UNIT 12 THE BASICS

Structure

12.1 INTRODUCTION

In Unit 9 we introduced you to rings, and then to special rings whose speciality lay in the properties of their multiplication. In this unit we will introduce you to yet another type of ring, namely, an integral domain. You will see that an integral domain is a ring with identity in which the product of two non-zero elements is again a non-zero element. We will discuss various properties of such rings.

Next, we will look at rings like Q, R, C, and Z_p (where p is a prime number). In these rings the non-zero elements form an abelian group under multiplication. Such rings are called fields. These structures are very useful, one reason being that we can "divide" in them.

Related to integral domains and fields are certain special ideals called prime ideals and maximal ideals, In this unit we will also discuss them and their corresponding quotient rings.

Finally, we shall see how to construct the smallest field that contains a given integral domain. This is essentially the way that Q is constructed from Z. We call such a field the field of quotients of the corresponding integral domain.

In this unit we have tried to introduce you to a lot of new concepts. You may need some time to grasp them. Don't worry. Take as much time as you need. But by the time you finish it, make sure that you have attained the following objectives. Only then will you be comfortable in the remaining units of this course.

Objectives

After reading this unit; you should be able to

- check whether an algebraic system is an integral domain or not;
- obtain the characteristic of any ring;
- check whether an algebraic system is a field or not;
- define and identify prime ideals and maximal ideals;
- prove and use simple properties of integral domains and fields;
- construct or identify the field of quotients of an integral domain.

12.2 INTEGRAL DOMAINS

You know that the product of two non-zero integers is a non-zero integer, i.e., if $m, n \in Z$ such that $m \neq 0$, $n \neq 0$, then $mn \neq 0$. Now consider the ring Z_6. We find that $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$, yet $\bar{2}.\bar{3} = \bar{0}$. So, we find that the product of the non-zero elements $\bar{2}$ and $\bar{3}$ in Z_6 is zero. As you will soon realise, this shows that $\bar{2}$ (and $\bar{3}$) is a zero divisor, i.e., $\bar{0}$ is divisible by $\bar{2}$ (and $\bar{3}$).

So, let us see what a zero divisor is.

Definition: A non-zero element a in a ring R .is called a **zero divisor** in **R if** there **exists** a non-zero element b in R such that ab = 0.

(Note that b will be a zero divisor too!)

Now do you agree that $\bar{2}$ is a zero divisor in Z,? What about $\bar{3}$ in Z_4? Since $\bar{3}.x \neq \bar{0}$ for every non-zero x in Z_4, $\bar{3}$ is not a zero divisor in Z_4.

Our short discussion may help you to do the following exercise.

E 1) Let $n \in N$ and $m \mid n$, $1 < m < n$. Then show that $\bar{m}$ is a zero divisor in Z_n.

Now ldt us look at an example of a zero divisor in C[0,1]. Consider the function $f \in C[0,1]$ given by

$$f(x) = \begin{cases} x - \frac{1}{2}, & 0 \leq x \leq 1/2 \\ 0, & 1/2 \leq x \leq 1 \end{cases}$$

Let us define $g : [0,1] \to R$ by

$$g(x) = \begin{cases} 0, & 0 \leq x \leq 1/2 \\ x - 1/2, & 1/2 \leq x \leq 1 \end{cases}$$

Then $g \in C[0,1]$, $g \neq 0$ and $(fg)(x) = 0 \; \forall \; x \in [0,1]$. Thus, fg is the zero function. Hence, f is a zero divisor in C[0,1].

For another example, consider the Cartesian product of two non-trivial rings A and B. For every $a \neq 0$ in A, (a,0) is a zero divisor in A x B. This is because, for any $b \neq 0$ in B. (a,0)(0,b) = (0.0).

Now let us look at the ring $\wp(X)$, where X is a set with at least two elements, Each non-empty proper subset **A** of X is a zero divisor because $A.X^c = A \cap A^c = \phi$, the zero element of $\wp(X)$.

Try these exercises now.

E 2) List all the zero divisors in Z.

E 3) For which rings with unity will 1 be a zero divisor?

E 4) Let R be a ring and $a \in R$ be a zero divisor. Then show that every element of the principal ideal Ra is a zero divisor.

Let us now talk of a type of ring that is without zero divisors.

Definition: We call a non-zero ring R an **integral domain** if

i) R is with identity, and

ii) R has no zero divisors.

Thus, an integral domain is a non-zero ring with identity in which the product of two non-zero elements is a non-zero element.

Several authors often shorten the term 'integral domains' to 'domains'. We will do so too,

This kind of ring gets its name from the set of integers, one of its best known examples. Other examples of domains that immediately come to mind are Q, R and C. What about C[0,1]? You have already seen that it has zero divisors. Thus C[0,1] is not a domain,

The next result gives us an important class of examples **of** integral domains.

Theorem 1 : Z_p is an integral domain iff p is a prime number.

Proof : Firstly, let us assume that p is a prime number. Then you know that Z_p is a non-zero ring with identity. Let us see if it has zero divisors. For this, supppose $\bar{a}, \bar{b} \in Z_p$ satisfy $\bar{a}\,\bar{b} = \bar{0}$. Then $\overline{ab} = \bar{0}$, i.e., $p \mid ab$. Since p is a prime number, using E 25 of Unit 1 we see that $p \mid a$ or $p \mid b$. Thus, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. What we have shown is that if $\bar{a} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$, then $\bar{a}\,\bar{b} \neq \bar{0}$. Thus, Z_p is without zero divisors, and hence, is a domain.

Conversely, we will show that if p is not a prime, then Z_p is not a domain, So, suppose p is not a prime. If p = 1, then Z, is the trivial ring, which is not a domain.

If p is a composite number and $m \mid p$, then by E 1 you know that $\bar{m} \in Z_p$ is a zero divisor. Thus, Z_p has zerodivisors. Hence, it is not a domain.

Try this exercise now.

E 5) Which of the following rings are not domains? Why?
Z_4, Z_5, $2Z$, $Z + iZ$, $R \times R$, $\{0\}$.

Now consider a ring R. We know that the cancellation law for addition holds in R, i.e., whenever a+b = a+c in R, then b = c. But, does ab = ac imply b = c? It need not. For example, 0.1 = 0.2 in Z but 1 # 2. So, if a = 0, ab = ac need not imply b = c. But, if a # 0 and ab = ac, is it true that b = c'? We will prove that this is true for integral domains.

