UNIVERSITY OF CALICUT

SCHOOL OF DISTANCE EDUCATION

M.Sc Mathematics

(II SEMESTER)

(2019 Admn Onwards)

CORE COURSE : MTH2C06

ALGEBRA-II

190556

ALGEBRA-II

STUDY MATERIAL SECOND SEMESTER

CORE COURSE : MTH2C06

M.Sc Mathematics

(2019 Admn Onwards)

UNIVERSITY OF CALICUT
SCHOOL OF DISTANCE EDUCATION
Calicut University- PO, Malappuram,
Kerala, India - 673 635

UNIVERSITY OF CALICUT

SCHOOL OF DISTANCE EDUCATION

M.Sc Mathematics

(II SEMESTER)

(2019 Admn Onwards)

CORE COURSE : MTH2C06

ALGEBRA-II

Prepared by:

RAVEESH. R VARRIER,

Assistant Professor (Mathematics),

St. Aloysius College, Thrissur

Scrutinized By:

DR.SINI.P,

Assistant Professor, Department of Mathematics, University of Calicut

RING AND IDEALS

Addition, subtraction and multiplication are defined, division needn't be.

(**A**, +, **.**) is a **ring** when *addition* (+) and *multiplication* (**.**) are *well-defined* internal operations over the set **A** with the following properties:

- (**A**,+) is a commutative group whose identity element is called 0 (zero).
- Multiplication is an associative (not necessarily commutative) internal operation which is *distributive* over addition. That's to say:
  For all x, y and z element of A then x.(y + z) = x.y + x.z and
- (x + y).z = x.z + y.z

Optional properties of a ring can be indicated by specific qualifiers:

Ring with unity : There's a multiplicative neutral element:1.x= x.1 = x

Commutative Ring : Every x,y element of **A** , x.y = y.x

Division Ring : Any nonzero element has a multiplicative inverse.

Integral Ring : The product of two nonzero elements is nonzero.

(Z,+, .) ,(R,+, .),(C,+, .),(Q,+, .),(nZ,+, .)are some examples of ring.

An **integral domain** is a *commutative integral ring*. A **field** is defined as a *commutative* division ring.

(Z,+, .) ,(R,+, .),(C,+, .),(Q,+, .),(nZ,+, .)are some examples of integral domain.

Ideal

For an arbitrary ring A, let Ibe a additive group. Then I is called a **left ideal** of A if it is an additive subgroup of A that "absorbs multiplication from the left by elements of A ; that is, I is a **left ideal** if it satisfies the following two conditions:

1. I is a additive subgroup of A.
2. For every x∈ I and every r ∈A, the product $rx \in I$

A **right ideal** is defined with the condition "$r\,x \in I$" replaced by "$x\,r \in I$". A **two-sided ideal** is a left ideal that is also a right ideal, and is sometimes simply called an ideal.

Ideals of Z are of the form nZ. A field F has only 2 ideals {0} and F itself.

If I is a subset of R. Then I is an ideal if 'a-b' belong to I for every a,b belongs to I and 'ax' belongs to I for every 'x' belong to I and 'a' belongs to R.

Maximal Ideal: A maximal ideal of a ring *R* is an ideal *M* different from *R* such that there is no proper ideal *N* of R properly containing *M*.

Example: Let p be a prime positive integer. We know thatZ/pZ is isomorphictoZp. We know thatZp is a simple group, and consequentlypZ must be a maximal normal subgroup ofZ. SinceZ is an abelian group and hence every subgroup is a normal subgroup, we see that pZis a maximal proper subgroup of Z. Since pZ is an ideal of the ring Z, it follows that pZ is a maximal ideal of Z. We know that Z/pZ is isomorphic to the ring Zp, and that Zpis actually a field. Thus Z/pZ is a field. This illustrates the next theorem.

Theorem: Let *R*be a commutative ring with unity. Then *M* is a maximal ideal of *R* if and only if *R / M*is field.

Proof : Suppose M is a maximal ideal in *R*. Observe that if *R* is a commutative ring with unity,then*R / M*is also a nonzero commutative ring with unity if *M # R,*which is the case if M is maximal. Let (a + M) ∈ R / M, with a ∉ M, so that

a + M is not the additive identity element of R / M. Suppose a + M has no multiplicative inverse in R/M. Then the set (R /M) (a+M) = {(r+m)(a+M)∈R/M}does not contain 1+M. We easily see that (R / M)(a + M) is an ideal of *R / M*. It is nontrivial because a∈M, and it is a proper ideal because it does not contain 1 + *M*. If $\gamma: R \to R/M$ is the canonical homomorphism, then $\gamma^{-1}[(R/M)(a+M)]$is a proper ideal of R properly containing*M*. But this contradicts our assumption that Mis a maximal ideal, so a + M must have a multiplicative inverse in R /M.

Conversely, suppose that*R / M*is a field. If *N*is any ideal of *R*such that

$M \subset N \subset R$ and γ is the canonical homomorphism of R onto R/M, then $\gamma[N]$ is an ideal of R/M with $\{(0+M)\} \subset \gamma[N] \subset R/M$. But this is contradiction, since the field R/M contains no proper nontrivial ideals. Hence if R/M is a field, M is maximal.

Example: Since Z/nZ is isomorphic to Z_n and Z_n is a field if and only if n is a prime, we see that the maximal ideals of Z are precisely the ideals pZ for prime integers p.

Corollary : A commutative ring with unity is field if and only if it has no proper nontrivial ideals.

Proof : A field has no proper nontrivial ideals. Let I be an ideal of field F, then I can be equal to $\{0\}$ or not equal to $\{0\}$. If $I \neq \{0\}$ there exist some nonzero element in I, let it be a, then inverse of a belongs to F and their product belong to I. So 1 belong to I. Hence I = F.

Conversely, if a commutative ring R with unity has no proper nontrivial ideals, then {0} is a maximal ideal and,R/{0}, which is isomorphic to R, is a field.

The factor ring R/Nwill be an integral domain if and only if (a + N)(b +N) = N implies that either.

$$a + N = N \text{ or } b + N = N$$

This is exactly the statement that R / N has no divisors of 0, since the coset N plays the role of 0 in R/N. Looking at representatives, we see that this condition amounts to saying that$ab \in N$ implies that either $a \in N$ *or* $b \in N$.

Example: All ideals of Z are of the form nZ. For n = 0, we have nZ = {0}, and Z/{0} ≅ Z, which is an integral domain. For n > 0, we have Z/nZ ≅ Zn and Zn is an integral domain are of the form pZ, where is a prime. Of course,Z/pZ is actually a field, so that pZ is a maximal ideal of Z.

Note that for a product of integers to be in pZ, the prime p must divide either r or s.

Definition An ideal $N \neq R$ in a commutative ring *R* is prime ideal if $ab \in N$ implies that either $a \in N$ or $b \in N$ for a, b $\in$ R.

Note that {0} is a prime ideal in Z, and indeed, in any integral domain.

Example: Note that Z x {0} is a prime ideal of Z x Z, for if (a, b) (c, d) belongs to Z x {0}, then we must have bd = 0 in Z. This implies that either b =0

so (a, b) $\in$ Z x {0} or d = 0 so (c,d) $\in$ Z x {0}. Note that (Z x Z)/ (Z x {0}) Is isomorphic to Z , which is an integral domain.

Theorem: Let *R* be a commutative ring with unity, and let $N \neq R$ be an ideal in *R*. Then *R/N* is an integral domain if and only if *N* is a prime ideal in *R*.

Corollary: Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof If M is maximal in R, then R/M is a field, hence an integral domain, and therefore M is a prime ideal.

Note: For a commutative ring R with unity:

1. An ideal M of R is maximal if and only if R/M is a field.
2. An ideal N of R is prime if and only if R/N is an integral domain.
3. Every maximal ideal of R is a prime ideal.

We now proceed to show that the rings Z and Zn form foundations upon which all rings with unity rest, and that Q and Zp perform a similar service for all fields. Let R be any ring with unity 1. Recall that by n-1 we mean 1+1+….. +1 for n > 0 summands for n > 0, and (-1)+(-

1)+……..+(-1)for |n|summands for n < 0, while n.1 = 0 for n = 0

Theorem: If R is a ring with unity 1, then the map $\phi : Z \to R$ given by

$\phi(n) = n.1$ for $n \in Z$ is a homomorphism of Z into R.

Proof: Observe that

$\phi(n + m) = (n + m).1 = (n.1) + (m.1) = \phi(n) + \phi(m)$

The distributive laws in R show that

$$\underbrace{(1+1+....+1)}_{n\ ....} \underbrace{(1+1+.....+1)}_{m\ .....} = \underbrace{(1+1+...+1)}_{nm\ ....}$$

Thus (n . 1) (m.1) = (nm).1 for n, m > 0. Similar arguments with the distributive laws show that for all n, m∈ Z,we have.(n.1)(m.1) = (nm) .1

Thus$\phi(nm) = (nm).1 = (n.1)(m.1) = \phi(n)\phi(m)$.

Corollary: If R is a ring with unity and characteristic n >1, then *R* contains a subring

isomorphic to Z if *R* has characteristic 0 then *R* contains subring isomorphic to Z.

Proof: The map ϕ: Z $\rightarrow$R given by ϕ (m) =m.1 for m $\in$ Z is a homomorphism. The kernel must be an ideal in Z. All ideals in Z are of the forms sZ for some s$\in$ Z. We see that if R has characteristic n>0, then the kernel ofϕ is nZ. Then the imageϕ{Z}$\leq$R is isomorphic to Z / nZ $\cong$ Z. If the characteristic of R is 0, is then m 1 $\neq$ 0 for all m $\neq$ 0, so the kernel of ϕ is {0}. Thus, the image ϕ[Z] $\leq$ R is isomorphic to Z.

Theorem: A field is either of prime characteristic p and contains a subfield isomorphic to Zp or of characteristic 0 and contains a subfield isomorphic to Q.

Proof: If the characteristic of F is not0,the above corollary shows that F contains a subring isomorphic to Zn. Then *n* must be a prime p or F would have 0 divisors. If F is of characteristic 0 then F must contain a subring isomorphic to Z.

show that F must contain a field of quotients of this subring and that this field of quotients must be isomorphic to Q.

Thus every field contains either a subfield isomorphic to Zp for some prime p or a subfield isomorphic to Q. These fields Zp and Q are the fundamental building blocks on which all fields rest.

Definition: The fields Zp and Q are prime fields.

Ideal Structure in F [x]

Note that for a commutative ring *R* with unity and $a \in R$, the set $\{ra|r \in R\}$ is an ideal in *R* that contains the element a.

Definition: If R is a commutative ring with unity and $a \in R$, the ideal $\{ra|r \in R\}$ of all multiples of a is the principal ideal generated by a and is denoted by<a>.

An ideal *N* of *R* is a principal ideal if *N* = <a>for some $a \in R$.

Example: Every ideal of the ring Z is of form nZ , which is generated by n, so every ideal of Z is a principal ideal.

Example: The ideal <x>in*F[x]* consists of all polynomials in *F[x]*having zero constant term.

The next theorem is another simple but very important application of the division algorithm for $F[x]$.

Theorem: If F is a field, every ideal in *F[x]*is principal.

Proof: Let N be an ideal of *F[x]*. If $N = \{0\}$, then $N = \langle 0 \rangle$, Suppose that $N \neq \{0\}$, and let g(x) be a nonzero element of N of minimal degree. If the degree of g(x) is 0, then $g(x) \in F$and is a unit, so $N = F[x] = \langle 1 \rangle$, so N is principal. If the degree of g (x) is ≥ 1, let*f*(x) be any element of N. Then,

Then $f(x) = g(x)q(x)+r(x)$, where r (x) = 0 or (degree r(x)) < (degree g (x)). Now *f*

(x)∈ N and g (x)∈ N Imply that *f(x)* – g(x)q(x) = r(x) is in N by definition of an ideal. Since g(x) is a nonzero element of minimal degree in *N*, we must haver(x) = 0, Thus*f (x)* = g(x)q(x)and N = ⟨g (x)⟩.

Theorem:

An ideal⟨p(x)⟩≠ {0} is maximal ifand only if p(x) is irreducible over*F*.

Proof : Suppose that ⟨p(x)⟩≠ {0} is a maximal ideal of F[x]. Then⟨p(x)⟩≠*F*[x], so p(x)∉ *F*. Letp(x)= *f*(x) *g*(x) be a factorization of p(x) in *F*[x]. Since⟨p(x)⟩is a maximal ideal and hence also a prime ideal, that implies that *f* (x) ∈⟨p(x)⟩or *g(x)* ∈⟨p (x)⟩; that is, either*f*(x) or *g* (x) has p(x) as a factor. But then we can't have the degrees of both *f* (x) and g(x) less than the degree of p(x), This shows that p(x) is irreducible over F.

Conversely, if p(x) is irreducible over*F,* suppose that N is an ideal such that⟨p(x)⟩⊆

$N \subseteq F[x]$. Now N is a principal ideal,so $N = \langle g(x) \rangle$ for some

$g(x) \in N$. Then $p(x) \in N$ implies that $p(x) = g(x)q(x)$ for some $q(x) \in F[x]$. But p(x) is irreducible, Which implies that either g(x) or q(x) is of degree 0. If g(x) is of degree 0, that is, a nonzero constant in$F$, then g(x) is an unit in $F[x]$,

so$\langle g(x) \rangle = N = F[x]$.If q (x) is of degree 0, then $q(x) = c$, where $c \in F$,and

$g(x) = (1/c)p(x)$ is in $\langle p(x) \rangle$, so $N = \langle p(x) \rangle$. Thus $\langle p(x) \rangle \subset N \subset F[x]$ is impossible, so $\langle p(x) \rangle$ is maximal.

Example: The polynomial $x^3+3x+2$is irreducible in $Z_5[x]$,

so $Z_5[x]/\langle x^3+3x+2 \rangle$is a field,

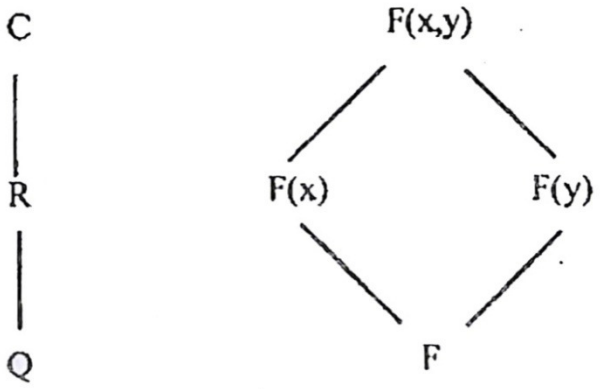
Similarly, we knowx^2-2 is irreducible in Q[x], so $Q[x]/\langle x^2-2 \rangle$ is a field.

INTRODUCTION TO EXTENSION FIELDS

The field of rational numbers lies inside the real numbers. The real numbers lie inside the complex numbers. It is interesting to answer the question whether or not some field F is contained in a larger field. We saw that $Z_2[x]/<x^2+x+1>$ is a field of order 4 whereas $R[x]/<x^2+1>$ is a field isomorphic to the complex numbers. Does there exist finite field of order 10. Following chapters will provide more ideas about both finite and infinite fields.

Definition 1.1: A field E is an extension field of a field F if F $\leq$E ie: F is a subfield of E. The operations of F are those of E restricted to F.

Thus R is an extension field of Q and C is an extension field of both R and Q. This can be represented as a lattice diagram with largest field being on top.



If we are given a field F and a polynomial p(x) $\in F[x]$, we wish to find a field E containing F such that p(x) factors into linear factors over E[x]

For example, consider F = Q and let f(x) = $x^4 - 5x^2 + 6$. This we can write into $(x^2 - 2)$ $(x^2 - 3)$, both are irreducible in Q. Now f(x) = $(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{3})(x-\sqrt{3})$ in R[x]. It is possible to find a smaller field than R in which f(x) has a zero, namely E_1= $Q(\sqrt{2}) = \{a+b\sqrt{2}; a,b \in Q\}$. $Q(\sqrt{2})$ is the smallest field containing both Q and $\sqrt{2}$.But still in this field, we cannot find all zeros of f(x). But if we

extend further and get $E_2 = Q(\sqrt{2}, \sqrt{3}) = \{a+b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\}$ where we can find all roots of f(x). We can find that both $\sqrt{2}$ and $\sqrt{3}$ belongs to E_2.

Note: F(α) is adjoining α to the field F ie: the smallest field containing both F and α.

Theorem 1.2 : Fundamental Theorem of field theory (Kroneeker's Theorem) : Let F be a field and f (x) a nonconstant polynomial in F [x]. Then there is an extension field E of F in which f (x) has a zero.

Proof : We know the fact that f (x) has a factorization in F[x] into polynomials and has a irreducible factor, say p (x), Clearly, it suffices to construct an extension field E of F in which p (x) has a zero. Our candidate for E is F[x] /< p(x)>. Since < p(x)> is a maximal ideal in F [x], so this is a field.

Also, since the mapping $\phi : F \rightarrow E$ given by $\phi(a) = a +<p(x)>$ is one to one and preserves both operations, E has a subfield isomorphic to F. We

may think of E as containing F if we simply identify the coset a + <p(x)> with its unique coset representative a that belongs to F. That is think of a + <p(x)> as just a and vice versa.

Finally, to show that p(x) has a zero in E

Write $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots\ldots\ldots + a_0$

Then, in E $x + p(x)$ is a zero of $p(x)$. For

$P(x + < P(x) >)$

$= a_n(x + < p(x) >)^n + a_{n-1}(x + < p(x) >)^{n-1} + \ldots\ldots\ldots\ldots + a_0$

$=$

$a_n(x^n + < p(x) >) + a_{n-1}(x^{n-1} + < p(x) >) + \ldots\ldots\ldots\ldots + a_0$

$= a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots\ldots + a_0 + < p(x) >$

$= p(x) + < p(x) > = 0 + < p(x) > = 0$

Example 1.3 : Let $f(x) = x^2 - 2 \in Q[x]$. Then, the irreducible factorization of

$f(x)$ over Q is $(x+\sqrt{2})(x-\sqrt{2})$. So to find extension E of Q in which f(x) has a zero, we may take $E = Q[x] / <x^2-2>$, a field isomorphic to $Q(\sqrt{2})$.

Definition 1.4 : An element α of an extension field E over F is algebraic over F if $f(\alpha) = 0$ for

some nonzero polynomial f (x) ∈ F[x]. An element in E that is not algebraic over F is transcendental over F.

Definition 1.5 : An element of C that is algebraic over Q is an algebraic number A transcendental number is an element of C that is transcendental over Q.

Theorem 1.6 : Let E be an extension field of F and $\alpha \in E$. Then α is transcendental over F if and only if F(α) is isomorphic to F(x), the field of fractions of F[x].

Proof : Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism for α. Then α is transcendental over F if and only if ϕ_α(p(x)) = p (α) ≠ 0 for all nonconstant polynomials p(x) ∈ F[x]. This is true if and only if $\ker \phi_\alpha = (0)$ that is, it is true exactly when ϕ_α is one – to – one. Hence E must contain a copy of F[x]. The smallest field containing F[x] is the field of fractions F[x]. Hence E must contain a copy of this field.

Almost all real numbers are transcendental over Q.

The following theorem will give the distinction between elements that are algebraic over a field and elements that are transcendental over a field.

