $a \neq 0$ and $b = 0$, then $a^2 - 2b^2 = a^2 \neq 0$.

Case (ii) $a = 0$ and $b \neq 0$, then $a^2 - 2b^2 = -2b^2 \neq 0$.

Case (iii) $a \neq 0$ and $b \neq 0$. Suppose $a^2 - 2b^2 = 0$.

Then $a^2 = 2b^2$ so that $a^2/b^2 = 2$.

Hence $a/b = \pm\sqrt{2}$.

Now, $a/b \in \mathbf{Q}$ and $\sqrt{2} \notin \mathbf{Q}$. This is a contradiction.

Hence $a^2 - 2b^2 \neq 0$.

$$\therefore \quad \frac{1}{a+b\sqrt{2}} = \left(\frac{a}{a^2-2b^2}\right) - \left(\frac{b}{a^2-2b^2}\right)\sqrt{2} \in F$$

and is the inverse of $a + b\sqrt{2}$.

Hence F is a field.

Problem 2. $\mathbf{Z}$ is the ring of integers and R is any ring.

Then $\mathbf{Z} \times R = \{(m, x)/m \in \mathbf{Z}$ and $x \in R\}$. We define $\oplus$ and $\odot$ on $\mathbf{Z} \times R$ as follows. $(m, x) \oplus (n, y) = (m+n, x+y)$; $(m, x) \odot (n, y) = (mn, my+nx+xy)$ where nx and my denote respectively the concerned multiples of the elements x and y in R. Prove that $\mathbf{Z} \times R$ is a ring under $\oplus$ and $\odot$. Also prove that $\mathbf{Z} \times R$ is commutative iff R is commutative.

Solution. Clearly $\mathbf{Z} \times R$ is an abelian group under $\oplus$ with $(0, 0)$ as the identity element and the additive inverse of (m, x) is $(-m, -x)$. Clearly $\mathbf{Z} \times R$ is closed under $\odot$.

Let $(m, x), (n, y), (p, z) \in \mathbf{Z} \times R$.

$$[(m, x) \odot (n, y)] \odot (p, z)$$
$$= (mn, my + nx + xy) \odot (p, z)$$
$$= (mnp, mnz + p(my + bx + xy) + (my + nx + xy)z)$$
$$= (mnp, mnz + pmy + pnx + pxy + myz + nxz + xyz)$$

Now, $(m, x) \odot [(n, y) \odot (p, z)]$
$$= (m, x) \odot (np, nz + py + yz)$$
$$= (mnp, m(nz + py + yz) + npx + x(nz + py + yz))$$
$$= (mnp, mnz + mpy + myz + npx + nzx + pxy + xyz)$$

Hence $\odot$ is associative.

Now, $(m, x) \odot (1, 0) = (m, x)$ and

$(1, 0) \odot (m, x) = (m, x)$

$\therefore$ $(1, 0)$ is the identity element of $\mathbf{Z} \times R$.

Now, $(m, x) \odot [(n, y) \oplus (p, z)]$
$= (m, x) \odot (n + p, y + z)$
$= (m(n + p), m(y + z) + (n + p)x + x(y + z))$
$= (mn + mp, my + mz + nx + px + xy + xz)$
$= (mn + mp, my + nx + xy + mz + px + xz)$
$= (mn, my + nx + xy) \oplus (mp, mz + px + xz)$
$= (m, x) \odot (n, y) \oplus (m, x) \odot (p, z)$

$\therefore$ Left distributive law is true.

Similarly we can verify the right distributive law,

$$[(m, x) \oplus (n, y)] \odot (p, z)$$
$$= (m, x) \odot (p, z) \oplus (n, y) \odot (p, z)$$

Hence $\mathbf{Z} \times R$ is a ring with identity.

Suppose R is commutative.

Then $(m, x) \odot (n, y) = (mn, my + nx + xy)$
$= (nm, nx + my + yx)$
(since R is commutative $xy = yx$)
$= (n, y) \odot (m, x)$

$\therefore$ $\mathbf{Z} \times R$ is commutative.

Conversely, suppose $\mathbf{Z} \times R$ is commutative.

Hence $(m, x) \odot (n, y) = (n, y) \odot (m, x)$

$(mn, my + nx + xy) = (nm, nx + my + yx)$

Hence $my + nx + xy = nx + my + yx$
$= my + nx + yx$

$\therefore$ $xy = yx$

$\therefore$ R is commutative.

Problem 3. Give examples of

(i) a finite commutative ring with identity which is not an integral domain.
(ii) a finite non-commutative ring.
(iii) an infinite non-commutative ring with identity. (iv) an infinite ring having no identity.

Solution.

(i) $A = (\mathbf{Z}_4, \oplus, \odot)$ is a finite commutative ring with identity 1.
We have $2 \odot 2 = 0$. Thus 2 is a zero-divisor in A and hence A is not as integral domain.

(ii) Consider the set $M_2(\mathbf{Z}_3)$ of all matrices with entries from $\mathbf{Z}_3$. Clearly $M_2(\mathbf{Z}_3)$ is finite and is also a ring under matrix addition and multiplication.

Further $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$ and hence $M_2(\mathbf{Z}_3)$ is non-commutative.

(iii) $M_2(\mathbf{R})$ is an infinite non-commutative ring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(iv) $(2\mathbf{Z}, +, \cdot)$ is an infinite ring with no identity.

Problem 4. Prove that the only idempotent elements of an integral domain are 0 and 1.

Solution. Let R be an integral domain.

Let $a \in R$ be an idempotent element.

Then $a^2 = a$ so that $a^2 - a = a(a - 1) = 0$.

Since R has no zero-divisors,

$$a(a-1)=0 \Rightarrow a=0 \text{ or } a-1=0.$$

Hence $a=0$ or $a=1$.

Hence 0 and 1 are the only idempotent elements of R.

Problem 5. Let F be a finite field with n elements. Prove that $a^n=a$ for all $a \in F$.

Solution. If $a=0$, then obviously $a^n=a=0$.

Hence, let $a \neq 0$.

Since F is a field, $F-\{0\}$ is a group under multiplication and $|F-\{0\}|=n-1$.

Hence $a^{n-1}=1$ (by Theorem 3.35)

$\therefore \quad a^n=a$.

Problem 6. Prove that in the case of a ring with identity the axiom $a+b=b+a$ is redundant. (ie.,) The axiom $a+b=b+a$ can be derived from the other axioms of the ring.

Solution. Using the two distributive laws of a ring.

$$\begin{aligned}(1+1)(a+b) &= 1(a+b)+1(a+b)\\ &= a+b+a+b \text{ and}\\ (1+1)(a+b) &= (1+1)a+(1+1)b\\ &= a+a+b+b.\end{aligned}$$

$$\therefore \quad a+b+a+b=a+a+b+b.$$

Hence $b+a=a+b$ (by cancellation laws).

Problem 7. If the additive group of a ring R is cyclic prove that R is commutative. Deduce that a ring with 7 elements is commutative.

Solution. $(R,+)$ is a cyclic group.

Let $R=\langle a\rangle$. Let $x, y \in R$.

Then $x=ma$ and $y=na$ where $m, n \in \mathbf{Z}$.

Now, $xy=mana$

$$\begin{aligned}&= (\underbrace{a+a+\ldots\ldots+a}_{m \text{ times}})(\underbrace{a+a+\ldots\ldots+a}_{n \text{ times}})\\ &= mn\,a^2=nm\,a^2=na\,ma\\ &= yx.\end{aligned}$$

Hence R is a commutative ring.

Now, let R be a ring with 7 elements.

Then $(R,+)$ is a group of order 7.

Hence $(R,+)$ is cyclic.

Hence R is commutative.

Problem 8. Let R and R' be rings and $f: R \to R'$ be an isomorphism. Then

(i) R is commutative $\Rightarrow R'$ is commutative.

(ii) R is ring with identity $\Rightarrow R'$ is a ring with identity.

(iii) R is an integral domain $\Rightarrow R'$ is an integral domain.

(iv) R is a field $\Rightarrow R'$ is a field.

Solution. (i) Let $a', b' \in R'$. Since f is onto, there exists $a, b \in R$ such that $f(a)=a'$ and $f(b)=b'$. Now,

$$\begin{aligned}a'b' &= f(a)f(b)\\ &= f(ab) \text{ (since } f \text{ is an isomorphism)}\\ &= f(ba) \text{ (since } R \text{ is a commutative ring)}\\ &= f(b)f(a)\\ &= b'a'.\end{aligned}$$

$\therefore \quad R'$ is a commutative ring.

(ii) Let $1 \in R$ be the identity element of R.

Let $a' \in R'$. Then there exists $a \in R$ such that $f(a)=a'$.

Now, $f(1)a'=f(1)f(a)=f(1a)$

$$=f(a)=a'.$$

Similarly $a'f(1)=a'$ and hence $f(1)$ is the identity element in R'.

$\therefore \quad R'$ is a ring with identity.

(iii) Let R be an integral domain. Then by (i) and (ii), R' is a commutative ring with identity.

Now, we prove that R' has no zero-divisors.

Let $a', b' \in R'$ and let $a'b'=0$.

Since f is onto there exist $a, b \in R$ such that $f(a)=a'$ and $f(b)=b'$.

$\therefore \quad a'b' = 0 \Rightarrow f(a)f(b) = 0.$

$\Rightarrow f(ab) = 0$

$\Rightarrow ab = 0$ (since f is 1-1)

$\Rightarrow a = 0$ or $b = 0$

(since R is an integral domain)

$\Rightarrow f(a) = 0$ or $f(b) = 0.$

$\Rightarrow a' = 0$ or $b' = 0.$

$\therefore \quad R'$ is an integral domain.

(iv) We need to prove that every non-zero element in R' has an inverse. Let $a' \in R'$ and $a' \neq 0$.

Then there exists $a \in R - \{0\}$ such that $f(a) = a'$

Now, $f(a^{-1})a' = f(a^{-1})f(a)$

$= f(a^{-1}a) = f(1).$

Hence $f(a^{-1})$ is the inverse of a'.

Problem 9. Prove that the only isomorphism $f : \mathbf{Q} \to \mathbf{Q}$ is the identity map.

Solution. Since f is an isomorphism $f(0) = 0$ and $f(1) = 1$. Now, let n be a positive integer.

$f(n) = f(1 + 1 + \ldots + 1)$ (written n times)

$= f(1) + f(1) + \ldots + f(1)$ (written n times)

$= 1 + 1 + \ldots\ldots + 1$ (written n times)

$= n.$

Now, if n is a negative integer, let $n = -m$ where $m \in \mathbf{N}$.

Then $f(n) = f(-m) = -f(m) = -m = n.$

Thus for any integer n, $f(n) = n$.

Now, let $a \in \mathbf{Q}$. Then $a = p/q$ where $p, q \in \mathbf{Z}$.

Hence

$f(a) = f(p/q) = f(pq^{-1}) = f(p)f(q^{-1})$

$f(p)[f(q)]^{-1} = pq^{-1} = p/q = a.$

Hence f is the identity map.