Theorem 2: A ring R has no zero divisors if and only if the cancellation law for multiplication holds in R (i.e., if $a,b,c \in R$ such that $a \neq 0$ and $ab = ac$, then $b = c$.)

Proof: Let us first assume that R contains no zero divisors. Assume that $a,b,c \in R$ such that $a \neq 0$ and $ab = ac$. Then $a(b-c) = ab - ac = 0$. As a # 0, and R has no zero divisors, we get $b - c = 0$, i.e., b = c.

Thus, if ab = ac and $a \neq 0$, then b = c.

Conversely, assume that the cancellation law for multiplication holds in R. Let $a \in R$ such that $a \neq 0$. Suppose ab = 0 for some $b \in R$. Then $ab = 0 = a0$. Using the cancellation law for multiplication, we get b = 0. So, a is not a zero divisor, i.e., R has no zero divisors.

Using this theorem we can immediately say that the cancellation law holds for multiplication in an integral domain.

Now, you can use this property of domains to solve. the following exercises.

E 6) In a domain, show that the only solutions of the equation $x^2 = x$ are x = 0 and x = 1.

E 7) Prove that 0 is the only nilpotent element (see Example 9 of Unit 10) in a domain.

Now let us introduce a number associated with an integral domain; in fact, with any ring.

For this let us look at Z_4 first. We know that $4x = \bar{0}\ \forall\ x \in Z_4$. In fact, $8x = \bar{0}$ and $12x = \bar{0}$ also for any $x \in Z_4$.

But 4 is the least element of the set $\{n \in N \mid nx = \bar{0}\ \forall\ x \in Z_4\}$. This shows that 4 is the characteristic of Z_4, as you will see now.

Definition: Let R be a ring. The least positive integer n such that $nx = 0\ \forall\ x \in R$ is called the **characteristic** of R. If there is no positive integer n such that $nx = 0\ \forall\ x \in R$, then we say that the characteristic of R is zero.

We denote the characteristic of the ring R by **char R**.

You can see that char $Z_n = n$ and char Z = 0.

A ring R is without zero divisors if for $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

The following exercises will give you some practice in obtaining the characteristic of a ring.

E 8) Show that char $\wp(X) = 2$, where X is a non-empty set.

E 9) Let R be a ring and char R = m. What is char (R × R)?

Now let us look at a nice result for integral domains. It helps in considerably reducing our labour when we want to obtain the characteristic of a domain.

Theorem 3: Let m be a positive integer and R be an integral domain. Then the following conditions are equivalent.

a) $m\,1 = 0$.

b) $ma = 0$ for all $a \in R$.

c) $ma = 0$ for some $a \neq 0$ in R.

Proof: We will prove (a) ⇒ (b) ⇒ (c) ⇒ (a).

(a) ⇒ (b) : We know that $m\,1 = 0$.

Thus, for any $a \in R$, $ma = m(1a) = (m1)(a) = 0a = 0$, i.e., (b) holds.

(b) ⇒ (c) : If $ma = 0\ \forall\ a \in R$, then if is certainly true for some $a \neq 0$ in R.

(c) ⇒ (a): Let $ma = 0$ for some $a \neq 0$ in R. Then $0 = ma = m(1a) = (m1)a$. As $a \neq 0$ and R is without zero divisors, we get $m1 = 0$.

What Theorem 3 tells us is that to find the characteristic of a domain we only need to look at the set $\{n.1 \mid n \in N\}$.

Let us look at some examples.

i) char Q = 0, since $n.1 \neq 0$ for any $n \in N$.

ii) Similarly, char R = 0 and char C = 0.

iii) You have already seen that chat' $Z_n = n$. Thus, for any positive integer n, there exists a ring with characteristic n.

Now let us look at a peculiarity of the characteristic of a domain.

Theorem 4 : The characteristic of an integral domain is either zero or a prime number.

Proof: Let R be a domain. We will prove that if the characteristic of R is not zero, then it is a prime number. So suppose char R = m, where $m \neq 0$. So m is the least positive integer such that $m.1 = 0$. We will show that m is a prime number by supposing that it is not, and then proving that our supposition is wrong.

So suppose m = st, where $s,t \in N$, $1 < s < m$ and $1 < t < m$. Then $m.1 = 0 \Rightarrow (st).1 = 0 \Rightarrow (s.1)(t.1) = 0$. As R is without zero divisors, we get $s.1 = 0$ or $t.1 = 0$. But, s and t are less than m. So, we reach a contradiction to the fact that m = char R. Therefore, our assumption that m = st, where $1 < s < m$, $1 < t < m$ is wrong. Thus, the only factors of m are 1 and itself. That is, m is a prime number.

You can now use your knowledge of characteristics to solve the following exercises.

E 10) Let R be an integral domain of characteristic p. Prove that

a) $(a+b)^p = a^p + b^p$ and

$(a-b)^p = a^p - b^p$ for all a, $b \in R$.

b) the subset $\{a^p \mid a \in R\}$ is a subring of R.

c) the map $\phi : R \to R : \phi(a) = a^p$ is a ring monomorphism.

d) if R is a finite integral domain, then ϕ is an isomorphism.

E 11) Let R be a ring with unity 1 and char R = m. Define f : Z → R : f(n) = n. 1. Show that f is a homomorphism. What is Kerf?

E 12) Find the characteristic of $\mathbb{Z}_3 \times \mathbb{Z}_4$. Use this ring as an example to show why Theorems 3 and 4 are only true for integral domains.

We will now see what algebraic structure we get after we impose certain restrictions on the multiplication of a domain. If you have gone through our course Linear Algebra, you will already be familiar with the algebraic system that we are going to discuss, namely, a field.

12.3 FIELD

Let (R, +, .) be a ring. We know that (R, +) is an abelian group. We also know that the operation . is commutative and associative. But (R,.) is not an abelian group. Actually, even if R has identity, (R,.) will never be a group since there is no element a ∈ R such that a.0 = 1. But can (R\{0},.) be a group? It can, in sotne cases. For example, from Unit 2 you know that Q* and R* are groups with respect to multiplication. This allows us to say that Q and R are fields, a term we will now define.

Definition: A ring (R, +, .) is called a field if (R\{0},.) is an abelian group.

Thus, for a system (R,+,.) to be a field it must satisfy the ring axioms R1 to R6 as well as the following axioms.

i) . is commutative,

ii) R has identity (which we denote by 1) and $1 \neq 0$, and

iiii) every non-zero element x in R has a multiplicative inverse, which we denote by x^{-1}.

