UNIT 15 IRREDUCIBILITY AND FIELD EXTENSIONS

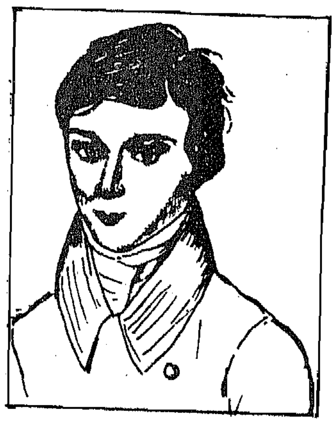
Structure

15.1 INTRODUCTION

In the previous unit we discussed various kinds of integral domains, including unique factorisation domains. Over there you saw that Z[x] and Q[x] are UFDs. Thus, the prime and irreducible elements coincide in these rings. In this unit we will give you a method for obtaining the prime (or irreducible) elements of Z[x] and Q[x]. This is the Eisenstein criterion, which can also be used for obtaining the irreducible elements of any polynomial ring over a UFD.

After'this we will introduce you to field extensions and subfields. We will use irreducible polynomials for obtaining field extensions of a field F from F[x]. We will also show you that every field is a field extension of Q or Z_p for some prime p. Because of this we call Q and the Z_ps prime fields. We will discuss these fields briefly.

Finally, we will look at finite fields. These fields were introduced by the young French mathematician Evariste Galois (Fig. 1) while he was exploring number theory. We will discuss some properties of finite fields which will show us how to classify them.



Pig. 1: Evariste Galois (1811-1832)

Before reading this unil wc suggest that you go through the definitions of irreducibility from Unit 14. We also suggest that you go through Units 3 and 4 of the Linear Algebra course if you want to understand the proof of Theorem 7 of this unit. We have kept the proof optional. But once you know what a vector space and its basis are, then the proof is very simple.

Objectives

After reading this unit, you should be able to

- prove and use Eisenstein's criterion for irreducibility in Z[x] and Q[x];
- obtain field extensions of a field F from F[x];
- obtain the prime field of any field;
- use the fact that any finite field F has p^n elements, where char F = p and $\dim_{Z_p} F = n$.

15.2 IRREDUCIBILITY IN Q[X]

In Unit 14 we introduced you to irreducible polynomials in F[x], where F is a field. We also stated the Fundamental Theorem of Algebra, which said that a polynomial over C is irreducible iff it is linear. You also learnt that if a polynomial over R is irreducible, it must have degree 1 or degree 2. Thus, any polynomial over R of degree more than 2 is reducible. And, using the quadratic formula, we know which quadratic polynomials over R are irreducible.

Now let us look at polynomials over Q. Again, as for any field F, a linear polynomial over Q is irreducible. Also, by using the quadratic formula we can explicitly obtain the roots of any quadratic polynomial over Q, and hence figure out whether it is irreducible or not. But, can you tell whether $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ is irreducible over **Q** or not? In two seconds we can tell you that it is irreducible, by using the Eisenstein criterion. This criterion was discovered by the nineteenth century mathematician Ferdinand Eisenstein. In this section we will build up the theory for proving this useful criterion.

Let us start with a definition.

Definition: Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x]$. We define the **content** of f[x] to be the g.c.d of the integers $a_0, a_1, \ldots, a_n$.

We say that f(x) is **primitive** if the content of f(x) is 1.

For example, the content of $3x^2 + 6x + 12$ is the g.c.d. of 3,6 and 12, i.e., 3. Thus, this polynomial is not primitive. But $x^5 + 3x^2 + 4x - 5$ is primitive, since the g.c.d of 1,0,0,3,4,–5 is 1.

You may like to try the following exercises now.

E 1) What are the contents of the following polynomials over **Z**?

a) $1 + x + x^2 + x^3 + x^4$

b) $7x^4 - 7$

c) $5(2x^2 - 1)(x + 2)$.

E 2) Prove that any polynomial $f(x) \in \mathbf{Z}[x]$ can be written as dg(x), where d is the content of f(x) and g(x) is a primitive polynomial.

We will now prove that the product of primitive polynomials is a primitive polynomial. This result is well known as Gauss' **lemma.**

Theorem 1: Let f(x) and g(x) be primitive polynomials. Then so is f(x) g(x).

