UNIT 13 : SPLITTING FIELD

UNIT STRUCTURE

13.1 Learning Objectives

13.2 Introduction

13.3 Splitting Field : Definitions and Examples

13.4 Properties of Splitting Field

13.5 Finite Splitting Field

13.6 Let Us Sum Up

13.7 Answer to Check Your Progress

13.8 Further Reading

13.9 Model Questions

13.1 LEARNING OBJECTIVES

After studying this unit, you will be able to

- define and find a splitting field of a polynomial over a given field;
- prove that the splitting field of a polynomial over a given field is unique upto isomorphism;
- prove that every finite field is a splittting field of a polynomial;
- prove the existence and uniqueness of spiltting fields having p^n elements,for every prime p and $n \in N$.

13.2 INTRODUCTION

In the previous unit,we studied algebraic extensions.We know that given an irreducible polynomial $p(x)$ over a field K, $K[x]/\langle p(x)\rangle$ is an extension field of K containing one root of $p(x)$.However this extension field may not contain all the other roots of $p(x)$.

We see that a extension $E|F$ contains all the roots of a given polynomial $f(x)$ over the field F and such extension exists.We will also see that there is a "smallest " extension field with the property which is called a splitting field $f(x)$ over F .

13.3 SPLITTING FIELD : DEFINITIONS AND EXAMPLES

Let E be an extension field of F and let $f(x) \in F[x]$ with degree at least one.We say that $f(x)$ spilts in E if there are elements $a \in F$ and $a_1, a_2, ..., a_n \in E$ such that

$$f(x) = a(x - a_1)(x - a_2), ..., (x - a_n)$$

We call E is a splitting field for $f(x)$ over F if $E = F(a_1, a_2, ..., a_n)$.

Note that a splitting field of a polynomial over a field depends not only on the polynomial but on the field as well.Indeed,a splitting field of $f(x)$ over F is just a smallest extension field of F in which $f(x)$ splits.

Example 1: Consider the polynomial $f(x) = x^2 + 1 \in Q[x]$.Since $x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$,we see that $f(x)$ splits in C,but a splitting Q is $Q[i] = \{r + si : r, s \in Q\}$.A splitting field $x^2 + 1$ over R is C.Likewise, $x^2 - 2 \in Q[x]$ splits in R,but a splitting field over Q is

$$Q(\sqrt{2}) = \{r + s\sqrt{2} : r, s \in Q\}$$

Example 2. Let $f(x) = x^3 - 2$.Then $f(x)$ is irreducible over Q by Eisenstein's Criterion.The zeros of $f(x)$ are $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2$ where ω is a complex cubic roots of unity.So a splitting field $f(x) = x^3 - 2$ over Q is the field $Q\left(2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2\right)$,which is the same as the field $Q\left(2^{\frac{1}{3}}, \omega\right)$.

Example 3: Let $f(x) = x^3 - 2$ over Z_3.

Then $f(x) = x^3 - 2$

$$= x^3 + \bar{1}$$

$$= \left(x + \bar{1}\right)^3 \text{ in } Z_3[x].$$

Hence,a splitting field over Z_3 is $Z_3\left(-\bar{1}, -\bar{1}, -\bar{1}\right) = Z_3$.

13.4 PROPERTIES OF SPLITTING FIELD

Theorem 13.4.1: Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$.Then there exists a splitting field E for $f(x)$ over F.

Proof : We prove the theorem by induction on degree of $f(x)$.Let deg $f(x)=1$.Then $f(x)$ is linear and is of the form $\alpha x+\beta$ for some $\alpha,\beta\in F$ with $\alpha\neq 0$.Then $f(x)=\alpha x+\beta$ has only zero is $-\beta\alpha^{-1}\in F$ .Here we can take $E=F$ and thus the result holds for deg $f(x)=1$.

Now suppose that the statement is true for all fields and all polynomials of degree less than that of $f(x)$.Then there is an extension E of F in which $f(x)$ has a zero,say, a_1.Then we may write $f(x)=(x-a_1)g(x)$,where $g(x)\in E[x]$.

Since $\deg g(x)<\deg f(x)$,by induction ,there is a field K that contains E and all the zeros of $f(x)$,say $a_2,a_3,...,a_3$.Clearly,a splitting field $f(x)$ over F is $F(a_2,a_3,...,a_3)$.

Example 1: Consider $f(x)=x^4-x^2-2$

$$=(x^2-2)(x^2+1) \text{ over } Q.$$

Obiously,the zeros of $f(x)$ in C are $\pm\sqrt{2}$ and $\pm i$ .So the spiltting field for $f(x)$ over Q is

$$\begin{aligned} Q(\sqrt{2},i) &= Q(\sqrt{2})(i) \\ &= \{\alpha+\beta i:\alpha,\beta\in Q(\sqrt{2})\} \\ &= \{(a+b\sqrt{2})+(a+b\sqrt{2})i:a,b,c,d\in Q\} \end{aligned}$$

Example 2: Consider $f(x)=x^2+x+2$ over Z_3

$$Z_3=[x-(1+i)][x-(1-i)]$$

Therefore $Z_3(i)=\{a+bi:a,b\in Z_3\}$is a splitting field of $f(x)$ over Z_3.