Just as a matter of information we would like to tell you that a ring that satisfies only (ii) and (iii) above, is called a division ring or a skew field or a **non-commutative** field. Such rings are very important in the study of algebra, but we will not be discussing them in this course.

Let us go back to fields now. The notion of a field evolved daring the 19th century through the research of the German mathematicians Richard Dedekind and Leopold Kronecker in algebraic number theory. Dedekind used the German word Körper, which means field, for this concept. This is why you will often find that a field is denoted by K.

As you may have realised, two of the best known examples of fields are R and C. These were the fields that Dedekind considered. Yet another example of a field is the following ring.

Example **1:** Show that $Q + \sqrt{2}Q = \{a + \sqrt{2}b \mid a, b \in Q\}$ is a field.

Solution : From Unit 9 you know that $F = Q + \sqrt{2}Q$ is a commutative ring with identity $1 + \sqrt{2}.0$.

Now, let $a + \sqrt{2}b$ be a non-zero element of F. Then either $a \neq 0$ or $b \neq 0$. Now, using the rationalisation process, we see that

$$(a+\sqrt{2}b)^{-1} = \frac{1}{a+\sqrt{2}b} = \frac{a-\sqrt{2}b}{(a+\sqrt{2}b)(a-\sqrt{2}b)} = \frac{a-\sqrt{2}b}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} + \sqrt{2}\,\frac{(-b)}{a^2-2b^2} \in F$$

(Note that $a^2-2b^2 \neq 0$, since $\sqrt{2}$ is not rational and either $a \neq 0$ or $b \neq 0$.)

Thus, every non-zero element has a multiplicative inverse. Therefore, $Q + \sqrt{2}Q$ is a field.

Can you think of an example of a ring that is not a field? Does every non-zero integer have a multiplicative inverse in Z? No. Thus, Z is not a field.

By now you have seen several examples of fields. Have you observed that all of them happen to be integral domains also? This is not a coincidence. In fact, we have the following result.

Theorem 5: Every field is an integral domain.

Proof: Let F be a field. Then F # {0} and 1 ∈ F. We need to see if F has zero divisors. So. let a and b be elements of F such that ab = 0 and a ≠ 0. As a ≠ 0 and F is a field, a^{-1} exists. Hence, b = 1. b = (a–la) b = a^{-1} (ab) = a^{-1} 0 = 0. Hence, if a ≠0 and ab = 0, we get b = 0, i.e., F has no zero divisors. Thus, F is a domain.

Now you try these exercises!

E 13) Which of the following rings are not fields'?

$2\mathbb{Z}, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Q} \times \mathbb{Q}$

E 14) Will a subring of a field be a field? Why?

Theorem 5 may immediately prompt you to ask if every domain is a field. You have already seen that Z is a domain but not a field. But if we restrict ourselves to finite domains, we find that they are fields.

Theorem *6:* Every finite integral domain is a field.

Proof: Let R = {$a_0 = 0, a_1 = 1, a_2, \ldots, a_n$} be a finite domain. Then R is commutative also. To show that R is a field we must show that every non-zero element of R has a multiplicative inverse.

So, let $a = a_i$ be a non-zero element of R (i.e., $i \neq 0$). Consider the elements $aa_1, \ldots, aa_n$. For every $j \neq 0$, $a_j \neq 0$; and since a # 0, we get $aa_j \# 0$.

Hence, the set $\{aa_1, \ldots, aa_n\} \subseteq \{a_1, \ldots, a_n\}$.

Also, $aa_1, aa_2, \ldots, aa_n$ are all distinct elements of the set $\{a_1, \ldots, a_n\}$, since $aa_j = aa_k \Rightarrow a_j = a_k$, using the cancellation law for multiplication.

Thus, $\{aa_1, \ldots, aa_n\} = \{a_1, \ldots, a_n\}$.

In particular, $a_1 = aa_j$, i.e., $1 = aa_j$ for some j. Thus, a is invertible in R. Hence every non-zero element of R has a multiplicative inverse. Thus. R is a field.

A field whose underlying set is finite is called a finite field.

Using this result we can now prove a theorem which generates several examples of finite fields.

Theorem 7 : $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof : From Thorern 1 you know that $\mathbb{Z}_n$ is a domain if and only if n is a prime number. You also know that $\mathbb{Z}_n$ has only n elements. Now we can apply Theorem 6 to obtain the result.

Theorem 7 unleashes a load of examples of fields : $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$, and so on. Looking at these examples, and other examples of fields, can you say anything about the characteristic of a field? In fact, using Theorems 4 and 5 we can say that.

Theorem **8:** The characteristic of a field is either zero or a prime number.

So far the examples of finite fields that you have seen have consisted of p elements, for some prime p. In the following exercise we give you an example of a finite field for which this is not so.

E 15) Let R = {0,1,a,1+a}. Define + and . in R as given in the following Cayley tables.

+	0	1	a	1+a
0	0	1	a	1+a
1	1	0	1+a	a
a	a	1+a	0	1
1+a	1+a	a	1	0

and

.	0	1	a	1+a
0	0	0	0	0
1	0	1	a	1+a
a	0	a	1+a	1
1+a	0	1+a	1	a

Show that R is a field. Find the characteristic of this field.

Let us now look at an interesting condition for a ring to be a field.

Theorem 9: Let R be a ring with identity. Then R is a field if and only if R and $\{0\}$ are the only ideals of R.

Proof: Let us first assume that R is a field. Let I be an ideal of R. If $I \neq \{0\}$, there exists a non-zero element $x \in I$. As $x \neq 0$ and R is a field, $xy = 1$ for some $y \in R$. Since $x \in I$ and I is an ideal, $xy \in I$, i.e., $1 \in I$.

Thus, by Theorem 4 of Unit 10, $I = R$. So, the only ideals of R are $\{0\}$ and R.

Conversely, assume that R and $\{0\}$ are the only ideals of R. Now, let $a \neq 0$ be an element of R. Then you know that the set $Ra = \{ra \mid r \in R\}$ is a non-zero ideal of R. Therefore, $Ra = R$. Now, $1 \in R = Ra$. Therefore, $1 = ba$ for some $b \in R$, i.e., a^{-1} exists. Thus, every non-zero element of R has a multiplicative inverse. Therefore, R is a field.

This result is very useful. You will be applying it again and again in the rest of the units of this block.

Using Theorem 9, we can obtain some interesting facts about field homomorphisms (i.e., ring homomorphisms from one field to another). We give them to you in the form of an exercise.