Proof: Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x]$ and

$g(x) = b_0 + b_1x + \ldots + b_mx^m \in \mathbf{Z}[x]$, where the

g.c.d of $a_0, a_1, \ldots, a_n$ is 1 and the g.c.d of $b_0, b_1, \ldots, b_m$ is 1. Now

$f(x)\,g(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}$,

where $c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0$.

To prove the result we shall assume that it is false, and then reach a contradiction. So, suppose that f(x) g(x) is not primitive. Then the g.c.d of $c_0, c_1, \ldots, c_{m+n}$ is greater than 1, and hence some prime p must divide it. Thus, $p \mid c_i \ \forall\ i = 0, 1, \ldots, m+n$. Since f(x) is primitive, p does not divide some a_i. Let r be the least integer such that $p \nmid a_r$. Similarly, let s be the least integer such that $p \nmid b_s$.

Now consider

$$c_{r+s} = a_0b_{r+s} + a_1b_{r+s-1} + \ldots + a_rb_s + \ldots + a_{r+s}b_0$$

$$= a_rb_s + (a_0b_{r+s} + a_1b_{r+s-1} + \ldots + a_{r-1}b_{s+1} + a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0)$$

By our choice of r and s, $p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}$, and $p \mid b_0, p \mid b_1, \ldots, p \mid b_{s-1}$. Also $p \mid c_{r+s}$.

Therefore, $p \mid c_{r+s} - (a_0b_{r+s} + \ldots + a_{r-1}b_{s+1} + a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0)$

i.e., $p \mid a_rb_s$.

$\Rightarrow p \mid a_r$ or $p \mid b_s$, since p is a prime.

But $p \nmid a_r$ and $p \nmid b_s$. So we reach a contradiction. Therefore, our supposition is false. That is, our theorem is true.

Let us shift our attention to polynomials over **Q** now.

Consider any polynomial over Q, say $f(x) = \frac{3}{2}x^3 + \frac{1}{5}x^2 + 3x + \frac{1}{3}$. If we take the l.c.m of

.ll the denominators, i.e., of 2,5,1 and 3, i.e., 30 and multiply f(x) by it, what do we get? We get

$30f(x) = 45x^3 + 6x^2 + 90x + 10 \in \mathbb{Z}[x]$

Using the same process. we can multiply any $f(x) \in \mathbb{Q}[x]$ by a suitable integer d so that $df(x) \in \mathbb{Z}[x]$. We will use this fact while relating irreducibility in $\mathbb{Q}[x]$ with irreducibility in $\mathbb{Z}[x]$.

Theorem 2: If $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

Proof: Let us suppose that f(x) is not irreducible over $\mathbb{Q}[x]$. Then we should reach a contradiction. So let $f(x) = g(x)\,h(x)$ in $\mathbb{Q}[x]$, where neither g(x) nor h(x) is a unit, i.e., $\deg g(x) > 0$, $\deg h(x) > 0$. Since $g(x) \in \mathbb{Q}[x]$, $3\ m \in \mathbb{Z}$ such that $mg(x) \in \mathbb{Z}[x]$. Similarly, $3\ n \in \mathbb{Z}$ such that $nh(x) \in \mathbb{Z}[x]$. Then,

$$mnf(x) = mg(x)\,nh(x) \qquad \dots (1)$$

Now, let us use E2. By E2, $f(x) = rf_1(x)$, $mg(x) = sg_1(x)$, $nh(x) = th_1(x)$, where r, s and t are the contents of f(x), mg (x) and nh (x) and $f_1(x)$, $g_1(x)$, $h_1(x)$ are primitive polynomials of positive degree.

Thus, (1) gives us

$$mnrf_1(x) = stg_1(x)\,h_1(x) \qquad \dots (2)$$

Since $g_1(x)$ and $h_1(x)$ are primitive, Theorem 1 says that $g_1(x)\,h_1(x)$ is primitive. Thus, the content of the right hand side polynomial in (2) is st. But the content of the left hand side polynomial in (2) is mnr. Thus, (2) says that mnr = st.

Hence, using the cancellation law in (2), we get $f_1(x) = g_1(x)\,h_1(x)$.

Therefore, $f(x) = rf_1(x) = (rg_1(x))\,h_1(x)$ in $\mathbb{Z}[x]$, where neither $rg_1(x)$ nor $h_1(x)$ is a unit. This contradicts the fact that f(x) is irreducible in $\mathbb{Z}[x]$.