Theorem 1.7 : Let E be an extension field of the field F and let $\alpha \in$ E. If α is transcendental over F, then $F(\alpha) \approx F(x)$. If α is algebraic over F, then $F(\alpha) \approx F(x) \ / \ < p(x) >$, where p(x) is a polynomial in F[x] of minimum degree such that $p(\alpha) = 0$. Moreover p(x) is irreducible over F.

Proof : Proof : Second part of the theorem we already proved. Now we prove first part. Let $\phi_\alpha : F[x] \to$ E be the evaluation homomorphism. The kernel of this map is the minimal polynomial p(x) of α. By the first isomorphism Theorem for rings, the image of ϕ_α, in E is isomorphic to $F(\alpha)$ since it contains both F and α.

Theorem 1.8 : Let E be an extension field of a field F and$\alpha\in$ E with αalgebraic over E. Then there is a unique irreducible monic polynomial p(x)$\in F[x]$ of smallest degree such that $p(\alpha) = 0.$ If f(x) is another monic polynomial in F[x] such that $f(\alpha)=0,$ then p(x) divided f(x).

The unique monic polynomial p(x) of this theorem is called the irreducible polynomial for αover F denoted by irr (α, F) The degree of p(x) is the degree of αover F, is denoted by deg(α, F) .

Proof : Let ϕ_α: F [x] $\rightarrow$ E be the evaluation homomorphism. The kernel of ϕ_α is a principal ideal generated by some p(x) $\in F[x]$ with deg $p(x) \geq 1$. We know that such a polynomial exists. Since F[x] is a principal ideal domain and α is algebraic. The ideal < p (x) >consists exactly of those elements of F[x] having α as a zero. If f(α) = 0and f(x) is not the zero polynomial, then f(x) $\in <p\,(x)>$ and p(x) divides f(x). So p(x) is a polynomial of minimal degree having α as a zero.

Any other polynomial of the same degree having αas a zero must have the form β p(x) for some $\beta \in F$.

Suppose now that p(x) = r(x)s(x) is a factorization of p(x) into polynomials of lower degree. Since $p(\alpha) = 0 \Rightarrow r(\alpha)\ s(\alpha) = 0$: consequently, either $r(\alpha) = 0\ or\ s(\alpha) = 0$: which contradicts that p(x) is of minimal degree. Therefore p(x) must be irreducible.

Example 1.9 : Let f(x) =x^2-2 and g(x)=x^2-3 These polynomials are the irreducible polynomials of $\sqrt{2}$ and $\sqrt{3}$ respectively.$\sqrt{2} \in$ R is algebraic of degree 2 over Q but algebraic of degree 1 over R, for irr ($\sqrt{2}$, R) = x - $\sqrt{2}$

Definition 1.10 : An extension field E of a field F is simple extension of F if E = F (α) for some $\alpha \in$ E.

Theorem 1.11 : Let E = F(α) be a simple extension of F, where $\alpha \in$ E is algebraic over F.

Suppose that the degree of irr(α, F) is n. Then every element $\beta \in E.$ can be expressed uniquely in the form.

$$\beta = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} \; for \; b_i \in F$$

Proof : Since $\phi_\alpha \; (F[x]) = F[\alpha] = F(\alpha)$, every element in E = F (α) must be of the form $\phi_\alpha (f(x)) = f(\alpha)$ where f(α) is a polynomial in α with coefficients in F.

Let p(x) = $x^n + a_{n-1}x^{n-1} + ... + a_0$ be the minimal polynomial ofα. Then p(α) =0;hence,

$$\alpha^n = -a_{n-1}\alpha^{n-1} - ..... - a_0$$

Similarly,

$$\begin{aligned} \alpha^{n+1} &= \alpha\alpha^n \\ &= -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - ... - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} .... - a_0) - a_{n-2}\alpha^{n-1} - ... - a_0\alpha \\ &= -a_{n-2}\alpha^{n-1} - ... - a_0\alpha \end{aligned}$$

Continuing in this manner, we can express every monomialα^m, $m \geq n$ as a linear combination of powers of α that are less than n.

Hence, any $\beta \in F(\alpha)$ can be written as

$$\beta = b_0 + b_1\alpha + \ldots\ldots\ldots\ldots\ldots + b_{n-1}\alpha^{n-1}$$

To show uniqueness, suppose that

$$\beta = b_0 + b_1\alpha + \ldots\ldots\ldots\ldots + b_{n-1}\alpha^{n-1} = c_n + c_1\alpha + \ldots\ldots + c_{n-1}\alpha^{n-1}$$

for b_i and c_i in F

Then

g(x)=

$(b_0 - c_0) + (b_1 - c_1)x + \ldots\ldots\ldots + (b_{n-1} - c_{n-1})x^{n-1}$ is in F[x] and g(α) = 0. Since the degree of g(x) is less than the degree of p(x), the irreducible polynomial of α, g(x) must be the zero polynomial. Consequently.

$$b_0 - c_0 = b_1 - c_1 = \ldots\ldots\ldots = b_{n-1} - c_{n-1} = 0 \; or \; b_i = c_i \; for \; i = 0, 1, \ldots\ldots, n-1$$

Examples 1.12

(i) Since $x^2 + 1$ is irreducible over R, $\langle x^2 + 1 \rangle$ is a maximal ideal in R[x]. So E = R[x] / $\langle x^2 + 1 \rangle$ is a field extension of R that contains a root of $x^2 + 1$.

Let = x + $<x^2 + 1>$We can identify E with the complex numbers. We know E is isomorphic to R $(\alpha) = \{a + b\alpha : a, b \in R\}$. We know that $\alpha^2 = -1$

Since $\alpha^2 + 1 = (x + <x^2 + 1>)^2 + (1 + <x^2 + 1>)$

$= x^2 + 1 + <x^2 + 1> = 0$

Hence, we have an isomorphism of R(α)with C defined by the map that takes a + bαto a + bi

(ii) The polynomial $p(x) = x^2 + x + 1$ in $Z_2[x]$ is irreducible over Z_2 since neither element 0 nor element 1 of Z_2 is a root of p(x). We know that there is an extension field E of Z_2 containing a zero α of $x^2 + x + 1$.

Let it be denoted by $Z_2(\alpha)$. $Z_2(\alpha)$ has as elements $0 + 0\alpha$, $1 + 0\alpha$, $0 + 1\alpha$and

$1 + 1\alpha$(that is$1 + \alpha$). This gives a finite field of four elements.

ALGEBRAIC EXTENSIONS:

Let E be a field extension of a field F. If we regard E as a vector space over F, then we can use

linear algebra to solve the problems that we will encounter inour study of fields. The elements in the field E are vectors, the elements in the field F are scalars. We can think of addition in E as adding vectors. When we multiply an element in E by an element of F, we are multiplying a vector by a scalar. We can consider E = F(α) in a finite dimensional vector space over F with basis {1,α, α^2……. α^{n-1}}

If an extension field E of a field F is a finite dimensional vector space over F of dimension n, then we say that E is a finite extension of degree n over F. We write [E : F] = n.

Theorem 1.13 : Every finite extension field E of a field F is an algebraic extension.

Proof : Let α∈ E since [E : F] = n the elements 1,α,……,α^n cannot be linearly independent. Hence there exist a∈ F, not all zero such that

$$a_n \alpha^n + \ldots\ldots\ldots\ldots + a_1\alpha + a_0 = 0$$

Therefore,

P(x) = $a_n x^n + \ldots\ldots\ldots\ldots + a_1 x + a_0 \in$ F [x] is a nonzero polynomial with $p(\alpha) = 0$

The converse is not true, for otherwise, the degrees of the elements of every algebraic extension of E over F would be bounded. But Q($\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}$ …) is an algebraic extension of Q that contains elements of finite degree over Q.

Next Theorem is also called the Tower Law.

Theorem 1.14 : Let K be a finite extension field of the field E and let E be a finite extension field of the field F. Then K is a finite extension field of F and

[K : F] = [K : E] [E : F]

Proof : Let X = $(x_1, x_2, \ldots x_n)$ be a basis for K over E and let Y= $(y_1, y_2, \ldots y_m)$ be a basis for E over F. It suffices to prove that

$YX = \{y_j x_i / 1 \le j \le m, 1 \le i \le n\}$ is a basis for K over F.

To do this let a $\in$ K. Then there are elements $b_1, b_2, \ldots\ldots b_n \in$ E such that

$$a = b_1 x_1 + b_2 x_2 + \ldots + b_n x_n$$

And for each i = 1. 2...n, there are elements $c_{11}, c_{12}, c_{13} \ldots \in$ F such that

$b_1 = c_{i1} y_1 + c_{i2} y_2 + \ldots\ldots\ldots + c_{im} y_m$ Thus,

$$a = \sum_{i=1}^{n} b_i x_i = \sum_{i-1}^{n} (\sum_{j=1}^{m} C_{i,} y_j)\ x_i = \sum_{i.j} C_{ij} (y_j\ x_i)$$

This proves that YX spans K over F.

Now, suppose there are elements c_{ij} in F such that

$$0 = \sum_{i.j} c_{ij} (y_j\, x_i) = \sum_{i} \sum_{j} (c_{ij} y_j)\, x_i$$

Then since each $c_{ij} y_j \in$ E and X is a basis for K over F, we have

$\sum_{i} c_{ij} y_j = 0$ for each i.

But each $c_j \in$ F and Y is a basis for E over F, so each c_{ij}=0. This proves that the set YX is linearly independent over F.

Corollary 1.15 : If F_i is a field for i = 1, … k and F_{i+1} is a finite extension of F_i then F_k is a finite extension of F_1 and

$[F_k : F_1] = [F_k : F_{k-1}]$ …….$[F_2 : F_1]$

Theorem 1.16 : Let E be an extension field of F. If $\alpha \in E$ is algebraic over F with minimal polynomial p(x) and $\beta \in F(\alpha)$ with minimal polynomial q(x),

then deg q(x) divides deg p(x).

Proof: We know that deg p(x) = $[F(\alpha) : F]$ and deg q(x) = $[F(\beta) : F]$

Since $F \leq F(\beta) \leq F(\alpha)$

$[F(\alpha) : F] = [F(\alpha) : F(\beta)]\,[F(\beta) : F]$

Theorem 1.17 : Let E be a field extension of F. Then the following statements are equivalent.

1. E is a finite extension of F
2. There exists a finite numbers of algebraic elements $\alpha_1, \alpha_2, \ldots\ldots \alpha_n \in E$

such that E = F ($\alpha_1, \ldots, \alpha_n$).

3. There exists a sequence of fields

$E = F(\alpha_1 \ldots\ldots \alpha_n) \supset F(\alpha_1 \ldots\ldots\ldots\ldots\ldots\ldots \alpha_{n-1})$

$\supset \ldots\ldots\ldots \supset F(\alpha_1) \supset F$

where each field $F(\alpha_1 .....\alpha_i)$ is algebraic over $F(\alpha_1 .....\alpha_{i-1})$

Proof: (1) $\Rightarrow$(2) Let E be a finite algebraic extension of F. Then E is a finite dimensional vector space over F and there exists a basis consisting of elements $\alpha_1 .....\alpha_n$ in E such that $E = F(\alpha_1 .....\alpha_n)$. Each α_1 is algebraic over F by Theorem 1.13

(2) $\Rightarrow$(3) Suppose that $E = F((\alpha_1 .....\alpha_n)$ where every α_i is algebraic over F. Then

$$E = F(\alpha_1 .....\alpha_n) \supset F(\alpha_1 .....\alpha_{n-1}) \supset .....F(\alpha_1) \supset F$$

Where each field $F(\alpha_1 .....\alpha_l)$ is algebraic over $F(\alpha_1 .....\alpha_{l-1})$

(3) $\Rightarrow$(1) Let $E = F(\alpha_1 .....\alpha_n) \supset F(\alpha_1 .....\alpha_{n-1}) \supset .....F(\alpha_1) \supset F.$

where each field $F(\alpha_1 .....\alpha_i)$ is algebraic over $F(\alpha_1 .....\alpha_{i-1})$

Since F $(\alpha_1 .....\alpha_i) = F(\alpha_1 .....\alpha_{i-1})(\alpha_i)$ is simple extension and α_i is algebraic over F $(\alpha_1 .....\alpha_{i-1})$ it follows that

[F $(\alpha_1 .....\alpha_i) : F(\alpha_1 .....\alpha_{i-1})$]is finite for each i.

Therefore, [E : F] if finite

Example 1:18

1. Since{1,√3} is a basis for Q(√3, √5) over Q(√5) and {1,√5} is a basis for Q(√5) over Q, the proof of Theorem 1.14 shows that {1. √3, √5, √15} is a basis for Q(√3,√5) over Q.

2. Consider Q ($\sqrt[3]{2}, \sqrt[2]{3}$). Then

[Q ($\sqrt[3]{2}, \sqrt[2]{3}$):Q] = 6. We have.

[Q ($\sqrt[3]{2}, \sqrt[2]{3}$):Q] = [Q ($\sqrt[3]{2}, \sqrt[2]{3}$): Q $\sqrt[3]{2}$]. $[Q\sqrt[3]{2} : Q]$=3.2=6.

The polynomials are x^3-2 over Q and $x^2 - 3$ over $(Q\sqrt[3]{2})$

3. If $f(x) = 15x^4 - 10x^2 = 9x + 21$ is irreducible over Q. Let β be a zero of f(x) in some extension of Q. Then, even though we don't know what β is, we can still prove that $\sqrt[3]{2}$ is not an element of $Q(\beta)$.

For, if so then

$$Q < Q(\sqrt[3]{2}) \leq Q(\beta) \text{ and}$$
$$4 = [Q(\beta) : Q] = [Q(\beta) : Q(\sqrt[3]{2})]\ Q(\sqrt[3]{2} : Q]$$

implies that 3 divides 4.

Note that this argument cannot be used to show that $\sqrt{2}$ is not contained in $Q(\beta)$.

4.Consider $Q(\sqrt{3}, \sqrt{2})$. we prove that

$Q(\sqrt{3}, \sqrt{2}) = Q(\sqrt{3} + \sqrt{2})$

The inclusion of $Q(\sqrt{3} + \sqrt{2}) \leq Q(\sqrt{3}, \sqrt{2})$ is clear

Now note that, since

$(\sqrt{3} + \sqrt{2})^3 = 15\sqrt{3} + 11\sqrt{2} = 11(\sqrt{3} + \sqrt{2}) + 4\sqrt{3}$ and

$(\sqrt{3} + \sqrt{2})^3$ and $11(\sqrt{3} + \sqrt{2})$ both belong to Q ($\sqrt{3}$ + $\sqrt{2}$) so does their difference $4\sqrt{3}$ Therefore

¼ $(4\sqrt{3}) = \sqrt{3} \in Q(\sqrt{3} + \sqrt{2})$ of course

$\sqrt{2} = (\sqrt{3} + \sqrt{2}) - \sqrt{3} \in Q(\sqrt{3} + \sqrt{2})$ as well

Thus $Q(\sqrt{3}, \sqrt{2}) \leq Q(\sqrt{3} + \sqrt{2})$

Let us determine an extension field of Q containing $\sqrt{3} + \sqrt{2}$. It is easy to determine that the irreducible polynomial of $\sqrt{3} + \sqrt{2}$ is

$x^4 - 2x^2 - 7$. It follows that

$[Q(\sqrt{3} + \sqrt{2}) : Q] = 4$

We know that $\{1, \sqrt{3}\}$ is a basis for $Q(\sqrt{3})$ over Q. Hence $\sqrt{3} + \sqrt{2}$ cannot be in $Q(\sqrt{3})$. It follows that $\sqrt{2}$ cannot be in $Q(\sqrt{3})$,Therefore

$\{1, \sqrt{2}\}$ is a basis for

Q ($\sqrt{3}$, $\sqrt{2}$) = (Q($\sqrt{3}$)) ($\sqrt{2}$) over Q ($\sqrt{3}$) and

{1, $\sqrt{3}$, $\sqrt{2}$, $\sqrt{6}$} is a basis for

Q($\sqrt{3}$, $\sqrt{2}$) = Q ($\sqrt{3}$ + $\sqrt{2}$) over Q.

5. Compute a basis for Q ($\sqrt[3]{5}$,$\sqrt{5}$i)

We know that $\sqrt{5}$i does not belongs to Q ($\sqrt[3]{5}$), so[$Q(\sqrt[3]{5},\sqrt{5}i):Q(\sqrt[3]{5})]=2$

{1, $\sqrt{5}$i} is a basis for $Q(\sqrt[3]{5},\sqrt{5}i)$ over $Q(\sqrt[3]{5})$

We also know that {1, $\sqrt[3]{5},(\sqrt[3]{5})^2$ } is a basis for $Q(\sqrt[3]{5})$ over Q.

Hence, a basis for Q ($\sqrt{5},\sqrt[3]{5}$) over Q is $\{1,\sqrt{5}i,\sqrt[3]{5},\left(\sqrt[3]{5}\right)^2,(\sqrt[6]{5})^5 i,\left(\sqrt[6]{5}\right)^7 i=5\sqrt[6]{5}j or \sqrt[6]{5}i\}$

Note that $\sqrt[6]{5}$i is a zero of x^6+5. We can show that this polynomial is irreducible over Q using Eisenstein's criterion, where we let p=5. Consequently,

$$Q<Q(\sqrt[3]{5})<Q(\sqrt[3]{5},\sqrt{5}i).$$

But it must be the case that

$Q(\sqrt[6]{5}i)=Q(\sqrt[3]{5},\sqrt{5}i)$since the degree of both of these extensions is 6.

Theorem 1.19 : Let E be an extension field of F. The set of elements in E that are algebraic over F form a field.

Proof : Let $\alpha,\beta\in E$ be algebraic over F. Then F (α,β) is a finite extension of E Since every element of F(α,β) is algebraic over F, $\alpha\pm\beta,\alpha\beta$ and $\alpha/\beta(\beta\neq 0)$ are all algebraic over F. Hence the set of elements in E that are algebraic over F forms a field.

Definition 1.20 : Let E be a field extension of a field F. We define the algebraic closure of a field F in E to be the field consisting of all elements in E that are algebraic over F. A field F is algebraically closed if every nonconstant polynomial in F[x] has a zero in F.

Theorem 1.21 :A field F is algebraically closed if and only if every nonconstant polynomial in F[x] factors into linear factors over F[x].

Proof : Let F be an algebraically closed field. If p(x) $\in$ F[x] is a nonconstant polynomial then p(x) has a zero in F, say α . Therefore $x-\alpha$ must be a factor of p(x) and so p(x) $=(x-\alpha)\ q_1(x)$, where deg $q_1(x)$ = deg (p(x)) – 1. Continue this process with $q_1(x)$ to find a factorization.

$$P(x) = (x-\alpha)\,(x-\beta)\,q_2(x),$$

where deg $q_2(x)$ = deg (p(x)) - 2. The process must eventually stop since the degree of p(x) is finite.

Conversely, suppose that every nonconstant polynomial p(x) in F[x] factors into linear factors. Let ax – b be such a factor. Then (b / a) is a zero of p(x). consequently, F is algebraically closed.

Corollary1.22: An algebraically closed field F has no proper algebraic extension E.

Proof : Let E be an algebraic extension of F then $F \leq E$. For $\alpha \in E$. the irreducible polynomial of α is $x - \alpha$. Therefore $\alpha \in$ F and F = E.

Note : Every field F has a unique algebraic closure.