At the same time,by Theorem 12.12.16 the element $x+\langle x^2+x+2\rangle$ of $F=Z_3[x]/\langle x^2+x+2\rangle$ is a zero of $f(x)$.Since $f(x)$ has degree 2,it follows from factor theorem that the other zero of $f(x)$ must also be in F.Thus $f(x)$splits in F and F is also a splitting field of $f(x)$over Z_3.

Let $\beta=x+\langle x^2+x+2\rangle$.With this identification,the field $F=Z_3[x]/\langle x^2+x+2\rangle$can be represented as

$\{0,1,2,\beta,2\beta,\beta+1,2\beta+1,\beta+2,2\beta+2\}$. Since β is a zero for $f(x)$,So

$$f(\beta)=0 \Rightarrow \beta^2+\beta+2=0$$
$$\Rightarrow \beta^2=-\beta-2$$
$$=2\beta+1$$

To obtain the factorization of $f(x)$ in F,we simply long divide as follows

$$\begin{array}{l} x+(\beta+1) \\ x-\beta \;\; x^2+x+2 \\ \qquad\; x^2-\beta x \\ \qquad\; (\beta+1)x+2 \\ \qquad\; (\beta+1)x-(\beta+1)\beta \\ \qquad\; (\beta+1)\beta+2=\beta^2+\beta+2 \end{array}$$

So $x^2+x+2=(x-\beta)(x+\beta+1)$.Thus,we have find to splitting field for x^2+x+2 over Z_3 ,one is of the form $F(a)$ and one of the form $F[x]/\langle p(x)\rangle$.

Theorem 13.4.2.Let F be a field and $p(x)\in F[x]$ be irreducible over F.If a is a zero of $p(x)$ in some extension E of F,then $F(a)$ is isomorphic to $F[x]/\langle p(x)\rangle$.

Furthermore,if $\deg p(x)=n$,then every member of $F(a)$ can be uniquely expressed in the form

$c_{n-1}a^{n-1}+c_{n-2}a^{n-2}+\cdots+c_1a+c_0$ where $c_0,c_1,c_2,...,c_{n-1}\in F$.

Proof : Consider the map $\phi: F[x]\to F[a]$ defined by $\phi(f(x))=f(a)$.

Then clearly ϕ is a ring epimorphism.Then by fundamental theorem of ring homomorphism,

$$F[x]/\ker\phi \cong F(a)$$

Now we claim that $\ker\phi=\langle p(x)\rangle$ .Since $p(a)=0$,so $\langle p(x)\rangle\subseteq\ker\phi$ .Again since $p(x)\in F[x]$ is an irreducible over F ,so $\langle p(x)\rangle$ is a maximal ideal in $F[x]$.Thus $\langle p(x)\rangle\subseteq\ker\phi\subseteq F[x]$ and $\ker\phi\neq F[x]$imply that $\ker\phi=\langle p(x)\rangle$ .Hence

$$F[x]/\langle p(x)\rangle \cong F(a)$$

The second part of the theorem follows from the fact that every element of $F[x]/\langle p(x)\rangle$ can be expressed uniquely in the form

$$c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0 + \langle p(x)\rangle$$

where $c_0, c_1, c_2, ..., c_{n-1} \in F$ and the natural isomorphism from $F[x]/\langle p(x)\rangle$ to $F(a)$ carries $c_k x^k + \langle p(x)\rangle$ to $c_k a^k$.

Corollary 13.4.3.Let F be a field and let $p(x) \in F[x]$ be irreducible over F.If a is a zero of $p(x)$ in some extension of E of F and b is a zero of $p(x)$ in some extension E' of F,then the field $F(a)$ and $F(b)$ are isomorphic.

Proof : $F(a) \cong F[x]/\langle p(x)\rangle \cong F(a)$

Example 1:Consider the irreducible polynomial $f(x) = x^6 - 2$ over Q.Since $\sqrt[6]{2}$ is a zero of $f(x)$,therefore the set $\left\{1, 2^{\frac{1}{6}}, 2^{\frac{2}{6}}, 2^{\frac{3}{6}}, 2^{\frac{4}{6}}, 2^{\frac{5}{6}}\right\}$ is a basis of $Q(\sqrt[6]{2})$ over Q and $Q(\sqrt[6]{2}) \cong Q[x]/\langle x^6 - 2\rangle$.

Lemma 13.4.4 Let $\sigma : F \to F'$ be a field isomorphism.Then σ induces an isomorphism $\bar{\sigma} : F[x] \to F'[x]$ defined as $\bar{\sigma}(\sum a_i x^i) = \sum \sigma(a_i) x^i$ .Further $\bar{\sigma}$ maps irreducible polynomials to irreducible polynomials.