Thus, our supposition is false. Hence, f(x) must be irreducible in $\mathbb{Q}[x]$.

What this result says is that to check irreducibility of a polynomial in $\mathbb{Q}[x]$, it is enough to check it in $\mathbb{Z}[x]$. And, for checking it in $\mathbb{Z}[x]$ we have the terrific Eisenstein's criterion, that we mentioned at the beginning of this section.

Theorem 3 (Eisenstein's Criterion) : Let $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$. Suppose that for some prime number p,

i) $p \nmid a_n$,

ii) $p \mid a_0, p \mid a_1, ..., p \mid a_{n-1}$, and

iii) $p^2 \nmid a_0$.

Then f(x) is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$).

Proof: Can you guess our method of proof? By contradiction, once again! So suppose f(x) is reducible in $\mathbb{Z}[x]$.

Let $f(x) = g(x)\,h(x)$,

where $g(x) = b_0 + b_1x + ... + b_mx^m$, $m > 0$ and

$h(x) = c_0 + c_1x + ... + c_rx^r$, $r > 0$.

Then $n = \deg f = \deg g + \deg h = m + r$, and

$a_k = b_0c_k + b_1c_{k-1} + ... + b_kc_0 \ \forall\ k = 0, 1 ..., n.$

Now $a_0 = b_0c_0$. We know that $p \mid a_0$. Thus, $p \mid b_0c_0$ $\therefore$ $p \mid b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Let us suppose that $p \mid b_0$ and $p \nmid c_0$.

Now let us look at $a_n = b_mc_r$. Since $p \nmid a_n$, we see that $p \nmid b_m$ and $p \nmid c_r$. Thus, we see that for some i, $p \nmid b_i$. Let k be the least integer such that $p \nmid b_k$. Note that $0 < k \le m < n$.

Therefore, $p \mid a_k$.

Now, $a_k = (b_0 c_k + .. + b_{k-1} c_1) + b_k c_0$.

Since $p \mid a_k$ and $p \mid b_0$, $p \mid b_1, ..., p \mid b_{k-1}$, we see that $p \mid a_k - (b_0c_k + ... + b_{k-1}c_1)$, i. e., $p \mid b_kc_0$. But $p \nmid b_k$ and $p \nmid c_0$. So we reach a contradiction.

Thus, f(x) must be irreducible in **Z**[x].

Let us illustrate the use of this criterion.

Example 1: Is $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ irreducible in **Q**[x]?

Solution: By looking at the coefficients we see that the prime number 3 satisfies the conditions given in Eisenstein's criterion. Therefore, the given polynomial is irreducible in **Q**[x].

Example 2: Let p be a prime number. Is $\mathbf{Q}[x]/<x^3 - p>$ a field?

Solution : From Unit 14 you know that for any field F, if f(x) is irreducible in F[x], then <f(x)> is a maximal ideal of F[x].

Now, by Eisenstein's criterion, x^3–p is irreducible since p satisfies the conditions given in Theorem 3. Therefore, $<x^3–p>$ is a maximal ideal of Q[x].

From Unit 12 you also know that if R is a ring, and M is a maximal ideal of R, then R/M is a field.

Thus, $\mathbf{Q}[x] /<x^3–p>$ is a field.

In this example we have brought out an important fact. We ask you to prove it in the following exercise.

E 3) For any'n ∈ N and prime number p, show .that x^n–p is irreducible over **Q**[x]. Note that this shows us that we can obtain irreducible polynomials of any degree over **Q**[x].

Now let us look at another example of an irreducible polynomial. While solving this we will show you how Theorem 3 can be used indirectly.

Example 3: Let p be a prime number. Show that

$f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible in **Z**[x]. f(x) is called the pth cyclotomic polynomial.

Solution : To start with we would like you to note that f(x) = g(x) h(x) in **Z**[x] iff f(x + 1) = g(x + 1) h(x t 1) in **Z**[x]. Thus, f(x) is irreducible in **Z**[x] iff f(x+1) is irreducible in **Z**[x].

$$\text{Now, } f(x) = \frac{x^p - 1}{x - 1}.$$

$$\therefore \quad f(x+1) = \frac{(x+1)^p - 1}{x}$$

$$= \frac{1}{x}(x^p + {}^pC_1\, x^{p-1} + ... + {}^pC_{p-1}\, x + 1-1), \text{ (by the binomial theorem)}$$

$$= x^{p-1} + px^{p-2} + {}^pC_2x^{p-3} + ...+ {}^pC_{p-2}\, x + p.$$

Now apply Eisenstein's criterion taking p as the prime. We find that f(x+1) is irreducible. Therefore, f(x) is irreducible.