Example 1.23

1.Suppose that E is an extension of F and a, b $\in$ E. If a is algebraic over F of degree m, and b is a algebraic over F of degree n, where m and n are relatively prime, show that [F(a, b) : F] = mn

Proof : We have [F(a, b) : F] is divisible by both m = [F(a):F] and n = [F(b) : F]

2. Let E be a finite extension on R. Use the fact that C is algebraically closed to prove that E = C or E = R

Proof : E must be an algebraic extension of R so that E $\leq$ C. But then

$$[C : E] [E : R] = [C : R] = 2$$

Hence either [C : E] or [E : R] must be equal to 1.

3.Suppose that p(x) $\in$ F [x] and E is a finite extension of F. If p(x) is irreducible over F and deg p(x) and [E : F] are relatively prime, show that p(x) is irreducible ever E.

Proof : Let a be a zero of p(x) in some extension of F. First note that

[E(a) : E] $\leq$ [F(a) : F] = deg p(x). Also we have

[E(a) : F(a)] [F(a) : F] = [E(a) : E] [E:F] This implies deg p(x) divides [E(a) : E] so that deg p(x) = [E(a) : E]

4. If α and β are transcendental over Q, show that either $\alpha\ \beta$ or a $\alpha + \beta$ is also transcendental over Q.

Proof : If $\alpha + \beta$ and $\alpha\beta$ are algebraic then so is $\sqrt{[(\alpha+\beta)^2 - 4\alpha\beta]}$ that is α - β is also algebraic. It leads to say that α and β are algebraic.

RULER AND COMPASS CONSTRUCTIONS

We can prove the impossibility of performing a number of geometricconstruction in a finite number of steps using straight edge and compass alone. A straight edge is not a ruler. We cannot measure arbitrary lengths with a straight edge. It is merely a tool for drawing a line through two points. Those impossible construction include the following.

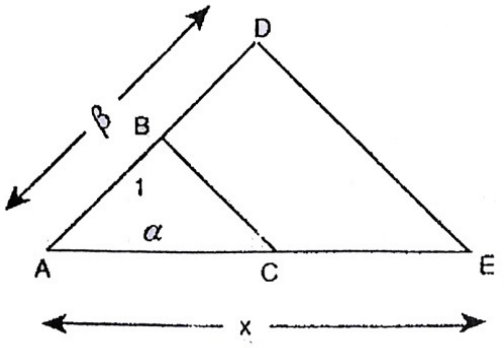
- the trisection of an arbitrary angle
- the construction of the edge of a cube having twice the volume of some given cube
- the construction of square having the same area as a given circle

Definition 2.1 : A real number α is constructible if one can construct line segment of length $|\alpha|$ in a

finite number of steps from this segment of unit length by using a straightedge and a compass.

Theorem 2.3 : The set of all constructible real numbers forms a subfield F of the field of real numbers.

Proof :

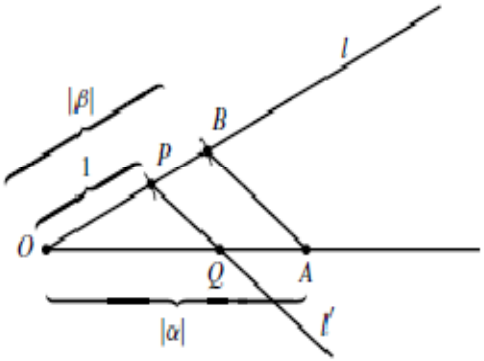


Let α and β be the constructible numbers. We must show that $\alpha+\beta,\ \alpha-\beta, \alpha\beta, and \frac{\alpha}{\beta}\ (\beta \neq 0)$ are also constructible numbers. We can assume that both α and β are positive with $\alpha > \beta$. It is quite obvious how to construct and $\alpha+\beta$ and $\alpha-\beta$.

To find a line segment with length $\alpha\beta$, we

assume that $\beta > 1$ and construct the triangle in figure such that triangles ΔABC and ΔADE are similar.

Since $\frac{\alpha}{1} = \frac{x}{\beta}$ the line segment x has length $\alpha\,\beta$.



Construct the triangle ΔOPQ andΔOAB,they are similar then $\frac{OQ}{1} = \frac{\alpha}{\beta}$ .So OQ has length$\frac{\alpha}{\beta}$and $\frac{\alpha}{\beta}$is constructible.

Theorem 2.4: If αis a constructible number, then √αis a constructible number. **Proof :** In the earlier

figure, the triangles ΔABD, ΔBCD and ΔABC are similar, hence.

$$\frac{1}{x} = \frac{x}{\beta} \text{ or } x^2 = \alpha$$

Theorem 2.5 : The field F of constructible real numbers consists precisely of all real numbers that we can obtain from Q by taking square roots of positive numbers a finite number of times and applying a finite number of field operations.

Proof : Since Q is the smallest subfield of R, the field F of all constructible real numbers contain Q. Regarding a given segment [0,1] of length 1 as the basic unit on the X-axis, any point (q_1, q_2) in the plane that we can locate by using a compass and a straightedge can be found in one of the following three ways.

1.as an intersection of two lines, each of which passes through two known points having rational coefficients.

2. as in intersection of a line that passes through two points having rational co-ordinates and a circle whose centre has rational co-ordinates and the square of whose radius is rational.

3. as an intersection of two circles whose centers have rational co-ordinates and the squares of whose radii are rational.

A simultaneous solution of two linear equations with rational coefficients can only lead to rational values of x and y, giving us no new points. However, finding a simultaneous solution of a linear equation with rational coefficients and a quadratic equation with rational coefficients, as in case 2, leads upon, substitution, to a quadratic equation. Such an equation, when solved by the quadratic formula, may have solution involving square roots of numbers that are not squares in Q.

If H is the smallest field containing those new real numbers constructed so far, the argument

shows that the next new number constructed lies in a field H($\sqrt{\alpha}$) for some $\alpha \in$ H where $\alpha >$ 0.

We already proved that if α isconstructible then $\sqrt{\alpha}$ is also constructible. **Corollary 2.6 :** If γ is constructible and $\gamma \notin$ Q, then there is a finite sequence of real numbers $\alpha_1\ \alpha_{2,} \ldots\ldots \alpha_n = \gamma$ such that $Q(\alpha_1, \alpha_{2,} \ldots\ldots, \alpha_i)$ is an extension of Q ($\alpha_{1,} \alpha_2, \ldots\ldots\ldots, \alpha_{i-1}$)of degree 2. In particular, [Q (γ) : Q] = 2^r for some integer $r \geq 0$.

Proof : The existence of the α_i follows from earlier theorem. Then

2^n = [Q ($(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$: Q]

= [Q ($\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$) : Q (γ)] [Q (γ) :Q]

by Tower law.

Hence [Q (γ) : Q] = 2^r for some integer $r \geq 0$.

Theorem 2.7 : Doubling the cube is impossible : Let the given cube have a side of length 1, and hence a volume of 1. The cube being sought

would have to have a volume of 2, and hence a side of length $\sqrt[3]{2}$. *But* $\sqrt[3]{2}$ is a zero of irreducible $x^3 - 2$ over Q. i.e.,

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

But for the possible construction, by Corollary 2.6, we should have $3 = 2^r$ for some r, which is impossible.

Squaring the circle is impossible : Let the given circle have a radius of 1, and hence an area of π. We would need to construct a square of side $\sqrt{\pi}$. But π is transcendental over Q, so $\sqrt{\pi}$ is transcendental over Q also.

Trisecting the angle is impossible: That is, there exists an angle that cannot be trisected with a straightedge and a compass.

We will show that the angle 60^0 is constructible but cannot be trisected. We know the angle θ can be constructed if an only if $|\cos\theta|$can be constructed.

$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

Let $\theta = 20^0$ Let $\alpha = \cos 20$

Hence ½ =

$4\alpha^3 - 3\alpha$ *i.e., a zero of* $8x^3 - 6x - 1$

Now $8x^3 - 6x - 1 = f(2x - 1)$, where $f(x) = x^3 + 3x^2 - 3$

An immediate application of Eisenstein's criterion for irreducibility shows that the polynomial f is irreducible over Q, and thus.

$[Q(\alpha) : Q] = 3$. It follows that angle of 60 cannot be trisected.

FINITE FIELDS

Theorem 3.1 : Let E be a finite extension of degree n over a finite filed F. If F has q elements, then E has q^n elements.

Proof : Let $\{\alpha_1, ..., \alpha_n\}$ be a basis for E as a vector space over F. Then every $\beta \in E$ can be uniquely written in the from

$\beta = b_1\alpha_1 + ... + b_n \alpha_n$ for $b_i \in F$. Since each b_i may be any of the q elements of F, the total number of such distinct linear combinations of the α_i *is* q^n.

Theorem 3.2 : If E is finite field of characteristic p, then E contains exactly p^n elements for some positive integer n.

Proof : Every finite field E is a finite extension of a prime field isomorphic to the field Z_p, where p is the characteristic of E. Now Z_p contains p elements. So by Theorem 3.1, the result follows.

Theorem 3.3 : Let E be a field of p^n elements contained in an algebraic closure $\bar{z}_p$ of Z_p. The elements of E are precisely the zeros in $\overline{z_p}$ of the polynomial

$$x^{p^n} - x \ \ in \ Z_p \ [x]$$

Proof : The set E of non zero elements of E form a multiplicative group of order $p^n - 1$. *Let* $a \in E^n$ Then order of a divides $p^n - 1$. For every $\alpha \in E$ we have

$\propto^{p^n-1} = 1$ i.e.,$\propto^{p^n} = \propto$ every element of E is a root of $x^{p^n} - x = 0$.

i.e, every element in E is zero of $x^{p^n} - x$. *Since* $x^{p^n} - x$ can have almost p^n zeros, we can see that E contains precisely the zeros of $x^{p^n} - x$ in $\overline{Z_P}$.

Definition 3.4 : An element α of a field is an n^{th} root of unity if $\alpha^n = 1$. It is a primitive n^{th} root of unity if $\alpha^n = 1$ *but* $\alpha^m \neq 1$ for $0 < m < n$.

Example : Consider Z_{11}, 2 is a primitive root of unity.

Theorem 3.5 : The multiplicative group of nonzero elements of a finite field is cyclic.

Theorem 3.6 :A finite extension E of a finite field F is a simple extension of F. **Proof :** By Theorem 3.5, E^* is cyclic. Let α be a generator. Then E = F (α)

Lemma 3.7 : If F is finite field of characteristic p with algebraic closure $\overline{F}$ then $x^{p^n} - x$ has p^n distinct zeros of $\overline{F}$.

Proof : We show that $x^{p^n} - x$ has no zeros of multiplicity greater than 1 in $\overline{F}$. Now 0 is a zero of $x^{p^n} - x$ of multiplicity 1.

Suppose $\alpha \neq 0$ is a zero of $x^{p^n} - x$, and hence is a zero of f (x) = $x^{p^{n-1}} - 1$.

Then x-α is a factor of f (x) in $\overline{F}$ [x].

We have

$$\frac{f(x)}{(x-\alpha} = g(x) = x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \ldots\ldots + \alpha^{p^n-4} + \ldots\ldots + \alpha^{p^n-3} x + \alpha^{p^n-2}$$

Now g(x) has $p^n - 1$ summands and in $g(\alpha)$, each summand is

$$\alpha^{p^n-2} = \alpha^{p^n-1} / \alpha = 1/\alpha$$

Thus g (α) = $(p^n - 1)\ (1/\alpha) = -(1/\alpha)[\ p^n \equiv 0 \pmod{p}\ ]$

Therefore g $(\alpha) \neq 0$, so α is zero of f (x) of multiplicity 1.

Theorem 3.8 : A finite GF (p^n) of p^n elements exists for every prime power p^n. This field is called Galois field of order p^n.

Proof : Let $\overline{Z_p}$ be an algebraic closure of Z_p and let K be the subset of $\overline{Z_p}$ consisting of all zeros of $x^{p^n} - x$ in $\overline{Z_p}$.

Then for $\alpha, \beta \in K$, the equations

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

$(\alpha\beta)^{P^n} = \alpha^{P^n}\ \beta^{P^n} = \alpha\beta$

This shows that K is closed under addition, subtraction, and multiplication Now 0 and 1 are

zeros of $x^{P^n} - x$, For $\alpha \neq 0, \alpha^{P^n} = \alpha$ implies that$(1/a)^{p^n} = (1/a)$

Thus K is subfield of $\overline{Z_p}$ containing p^n elements .Therefore, K is the desired field of p^n elements since we proved that $x^{p^n} - x$ has p^n distinct zeros in $\overline{Z_p}$.

Corollary 3.9 : If F is any finite field, then for every positive integer n, there is an irreducible polynomial in F[x] of degree n.

Proof : Let F have q = p^r elements, where p is the characteristic of F, Then by earlier theorem, there is a field $K \leq \overline{F}$ containing Z_p (upto isomorphism) and consisting precisely of the zeros of $x^{P^{nr}} - x$, Every element of F is a zero of $x^{P^n} - x$, by Theorem 3.3. Now $p^{rs} = P^r P^{r(s-1)}$. Applying this equation repeated to the exponents and using the fact that for $\alpha \in F$ we have

$\alpha^{p^r} = \alpha$. We see that for $\alpha \in F$,

$\alpha^{p^{rn}} = \alpha^{p^r (n-1)} = \ldots\ldots\ldots\ldots = \alpha^{p^r} = \alpha$

Thus F $\leq K$. Then Theorem 3.1 shows that we must have [K : F] = n. We have seen that K is simple over F by Theorem 3.5. So K = F (β) for some $\beta \in K$. Therefore, irr (β, F) must be degree n.

Examples 3.10

1.Let $\overline{Z_2}$ be an algebraic closure of Z_2, and let $\alpha, \beta \in \overline{Z_2}$ be zeroes of $x^3 + x^2 + 1$ and $x^3 + x + 1$ respectively. Show that $Z_2(\alpha) \cong Z_2(\beta)$

Answer : We have

irr $(\alpha, Z_2) = 3$, deg $(\alpha, Z_2) = 3$

Therefore $Z_2(\alpha)$ contains $2^3 = 8$ elements

Similarly $Z_2(\beta)$ contains 8 elements.

By Theorem 3.3, $Z_2(\alpha)$ is isomorphic to the splitting field of $x^8 - x$ over Z_2 Similarly $Z_1(\beta)$ also

Therefore $Z_2(\alpha) \cong Z_2(\beta)$

2.Show that every irreducible polynomial in $Z_p[x]$ is divisor of $x^{p^n} - x$ for some n.

Answer : Let f (x) $\in Z_p[x]$ be an irreducible polynomial of degree d overZ_p Then by Kronecker's theorem there is one element a in an extension field of Z_p such that f $(a) = 0$.

Then $[Z_p(a) : Z_p] = \deg \text{irr}(a, Z_p) = d$

$\therefore Z_p(a)$ contains p^d elements.

$\therefore a \in Z_P(a)$ gives $a^{p^d} = a$

i.e., a is a zero of $x^{p^d} - x$

i.e. f (x) divides $x^{p^d} - x$

3. Show that a finite field of p^n elements has exactly one subfield of p^n elements for each divisor m of n.

Answer : First we prove that for every divisor m of n, the field F with p^n elements has a subfield of p^m elements.

First we show that $X^m - 1$ divides x^n-1 over a field F iff m divides n.

Let n = k m + r, $0 \le r < m$, Then

$$x^n - 1 = x^n \left(\sum_{1=0}^{k-1} x^{im}\right)(x^m - 1) + x^r - 1$$

Therefore, $x^m - 1$ divides $x^n - 1$ iff $x^r - 1$

Also $x^r - 1 = 0$ iff r = 0

Hence $x^m - 1$ divides $x^n - 1 \Leftrightarrow$ m divides n.

From this it follows that $x^{p^m} - x$ divides $x^{p^n} - x$ if m divides n

Let f(x) = $x^{p^n} - x$ and g (x) = $x^{p^n} - x$

Since m divides n, f (x) is divisible by g (x).

Let F^1 be the set of all zeros of g (x) in F. Then F^1 is a subfield of F. Since g (x) has p^m distinct zeros, F^1 is a subfield of F with p^m elements.

If K is any other subfield of F which containing p^m elements then K and F^1 are isomorphic. Therefore upto isomorphism, there is exactly one subfield of F with p^m elements.

4. Let F be a finite field of p^n elements containing the prime subfield $Z_{p.}$ Show that if $\alpha \in F$ is generator of the cyclic group<F, **>** of non zero elements of F, then deg $(\alpha, Z_p) = n$

Answer : Since F contains p^n elements. [F : Z_p] = n. Also, since a is a generator of the multiplicative group <F^*,.>, we have F=$Z_p(\alpha)$. Hence

{ $1, \alpha, \alpha^2, ..., \alpha^n$ } cannot be linearly independent over Z_p. Therefore there are n elements a_0 $.....a_{n-1}$ in Z_p such that $a_0 + a_1\alpha + ...+ ....a_{n-1}\alpha^{n-1} + \alpha^n = 0$, where not all a_i equal to zero. Hence deg $(\alpha, Z_p) = n$

5. Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $Z_p[x]$ of a degree d dividing n.

Answer : Let be divisor of n and let p (x) be a monic irreducible polynomial d over Z_p $(=F_p)$. Then the splitting field of p (x) is F^{p^d}. Since d is divisor of in.

$$F^{p^d} \leq F^{p^n}$$

F^{p^n} is the splitting field of $x^{p^n} - x$ over Z_p and every zero of $x^{p^n} - x$ is of multiplicity one in F^{p^n}

Hence every zero of p(x) is a zero of $x^{p^n} - x$

$\Rightarrow p(x)$ divides $x^{p^n} - x$

$\Rightarrow x^{p^n} - x$ is the product of monic irreducible polynomials whose degree is a divisor of n

6. Show that two finite fields of the same order p^n are isomorphic

Answer : Let F a finite field of order p^n. Then F can be considered as a finite extension of Z_p and [F : Z_P] = n. The non zero elements of F form a cyclic group under multiplication. Let α be generation of it. Then F = $Z_p(\alpha)$. Therefore the set $\{1, \alpha, \alpha^2, ... \alpha^{n-1}\}$ from a basis for F over Z_p.

i.e., F = $\{ a_0 + a_1\alpha + ...+ a_{n-1}\alpha^{n-1} / a_i \in Zp \}$

Let p(x) be an irreducible polynomial of degree n over Z_p

Then Z_p [x] / <p(x) >is a field.

and Z_p [x] / < [$a_0 + a_1$ x + …….. + a_{n-1} x^{n-1} /$a_i \in Z_p$]>

Define $\phi: F \rightarrow \frac{Z_p[X]}{< p(x) >}$ *by*

$\phi(a_0 + a_1\alpha + \ldots\ldots + a_{n-1}a^{n-1}) = a_0 + a_1 x + \ldots\ldots + a_{n-1} x^{n-1}$

Then ϕ is an isomorphism of F with $\frac{Z_p[x]}{< p(x) >}$

Hence any finite field with

P^n elements is isomorphic with $\frac{Z_p[x]}{< p(x) >}$

Hence two finite field of p^n elements are isomorphic.

AUTOMORPHISMS OF FIELDS

Definition 4.1. An isomorphism of a field onto itself is an automorphism of the field.

Lemma 4.2. The set of all automorphism of a field E is a group under composition of function.