Exercises

1. Give examples of
   (a) a commutative ring with zero divisors.
   (b) a non-commutative ring with zero divisors.
   (c) an integral domain which is not a field.
   (d) a skew field which is not a field.
   (e) a commutative ring with identity which is not an integral domain.
2. Prove that a ring R is commutative iff for all $a, b \in R$, $(a + b)^2 = a^2 + 2ab + b^2$.
3. In $\mathbf{R} \times \mathbf{R}$ we define $+$ and $\cdot$ by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Prove that $\mathbf{R} \times \mathbf{R}$ is a field. [Multiplicative inverse of (a, b) is $(a/(a^2 + b^2), -b/(a^2 + b^2))$].
4. Prove that if a ring R is both an integral domain and a skew field then it is a field.
5. Prove that $\{0, 1, a, b\}$ is a field under the operations defined by the following Cayley tables.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

6. Prove that the set of all real numbers of the form $a + \sqrt[3]{7}\, b + \sqrt[3]{49}\, c$ where $a, b, c \in \mathbf{Q}$ forms an integral domain under usual addition and multiplication.
7. Prove that the set of all 2×2 matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ where $a, b \in \mathbf{Z}$ forms a commutative ring with unity under matrix addition and matrix multiplication but is not an integral domain.
8. Determine which of the following are true and which are false.

(a) Any field is an integral domain.

(b) In any integral domain every non-zero element has an inverse.

(c) $\mathbf{Z}_5$ is a field.

(d) $3\mathbf{Z}$ is an integral domain.

(e) Set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ where $a, b \in \mathbf{R}$ is a ring.

(f) Every ring has a multiplicative identity.

(g) The non-zero elements of a field is a group under multiplication.

(h) Any finite commutative ring has an identity.

(i) $\{0\}$ is an integral domain.

(j) Any commutative skew field is a field.

(k) A ring can have more than one multiplicative identity.

(l) Any ring with identity is commutative.

(m) Any ring with odd number of elements is commutative.

(n) The set of all 2×2 non-singular matrices with entries from $\mathbf{R}$ is a skew field under matrix addition and matrix multiplication.

Answers.

8. (a) T (b) F (c) T (d) F (e) T (f) F (g) T (h) F (i) F (j) T (k) F (l) F (m) F (n) F.

4.5. Characteristic of a ring

Let R be a ring. Then $(R, +)$ is a group. For any $a \in R$ we have $na = a + a + \ldots + a$ (written n times).

Note. For the ring $\mathbf{Z}_6$ we have $6a = 0$ for all $a \in \mathbf{Z}_6$.

Definition. Let R be a ring. If there exists a positive integer n such that $na = 0$, for all $a \in R$ then the least such positive integer is called the ***characteristic of the ring*** R. If no such positive integer exists then the ring is said to be of *characteristic zero*.

Examples

1. $\mathbf{Z}_6$ is a ring of characteristic 6.
   In general $\mathbf{Z}_n$ is a ring of characteristic n.
2. $\mathbf{Z}$ is a ring of characteristic zero, since there is no positive integer n such that $na = 0$ for all $a \in \mathbf{Z}$.
3. $M_2(\mathbf{R})$ is a ring of characteristic zero.
4. $(\wp(S), \Delta, \cap)$ is a ring of characteristic 2, since $2A = A \Delta A = \Phi$ for all $A \in \wp(S)$.
5. Any Boolean ring is of characteristic 2 (refer solved problem 1 of 4.2).

Theorem 4.14. Let R be a ring with identity 1. If 1 is an element of finite order in the group $(R, +)$ then the order of 1 is the characteristic of R. If 1 is of infinite order, the characteristic of the ring is 0.

Proof. Suppose the order of 1 is n. Then n is the least positive integer such that $n \cdot 1 = 0$

(ie.,) $1 + 1 + \ldots + 1 (n \text{ times}) = 0$. Now, let $a \in R$.

$$\begin{aligned} \text{Then, } na &= a + a + \ldots + a (n \text{ times}) \\ &= 1 \cdot a + 1 \cdot a + \ldots + 1 \cdot a \\ &= (1 + 1 + \ldots + 1)a. \\ &= 0 \cdot a \\ &= 0. \end{aligned}$$

Thus $na = 0$ for all $a \in R$.

Hence the characteristic of the ring is n.

If 1 is of infinite order then there, is no positive integer n such that $n \cdot 1 = 0$. Hence the characteristic of the ring is 0.

Theorem 4.15. The characteristic of an integral domain D is either 0 or a prime number.

Proof. If the characteristic of D is 0 then there is nothing to prove. If not be the characteristic of D be n.

If n is not prime, let $n = pq$ where $1 < p < n$ and $1 < q < n$.

Since characteristic of D is n we have $n \cdot 1 = 0$.

Hence $n \cdot 1 = pq \cdot 1 = (p \cdot 1)(q \cdot 1) = 0$.

Since D is an integral domain either $p \cdot 1 = 0$ or $q \cdot 1 = 0$.

Since p, q are both less than n, this contradicts the definition of the characteristic of D.

Hence n is a prime number.

Corollary. The characteristic of any field is either 0 or a prime number.

Proof. Since every field is an integral domain the result follows.

Note.

1. The characteristic of an arbitrary ring need not be prime. For example $\mathbf{Z}_6$ is of characteristic 6.
2. The converse of the above theorem is not true. (ie.,) If the characteristic of a ring R is prime then R need not be an integral domain. For example the ring $(\wp(S), \Delta, \cap)$ is of characteristic 2 but it is not an integral domain. If A and B are two disjoint nonempty subsets of S we have $A \cap B = \Phi$ and hence A and B are zero divisors in $\wp(S)$.

Theorem 4.16. In an integral domain D of characteristic p, the order of every element in the additive group is p.

Proof. Let $a \in D$ be any non-zero element.

Let the order of a be n. Then n is the least positive integer such that $na = 0$.

Now, by the definition of the characteristic of D we have $pa = 0$.

Hence $n|p$. Now, since p is prime, $n = 1$ or $n = p$.

If $n = 1$, $na = a = 0$ which is a contradiction.

Hence $n = p$. Thus the order of a is p.

Note. The above result is not true for an arbitrary ring. For example the characteristic of the ring $\mathbf{Z}_6$ is 6 whereas the order of $2 \in \mathbf{Z}_6$ is 3.

Exercises

1. Prove that any integral domain of characteristic zero is infinite.
2. Show that the characteristic of $M_2(\mathbf{Z}_3)$ is 3.
3. Give an example of an infinite ring of characteristic not zero.
4. In a field of characteristic p show that $(a \pm b)^p = a^p \pm b^p$.
5. Let a, b be arbitrary elements of a ring R whose characteristic is 2 and let $ab = ba$. Then show that $(a+b)^2 = a^2+b^2 = (a-b)^2$.
6. Determine which of the following are true and which are false.
   (a) $n\mathbf{Z}$ is of characteristic n.
   (b) The characteristic of any ring is either 0 or a prime number.
   (c) The characteristic of $\mathbf{Q}$ is zero.
   (d) The characteristic of any finite ring is not zero.
   (e) The characteristic of any field is zero.

Answers.

6. (a) F (b) F (c) T (d) T (e) F.

4.6. Subrings

Definition. A non-empty subset S of a ring $(R, +, \cdot)$ is called a **subring** if S itself is a ring under the same operations as in R.

Examples

1. $2\mathbf{Z}$ is a subring of $\mathbf{Z}$.
2. $\mathbf{Z}$ is a subring of $\mathbf{Q}$.
3. $\mathbf{Q}$ is a subring of $\mathbf{R}$.
4. $\mathbf{R}$ is a subring of $\mathbf{C}$.
5. The set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is a subring of $M_2(\mathbf{R})$.
6. $\{0\}$ and R are subrings of any ring R. They are called the **trivial subrings** of R.
7. $S = \{a + b\sqrt{2}/a, b \in \mathbf{Q}\}$ is a subring of R.
8. $\{0, 2\}$ is a subring of $\mathbf{Z}_4$.

Theorem 4.17. A non-empty subset S of a ring R is a subring iff $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$.

roof. Let S be a subring of R.

Then $(S, +)$ is a subgroup of $(R, +)$.

Hence, $a, b \in S \Rightarrow a - b \in S$.

Also since S itself is a ring $ab \in S$.

Conversely, let S be a non-empty subset of R such hat $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$.

Then $(S, +)$ is a subgroup of $(R, +)$.

Also S is closed under multiplication.

The associative and distributive laws are conse- quences of the corresponding laws in R.

Hence S is a subring.

Solved problems

Problem 1. Let X be any set and let F be the set of all finite subsets of X. Then F is a subring of $(\wp(X), \Delta, \cap)$.

Solution. Let $A, B \in F$. Then A and B are finite sets. Hence $(A - B) \cup (B - A) = A \Delta B$ is a finite set so that $A \Delta B \in F$.

Similarly $A \cap B \in F$. Thus F is a subring.

Problem 2. Let R be a ring with identity.

Then $S = \{n \cdot 1 / n \in \mathbf{Z}\}$ is a subring of R.

Solution. Let $a, b \in S$. Then $a = n \cdot 1$ and $b = m \cdot 1$ for some $n, m \in \mathbf{Z}$.

Hence $a - b = n \cdot 1 - m \cdot 1 = (n - m) \cdot 1 \in S$.

Also $ab = (n \cdot 1)(m \cdot 1) = (nm) \cdot 1 \in S$.

Hence S is a subring of R.

Problem 3. Given an example of

(a) a ring without identity in which a subring has an identity.

(b) a subring without identity, of a ring with identity.

(c) a ring with identity 1 in which a subring has identity $1' \neq 1$.

(d) a subring of a non-commutative ring which is commutative.

(e) a subring of a field, which is not a field.

Solution. (a) Consider the set R of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ where $a, b \in \mathbf{R}$.

Then R is a ring under matrix addition and multiplication (verify).

We now prove that this ring does not have an identity. Let $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$ be a matrix such that $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$

$= \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$.

Now,

$$\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} ac & 0 \\ bd & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}.$$

$\Rightarrow ac = a$ and $ad = b \Rightarrow c = 1$ and $d = ba^{-1}$.

Hence the matrix $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$ depends on the matrix $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ so that the ring R does not have an identity element.

However the subring S of R consisting of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ has $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ as identity.

(b) $2\mathbf{Z}$ is a subring of $\mathbf{Z}$. $\mathbf{Z}$ has 1 as the identity but $2\mathbf{Z}$ doesnot have an identity.

(c) $M_2(\mathbf{R})$ is a ring with the identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

The subring $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \Big/ a \in \mathbf{R} \right\}$ has the identity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

(d) Example given in (c).

(e) $\mathbf{Q}$ is a field. $\mathbf{Z}$ is a subring of $\mathbf{Q}$ but $\mathbf{Z}$ is not a field.

Theorem 4.18. The intersection of two subrings of a ring R is a subring of R.

Proof. Let A, B be two subrings of R.

Let $a, b \in A \cap B$. Then $a, b \in A$ and B.