You can try these exercises now.

E 4) If $a_0 + a_1x + ... + a,\ x^n \in \mathbf{Z}[x]$ is irreducible in **Q**[x], can you always find a prime p that satisfies the conditions (i), (ii) and (iii) of Theorem 3?

E 5) Which of the following elements of **Z**[x] are irreducible over Q?

a) $x^2 - 12$

b) $8x^3 + 6x^2 - 9x + 24$

c) $5x + 1$

E 6) Let p be a prime integer. Let a be a non-zero non-unit square-free integer, i.e., $b^2 \nmid a$ for any $b \in$ **Z**. Show that **Z**[x]/<x^p+a> is an integral domain.

E 7) Show that $x^p + \bar{a} \in$ $\mathbf{Z}_p[x]$ is not irreducible for any $\bar{a} \in$ Z,.

(**Hint:** Does E 13 of Unit 13 help?)

So far we have used the fact that if $f(x) \in$ **Z**[x] is irreducible over **Z**, then it is also irreducible over Q. Do you think we can have a similar relationship between irreducibility in **Q**[x] and **R**[x]? To answer this, consider $f(x) = x^2 - 2$. This is irreducible in **Q**[x], but $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ in **R**[x]. Thus, we cannot extend irreducibility over **Q** to irreducibility over **R**.

But, we can generalise the fact that irreducibility in **Z**[x] implies irreducibility in **Q**[x]. This is not only true for Z and Q; it is true for any UFD R and its field of quotients F (see Sec. 12.5). Let us state this relationship explicitly.

Theorem **4:** Let R be a UFD with field of quotients F.

i) If $f(x) \in$ R[x] is an irreducible primitive polynomial, then it is also irreducible in F[x].

'ii) (Eisenstein's Criterion) Let $f(x) = a_0 + a_1x + ... +$ a, $x^n \in$ R[x] and $p \in$ R be a prime element such that $p \nmid$ a,, $p^2 \nmid a_0$ and $p \mid a_i$ for $0 \leq i < n$.Then f(x) is irreducible in F[x].

The proof of this result is on the same lines as that of Theorems 2 and 3. We will not be doing it here. But if you are interested, you should try and prove the result yourself.

Now, we have already pointed out that if F is a field and f(x) is irreducible over F, then F[x]/<f(x)> is a field. How is this field related to F? That is part of what we will discuss in the next section.

15.3 FIELD EXTENSIONS

In this section we shall discuss subfields and field extensions. To start with let us define these terms. By now the definition may be quite obvious to you.

Definition: A non-empty subset S of a field F is called a **subfield** of F if it is a field with respect to the operations on F. If S≠F, then S is called a proper **subfield** of **F.**

A field K is called a field extension of F if F is a subfield of K. Thus, *Q* is a subfield of **R** and R is a field extension of **Q.** Similarly, C is a field extension of Q as well as of R.

Note that a non-empty subset S of a field F is a subfield of F iff

i) S is a subgroup of (F,+), and

ii) the set of all non-zero elements of S forms a subgroup of the group of non-zero elements of F under multiplication.

Thus, by Theorem 1 of Unit **3,** we have the following theorem:

Theorem 5: A non-empty subset S of a field F is a subfield of F if and only if

i) $a \in S, b \in S \Rightarrow a-b \in S$, and

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

Why don't you use Theorem 5 to do the following exercise now.

E 8) Show that

a) $Q + iQ$ is a subfield of C.

b) $\mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ is not a subfield of $\mathbf{R}$.

Now, let us look at a particular field extecsion of a field F. Since F[x] is an integral domain, we can obtain its field of quotients (see Unit 12). We denote this field by F(x). Then F is a subfield of F(x). Thus, F(x) is a field extension of F. Its elements are expressions of the form $\frac{f(x)}{g(x)}$, where $f(x), g(x) \in F[x]$ and $g(x) \neq 0$.