Lemma 13.4.5 Let F , F' be fields and σ be an isomorphism from F to F' ,extended to $\bar{\sigma} : F[x] \to F'[x]$.Let $p(x) \in F[x]$ be an irreducible polynomial .Then $\bar{\sigma}(p(x)) \in F'[x]$ is also irreducible (by Lemma 13.4.4).If a is a zero of $p(x)$ in some extension of F and b is a zero of $\bar{\sigma}(p(x))$ in some extension of F' ;then σ can be extended to an isomorphism $\bar{\sigma} : F(a) \to F'(b)$ such that $\bar{\sigma}(a) = b$.

Proof : By lemma 13.4.4, $\exists\ \bar{\sigma} : F[x] \to F'[x]$ such that $p(x)$ is irreducible over F implies $\bar{\sigma}(p(x))$ is irreducible over F' .Under this

isomorphism,the maximal ideal $\langle p(x)\rangle$ is mapped onto the maximal ideal $\langle \bar{\sigma}(p(x))\rangle$ and hence

$\psi : F[x]/\langle p(x)\rangle \to F'[x]/\langle \bar{\sigma}(p(x))\rangle$ defined by

$\psi(f(x)+\langle p(x)\rangle) = \bar{\sigma}(f(x))+\langle \bar{\sigma}(p(x))\rangle$ is an ring isomorphism.

Since a and b are roots of $p(x)$ and $\bar{\sigma}(p(x))$ respectively,by theorem 13.4.2,

$F[x]/\langle p(x)\rangle \cong F(a)$ and $F'[x]/\langle \bar{\sigma}(p(x))\rangle \cong F'(b)$.

If $\phi : F[x]/\langle p(x)\rangle \to F(a)$ and $\phi' : F'[x]/\langle \bar{\sigma}(p(x))\rangle \to F'(b)$ are isomorphisms,then the composition $\bar{\sigma} = \phi' \circ \psi \circ \phi^{-1}$ is an isomorphism from $F(a)$ to $F'(a)$.

Now for any $\alpha \in F$,we have

$$\bar{\sigma}(\alpha) = (\phi' \circ \psi \circ \phi^{-1})(\alpha)$$
$$= \phi'\psi(\phi^{-1}(\alpha))$$
$$= \phi'(\psi(\alpha) + \langle p(x)\rangle)$$
$$= \phi'(\bar{\sigma}(\alpha)) + \langle \bar{\sigma}(p(x))\rangle$$
$$= \bar{\sigma}(\alpha)$$

Thus $\bar{\sigma}/F(a) = \bar{\sigma}$

Also $\bar{\sigma}(a) = (\phi' \circ \psi \circ \phi^{-1})(a)$

$$= \phi' \circ \psi(\phi^{-1}(a))$$
$$= \phi'(\psi(x + \langle p(x)\rangle))$$
$$= \phi'(\bar{\sigma}(x + \langle \bar{\sigma}(p(x))\rangle))$$
$$= \phi'(x + \langle \bar{\sigma}(p(x))\rangle) \qquad [\because \bar{\sigma}(x) = x]$$
$$= b \quad \because b \text{ is a zero of } \bar{\sigma}(p(x)).$$

Thus $\bar{\sigma}$ is the required isomorphism between $F(a)$ and $F'(b)$,which

extends σ and $\bar{\sigma}(a)=b$.

Now, let us use this lemma to prove that the theorem showing the uniquenessof the splitting field of a polynomial over a given field.

Theorem 13.4.6.Let $\sigma: F \to F'$ be a field isomorphism extending to the ring isomorphism $\bar{\sigma}: F[x] \to F'[x]$.Let $f(x) \in F[x]$ and E and E' be splitting fields of $f(x)$ and $\bar{\sigma}(f(x))$respectively.Then,there exists an isomorphism from E to E' which is an extension of σ.

Proof:We will prove this by induction on $\deg(f(x))$.If $\deg(f(x))=1$,then $E=F$, $E'=F'$ and theorem holds trivially.Assume that the theorem holds for polynomials of degree not exceeding $n-1$.

Now let $f(x) \in F[x]$ with $\deg(f(x))=n$.Let $p(x)$be an irreducible factor of $f(x)$ over F, a be a root of $p(x)$and b be a root of $\bar{\sigma}(p(x))$.By lemma 13.4.5, σ can be extended to an isomorphism $\bar{\sigma}$ from $F(a)$ to $F'(b)$mapping a to b.

Let us write $f(x)=(x-a)g(x)$ in $F(a)[x]$,so that

$\bar{\sigma}(f(x))=\bar{\sigma}(f(x))=(x-b)\bar{\sigma}(g(x))$.