Since A and B are subrings $a - b$ and $ab \in A$ and B.

$\therefore$ $a - b$ and $ab \in A \cap B$.

$\therefore$ $A \cap B$ is subring of R (by Theorem 4.17).

Note.

1. The union of the two subrings of a ring need not be a subring.
2. The union of two subrings of a ring is again a subring iff one is contained in the other (proof as in theorem 3.20).

Definition. A non-empty subset S of a field $(F, +, \cdot)$ is called a ***subfield*** if S itself is a field under the same operations as in F.

For example, $\mathbf{Q}$ is a subfield of $\mathbf{R}$ and $\mathbf{R}$ is a subfield of $\mathbf{C}$.

Theorem 4.19. A non-empty subset S of a field F is a subfield iff

(i) $a, b \in S \Rightarrow a - b \in S$ and
(ii) $a, b \in S$ and $b \neq 0 \Rightarrow ab^{-1} \in S$.

The proof follows by applying Theorem 3.17 to the groups $(F, +)$ and $(F - \{0\}, \cdot)$.

Exercises

1. Prove that every subgroup of $(\mathbf{Z}, +)$ is a subring of the ring of integers. (Hint: Any subgroup of $\mathbf{Z}$ is $n\mathbf{Z}$ for some n).
2. Prove that every subgroup of $(\mathbf{Z}_n, \oplus)$ is a subring of $(\mathbf{Z}_n, \oplus, \odot)$.
3. Find all the subrings of $\mathbf{Z}_8$, $\mathbf{Z}_{12}$ and $\mathbf{Z}_{13}$.
4. Let A and B be two rings. In $A \times B$ we define.

   $(a_1, b_1) \oplus (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ and
   $(a_1, b_1) \odot (a_2, b_2) = (a_1 a_2, b_1 b_2)$.

   Show that $A \times B$ is a ring. This ring is called the **direct sum** of the rings A and B and is denoted by $A \oplus B$.
5. If A and B are two rings with identity, pr that $A \oplus B$ is also a ring with identity.
6. Let A be a ring with identity 1 and B ring without identity. Then show that A is a ring without identity. Prove also $S = \{(a, 0)/a \in A\}$ is a sub ring of A with identity $(1, 0)$.
7. If A and B are fields, is $A \oplus B$ a field?
8. Prove that the intersection of two subfield a field F is a subfield of F.
9. Let R be a ring and let a be a fixed elemen R. Let $I_a = \{x \in R/ax = 0\}$. Show that I a subring of R.
10. Let R be a finite ring and S be a subring of Show that the order of S divides the order of

4.7. Ideals

We now introduce the concept of an ideal in a ri Ideals play an important role in the development of r theory similar to the role played by normal subgrou in group theory.

Definition. Let R be a ring. A non-empty subset R is called a ***left ideal*** of R if

(i) $a, b \in I \Rightarrow a - b \in I$.
(ii) $a \in I$ and $r \in R \Rightarrow ra \in I$.

I is called a ***right ideal*** of R if

(i) $a, b \in I \Rightarrow a - b \in I$.
(ii) $a \in I$ and $r \in R \Rightarrow ar \in I$.

I is called an ***ideal*** of R if I is both a *left ideal* and *right ideal*.

Thus in an ideal the product of an element in th ideal and an element in the ring is an element of th ideal. In a commutative ring the concepts of the le ideal, right ideal and ideal coincide.

Examples

1. In any ring, R, $\{0\}$ and R are ideals. They are called **improper ideals** of R.
2. $2\mathbf{Z}$ is an ideal of $\mathbf{Z}$.

Proof. Let $a, b \in 2\mathbf{Z}$. Then $a - b \in 2\mathbf{Z}$. Let $a \in 2\mathbf{Z}$ and $b \in \mathbf{Z}$. Then ab is even and hence $ab \in 2\mathbf{Z}$. Thus $2\mathbf{Z}$ is an ideal of $\mathbf{Z}$.

In general $n\mathbf{Z}$ is an ideal of $\mathbf{Z}$ (prove).

3. In $M_2(\mathbf{R})$ the set S of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal and it is not a right ideal.

Clearly $A, B \in S \Rightarrow A - B \in S$.

Now, let $A \in S$ and $B \in M_2(\mathbf{R})$.

Let $A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ and $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$.

Then $BA = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$

$$= \begin{pmatrix} pa + qb & 0 \\ ra + sb & 0 \end{pmatrix} \in S.$$

Hence S is a left ideal. However

$$AB = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

$$= \begin{pmatrix} ap & aq \\ bp & bq \end{pmatrix} \notin S.$$

Hence S is not a right ideal.

4. Let R be any ring. Let $a \in R$.

Let $aR = \{ax / x \in R\}$. Then aR is a right ideal of R.

Similarly $Ra = \{xa / x \in R\}$ is a left ideal of R.

Let $ax, ay \in aR$.

Then $ax - ay = a(x - y) \in aR$.

Let $ax \in aR$ and $y \in R$.

Then $(ax)y = a(xy) \in aR$.

Thus aR is a right ideal.

Similarly Ra is a left ideal of R.

Definition. If R is a commutative ring then $aR = Ra$ is an ideal. This is called the ***principal ideal*** generated by a and is denoted by (a).

Note. If R is a commutative ring with identity 1 then $a = a1 \in (a)$. This may not be true if the ring R does not have an identity.

For example, consider the ring $2\mathbf{Z}$. Here $(4) = \{0, \pm, 8, \pm 16, \pm 24, \ldots\ldots\}$ and $4 \notin (4)$.

Remark.

(i) Every left ideal of a ring R is a subring of R.
Let I be a left ideal of R. Let $a, b \in I$. Then by definition, $a - b$ and $ab \in I$. Hence I is a subring of R.

(ii) Similarly every right ideal of R is also a subring of R.

(iii) *Any ideal of R is a subring of R.* (by (i) and (ii))

(iv) However, a subring of R need not be an ideal of R.

For example, $\mathbf{Z}$ is a subring of $\mathbf{Q}$ but $\mathbf{Z}$ is not an ideal of $\mathbf{Q}$ since $1 \in \mathbf{Z}$ and $\frac{1}{2} \in \mathbf{Q}$ but $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbf{Z}$.

Theorem 4.20. Let R be a ring with identity 1. If I is an ideal of R and $1 \in I$, then $I = \mathbf{R}$.

Proof. Obviously $I \subseteq R$. Now, let $r \in R$.

Since $1 \in I, r \cdot 1 = r \in I$. Thus $R \subseteq I$.

Hence $R = I$.

Theorem 4.21. Let F be any field. Then the only ideals of F are $\{0\}$ and F.

(ie.,) *A field has no proper ideals.*

Proof. Let I be an ideal of F. Suppose $I \neq \{0\}$.

We shall prove that $I = F$. Since $I \neq \{0\}$, there exists an element $a \in I$ such that $a \neq 0$.

Since F is a field a has a multiplicative inverse $a^{-1} \in F$.

Now, $a \in I$ and $a^{-1} \in F \Rightarrow aa^{-1} = 1 \in I$.

Hence by theorem 4.20, $I = F$.

Theorem 4.22. Let R be a commutative ring with identity. Then R is a field iff R has no proper ideals.

Proof. If R is a field, by theorem 4.21, R has no proper ideals.

Conversely, suppose R has no proper ideals.

To prove that R is a field we need to show that every non-zero element in R has an inverse. Let $a \in R$ and $a \neq 0$.

Consider the principal ideal aR.

Since R is a ring with identity, $a = a \cdot 1 \in aR$.

$\therefore$ $aR \neq \{0\}$. Since R has no proper ideals, $aR = R$.

Hence there exists $x \in R$ such that $ax = 1$.

Thus x is the inverse of a. Hence R is a field.

Definition. An integral domain R is said to be a ***principal ideal domain (PID)*** if every ideal of R is a principal ideal.

Examples

1. $\mathbf{Z}$ is a principal ideal domain since any ideal of $\mathbf{Z}$ is of the form $n\mathbf{Z}$.
2. Any field F is a principal ideal domain since the only ideals of F are (0) and (1) $= F$ (by theorem 4.21).

Exercises

1. Show that intersection of two left ideals of a ring R is again a left ideal of R. Prove similar results for right ideals and ideals.
2. Let I_1 and I_2 be two ideals of R.
   Let $I_1 + I_2 = \{a + b / a \in I_1, b \in I_2\}$.
   Show that $I_1 + I_2$ is an ideal of R.
3. Let X be a non-empty set. For any non-empty subset A of X show that $\{A, \Phi\}$ is a subring but not an ideal of the ring $(\wp(X), \Delta, \cap)$.
4. Let A and B be any two rings. Show that $A \times \{0\}$ and $\{0\} \times B$ are ideals of $A \oplus B$.
5. Prove that $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \Big/ a, b \in \mathbf{R} \right\}$ is a subring but not an ideal of $M_2(\mathbf{R})$.
6. Determine which of the following statements are true and which are false.
   (a) A subring of a commutative ring is commutative.
   (b) A subring of a ring with identity is again a ring with identity.
   (c) The identity element of a subring is the same as the identity element of the ring.
   (d) The set of all non-singular 2×2 matrices is a subring of $M_2(\mathbf{R})$.
   (e) Every subring of a ring R is an ideal of R.
   (f) Every ideal of a ring R is a subring of R.
   (g) $\mathbf{Z}$ is an ideal of $\mathbf{R}$.
   (h) $\mathbf{Q}$ is an ideal of $\mathbf{R}$.
   (i) $\{0, 2\}$ is an ideal of $\mathbf{Z}_4$.
   (j) $\{0, 1\}$ is an ideal of $\mathbf{Z}_4$.
   (k) In a commutative ring every left ideal is a right ideal.
   (l) $\mathbf{R}$ has no proper ideals.
   (m) $\mathbf{Q}$ is a principal ideal domain.
   (n) $\mathbf{Z}$ is a principal ideal domain.

Answers.

6. (a) T (b) F (c) F (d) F (e) F (f) T (g) F (h) F (i) T (j) F (k) T (l) T (m) T (n) T.

4.8. Quotient rings

Let R be a ring. Let $(I, +)$ be a subgroup of $(R, +)$. Since addition is commutative in R, I is a normal subgroup of $(R, +)$ and hence the collection $R/I = \{I + a / a \in R\}$ is a group under the operation defined by $(I+a)+(I+b) = I+(a+b)$. To make R/I a ring, we have to define a multiplication in R/I. It is natural to define $(I+a)(I+b) = I+ab$. But we have to prove that this multiplication is well defined (ie.,) it is independent of the choice of the representatives from the casets. We shall prove that this happens iff I is an ideal.

Theorem 4.23. Let R be a ring and I be a subgroup of $(R, +)$. The multiplication in R/I given by $(I + a)(I + b) = I + ab$ is well defined iff I is an ideal of R.

Proof. Let I be an ideal of R.

To prove multiplication is well defined, let $I + a_1 = I + a$ and $I + b_1 = I + b$.

Then $a_1 \in I + a$ and $b_1 \in I + b$.