There is another way of obtaining a field extension of a field F from F[x]. We can look at quotient rings of F[x] by its maximal ideals. You know that an ideal is maximal in F[x] iff it is generated by an irreducible polynomial over F.
So, F[x]/<f(x)> is a field iff f(x) is irreducible over F.

Now, given any $f(x) \in F[x]$, such that deg $f(x) > 0$, we will show that there is a field monomorphism from F into F[x]/<f(x)>. This will show that F[x)/<f(x)> contains an isomorphic copy of F; and hence, we can say. that it contains F.
So, let us define $\phi : F \to F[x]/<f(x)>: \phi(a) = a + <f(x)>$.

Then $\phi(a+b) = \phi(a) + \phi(b)$, and

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

Thus, ϕ is a ring homomorphism.

What is Ker ϕ ?

Ker ϕ $= \{a \in F \mid a + <f(x)> = <f(x)>\}$

$= \{a \in F \mid a \in <f(x)>\}$

$= \{a \in F \mid f(x) \mid a\}$

$= \{0\}$, since deg $f > 0$ and deg $a \leq 0$.

Thus, ϕ is 1–1, and hence an inclusion.

Hence, F is embedded in F[x]/<f(x)>.

Thus, if f(x) is irreducible in F[x], then F[x]/<f(x)> is a field extension of F.

Now for a related exercise !

E 9) Which of the following rings are field extensions of Q?

a) $\mathbf{Q}[x]/<x^3 + 10>$,

b) $\mathbf{R}[x]/<x^2 + 2>$,

c) Q,

d) $\mathbf{Q}[x]/<x^2 - 5x + 6>$.

Well, we have looked at field extensions of any field F. Now let us look at certain fields, one of which F will be an extension of.

15.3.1 Prime Fields

Let us consider any field F. Can we say anything about what its subfields look like? Yes, we can say something about one of its subfields. Let us prove this very startling and useful fact. Before going into the proof we suggest that you do a quick revision of Theorems 3, 4 and 8 of Unit 12. Well, here's the result.

Theorem 6 : Every field contains a subfield isomorphic to Q or to $\mathbf{Z}_p$, for some prime number p.

Proof : Let F be a field. Define a function

$f: \mathbf{Z} \to F: f(n) = n.1 = 1 + 1 + \ldots + 1$ (n times).

In E 11 of Unit 12 you have shown that f is a ring homomorphism and Ker f = pZ, where p is the characteristic of F.

Now, from Theorem 8 of Unit 12 you know that char F = 0 or char F = p, a prime. So let us look at these two cases separately.

Case 1 (char F = 0) : In this case f is one-one. $\therefore$ $\mathbf{Z} \simeq f(\mathbf{Z})$. Thus, $f(\mathbf{Z})$ is an integral domain contained in the field F. Since F is a field, it will also contain the field of quotients of $f(\mathbf{Z})$. This will be isomorphic to the field of quotients of Z, i.e., Q. Thus, F has a subfield which is isomorphic to Q.

Case 2 (char F = p, for some prime p) :

Since p is a prime number, $\mathbf{Z}/p\mathbf{Z}$ is a field.

Also, by applying the Fundamental Theorem of Homomorphism to f, we get $\mathbf{Z}/p\mathbf{Z} \simeq f(\mathbf{Z})$.

Thus, $f(\mathbf{Z})$ is isomorphic to $\mathbf{Z}_p$ and is contained in F. Hence, F has a subfield isomorphic to $\mathbf{Z}_p$.

Let us reword Theorem 6 slightly. What it says is that :

Let F be a field.

i) If char F = 0, then F has a subfield isomorphic to *Q*.

ii) If char F = p, then F has a subfield isomorphic to Z_p.

Because of this property of **Q** and Zp (where p is a prime number) we call these fields **prime fields.**

Thus, the prime fields are **Q**, $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$, etc.

We call the subfield isomorphic to a prime field (obtained in Theorem 6), the **prime subfield** of the given field.

Let us again reword Theorem 6 in terms of field extensions. What it says is that **every field Is a Weld extension of a prime field.**

Now, suppose a field F is an extension of a field K. Are the prime subfields of K and F isomorphic or not? To answer this let us look at char K and char F. We want to know if char K = char F or not. Since F is a field extension of K, the unity of F and K is the same, namely, 1. Therefore, the least positive integer n such that n.1 = 0 is the same for F as well as K. Thus, char K = char F. Therefore, the prime subfields of K and F are isomorphic.