Since E is a splitting field of $f(x)$over F,it is a splitting field of $g(x)$over $F(a)$.Similarly E' is a splitting field of $\bar{\sigma}(g(x))$ over $F'(b)$.As $\deg g(x)=n-1$,by induction $\bar{\sigma}$ can be extended to an isomorphism $\bar{\sigma}'$ from E to E'.Since $\bar{\sigma}'$ is an extension of $\bar{\sigma}$, $\bar{\sigma}'/_F=\sigma$.

Thus,the theorem is true for a polynomial of degree n and hence for all polynomials.

Corollary 13.4.7.The splitting field of a polynomial over a field F is unique upto isomorphism.

Proof : The result follows immediately from theorem 13.4.6,on taking $F=F'$ and σ as the identity map.

Example 2: Consider the polynomial $f(x)=x^4+4$ over Q.

Note that $f(x)=x^4+4$

$$=(x^2+2)^2-4x^2$$

$$=(x^2-2x+2)(x^2+2x+2) \text{ in } Q[x].$$

By Eisenstein's criterion, x^2-2x+2 and x^2+2x+2 are irreducible over Q.Their roots,in C,are $1\pm i$ and $-1\pm i$.Thus,the splitting field of $f(x)$

over Q will be $Q(1+i,1-i,-1+i,-1-i)$.i.e., $Q(i)$.

Here,we can see that $[Q(i):Q]=2<\deg(x^4+4)$.

Example 3: Consider the polynomial $f(x)=x^n-1$ over Q,where $n\in N$.

As we know,the roots of $x^n-1=0$ are the nth roots of unity.Using De Moivre's theorem,the roots are $e^{\frac{2\pi ik}{n}}=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}$ where $k=0,1,2,\cdots,n-1$.

Thus the splitting field is $Q\left(1,e^{\frac{2\pi i}{n}},e^{\frac{4\pi i}{n}},...,e^{\frac{2(n-1)\pi i}{n}}\right)$.

Now let $\zeta_n=e^{\frac{2\pi i}{n}}$.Then $e^{\frac{2k\pi i}{n}}=\zeta_n^k$ for all $k=0,1,2,\cdots,n-1$.

Thus $F=Q(1,\zeta_n,\zeta_n^2,\cdots,\zeta_n^{n-1})$

$=Q(\zeta_n)$



CHECK YOUR PROGRESS

Q 1. Show that x^2+3 and x^2+x+1 has same splitting field.Also find the degree of splitting field.

Q 2. Find the splitting field of x^3-3x+1 over Q.

Q 3. Find the splitting field of x^4-1 over Q.Also find the degree of splitting field.

Q 4. Find the degree of splitting field of $x^5-3x^2+x^2-3$ over Q.

13.5 FINITE SPLITTING FIELDS

We have studied fields of different kinds,including Q and Z_p,where p is a prime.We have noted that Z_p has p elements,and hence it is a finite fields.As we know,a field has at least two elements 0,1.Thus,the smallest field having only two elements is Z_2.Further,recall that any finite field contains its prime subfield, Z_p,for some prime p.Hence the characteristic of a finite field is always a prime number.

Example 1:Consider the polynomial $f(x)=x^p-x$ where p is prime.

By Fermat's little theorem,every element of Z_p is zero of $f(x)$.Thus

all p zeros of $f(x)$ are in Z_p and hence, Z_p is the splitting field of $f(x)$ over Z_p.

Lemma 13.5.1.Let F be a finite field .Then F has p^n elements,for some prime p and positive integer n.

Proof: Since F is a finite field,its characteristic must be a prime (say) p .Therefore,the prime subfield P of F is isomorphic to Z_p .So F can be considered as a vector space over Z_p .Since F is finite, $[F:P]$ is finite,say n.

Thus, F has p^n elements.

Note :Every finite field is the splitting field of some polynomial over Z_p.

Definition: Let F be a finite field and let $f(x) \in F[x]$ split over its splitting field E as

$$f(x) = a(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_r$ are distinct zeros of $f(x)$ in E and $n_i \geq 1$ for all $i \in \{1,2,\cdots,r\}$.The zero α_i is called a multiple zero of $f(x)$ if $n_i > 1$ and is called a simple zero if $n_i = 1$.The integer n_i is called the multiplicity of the zero α_i .

For instance, $x^4 - 4x^2 + 3 \in Q[x]$ has only simple zero in R ,namely $\pm 1, \pm 3$ .But $(x+2i)^2(x-5) \in C[x]$ has one multiple zero $-2i$ and one simple zero 5.

Definition : Let F be a field and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial over F .Then the formal derivative of $f(x)$ is the polynomial

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x]$$

For instance,if $f(x) = 3x^5 + 0.7x^2 + \pi x \in R[x]$, then

$f'(x) = 15x^4 + 1.4x + \pi.$

Similarly, if $f(x) = 3x^5 + 2x \in Z_5[x]$,then $f'(x) = 2 \in Z_5[x]$,since $5 = 0$ in Z_5.

