International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Discussion about the Field Extension, Degree of Field Extension and Algebraic Extension

Vinit Chauhan[1], Nagesh Kumar Singh[2]

[1] NET (CSIR-JRF), M.Sc., Dr.B.R.Ambedkar University, Agra (U.P.) 282004 India

[2] NET, M.Sc., D.D.U. University, Gorakhpur (U.P.) 273009 India

Abstract: ***This paper is about the extension of field, a structure which equipped two binary operations and occupied some properties. In this discussion we are discussing simple field extension degree of field extension and algebraic extension.***

Keywords: Number field, function field, algebraic element, transcendental element, irreducible polynomial of an algebraic element, algebraic extension, Simple field extension, degree of a field extension, and compositum of fields.

1. Introduction

In our discussion of ring, we study a special class which we called a field. Field plays a central role in algebra. Due to the brilliant French mathematician Evariste Galois, which have served as guiding inspiration for algebra as it is today? In this paper will be devoted to a study of theory of field extension and also some discussion on Galois Theory.

2. Some examples of Fields

The main examples of fields that we consider are:
(1) Number fields: A number field F is a subfield of $\mathbb{C}$. Any such field contains the field Q of rational numbers.
(2) Finite fields: If K is a finite field, we consider $\psi : \mathbf{Z} \to K$, $\psi(1) = 1$. Since K is finite, $ker\ \psi$ is non zero, hence it is a prime ideal of $\mathbf{Z}$, say generated by a prime number p. Hence $\mathbf{Z}/\mathbf{Z}_p := F_p$ is isomorphic to a subfield of K. The finite field F_p is called the prime field of K.
(3) Function fields: Let x be an indeterminate and $\mathbb{C}(x)$ be the field of rational functions, i.e. it consists of p(x)/q(x) where p(x), q(x) are polynomials and q(x) is non zero. Let $f(x, y) \in \mathbb{C}[x, y]$ be an irreducible polynomial.
Suppose f (x, y) is not a polynomial in x alone and write

$$f(x, y) = y^n + a_1(x)y^{n-1} + \cdots + a_n(x), \quad a_i(x) \in \mathbb{C}[x].$$

By Gauss' lemma $f(x, y) \in \mathbb{C}[x, y]$ is an irreducible polynomial. Thus $(f(x, y))$ is a maximal ideal of $\mathbb{C}[x,y]/f(x, y)$ is a field. K is called the function field of the curve defined by $f(x,y) = 0$ in $\mathbb{C}^2$.

Characteristic of a field: Let R be a commutative ring with identity e.

3. Isomorphism

Define the ring homomorphism $f : \mathbf{Z} \to R$ by $f(n) = ne$. Then Ker f = (n) for some integer n. If n = 0, then $\mathbf{Z}$ is isomorphic to a subring of R. In this case we say that R has characteristic zero. If R is a domain then $\mathbf{Z}/(n)$ is a domain as it is isomorphic to a subring of R. Hence n is a prime number, say p. Therefore the finite field F_p is isomorphic to a subfield of R. In this case, we say that R has characteristic p. Thus any field F contains either an isomorphic copy of Q or F_p.

4. Field Extension and Irreducibility

Definition 4.1. (i) Let K be a subfield of a field F. We say F is an extension field of K. We also say that K is a base field. We also write this as F/K.
(ii) An element a ∈ F is called algebraic over K if there exists a nonzero polynomial $f(x) \in K[x]$ such that f (a) = 0. If every element of F is algebraic over K then we say that F is an algebraic extension of K.
(iii) An element a ∈ F which is not algebraic over K is called a transcendental element over K.

Example 4.2. It is known that the base e of the natural logarithm and π are transcendental over Q. Since $(\pi i)^2 = -\pi^2$, πi is a root of $x^2 - \pi^2 \in \mathbb{C}[x]$. Hence πi is algebraic over $\mathbb{C}$. However πi is not algebraic over Q. Thus the property of being algebraic depends upon the base field
Example 4.3. Let K be a finite field whose characteristic is a prime number p. Then K has a subfield F with p elements. Since K is finite, it is a finite dimensional F -vector space. If $dim_F K = n$ then K has p^n elements. If a ∈ K then the set $\{1, a, a^2, \ldots, a^n\}$ is linearly dependent. Let $b_0, b_1, \ldots, b_n \in F$, not all zero, so that $b_0 + b_1 a + \cdots + b_n a^n = 0$. Hence 'a' is a root of the nonzero polynomial $b_0 + b_1 x + \cdots + b_n x^n$. Therefore b is

algebraic over F and hence K/F is an algebraic extension.