$\therefore \quad a_1 = i_1 + a$ and $b_1 = i_2 + b$ where $i_1, i_2 \in I$.

Hence $a_1 b_1 = (i_1 + a)(i_2 + b) = i_1 i_2 + i_1 b + a i_2 + ab$.

Now since I is an ideal we have $i_1 i_2, i_1 b, a i_2 \in I$.

Hence $a_1 b_1 = i_3 + ab$ where $i_3 = i_1 i_2 + i_1 b + a i_2 \in I$.

$\therefore \quad a_1 b_1 \in I + ab$.

Hence $I + ab = I + a_1 b_1$.

Conversely suppose that the multiplication in R/I given by $(I + a)(I + b) = I + ab$ is well defined.

To prove that I is an ideal of R.

Let $i \in I$ and $r \in R$. We have to prove that $ir, ri \in I$.

Now, $I + ir = (I + i)(I + r) = (I + 0)(I + r)$

$= I + 0r = I$.

$\therefore \quad ir \in I$. Similarly $ri \in I$.

Hence I is an ideal.

Definition. Let R be any ring and I be an ideal of R. We have two well defined binary operations in R/I given by $(I + a) + (I + b) = I + (a + b)$ and $(I + a)(I + b) = I + ab$. It is easy to verify that R/I is a ring under these operations.

The ring R/I is called the ***quotient ring of R modulo I***.

Examples

1. The subset $I = \{0, 3\}$ of $\mathbf{Z}_6$ is an ideal (verify) $Z_6/I = \{I, I + 1, I + 2\}$ is a ring isomorphic to $\mathbf{Z}_3$.

   Here $\mathbf{Z}_6$ is not an integral domain but the quotient ring $\mathbf{Z}_6/I$ is an integral domain.

2. The subset $p\mathbf{Z}$ where p is prime is an ideal of the ring $\mathbf{Z}$.
   $\mathbf{Z}/p\mathbf{Z} = \{p\mathbf{Z}, p\mathbf{Z} + 1 \ldots\ldots, p\mathbf{Z} + (p - 1)\}$.
   It is easy to see that the ring $\mathbf{Z}/p\mathbf{Z} \simeq \mathbf{Z}_p$. Here $\mathbf{Z}$ is an integral domain but not a field whereas $\mathbf{Z}/p\mathbf{Z}$ is a field.

Exercises

1. Let R be a ring and I be an ideal of R. Prove that (i) if R is commutative then R/I is commutative. (ii) if R is a ring with identity then R/I is a ring with identity.
2. Find all ideals I of $\mathbf{Z}_{12}$. In each case compute $\mathbf{Z}_{12}/I$.
3. Give addition and multiplication tables for the ring $3\mathbf{Z}/12\mathbf{Z}$. Is the ring isomorphic to $\mathbf{Z}_4$?
4. Determine which of the following statements are true and which are false.
   Let R be a ring and I an ideal of R. Then,
   (a) R is commutative $\Rightarrow$ R/I is commutative.
   (b) R/I is commutative $\Rightarrow$ R is commutative.
   (c) R is a ring with identity $\Rightarrow$ R/I is a ring with identity.
   (d) R/I is a ring with identity $\Rightarrow$ R is a ring with identity.
   (e) R is an integral domain $\Rightarrow$ R/I is an integral domain.
   (f) R/I is an integral domain $\Rightarrow$ R is an integral domain.
   (g) R is a field $\Rightarrow$ R/I is a field.
   (h) R/I is a field $\Rightarrow$ R is a field.

Answers.

4. (a) T (b) F (c) T (d) F (e) F (f) F (g) F (h) F

4.9. Maximal and prime ideals

We have seen that if R is a ring and I is an ideal of R then R/I is a ring. Further is R is commutative then R/I is also commutative. We now proceed to answer the following questions for commutative rings with identity. Which ideals I give rise to quotient rings that are (i) fields (ii) integral domains?

Definition. Let R be a ring. An ideal $M \neq R$ is said to be a ***maximal ideal*** of R if whenever U is an ideal of R such that $M \subseteq U \subseteq R$ then either $U = M$ or $U = R$. That is, there is no proper ideal of $\mathbf{R}$ properly containing M.

Examples

1. (2) is a maximal ideal in **Z**. For, let U be an ideal properly containing (2).

   $\therefore$ U contains an odd integer say, $2n+1$.

   $\therefore$ $1 = (2n+1) - 2n \in U$.

   $\therefore$ $U = \mathbf{Z}$ (by theorem 4.20).

   Thus there is no proper ideal of **Z** properly containing (2). Hence (2) is a maximal ideal of **Z**.

2. Let p be any prime. Then (p) is maximal ideal in **Z**.

   Let U be any ideal of **Z** such that $(p) \subseteq U$. Since every ideal of **Z** is a principal ideal $U = (n)$ for some $n \in \mathbf{Z}$.

   Now, $p \in (p) \subseteq U \Rightarrow p \in U = (n)$.

   $\therefore$ $p = nm$ for some integer m.

   Since p is prime either $n = 1$ or $n = p$.

   Suppose $n = 1$. Then $U = \mathbf{Z}$.

   Suppose $n = p$. Then $U = (p)$.

   $\therefore$ There is no proper ideal of **Z** properly containing (p). Hence (p) is a maximal ideal in **Z**.

3. In any field F, (0) is a maximal ideal of F since the only ideals of F are (0) and F. (refer Theorem 4.21)

4. Let R be the ring of all real valued continuous functions on [0,1].

   Let $M = \{f \in R / f(1/2) = 0\}$.

   Clearly M is an ideal of R.

   Let U be any ideal of R properly containing M.

   $\therefore$ There exists a function $g(x) \in U$ such that $g(1/2) \neq 0$. Let $g(1/2) = c$.

   Take $h(x) = g(x) - c$.

   $\therefore$ $h(1/2) = g(1/2) - c = c - c = 0$.

   $\therefore$ $h(x) \in M \subseteq U$.

   Also $g(x) \in U$. Hence $g(x) - h(x) \in U$.

   $\therefore$ $c \in U$.

   $\therefore$ $1 = cc^{-1} \in U$.

   $\therefore$ $U = R$ (by theorem 4.20).

   Thus there is no proper ideal of R properly containing M. Hence M is maximal in R.

5. (4) is not a maximal ideal in **Z**. For, (2) is a proper ideal of **Z** properly containing (4).

Theorem 4.24. Let R be a commutative ring with identity. An ideal M of R is maximal iff R/M is a field.

Proof. Let M be a maximal ideal in R.

Since R is a commutative ring with identity and $M \neq R$, R/M is also a commutative ring with identity.

Now, let $M + a$ be a non-zero element in R/M so that $a \notin M$. We shall now prove that $M + a$ has a multiplicative inverse in R/M.

Let $U = \{ra + m / r \in R \text{ and } m \in M\}$.

We claim that U in an ideal of R.

$$(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in U.$$

Also, $r(r_1a + m_1) = (rr_1)a + rm_1 \in U$ (since $rm_1 \in M$).

$\therefore$ U is an ideal of R.

Now, let $m \in M$. Then $m = 0a + m \in U$.

$\therefore$ $M \subseteq U$.

Also $a = 1a + 0 \in U$ and $a \notin M$.

$\therefore$ $M \neq U$.

$\therefore$ U is an ideal of R properly containing M.

But M is a maximal ideal of R.

$\therefore$ $U = R$. Hence $1 \in U$.

$\therefore$ $1 = ba + m$ for some $b \in R$.

Now,

$$M + 1 = M + ba + m = M + ba \text{ (since } m \in M)$$
$$= (M + b)(M + a).$$

Hence $M + b$ is the inverse of $M + a$.

Thus every non-zero element of R/M has an inverse.

Hence R/M is a field.

Conversely, suppose R/M is a field.

Let U be any ideal of R properly containing M.

$\therefore$ There exists an element $a \in U$ such that $a \notin M$.

$\therefore$ $M + a$ is a non-zero element of R/M.

Since R/M is a field $M + a$ has an inverse, say $M + b$.

$\therefore$ $(M + a)(M + b) = M + 1$.

$\therefore$ $M + ab = M + 1$.

$\therefore$ $1 - ab \in M$.

But $M \subseteq U$. Hence $1 - ab \in U$.

Also $a \in U \Rightarrow ab \in U$.

$\therefore$ $1 = (1 - ab) + ab \in U$. Thus $1 \in U$.

$\therefore$ $U = R$. Thus there is no proper ideal of R properly containing M. Hence M is a maximal ideal in R.

Definition. Let R be a commutative ring. An ideal $P \neq R$ is called a ***prime ideal*** if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Examples

1. Let R be an integral domain. Then (0) is a prime ideal of R.
   For, $ab \in (0) \Rightarrow ab = 0$
   $\Rightarrow a = 0$ or $b = 0$(since R is an $I.D.$)
   $\Rightarrow a \in (0)$ or $b \in (0)$.

2. (3) is a prime ideal of $\mathbf{Z}$.
   For, $ab \in (3) \Rightarrow ab = 3n$ for some integer n.
   $\Rightarrow 3 | ab$
   $\Rightarrow 3 | a$ or $3 | b$
   $\Rightarrow a \in (3)$ or $b \in (3)$.
   $\therefore$ (3) is a prime ideal.

Note. In fact for any prime number p, the ideal (p) is a prime ideal in $\mathbf{Z}$.

(4) is not a prime ideal in $\mathbf{Z}$.

For, $2 \times 2 \in (4)$. But $2 \notin (4)$.

Theorem 4.25. Let R be any commutative ring with identity. Let P be an ideal of R. Then P is a prime ideal $\Leftrightarrow$ R/P is an integral domain.

Proof. Let P be a prime ideal.

Since R is a commutative ring with identity R/P is also commutative ring with identity.

Now, $(P + a)(P + b) = P + 0$

$\Rightarrow P + ab = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ or $b \in P$(since P is a prime ideal)

$\Rightarrow P + a = P$ or $P + b = P$

Thus R/P has no zero divisors.

$\therefore$ R/P is integral domain.

Conversely, suppose R/P is an integral domain.

We claim that P is a prime ideal of R.

Let $ab \in P$. Then $P + ab = P$.

$\therefore$ $(P + a)(P + b) = P$.

$\therefore$ $P + a = P$ or $P + b = P$. (since R/P has no zero-divisors)

$\therefore$ $a \in P$ or $b \in P$.

$\therefore$ P is a prime ideal of R.

Corollary. Let R be a commutative ring with identity. Then every maximal ideal of R is a prime ideal of R.

Proof. Let M be a maximal ideal of R.

$\therefore$ R/M is a field. (by theorem 4.24)

$\therefore$ R/M is an integral domain. (by theorem 4.8)

$\therefore$ M is a prime ideal. (by theorem 4.25)

Note. The converse of the above statement is not true. For example, (0) is a prime ideal of $\mathbf{Z}$ but not a maximal ideal of $\mathbf{Z}$.

Exercises

1. Prove that in $\mathbf{Z}$, (6) is not a maximal ideal.
2. Prove that for any composite number n, the ideal (n) is not a maximal ideal of $\mathbf{Z}$.
3. Prove that (n) is a maximal ideal in $\mathbf{Z}$ iff n is a prime number.