So, now can you do the following exercises?

E 10) Show that the smallest subfield of any field is its prime subfield.

E 11) Let F be a field which has no proper subfields. Show that F is isomorphic to a prime field.

E 12) Obtain the prime subfields of **R**, Z_5 and the field given in E 15 of Unit 12.

E 13) Show that given any field, if we know its characteristic then we can obtain its prime subfield, and vice versa.

A very important fact, brought out by E 10 and E 11 is that: a **field is a prime field iff it has no proper subfields.**

Now let us look at certain field extensions of the fields $\mathbf{Z}_p$.

15.3.2 Finite Fields

You have dealt a lot with the finite fields $\mathbf{Z}_p$. Now we will look at field extensions of these fields. You know that any finite field F has characteristic p, for some prime p. And then F is an extension of $\mathbf{Z}_p$. Suppose F contains q elements. Then q must be a power of p. That is what we will prove now.

Theorem 7 : Let F be a finite field having q elements and characteristic p. Then $q = p^n$, for some positive integer n.

The proof of this result uses the concepts of a vector space and its basis. These are discussed in Block 1 of the Linear Algebra course. So, if you want to go through the proof, we suggest that you quickly revise Units 3 and 4 of the Linear Algebra course. If you are not interested in the proof, you may skip it.

Proof of Theorem 7 : Since char F = p, F has a prime subfield which is isomorphic to $\mathbf{Z}_p$. We lose nothing if we assume that the prime subfield is $\mathbf{Z}_p$. We first show that F is a vector space over $\mathbf{Z}_p$ with finite dimension.

Recall that a set V is a vector space over a field K if

i) we can define a binary operaiion + on V such that (V, +) is an abelian group,

ii) we can define a 'scalar multiplication'. : $K \times V \to V$ such that $\forall$ a, b $\in$ K and v, w $\in$ V,

$$a.(v + w) = a.v + a.w$$

$$(a + b).\ v = a.v + b.v$$

$$(ab).\ v = a.(b.v)$$

$$1.v = v.$$

Now, we know that (F, +) is an abelian group. We also know that the multiplication in F will satisfy ell the conditions that the scalar multiplication should satisfy. Thus, F is a vector space over $\mathbf{Z}_p$. Since F is a finite field, it has a finite dimension over $\mathbf{Z}_p$.
Let $\dim_{\mathbf{Z}_p} F = n$. Then we can find $a_1, \ldots, a_n$ a F such that

$$F = \mathbf{Z}_p a_1 + \mathbf{Z}_p a_2 + \ldots + \mathbf{Z}_p a_n.$$

We will show that F has p^n elements.

Now, any element of F is of the form

$$b_1 a_1 + b_2 a_2 + \ldots + b_n a_n, \text{ where } b_1, \ldots, b_n \in \mathbf{Z}_p.$$

Now, since $o(\mathbf{Z}_p) = p$, b_1 can be any one of its p elements.

Similarly, each of $b_2, b_3, \ldots, b_n$ has p choices. And, corresponding to each of these choices we get a distinct element of F. Thus, the number of elements in F is
$p \times p \times \ldots \times p$ (n times) $= p^n$.

The order of a finite field is the number of elements in it.

The utility of this result is something similar to that of Lagrange's theorem. Using this result we know that, for instance, no field of order 26 exists. But does a field of order 25 exist? Does Theorem 7 answer this question? It only says that a field of order 25 can exist. But it does not say that it does exist. The following exciting result, the proof of which is beyond the scope of this course, gives us the required answer. This result was obtained by the American mathematician E.H. Moore in 1893.

Theorem 8 : For any prime number p and $n \in \mathbf{N}$, there exists a field with p^n elements. Moreover, any two finite fields having the same number of elements are isomorphic.

Now, you can utilise your knowledge of finite fields to solve the following exercises. The first exercise is a generalisation of E 13 in Unit 13.

E 14) Let F be a finite field with p^n elements. Show that $a^{p^n} = a \ \forall \ a \in F$. And hence. show that $x^{p^n} - x = \prod_{a_i \in F} (x - a_i)$.

(Hint : Note that $(F \setminus \{0\}, .)$ is a group of order $p^n - 1$.)