Proposition 4.4. Let F/K be a field extension and $\alpha \in F$ be algebraic over K. Then there exists a unique monic irreducible polynomial $f(x) \in K[x]$ suchthat $f(\alpha) = 0$.

Proof. Define $\psi : K[x] \to F$ *by* $\psi(g(x)) = g(\alpha)$. Since ψ is a ring homomorphism and α is algebraic, $ker\ \psi = I$ is a nonzero ideal of $K[x]$. Since $K[x]$ is a PID and K[x]/I is isomorphic to a subfield of F, I is generated by an irreducible polynomial h(x) ∈ K[x]. If g(α) = 0 then $g(x) = h(x)h_1(x)$ for some polynomial $h_1(x) \in K[x]$. If g is irreducible, then $g = \alpha h(x)$ for some $\alpha \in K^{\times} = K \setminus \{0\}$. If g and h are taken to be monic, then g = h.

Definition 4.5. The irreducible monic polynomial in F [x] whose root is $\alpha \in K$ is denoted by $irr(\alpha, F)$ and it is called the irreducible monic polynomial of α over F. The degree of irr (α, F) is called the degree of α and it is written as $deg_F \alpha$.

Example 4.6. (i) $\sqrt{i} \in \bar{\square}$ Satisfy $f(x) = x^4 + 1 = 0$ .show that $\sqrt{f(x)} = irr(\sqrt{i}, Q)$ Consider the field $Q(i)$ = smallest field containing Q and i. Then $irr\ (\sqrt{i}, Q(i)) = x^2 - i$.

ii) Let p be a prime number and $\zeta_p = e^{2\pi i/p}$. Then $x^p - 1 = 0$ is satisfied by ζ_p. Since $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$ and $\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over Q, $irr(\zeta_p, Q) = \Phi_p(x)$.

Simple field extensions: Let K ⊂ F be a field extension. Let α, β ∈ F be transcendental. Define ψ : K[x] → F such that $\psi(g(x)) = g(\alpha)$. Then ker $\psi = \{0\}$. Thus K[x] ≅ K[α] and hence K (α) ≅ K (β) by an isomorphism σ such that σ(α) = β and $\sigma|_K = id_K$. The situation is quite diff erent for algebraic elements

Proposition 4.7. Let F ⊂ K be a field extension and α ∈ K be algebraic over F and $f(x) = irr\ (\alpha, F)$. Let $n = deg\ f$. Then
(i) $F[\alpha] = F(\alpha) \cong F[x]/(f(x))$. (ii) $dim_F F\ (\alpha) = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an F - basis of F (α).

Proof. Consider the substitution homomorphism
ψ : F [x] → F [α] such that $\psi(x) = \alpha, \psi|_F = id_F$
Then $ker\psi = (f(x))$ where $f(x) = irr(\alpha, F)$. Hence $F[x]/(f(x)) \cong F[\alpha]$. since $(f(x))$ is a maximal ideal, F [α] is a field, so F [α] = F (α).
Let g(α) ∈ F [α] and $g(x) = f(x)q(x) + r(x)$ where q, r ∈ F[x], and $degr(x) < degf(x)$) or r(x) = 0. Then g(α) = r(α). Thus F [α] is an F −vector space generated by $1, \alpha, \ldots, \alpha^{n-1}$ Where n = deg f (x). Suppose that $\sum_{i=0}^{n-1} a_i \alpha^i = 0$. If a_i are not all zero then $\sum_{i=0}^{n-1} a_i x^i$ is a nonzero polynomial of degree less than deg f (x) satisfied by α. This contradicts minimality of degree f(x). Thus $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an F - vector space basis of F [α]. Hence $dim_F F[\alpha] = deg\ irr(\alpha, F)$.