4. Prove that (4) is a maximal ideal but not a prime ideal in the ring of even integers.
5. Find all prime ideals and maximal ideals of $\mathbf{Z}_{12}$.
6. Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal of R.

Answers.

5. (2) and (3) are prime ideals and also maximal ideals.

4.10. Homomorphism of rings

Definition. Let R and R' be rings. A function $f : R \to R'$ is called a ***homomorphism*** if

(i) $f(a+b) = f(a) + f(b)$ and
(ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

If f is 1-1, then f is called a ***monomorphism***. If f is onto, then f is called an ***epimorphism***. A homomorphism of a ring onto itself is called an ***endomorphism***.

Note.

1. Obviously an isomorphism of a ring is a homomorphism and a 1-1, onto homomorphism is an isomorphism.
2. The name homomorphism is used for mapping between groups and between rings. In groups, a homomorphism preserves the binary operation of the group. Since rings have two binary operations, a ring homomorphism is defined as a mapping preserving the two binary operations in a ring.
3. Condition (i) of ring homomorphism says that f is a group homomorphism from the additive group $(R, +)$ to the additive group $(R', +)$.

Examples

1. $f : R \to R'$ defined by $f(a) = 0$ for all $a \in R$ is obviously a homorphism. f is called the *trivial homomorphism.*

2. Let R be any ring. The identity map $i : R \to R$ is obviously a homomorphism.

3. Let R be any ring. $f : R \times R \to R$ given by $f(x, y) = x$ is a ring homomorphism.

For,

$$f[(a,b)+(c,d)] = f(a+c, b+d) = a+c$$
$$= f(a,b) + f(c,d).$$

Also, $f[(a,b)(c,d)] = f(ac, bd) = ac$
$$= f(a,b)\,f(c,d).$$

4. $f : \mathbf{Z} \to \mathbf{Z}_n$ defined by $f(x) = r$ where $x = qn + r, 0 \le r < n$ is a homomorphism.

For, let $a, b \in \mathbf{Z}$.

Let $a = q_1 n + r_1$ where $0 \le r_1 < n$,
$b = q_2 n + r_2$ where $0 \le r_2 < n$,
$r_1 + r_2 = q_3 n + r_3$ where $0 \le r_3 < n$,
and $r_1 r_2 = q_4 n + r_4$ where $0 \le r_4 < n$.

Now,

$$(a+b) = (q_1 + q_2)n + r_1 + r_2$$
$$= (q_1 + q_2 + q_3)n + r_3.$$

$\therefore\ f(a+b) = r_3 = r_1 \oplus r_2 = f(a) \oplus f(b)$.

Also,

$$ab = (q_1 n + r_1)(q_2 n + r_2)$$
$$= n(q_1 q_2 n + r_1 q_2 + r_2 q_1) + r_1 r_2$$
$$= n(q_1 q_2 n + r_1 q_2 + r_2 q_1 + q_4) + r_4$$

$\therefore\ f(ab) = r_4 = r_1 \odot r_2 = f(a) \odot f(b)$.

Hence f is a homomorphism.

5. Let R be a ring and I be an ideal of R. Then $\Phi : R \to R/I$ defined by $\Phi(x) = I + x$ is a ring homomorphism. Φ is called the *natural* ***homomorphism***.

$$\Phi(x+y) = I + (x+y)$$
$$= (I + x) + (I + y)$$
$$= \Phi(x) + \Phi(y).$$

$$\Phi(xy) = I + xy$$
$$= (I + x)(I + y)$$
$$= \Phi(x)\Phi(y).$$

Hence Φ is a ring homomorphism.

Theorem 4.26. Let R and R' be rings and $f : R \to R'$ be a homomorphism. Then,

(i) $f(0) = 0'$

(ii) $f(-a) = -f(a)$ for all $a \in R$.

(iii) If S is a subring of R, then $f(S)$ is a subring of R'. In particular $f(R)$ is a subring of R'.

(iv) If S is an ideal of R, then $f(S)$ is an ideal of $f(R)$.

(v) If S' is a subring of R', then $f^{-1}(S')$ is a subring of R.

(vi) If S' is an ideal of $f(R)$, then $f^{-1}(S')$ is an ideal of R.

(vii) If R is a ring with identity 1 and $f(1) \neq 0'$, then $f(1) = 1'$ is the identity of $f(R)$.

(viii) If R is a commutative ring then $f(R)$ is also commutative.

Proof. Since f is a homomorphism of the group $(R, +)$ to $(R', +)$, the results (i) and (ii) follow from Theorem 3.55

(iii) Since S is a subring of R, $(S, +)$ is a subgroup of $(R, +)$ and hence $f(S)$ is a subgroup of $(R', +)$.

Now, let $a', b' \in f(S)$.

Then $a' = f(a)$ and $b' = f(b)$ for some $a, b \in S$.

$\therefore \quad a'b' = f(a)f(b) = f(ab) \in f(S)$.

Hence $f(S)$ is a subring of R'.

(iv) Let S be an ideal of R.

To prove that $f(S)$ is an ideal of $f(R)$ it is enough if we prove that $r' \in f(R)$ and $a' \in f(S) \Rightarrow r'a'$ and $a'r' \in f(S)$.

Let $r' = f(r)$ and $a' = f(a)$ where $r \in R$ and $a \in S$.

Now, since S is an ideal of R, ra and $ar \in S$.

Hence $f(ra) = f(r)f(a) = r'a' \in f(S)$.

Similarly $a'r' \in f(S)$.

Hence $f(S)$ is an ideal of $f(R)$.

(v) Let S' be a subring of R'. Since $(S', +)$ is a subgroup of $(R', +)$, $f^{-1}(S')$ is a subgroup of $(R, +)$.

Now, let $a, b \in f^{-1}(S')$.

Then $f(a), f(b) \in S'$.

$\therefore \quad f(ab) = f(a)f(b) \in S'$ (since S' is a subring of R).

$\therefore \quad ab \in f^{-1}(S')$.

Hence $f^{-1}(S')$ is a subring of R.

(vi) Proof is similar to that of (v).

(vii) Let R be a ring with identity 1. Let $a' \in f(R)$.

Then $a' = f(a)$ for some $a \in R$.

Now, $a'f(1) = f(a)f(1)$
$= f(a1) = f(a) = a'$.

Similarly $f(1)a' = a'$. Also $f(1) \neq 0$.

Hence $f(1)$ is the identity of $f(R)$.

(viii) Proof is left to the reader.

Definition. The **kernel** K of a homomorphism f of a ring R to a ring R' is defined by

$\{a/a \in R \text{ and } f(a) = 0\}$.

Theorem 4.27. Let $f : R \to R'$ be a homomorphism. Let K be the kernel of f. Then K is an ideal of R.

Proof. By definition, $K = f^{-1}(\{0\})$.

Since $\{0\}$ as an ideal of $f(R)$, by (vi) of theorem 4.26, K is an ideal of R.

Theorem 4.28. ***(The fundamental theorem of homomorphism)***

Let R and R' be rings and $f : R \to R'$ be an epimorphism. Let K be the kernel of f. Then $R/K \approx R'$.

Proof. Define $\Phi : R/K \to R'$ by $\Phi(K+a) = f(a)$.

(i) Φ *is well defined*, for, let $K + b = K + a$.

Then $b \in K + a$.

$\therefore \quad b = k + a$ where $k \in K$.

$$\therefore \quad f(b) = f(k+a) = f(k) + f(a)$$
$$= 0 + f(a) = f(a).$$
$$\therefore \quad \Phi(K+b) = f(b) = f(a) = \Phi(K+a).$$

(ii) *Φ is 1-1.*
For, $\Phi(K+a) = \Phi(K+b) \Rightarrow f(a) = f(b)$

$$\Rightarrow f(a) - f(b) = 0$$
$$\Rightarrow f(a) + f(-b) = 0$$
$$\Rightarrow f(a-b) = 0$$
$$\Rightarrow a - b \in K$$
$$\Rightarrow a \in K + b$$
$$\Rightarrow K + a = K + b.$$

(iii) *Φ is onto.*
For, let $a' \in R'$
Since f is onto, there exists $a \in R$ such that $f(a) = a'$.
Hence $\Phi(K+a) = f(a) = a'$.

(iv) *Φ is homomorphism.*
For,

$$\Phi[(K+a)+(K+b)] = \Phi[K+(a+b)]$$
$$= f(a+b)$$
$$= f(a) + f(b)$$
(since f is a homomorphism)
$$= \Phi(K+a) + \Phi(K+b).$$

and $\Phi[(K+a)(K+b)] = \Phi(K+ab)$
$$= f(ab)$$
$$= f(a)f(b)$$
(since f is a homomorphism)
$$= \Phi(K+a)\Phi(K+b).$$

Hence Φ is an isomorphism.
Hence $R/K \simeq R'$

Solved Problems

Problem 1. The homomorphic image of an integral domain need not be an integral domain.

Solution. $f : \mathbf{Z} \to \mathbf{Z}_4$ defined by $f(a) = r$ where $a = 4q + r, 0 \leq r < 4$ is a homomorphism of $\mathbf{Z}$ onto $\mathbf{Z}_4$. Here $\mathbf{Z}$ is an integral domain and $\mathbf{Z}_4$ is not an integral domain since $2 \odot 2 = 0$.

Problem 2. Any homomorphism of a field to itself is either one-one or maps every element to 0.

Solution. Let F be a field and $f : F \to F$ be a homomorphism. Let K be the kernel of f. Then K is an ideal of F. By theorem 4.21, $K = \{0\}$ or $K = F$.

If $K = \{0\}$ then f is 1-1.

If $K = F$, then $f(a) = 0$ for all $a \in F$.

Exercises

1. If R, R', R'' are rings and if $f : R \to R'$ and $g : R' \to R''$ are homomorphisms, then $g \circ f : R \to R''$ is a homomorphism.
2. Let R, R' be rings and $f : R \to R'$ be an epimorphism. Then if R is a skew field, so is R'.
3. Determine which of the following are homomorphisms. If so find the kernel.
   (a) $f : \mathbf{C} \to \mathbf{C}$ defined by $f(z) = \bar{z}$.
   (b) $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(a) = 2a$.
   (c) Let $R = \{m + n\sqrt{2}/m, n \in \mathbf{Z}\}$. R is a ring under usual addition and multiplication. Define $f : R \to R$ by $f(m + n\sqrt{2}) = m - n\sqrt{2}$.
   (d) $f : \mathbf{C} \to M_2(\mathbf{R})$ defined by $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
   (e) $f : \mathbf{Z} \to \mathbf{Z}_n$, f as defined in example 4 of section 4.10.
   (f) $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(x) = x^2 + 3$.
4. Let R be a commutative ring with identity. Prove that if f is homomorphism from f onto a field F then $Ker\ f$ is a maximal ideal of R.

5. Determine which of the following are true and which are false.

(a) Every homomorphism is an isomorphism.