E 15) Let F be a finite field with p^n elements. Define f : F → F : f(a) = a^p. Show that f is an automorphism of F of order n, i e., f is an isomorphism such that $f^n = I$, and $f^r \neq I$ for r < n.

f is called the **Frobenius automorphism of F,** after the mathematician Georg Frobenius ,1848–1917).

E 16) Let F be a field such that a ∈ F iff a is a root of $x^{27} - x \in F[x]$.

a) What is char F?

b) Is $\mathbb{Z}_2 \subseteq F$?

c) Is $Q \subseteq F$?

d) Is $F \subseteq Q$? Why?

E 17) Any two infinite fields are isomorphic. True or false? Why? Remember that isomorphic structures must have the same algebraic properties.

We close our discussion on field extensions now. Let us go over the points that we have covered in this unit.

15.4 SUMMARY

We have discussed the following points in this unit.

1) Gauss' lemma, i.e., the product of primitive polynomials is primitive.

2) Eisenstein's irreducibility criterion for polynomials over Z and Q. This states that if $f(x) = a_0 +$ a, x $+ \ldots + a_nx^n \in Z[x]$ and there is a prime p ∈ Z such that

i) $p \mid a_i \ \forall \ i = 0, 1, \ldots, n-1$.

ii) $p \nmid$ a,, and

iii) $p^2 \nmid a_0$,

then f(x) is irreducible over Z'(and hence over Q).

3) For any n ∈ N, we can obtain an irreducible polynomial over Q of degree n.

4) Definitions and examples of subfields and field extensions.

5) Different ways of obtaining field extensions of a field F from F[x].

6) Every field contains a subfield isomorphic to a prime field.

The prime fields are Q or Z_p, for some prime p.

7) The number of elements in a finite field F is p^n, where char F = p and $\dim_{Z_p} F = n$.

8) Given a prime number p and n ∈ N, there exists a field containing p^n elements. Any two finite fields with the same number of elements are isomorphic.

9) If F is a finite field with p^n elements, then $x^{p^n} - x$ is a product of p^n linear polynomials over F.

Now we have reached the end of this unit as well as this course. We hope that we have been able to give you a basic understanding of the nature of groups, rings and fields. We also hope that you enjoyed going through this course.

15.5 SOLUTIONS/ANSWERS

E 1) a) 1, b) 7, c) 5

E 2) Let $f(x) = a_0 +$ a, x $+ \ldots + a_nx^n$ and let the content of f(x) be d. Let $a_i = db_i \ \forall \ i = 0, 1, \ldots, n$. Then the g.c.d of $b_0, b_1, \ldots, b_n$ is 1. Thus, $g(x) = b_0 +$ b, x $+ \ldots + b_nx^n$ is primitive. Also,

$f(x) = db_0 + db_1 x + \ldots + db_nx^n = d(b_0 + b_1 x + \ldots + b_nx^n) = d\,g(x)$.

E 3) $f(x) = x^n - p = a_0 + a_1 x + ... + a_n x^n$;

where $a_0 = -p, a_1 = 0 = ... = a_{n-1}, a_n = 1$

Thus, $p \mid a_i \; \forall \; i = 0, 1, ..., n - 1, p^2 \nmid a_0, p \nmid a_n$.

So, by the Eisenstein criterion, $f(x)$ is irreducible over **Q**.

E 4) Not necessarily.

For example, there is no p that satisfies the conditions for $f(x)$ in Example **3.**

E 5) All of.them. (a) and (b), because of Eisenstein's criterion; and (c), because any linear polynomial is irreducible.

E 6) Since $a \neq 0, \pm 1, \exists$ a prime q such that $q \mid a$. Also $q^2 \nmid a$, since a is square-free. Then, using q as the prime, we can apply Eisenstein's criterion to find that $x^p + a$ is irreducible in **Z**[x]. Thus, it is **a** prime element of **Z**[x]. Hence, $< x^p + a >$ is a prime ideal of **Z**[x].

Hence the result.

E 7) By E 13 of Unit 13 we know that $\bar{a}^p = \bar{a} \; \forall \; \bar{a} \in \mathbf{Z}_p$. Now consider

$x^p + \bar{a} \in \mathbf{Z}_p[x]$.

$\overline{p-a}$ is a zero of this polynomial, since

$(\overline{p-a})^p + \bar{a} = \overline{p-a} + \bar{a} = \bar{p} = \bar{0}$ in $\mathbf{Z}_p$.