Proof : If σ and τ are automorphism of E, then so are $\sigma\tau$ and σ^{-1} . The identity is certainly an automorphism, hence, the set of all automorphisms of a field F is a group.

Definition 4.3. If σ is an isomorphism of a field E onto some field, then an element a of E is left fixed by σ, if $\sigma(a) = a$. A collection S of isomorphisms of E leaves a subfield F of E fixed if each $a \in F$ is left fixed by every $\sigma \in S$. If $\{\sigma\}$ leaves F fixed, then σ leaves F fixed.

Example : Consider the fields

$Q \subset Q(\sqrt{5}) \subset Q(\sqrt{3}, \sqrt{5})$. Then for $a, b \in Q(\sqrt{5})$

σ (a + b√3) = a - b√3is an automorphism of Q (√3, √5)leaving Q(√5) fixed. Similarly σ (a + b√5) = a - b√5 is an automorphism of Q (√3, √5) leaving Q(√3) fixed.

Theorem 4.4. Let E be a field extension of F. Then the set of all automorphisms of E that fix F elementwise is a group, that is, the set of all automorphisms

σ : E $\rightarrow$ E such that $\sigma(\alpha)=\alpha$ for all $\alpha \in$ F is group.

Proof : We need only show that the set of automorphism of E that fix F elementwise is a subgroup of the group of all automorphism of E. Let σ and τbe two automorphism of E such that $\sigma(\alpha)=\alpha$ and $\tau(\alpha)=\alpha$for all $\alpha \in F$. Then $\sigma\tau(\alpha)=\alpha$ and $\sigma^{-1}(\alpha)=\alpha$. Since the identity fixes every element of E, the set of

automorphisms of E that leave elements of F fixed is a subgroup of the entire group of automorphisms of E.

Definition 4.5 : Let E be an algebraic extension of a field F. Two elements $\alpha, \beta \in$ E are conjugate over F if they have the same irreduciblepolynomial

i.e. if $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$. i.e., for example, in the field Q(√3) the elements √3 and -√3 are conjugate over Q since they are both roots of the irreducible polynomial x^2-3.

Theorem 4.6: Let F be a field, and let α and β be algebraic over F with

$\deg(\alpha, F) = n.$ The map $\psi_{a.,\beta} : F(\alpha) \to F(\beta)$ defined by

$$\psi_{a.,\beta}(c_0 + c_1\alpha + \ldots\ldots\ldots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \ldots\ldots\ldots + c_{n-1}\beta^{n-1}$$

for $c_i \in F$ is an isomorphism of F is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugates over F.

Proof : Suppose the map $\psi_{a.,\beta}$ defined is an isomorphism.

Let irr $(\alpha, F) = a_0 + a_1 x + \ldots\ldots\ldots + a_n x^n$. By definition of irr (α, F)

$$a_0 + a_1 \alpha + \ldots\ldots\ldots + a_n \alpha^n = 0$$

So $\psi_{a.,\beta}(a_0 + a_1 \alpha + \ldots\ldots\ldots + a_n \alpha^n) = a_0 + a_1 \beta + \ldots\ldots\ldots + a_n \beta^n = 0$

Since irr (α, F) is the minimal polynomial and by the definition of irreducible polynomial, irr(β, F) divides irr(α,F). Using $(\psi_{a.,\beta})^{-1} = \psi_{\beta.\alpha}$, the same argument shows tha irr (α, F) divides irr (β, F). Since both irr (α, F) and irr (β, F) are monic, irr (α, F) = irr (β, F). so α and β are conjugate over F.

Conversely, suppose irr (α, F) = irr (β, F) = p(x).

Then the evaluation homomorphisms.

$\phi_\alpha : F[x] \to F(\alpha)$ and $\phi_\beta : F[x] \to F(\beta)$ both have the same kernel <p(x)>

Let ϕ be a homomorphism of a ring R into a ring $R^1$with kernel K. Then we know that ϕ[R] is a ring and there is a canonical isomorphism of ϕ[R] with R/K. applying this result to ϕ_α and ϕ_β , we get the following.

Corresponding to ϕ_α :F[x] $\to F(\alpha)$, there is a natural isomorphismψ_α mapping F[x]/<p(x)> onto ϕ_α[F[x]] = F(α).Similarly, ϕ_β gives rise to an isomorphism ψ_β mapping F[x]/<p(x)> onto onto F(β).

Considerthe composition of two isomorphism $\psi_{\alpha.\beta} = \psi_\beta(\psi_\alpha)^{-1}$

This is an isomorphism. This maps F (α) onto F (β).

Also for $(c_0 + c_1\alpha + \ldots\ldots\ldots + c_{n-1}\alpha^{n-1}) \in F(\alpha)$, we have

$$\psi_{\alpha.\beta}(c_0 + c_1\alpha + \ldots\ldots\ldots + c_{n-1}\alpha^{n-1})$$

$$= \psi_\beta(\psi_\alpha)^{-1}(c_0 + c_1\alpha + \ldots\ldots\ldots + c_{n-1}\alpha^{n-1})$$

$$= \psi_\beta[(c_0 + c_1x + \ldots\ldots\ldots + c_{n-1}x^{n-1}) + \langle p(x)\rangle]$$

$$= c_0 + c_1\beta + \ldots\ldots\ldots + c_{n-1}\beta^{n-1}$$

Thus $\psi_{\alpha,\beta}$ is the map defined in the statement of the Theorem.

Corollary 1 : Let α be algebraic over a field F. Every isomorphism ψ mapping $F(\alpha)$ into $\overline{F}$ such that $\psi(a) = a$ for all $a \in F$ maps α onto a conjugate β of α over F. Conversely for each conjugate β of α over F there exists exactly one

isomorphism $\psi_{\alpha,\beta}$ of $F(\alpha)$into $\overline{F}$ mapping α onto β and mapping each $a \in F$ onto itself.

Proof : Let ψ be an isomorphism mapping $F(\alpha)$ into $\overline{F}$.

$\psi(a)= a$ for $a \in F$. Let irr $((\alpha, F) = a_0 + a_1x+ \ldots\ldots\ldots +a_nx^n$.

Then $a_0 + a_1\alpha+ \ldots\ldots+a_n\alpha^n= 0$. So

$0 = \psi(a_0 + a_1\alpha + \ldots\ldots\ldots+a_n\alpha^n) = a_0 + a_1\psi(\alpha) + \ldots\ldots+a_n\psi(\alpha^n)$ and $\beta=\psi(\alpha)$ is a conjugate ofα.

Conversely, for each conjugate β of α over F, the isomorphism$\psi_{\alpha,\beta}$ of earlier Theorem is an isomorphism with the desired properties. That $\psi_{\alpha,\beta}$ is the only such isomorphism follows from the fact that an isomorphism of $F(\alpha)$ is completely determined by its values on elements of F and its values ofα.

Corollary 2 : Complex zeros of polynomials with real coefficients occur in conjugate pairs.

Proof : We know C = R(i) = R (-i). Also irr (i, R) = irr (-i, R). So i and – i are conjugate over R. By the above theorem the map $\psi_{i\text{-}i} : C \to C$ given by

$\psi_{i\text{-}i}(a + bi) = (a - bi)$ is an isomorphism.

Thus, if for $a, \in R$,

$f(a + bi) = a_0 + a_1 (a + bi) + \ldots\ldots\ldots\ldots + a_n(a + bi)^n = 0$

then $0 = \psi_{i\text{-}i}(f(a + bi)) = a_0 + a_1 (a - bi) + \ldots\ldots\ldots + a_n (a - bi)^n$

$= f(a - bi)$

that is f (a – bi) = 0 also.

Theorem 4.7 : Let $\{\sigma_i / i \in I\}$ be a collection of automorphism of a field E. Then the set $E_{\{\sigma_i\}}$ of all $a \in E$ left fixed by every σ_i for $i \in I$ forms a subfield of E.

Proof : If σ_i (a) = a and σ_i (b) = b for all $i \in I$, then

σ_i $(a \pm b) = \sigma_i$ (a) + σ_i (b) = $a \pm b$ and

σ_i (a b) = σ_i (a) σ_i (b) = a b and for all i $\in$ I.

Also, if b $\neq 0$ then

σ_i (a / b) = σ_i (a) / σ_i (b) = a / b and for all i $\in$ I.

Since the σ_i are automorphisms, we have

σ_i (0) = 0 and σ_i (1) = 1 for all i $\in$ I. Hence

0, 1 $\in$ $E_{\{\sigma_i\}}$ Thus $E_{\{\sigma_i\}}$ is a subfield of E.

Definition : The field $E_{\{\sigma_i\}}$ of above Theorem is the fixed field of $\{\sigma_i / i \in I\}$. For a single automorphism σ, we shall refer to $E_{\{\sigma\}}$ as the fixed field of σ.

Example : Let K = Q ($\sqrt[3]{2}$). The minimal polynomial of $\sqrt[3]{2}$ over Q is $x^3 - 2$. It has only one real root namely $\sqrt[3]{2}$. K is a field of real

numbers. So $\sqrt[3]{2}$ is the only root of $x^3 - 2$ in K. Let σ be any automorphism of K. Then $\sigma(\sqrt[3]{2}) \in K$ is a root of x^3 - 2. So $\sqrt[3]{2} = \sigma(\sqrt[3]{2})$. Let x be any element of K. x can be expressed as

$$\alpha + (\sqrt[3]{2})\beta + (\sqrt[3]{2})^2 \gamma, \alpha, \beta, \gamma \in Q,$$

$$\text{So } \sigma(x) = \sigma(\alpha) + \sigma(\sqrt[3]{2})\sigma(\beta) + \left[\sigma(\sqrt[3]{2})\right]^2 \sigma(\gamma)$$

So $\sigma(x) = \sigma(\alpha) + \sigma(\sqrt[3]{2})$

$\sigma(\beta) + [\sigma(\sqrt[3]{2})]^2 \ \sigma(\gamma)$

$= \quad a + \sqrt[3]{2}\,\beta + (\sqrt[3]{2})^2 \ \gamma = x$

That means σ = I, the identity automorphism. Thus Aut (K) = {I}. Hence in this case K itself is the fixed field under Aut (K).

Theorem : Let E be a field and let F is a subfield of E. Then the set G (E/F) of all automorphism of E leaving F fixed forms a subgroup of the group of all automorphisms of E. (The group G (E/F) is

the group of automorphisms of E leaving F fixed or more briefly, the group of E over F).

Proof ; For $\sigma \in G$ (E / F) and $a \in$ F, we have

$$\sigma\tau(a) = (\sigma)(\tau(a)) = \sigma(a) = a$$

So $\sigma\tau \in G(E/F)$. The identity automorphism I is in G (E/F). Also if $\sigma(a) = a$ for all $a \in$ F, then $a = \sigma^{-1}(a)$, so $\sigma \in$ G (E / F) implies that $\sigma^{-1} \in$ (E / F). Thus G(E/ F) is a subgroup of the group of all automorphisms of E.

Since every element of F is left fixed by every element of G (E / F), it follows that the field $E_{G(E/F)}$ of all elements of E left fixed by G (E/F) contains F.

Theorem 4.9 : Let F be a finite field of characteristic p. Then the map

$\sigma_p : F \to F$ defined by $\sigma_P(a) = a^p$ for $a \in F$ is an automorphism, the Frobenius automorphism of F. Also the fixed field of σ_p over F is Z_p

$$F_{\{\sigma_p\}} \cong Z_p$$

Proof : Let $a, b \in F$. Then

$$(a+b)^p = a^p + (p.1)\, a^{p-1} b + \ldots\ldots\ldots + b^p$$

$\sigma_p(a+b) = (a+b)^p = a^p + b^p$ (Since F is of characteristic p)

$$= \sigma_p(a) + \sigma_p(b)$$

Also $\sigma_p(ab) = (ab)^p = \sigma_p(a)\,\sigma_p(b)$

So σ_p is at least homomorphism. If $\sigma_p(a) = 0$. then $a^p = 0$ and $a = 0$, so the kernel of σ_p is $\{0\}$, and σ_p is a one-to-one map. Finally, since F is finite, σ_p is onto, by counting. Thus σ_p is an automorphism of F.

The prime field Z_p must be contained (upto isomorphism) in F, is of characteristic p. For c

$\in Z_p$,We have σ_p (c) = c by Fermat's theorem. Thus the polynomial x^p-x has p zeros in F, namely the elements in Z_p. We know that a polynomial of degree n over a field can have atmost n zeros in the field. Since the elements fixed under σ_p are precisely the zeros in F of x^p –x. Hence Zp=$\boldsymbol{F}_{\{\sigma_p\}}$

Examples 4.10

1) Let α be algebraic of degree n over F. Show that there are atmost n different isomorphisms of F (α) onto a subfield of F leaving F fixed.

Answer : We use following Theorem to prove the required result.

Let α be algebraic over a field F. Every isomorphism ψ mapping F(α) into $\overline{F}$ such that ψ (a) = a for $a \in$ F maps a onto a conjugate β of α over F.

Conversely, for each conjugate β of α over F, there exists exactly one isomorphism $\psi_{a.\beta}$ of F(α) into $\overline{F}$ mapping α into β and mapping each $a \in$ F onto itself.

Here deg. (α, F) = n

Hence the irr (α,F) has atmost n distinct roots in $\overline{F}$. So there exists atmost n isomorphisms of F(α) into $\overline{F}$.

2) Let F $(\alpha_1, \alpha_2 \ldots . \alpha_n)$ be an extension field of F: Show that any automorphism

σ of F$(\alpha_1, \alpha_2 \ldots . \alpha_n)$ leaving F fixed is completely determined by the n values $\sigma(\alpha_i)$.

Answer : Every element of F$(\alpha_1, \ldots . \alpha_n)$ can be expressed as a linear combination of product of powers of $\alpha_1, \alpha_2, \ldots \alpha_n$ with elements in F where the powers of each a_1 may be positive, negative or zero.

Also $\sigma(\alpha^{j}{}_{i}) = [\sigma(\alpha_i)]^j$ for each i = 1,2, ...n and j $\in$ z. Therefore the automorphism σ is determined by the n values $\sigma(\alpha_i)$ i = 1, 2, ...n

3) Let E be an algebraic extension of a field F and let σ be an automorphism of E leaving F fixed. Let $\alpha \in$ E. Show that σ induces a permutation of the set of all zeros of irr (α,F) that are in E.

Answer : Let irr (α,F) = $a_0 + a_1 x + \ldots\ldots\ldots + a_n x^n$

Now $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$

So $\sigma(a_0 + a_1\alpha + \ldots\ldots\ldots + a_n a^n) = 0$

i.e, $a_0 + a_1\sigma(\alpha) + \ldots + a_n\sigma(\alpha^n) = 0$

i.e., $\sigma(\alpha)$ satisfies the equation.

$a_0 + a_1 x + \ldots + a_n x^n = 0$. Hence whenever α is zero, $\sigma(\alpha)$ is also a zero of its irreducible polynomial (irr (α,F))

Therefore σ induces a permutation of the set of all zeros of irr (α, F) that are in E

4) Let E be an algebraic extension of a field F. Let S = $\{\sigma_i / i \in I\}$ be a collection of automorphisms of E such that every σ_i leaves each element of F fixed. Show that if S generates the subgroup H of G (E/F) then $E_S = E_H$

Answer : Since the subgroup H of G(E/F) is generated by S, every element of H is a finite product of integral powers of the σ_i's.

Also S ≤ H $\quad \therefore E_H \leq E_s$

Now let a ∈ E_s

Let $\sigma \in M$

Then $\sigma = \sigma_1^{i_1} \sigma_2^{i_2} \ldots\ldots \sigma_n^{i_n}$

$$\therefore \quad \sigma(a) = \sigma_1^{i_1}(\sigma_2^{i_2}(\ldots\ldots(\sigma_n^{i_n}(a)) = \sigma_1^{i_1}(a)$$

Since $\sigma_n^{i_n}(a) = \sigma_n(\sigma_n(.....(\sigma_n(a))$ n times and each time a is left fixed.

Therefore σ (a) = a

i.e., a $\in E_H$ $\quad \therefore Es \leq E_H$

Hence $E_s = E_H$

5) Prove the following sequence of theorems

a) An automorphism of a field E carries elements that are squares of elements in E onto elements that are squares of elements of E.

b) If σ is an automorphism of R and a < b where a,b $\in$ R, then σ (a) $< \sigma$ (b)

c) The only automorphism of R is the identity automorphism.

Solution :

a) Let a $\in$ E be such that $a = b^2$ for some b $\in$ E. If ϕ is an automorphism of E, then ϕ (a) = ϕ (b^2) = [ϕ (b)]^2

i.e., ϕ (a) is also a square

b) Let $r \in R$ and $r > 0$. Then $r = s^2$ for $s \in R$.

$\sigma(r) = (s^2) = [\sigma(s)]^2 > 0$

i.e., $r > 0 \Rightarrow \sigma(r)\ 0$

Let a,b be such that $a < b$

$\therefore b - a > 0 \Rightarrow \phi(b - a) > 0$

i.e., $\phi(b) > \phi(a)$

c) Let σ be an automorphism of R then $\sigma(1) = 1$. Hence $\sigma(n) = n$ for all positive integer n.

Also $\sigma(0) = 0$ $\sigma(-n) = -n$

$\sigma(m^{-1}) = [\sigma(m)]^{-1} = m^{-1}$ for all non zero integers m.

Thus $\sigma(nm^{-1}) = \sigma(n)\ \sigma(m^{-1}) = nm^{-1}$

Let $r \in R$ and let $p < r < q$ where $p,q \in Q$

Then $\sigma(p) = p < \sigma(r) < \sigma(q) = q$

Thus given any rational numbers p, q such that p < r < q, both r and σ (r) are in the interval between p and q

So σ (r) = r for all …. $\in$ R

Hence identity is the only automorphism of R.

THE ISOMORPHISM EXTENSION THEOREM

We know that if $\alpha, \beta \in$ E are conjugate over F, then there is an isomorphism $\psi_{\alpha.\beta}$ of F(α) onto F(β). $\alpha, \beta \in$ E implies F(α) $\leq E$. W. Now we are extending the domain of definition of $\psi_{\alpha.\beta}$ from F(α) to a bigger fields, perhaps all of E, and whether this might perhaps leads to an automorphism of E.

Theorem 5.1. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F^1. Let $\overline{F}^1$ be an algebraic closure of F^1. Then σ can be extended to an isomorphism ϑ of E onto a subfield of $\overline{F}^1$ such that ϑ (a) = σ (a) for all a $\in$ F.

Corollary 5.2 : If E$\leq \overline{F}$ is an algebraic extension of F and $\alpha, \beta \in$ E are conjugate over F then the conjugation isomorphism $\psi_{\alpha.\beta} : F(\alpha) \to F(\beta)$ can be

extended to an isomorphism of E onto a subfield of $\overline{F}$.

Proof: The proof immediate from the above theorem replace F by $F(\alpha)$, F^1 by $F(\beta)$ and $\overline{F}^1$ by $\overline{F}$ in the statement of the above theorem.

Corollary 5.3 : Let $\overline{F}$ and $\overline{F}^1$ be two algebraic closures of $\overline{F}$. Then $\overline{F}$ is isomorphic to $\overline{F}^1$ under isomorphism leaving each element of F field.