Properties of derivative: If $f(x)$ and $g(x)$ are polynomials over F ,then

(i) $[f(x)+g(x)]' = f'(x)+g'(x)$

(ii) $[af(x)]' = af'(x)$

(iii) $[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$

Lemma 13.5.4. Let F be a field and $f(x)$ be a non-constant polynomial over F .Then all the zeros of $f(x)$ are simple (in the splitting field of $f(x)$) if and only if $f(x)$ and its derivative $f'(x)$ are relatively prime.

Theorem 13.5.5.(Existence and Uniqueness of finite fields):For each prime number p and each integer $n \geq 1$,there exists exactly one field (upto isomorphism) with p^n elements,namely,the splitting field of the polynomial $f(x) = x^{p^n} - x$ over Z_p and these are the only finite fields.

Proof: We shall first prove that there exists a field of order p^n for each prime p and $n \in N$.

Consider $f(x) = x^{p^n} - x$ over the field Z_p and let E be the splitting field of $f(x)$ over Z_p .Since the characteristic of Z_p is p , $f'(x) = -1$. Therefore $f(x)$ and $f'(x)$ are relatively prime and hence,by lemma 13.5.4, all the zeros of $f(x)$ in E are distinct.

Now, let K be the set of all the zeros of $f(x)$ in E .Let $\alpha, \beta \in K$ .Then $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. Since $\text{char}E = p$, $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$.

Now $(\alpha \pm \beta)^{p^n} = \left\{(\alpha \pm \beta)^{p^{n-1}}\right\}^p$ and by induction,we get

$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$

Also $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n}$

Therefore, if α and β are zeros of $f(x)$,then so are $\alpha \pm \beta$ and $\alpha\beta$ .Clearly $0,1 \in K$. Thus K is a subfield of E .As the prime subfield is contained in every subfield of E , $Z_p \subseteq K$.

Thus K is the splitting field of $f(x)$ and contains exactly p^n elements.Since the splitting field is unique upto isomorphism,it follows that $E = K$ .Hence,for any positive integer n and prime number p ,the splitting field of the polynomial $f(x) = x^{p^n} - x$ over Z_p is a field having p^n elements.

Next we prove uniqueness part of the theorem.So,let E and K be two finite fields having the same number of elements,say p^n ,for some positive integer n and prime number p .Then E and K are the splitting

fields of $f(x)=x^{p^n}-x$ over Z_p as both the fields E and K have the same characterstic p .Since the splitting fields of a polynomial are unique upto is isomorphism, $E\cong K$. Thus upto isomorphism,there are exactly one field with p^n elements.This field is denoted by $GF(p^n)$.

Remark: Note that there can be several fields of order p^n .However,they will all be isomorphic,not equal.For example, x^2+1 and x^2-x-1 are both irreducible over Z_3 .Hence $K=Z_3[x]\big/\langle x^2+1\rangle$ and $L=Z_3[x]\big/\langle x^2-x-1\rangle$ are both field having q elements.Hence both are isomorphic to Z_q .But $K\neq L$,since $\overline{x^2+1}=\bar{0}$ in K but $\overline{x^2+1}=\overline{x+2}\neq\bar{0}$ in L .

Example 1:Give an explicit construction of a field with 4 elements.

Solution: By theorem 13.5.5,we know that there exists a finite field with $2^2=4$ elements,viz $GZ_2(2^2)=GZ_4(4)$ with characterstic 2.

We also know that $GZ_4(4)$ is the splitting field of x^4-x over Z_2 .Let $GZ_4(4)=\{0,1,\alpha,\beta\}$ .Now $x^4-x=x(x-1)(x^2+x+1)$

We can see that x^2+x+1 is irreducible over Z_2 .Also α,β have to be zeros of x^2+x+1 .So $\alpha^2+\alpha+1=0$ and

$$\alpha+\beta=-1$$
$$\Rightarrow \alpha+\beta=1 \text{ ,since } \operatorname{char}GZ_4(4)=2$$
$$\Rightarrow \beta=-\alpha+1$$
$$\therefore \beta=\alpha+1 \text{,since } \operatorname{char}GZ_4(4)=2$$

Thus $GZ_4(4)=\{0,1,\alpha,1+\alpha\}$ and a basis of Z_4 over Z_2 is $\{1,\alpha\}$.



CHECK YOUR PROGRESS

Q 5. Construct a field with 9 elements.

Q 6. Show that the product of the non-zero elements of $GF(p^n)$ is -1.

Q 7. Let F be a field of characterstic p .Let b be a root of $f(x)=x^p-x-a\in F[x]$.Show that splitting field of $f(x)$ over F is $F(b)$.

Q 8. Let $f(x)=x^4+x^2+1\in Q[x]$. Show that splitting field of $f(x)$ over Q is $Q(\omega)$ and $[Q(\omega):Q]=2$.