(b) Every isomorphism is a homomorphism.

(c) A homomorphism is 1-1 iff its kernel is $\{0\}$.

(d) In a ring homomorphism, identity element is mapped into identity.

(e) A homomorphic image of an integral domain is an integral domain.

(f) A homomorphic image of a skewfield is a skewfield.

(g) Homomorphic image of a field is a field.

(h) If $f : R \to R'$ is a homomorphism and R is commutative then R' is commutative.

Answers.

3. (a) $Ker f = \{0\}$ (b) Not a homomorphism (c) $Ker f = \{0\}$ (d) $Ker f = \{0\}$ (e) $Ker f = n\mathbf{Z}$ (f) Not a homomorphism.

5. (a) F (b) T (c) T (d) F (e) F (f) F (g) F (h) F.

4.11. Field of quotients of an integral domain

If D is an integral domain, the non-zero elements in D may or may not have multiplicative inverses. For example in $\mathbf{Z}$ all the non-zero elements except 1 and -1 do not have multiplicative inverses. We know that an integral domain in which every non-zero element has a multiplicative inverse is a field. In this section we construct a field F which contains the given integral domain D. This field will be the smallest field containing D. For example $\mathbf{Z}$ is contained in the field $\mathbf{Q}$ and all the elements of $\mathbf{Q}$ can be expressed as quotients of integers. The construction of the quotient field of an integral domain is motivated at every step by the well known behaviour of the field of rational numbers.

We note that every element of $\mathbf{Q}$ can be expressed as a quotient p/q where $p, q \in \mathbf{Z}$ and $q \neq 0$. Further the two fractions 2/3 and 4/6 represent the same rational number. In general two fractions a/b and c/d, where $b, d \neq 0$ represent the same rational number iff $ad = bc$. Also $(a/b) + (c/d) = (ad + bc)/bd$ and $(a/b)(c/d) = ac/bd$. The elements of $\mathbf{Z}$ can be thought of as fractions of the form $a/1$.

The construction of the field of quotients F of an integral domain D is carried out in the following four stages

(i) Specify the elements of F.
(ii) Define addition and multiplication in F.
(iii) Show that F is a field under these operations.
(iv) D can be embedded in F.

Stage (i) Let D be an integral domain.

Let $S = \{(a, b)/a, b \in D \text{ and } b \neq 0\}$.

We are going to think of the ordered pair (a, b) as one representing a formal quotient a/b. For example, if $D = \mathbf{Z}$, the pair $(1, 2)$ will eventually represent the fraction 1/2.

Definition. Two elements (a, b) and $(c, d) \in S$ are defined to be equivalent iff $ad = bc$. If (a, b) is equivalent to (c, d) we write $(a, b) \sim (c, d)$.

Lemma 1. $\sim$ is an equivalence relation in S.

Proof. Let $(a, b) \in S$.

$(a, b) \sim (a, b)$ since $ab = ba = ab$.

Hence $\sim$ is reflexive.

Now, $(a, b) \sim (c, d) \Rightarrow ad = bc$

$\Rightarrow cb = da \Rightarrow (c, d) \sim (a, b)$.

Hence $\sim$ is symmetric.

Now, let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$.

Now to prove that $(a, b) \sim (e, f)$ we must prove that $af = be$.

Case (i) Let $c = 0$. Now, $ad = bc$ and $cf = de$.

$\therefore \quad ad = 0$ and $de = 0$.

But $d \neq 0$. Hence $a = 0$ and $e = 0$.

$\therefore \quad af = be = 0$.

Case(ii) Let $c \neq 0$.

We have $ad = bc$ and $cf = de$.

$\therefore$ $adcf = bcde$.

$\therefore$ $af = be$ (by cancellation law)

$\therefore$ $\sim$ is transitive.

Hence $\sim$ is an equivalence relation on S.

Consider the equivalence class containing (a, b), Let it be denoted by $\frac{a}{b}$. Let $F = \left\{ \frac{a}{b} \middle/ (a, b) \in S \right\}$.

Stage (ii) Let $\frac{a}{b}, \frac{c}{d} \in F$. We now define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Since D is an integral domain and $b, d \neq 0$, we have $bd \neq 0$.

$\therefore$ $\frac{ad + bc}{bd}$ and $\frac{ac}{bd} \in F$.

Lemma 2. Addition and multiplication defined above are well defined.

Proof. Let $(a_1, b_1) \in \frac{a}{b}$ and $(c_1, d_1) \in \frac{c}{d}$.

$\therefore$ $a_1 b = b_1 a$ and $c_1 d = d_1 c$. ... (1)

$\therefore$ $a_1 bdd_1 = b_1 add_1$ and $c_1 dbb_1 = d_1 cbb_1$.

$\therefore$ $(a_1 d_1 + b_1 c_1)bd = (ad + bc)b_1 d_1$.

$\therefore$ $\frac{ad + bc}{bd} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1}$.

$\therefore$ $\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}$.

$\therefore$ Addition is well defined.

Also from (1), $a_1 bc_1 d = b_1 ad_1 c$.

$\therefore$ $(ac, bd) \sim (a_1 c_1, b_1 d_1)$.

$\therefore$ $\frac{a}{b} \cdot \frac{c}{d} = \frac{a_1}{b_1} \cdot \frac{c_1}{d_1}$.

$\therefore$ Multiplication is well defined.

Lemma 3. Stage (iii) F is a field with the addition and multiplication defined above.

Proof. It can easily be verified that addition is commutative and associative.

$\frac{0}{1}$ is the zero of F and $\frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$.

$\therefore$ $(F, +)$ is an abelian group.

Clearly multiplication is commutative and associative. $\frac{1}{1}$ is the identity of F.

If $\frac{a}{b}$ is a non-zero element of F, then $a \neq 0$.

$\therefore$ $\frac{b}{a} \in F$ and is the inverse of $\frac{a}{b}$.

Now, $\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\left(\frac{cf + de}{df}\right)$

$$= \frac{acf + ade}{bdf}$$

$$= \frac{acfb + adeb}{bdfb}$$

$$= \frac{ac}{bd} + \frac{ae}{bf}$$

$$= \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}.$$

$\therefore$ F is a field.

Stage (iv) The field F contains a subring R which is isomorphic to D.

Lemma 4. The map $f : D \to F$ given by $f(a) = \frac{a}{1}$ is an isomorphism of D onto $f(D)$.

Proof. Let $a, b \in D$.

Then $f(a + b) = \frac{a + b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$

and $f(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = f(a)f(b)$.

Also f is 1-1. For, $f(a) = f(b) \Rightarrow \frac{a}{1} = \frac{b}{1}$

$$\Rightarrow (a, 1) \sim (b, 1)$$

$$\Rightarrow a1 = 1b$$

$$\Rightarrow a = b.$$

$\therefore$ f is an isomorphism.

Thus we have proved the following.

Theorem 4.29. Any integral domain D can be embedded in a field F and every element of F can be expressed as a quotient of two elements of D.

Definition. The field F which we have constructed above is called the ***field of quotients*** of D.

Theorem 4.30. The field of quotients F of an integral domain D is the smallest field containing D. (ie.,) If F' is any other field containing D then F' contains a subfield isomorphic to F.

Proof. Let $a, b \in D$ and $b \neq 0$.

Then $a, b \in F'$ and since F' is a field $ab^{-1} \in F'$.

Now, let F be the quotient field of D.

We define $f : F \to F'$ by $f(a/b) = ab^{-1}$.

f is well defined; for, let $(a_1, b_1) \sim (a, b)$.

Then $a_1 b = b_1 a$. Hence $a_1 b_1^{-1} = ab^{-1}$.

f is 1-1, since $f(a/b) = f(c/d) \Rightarrow ab^{-1} = cd^{-1}$

$$\Rightarrow ad = bc$$

$$\Rightarrow a/b = c/d.$$

Now, let $a/b, c/d \in F$.

$$\begin{aligned} \text{Then } f[(a/b) + (c/d)] &= f[(ad + bc)/bd] \\ &= (ad + bc)(bd)^{-1} \\ &= (ad + bc)d^{-1}b^{-1} \\ &= ab^{-1} + cd^{-1} \\ &= f(a/b) + f(c/d). \end{aligned}$$

$$\begin{aligned} \text{Also, } f[(a/b)(c/d)] &= f[(ac)/(bd)] \\ &= (ac)(bd)^{-1} \\ &= acd^{-1}b^{-1} \\ &= ab^{-1} \cdot cd^{-1} \\ &= f(a/b)f(c/d). \end{aligned}$$

Thus F is isomorphically embedded in F'.

Solved problems

Problem 1. Describe the quotient field of the integral domain $D = \{a + b\sqrt{2}/a, b \in \mathbf{Z}\}$.

Solution. The set of real numbers R is a field containing the given integral domain D.

Hence by theorem 4.30, R contains a subfield isomorphic to the field of quotiens of D.

This subfield is precisely the set of all real numbers of the form $(a + b\sqrt{2})/(c + d\sqrt{2})$ where $c + d\sqrt{2} \neq 0$.

$(a + b\sqrt{2})/(c + d\sqrt{2})$ is of the form $p + q\sqrt{2}$ where p and q are rational numbers. Thus the quotient field of D is $\{p + q\sqrt{2}/p, q \in \mathbf{Q}\}$.

Problem 2. If D and D' are isomorphic integral domains then their quotient fields are also isomorphic.

Solution. Let $f : D \to D'$ be an isomorphism. Let F and F' be the quotient fields of D and D' respectively. Consider $\Phi : F \to F'$ given by $\Phi(a/b) = f(a)/f(b)$. Φ is an isomorphism of F onto F' (verify).

Exercises

1. Show that the field of quotients of any field is itself.
2. Let R be a ring which may or may not have a unit element. In $\mathbf{Z} \times R$ we define
   $(n, r) + (m, s) = (n + m, r + s)$ and
   $(n, r)(m, s) = (nm, mr + ns + rs)$ [Notice that since m and n are integers mr and ns are meaningful]. Prove that S is a ring with identity and R can be embedded in S. [This shows that any ring can be embedded in a ring with identity].
3. Determine which of the following statements are true and which are false.
   (a) $\mathbf{R}$ is a field of quotients of $\mathbf{R}$.
   (b) $\mathbf{Q}$ is a field of quotients of $\mathbf{Z}$.
   (c) $\mathbf{R}$ is a field of quotients of $\mathbf{Z}$.
   (d) If D is any field then the field of quotients of D is isomorphic to D.

Answers.

3. (a) T (b) T (c) F (d) T.

(iii) $b < c \Rightarrow c - b \in S$.
Hence $(a + c) - (a + b) = c - b \in S$.
$\therefore \quad a + b < a + c$.

(iv) $b < c \Rightarrow c - b \in S$. Also $a \in S$.
Hence $a(c - b) \in S$.
$\therefore \quad ac - ab \in S$. Hence $ab < ac$.

Theorem 4.34. The field of complex numbers is not an ordered field.

Proof. Suppose **C** is an ordered field. Let S be a set of positive elements of **C**. Consider the complex number i.

Then either $i \in S$ or $-i \in S$.