Proposition 4.8. Let K/F be a field extension and α ∈ K be algebraic over F. Then F (α)/F is an algebraic extension.
Proof. If β ∈ F (α) and $\beta \neq 0$ then $\{1, \beta, \beta^2, \ldots, \beta^n\}$ is a linearly dependent subset of F (α) since $dim_F F(\alpha) = n$. Hence there exist $a_0, a_1, \ldots, a_n \in$ F not all zero so that $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. Hence β is algebraic. Therefore $F(\alpha)/F$ is an algebraic extension.

Proposition 4.9. Let α, β ∈ K ⊇ F be algebraic over F. Then there exists an F-isomorphism ψ : F (α) → F (β) such that ψ(α) = β if and only if $irr(\alpha, F) = irr(\beta, F)$.
Proof. Let $f(x) = irr(\alpha, F)$ and $g(x) = irr(\beta, F)$. Then ψ (f (α)) = f (β) = 0. Thus g(x)|f (x). Since g, f are monic and irreducible, g(x) = f (x).

Conversely, suppose $irr(\alpha, F) = irr(\beta, F)$. Then F (α) ≅ F [x]/(f (x)) ≅ F (β) and the isomorphism are F -isomorphism. Hence F (α) and F (β) are F-isomorphic

Proposition 4.10. Let F ⊆ K, K′ be two field extensions of F. ψ : K → K′ be an F - isomorphism. Let α ∈ K be a root of $f(x) \in F[x]$.
Then (α) is a root of $f(x)$.

Example 4.11. (i) Let $f(x) = x^3 - 2 \in Q[x]$. By Eisenstein criterion $f(x)$ is irreducible over Q.
The roots of $f(x)$ are $\alpha, \alpha w, \alpha w^2$ where α is the real cube root of 2 and w is the complex cube root of 1. Thus the fields $Q(\alpha), Q(\alpha w), Q(\alpha w^2)$ $are Q$ −isomorphic.
(ii) Since $irr(i, \square) = x^2 + 1, \square[x]/(x^2 + 1) = \square(i) = \square$
iii) The polynomial $f(x) = x^2 + x + 1$ is irreducible over F_2. Hence $K = F_2[x]/(f(x))$ is a field which is a two dimensional F_2. −vector space. Hence K is a field with four elements.
(iv) The polynomial $g(x, y) = y^3 - x(x+1)(x-1)$ is irreducible in C(x)[y] by Eisenstein's criterion. Hence C(x)[y]/(g(x, y)) is a simple field extension of the function field C(x)

5. Degree of Field Extension

Definition 5.1. Let F ⊆ K be a field extension. The dimension of the

F -vector space K, denoted by [K: F] is called the degree of the field extension K/F.

For an algebraic element α ∈ K, $dim_F F(\alpha) = deg\ irr(\alpha, F)$. If [K: F] < ∞, then F ⊆ K is called a finite extension.

Proposition 5.2. A finite extension K/F is an algebraic extension.

Proof. Let [K: F] = n and β ∈ K. Then $1, \beta, \ldots, \beta^n$ are linearly dependent over F. Hence there exist $a_0, a_1, \ldots, a_n$, not all zero in F such that $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then β is a root of f (x). Hence β is algebraic over F.

Corollary 5.3. Every irreducible polynomial over □ has degree ≤ 2.

Proof. Let f (x) ∈ □ [x] be irreducible and α ∈ □ a root of f (x). Then □ [α] ⊆ □ . If α ∈ □ , deg f (x) = 1. If α ∉ □ , then [□ [α] : □] ≥ 2. Thus □ = □ [α]. Since [□ : □] = 2, $degf(x) = 2$.

Example 5.4. (1) Since $irr\ (i, \square) = x^2 + 1, [\square : \square] = 2$ as □ □ □ (i)

(2)Since $irr(\zeta_p, Q) = x^{p-1} + x^{p-2} + \cdots + x + 1$,

$\left[Q(\zeta_p) : Q\right] = p - 1$.