Proof: By Theorem 5.1, the identity isomorphism of F onto F can be extended to an isomorphism τ mapping F onto a subfield of $\overline{F}^1$ that leaves F fixed. We need only show that τ is onto $\overline{F}^1$. But by Theorem 5.1, the map τ^{-1} from $\tau[F]$ to $\overline{F}$ can be extended to an isomorphism of $\overline{F}^1$ onto a subfield of $\overline{F}$. Since τ^{-1} is already onto $\overline{F}$, we must have $\tau[\overline{F}] = \overline{F}^1$.

Note: For a finite extension E of a field F, we would like to count how many isomorphism there are of E, onto a subfield of $\overline{F}$ that leave F fixed. We will see that there are only finite number of

isomorphism, since every automorphism in G(E/F) is such an isomorphism, a count of these isomorphisms will include all these isomorphisms.

Theorem 5.4 : Let E be a finite extension of a field F. Let σ be isomorphism of F onto a field F^1, and let $\overline{F}^1$ be an algebraic closure of F^1. Then the number of extensions of σ to an isomorphism ϑ of E onto a subfield of $\overline{F}^1$ is finite, and independent of F^1, $\overline{F}^1$ and σ. That is the number of extensions is completely determined by the two fields E and F, it is intrinsic to them.

Proof: The diagram below is constructed in the following way.Consider the isomorphisms σ_1 : $F \rightarrow F_1'$ (onto map) $\sigma_2 : F \rightarrow F_2'$ (onto map)

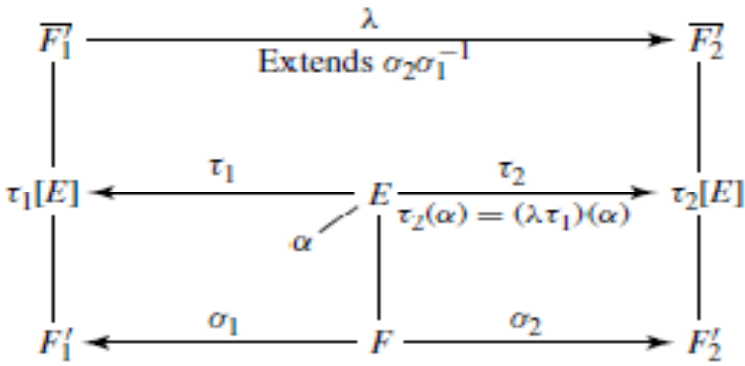
where $\overline{F_1'}$ and $\overline{F_2'}$ are algebraic closures of F_1' and F_2' respectively. Now $\sigma_2\ \sigma_1^{-1}$ is an isomorphism of F_1' onto F_2' .Then by theorem 5.1 and corollary 5.3 there is an isomorphism $\boldsymbol{\lambda}$ from F_1' onto F_2' .Extending this isomorphism $\sigma_2\ \sigma_1^{-1}$

from F_1' onto F_2'.By diagram corresponding to each τ_1: E→ $\overline{F_1'}$ that extends σ_1 we obtain an isomorphism τ_2: E→ $\overline{F_2'}$ by starting at E and going first to the left,then up,and then to the right. $\tau_2(\alpha)= \boldsymbol{\lambda}\tau_1(\alpha)$ for $\alpha \in E$. Clearly τ_2 extends σ_2 . The fact that we could have started with τ_2 and recovered τ_1 by defining $\tau_1(\alpha)= (\boldsymbol{\lambda^{-1}}\tau_2)(\alpha)$,

that is by chasing the other way around the diagram, shows that the correspondence between τ_1: E→ $\overline{F_1'}$ and τ_2: E→ $\overline{F_2'}$ is one to one.

In view of this one to one correspondence, the number of **τ**extending**σ** is independent of F',$\overline{F'}$ and **σ.** That the number of mapping extending σ is finite follows from the fact that since E is a finite extension of F,

E=$(\alpha_1,\ldots,\alpha_n)$ for some $\alpha_1,\ldots,\alpha_n$ in E. Then there are only a finite number of possible candidates for the inages $\tau(\alpha_i)$ in $\overline{F'}$



Definition 5.5 : Let E be a finite extension of a field F. The number of isomorphisms of E into $\overline{F}$ leaving F fixed is the index {E : F} of E over F.

Corollary 5.6 : If $F \leq E \leq$ K, where K is a finite extension field of the field F, then { K : F } = { K : E } { E : F }

Proof : It follows from Theorem 5.4 that each of the {E : F} isomorphisms $\tau_1 : E \to \overline{F}$ leaving F field has {K : E} extensions to an isomorphism of K into $\overline{F}$.**Exercise 5.7 :** Let E = Q ($\sqrt{2}$,$\sqrt{3}$). For each isomorphic mapping of a subfield of E, give all

extensions of the mapping to a isomorphic mapping of E into subfield of $\overline{Q}$.

The identity map will have extension by isomorphism theorem, then the conjugate mapping $\psi_{\sqrt{2},\sqrt{-2}}$ and $\psi_{\sqrt{3},\sqrt{-3}}$ and their composition $\psi_{\sqrt{2},\sqrt{-2}} \circ \psi_{\sqrt{3},\sqrt{-3}}$can also have isomorphic of E into subfiled of $\overline{Q}$, so the {E:Q}=4.

Exercise 5.8 : Let σ be the automorphism of Q(π) that maps π onto –π

(a) Describe the fixed field of σ

(b) Number of isomorphisms from $Q(\sqrt{2})$ to $Q(\sqrt{3})$ is zero.

Solution : Givenσ: Q(π)→Q(π)

Such that $\sigma(\pi) = -\pi$

(a) Consider $\sigma(\pi^2)$ = $\sigma(\pi)\sigma(\pi)$

= $-\pi - \pi = \pi^2$

Thus fixed field of σ is Q(π^2)

(b) Number of isomorphisms from Q($\sqrt{2}$) to Q($\sqrt{3}$) is zero.

Since $\sqrt{2}\ and\ \sqrt{3}$ are not conjugate. If $\sqrt{2}\ map\ to\ \sqrt{3}$ then 2 will have two images 2 and 3,it's a contradiction.

$\varphi(2) = 2\ since\ 2\ belongs\ to\ Q, also$

$\varphi(2) = \varphi(\sqrt{2}.\sqrt{2}) = \varphi(\sqrt{2})\varphi\sqrt{(2)} = \sqrt{3}.\sqrt{3}$

=3.

SPLITTING FIELDS

Suppose E is an algebraic extension of a field F. If $\alpha \in E$ and $\beta \in \overline{F}$ is a conjugate of α over F, then there is a conjugation isomorphism.

$\psi_{\alpha.\beta} : F(\alpha) \to F(\beta)$

By an earlier result $\psi_{\alpha.\beta}$ can be extended to an isomorphism mapping E onto a subfield of $\overline{F}$. Now if β does not belongs to E, such an isomorphic mapping of E cannot be an automorphism of E. Thus, if an algebraic extension E of a field F is such that all its isomorphic mapping onto subfield of $\overline{F}$ leaving F fixed are actually automorphism of E, then for every $\alpha \in E$, all conjugates of α over F must be in E also.

Definition 6.1 : Let F be a field with algebraic closure $\overline{F}$. Let $\{f_i(x) / i \in I\}$ be a collection of polynomials in F[x]. A field $E \leq \overline{F}$ is the splitting field of $\{f_i(x)/i \in I\}$ over F if E is the smallest subfield of $\overline{F}$ containing F and all the zeroes in $\overline{F}$

of each of the f_i (x) for i $\in$ I. A field K$\leq \overline{F}$ is a splitting field over F if it is the splitting field of some set of polynomials in F[x].

Note : For one polynomial f(x) $\in$ F[x], we shall often refer to the splitting field of {f(x)} over F as the splitting field of f(x) over F. Note that the splitting field of {f(x) / i$\in$I} over F in $\overline{F}$ is the intersection of all subfields of $\overline{F}$ containing F and all zeroes in $\overline{F}$ of each f_i (x) for i $\in$ I. Thus such a splitting field surely does exist.

Splitting fields over F are precisely those fields E $\leq \overline{F}$ with the property that all isomorphic mappings of E onto a subfield of $\overline{F}$ leaving F fixed are automorphism of E.

Theorem 6.2 : A field E, where F $\leq$ E $\leq \overline{F}$ is a splitting field over F if and only if every automorphism of $\overline{F}$ leaving F fixed maps E onto itself and thus induces an automorphism of E leaving F fixed.

Proof: Let E be the splitting field over F in $\overline{F}$ of $\{f_i(x) / i \in I\}$,and let σ be an automorphism of $\overline{F}$ leaving F fixed. Let $\{\alpha_j / j \in J\}$ be the collection of all zeroes in $\overline{F}$ of all the $f_i(x)$ for $i \in I$. We have a fixed α_j, the filed $F(\alpha_j)$has as elements all expressions of the form $g(\alpha_j)=a_0 + a_1\alpha_j + \cdots + a_{n_j-1}\alpha_j^{n_j-1}$, where n_j is the degree of $irr(\alpha_j, F)$ and a_k belongs to F. Consider the set S of all finite sums of finite products of elements of the form $g(\alpha_j)$ for all $j \in J$. The set S is a subset of E closed under addition and multiplication and containing 0,1, and the additive inverse of each element. Since element of S is in some $F(\alpha_1, \ldots, \alpha_r)$ subset of S, we see that S also contains the multiplicative inverse of each non zero element. Thus S is a subfield of E containing all α_j for $j \in J$, By definition of the splitting field E of $\{f_i(x) / i \in I\}$,we see that S =E. Then $\{\alpha_j / j \in J\}$ generates E over F, in the sense that taking finite

sums and products. So the value of σ on any element of E is completely determined by the values $\sigma(\alpha_j)$, But $\sigma(\alpha_j)$ must also be a zero of $\text{irr}(\alpha_j, F)$. By Theorem $\text{irr}(\alpha_j, F)$ divides $f_i(x)$ for which $f_i(\alpha_j) = 0$, so $\sigma(\alpha_j)$ belongs to E also. Thus σ maps E onto a subfield of E isomorphically. However, the same is true of the automorphism σ^{-1} of $\bar{F}$. Since for β element of E, $\beta = \sigma(\sigma^{-1}(\beta))$, we see that σ maps E onto E, and thus induces an automorphism of E.

Suppose, conversely, that every automorphism of $\bar{F}$leaving F fixed induces an automorphism of E. Let g(x) be an irreducible polynomial in F[x] having a zero α in E. If β is any zero of g(x) in $\bar{F}$, then by Theorem , there is a conjugation isomorphism $\Psi_{\alpha,\beta}$of F(α) onto F(β) leaving F fixed , then $\Psi_{\alpha,\beta}$ can be extended to an isomorphism τ of $\bar{F}$ onto a subfield of $\bar{F}$. But then τ must have been onto $\bar{F}$, so τ is an automorphism

of $\bar{F}$leaving F fixed. Then by assumption ,τ induces an automorphism of E, so $\tau(\alpha) = \beta$ is in E. We have shown that if g(x) is an irreducible polynomial in F[x] having one zero in E, then all zeroes of g(x) in $\bar{F}$is in E. Hence if $\{g_k(x)\}$ is the set of all irreducible polynomials in F[x] having a zero in E, then E is the splitting field of $\{g_k(x)\}$.

Definition 6.3 : Let E be an extension field of a field F. A polynomial f(x)$\in$ F[x] splits in E if it factors into a product of linear factors in E [x].

Corollary 6.4 : If E $\leq \overline{F}$ is a splitting field over F, then every irreducible polynomial in F[x] having a zero in E splits in E.

Proof: If E is a splitting field over F in $\overline{F}$, then every automorphism of $\overline{F}$ induces an automorphism of E. The second half of the proof of the theorem 6.2 showed precisely that E is also the splitting field over F of the set $\{g_k(x)\}$ of all irreducible polynomials in F[x] having a zero in

E. Thus an irreducible polynomial f(x) of F[x] having a zero in E has all zeroes in $\bar{F}$is in E. Therefore, its factorization into linear factors in $\bar{F}[x]$, actually takes place in E[x], so f(x) splits in E.

Corollary 6.5 : If $E \leq \bar{F}$ is a splitting field over F, then every isomorphic mapping of E onto a subfield of $\bar{F}$ and leaving F fixed is actually an automorphism of E. In particular, if E is splitting field of finite degree over F, then$\{ E : F \} = | G (E / F) |$

Proof: Every isomorphism σ of E onto a subfield of $\bar{F}$ leaving F fixed can be extended to an automorphism τ of $\bar{F}$. If E is a splitting field over F, then by 6.2 τ restricted to E,that is σ, is an automorphism of E. Thus for a splitting field E over F, every isomorphic mapping of E onto a subfield of $\bar{F}$ and leaving F fixed is actually an automorphism of E.

The equation {E:F}=|G(E/F)| then follows immediately for a splitting field E of finite degree over F, since {E:F} was defined as the number of different isomorphic mappings of E onto a subfield of $\overline{F}$ and leaving F fixed.

Exercise 6.6

1) Let α be a zero of $x^3 + x^2 + 1$ over Z_2 show that $x^3 + x^2 + 1$ splits in $Z_2(\alpha)$ Ans: Since irr $(\alpha, Z_2) = x^3 + x^2 + 1$

$\{1, \alpha, \alpha^2\}$ from a basis for $Z_2(\alpha)$ over Z_2

$$\therefore Z_2(\alpha) = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$$

Now $x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + 1 + \alpha + \alpha^2)$

i.e., $x^3 + x^3 + 1$ splits in $Z_2(\alpha)$

2) Let f(x) be a polynomial in F[x] of degree n.

Let $E \leq \overline{F}$ be the splitting field of f(x) over F in $\overline{F}$. What bounds can be put in [E : F] ?

Ans : We prove that $1 \leq [\, E : F \,] \leq n!$, we prove the result by induction in n.

First let n = 1. that is the polynomial f(x) linear say f(x) = $\alpha x + \beta$, $\alpha, \beta \in F, \alpha \neq 0$ Then the only one root of it is $-\beta\alpha^{-1}$ which is in F. Then [E : F] = 1

Therefore the result holds for n = 1

Assume that the result holds for every natural number less than n.

Let deg f(x) = n **>** 1

We have the result if f(x) $\in$ F[x] is of degree n, then there is a finite extension L of in which f(x) has a root. Also [L : F] $\leq$ deg f(x)

Thus we got extension field L of F, with [L : F] $\leq$ n and an $\alpha \in$ L such that f (α) = 0

Hence f(x) = (x-α) q(x), where deg q(x) = n-1 and q(x)$\in$ L[x]

By induction hypothesis there is an extension field E of L containing all n – 1 roots of q(x), and

$[E : L] \leq (n-1)!$

Now $[E : F] = [E : F][L : F] \leq (n-1)!\, n = n!$

Also $\alpha \in L$ gives $\alpha \in E$ i.e. E contains all the n roots of f(x).

$\therefore$ By induction the result is true for all $n \geq 1$.

Hence $1 \leq [E : F] \leq n!$

3) Show that if [E:F] = 2, then E is a splitting field over F.

Ans: $[E : F] = 2$. Then $E = F(\alpha)$ for some $\alpha \in E$. $\{1, \alpha, \alpha^2\}$ cannot be a linearly independent subset of E. Therefore, there are elements a_0, a_1, a_2 not all zero in F such that $a_0 + a_1\alpha + a_2\alpha^2 = 0$.

If $a_2 = 0$. then α satisfies the polynomial $a_0 + a_1 x$ and hence E is a splitting field. Suppose $a_2 \neq 0$

then $a_0 + a_1 x + a_2 x^2 = (x - \alpha)(a_2 x + a_2\alpha + a_1)$

The other zero is $-(a_1 + a_2\alpha) / a_2$ which is in E.

i.e., $a_0 + a_1 x + a_2 x_2$ splits in E

Hence E is a splitting field over F.

4) Show that for F ≤ E ≤ $\overline{F}$, E is a splitting field over F if an only if E contains all conjugates over F in $\overline{F}$ for each of its elements.

Ans: Let $\alpha \in$ E and β be a conjugate of α over F in $\overline{F}$. Then there exists the conjugation isomorphism

$\psi_{\alpha.\beta} : F(\alpha) \to F(\beta)$ mapping α onto β and leaving F fixed.

By isomorphism extension theorem. $\psi_{\alpha.\beta}$ can be extended to an automorphism of $\overline{F}$. Now we have the theorem "A field E where F ≤ E ≤ $\overline{F}$ is a splitting field over F if and only if every automorphism of $\overline{F}$ leaving F fixed maps E onto itself and thus induces an automorphism of E leaving F fixed"

Therefore E is a splitting field if and only if $\beta \in$ E i.e., if and only if all conjugtaes of each element of E.

5) Show that $Q(\sqrt[3]{2})$ has only the identity automorphism

Ans: Let $\alpha = \sqrt[3]{2}$, the real cube root of 2.

Let $F = Q(\sqrt[3]{2}) \subseteq R$, and let $f(x) = x^3 - 2$

Let σ be an automorphism of F.

Since α is a zero of f (x), $\sigma(\alpha)$ is a root of σ (f (x)) = f (x) in R.

Hence $\sigma(\alpha) = \alpha$

Now $[Q(\alpha) : Q] = \deg \text{irr}(\alpha, Q) = 3$

and $\{1, \alpha, \alpha^2\}$ is a basis for $Q(\alpha)$ over Q

$\therefore \sigma(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 / a_i \in Q\}$

Since $\alpha(a_i) = a_i$ and $\sigma(\alpha) = \alpha$

σ leaves every element of $Q(\alpha)$ fixed i.e…, σ is the identity map of $Q(\alpha)$

6) Show that for a prime, the splitting field over Q of $x^p - 1$ is of degree p–1 over Q.

Ans : Let $f(x) = x^p - 1 \in Q[x]$

Now $f(x) = (x - 1)g(x)$, where

$g(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$

Also $g(x) = \dfrac{x^p - 1}{x - 1}$

Hence g(x+1)= $\frac{(x+1)^p - 1}{x}$

= $x^{p-1} + (pC_1)x^{p-2} + \ldots\ldots + (pC_{p-1})$

Now p is prime such that p / (pC_r) for all 1 $\leq r \leq p-1$

Also p^2 does not divide (pC_{p-1})

Hence by Eisenstein's criterion, g (x + 1) is irreducible Q.

Hence g(x) is irreducible over Q.

Let $\xi = e^{2i\pi 1p}$ where $i^2 = -1$

Then the roots of f(x) are $\xi, \xi^2 \ldots\ldots \xi^{p-1}$

and roots of g(x) are $\xi, \xi^2 \ldots\ldots \xi^{p-1}$

Now the splitting field of f(x) is

S = $Q(1, \xi, \xi^2 \ldots\ldots \xi^{p-1}) = Q(\xi)$

Also g(x) = irr (ξ, Q)

$\therefore [S : Q] = p-1$

7) Let $\overline{F}$ and $\overline{F}'$ be two algebraic closure of a field F, and let f(x) $\in$ F[x]. Show that the splitting field E over F of f(x) in $\overline{F}$ is isomorphic to the splitting field E^1 over F of f(x) in $\overline{F}'$.

Ans: Since $\overline{F}$ and $\overline{F}$ are two algebraic closures of the field F there is an isomorphism

$\sigma : \overline{F} \to \overline{F}$ such that σ (a) = a for a $\in$ F.

We prove the result by induction on deg f(x).

If deg f (x) = 1. then E = F = E^1

Therefore the result holds by taking the identity mapping of F onto F.

Assume the result holds good for all polynomials of degree less than n.