E 16) Let $f : F \to K$ be a field homomorphism. Show that either f is the zero map or f is 1–1.

E 17) Let R be a ring isomorphic to a field F. Show that R must be a field.

E 17 again goes to show that isomorphic algebraic structures must be algebraically identical.

Now that we have discussed domains and fields, let us look at certain ideals of a ring, with respect to which the quotient rings are domains or fields.

12.4 PRIME AND MAXIMAL IDEALS'

In $\mathbb{Z}$ we know that if p is a prime number and p divides the product of two integers a and b, then either p divides a or p divides b. In other words, if $ab \in p\mathbb{Z}$, then either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. Because of this property we say that $p\mathbb{Z}$ is a prime ideal, a term we will define now.

Definition: A proper ideal P of a ring R is called a prime ideal of R if whenever $ab \in P$ for $a, b \in R$, then either $a \in P$ or $b \in P$.

You can see that $\{0\}$ is a prime ideal of Z because $ab \in \{0\} \Rightarrow a \in \{0\}$ or $b \in \{0\}$, where $a,b \in \mathbb{Z}$.

Another example of a prime ideal is

Example 2: Let R be an integral domain. Show that $I = \{(0,x) \mid x \in R\}$ is a prime ideal of $R \times R$.

Solution : Firstly, you know that I is an ideal of $R \times R$. Next, it is a proper ideal since $I \neq R \times R$. Now, let us check if I is a prime ideal or not. For this let $(a_1,b_1), (a_2,b_2) \in R \times R$ such that $(a_1,b_1)(a_2,b_2) \in I$. Then $(a_1a_2, b_1b_2) = (0,x)$ for some $x \in R$ $\therefore a_1a_2 = 0$, i.e., $a_1 = 0$ or $a_2 = 0$, since R is a domain. Therefore, $(a_1,b_1) \in I$ or $(a_2, b_2) \in I$. Thus, I is a prime ideal.

Try the following exercises now. They will help you get used to prime ideals.

E 18) Show that the set $I = \{f \in C[0,1] \mid f(0) = 0\}$ is a prime ideal of $C[0,1]$.

E 19) Show that a ring R with identity is an integral domain if and only if the zero ideal $\{0\}$ is a prime ideal of R.

Now we will prove the relationship between integral domains and prime ideals.

Theorem **10 :** An ideal P of a ring R with identity is a prime ideal of R if and only if the quotient ring R/P is an integral domain.

Proof : Let us first assume that P is a prime ideal of R. Since R has identity, so has R/P. Now, let a+P and b+P be in R/P such that (ai-P) (b+P) = P, the zero element of R/P. Then ab+P = P, i.e., ab ∈ P. As P is a prime ideal of R either a ∈ P or b ∈ P. So either a+P = P or b+P = P.

Thus, R/P has no zero divisors.

Hence, R/P is an integral domain.

Conversely, assume that R/P is an integral domain. Let a,b ∈ R such that ab ∈ P. Then ab + P = P in R/P, i.e., (a+P) (b+P) = P in R/P. As R/P is an integral domain, either a+P = P or b+P = P, i.e., either a ∈ P or b ∈ P. This shows that P is a prime ideal of R.

Using Theorem 10 and Theorem 1 we can say that an ideal $m\mathbb{Z}$ of Z is prime iff m is a prime number. Can we generalise this relationship between prime numbers and prime ideals in $\mathbb{Z}$ to any integral domain? To answer this let us first try and suitably generalise the concepts of divisibility and prime elements.

Definition : In a ring R, we say that an element a **divides** an element b (and denote it by a | b) if b = ra for some r ∈ R. In this case we also say that a is a **factor** of b, or a is a divisor **of** b.

Thus, $\bar{3}$ divides $\bar{6}$ in $\mathbb{Z}_7$, since $\bar{3}.\bar{2} = \bar{6}$.

Now let us see what a prime element is.

Definition : **A** non-zero element p of an integral domain R is called a **prime clement** if

i) p does not have a multiplicative inverse, and

ii) whenever a, b ∈ R and p | ab, then p | a or p | b.

Can you say what the prime elements of $\mathbb{Z}$ are? They are precisely the prime numbers and their negatives.

Now that we know what a prime element is, let us see if we can relate prime ideals and prime elements in an integral domain.

Theorem **11 :** Let R be an integral domain. A non-zero element p ∈ R is a prime clement if and only if Rp is **a** prime ideal of R.

Proof : Let us first assume that p is a prime element in R. Since p does not have a multiplicative inverse, 1 ∉ Rp. Thus, Rp is a proper ideal of R. Now let a, b ∈ R such that ab ∈ Rp. Then ab = rp for some r ∈ R

⇒ p | ab

x ∈ R has a multiplicative inverse iff Rx = R.

⇒ p | a or p | b, since p is a prime element.

⇒ a = xp or b = xp for some x ∈ R.

⇒ a ∈ Rp or b ∈ Rp.

Thus ab ∈ Rp ⇒ either a ∈ Rp or b ∈ Rp, i.e., Rp is a prime ideal of R.

Conversely, assume that Rp is a prime ideal. Then Rp ≠ R. Thus, 1 ∉ Rp, and hence, p does not have a multiplicative inverse. Now suppose p divides ab, where a, b ∈ R. Then ab = rp for some r ∈ R, i.e., ab ∈ Rp.

As Rp is a prime ideal, either a ∈ Rp or b ∈ Rp. Hence, either p | a or p | b. Thus, p is a prime element in R.

Theorem 11 is very useful for checking whether an element is a prime element or not, or for finding out when a principal ideal is a prime ideal. For example, now we can use E 19 to say that 0 is a prime element of R iff R is a domain.

Prime ideals have several useful properties. In the following exercises we ask you to prove some of them.

E 20) Let $f : R \to S$ be a ring epimorphism with kemel N. Show that

a) if J is a prime ideal in S, then $f^{-1}(J)$ is a prime ideal in R.

b) if I is a prime ideal in R containing N, then f(I) is a prime ideal in S.

c) the map ø between the set of prime ideals of R that contain N and the set of all prime ideals of S given by $\phi(I) = f(I)$ is a bijection.

E 21) If I, and I_2 are ideals of a ring such that neither I_1 nor I_2 contains the other, then show that the ideal $I_1 \cap I$, is not prime.