(3) Algebraic extension of a field may not be finite. Consider the chain of fields $Q \subseteq Q(2^{1/2}) \subseteq \cdots \subseteq Q(2^{1/2^n}) \subseteq \cdots$ their union K contains the algebraic numbers $\alpha_n = 2^{1/2^n}$ for all n and αn is a root of the irreducible polynomial $f_n(x) = x^{2^n} - 2$. Hence $[K : Q] \geq 2^n$ for all n. Thus $[K : Q] = \infty$.

(4) Quadratic Extensions: If [K: F] = 2 then K is called a quadratic extension of F. Let α ∈ K \F then {1, α} is a basis of K over F. Hence $\alpha^2 = a\alpha + bn$ for some a, b ∈ F.

Therefore $f(x) = irr(\alpha, F) = x^2 - ax - b$. The roots of $f(x)$ are $a \pm \sqrt{a^2 + 4ab}/2$ if Char F ≠ 2 therefore $F(\sqrt{a^2 + 4b})$

Definition 5.5. A chain of fields $F_1 \subset F_2 \subset \cdots \subset F_n$ is called a tower of fields if F_i is a subfield of F_{i+1}, for all $i = 1, 2, \ldots, n-1$.

Proposition 5.6. If K ⊆ F ⊆ L is a tower of fields then

$$[L : F][F : K] = [L : K].$$

Proof. If either F/K or L/F are infinite dimensional, then L/K is also infinite dimensional. Thus we may assume that F/K and L/F are finite. Suppose that $[F : K] = m$ *and* $[L : F] = n$. Let $x_1, x_2, \ldots, x_n$ be a basis of L over F and $y_1, y_2, \ldots, y_m$ be a basis of F over K.

We claim that the set

$B = \{x_j y_j \mid i = 1, 2, \ldots n,\ and\ j = 1, 2, \ldots, m\}$ is a vector space basis of L over K. Let z ∈ L.

Thus z = $f_1x_1 + \cdots + f_nx_n$, for some $f_1, f_2, \ldots, f_n \in F$ we write $f_i = \sum_{i=1}^{n} K_{ij} y_j$ therefore

$z = \sum_{l=1}^{n} x_l f_l = \sum_{l=1}^{n} \sum_{j=1}^{m} x_l K_{lj} y_j$. Thus B generate Las K-vector space. Suppose $\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij}\, x_i\, y_j = 0$. Then $\sum_{i=1}^{n} [\sum_{j=1}^{m} a_{ij} y_j] x_i = 0$. Since x1 . . . , xn are F -linearly independent. Therefore $\sum_{i=1}^{n} a_{ij}\, x_i\, y_j = 0$ for each i. By linear independence of $y_1, \ldots, y_n$ to see that all the $a_{ij} = 0$.

Corollary 5.7. Let F ⊆ K be a finite field extension. Then $deg\ irr(\alpha, F)\ divides\ [K : F]$, for all α ∈ K.

Proof. Since F ⊆ F (α) ⊆ K, we have

$$[K : F] = [K : F(\alpha)][F(\alpha) : F]$$

Thus $deg\ irr(\alpha, F)\ divides\ [K : F]$, .

Proposition 5.8. Let K/F be a field extension. If $a_1, a_2, \ldots, a_n \in$ K are algebraic over F then F ($a_1, a_2, \ldots, a_n$) is a finite algebraic extension of F.

Proof. Since ai is algebraic over F, it is algebraic over F ($a_1, a_2, \ldots, a_{i-1}$). Thus $[F(a_1, a_2, \ldots, a_i) : F(a_1, a_2, \ldots, a_{i-1})]$ is finite for all i. Therefore the field $F(a_1, a_2, \ldots, a_n)$ is a finite extension of F. Hence it is algebraic.

Corollary 5.9. Let E/F and K/E be algebraic extensions. Then K/F is an algebraic extension.

Proof. Let a ∈ K and let a be a root of $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in E[x]$.Consider the field $L = F(a_0, a_1, \ldots, a_{n-1})$. Then a is algebraic over L. Hence $L(a)$ is a finite extension of L. Since $a_0, a_1, \ldots, a_{n-1}$ are algebraic over F, L is a finite extension of F. Hence $L(a)$ is a finite extension of F. Hence a is algebraic over F.