Let deg f (x) = n. Let p(x) be an irreducible factor of f(x) and c_1 be a root of p(x) and $c_1^{\,1}$ be a root of p(x) in E^1. Then the identity mapping of F can be extended to an isomorphism $\overline{\alpha_1}$ of $F(c_1)$ onto $F(c_1^{\,1})$. Extend α_1 to an isomorphism $\overline{\alpha_1}$ of $F(c_1)$ [x] onto F $(c_1^{\,1})$ [x] onto $F(c_1^{\,1})$ [x].

Now f (x) = $(x - c_1)$ f_1 (x) in F (c_2) [x] and

f (x) = $(x - c_1^{\,1}) f_1^{\,1}$ (x) in F (c_2) [x]

where $f_1^{\,1}$ (x) = $\overline{\alpha_1}$ (f_1 (x))

Clearly E is a splitting field for $f_1(x)$ over $F(c_1)$ and F^1 is a splitting field of $f_1(x)$ Since deg $f_1(x)$ =

n – 1 = deg f_1^1 (x), α_1 can be extended to an isomorphism of E onto E^1 by induction hypothesis.

8) Find the splitting field over Q for the polynomial $x^4 + 4$

Solution : We have the factorization $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ where the factors are irreducible by Eisenstein's criterion. The roots are 1+i , 1-i , -1+i ,-1-i so the splitting field is Q (i), which has degree 2 over Q.

An alternate solution is to solve $x^4 = -4$. To find one root, use De Moivre's Theorem to get $(1/\sqrt{2}) + (1\sqrt{2})$ i and then multiply by $\sqrt{2}$ to get 1+i. The other roots are found by multiplying the powers of i, because it is primitive 4^{th} root of unity.

9) Find the degree of the splitting field over Z_2 for the polynomial $(x^3+x+1)(x^2+x+1)$

Solution : The two polynomials are irreducible. Therefore the splitting field must have subfields

of degree 3 and of degree 2, so the degree of the splitting field over Z_2 must be 6.

10) Find the degree [F:Q], where F is the splitting field of the polynomial x^3-11 over the field Q of rational numbers.

Solution: Letting αbe the cube root of 11, the roots of the polynomial are α, $\omega\alpha$ and $\omega^2\alpha$where ω is a primitive cube root of unity, Since ω is not real, it cannot belong to $Q(\alpha)$. Sinceω is a root of x^2+x+1 and $F = Q(\alpha,\omega)$ we have $[F : Q] = 6$

11) Determine the splitting field over Q for $x^4 + x + 1$.

Solution: This polynomial is not irreducible. In fact $x^6 - 1$ factors in two ways and provides an important clue. Note that

$$x^6 - 1 = (x^3)^2 - 1 = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$$ and

$$x^6 - 1 = (x^3)^2 - 1 = (x^2 - 1)(x^2 + x + 1)(x^2 - x + 1)$$

Thus $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ and the roots of the first factors are the primitive 3rd roots of unity, while the roots of the second factor are the primitive 6th roots of unity. Adjoining a root of $x^2 - x + 1$ gives all 4 roots, and so the splitting field has degree 2 over Q.

12) Determine the splitting field over Q for x^4+2.

Solution: To get the splitting field F, we need to adjoin the 4th roots of -2, which have the form $\omega^i\alpha$ where α is the 4th root of 2, ω Is primitive 8th root of unity and I =1, 3, 5, 7. To construct these roots we only need to adjoin α and i.

To show this, using the polar form $\cos\theta + i\sin\theta$ Of the complex numbers, we can see that

$\omega = (\sqrt{2}/2) + (\sqrt{2}/2)\,i, \omega^3 = -(\sqrt{2}/2) + (\sqrt{2}/2)\,i.$

$\omega^5 = -(\sqrt{2}/2) - (\sqrt{2}/2) - (\sqrt{2}/2)\,i,$

$\omega^7 = (\sqrt{2}/2) - (\sqrt{2}/2)\,i$

Thus $\alpha\sqrt{2} = \omega\alpha + \omega^7\alpha$ must belong to F, and then the cube of this element, which is 4 α must also belong to F. Therefore α belongs to F and the square of this element is $\sqrt{2}$, so it follows that $\sqrt{2}$ belongs to F, and therefore i belongs to F. The splitting field is thus $Q(\alpha, i)$ which has degree 8 over Q.

SEPARABLE EXTENSIONS

Our aim is to determine, for a finite extension E of F, under what conditions {E : F} = [E : F]

Definition 7.1 : Let f (x) ∈ F[x]. An element α of $\bar{F}$ such that f (α) = 0 a zero of

f (x) of multiplicity n if n is the greatest integer such that $(x-\alpha)^n$ is a factor of

f (x) in $\bar{F}$ [x]

Theorem 7.2 : Let f (x) be irreducible in F[x] Then all zeros of f (x) in $\bar{F}$ have the same multiplicity.

Proof: Let α and β be zeroes of f(x) in $\bar{F}$. Then by theorem there is a conjugation isomorphism $\Psi_{\alpha,\beta}$of F(α) onto F(β) leaving F fixed , then $\Psi_{\alpha,\beta}$ can be extended to an isomorphism τ of $\bar{F}$ onto a subfield of $\bar{F}$. But then τ must have been onto $\bar{F}$, so τ is an automorphism of $\bar{F}$leaving F fixed. Then τ induces a natural isomorphism τ_x: $\bar{F}[x] \to \bar{F}[x]$ with τ_x(x)= x. Now τ leaves f(x)

fixed ,since f(x) element of F[x] and $\Psi_{\alpha,\beta}$ leaves F fixed. However,

$\tau_x((x-\alpha)^v) = (x-\beta)^v$. From this we get that the multiplicity of β in f(x) is greater than or equal to the multiplicity of α, A symmetric argument gives the reverse inequality, so the multiplicity of α equals that of β.

Corollary 7.3 : If f (x) is irreducible in F [x]then f (x) has a factorization in

$\overline{F}$ [x] of the form

a $\prod_i (x-\alpha_i)^{\gamma}$where α_i are the distinct zeros of f (x) in $\overline{F}$ and a∈ F.

Theorem 7.4 : If E is a finite extension of F, then { E : F} divides [E : F].

Proof: If E is finite over F, then $E = F(\alpha_1, \cdots, \alpha_n)$, where $\alpha_i \in F$. Let

irr(α_i, $F(\alpha_1, \cdots, \alpha_{i-1})$) have $\alpha_i$as one of $n_i$distinct zeros that are all of a common multiplicity v_i .Then

$[F(\alpha_1, \cdots, \alpha_i) : F(\alpha_1, \cdots, \alpha_{i-1})] = n_i v_i = \{F(\alpha_1, \cdots, \alpha_i) : F(\alpha_1, \cdots, \alpha_{i-1})\} v_i$.

$[E : F] = \prod_i nivi$ and $\{E : F\} = \prod_i ni$

Therefore, $\{E : F\}$ divides $[E : F]$.

Definition 7.5 : A finite extension E of F is a separable extension of F if { E : F} = [E : F]. An element α of $\overline{F}$ is separable over F if F(α) is a separable extension of F. An irreducible f (x) ∈ F [x] is separable over F if every zero of f(x) in $\overline{F}$ is separable over F.

The field E=Q[√2, √3] is separable over Q since we know { E : Q} = 4= [E : Q]

We know that {F(α) : F} is the number of distinct zeros of irr (α, F). Also, the multiplicity of α in irr (α, F) is the same as the multiplicity of each conjugate of α over F. Thus α is separable over F if and only if irr (α, F) has all zeros of multiplicity 1. Thus an irreducible polynomial f

(x)∈ F [x] is separable over F if and only if f (x) has all zeros of multiplicity 1.

Theorem 7.6 : If K is a finite extension of E and E is a finite extension of F, that is $F \leq E \leq K$, then K is separable over F if and only if K is separable over E and E is separable over F.

Proof: We have {K:F}={K:E}{E:F} and also [K:F]=[K:E][E:F]

If K is separable over, {K:F}=[K:F] also {K:E} divides[K:E] and {E:F} divides [E:F]. so we get {K:E}=[K:E] ,{E:F}=[E:F].

Conversely if K is separable over E and E is separable over F.

Then clearly K is separable over F.

Corollary : If E is a finite extension of F, then E is separable over F if and only if each αin E is separable over F.

Proof: Suppose that E is sepearble over F, and let α element of E.

Then F$\leq F(\alpha)\leq E$, and then by 7.6 $F(\alpha)$ is seperable over F.

Suppose , conversely, that every α in E is separable over F. Since E is a finite extension of F, there exists $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

F < F(α_1) < F(α_1,α_2) <…< E = F($\alpha_1, \alpha_2, \ldots, \alpha_n$)

Now since α_i is sepearble over F, $\alpha_i$is seperable over F($\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$) because q(x) = irr($\alpha_i$,F($\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$)) divides irr($\alpha_i, F$), so that $\alpha_i$is zero of q(x) of multiplicity one. Thus F($\alpha_1, \alpha_2, \ldots, \alpha_i$) is seperable over F($\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$), so E is seperable over F by 7.6, extended by induction.

Definition 7.7 : A field is perfect if every finite extension is a separable extension.

Theorem 7.8 : Every field of characteristic zero is perfect.

Proof: Let E be a finite extension of a field F of characteristic zero, and let α element of E. Then

f(x) = irr(α,F) factors in $\bar{F}$[x] into $\prod_i (x - \alpha_i)^v$, where the α_i

are the distinct zeroes of irr(α,F) and we say α = α_1.

Thus f(x) = $(\prod_i (x - \alpha_i))^v$ and since $v.1 \neq \bar{0}$ for a field F of characteristic zero, we must have $\prod_i (x - \alpha_i)$ belongs to F[x] by the lemma (Let $\bar{F}$ be an algebraic closure of F, and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be any monic polynomial in $\bar{F}$[x]. If $(f(x))^m \in F[x]$ and $m \cdot 1 \neq 0$ in F, then $f(x) \in F[x]$, that is, all $a_i \in F$). Since f(x) is irreducible and of minimal degree in F[x] having αas zero, we then see that $v = 1$. Therefore, α is seperable over F for all α belongs to E. Then E is seperable extension of F.

Theorem 7.9 : Every finite field is perfect

Proof: Let F be a finite field of characteristic p, and let E be a finite extension of F. Let $\alpha \in E$. We need to show that α is separable over F . Now $f(x) = \text{irr}(\alpha, F)$ factors in $\bar{F}$ into $\prod_i (x - \alpha_i)^v$, , where the α_i are

the distinct zeroes of irr(α,F) and we say $\alpha = \alpha_1$. Let $v = p^t e$,where p does not divide e.

Then f(x) = $\prod_i (x - \alpha_i)^v$, $f(x) = (\prod_i (x - \alpha_i)^{p^t})^e$, is in F[x], and by lemma (Let $\bar{F}$be an algebraic closure of F, andlet$f$ (x) = $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be any monic polynomial in $\bar{F}$[x]. If $(f(x))^m \in F[x]$ and $m \cdot 1 \neq 0$ in F, then $f(x) \in F[x]$, that is, all $a_i \in F$). $\prod_i (x - \alpha_i)^{p^t}$ is in F[x] since e.1≠ 0in F.

Since $f(x)$ = irr(α, F) is of minimal degree over F having α as a zero, we must have e = 1. This shows that $f(x) = (\prod_i (x - \alpha_i)^{p^t}) = \prod_i (x^{p^t} - \alpha_i{}^{p^t})$. Thus, if we regard f(x) as $g(x^p)$, we must have g(x) belongs to F[x]. Now g(x) is seperable over F with distinct zeros $\alpha_i{}^{p^t}$. Consider F($\alpha_1{}^{p^t}$) = F(α^{p^t}). Then F(α^{p^t}) is seperable over F. Since $x^{p^t} - \alpha^{p^t} = (x - \alpha)^{p^t}$, we see that α is the only zero of

$x^{p^t} - \alpha^{p^t}$ in $\bar{F}$. As a finite dimensional vector space over a finite filed F, F(α^{p^t}) must be again a finite field. Hence the map σ_p: F(α^{p^t})→ F(α^{p^t}) given by $\sigma_p(a) = a^p$for a inF(α^{p^t}) is an automorphism of F(α^{p^t}), Conxequently, $(\sigma_p)^t$ is also an automorphism of F(α^{p^t}), and $(\sigma_p)^t(a) = a^{p^t}$. Since an automorphism of F(α^{p^t}) is an onto map, there is β belongs to F(α^{p^t}) such that $(\sigma_p)^t(\beta) = \alpha^{p^t}$. But then $\beta^{p^t} = \alpha^{p^t}$, and we saw that α was only zero of $x^{p^t} - \alpha^{p^t}$, so we must have β = α. Since β belongs to F(α^{p^t}), we have Fα) = F$\left(\alpha^{p^t}\right)$, then F(α) is seperable over F.

Therefore, α is seperable over F and t =0. We have shown that α belongs to F is seperable over F.Then E is a sepearble extension of F.

Note : For finite extensions E of perfect fields F, we have [E : F] = [E : F]

Primitive Element Theorem :

A primitive element for an extension field E of field F is an element α of E such that $E = F(\alpha)$, or in other words, such that E is generated by α over F. This means that every elements of E can be written as a quotient of two polynomials in α with coefficients from F.

If the extension E/F admits a primitive elements, then E is either a finite extension of F, in case $\alpha$is an algebraic element of E over F or E is isomorphic to the field of rational functions over F in one indeterminate, if α is a transcendental element of E over F.

The primitive element theorem answers the question of which finite field extension has primitive elements. It is not, for example, immediately obvious that if one adjoins to the field Q of rational numbers roots of both polynomials

$x^2 - 2$ and $x^2 - 3$ say α and β respectively, to get a field K = Q (α, β) of degree 4 over Q, that K is $Q(\gamma)$ for a primitive element γ. One can in fact check that with $\gamma = \alpha + B$ and we can write α, β and $\alpha\beta$ in terms of γ with integer co-efficients. Taking these as a system of linear equations., one can solver for α and β over Q which implies that this choice of γ is indeed a primitive element in this example. The general primitive element theorem states.

The field extension E over F is finite and has a primitive element if and only if there are only finitely many intermediate fields K with $F \leq K \leq E$. In this form the theorem is rarely used. Another form is given below.

Theorem 7.10 : Primitive Element Theorem :

Let E be a finite separable extension of a field F. Then there exists $\alpha \in E$ such that E = F(α). That is, a finite separable extension of a field is a simple extension.

Proof: We already know that there is no problem if F is a finite field. Suppose that E is finite extension of an in finite field. We will prove the result for F(α, β). The general case easily follows when we use mathematical induction. Let f(x) and g(x) be the minimal polynomials of α and β respectively. Let K be the field in which both f(x) and g(x) split. Suppose that f(x) have zeroes $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ inK and g(x) have zeros $\beta = \beta_1, \beta_2, ..., \beta_n$ in K. All of these zeros have multiplicity 1, since E is separable over F, Since F is infinite, we can find an a in F such that.

$$a \neq \frac{(\alpha_i - \alpha)}{(\beta - \beta_j)}$$ for all iand j with j $\neq$ i

Therefore, $a(\beta - \beta_j) \neq \alpha_i - \alpha.$

Let $\nu = \alpha + a\beta$

Then $\nu = \alpha + a\beta \neq \alpha_i + a\beta_j$

Hence $\nu - a\beta_j \neq \alpha_i$ for all i, j with j$\neq$1

Define h(x) belongs to F(ν)[x] by h(x) = f (ν- a x). Then

h(β) = = f(α) = 0 However,

$h(\beta_j) \neq 0$ for j ≠ 1

Hence, h(x) and g(x) have a single common factor in $F(\gamma)$ [x] : that is, the irreducible polynomial β over F(ν) must be linear, since β is the only zero common to both g (x) and h (x).

So $\beta \in F(\nu)$ and $\alpha = \nu - \alpha\beta$ is in $F(\nu)$.

Hence F(ν) = F(r)

Corollary 7.11 : A finite extension of a field of characteristic zero is a simple extension.

Exercise 7.12 :

1) Show that if $\alpha, \beta \in \overline{F}$ are both separable over F, then $\alpha \pm \beta, \alpha\beta$ and α/β if $\beta \neq 0$ are all separable over F.

Ans: Since α, β are separable over F,

$F(\alpha), F(\beta)$ are separable over F,

Also $F \leq F(\alpha) \leq F(\alpha, \beta)$

Now $\{F(\alpha) : F\} = [F(\alpha) : F]$

$\{F(\beta) : F\} = [F(\beta) : F]$

Since β is separable over F, it is separable over F(α), *i.e.*, $F(\alpha, \beta)$ is a separable extension of F (α).

$\{F(\alpha, \beta) : F(\alpha)\} = [F(\alpha, \beta) : F(\alpha)]$

Now $\{F(\alpha, \beta) : F\} =$

$\{F(\alpha, \beta) : F(\alpha)\}\{F(\alpha) : F\}$

$=$

$[F(\alpha, \beta) : F(\alpha)]\,[F(\alpha) : F]$

$= [F(\alpha, \beta) : F]$

i.e., $F(\alpha, \beta)$ is separable over F

i.e., $\alpha \pm \beta, \alpha\beta$ and α / β for $\beta \neq 0$ are separable over F.

2) Show that $\{1, y, \ldots\ldots\ldots y^{n-1}\}$ is a basis for $Z_p(y)$ over $Z_p(y^p)$, where y is an indeterminate.

Proof Let $\alpha = y$ hence $\alpha^p = y^p$

$\therefore y^p$ satisfies $x^p - y^p$ over $Z_p(y^p)$

So y is algebraic over $Z_p(y^p)$

Now $x^p - y^p = (x-y)^p$ since p is the characteristic of the field.

Therefore, y is a zero of multiplicity p. Since $x^p - y^p$ of degree p, it follows that y is the only zero and y $\notin Z_p(y^p)$. So $x^p - y^p$ is irreducible over $Z_p(y^p)$.

i.e., irr (y $\notin Z_p(y^p)$)= $x^p - y^p$

So {1, y…. y^{p-1}} form a basis of $Z_p(y)$ over $Z_p(y^p)$

3) Let E be a finite field of order p^n

a) Show that the Frobenius automorphism σ_p has order n

b) Deduce from part (a) that G (E/ Z_p) is cyclic of order n with generator σ_p.

Proof :

a) $\sigma_p : E \to E$ is defined by

$\sigma_p(a) = a^p$ for all $a \in E$

$\sigma_p{}^n(a) = a^{p^n} = e$

i.e., $a^{p^n} = I$, the identity automorphism of E.

Hence ord $(\sigma_p) = m$ divides n

Every element of E satisfy the polynomial $x^{p^n} - x.$ If σ_{pr} were identity for

$1 \le r \le n$, then we have every element of E satisfies $x^{p^r} - x.$

i.e., $x^{p^r} - x = 0$ has more than p^r solutions, a contradiction.

Hence ord $(\sigma_p) = n$

b) E is a finite extension of Z_p and is a splitting field

Hence $|G(E / Z_p)| = \{E : F\}$. Also $\{E : F\} = [E : F]$

So $| G(E / Z_p)| = n$

Now σ_p is of order n.

Hence G (E / Z_p) is cyclic of order n with generator σ_p.

GALOIS THEORY

Definition 8.1 : A finite extension K of F is a finite normal extension of F if K is a separable splitting field over K.