Now consider the ideal 2 2 in Z. Suppose the ideal nZ in Z is such that $2\mathbf{Z} \subseteq n\mathbf{Z} \subseteq \mathbf{Z}$. Then $n \mid 2$. $\therefore n = \pm 1$ or $n = \pm 2$. $\therefore n\mathbf{Z} = \mathbf{Z}$ or $n\mathbf{Z} = 2\mathbf{Z}$.

This shows that no ideal can lie between 2Z and Z. That is, 2 2 is maximal among the proper ideals of Z that contain it. So we say that it is a "maximal ideal". Let us define this expression.

Definition : A proper ideal M of a ring R is called a **maximal ideal** if whenever I is an ideal of R such that $M \subseteq I \subseteq R$, then either I = M or I = R.

Thus, a proper ideal M is a maximal ideal if there is no proper ideal of R which contains it. An example that comes to mind immediately is the zero ideal in any field F. This is maximal because you know that the only other ideal of F is F itself.

To generate more examples of maximal ideals, we can use the following characterisation of such ideals.

Theorem 12: Let **R** be a ring with identity. An ideal M in R is maximal if and only if R/M is a field.

Proof: Let us first assume that M is a maximal ideal of R. We want to prove that R/M is a field. For this, it is enough to prove that R/M has no non-zero proper ideals (see Theorem 9). So, let I be an ideal of R/M. Consider the canonical homomorphism $\eta : R \to R/M : \eta(r) = r + M$. Then, from Theorem 3 of Unit 11, you know that $\eta^{-1}(I)$ is an ideal of R containing M, the kernel of η. Since M is a maximal ideal of R, $\eta^{-1}(I) = M$ or $\eta^{-1}(I) = R$. Therefore, $I = \eta(\eta^{-1}(I))$ is either $\eta(M)$ or $\eta(R)$. That is, $I = \{\bar{0}\}$ or I = R/M, where; = O+M = M. Thus, R/M is a field.

Conversely, let M be an ideal of R such that R/M is a field. Then the only ideals of R/M are $\{\bar{0}\}$ and R/M. Let I be an ideal of R containing M. Then, as above. $\eta(1) = \{\bar{0}\}$ or, $\eta(I) = R/M$.

$\therefore I = \eta^{-1}(\eta(I))$ is M or R. Therefore, M is a maximal ideal of R.

Now look at the following consequence of Theorem 12 (and a few other theorems too).

Corollary : Every maximal ideal of a ring with identity is a prime ideal.

We ask you to prove it in the following exercise.

E 22) Prove the corollary given above.

Now, the corollary is a one-way statement. What about the converse? That is, is every prime ideal maximal? What about the zero ideal in Z? Since Z is a domain but not a field and $Z \simeq \mathbf{Z}/\{0\}, \mathbf{Z}/\{0\}$ is a domain but not a field. Thus. (0) is a prime ideal but not a maximal ideal of Z.

Now let us use Theorem 12 to get some examples of maximal ideals.

Example 3: Show that an ideal mZ of Z is maximal iff m is a prime number.

Solution : From Theorem 7 you know that Z_m is a field iff m is a prime number. You

also know that $\mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}_m$. Thus, by E 17, $\mathbf{Z}/m\mathbf{Z}$ is a field iff m is prime. Hence. by Theorem 12, $m\mathbf{Z}$ is maximal in Z iff m is a prime number.

Example 4: Show that $\bar{2}\mathbf{Z}_{12}$ is a maximal ideal of $\mathbf{Z}_{12}$, whereas $(\bar{0},\bar{4},\bar{8})$ is not.

Solution : You .know that $\mathbf{Z}_{12} \simeq \mathbf{Z}/12\mathbf{Z}$ and $\bar{2}\mathbf{Z}_{12} \simeq 2\mathbf{Z}/12\mathbf{Z}$. Thus, by E 23 of Unit 11, *we* see that $\mathbf{Z}_{12}/\bar{2}\mathbf{Z}_{12} \simeq (\mathbf{Z}/12\mathbf{Z})/(2\mathbf{Z}/12\mathbf{Z}) \simeq 2/22 \simeq \mathbf{Z}_2$, which is. a field. Therefore, $\bar{2}\mathbf{Z}_{12} = \{\bar{0}, \bar{2},\bar{4},\bar{6},\bar{8},\bar{10}\}$ is maximal in Z_{12}.

Now. $\{\bar{0},\bar{4},\bar{8}\} = \bar{4}\mathbf{Z}_{12} \subsetneq \bar{2}\mathbf{Z}_{12} \subsetneq \mathbf{Z}_{12}$.

Therefore, $(\bar{0},\bar{4},\bar{8})$ is not maximal in $\mathbf{Z}_{12}$.

Try the following exercises now.

E **23)** Show that $\{\bar{0}, \bar{2},\bar{4},\bar{6},\bar{8}\}$ is maximal in $\mathbf{Z}_{10}$.

E 24) Use Example 4 of Unit 11 to prove that the ideal $\{f \in C[0,1] \mid f(\frac{1}{2}) = 0\}$ is maximal in $C[0,1]$.

So, let us ***see*** what we have done in this section. We first introduced you to a special ideal of a ring, called a prime ideal. Its speciality lies in the fact that the quolient ring corresponding to it is an integral domain.

Then we discussed a special kind of prime ideal, i.e., a maximal ideal. Why do we consider such an ideal doubly special? Because, the quotient ring cotresponding to it is a Field, and a field is a very handy algebraic structure to deal with.

Now, if we restrict our attention to domains, can you think of any other method of obtaining a field from a domain? In the next section we look at such a method.

12.5 FIELD OF QUOTIENTS

Consider Z and **Q.** You know that every element of Q is of the form $\frac{a}{b}$, where $a \in \mathbf{Z}$ and $b \in Z^*$. Actually, we can also denote $\frac{a}{b}$ by the ordered pair $(a,b) \in Z \times \mathbf{Z}^*$. Now, in **Q** we know that $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. Let us put a similar relation on the elements of $\mathbf{Z} \times \mathbf{Z}^*$.

Now, we also know that the operations on **Q** are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \; \forall \; \frac{a}{b}, \frac{c}{d} \in \mathbf{Q}.$$

Keeping these in mind we can define operations on $\mathbf{Z} \times \mathbf{Z}^*$. Then we can suitably define an equivalence relation on $Z \times \mathbf{Z}^*$ to get a field isomorphic to **Q.**

We can generalise this procedure to obtain a field from any integral domain. So, take an integral domain R. Let K be the following set of ordered pairs:

$$K = \{(a,b) \mid a,b \in R \text{ and } b \neq 0\}$$

We define a relation $\sim$ in K by

$(a,b) \sim (c,d)$ if $ad = bc$.