Q 9. Show that the splitting field of x^4+1 over Q is $Q(\sqrt{2},i)$ whose degree over Q is 4.

Q 10. Identify the splitting fields of the following polynomials:

(i) $f(x)=(x^3-2)(x^2+x+1)$ over Q,

(ii) $f(x)=(x^3-5)^2$ over Q,

(iii) $f(x)=x^6+1$ over Z_2.



13.6 LET US SUM UP

- Let E be an extension field of F and let $f(x)\in F[x]$ with degree at least one. We say that $f(x)$ splits in E if there are element $a\in F$ and $a_1,a_2,\cdots,a_n\in E$ such that $f(x)=a(x-a_1)(x-a_2)\cdots(x-a_n)$.
  We call E is a splitting field for $f(x)$ over F if $E=F(a_1,a_2,\cdots,a_n)$.
- Let F be a field and $f(x)$ be a non constant polynomial in $F[x]$. Then there exists a splitting field E of $f(x)$ over F.
- Let F be a field and $p(x)\in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)\cong F[x]/\langle p(x)\rangle$.
  Furthermore, if $\deg p(x)=n$, then every memnber of $F(a)$ can be uniquely expressed in the form
  $c_{n-1}a^{n-1}+c_{n-2}a^{n-2}+\cdots+c_1a+c_0$ where $c_0,c_1,c_2,\cdots,c_{n-1}\in F$.
- Let F be a field and $p(x)\in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then the field $F(a)$ and $F(b)$ are isomorphism.
- Let $\sigma:F\to F'$ be a field isomorphism. Then σ induces an isomorphism $\overline{\sigma}:F[x]\to F'[x]$ defined as $\overline{\sigma}(\sum a_ix^i)=\sum\sigma(a_i)x^i$.
  Further $\overline{\sigma}$ maps irreducible polynomials to irreducible polynomials.
- Let F and F' be two fields and $\sigma:F\to F'$ be an isomorphism extended to $\overline{\sigma}:F[x]\to F'[x]$. Let $p(x)\in F[x]$ be an irreducible

polynomial.Then $\bar{\sigma}(p(x)) \in F'[x]$ is also irreducible.If a is a zero of $p(x)$ in some extension of F and b is a zero of $\bar{\sigma}(p(x))$in some extension of F',then σ can be extended to an isomorphism $\bar{\sigma}: F(a) \to F'(b)$such that $\bar{\sigma}(a) = b$.

- Let $\sigma: F \to F'$ be a field isomorphism ,extending to the ring isomorphism. $\bar{\sigma}: F[x] \to F'[x]$.Let $f(x) \in F[x]$ and E and E' be splitting field of $f(x)$ and $\bar{\sigma}(f(x))$ over F and F' respectively.Then there exists an isomorphism from E and E',which is an extension of σ.
- Let F be a finite field.Then F has p^n elements for some prime p and posditive integer n.
- Let F be a field and $f(x)$ be a nonconstant polynomial over F.Then all the zero of $f(x)$ are simple (in the splitting field of $f(x)$) if and only if $f(x)$ and its derivative $f'(x)$ are relatively prime.
- For each prime number p and each integer $n \geq 1$,there exists exactly one field (upto isomorphism) with p^n elements,namely the splitting field of the polynmomial $f(x) = x^{p^n} - x$ over Z_p and these are the only finite fields.

13.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q.No. 1.

The polynomials $f(x) = x^2 + 3$ and $g(x) = x^2 + x + 1$ have no rational zeros,so they are irreducible over Q (Note in general,if $f(x)$ is a polynomial of degree >3 over a field F such that $f(x)$ has no root in F,we cannot say that $f(x)$is irreducible).The zeros of $f(x)$ are $\pm\sqrt{-3}$, so $Q(\sqrt{-3})$ is the splitting field of $f(x)$. If $\omega = \frac{-1+\sqrt{-3}}{2}$, then ω, ω^2 are the zeros of $g(x) = x^2 + x + 1$.So $F(\omega)$is the splitting field of $g(x)$. Now $\sqrt{-3} = 2\omega + 1 \in Q(\omega)$ gives $Q(\sqrt{-3}) \subseteq Q(\omega)$. Again

$\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2} \in Q\left(\sqrt{-3}\right)$ gives $Q(\omega) \subseteq Q\left(\sqrt{-3}\right)$.

So $Q(\omega) = Q\left(\sqrt{-3}\right)$.

Hence $f(x)$ and $g(x)$ have the same splitting field.

Ans to Q. No. 2

Since the polynomial $f(x) = x^3 - 3x + 1$ over Q has no rational zeros,so it is irreducible over Q.Its zeros in R are

$$-2\cos\frac{\pi}{9}, 2\cos\frac{2\pi}{9}, 2\cos\frac{4\pi}{9}$$

Let $\alpha = -2\cos\frac{\pi}{9}$.Consider $Q(\alpha) \subseteq E$,the splitting field of $x^3 - 3x + 1$.

