Corollary: For every prime p, Z_p, the ring of integers modulo p, is a field.

Pf:- $Z_p = \{0, 1, 2, \ldots, p-1\}$

clearly Z_p is a finite set.

Since every finite integral domain is a field so it is enough to show Z_p is an integral domain. For this it is enough to show that Z_p has no zero divisors.

Suppose that $a, b \in Z_p$ and $a \times_p b = 0$

then $p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$ [by Euclids Lemma]

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

$\therefore Z_p$ is an integral domain. As Z_p is finite so Z_p is a field.

Euclid's Lemma: If p is a prime number and $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Ex. Show that $Z \oplus Z$ is a ring but not an integral domain.

Soln:-

$$Z \oplus Z = \{(a, b) \mid a, b \in Z\}$$

For $x = (a_1, b_1)$, $y = (a_2, b_2) \in Z \oplus Z$

$x + y = (a_1 + a_2, b_1 + b_2) \in Z \oplus Z$ as $a_1 + a_2 \in Z$, $b_1 + b_2 \in Z$

$xy = (a_1 a_2, b_1 b_2) \in Z \oplus Z$ as $a_1 a_2 \in Z$, $b_1 b_2 \in Z$

For $x = (a_1, b_1)$, $y = (a_2, b_2)$, $z = (a_3, b_3)$ in $Z \oplus Z$, (How they to show)

(1) $x + y = y + x$

(2) $(x + y) + z = x + (y + z)$

(3) ~~For $x \in Z \oplus Z$, $\exists$~~

(3) $0 = (0, 0) \in Z \oplus Z$ and $x + 0 = x$

(4) For $x \in Z \oplus Z$, $\exists -x \in Z \oplus Z$ s.t. ~~$x + (-x) = 0$~~ $x + (-x) = 0$

(5) $x(yz) = (xy)z$

(6) $x \cdot (y + z) = xy + xz$ and $(y + z)x = yx + zx$

Let $x = (0, 2)$, $y = (1, 0)$ $(\mathbb{Z} \oplus \mathbb{Z}$

then neither $x = 0$ nor $y = 0$

But $xy = (0, 2)(1, 0) = (0, 0) = 0$.

$\therefore$ $\mathbb{Z} \oplus \mathbb{Z}$ is with zero divisors. Hence

$\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain.

EXAMPLE 9 Field with Nine Elements

Let $$Z_3[i] = \{a + bi \mid a, b \in Z_3\}$$
$$= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\},$$

where $i^2 = -1$. This is the ring of Gaussian integers modulo 3. Elements are added and multiplied as in the complex numbers, except that the coefficients are reduced modulo 3. In particular, $-1 = 2$. Table 13.1 is the multiplication table for the nonzero elements of $Z_3[i]$. ◆

EXAMPLE 10

Let $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$. It is easy to see that $Q[\sqrt{2}]$ is a ring. Viewed as an element of $\mathbf{R}$, the multiplicative inverse of any nonzero element of the form $a + b\sqrt{2}$ is simply $1/(a + b\sqrt{2})$. To verify that $Q[\sqrt{2}]$ is a field, we must show that $1/(a + b\sqrt{2})$ can be written in the form $c + d\sqrt{2}$. In high school algebra, this process is called "rationalizing the denominator." Specifically,

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

TABLE 13.1 Multiplication Table for $Z_3[i]$

	1	2	i	$1 + i$	$2 + i$	$2i$	$1 + 2i$	$2 + 2i$
1	1	2	i	$1 + i$	$2 + i$	$2i$	$1 + 2i$	$2 + 2i$
2	2	1	$2i$	$2 + 2i$	$1 + 2i$	i	$2 + i$	$1 + i$
i	i	$2i$	2	$2 + i$	$2 + 2i$	1	$1 + i$	$1 + 2i$
$1 + i$	$1 + i$	$2 + 2i$	$2 + i$	$2i$	1	$1 + 2i$	2	i
$2 + i$	$2 + i$	$1 + 2i$	$2 + 2i$	1	i	$1 + i$	$2i$	2
$2i$	$2i$	i	1	$1 + 2i$	$1 + i$	2	$2 + 2i$	$2 + i$
$1 + 2i$	$1 + 2i$	$2 + i$	$1 + i$	2	$2i$	$2 + 2i$	i	1
$2 + 2i$	$2 + 2i$	$1 + i$	$1 + 2i$	i	2	$2 + i$	1	$2i$

DEFINITION *Characteristic of a Ring*

The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.

