CHAPTER 12

Introduction to Rings

Motivation and Definition

Many sets are endowed with two operations, addition and multiplication. An abstract concept that takes this into consideration is the ring.

DEFINITION (Ring). A ring R is a nonempty set with two binary operations, usually denoted as addition and multiplication such that

(1) R with addition is an Abelian group.

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

(3) For all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

DEFINITION.

(1) A ring R is commutative if its multiplication is commutative.

(2) A ring R is a ring with identity if there is a multiplicative identity or unity $1 \neq 0$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

(3) A nonzero element a of a commutative ring with unity is a unit of the ring if there exists $a^{-1} \in R$ such that $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

(4) If $a \neq 0$ and b are in a commutative ring R, we say $a|b$ or a is a factor of b if there exists $c \in R$ such that $ac = b$. We write $a \nmid b$ if a does not divide b.

NOTE. a is a unit of R if $a|1$.

RECALL. na in an additive group means $\underbrace{a + a + \cdots + a}_{n \text{ terms}}$.

When there is a possibility of confusion, we will indicate this as $n \cdot a$.

Example.

(1) $\mathbb{Z}$ is a commutative ring with *unity* 1. 1 and -1 are the only units.

(2) $\mathbb{Z}_n$ with addition and multiplication modulo n is a commutative ring with identity. The set of units is $U(n)$.

(3) The set $\mathbb{Z}[x]$ of all polynomials in x with integer coefficientsunder ordinary addition and multiplication of polynomials is a commutative with identity $f(x) = 1$.

(4) $M_2(\mathbb{Z})$, the set of 2×2 matrices with integer entries is a noncommutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(5) The set $3\mathbb{Z}$ of multiples of 3 under ordinary addition and multiplication is a commutative ring without identity.

(6) $F = \{f : \mathbb{R} \to \mathbb{R}\}$ is a commutative ring with identity where

$$(f + g)(x) = f(x) + g(x) \text{ and } (fg)(x) = f(x)g(x).$$

$f(x) = 0$ is the zero function and $g(x) = 1$ is the identity.

(7) Let $R_1, R_2, \dots, R_n$ be rings. Then

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2, \dots, a_n) | a_i \in R_i\}$$

is a ring with componentwise addition and multiplication, i.e.,

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

and

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n).$$

This is the <u>direct sum</u> of $R_1, R_2, \dots, R_n$.

Properties of Rings

THEOREM (12.1 — Rules of Multiplication). *Let $a, b, c \in R$, a ring. Then*

(1) $a0 = 0a = 0$.

PROOF.

$$0 + a0 = a0 = a(0 + 0) = a0 + a0 \Longrightarrow a0 = 0 \text{ by right cancellation.}$$
$$0a + 0 = 0a = (0 + 0)a = 0a + 0a \Longrightarrow 0a = 0 \text{ by left cancellation.}$$

□

(2) $a(-b) = (-a)b = -(ab)$.

PROOF.

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

The second part is analogous. □

(3) $(-a)(-b) = ab$.

PROOF.

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

□

(4) $a(b - c) = ab - ac$ *and* $(b - c)a = ba - ca$.

PROOF.

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

The other is similar. □

If R has a unit element 1, then

(5) $(-1)a = -a$.

PROOF. Follows directly.from (2). □

(6) $(-1)(-1) = 1$.

PROOF. Follows directly.from (3). □

THEOREM (12.2 — Uniqueness of the Unit and Inverses). *If a ring has an identity, it is unique. If a ring element has a multiplicative inverse, it is unique.*

PROOF. Same as for groups. □

NOTE. In general, if $a \neq 0$ and $ab = ac$, we cannot conclude $b = c$ (a may not have a multiplicative inverse). Also, if $a^2 = a$, we cannot conclude $a = 0$ or $a = 1$ (the ring may not have a unit 1). We do not have a multiplicative group.

Subrings

DEFINITION (Subring). A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

THEOREM (12.3 — Subring Test). *A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication, i.e., if $a, b \in S \Longrightarrow a - b \in S$ and $ab \in S$.*

PROOF.

Since $a, b \in S \Longrightarrow a - b \in S$, S is an Abelian group by the one-step subgroup test. The associative and distributive properties of S follow from those of R. The closure condition assures that multiplication in S is a binary operation. □

EXAMPLE.

(1) $\{0\}$, the trivial subring, and R are subrings of any ring R.

(2) $\{0, 3, 9\}$ is a subring of $\mathbb{Z}_{12}$. Although 1 is the identity of $\mathbb{Z}_{12}$, 9 is the identity of the subring.

(3) For all positive integers n, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ is a subring of $\mathbb{Z}$.

(4) The <u>Gaussian integers</u> $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

(5) $\{f : \mathbb{R} \to \mathbb{R} : f(a) = 0\}$ for some fixed $a \in \mathbb{R}$ is a subring of
$F = \{f : \mathbb{R} \to \mathbb{R}\}$. So is $\{f : \mathbb{R} \to \mathbb{R} | f \text{ is continous}\}$.

(6) The set $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}$ of diagonal matrices is a subring of all 2×2 matrices over $\mathbb{Z}$.

We can use a subring lattice diagram to show the relationship between a ring and its various subrings. In this diagram, any ring is a subring of all the rings it is connected to by one or more upward lines.

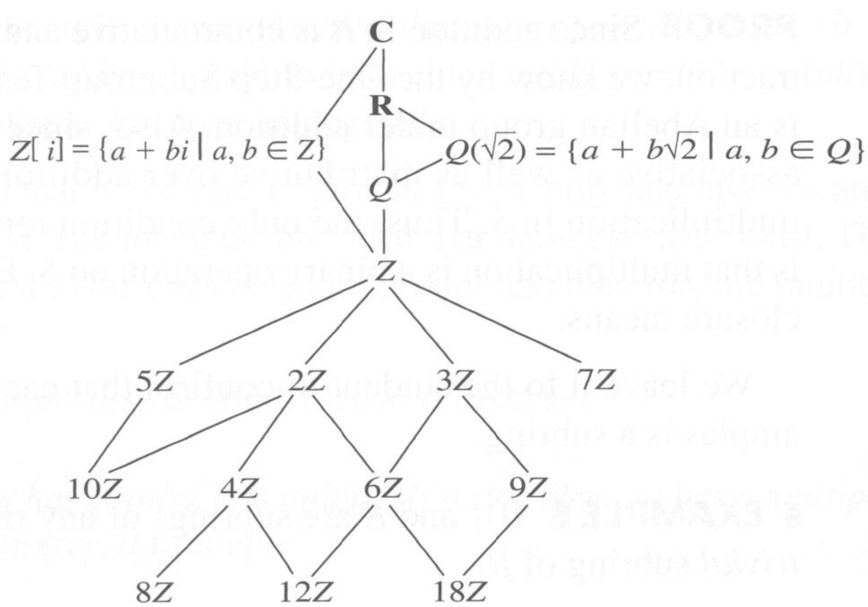

Figure 12.1 Partial subring lattice diagram of C.