Now $2\cos\frac{2\pi}{9} = 4\cos^2\frac{\pi}{9} - 2$

$$= \alpha^2 - 2 \in Q(\alpha)$$

and $2\cos\frac{4\pi}{9} = 4\cos^2\frac{2\pi}{9} - 2 = \left(\alpha^2 - 2\right)^2 - 2 \in Q(\alpha)$

So all the zeros of $f(x) = x^3 - 3x + 1$ are in $Q(\alpha)$.Thus $E \subseteq Q(\alpha)$.

Hence $E = Q(\alpha)$.

Ans to Q. No. 3

The zeros of $f(x) = x^4 - 1$ over Q are $1, -1, i, -i$ where $i = \sqrt{-1}$.So the splitting field of $f(x)$ over Q is Q (i)

$$[Q(i) : Q] = 2$$

Ans to Q. No. 4

Let $f(x) = x^5 - 3x^3 + x^2 - 3 = (x^2 - 3)(x^3 + 1)$

The zeros of the Polynomial are $\pm\sqrt{3}, -1, \frac{1 \pm \sqrt{3}}{2} \in C$

So, the splitting field of f(x) over R is

$$K = Q\left(\pm\sqrt{3}, -1, \frac{1 \pm i\sqrt{3}}{2}\right)$$

$$= Q\left(\sqrt{3}, i\right)$$

Now $[K : Q] = [K : Q(i)][Q(i) : Q] \leq 2.2 = 4$ as minimal polynomial of i over Q is $x^2 + 1$ .Also, $[K : Q] = \left[K : Q\left(\sqrt{3}\right)\right]\left[Q\left(\sqrt{3}\right) : Q\right]$ shows that 2

is a factor of $[K:Q]$.So we get $[K:Q]=2$ or 4.In case $[K:Q]=2$,we get $[K:Q(\sqrt{3})]=1$ i.e. $K=Q(\sqrt{3})$ which is absurd as $i\in Q$ but $i\notin Q(\sqrt{3})$.

Hence $[K:Q]=4$.

Ans to Q. No. 5

The field is $GF(Z_9)$,the splitting field of x^9-x over Z_3.

Now $x^9-x=x(x-1)(x-2)(x^2+1)(x^2-x-1)(x^2+x-1)$ as a product of irreducible polynomials over Z_3.If α is a a zero of x^2+1 over Z_3,then $\{1,\alpha\}$ is an Z_3-basis of $G(Z_9)$.

So $G(Z_9)=\{0,1,2,\alpha,2\alpha,1+\alpha,1+2\alpha,2+\alpha,2+2\alpha\}$

Ans to Q. No. 6

Since every element of $GF_{p^n}(p^n)$ is the zero of $(x^{p^n}-x)$ over Z_n.Then nonzero elements of F_{p^n} are the zeros of $x^{p^n-1}-1$.

Thus $x^{p^n-1}-1=\prod_{i=1}^{p^n-1}(x-\alpha_i)$

Putting $x=0$ on both sides,we get

$-1=\prod_{i=1}^{p^n-1}(-\alpha_i)$

$(-1)^{p^n-1}\left(\prod_{i=1}^{p^n-1}\alpha_i\right)=-1$

For $p\neq 2$, p^n-1 is even and hence the result.

If $p=2$, $-1=1$ and hence the result.

Ans to Q. No. 7

Since b is a zero of $f(x)=x^p-x-a$,so $b^p-b=a$.

Also $(b+1)^p-(b+1)=b^p+1-b-1$ [$\because$ char $F=p$]

$=b^p-b=a$

$\therefore$ $b+1$ is a zero of $f(x)$.

Similarly $b+2$, $b+3$,..., $b+(p-1)$ are zeros of $f(x)$.Thus splitting field of $f(x)$ over $F=F(b,b+1,b+2,\cdots,b+(p-1))=F(b)$.

Ans to Q. No. 8

We have $\omega^2+\omega+1=0$,where $\omega=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$.

$\Rightarrow \omega^4+\omega^3+\omega^2=0$

$\Rightarrow \omega^4 + \omega^2 + 1 = 0$ as $\omega^3 = 1$

i.e. ω is a zero of $x^4 + x^2 + 1$ and so ω^2 is also a zero of $x^4 + x^2 + 1$.

$$\therefore f(x) = x^4 + x^2 + 1$$
$$= (x^2 - \omega^2)(x - \omega^4)$$
$$= (x-\omega)(x+\omega)(x-\omega^2)(x+\omega^2)$$

$\therefore$ Splitting field of $f(x)$ over Q is $Q(\omega, -\omega, \omega^2, -\omega^2) = Q(\omega)$

and $[Q(\omega) : Q] = 2$.