Definition 8.2 : If K is a finite normal extension of a field F, the G(K / F) is the Galois group of K over F.

Note: If E is a normal extension of F then [E:F]={E:F}=|G(E/F)|

The Fundamental Theorem of Galois Theory is one of the most elegant theorems in Mathematics. Figure 8.1 pictures the lattice of subgroups of the group of field automorphism of $Q(\sqrt[4]{2}, i)$. The integer along an upward lattice line from a group $H_1$to a group H_2 is the index of H_1 in H_2Figure 8.2 shows the lattice of subfields of $Q(\sqrt[4]{2,i})$. The integer along an upward line from a field K_1 to a field K_2 is the degree of K_2 over K_1.

Note that the lattice in Fig 8.2 is the lattic of Fig.8.1 turned upside down. This is one of many relationships between these two lattices. The Fundamental Theorem of Galois Theory relates the lattice of subfields of an algebraic extension E of a field F to the subgroup structure of the group of automorphisms of E that send each element of F to itself.

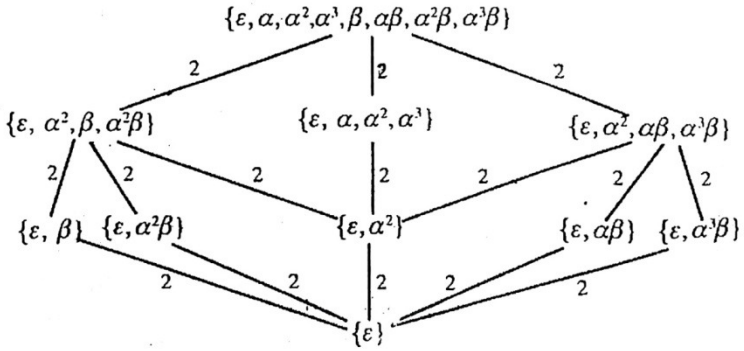


Figure 8.1

Figure 8.1 : Lattice of subgroups of the group of field automorphisms of $Q(\sqrt[4]{2}, i)$ where $\alpha : i \to$ i and $\sqrt[4]{2} \to i\sqrt[4]{2}, \beta : i \to -i \; and \; \sqrt[4]{2} \to \sqrt[4]{2}$.

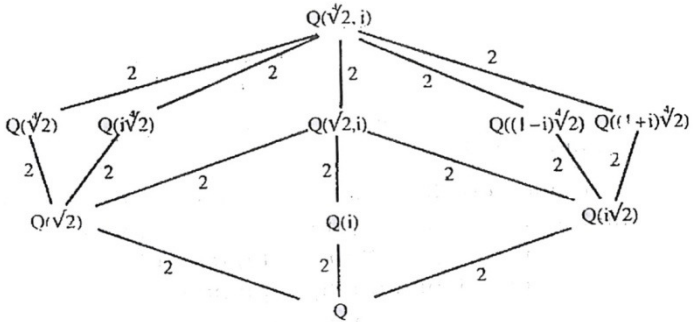


Figure : 8.2 : Lattice of subfields of $Q(\sqrt[4]{2}, i)$.

Examples 8.3

1) Consider the extension $Q(\sqrt{2})$ of Q. Since $Q(\sqrt{2}) = \{a + b\sqrt{2} / a,b \in Q\}$ and any automorphism ϕ of $Q(\sqrt{2})$ is completely determined by $\phi(\sqrt{2})$. Thus

$2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = (\phi(\sqrt{2}))^2$ and therefore, ϕ of $Q(\sqrt{2}) = \pm\sqrt{2}$. This proves that the group $G(Q(\sqrt{2})/Q)$ has two elements, the identity mapping and mapping that sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$

2) Consider the extension $Q(\sqrt[3]{2})$ of Q. An automorphism ϕ of $Q(\sqrt[3]{2})$ is completely determined by $\phi(\sqrt[3]{2})$. As earlier, we see that $\phi(\sqrt[3]{2})$ must be a cube root of 2. Since is a subset of the real number and $\sqrt[3]{2}$ is the only real cube root of 2, we must have $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus ϕ is the identity automorphism and $G(Q(\sqrt[3]{2})/Q)$ has only one element. The fixed field of G $(Q(\sqrt[3]{2})/Q)$ is $Q(\sqrt[3]{2})$.

3) Consider the extension $Q(\sqrt[4]{2}, i)$ of Q(i). Any automorphism ϕ of $Q(\sqrt[4]{2}, i)$ fixing Q(i) is completely determined by $\phi(\sqrt[4]{2},)$ .Since.

$$2 = \phi(2) = \phi(\sqrt[4]{2})^4 = \phi(\sqrt[4]{2})^4$$

We see that $\phi(\sqrt[4]{2})$ must be a fourth root of 2. Thus, there are utmost four possible automorphisms of $Q(\sqrt[4]{2}, i)$ fixing Q(i). If we define an automorphism α so that $\alpha(i) = i$ and

$\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$, then $\alpha \in G(Q(\sqrt[4]{2}, i)$ / Q(i) and α has order 4. Thus $G(Q(\sqrt[4]{2}, i)/Q(i)$ is a cyclic group of order 4. The fixed field of $\{\varepsilon, \alpha^2\}$ is Q $(\sqrt{2}, i)$, where ε is the identity automorphism. The lattice of subgroups of $G(Q(\sqrt[4]{2}, i)/Q(i)$ and the lattice of subfields of $Q(\sqrt[4]{2}, i)$ containing Q(i) are shown in figure 8.3.

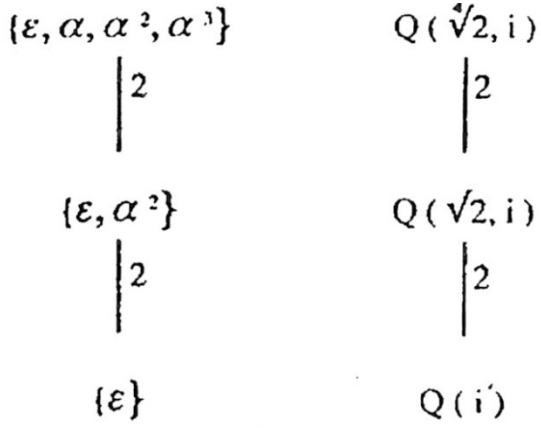


Fig. 8.3

4) Consider the extension $Q(\sqrt{3}, \sqrt{5})$ of Q.

Since

$Q(\sqrt{3},\ \sqrt{5})=[a+\sqrt{3}b+\sqrt{5}c+\sqrt{3}\ \sqrt{5}d\ /\ a,b,c,d\in Q)$ any automorphism ϕ of $Q(\sqrt{3},\ \sqrt{5})$ is completely determined by the two values $\phi\ (\sqrt{3})\ and\ \phi(\sqrt{5})$. This time there are four automorphisms.

ε	α	β	$\alpha\beta$
$\sqrt{3}\to\sqrt{3}$	$\sqrt{3}\to-\sqrt{3}$	$\sqrt{3}\to\sqrt{3}$	$\sqrt{3}\to-\sqrt{3}$
$\sqrt{5}\to\sqrt{5}$	$\sqrt{5}\to\sqrt{5}$	$\sqrt{5}\to-\sqrt{5}$	$\sqrt{5}\to-\sqrt{5}$

$G(Q(\sqrt{3}\sqrt{5})/Q)$ is isomorphic to $Z_2\oplus Z_2$. The fixed field of $\{\varepsilon,\alpha\}$ is $Q(\sqrt{5})$ fixed field of $\{\varepsilon,a\beta\}$ is $Q(\sqrt{15})$ The lattice of subgroups of G (Q($\sqrt{3},\sqrt{5})/Q)$ and the lattice of subfields of $Q(\sqrt{3},\sqrt{5})$ are shown in figure 8.4.

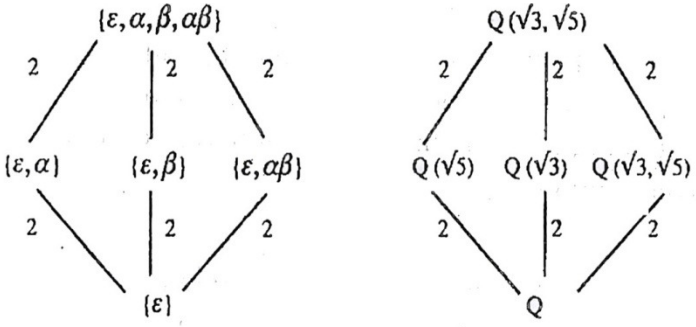


figure 8.4.

8.4 Theorem : Let K be a finite normal extension of F, and let E be an extension of F, where $F \leq E \leq K \leq \bar{F}$. Then K is a finite normal extension of E, and $G(K/E)$ is precisely the subgroup of $G(K/F)$ consisting of all those automorphisms that leave E fixed. Moreover, two automorphisms σ and τ in $G(K/F)$ induce the same isomorphism of E onto a subfield of $\bar{F}$ if and only if they are in the same left coset of $G(K/E)$ in $G(K/F)$.

Proof If K is the splitting field of a set $\{f_i(x)/i \in I\}$ of polynomials in $F[x]$, then K is the splitting field over E of this same set of polynomials viewed as elements of $E[x]$. Theorem shows that K is separable over E, since K is separable over F. Thus K is a normal

extension of E. This establishes our first contention.

Now every element of $G(K/E)$ is an automorphism of K leaving F fixed, since it even leaves the possibly larger field E fixed. Thus $G(K/E)$ can be viewed as a subset of $G(K/F)$. Since $G(K/E)$ is a group under function composition also, we see that $G(K/E) \leq G(K/F)$.

Finally, for σ and τ in $G(K/F)$, σ and τ are in the same left coset of $G(K/E)$ if and only if $\tau^{-1}\sigma \in G(K/E)$ or if and only if $\sigma = \tau\mu$ for $\mu \in G(K/E)$. But if $\sigma = \tau\mu$ for $\mu \in G(K/E)$, then for $\alpha \in E$, we have

$$\sigma(\alpha) = (\tau\mu)(\alpha) = \tau(\mu(\alpha)) = \tau(\alpha),$$

since $\mu(\alpha) = \alpha$ for $\alpha \in E$. Conversely, if $\sigma(\alpha) = \tau(\alpha)$ for all $\alpha \in E$, then

$$(\tau^{-1}\sigma)(\alpha) = \alpha$$

for all $\alpha \in E$, so $\tau^{-1}\sigma$ leaves E fixed, and $\mu = \tau^{-1}\sigma$ is thus in $G(K/E)$.

Theorem 8.5 (Main Theorem of Galois Theory)

Let K be a finite normal extension of a field F, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup

of $G(K/F)$ leaving E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ:

1. $\lambda(E) = G(K/E)$.

2. $E = K_{G(K/E)} = K_{\lambda(E)}$.

3. For $H \leq G(K/F)$, $\lambda(K_H) = H$.

4. $[K : E] = \lambda(E)$ and $[E : F] = (G(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $G(K/F)$.

5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, then $G(E/F) \cong G(K/F)/G(K/E)$.

6. The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.

Proof: We have really already proved a substantial part of this theorem. Let us see just how much we have left to prove.

Property 1 is just the definition of λ found in the statement of the theorem.

For Property 2, Theorem shows that $E \leq K_{G(K/E)}$.

Let $\alpha \in K$, where α does not belong to E. Since K is a normal extension of E, by using a conjugation isomorphism and the Isomorphism Extension Theorem, we can find an automorphism of K leaving E fixed and mapping α onto a different zero of irr(α, F). This implies that $K_{G(K/E)} \leq E$, so $E = K_{G(K/E)}$. This disposes of Property 2 and also tells us that λ is one to one, for if $\lambda(E_1) = \lambda(E_2)$, then by Property 2, we have $E1 = K_{\lambda(E_1)} = K_{\lambda(E_2)} = E2$.

Turning to Property 3, we must show that for $H \leq G(K/F)$, $\lambda(K_H) = H$. We know that $H \leq \lambda(K_H) \leq G(\mathrm{K/F})$. Thus what we really must show is that it is impossible to have H a *proper* subgroup of $\lambda(K_H)$. We shall suppose that $H < \lambda(K_H)$ and shall derive a contradiction. As a finite separable extension, $K = K_H(\alpha)$ for some $\alpha \in K$, by Theorem. Let $n = [K:K_H] = \{K:K_H\} = |G(K/K_H)|$.

Then H < G(K/KH) implies that |H | < |G(K/KH)|= n. Thus we would have to have H < [K: KH] = n. Let the elements of H be σ1, , σ|H|, and consider the polynomial $f(x) = \prod_{i=1}^{|H|}\big(x - \sigma_i(\alpha)\big)$. Then f (x) is of degree |H | < n. Now the coefficients of each power of x in f (x) are symmetric expressions in the $\sigma_i(\alpha)$. For example, the coefficient of x power |H |–1 is

$-\sigma_1(\alpha) - \sigma_2(\alpha) -\cdot \cdot \cdot- \sigma_{|H|}(\alpha)$. Thus these coefficients areinvariantundereachisomorphism $\sigma_i \in H$, since if

$\sigma \in H$,then$\sigma\ \sigma_1, \cdots, \sigma\sigma_{|H|}$is again the sequence $\sigma_1, , \sigma_{|H|}$, except for order, H being a group. Hence $f(x)$ has coefficients in K_H, and since some $\sigma_i$is ι, we see that some $\sigma_i(\alpha)$ is α, so $f(\alpha) = 0$.Therefore, we would have$\deg(\alpha, K_H) \leq |H| < n$
$= [K : K_H] = [K_H(\alpha) : K_H]$.This is impossible. Thus we have proved Property 3.

Property 4 follows from [K:E] = {K:E},[E:F] = {E:F} and by thorem 8.4.

We turn to Property 5 : Every extension E of F,$F \leq E \leq K$, is separable over F , by Theorem. Thus E is normal over F if and only if E is a splitting field over F . By the Isomorphism Extension Theorem, every isomorphism of E onto a subfield of F leaving F fixed can be extended to an *automorphism* of K , since K is *normal* over F . Thus the automorphisms of $G(K/F)$ induce all possible isomorphisms of E ontoasubfield of $\bar{F}$leaving F fixed. By Theorem, this shows that E is a splitting field over F , and hence is normal over F , if and only if for all $\sigma \in G(K/F)$ and $\alpha \in E$,$\sigma(\alpha) \in E$.

By Property 2, E is the fixed field of $G(K/E)$, so $\sigma(\alpha) \in E$ if and only if for all $\tau \in G(K/E)$, $\tau(\sigma(\alpha)) = \sigma(\alpha)$.

This in turn holds if and only if $(\sigma^{-1}\tau\sigma)(\alpha) = \alpha$ for all $\alpha \in E, \sigma \in G(K/F)$, and $\tau \in G(K/E)$. But this means that for all $\sigma \in G(K/F)$ and $\tau \in G(K/E)$, $\sigma^{-1}\tau\sigma$ leaves every element of E fixed, that is, $(\sigma^{-1}\tau\sigma) \in G(K/E)$.

This is precisely the condition that $G(K/E)$ be a normal subgroup of $G(K/F)$.

It remains for us to show that when E is a normal extension of F, $G(E/F) \cong G(K/F)/G(K/E)$. For $\sigma \in G(K/F)$, let σ_E be the *automorphism* of E induced by σ (we are assuming that E is a *normal* extension of F). Thus $\sigma_E \in G(E/F)$. The map $\varphi: G(K/F) \to G(E/F)$ given by $\varphi(\sigma) = \sigma_E$ for σ $G(K/F)$ is a homomorphism. By the Isomorphism Extension Theorem, every automorphism of E leaving F fixed can be extended to some automorphism of K; that is, it is τ_E for some $\tau G(K/F)$. Thus φ is onto $G(E/F)$. The kernel of φ is $G(K/E)$. Therefore, by the Fundamental Isomorphism Theorem,

$G(E/F) \cong G(K/F)/G(K/E)$. Furthermore, this isomorphism is anaturalone.

Galois Group of a polynomial

If f(x)$\in$ F[x] is such that every irreducible factor of f(x) is separable over F, then the splitting field K of f(x) over F is a normal extension of F. The Galois group G(K/F) is the galois group of the polynomial f(x) over F.

Proposition : Let K be an extension field of F and let f(x) be a polynomial in F[x]. Then any element of G (K/F) defines permutation of the roots of f(x) that lie in K.

Proposition : Let f(x) be a polynomial in F[x] with no repeated roots and let K be a splitting field for f(x) over F, If $\phi: F \to L$ is a field isomorphism that maps f(x) to g(x) in L[x] and E is a splitting field for g(x) over L, then there exist exactly [K:F] isomorphism.

$\theta: K \to E$ such that θ (a) = ϕ (a) for all a in F.

Proposition : Let F be a field, let f(x) be a polynomial in F[x], and let K be a splitting field for f(x) over F. If f(x) has no repeated roots, then.

$$|G(K/F)| = [K : F]$$

Proposition : Let F be a finite field and let K be an extension of F with [K:F]=m. Then G(K/F) is cyclic group of order m.

In this proposition, if we take $F = Z_p$, where p is a prime number, and K is an extension of degree m, then the generator of the cyclic group G(K/F) is the automorphism $\phi: K \to F$ defined by $\phi(x) = x^p$ for all x in K. This automorphism is called the Frobenius automorphism of K.

Problems :

1. Determine the group of all automorphism of a field with 4 elements.

Solution : The automorphism group consists of two elements. The identity mapping and the Frobenius automorphism. We know upto isomorphism there is only one field with 4

elements. Since x^2+x+1 is irreducible over Z_2. This field with 4 elements can be constructed $F = Z_2[x] / < x^2 + x + 1>$.Letting a be the coset of x, we have F={0, 1, a, 1+a} Any automorphism of F must leave 0 and 1 fixed, so only possibility for an automorphism other than the identity is to interchange a and 1+a since $x^2+x+1 \equiv 0$, we have $x^2 \equiv -x-1 \equiv x+1$, so $a^3 = 1+a$ and $(1+a)^2 = 1 + 2a + a^2 = a$. Thus the functions that fixes 0 and 1 while interchanging a and 1+a is in fact the Frobenius automorphism of F.

2. Find the Galois group over Q of the polynomial $x^2 - 2$.

Solution : We know that the splitting field of the polynomial x^2-2 has degree 2 over Q, and so the Galois group must be cyclic of order 2.

3. Find the Galois groups of x^3-2 over the fields Z_5 and Z_{11}

Solution : The polynomial is not irreducible over Z_5, since it factors as $x^3-2 = (x+2)(x^2-2x-1)$. The

quadratic factor will have a splitting field of degree 2 over Z_5, so the Galois group is cyclic of order 2.

A search in Z_{11} for roots of x^3-2 yields one and only one x = 7. Then x^3-2 can be factored as $x^3-2 = (x-7)(x^2+7)(x^2+7x+5)$, and the second factor must be irreducible. The splitting field has degree 2 over Z_n and can be described as $Z_n[x] / < x^2 + 7x + 5 >$. Thus the Galois group in cyclic of order 2

4. Find the Galois group of x^4-1 over the field Z_n

Solution : We need to find the splitting field of x^4-1 over Z_n.

We have $x^4-1 = (x-1)(x+1)(x^2+1)$. A quick check of ± 2 and ± 3 shows that they are not roots of x^2+1 over Z, so x^2+1 is irreducible over Z_7. To obtain the splitting field we must adjoin a root of x^2+1, so we get a splitting field

$Z_7[x] / \langle x^2+1 \rangle$ of degree 2 over Z_7. It follows that the Galois group of x^4-1 over Z_7 is cyclic of order 2.