We claim that $\sim$ is an equivalence relation. Let us see if this is so.

i) $(a,b) \sim (a,b) \; \forall \; (a,b) \in K$, since R is commutative. Thus, $\sim$ is reflexive.

ii) Let $(a,b), (c,d) \in K$ such that $(a,b) \sim (c,d)$. Then $ad = bc$, i.e., $cb = da$. Therefore, $(c,d) \sim (a,b)$. Thus, $\sim$ is symmetric.

iii) Finally, let $(a,b), (c,d), (u,v) \in K$ such that $(a,b) \sim (c,d)$ and $(c,d) \sim (u,v)$. Then $ad = bc$ and $cv = du$. Therefore, $(ad)v = (bc)v = bdu$, i.e., $avd = bud$. Thus, by the cancellation law for multiplication (which is valid for a domain), we get $av = bu$, i.e., $(a,b) \sim (u,v)$. Thus, $\sim$ is transitive.

Hence, $\sim$ is an equivalence relation.

Let us denote the equivalence class that contains (a,b) by $[a,b]$. Thus,
$[a,b] = \{(c,d) \mid c,d \in R, d \neq 0 \text{ and } ad = bc\}$.

Let F be the set of all equivalence classes of K with respect to $\sim$.

Let us define $+$ and $.$ in F as follows. (It might help you to keep in mind the rules for adding and multiplying rational numbers.)

$[a,b] + [c,d] = [ad+bc,bd]$ and

$[a,b] . [c,d] = [ac,bd]$.

Do you think $+$ and $.$ are binary operations on F?

Note that $b \neq 0$ and $d \neq 0$ in the integral domain R imply $bd \neq 0$. So, the right-hand.sides of the equations given above are well defined equivalence classes. Thus, the sum and product of two elements in F is again an element in F.

We must make sure that these operations are well defined.

So, let $[a,b] = [a',b']$ and $[c,d] = [c',d']$. We have to show that $[a,b] + [c,d] = [a',b'] + [c',d']$, i.e., $[ad+bc,bd] = [a'd'+b'c',b'd']$.

Now, $(ad+bc)\,b'd' - (a'd' + b'c')\,bd$

$= ab'dd' + cd'bb' - a'bdd' - c'dbb'$

$= (ab' - a'b)dd' + (cd' - c'd)\,bb'$

$= (0)\,dd' + (0)bb'$, since $(a,b) \sim (a', b')$ and $(c,d) \sim (c',d')$.

$= 0$.

Hence, $[ad+bc,bd] = [a'd' + b'c',b'd']$, i.e., $+$ is well defined.

Now, let us show that $[a,b] . [c,d] = [a',b'] . [c',d']$,

i.e., $[ac,bd] = [a'c',b'd']$.

Consider $(ac)\,(b'd') - (bd)\,(a'c')$

$= ab'cd' - ba'dc' = ba'cd' - ba'cd'$, since $ab' = ba'$ and $cd' = dc'$

$= 0$

Therefore, $[ac,bd] = [a'c',b'd']$. Hence, $.$ is well defined.

We will now prove that F is a field.

i) $+$ is associative : For $[a,b], [c,d], [u,v] \in F$,

$([a,b] + [c,d]) + [u,v] = [ad+bc,bd] + [u,v]$

$= [(ad+bc)v + ubd, Wv]$

$= [adv + b(cv+ud), bdv]$

$= [a,b] + [cv+ud,dv]$

$= [a,b] + ([c,d] + [u,v])$

ii) $+$ is commutative : For $[a,b], [c,d] \in F$,

$[a,b] + [c,d] = [ad+bc,bd] = [cb+da,db] = [c,d] + [a,b]$

iii) $[0,1]$ is the additive identity for F : For $[a,b] \in F$,

$[0,1] + [a,b] = [0.b+1.a, 1.b] = [a,b]$

iv) The additive inverse of $[a,b] \in F$ is $[-a,b]$:

$[a,b] + [-a,b] = [ab-ab,b^2] = [0,b^2] = [0,1]$, since $0.1 = 0.b^2$.

We would like you to prove the rest of the requirements for F to be a field (see the following exercise).

E 25) Show that. in F is associative, commutative, distributive over +, and $[1,1]$ is the multiplicative identity for F.

So we have put our heads together and proved that F is a field.

Now, let us define $f : R \to F : f(a) = [a,1]$. We want to show that f is a monomorphism.

Firstly, for $a, b \in R$,

$f(a+b) = [a+b,1] = [a,]] + [b,1]$.

$= f(a) + f(b)$, and

$f(ab) = [ab,1] = [a,1].[b,1] = f(a) . f(b)$.

Thus, f is a ring homomorphism.

Next, let $a,b \in R$ such that $f(a) = f(b)$. Then $[a,1] = [b,1]$, i.e., $a = b$. Therefore, f is 1-1.

Thus, f is a monomorphism.

So, Im f = f(R) is a subring of F which is isomorphic to R.

As you know, isomorphic structures are algebraically identical.

So, we can identify R with f(R), and think of R as a subring of F. Now, any element of F is of the form

$[a,b] = [a,1]\,[1,b] = [a,1]\,[b,1]^{-1} = f(a)\,f(b)^{-1}$, where $b \neq 0$. Thus, identifying $x \in R$ with $f(x) \in f(R)$, we can say that any element of F is of the form ab^{-1}, where $a,b \in R$, $b \neq 0$.

All that we have discussed in this section adds up to the proof of the following theorem.

A ring R is embedded in a ring S if there is a ring monomorphism from R to S.

Theorem 13 : Let R be an integral domain. Then R can be embedded in a field F such that every element of F has the form ab^{-1} for $a, b \in R$, $b \neq 0$.

The field F whose existence we have just proved is called the **field of quotients (or the field of fractions) of R.**

Thus, Q is the field of quotients of Z. What is the field of quotients of R? The following theorem answers this question.

Theorem 14 : Iff : $R \to K$ is a monomorphism of an integral domain R into a field K, then there exists a monomorphism

$g : F \to K : g([a,1]) = f(a)$, where F is the field of quotients of R.

We will not prove this result here, since it is a little technical. But let us look at this theorem closely. It says that **the field of quotients of an integral domain is** the smallest **field** containing it. Thus, the field of quotients of any field is the field itself. So, the field of quotients of R is R and of Z_p is Z_p, where p is a prime number.