Ans to Q. No. 9

The zeros of $x^4 + 1$ are given by

$$x = (-1)^{\frac{1}{4}}$$
$$= (\cos\pi + i\sin\pi)^{\frac{1}{4}}$$
$$= \cos\frac{1}{4}(2k\pi + \pi) + i\sin\frac{1}{4}(2k\pi + \pi), \text{where } k = 0,1,2,3$$
$$= \cos\frac{1}{4}(2k+1)\pi + i\sin\frac{1}{4}(2k+1)\pi, \text{where } k = 0,1,2,3$$

$$= \frac{1}{\sqrt{2}}(1+i), -\frac{1}{\sqrt{2}}(1-i), -\frac{1}{\sqrt{2}}(1+i), \frac{1}{\sqrt{2}}(1-i)$$

$\therefore$ Splitting field of $x^4 + 1$ over Q is

$$K = Q\left(\pm\frac{1}{\sqrt{2}}(1+i), \pm\frac{1}{\sqrt{2}}(1-i)\right)$$
$$= Q(\sqrt{2}, i)$$

Now $x^2 + 1 \in Q(\sqrt{2})[x]$ is irreducible over $Q(\sqrt{2})$.

$$\Rightarrow [Q(\sqrt{2}, i) : Q(\sqrt{2})] = \deg Irr(Q(\sqrt{2}), i)$$
$$= 2 \text{ as } i \text{ satisfies } x^2 + 1.$$

But $[Q(\sqrt{2}) : Q] = \deg Irr(Q\sqrt{2})$
$$= \deg(x^2 - 2)$$
$$= 2$$

$$\therefore [K : Q] = [K : Q(\sqrt{2})][Q(\sqrt{2}) : Q]$$
$$= 2.2$$
$$= 4$$

Ans to Q. No. 10

(i) The zeros of $f(x)=(x^3-2)(x^2+x+1)$ over Q are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, ω, ω^2, where ω is complex cubic roots of unity.

Thus, the splitting field of $f(x)$ over Q is

$$Q(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2,\omega,\omega^2)=Q(\sqrt[3]{2},\omega)$$

(ii) The zeros of $f(x)=(x^3-5)^2$ over Q are $\sqrt[3]{5},\sqrt[3]{5}\omega,\sqrt[3]{5}\omega^2$, where ω is complex cubic roots of unity. Thus the splitting field of $f(x)$ over Q is

$$Q(\sqrt[3]{5},\sqrt[3]{5}\omega,\sqrt[3]{5}\omega^2)=Q(\sqrt[3]{5},\omega)$$

(iii) We have $f(x)=x^6+1$ over Z_2

$$=x^6-1 \text{ over } Z_2$$

$$=(x^3-1)^2$$

$$=(x+1)^2(x^2+x+1)^2$$

The zeros are $1,1,\alpha,\alpha,1+\alpha,1+\alpha$ where α is a zero of the irreducible polynomial x^2+x+1 over Z_2. Hence, the splitting field of $f(x)$ over Z_2 is $Z_2(\alpha)$.



13.8 FURTHER READING

1) Fraleigh, John B : A first course in Abstract Algebra, Pearson Education (Singapure) Pvt. Ltd.

2) Singh, S and Qazi, Z : Modern Algebra, Vikas Publicasting House Pvt. Ltd, New Delhi - 110014.

3) Gallian,Joseph A:Contemporary Abstract Algebra (8th Ed.),Cengage Learning India Pvt. Ltd.,Delhi-110092.

4) Khanna,V.K. and Bhambri,S.K.:A course in Abstract Algebra (2002),Vikas Publishing House Pvt. Ltd.,New Delhi-110014.



13.9 MODEL QUESTIONS

Q 1: Show that the splitting field of x^6-1 over Q is same as that of x^4+x+1 over Q and $[E:Q]=2$.

Q 2: Find the splitting fields and their degrees of the following polynomials over Q:

(i) x^4-2 (ii) x^5-1

Q 3: Let $f(x)$ be a polnomial over Q of degree n and E denote its splitting field over Q.Give examples of polynomials $f(x)$ for which

(i) $[E:Q]=n$ (ii) $[E:Q]<n$

(iii) $n<[E:Q]<n!$ (iv) $[E:Q]=n!$

Q 4: Let F be a field of characterstic p and let $f(x)=x^p-a\in F[x]$.Show that $f(x)$ is irreducible over F or $f(x)$ splits in F.

Q 5: Let $f(x)\in F[x]$ and let $a\in F$.Show that $f(x)$ and $f(x+a)$ have the same splitting field over F.

Q 6: Find the splitting field of $f(x)=(x^2+x+2)(x^2+2x+2)$ over Z_3.Write $f(x)$ as a product of linear factor.

Q 7: Let F, K and L be fields with $F\subseteq K\subseteq L$.If L is a splitting field for some nonconstant polynomial $f(x)$ over F,show that 1 is a splitting field for $f(x)$ over K.

*** ***** ***