$i \in S \Rightarrow i^2, i^4 \in S \Rightarrow -1, 1 \in S$ and

$-i \in S \Rightarrow (-i)^2, (-i)^4 \in S \Rightarrow -1, 1 \in S$.

Thus in either case we get a contradiction.

Hence **C** is not an ordered field.

Definition. Let D be an ordered integral domain and $a \in D$. We define,

$$|a| = \begin{cases} a \text{ if } a \geq 0 \\ -a \text{ if } a < 0 \end{cases}$$

$|a|$ is called the ***absolute value*** of a.

Exercises

Show that in an ordered integral domain the following are true.

1. $|ab| = |a|\,|b|$.
2. $|a + b| \leq |a| + |b|$.
3. $a + x < a + y$ iff $x < y$.
4. If $a > 0$, then $ax < ay \Leftrightarrow x < y$.
5. If $a < 0$, then $ax < ay \Leftrightarrow x > y$.
6. $a < b \Leftrightarrow a^3 < b^3$.

4.13. Unique factorization domain (U.F.D.)

The reader is familiar with the concept of divisibility in **Z**. Further any integer can be uniquely expressed as a product of prime numbers. In this section we introduce the notation of divisibility and factorization in any commutative ring.

Definition. Let R be a commutative ring.

Let $a, b \in R$ and $a \neq 0$. We say that a ***divides*** b and write $a|b$ if there exists an element $c \in R$ such that $b = ac$. If $a|b$ we say that a is a ***divisor*** or a ***factor*** of b.

Examples

1. In **Z**, $2|6$ since $6 = 2 \times 3$. However in $2\mathbf{Z}$, 2 does not divide 6 since there is no element $c \in 2\mathbf{Z}$ such that $6 = 2c$.
2. In $\mathbf{Z}_5$, $2|3$ since $3 = 2 \odot 4$.
3. Let R be commutative ring with identity. Let u be a unit in R. Then u divides any element a of R.

   For, since u is a unit, u^{-1} exists and

   $u^{-1}u = uu^{-1} = 1$.

   $\therefore \quad a = 1a = (uu^{-1})a = u(u^{-1}a) = uc$ where $c = u^{-1}a \in R$.

   $\therefore \quad u|a$.
4. In a field F every non-zero element is a unit and hence every non-zero element divides every element of F.

Exercises

1. Let R be a commutative ring. Let $a, b, c \in R$ and $a \neq 0$. Prove that
   (a) $a|b$ and $a|c \Rightarrow a|(b \pm c)$.
   (b) $a|b$ and $a|c \Rightarrow a|bc$.
2. Let R be a commutative ring with identity. Let a be a non-zero element of R. Prove that $a|1$ iff a is a unit in R.

Definition. Let R be a commutative ring. Let a, b be two non-zero elements of R. Then a and b are said to be ***associates*** if $a|b$ and $b|a$.

Examples

1. In **Z**, for any non-zero integer a, a and $-a$ are associates. In general in any commutative ring

R with identity, for any non-zero element a of R, a and $-a$ are associates.

2. In $2\mathbf{Z}$, 2 does not divide 2. Hence 2 is not an associate of 2.

3. In $\mathbf{Z}_8$, 2 and 6 are associates.

   For, $2 = 6 \odot 3$ and hence $6|2$,

   Also, $6 = 2 \odot 3$ and hence $2|6$.

Exercises

1. Let R be a commutative ring with identity. In $R - \{0\}$ we define $a \sim b$ if a and b are associates. Prove that $\sim$ is an equivalence relation.
2. Is the above result valid if R does not have an identity?

Theorem 4.35. Let R be an integral domain. Let a and b be two non-zero elements of R. Then a and b are associates iff $a = bu$ where u is a unit in R.

Proof. Let a and b be associates. Then $a|b$ and $b|a$. Hence there exist elements $c, d \in R$ such that $b = ac$ and $a = bd$.

$$\therefore \quad a = bd = (ac)d = a(cd).$$

Now, since R is an integral domain cancellation law is valid in R.

$\therefore$ $1 = cd$ and hence c and d are units.

$\therefore$ $a = bd$ where d is a unit.

Conversely, let $a = bu$ where u is a unit in R.

Then $b|a$.

Also, $au^{-1} = b$ (since u is a unit).

$\therefore$ $a|b$ and hence a and b are associates.

Note. Let R be a commutative ring. Let a be a non-zero element of R. Then the units in R and the associates of a are divisors of a.

Definition. Let R be a commutative ring with identity. Let $a \in R$ and $a \neq 0$. a is called a ***prime*** or an ***irreducible element*** if a is not a unit and its only divisors are units in R and associates of a.

Thus a prime element is an element of R which cannot be factored in R in a non-trivial way.

Definition. An integral domain R is said to be a ***unique factorization domain (U.F.D.)*** if

(i) any non-zero element in R which is not a unit can be expressed as the product of a finite number of prime elements.

(ii) the factorization in (i) is unique up to the order and associates of the prime elements.

(ie.,) If $a = p_1 p_2 \ldots\ldots p_r = q_1 q_2 \ldots\ldots q_s$ where the p_i's and q_j's are prime elements, then $r = s$ and each p_i is an associate of some q_j.

For example $\mathbf{Z}$ is a *U.F.D.*

In the next few sections we give some more examples of *U.F.D.*

Definition. Let R be a *U.F.D.* Let $a, b \in R$. Then an element $d \in R$ is said to be a ***greatest common divisor*** (*g.c.d*) of a and b if

(i) $d|a$ and $d|b$.

(ii) $c|a$ and $c|b \Rightarrow c|d$.

The *g.c.d.* of a and b is denoted by (a, b).

Exercises

1. If d is a g.c.d. of a and b prove that any associate of d is also a *g.c.d* of a and b.
2. Prove that in a *U.F.D* any two elements have a g.c.d.

4.14. Euclidean domain

In this section we introduce an important class of rings called Euclidean domains and prove that every Euclidean domain is a unique factorization domain. The concept of Euclidean domain is motivated by the divisibility properties in $\mathbf{Z}$.

Definition. Let R be a commutative ring without zero-divisors. R is called an ***Euclidean domain*** or an ***Euclidean ring*** if for every non-zero element $a \in R$,

there is defined a non-negative integer $d(a)$ satisfying the following conditions.

(i) For any two non-zero elements $a, b \in R$, $d(a) \leq d(ab)$.

(ii) For any two non-zero elements $a, b \in R$, there exist $q, r \in R$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

Examples

1. $\mathbf{Z}$ is an Euclidean domain where $d(a) = |a|$.

Proof. $d(ab) = |ab| = |a||b| \geq |a| = d(a)$.

Let a, b be two non-zero elements of $\mathbf{Z}$. Let q be the quotient and r be the remainder when a is divided by b.

Then $a = qb + r$ and $0 \leq r < |b|$.
Hence $\mathbf{Z}$ is an Euclidean domain.

2. Any field F is an Euclidean domain where $d(a) = 1$ for all $a \in F - \{0\}$.

Proof. $d(a) = d(ab) = 1$ for all $a \in F - \{0\}$. Hence $d(a) \leq d(ab)$.

Also, $a = (ab^{-1})b + 0$ so that $q = ab^{-1}$ and $r = 0$.

$\therefore$ Condition (ii) is satisfied. Hence F is an Euclidean domain.

3. The ring of Gaussian integers $R = \{a+bi / a, b \in \mathbf{Z}\}$ is an Euclidean domain where we define $d(a + ib) = a^2 + b^2$.

Proof. Let $x = a + ib$ and $y = c + id$ be two non-zero elements in R. Then

$$\begin{aligned} d(xy) &= d[(a + ib)(c + id)] \\ &= d[(ac - bd) + i(ad + bc)] \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &\geq a^2 + b^2 \\ &= d(x). \end{aligned}$$

$\therefore \quad d(xy) \geq d(x)$.

Now, to prove condition (ii), let $\frac{a + bi}{c + di} = p + iq$.

Then $p = \frac{ac + bd}{c^2 + d^2}$ and $q = \frac{bc - ad}{c^2 + d^2}$ and hence $p, q \in \mathbf{Q}$.

Now, let $m, n \in \mathbf{Z}$ be such that $|p - m| \leq \frac{1}{2}$ and $|q - n| \leq \frac{1}{2}$.

Let $p - m = \alpha$ and $q - n = \beta$ so that $|\alpha| \leq \frac{1}{2}$ and $|\beta| \leq \frac{1}{2}$.

Now,

$$\begin{aligned} a + bi &= (c + di)(p + qi) \\ &= (c + di)[(\alpha + m) + (\beta + n)i] \\ &= (c + di)(m + ni) + r \\ &\qquad \text{where } r = (c + di)(\alpha + \beta i) \end{aligned}$$

Now, $a + bi, c + di, m + ni \in R$ and hence $r \in R$.

If $r \neq 0$, then

$$\begin{aligned} d(r) &= (c^2 + d^2)(\alpha^2 + \beta^2) \\ &\leq (c^2 + d^2)\left(\tfrac{1}{4} + \tfrac{1}{4}\right) \\ &< c^2 + d^2 \\ &= d(y). \end{aligned}$$

$\therefore \quad d(r) < d(y)$.

$\therefore \quad R$ is an Euclidean domain.

Theorem 4.36. Let R be an Euclidean domain and I be an ideal of R. Then there exists an element $a \in I$ such that $I = aR$. (ie.,) Every ideal of an Euclidean domain is a principal ideal.

Proof. If $I = \{0\}$, then we take $a = 0$. Hence we assume that $I \neq \{0\}$.

Let $a \in I$ be a non-zero element such that $d(a)$ is minimum. (This is possible since d takes only non-negative integer values).

Now, we claim that $I = aR$.

Let $x \in I$. Then there exist $q, r \in R$ such that $x = qa + r$ where $r = 0$ or $d(r) < d(a)$.

$\therefore$ Now, $a \in I \Rightarrow qa \in I$ (since I is an ideal).

Also $x \in I$. Hence $r = x - qa \in I$.

Now, suppose $r \neq 0$. Then $d(r) < d(a)$.

$\therefore$ r is an element of I such that $d(r) < d(a)$ which is a contradiction to the choice of a and hence $r = 0$.

$\therefore$ $x = qa$ and hence $I = aR$.

Theorem 4.37. Any Euclidean domain R has an identity element.

Proof. Since R is an ideal of R, there exists $c \in R$ such that $R = cR$.

$\therefore$ Every element of R is a multiple of c.

In particular $c = ec$ for some $e \in R$.

Now, let $x \in R$. Then $x = cy$ for some $y \in R$.

$\therefore$ $ex = e(cy) = (ec)y = cy = x$.

$\therefore$ e is the required identity element.

Theorem 4.38. Any Euclidean domain R is a principal ideal domain.

Proof. By definition of Euclidean domain R is a commutative ring without zero-divisors. By theorem 4.37 R has an identity element. Hence R is an integral domain. Also every ideal of R is a principal ideal. Hence R is a principal ideal domain.