Try these exercises now.

E 26) Is R the field of quotients of $Z + \sqrt{2}Z$? Or, is it C? Or, is it $Q + \sqrt{2}Q$? Why?

E 27) At what stage of the construction of the field F in Theorem 13 was it crucial to assume that R is a domain?

Let us now wind up this unit with a summary of what we have done in it.

12.6 SUMMARY

In this unit we have covered the following points.

1. The definition and examples of an integral domain.
2. The definition and examples of a field.
3. Every field is a domain.
4. A finite domain is a field.
5. The characteristic of any domain or field is either zero or a prime number.
6. The definition and examples of prime and maximal ideals.
7. The proof and use of the fact that a proper ideal I of a ring R with identity is prime (or maximal) iff R/I is an integral domain (or a field).
8. Every maximal ideal is a prime ideal.
9. An element p of an integral domain R is prime iff the principal ideal pR is a prime ideal of R.
10. Z_n is a field iff n is a prime number.
11. The construction of the field of quotients of an integral domain.

12.7 SOLUTIONS/ANSWERS

E 1) Let $n = mr$, where $r \in N$.

Then $\bar{m}\,\bar{r} = \bar{n} = \bar{0}$ in Z_n.

Since $1 < m < n$, $\bar{m} \neq \bar{0}$. Similarly, $\bar{r} \neq \bar{0}$.

Thus $\bar{m} \in Z_n$ is a zero divisor.

E 2) Z has no zero divisors.

E 3) For none, since $1.x = x \neq 0\ \forall\ x \neq 0$ in the ring.

E 4) Let $b \neq 0$ be in R such that $ab = 0$. Then, for any $r \in R$, $(ra)b = r(ab) = 0$ Thus, every element of Ra is a zero divisor.

E 5) Z_4, since 2 is a zero divisor.

$2Z$, since $1 \notin 2Z$.

$R \times R$, since (1,0) is a zero divisor.

{0}, since a domain must be non-zero.

E6) $x^2 = x \Rightarrow x(x-1) = 0 \Rightarrow x = 0$ or $x-1 = 0$

$\Rightarrow x = 0$ or $x = 1$.

E 7) Let R be a domain and $x \in R$ be nilpotent.

Then $x^n = 0$ for some $n \in N$. Since R has no zero divisors, this implies that $x = 0$.

E 8) We want to show that $2A = \emptyset\ \forall\ A \subseteq X$, and that 2 is the least such natural number.

Firstly, for any $A \subseteq X$,

$2A = A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset$

Also, since $X \neq \emptyset$, $1.X \neq \emptyset$. Thus, char $\wp(X) \neq 1$.

$\therefore$ char $\wp(X) = 2$.

E 9) Let char $(R \times R) = n$. We know that $nr = 0\ \forall\ r \in R$.

Now, let (r,s) be any element of $R \times R$.

Then $m(r,s) = (mr,ms) = (0,0)$, since $r,s \in R$.

Thus, $n \leq m$. .....(1)

On the other hand, if $r \in R$, then $(r,0) \in R \times R$

$\therefore n(r,0) = (0,0)$,

i.e., $(nr,0) = (0,0)$

i.e., $nr = 0$.

This is true for any $r \in R$.

$\therefore m \leq n$. .....(2)

Thus, (1) and (2) show that $m = n$, i.e., char R = char $(R \times R)$

E 10) a) By the binomial expansion (E 11 of Unit 9),

$(a+b)^p = a^p + {}^pC_1 a^{p-1} b + \ldots\ldots + {}^pC_{p-1} ab^{p-1} + b^p$

Since $p \mid {}^pC_n \; \forall \; n = 1, \ldots, p-1$, ${}^pC_n x = 0 \; \forall \; x \in R$ and $\forall \; n = 1, \ldots p-1$.

Thus, ${}^pC_1 a^{p-1} b = 0 = \ldots\ldots = {}^pC_{p-1} ab^{p-1}$

$\therefore (a+b)^p = a^p + b^p$.

You can similarly show that $(a-b)^p = a^p - b^p$.

b) Let $S = \{a^p \mid a \in R\}$

Firstly, $S \neq \emptyset$.

Secondly, let $\alpha, \beta \in S$. Then $\alpha = a^p$, $\beta = b^p$ for some $a,b \in R$.

Then $\alpha - \beta = (a-b)^p \in S$ and $\alpha\beta = (ab)^p \in S$.

Thus, S is a subriny of R.

c) $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$,

$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\,\phi(b)$.

Thus, ϕ is a ring homomorphism.

ϕ is 1–1 because

$\phi(a) = \phi(b) \Rightarrow a^p = b^p \Rightarrow (a-b)^p = 0$, from (a).

$\Rightarrow a-b = 0$, since R is without zero divisors.

$\Rightarrow a = b$.

d) We have to show that if R is finite then ϕ is surjective.

Let R have n elements. Since ϕ is 1–1, Im ϕ also has n elements.

Also Im $\phi \subseteq R$. Thus, Im $\phi = R$.

Hende, ϕ is surjective.

E 11) You can easily,show that f is a ring homomorphism.

Ker $f = \{n \in Z \mid n.1 = 0\}$

$= mZ$, since char R = m.

E 12) char $(Z_3 \times Z_4)$ = l.c.m. of char Z_3 and char Z_4 = 12.

Thus, the characteristic of $Z_3 \times Z_4$ is neither 0 nor a prime.

Note that $Z_3 \times Z_4$ is not a domain, since it has several zero divisors.

Now let us see why Theorem 3 is not valid for $Z_3 \times Z_4$.

Take $(\bar{1},\bar{0}) \in Z_3 \times Z_4$. Then $3(\bar{1},\bar{0}) = (\bar{0},\bar{0}) \in Z_3 \times Z_4$.

But 3 $(\bar{1},\bar{1}) \neq (\bar{0},\bar{0})$. Thus, Theorem 3(a) and Theorem 3(c) are not equivalent in this case.

E 13) $2\mathbf{Z}$ since $2 \in 2\mathbf{Z}$ is not invertible in $2\mathbf{Z}$.

$\mathbf{Z}_6$, since it is not a domain.

$\mathbf{Q} \times \mathbf{Q}$, since it is not a domain.

E 14) No. For example, Z is a subring of $\mathbf{Q}$, $\mathbf{Q}$ is a field, but Z is not.