Thus, $x^p + \bar{a}$ is reducible over $\mathbf{Z}_p$.

E 8) a) **Q** + i**Q** is a non-empty subset of **C.**

Now, let a+ib and c+id be in **Q**+i**Q**.

Then $(a + ib) - (c + id) = (a - c) + i\,(b - d) \in \mathbf{Q} + i\mathbf{Q}$.

Further, let $c + id \neq 0$, so that $c^2 + d^2 \neq 0$.

Then $(c + id)^{-1} = \frac{c-id}{c^2 + d^2}$

Thus, $(a + ib)\,(c + id)^{-1} = (a + ib)\frac{(c - id)}{c^2 + d^2}$

$$-\frac{(ac + bd)}{c^2 + d^2} \; i \frac{(bc - ad)}{c^2 + d^2} \in \mathbf{Q} \;\; i\,\mathbf{Q}.$$

Thus, **Q** + i**Q** is a subfield of **C.**

b) $2 \in Z + \sqrt{2}\mathbf{Z}$ but $2^{-1} \notin Z + \sqrt{2}\,Z$. Therefore,

$Z + \sqrt{2}\,Z$ is not a field, and hence not a subfield of R.

E 9) (a), (b) and (c).

E 10) Let F be a field and K be a subfield of F. Then, we have just seen that both K and F have isomorphic prime subfields.

Thus, K contains the prime subfield of F.

Thus, we have shown that every subfield of F must contain its prime subfield. Hence, this is the smallest subfield of F.

E 11) F must contain a prime subfield. But it contains no proper subfield. Hence, **it** must be its own prime subfield. That is, F must be isomorphic to a prime field.

E 12) **Q**, $\mathbf{Z}_5$, $\mathbf{Z}_2$, since their characteristics are 0,5 and **2,** respectively.

E 13) Let F be a field. Firstly, let us assume that char F = p is known. Then, by Theorem 6, we know the prime subfield of F. Conversely, let K be the **prime** subfield of F. Then we know char K, and as shown before E **10,** char F = **char** K. So we know char F.

E 14) Since $(F\setminus\{0\},.)$ is a group of order $p^n - 1$, $a^{p^n-1} = 1$ $\forall\ a \in F \setminus\{0\}$.

$\therefore\ a^{p^n} = a\ \forall\ a \in F\setminus\{0\}$. Also $0^{p^n} = 0$.

Thus, $a^{p^n} = a\ \forall\ a \in F$.

Now, $x^{p^n} - x \in F[x]$ can have at the most p^n roots in F (by Theorem 7 of Unit 13).

Also, each of the p^n elements of F is a root. Thus, these are all the roots of $x^{p^n} - x$.

$$\therefore\ x^{p^n} - x = \prod_{a_i \in F} (x - a_i).$$

E 15) $f(a + b) = (a + b)^p = a^p + b^p$ (using E 10 of Unit 12)

$= f(a) + f(b)$.

$f(ab) = (ab)^p = a^p b^p = f(a) f(b)$.

f is 1 – 1, by E 10(c) of Unit 12.

Hence, Im f has the same number of elements as the domain off, i.e., F. Further; Im f $\subseteq$ F $\therefore$ Im f = F, i.e., f is onto.

Hence, f is an automorphism.

Now, $f^n(a) = [f(a)]^n = (a^p)^n = a^{p^n} = a\ \forall\ a \in F$.

$\therefore\ f^n = I$.

Also, for $r < n$, $f^r(a) = a^{p^r}$

Now, we can't have $a^{p^r} = a\ \forall\ a \in F$, because'this would mean that the polynomial $x^{p^r} - x \in F[x]$ has more than p^r roots. This would contradict Theorem 7 of Unit 13. Thus, $f^r(a) \neq a$ for some $a \in F$. $\therefore\ f^r \neq I$ if $r < n$.

Hence, $o(f) = n$.

E 16) $a \in F$ iff $a^{27} = a$, i.e., $a^{3^3} = a$.

a) Char F = 3.

b) No, since char $Z_2 \neq$ char F.

c) No.

d) No, since $F \subseteq Q \Rightarrow$ char F = char Q = 0.

E 17) False.

For example, Q and R are both infinite, but Q has no proper subfields, while R does. Thus, Q and R are riot isomorphic.