Theorem 4.39. Let R be an Euclidean domain. Let a and b be two non-zero elements of R. Then

(i) b is not a unit in $R \Rightarrow d(a) < d(ab)$.
(ii) b is a unit in $R \Rightarrow d(a) = d(ab)$.

Proof. (i) Suppose b is not a unit in R.
By definition of Euclidean domain there exist elements $q, r \in R$ such that
$a = q(ab) + r$ ...(1)
where either $r = 0$ or $d(r) < d(ab)$.
Now, suppose $r = 0$ then $a = q(ab)$.

$\therefore$ $a - q(ab) = 0$.

$\therefore$ $a(1 - qb) = 0$.

Now, R has no zero-divisors and $a \neq 0$.
$\therefore$ $1 - qb = 0$. Hence $qb = 1$.
$\therefore$ b is a unit in R *which is a contradiction.*
$\therefore$ $r \neq 0$. Hence $d(r) < d(ab)$. ... (2)

Now, $r = a(1 - qb)$ (by 1)

$\therefore$ $d(r) = d[a(1 - bq)] \geq d(a)$. ... (3

$\therefore$ $d(a) \leq d(r) < d(ab)$ (by (2) and (3)

$\therefore$ $d(a) < d(ab)$.

(ii) Suppose b is a unit in R.
Now, $d(a) \leq d(ab)$.

Also $d(a) = d[(ab)b^{-1}] \geq d(ab)$.

$\therefore$ $d(a) \geq d(ab)$.

$\therefore$ $d(a) = d(ab)$.

Theorem 4.40. Let a be a non-zero element of an Euclidean domain R. Then a is a unit in R iff

$d(a) = d(1)$.

Proof. Suppose a is a unit in R.

$\therefore d(a) = d(aa^{-1})$ (by Theorem 4.39)
$= d(1)$.

Conversely, let $d(a) = d(1)$.

Suppose a is not a unit in R.

Then $d(1a) > d(1)$ (by Theorem 4.39)

$\therefore$ $d(a) > d(1)$ which is a contradiction.

$\therefore$ a is a unit.

Theorem 4.41. Let a be a non-zero element of an Euclidean domain R. If $d(a) = 0$, then a is a unit in R.

Proof. Suppose a is not a unit in R.

Then $d(1) < d(1a)$ (by theorem 4.39)

$\therefore$ $d(1) < d(a) = 0$. Hence $d(1) < 0$ which is a contradiction since d takes only non-negative values.

Theorem 4.42. Let R be an Euclidean domain. Then any two elements $a, b \in R$ have a g.c.d. and it is of the form $ax + by$ where $x, y \in R$.

Proof. Let $A = \{ax + by / x, y \in R\}$.

We claim that A is an ideal of R.

Let $u, v \in A$. Then $u = ax_1 + by_1$ and $v = ax_2 + by_2$.

$\therefore \quad u - v = a(x_1 - x_2) + b(y_1 - y_2) \in A.$

Now, let $c \in R$. Then

$$uc = (ax_1 + by_1)c$$
$$= a(x_1c) + b(y_1c) \in A.$$

$\therefore$ A is an ideal of R.

Now, since R is an Euclidean domain it is a principal ideal domain. Hence A is a principal ideal of R.

Now, let $d \in A$ be such that $A = (d)$.

$\therefore \quad d = ra + sb$ where $r, s \in R$.

Now, $a = 1a + 0b \in A$ and $b = 0a + 1b \in A$.

$\therefore \quad a = da_1$ and $b = db_1$ for some $a_1, b_1 \in R$.

$\therefore \quad d|a$ and $d|b$.

Now, suppose $l \in R$ and $l|a$ and $l|b$.

Then $l|(ra + sb)$ so that $l|d$.

$\therefore \quad d$ is the required g.c.d. of a and b.

Remark. The g.c.d of any two integers can be found by applying the Euclidean algorithm. A similar procedure can be used to find the g.c.d. of any two non-zero elements of an Euclidean domain R.

Let $a, b \in R - \{0\}$.

Let $a = bq_1 + r_1$ where either $r_1 = 0$ or $d(r_1) < d(b)$.

If $r_1 \neq 0$, let $b = r_1q_2 + r_2$ where either $r_2 = 0$ or $d(r_2) < d(r_1)$. In general if $r_i \neq 0$, let r_{i+1} be such that $r_{i-1} = r_iq_{i+1} + r_{i+1}$ where either $r_{i+1} = 0$ or $d(r_{i+1}) < d(r_i)$. Then the sequence $r_1, r_2, \ldots\ldots$ must terminate with some $r_n = 0$. If $r_1 = 0$, then b is a g.c.d. of a and b. If $r_1 \neq 0$ let $i > 1$ be the first integer such that $r_i = 0$. Then r_{i-1} is the g.c.d. of a and b.

Definition. Two elements a and b of an Euclidean domain R are said to be ***relatively prime*** if their g.c.d. is a unit in R.

Remark. If a and b are relatively prime, we may assume without loss of generality that $(a, b) = 1$.

Theorem 4.43. Let R be an Euclidean domain. Let $a, b, c \in R$. Then $a|bc$ and $(a, b) = 1 \Rightarrow a|c$.

Proof. Since $(a, b) = 1$, there exist $x, y \in R$ such that $ax + by = 1$.

$\therefore \quad acx + bcy = c$.

Now, $a|acx$. Also $a|bc \Rightarrow a|bcy$.

$\therefore \quad a|(acx + bcy)$. Hence $a|c$.

Theorem 4.44. Let p be a prime element in an Euclidean domain R. Let $a, b \in R$.

Then $p|ab \Rightarrow p|a$ or $p|b$.

Proof. Suppose p does not divide a.

Then $(p, a) = 1$ (since p is prime)

$\therefore \quad$ By theorem 4.43, we have $p|b$.

Corollary. Let p be a prime element in an Euclidean domain R. Let $a_1, a_2, \ldots\ldots\ldots, a_n \in R$.

Then $p|a_1a_2 \ldots\ldots a_n \Rightarrow p$ divides at least one a_i.

Theorem 4.45. Any Euclidean domain R is a *U.F.D.*

Proof. First we shall prove that any element a in R is either a unit or can be expressed as the product of a finite number of prime elements of R.

We prove this by induction on $d(a)$.

If $d(a) = d(1)$ then a is a unit in R (by Theorem 4.40).

Hence the assertion is true. Now, we assume that the result is true for all $x \in R$ such that $d(x) < d(a)$ and prove that the result is true for a.

If a is a prime there is nothing to prove.

If not, $a = bc$ where neither b or c is a unit in R.

$\therefore \quad d(b) < d(a)$ and $d(c) < d(a)$ (by Theorem 4.39).

Now, by induction hypothesis b and c can be written as the product of a finite number of prime elements.

Hence a can be expressed as a product of a finite number of prime elements.

We now prove the uniqueness.

Let $a = p_1p_2 \ldots p_r = q_1q_2 \ldots q_s$ where p_is and q_is are prime elements of R.

$\therefore \quad p_1|q_1q_2 \ldots q_s$.

$p_1 | q_i$ for some i. Without loss of generality we assume that $p_1 | q_1$. Since p_1 and q_1 are both prime elements of R, p_1 and q_1 must be associates.

$\therefore \quad q_1 = u_1 p_1$ where u_1 is a unit in R.

$\therefore \quad p_1 p_2 \dots p_r = u_1 p_1 q_2 q_3 \dots q_s$.

$\therefore \quad p_2 p_3 \dots p_r = u_1 q_2 q_3 \dots q_s$.

Now, if $r < s$, repeating the above argument r times the left side becomes 1 and the right side contains a product of some prime elements which is impossible.

Hence $r \geq s$.

Similarly $s \geq r$ and hence $r = s$.

Further we have shown that every p_i is an associate of some q_j and conversely. Hence the theorem.

Solved problems

Problem 1. Show that $1 + i$ is a prime element in the ring R of Gaussian integers.

Solution. Suppose $(a + bi) | (1 + i)$.

Then there exist an element $c + id \in R$ such that $(a + bi)(c + di) = 1 + i$.

$\therefore \quad d[(a + bi)(c + di)] = d(1 + i)$.

$\therefore \quad (a^2 + b^2)(c^2 + d^2) = 2$ and $a, b, c, d \in \mathbf{Z}$.

$\therefore \quad a^2 + b^2 = 1$ or $c^2 + d^2 = 1$.

$\therefore \quad d(a + ib) = d(1)$ or $d(c + id) = d(1)$.

$\therefore$ Either $a + ib$ or $c + id$ is a unit in R (by Theorem 4.40)

Hence $1 + i$ is a prime element of R.

Problem 2. Prove that 5 is not prime element in the ring R of Gaussian integers.

Solution. $5 = (2 + i)(2 - i)$
and $d(2 + i) = d(2 - i) = 5 > d(1)$.

Hence neither $2 + i$ nor $2 - i$ is a unit in R.

Hence 5 is not a prime element of R.

Problem 3. Find the g.c.d. of $16 + 7i$ and $10 - 5i$ in the ring R of Gaussian integers.

Solution. Let $a = 16 + 7i$ and $b = 10 - 5i$.

$$\therefore \quad \frac{a}{b} = \frac{16 + 7i}{10 - 5i} = \frac{(16 + 7i)(10 + 5i)}{(10 - 5i)(10 + 5i)}$$

$$= 1 + \frac{6i}{5} = 1 + i + \frac{i}{5}.$$

$\therefore \quad a = (1 + i)b + (1 + 2i)$.

Let $q_1 = 1 + i$ and $r_1 = 1 + 2i$.

Now, $\dfrac{b}{r_1} = \dfrac{10 - 5i}{1 + 2i} = 4 - 3i$ (verify)

$\therefore \quad b = (4 - 3i)(1 + 2i) + 0$.

Hence g.c.d. of a and b is $r_1 = 1 + 2i$.

Exercises

1. If a and b are associates in an Euclidean domain R, prove that $d(a) = d(b)$.
2. Is $\mathbf{Z}$, with $d(a) = a^2$ where $a \neq 0$, a Euclidean domain?
3. Prove that in the ring of Gaussian integers, an element x with $d(x) = p$ where p is a prime in $\mathbf{Z}$ is a prime element.
4. Prove that the element 7, $4 + 3i$ and $6 - 7i$ are not prime elements in the ring of Gaussian integers.
5. Find the g.c.d. of the following members in the ring of Gaussian integers
   (a) $1 + 6i$ and $5 - 15i$
   (b) $3 + 4i$ and $4 - 3i$
   (c) $11 + 7i$ and $18 - i$.
6. Express 7, 8 and $10 + 5i$ into prime factors in the ring of Gaussian integers.
7. Prove that $d(-a) = d(a)$ for any non-zero element a of an Euclidean ring.

Answers. 5(a) $7 - i$ (b) $3 + 4i$ (c) i

4.15. Every P.I.D is a U.F.D.

In this section we prove that every *P.I.D.* is a *U.F.D.*

Definition. Let R be a ring. We say that the ascending chain condition *(A.C.C)* holds for ideals in R if for every ascending chain of ideals