Corollary 5.10. Let K/F be a field extension. Then the set of elements of K which are algebraic over F is a subfield of K.

Proof. Let a, b ∈ K be algebraic over F. Then F (a, b) is a finite extension of F. Hence all elements of F (a, b) are algebraic over F. In particular, a ± b, ab and a/b if $b \neq 0$, are all algebraic over F.

Compositum of fields: Let L/k be a field extensions and E/k and F/k be intermediate field extensions. Then the smallest field containing E and F, to be denoted by EF, is called the compositum of F and F. Suppose $E = k(a_1, a_2, \ldots, a_n)$ and F is an extension of k. Then $EF = F(a_1, a_2, \ldots, a_n)$.

Example 5.11. Let m and n be co prime positive integers. Consider the subfields $E = Q(\zeta_m)$ *and* $F = Q(\zeta_n)$ *of* $\square$.
Then the compositum of E and F is $Q(\zeta_{mn})$.
Indeed, as m and n are coprime, there exist $p, q \in \square$ such that $mp + nq = 1$. Therefore

$$\zeta_{mn} = exp(2\pi i / mn) = exp(2p\pi i / n)\ exp(2q\pi i / m) = (\zeta_n)^p (\zeta_m)^q$$

We can estimate the degree of the compositum of two finite field extensions in terms of their degrees.

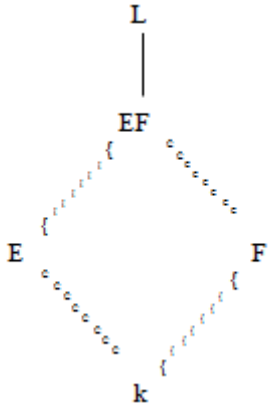
Proposition 5.12. Let L/k be a field extension and E/k, F/k be intermediate finite extensions fields. Then

$$[EF : k] \leq [E : k][F : k].$$

If [E : k] and [F : k] are coprime then equality holds.

Proof. Let $x_1, x_2, \ldots, x_m$ and $y_1, y_2, \ldots, y_n$ be bases of the $k-$vector spaces E and F respectively. Then it is easy to see that $E = k(x_1, x_2, \ldots, x_m)$ and $F = k(y_1, y_2, \ldots y_n)$. Therefore $EF = k(x_1, x_2, \ldots, x_m; y_1, y_2, \ldots y_n)$.

We have the following diagram of field extensions:



Since $EF = E(y_1, y_2, \ldots, y_n)$ we have $[EF : F] \leq n$. Since the degree is multiplicative in a tower of finite extensions, we have

$$[EF : k] = [EF : E][E : k] \leq mn$$

Since m and n both divide [EF : k], and (m, n) = 1, we get $mn \mid [EF : k]$.

Hence [EF : k] = mn.

6. Conclusion

An element a ∈ F is called algebraic over K if there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(a) = 0$. If every element of F is algebraic over K then we say that F is an algebraic extension of K
If a ∈ K then the set $\{1, a, a^2, \ldots, a^n\}$ is linearly dependent. Let $b_0, b_1, \ldots, b_n \in F$, not all zero, so that $b_0 + b_1 a + \cdots + b_n a^n = 0$. Hence a is a root of the nonzero polynomial $b_0 + b_1 x + \cdots + b_n x^n$. Therefore b is algebraic over F and hence K/F is an algebraic extension.
Let F ⊆ K be a field extension. The dimension of the

F -vector space K, denoted by [K : F] is called the degree of the field extension K/F. For an algebraic element α ∈ K, $dim_F F(\alpha) = deg\ irr(\alpha, F)$. If [K : F] < ∞, then F ⊆ K is called a finite extension.

Let L/K be a field extensions and E/K and F/K be intermediate field extensions. Then the smallest field containing E and F, to be denoted by EF, is called the compositum of F and F. Suppose $E = k(a_1, a_2, \ldots, a_n)$ and F is an extension of k. Then $EF = F(a_1, a_2, \ldots, a_n)$.

Author Profile

Vinit Chauhan received the M.Sc. degree from Dr. Bhim Rao Ambedkar University Agra, India in 2011.