5. Find the Galois group of x^3-2 over the field Z_7.

Solution : In this case, x^3-2 has no roots in Z_7, so it is irreducible. We first adjoin a root a of x^3-2 to Z_7., The resulting extension $Z_7(a)$ has degree 3 over Z_7, so it has $7^3 = 343$ elements, and each elements is a root of the polynomial $x^{343}-x$. Let b be a generator of the multiplicative group of the extension.Then $(b^{114})^3 = b^{342} = 1$, showing that $Z_7(a)$ contains a nontrivial cube root of 1. It follows that x^3-2 has three distinct roots in $Z_7(a)$ a, ab^{114} and ab^{224}, so therefore $Z_7(a)$ is a splitting field for x^3-2 over Z_7. Since the splitting field has degree 3 over Z_7 it follows that the Galois group or the polynomials is cyclic of order 3.

CYCLOTOMIC EXTENSIONS

The complex zeros of x^n-1 are 1, ω, ω^2, ω^{n-1} where $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$ Thus, the splitting field of x^n-1 over Q is $Q(\omega)$.This field is called the n^{th} cyclotomic extension of Q, and the irreducible factors of

x^n-1 over Q are called the cyclotomic polynomials.

Since ω generates a cyclic group of order n under multiplication, we know that the generators of $<\omega>$are the elements of the form ω^k where $1 \le k \le$ n and

gcd (n, k) =1. These generators are called the primitive n^{th} roots of unity, where by $\phi(n)$.we mean Euler's phifunction, which denotes the number of positives integers less than n and relatively prime to n. The polynomials whose zeros are the $\phi(n)$ primitive n^{th} roots of unity have a special name, cyclotomic polynomial.

Definition 9.1. For any positive integer n, let $\omega_1, \omega_2, \ldots\ldots\ldots \omega_{\phi(n)}$ denote the primitive n^{th} roots of unity. The n^{th} cyclotomic polynomial over Q is the polynomial

$$\phi_n \text{ (x)} = (x-\omega_1)\ (x-\omega_2), \ldots\ldots, \ (x-\omega_{\phi(n)})$$

ϕ_n (x) is monic and has degree $\phi(n)$

Example 9.2 : $\phi_1(x) = x-1$ since 1 is the only zero of x – 1, $\phi_2(x) = x+1$ since the zeros of x^2-1 are 1 and – 1 and – 1 is the only primitive root. $\phi_3(x) = (x-\omega)\ (x-\omega^2)$ where

$\omega = \cos(2\pi/3) + i \sin(2\pi/3)$

$\phi_3(x)$ can be written as $x^2 + x + 1$.

Now zeros of $x^4 - 1$ are ± 1 *and* $\pm$ i and only i and – i are primitive,

$$\phi_4(x) = (x-i)\ (x+i) = x^2 + 1.$$

Theorem 9.3 : For every positive integer n, x^n-1 = $\prod_{d/n} \phi_d(x)$ where the product runs over all positive divisors d of n.

Proof : Since polynomials on both sides are monic, it suffices to show that they have the sane zeros and all zeros have multiplicity 1. Let $\omega = \cos(2\pi / n) + i \sin(2\pi / n)$. Then $<\omega>$is a cyclic group of order n and

$<\omega>$contains all the roots of unity. We know that for each j, the order of w_j, divides n so that $(x - w^j)$ appears as a factor in$\phi_{(w^j)}$. Conversely, if $x - \alpha$ is a linear factor of $\phi_d(x)$ for some divisor d of n, then $\alpha^d = 1$ and therefore $a^n = 1$. Thus, $x - a$ is a factor of x^n-1. Finally, since no zero of x^n-1 can be a zero of $\phi_d(x)$ for two different d's the result is proved.

Theorem 9.4 : For every positive integer n, $\phi_n(x)$ has integer coefficients.

Theorem 9.5 : The cyclotomic polynomials $\phi_n(x)$ are irreducible over Z.

Theorem 9.6 : Let ω be a primitive n^{th} root of unity. Then $G(Q(\omega)/Q)$ is isomorphic to the group G_n which is the group consisting of elements of Z_n

relatively prime to n under multiplication module n. This group has $\phi(n)$ elements and is abelian.

Proof : Since 1, $\omega, \omega^2, \ldots\ldots \omega^{n-1}$ are all the n^{th} roots of unity, $\phi(\omega)$ is the splitting field of $x^n - 1$ over ϕ. For each k in G_n, ω^k is a primitive n^{th} root of unity, and by an earlier result, there is a field automorphism of $\phi(\omega)$, which we denote by ϕ_k that carries ω to ω^k and acts as the identity on Q. Moreover, there are all the automorphism of $\phi(\omega)$, since any automorphism must map a primitive n^{th} root of unity to a primitive n^{th} root of unity. Next, observe that for every r,s $\in G_n$

$$(\phi_r \phi_s)(\omega) = \phi_r(\omega^8) = (\phi_r(\omega)^8) = (\omega^r)^5 = \omega^{rx} = \phi_{rs}(\omega)$$

This shows that the mapping from G_n onto $G(Q(\omega)/Q)$ given by

$k \to \phi_k$ is a group homomorphism. Clearly the mapping is an isomorphism since

$\omega^r \neq \omega^s$ when r, s $\in G_n$ and $r \neq s$

For example, let $\alpha = \cos(2\pi/9) + i\sin(2\pi/9)$ and $\beta = \cos(2\pi/15) + i\sin(2\pi/15)$. Then

$G(Q(\alpha)/Q) \approx G_9 \approx Z_6$ and $G(Q(\beta)/Q) \approx G_{15} \approx Z_4 \oplus Z_6$

Constructible polygons

Our aim is to determine which regular n-gons are constructible with compass and a straightedge. We know that a regular n-gon is constructible if and only if $\mathrm{Cos}(2\pi/n)$ is a constructible real number.

Let $\xi = \cos 2\pi/n + i \sin 2\pi/n$

Then $\xi + 1/\xi = 2\cos 2\pi/n.$

Thus by a previous result we can conclude that the regular n-gon is constructible only if $\xi + 1/\xi$ generates an extension of Q of degree a power of 2.

If K is the splitting field of x^n-1over Q, then [K, Q] = $\phi(n)$, by the Theorem 9.6 If $\sigma \in G(K/Q)$ and $(\xi) = \xi^r$. then

$$\sigma(\xi + 1/\xi) = \xi^r + (1/\xi)^r = 2\cos 2\pi r/n$$

But for 1< r < n, we have 2cos $(2\pi r/n) = 2\cos(2\pi/n)$ only in the case that r = n – 1. Thus the only elements of G(K/Q), carrying $(\xi + 1/\xi)$ onto itself are the identity automorphism and the automorphism τ, with $\tau(\xi) = \xi^{n-1} = 1/\xi$. This shows that the subgroup of G(K/Q) leaving $Q(\xi + 1/\xi)$ fixed is of order 2. So by Galois theory.

Hence, $[Q(\xi + 1/\xi): \phi] = \phi(n)/2.$

Theorem 9.7 : The regular n-gon is constructible only if $\phi(n)/2$, and therefore also $\phi(n)$, is a power of 2.

Theorem 9.8 : The regular n-gon that might be constructible are those where the odd prime dividing n are Fermat primes whose squares do not divide n.

Proof : We know that the regular n-gon is constructible only if $\phi(n)/2$, and therefore also $\phi(n)$, is a power of 2. Let $n = 2^{\nu} P_1^{s_1} P_2^{s_2} \cdots P_l^{s_l}$,

where p_i are the distinct odd primes dividing n, then.

$$\phi(n)=2^{\nu-1}\,p_1^{\,s_1-1}\,p_2^{\,s_2-1}.....p_l^{\,s_1-1}(p_1-1).....(p_l-1)$$

If $\phi(n)$ is to be power of 2, then every odd prime dividing n must appear only to the first power and must be one more than a power of 2. Thus we must have each $p_i = 2^m+1$ for some m.

Since – 1 is a zero of $x^q + 1$ for q an odd prime, x + 1 divides $x^q + 1$ for q an odd prime. Thus if m = q u, where q is an odd prime, than $2^m + 1 = (2^u)^q + 1$ is divisible by $2^u + 1$. Therefore, for $p_i = 2^m + 1$ to be prime, it must be that m is divisible by 2 only, so p_i has to have the form

$p_i = 2^{(2^k)}+1$. a Fermat prime

Fermat conjectured that these numbers $2^{(2^k)}+1$ prime for all non negative integers k. But it is proved that this is true only for k=0,1,2,3 and 4.

Theorem 9.8 : Every element in$[Q(\xi+1/\xi)]$, in particular $\text{Cos}(2\pi/n)$ is constructible. Hence the

regular n-gon, where $\phi(n)$ is a power of 2 are constructible.

Proof : We saw that $[Q(\xi+1/\xi):Q]=\phi(n)/2.$ Suppose now that $\phi(n)$ is a power of 2. Let E be $Q(\xi+1/\xi).$

We saw that $[Q(\xi+1/\xi)$ is the subfield of K = Q (ξ) left fixed by $H_1=\{1,\tau\}$ where τ is the identity element of G(K/Q) and $\tau(\xi)=1/\xi.$ By Sylow theory, there exist additional subgroups H_j of order 2^j of G $(Q(\xi)/Q)$ for j = 0, 2, 3, …s such that

$\{e\}$ = H_0< H_1< ……. <H_s = G $(Q(\xi)/Q)$

By Galois theory,

$Q=K_{H_8}<K_{Hs-1}<$ …… < $K_{H1}=Q(\xi+1/\xi).$

and $[K_{Hi-1}:K_{Hi}]=2.$ Note that $(\xi+1/\xi)\in R, so\ Q(\xi+1/\xi)\subset R.$

We proved earlier that if a is constructible, then $\sqrt{a}$ is also constructible.

We have $K_{H_{j-1}} = K_{H_j}(\alpha_j)$, where $\alpha_j$is the zero of the quadratic equation. Hence we can see that every element in $(Q(\xi+1)/\xi)$, in particular cos $(2\pi/n)$is constructible.Hence regular n-gons where $\phi(n)$ is a power of 2 are constructible.

Theorem : The regular n-gon is constructible with a compass and straightedge if and only if all the odd primes dividing n are Fermat primes whose squares do not divide n.

Example 9.9 : The regular 7 – gon is not constructible, since 7 is not a Fermat prime. Similarly the regular 18-gon is not constructible. The regular 60-gon is constructible, since 60 = (2^2) (3) (5) and 3 and 5 are both Fermat primes.

INSOLVABILITY OF THE QUINTIC

Definition 10.1 : Let F be a field, and let f(x) $\in$ F[x]. We say that f(x) is solvable by radicals over F if f (x) splits in some extension F(a_1, a_2 ……..a_n) of F and there exist positive integers k_1, k_2 …..k_n such that

$a_1^{k_1} \in$ F and $a_i^{k_i} \in$ F(a_1, ……., a_{i-1}) for i = 2, 3, ……., n

So, a polynomial in F[x] is solvable by radicals if we can obtain all of its zeros by adjoining n^{th} roots (for various n) to F. In other words, each zero of the polynomial can be written as an expression involving elements of F combined by the operation of addition subtraction, multiplication, division and extraction of roots.

For example, consider $x^8 - 3$. Let $\omega = \cos(2\pi/8) + i \sin(2\pi/8)$. Then $x^8 - 3$ splits in $Q(\omega, \sqrt[8]{3})$, $\omega^8 \in Q$, and $(\sqrt[8]{3})^8 \in Q(\omega)$.

Thus $x^8 - 3$ is solvable by radicals over Q.

The problem of solving a polynomial equation for its zeros can be transformed into a problem about field extensions. At the same time, we can use the Fundamental Theorem of Galois Theory to transform a problem about field extensions into a problem about groups.

Definition 10.2 : We say that a group G is solvable if G has a series of subgroups.$\{e\} = H_0 \subset H_1 \subset ..... \subset H_k = G$, where, for each $0 \leq i \leq k$, H_i is normal in

H_{i+1} and H_{i+1}/H_i is Abelian.

Theorem 10.3 : Let F be a field of characteristic zero and let $a \in$ F. If E is the splitting field of $x^n - a$ over F, then the Galois group G (E / F) is solvable.

Proof : We first handle the case where F contains a primitive n^{th} root of unity ω. Let b be a zero of $x^n - a$,then all zeros of $x^n - a$ are b, $\omega b, \omega^2 b, ..., \omega^{n-1} b,$ and therefore E = F(b) In this case, we claim that G (E / F) is Abelian and hence

solvable. To see this, observe that any automorphism in G(E/F) is completely determined by its action on b. Also, since b is a zero of $x^n - a$, we know that any element of G (E / F) sends b to another zero of $x^n - a$. That is, any element of G (E / F) takes b to $\omega^i b$ for some i. Let ϕ *and* σ be two elements of G (E / F). Then since $\omega \in F$, ϕ *and* σ fix ω and ϕ (b) = $\omega^j b$ and $\sigma(b) = \omega^k b$ for some j and k.

Thus,

$$(\sigma\phi)(b) = \sigma(\phi(b)) = \sigma(\omega^j b) = (\omega^j)\sigma(b)$$

$$= \omega^j \omega^k b = \omega^{j+k} b,$$

Whereas,

$$(\phi\sigma)(b) = \phi(\sigma(b)) = \phi(\omega^k b) = \omega^k \phi(b)$$

$= \omega^k \omega^j = \omega^{k+j} b$, so that $\phi\sigma$ and $\phi\sigma$ agree on b and fix the elements of F. This shows that $\phi\sigma = \phi\sigma$ and therefore G(E/F) is Abelian.

Now suppose that F does not contain primitive n^{th} root of unity. Let ω be a primitive n^{th} root of unity and let b be a zero of $x^n - a$. Since ω

b is also a zero of $x^n - a$, we know both ω and ωb belong to E and therefore $\omega = \omega b / b$ is in E as well. Thus, $F(\omega)$ is contained in E, and $F(\omega)$ is the splitting field of $x^n - 1$ over F, Analogously to the case above, for any automorphisms ϕ and σ in

G ($F(\omega)$ / F) we have $\phi(\omega) = \omega^j$ for some j and $\sigma(\omega) = \omega^k$ for some k.

Then,

$$(\sigma\phi)(\omega)$$

$$= \sigma(\phi(\omega)) = \sigma(\omega^j) = (\sigma(\omega))^j = (\omega^k)^j$$

$$= (\omega^j)^k = (\phi(\omega))^k = \phi(\omega^k) = \phi(\sigma(\omega)) = (\phi\sigma)(\omega)$$

Since elements of G ($F(\omega)$ / F) are completely determined by their and action one ω, this shows that G($F(\omega)$ /F) is Abelian.

Because E is the splitting field of $x^n - a$ over $F(\omega)$ and $F(\omega)$ contains a primitive n^{th} root of unity, we know from the case we have already

done that G(F(ω)/F) is Abelian and by an earlier result, the series.

$\{e\} \subseteq G(E / F(\omega)) \subseteq G(E / F)$ is a normal series. Finally, since both G(E/F (ω)) and

$\frac{G(E/F)}{G(E/F(\omega))} = G(F(\omega) / F)$ are Abelian, G (E / F) is solvable.

Theorem 10.14 : Let F be a field of characteristic zero, and let $F \leq E \leq K \leq \overline{F}$, where E is a normal extension of F and K is an extension of by radicals. Then G(E / F) is a solvable group.

Theorem 10.15 : Let y_1, y_2, y_3, y_4, y_5 be independent transcendental real numbers over Q. The polynomial

$f(x) = \prod_{i=1}^{5} (x - y_i)$ is not solvable by radicals over F = Q (s_1, s_2, …..s_5) where s_i is the ith elementary symmetric function in y_1, y_2, …,y_5.

Let E = Q (y_1, y_2, y_3, y_4, y_5), and let $f(x) = \prod_{i=1}^{5} (x - y_i)$, Thus f(x) belongs to E[x].. Now the coefficients are

except possible for sign ,among the elementary symmetric functions in the y_i, namely

$$s_1 = y_1 + y_2 + \cdots + y_5,$$
$$s_2 = y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5,$$
$$\vdots$$
$$s_5 = y_1y_2y_3y_4y_5.$$

The coefficient of x^i in $f(x)$ is $\pm s_{5-i}$. Let $F = Q(s_1, s_2, \ldots, s_5)$; then $f(x)$ belongs to $F[x]$. Then E is the splitting field over F of $f(x)$. Since the $y_i$behave as indeterminatesoverQ,foreach$\sigma \in S_5$,thesymmetricgrouponfiveletters,σinducesanautomorphism $\bar{\sigma}$of E defined by $\bar{\sigma}(a) = a$ for $a \in Q$ and $\bar{\sigma}(y_i) = y_{\sigma(i)}$. *Since* $\prod_{i=1}^{5}$ $(x - y_i)$ is the same polynomial as $\prod_{i=1}^{5}$ $(x - y_{\sigma(i)})$,we have

$\bar{\sigma}(s_i) = s_i$ for each i, so $\bar{\sigma}$ leaves F fixed ,and hence $\bar{\sigma}$ element of G(E/F). Now S_5 has order 5!,so $|G(E/F)| \geq 5!$. Since the spilitting field of a polynomial of degree 5 over F has degree atmost 5! Over F, we see that $|G(E/F)| \leq 5!$. Thus $|G(E/F)| = 5!$, and the Galois group isomorphic to S_5 which is not solvable.

Example 10.16 : Consider $g(x) = 3x^5 - 15x + 5$. By Eisenstein's criterion g(x) is irreducible over Q. Since g (x) is continuous and g (-2) = - 61 and g (- 1) = 17, we know that g (x) has a real zero between -2 and -1. A similar analysis shows that g (x) also has real zeros between 0 and 1 and between 1 and 2.

Each of these real zeros has multiplicity one, as can verified by long divison

g (x) has no more than three real zeros, because Rolle's theorem guarantees that between each pair of real zeros of g (x) there must be a zero of $g^1(x)$. So, for g (x) to have four real zeros, g^1 (x) would have to have three real zeros, and it does not. Thus, the other two zeros of g (x) are non real complex numbers,

say a + bi and a-bi.

Let us denote the five zeros of g (x) by a_1, a_2, a_3,a_4, a_5 Since any automorphism of K= Q(a_1,a_2,a_3,a_4,a_5) is completely determined by its

act a on the a's and must permute a's, we know that G (K/Q) is isomorphic to a sub group of S_5, the symmetric group on five symbols. Since a1 is a zero of an irreducible polynomial of degree 5 over Q, we know that [Q (a1) : Q] = 5, and, therefore, 5 divides [K : Q]. Thus, the Fundamental Theorem of Galois Theory tells us that 5 also divides [G(K/Q)]. So by Cauchy's theorem, we know that G(K/Q) contains a 5-cycle. The mapping from C to C, sending a +b i to a – bi, is also an element of G(K/Q). Since this mapping fixes the three real zeros and interchanges the two complex zeros of g (x), we know that G(K / Q) contains a 2-cycle. But, the only subgroup of S_5 that contains both a 5-cycle and a 2-cycle is S_5. So G(K/Q) is isomorphic to S_5. Also S_5 is not solvable. Hence g(x) is not solvable by radicals.