E 15) From the tables you can see that R is commutative with identity and every non-zero element has an inverse. Thus, R is a field.

Also $2x = 0 \ \forall \ x \in \mathbf{R}$ and $1.x \neq 0$ for some $x \in R$.

Thus, char R = 2.

E 16) Ker f is an ideal of F. Thus. by Theorem 9,

Kerf = {0} or Kerf = F.

If Ker f = {0}, then f is 1–1.

If Ker f = F, then f = 0.

E 17) Let $\phi : F \to R$ be an isomorphism. Then $\phi(1)$ is the identity of Im ϕ = R. Also, since F is commutative, so is R. Now, let $r \in R$, $r \neq 0$. Since ϕ is onto, $\exists\ a \in F$ such that @(a)= r. Since $r \neq 0$, $a \neq 0$. Since F is a field, $\exists\ b \in F$ such that ab = 1.

Then $\phi(ab) = \phi(1)$, i.e., $r\phi(b) = \phi(1)$, i.e., r has a multiplicative inverse.

Thus, R is a field.

E 18) Firstly, I is an ideal of C[0,1]

(because $f,g \in I \Rightarrow f-g \in I$, and

$T \in C[0,1]$, $f \in I^*$ $Tf \in I$.)

Secondly, since any non–zero constant function is in

C [0, 1]\I, I is a proper ideal.

Finally, let $fg \in I$. Then $f(0)\,g(0) = 0$ in R. Since R is a domain, we must have $f(0) = 0$ or $g(0) = 0$, i.e., $f \in I$ or $g \in I$.

Thus, I is a prime ideal of C[0,1].

E 19) R is a ring with identity. Thus, we need to show that R is without zero divisors iff {0} is a prime ideal in R.

Now, {0} is a prime ideal in R

iff $ab \in \{0\} \Rightarrow a \in \{0\}$ or $b \in \{0\}$ for $a, b \in R$

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

iff R is without zero divisors.

So, we have shown what we wanted to show.

E 20) a) From Theorem 3 of Unit 11, you know that $f^{-1}(J)$ is an ideal of R. Since f is surjective and $J \neq S$, $f^{-1}(J) \neq R$.

Now, let $a,b \in R$ such that $ab \in f^{-1}(J)$.

$\Rightarrow$ $f(ab) \in J$.

$\Rightarrow$ $f(a)\,f(b) \in J$

$\Rightarrow$ $f(a) \in J$ or $f(b) \in J$, since J is a prime ideal.

$\Rightarrow$ a s $f^{-1}(J)$ or $b \in f^{-1}(J)$.

Thus, $f^{-1}(J)$ is a prime ideal in R.

b) Firstly, since f is onto, you know that $f(I)$ is an ideal of S. Also, since $1 \notin I$ and $f^{-1}(f(I)) = I$ (from Theorem 4 of Unit 11), $f(1) \notin f(I)$. Thus, $f(I) \neq S$.

Finally, let $x,y \in S$ such that $xy \in f(I)$.

Since $S = \text{Im } f$, $\exists$ a,b $\in$ R such that $x = f(a)$ and $y = f(b)$.

Then $f(ab) = xy \in f(I)$, i.e., $ab \in f^{-1}(f(I)) = I$.

$\therefore$ $a \in I$ or $b \in I$, i.e., $x \in f(I)$ or $y \in f(I)$.

Thus, $f(I)$ is a prime ideal of S.

c) ϕ is $1-1$: $\phi(I) = \phi(J) \Rightarrow f(I) = f(J)$

$\Rightarrow f^{-1}(f(I)) = f^{-1}(f(J)) \Rightarrow I = J$.

ϕ is onto : Let J be a prime ideal of S. Then $f^{-1}(J)$ is a prime ideal of R and $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$ (from Unit 11j. .Thus, $J \in \text{Im } \phi$.

E 21) Let $x \in I_1 \setminus I_2$ and $y \in I_2 \setminus I_1$. Then $xy \in I_1$ and $xy \in I_2$, since I_1 and I_2 are ideals.

$\therefore xy \in I_1 \cap I_2$. But $x \notin I_1 \cap I_2$ and $y \notin I_1 \cap I_2$.

Thus, $I_1 \cap I_2$ is not prime.

E 22) M is maximal in R

$\Rightarrow$ R/M is a field, by Theorem 12

$\Rightarrow$ R/M is a domain, by Theorem 5

$\Rightarrow$ M is prime in R, by Theorem 10

E 23) $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\} = \bar{2}\mathbf{Z}_{10}$ and $\mathbf{Z}_{10} / \bar{2}\mathbf{Z}_{10} \simeq \mathbf{Z}_2$, a field.

Thus, as in Example 4, $\{0,2,4,6,8\}$ is maximal in $\mathbf{Z}_{10}$.

E 24) In Unit 11 we have shown that this ideal in the kernel of the onto homomorphism $\phi : C[0,1] \to \mathbf{R} : \phi(f) = f(\frac{1}{2})$.

$\therefore$ $C[0,1]/\text{Ker } \phi \simeq$ R, a field.

Thus, Ker ϕ is maximal in $C[0,1]$.

E 25) You can prove all these properties by using the corresponding properties of R.

E 26) Any element of the field of quotients F is of the form $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, where $c+d\sqrt{2} \neq 0$, a,b,c,d $\in$ Z.

Now, $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \left(\frac{ac-2bd}{c^2-2d^2}\right) + \sqrt{2}\left(\frac{bc-ad}{c^2-2d^2}\right) \in \mathbf{Q} + \sqrt{2}\mathbf{Q}$

Thus, $F \subseteq Q + \sqrt{2}\mathbf{Q}$.

Also, any element of $Q + \sqrt{2}Q$ is $\frac{a}{b} + \sqrt{2}\frac{c}{d}$, a,b,c,d $\in$ Z, $b \neq 0$, $d \neq 0$.

Now, $\frac{a}{b} + \sqrt{2}\frac{c}{d} = \frac{ad+bc\sqrt{2}}{bd} = \frac{ad+bc\sqrt{2}}{bd+0\sqrt{2}}$ with ad, bc, bd $\in$ Z.

Thus, $\frac{a}{b} + \sqrt{2}\frac{c}{d} \in F$.

Hence, $Q + \sqrt{2}\mathbf{Q} \subseteq F$.

Thus, $F = Q + \sqrt{2}\mathbf{Q}$.

E 27) If R is not a domain, the relation ~ need not be transitive, and hence, F is not defined.