Thus, the ring of integers has characteristic 0, and Z_n has characteristic n. An infinite ring can have nonzero characteristic. Indeed, the ring $Z_2[x]$ of all polynomials with coefficients in Z_2 has characteristic 2. (Addition and multiplication are done as for polynomials with ordinary integer coefficients except that the coefficients are reduced modulo 2.) When a ring has a unity, the task of determining the characteristic is simplified by Theorem 13.3

Theorem 13.3 Characteristic of a Ring with Unity

Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

PROOF. If 1 has infinite order, then there is no positive integer n such that $n \cdot 1 = 0$, so R has characteristic 0. Now suppose that 1 had additive order n. Then $n \cdot 1 = 0$, and n is the least positive integer with this property. So, for any x in R, we have

$$nx = n(1x) = (n \cdot 1)x = 0x = 0.$$

Thus, R has characteristic n. ■

In the case of an integral domain, the possibilities for the characteristic are severely limited.

Theorem 13.4 **Characteristic of an Integral Domain**

The characteristic of an integral domain is 0 or prime.

PROOF. By Theorem 13.3, it suffices to show that if the additive order of 1 is finite, it must be prime. Suppose that 1 has order n and that $n = st$, where $1 \leq s, t \leq n$. Then

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1).$$

So, $s \cdot 1 = 0$ or $t \cdot 1 = 0$. Since n is the least positive integer with the property that $n \cdot 1 = 0$, we must have $s = n$ or $t = n$. Thus, n is prime. ∎

We conclude this chapter with a brief discussion of polynomials with coefficients from a ring—a topic we will consider in detail in later chapters. The existence of zero-divisors in a ring causes unusual results when one is finding roots of polynomials with coefficients in the ring. Consider, for example, the equation $x^2 - 4x + 3 = 0$. In the integers, we could find all solutions by factoring

$$x^2 - 4x + 3 = (x - 3)(x - 1) = 0$$

and setting each factor equal to 0. But notice that when we say we can find *all* solutions in this manner, we are using the fact that the only way for a product to equal 0 is for one of the factors to be 0—that is, we are using the fact that Z is an integral domain. In Z_{12}, there are many pairs of nonzero elements whose products are 0: $2 \cdot 6 = 0, 3 \cdot 4 = 0, 4 \cdot 6 = 0, 6 \cdot 8 = 0$, and so on. So, how do we find *all* solutions of $x^2 - 4x + 3 = 0$ in Z_{12}? The easiest way is simply to try every element! Upon doing so, we find four solutions: $x = 1$, $x = 3$, $x = 7$, and $x = 9$. Observe that we can find all solutions of $x^2 - 4x + 3 = 0$ over Z_{11} or Z_{13}, say, by setting the two factors $x - 3$ and $x - 1$ equal to 0. Of course, the reason why this works for these rings is that they are integral domains. Perhaps this will convince you that integral domains are particularly advantageous rings. Table 13.2 gives a summary of some of the rings we have introduced and their properties.

TABLE 13.2 Summary of Rings and Their Properties

Ring	Form of Element	Unity	Commutative	Integral Domain	Field	Characteristic
Z	k	1	yes	yes	no	0
Z_n, n composite	k	1	yes	no	no	n
Z_p, p prime	k	1	yes	yes	yes	p
$Z[x]$	$a_n x^n + \cdots + a_1 x + a_0$	$f(x) = 1$	yes	yes	no	0
nZ, $n > 1$	nk	none	yes	no	no	0
$M_2(Z)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	no	no	no	0
$M_2(2Z)$	$\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$	none	no	no	no	0
$Z[i]$	$a + bi$	1	yes	yes	no	0
$Z_3[i]$	$a + bi$; $a, b \in Z_3$	1	yes	yes	yes	3
$Z[\sqrt{2}]$	$a + b\sqrt{2}$; $a, b \in Z$	1	yes	yes	no	0
$Q[\sqrt{2}]$	$a + b\sqrt{2}$; $a, b \in Q$	1	yes	yes	yes	0
$Z \oplus Z$	(a, b)	$(1, 1)$	yes	no	no	0