IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Extension Fields and Zeros of Irreducible Polynomials

Mr. Madhav Thakur

Lecturer and Researcher, North East Frontier Technical University (NEFTU)

1. *Abstract*

Extension fields a wonderful part of mathematics (Abreact Algebra) for finding zeros of polynomials and its properties. In principle, I have focused on to understand the basic concept of extension field and to find the zeros of irreducible polynomial over extended or splitting field, theory and corollary with suitable examples and diagram where needed.

Keywords: Field, Extension Field, Zeros, Irreducible polynomial, Splitting Field.

2. Introduction

An abstract algebra is an important branch of Mathematics and fields are one of the most important part of Algebra, also one of the important objects of study. Fields's theory provides a useful generalization of many number systems, nature and zeros/roots of the polynomials. The study of extension field is specially study of polynomials. Generally, we know that an irreducible polynomial cannot be factorized. i.e., it cannot be warren into the product of two or more than two non-constant polynomials. It means zeros of polynomials do not find. So, we study all about the polynomials as well as its derivatives as its factor, zeros and irreducibility over field. Also, we see about splitting of field over some fields.

3. Extension Field

3.1. Definitions:

3.1.1 Field: A field F is a set of two composition laws "+" (Addition) and ". " (Multiplication) such that

(a) (F, +) is a commutative group,

(b) (F*, +) is a commutative group, where F* = F \ {0}

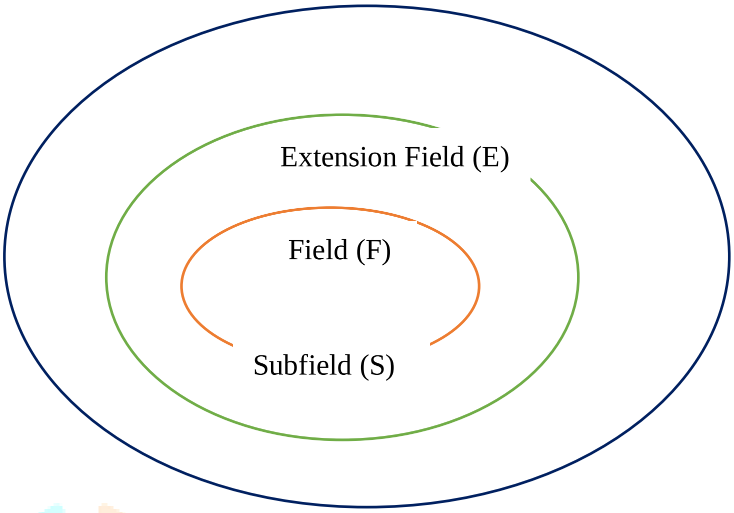
(c) and holds distributive law.

Hence, for a field a ring should be nonzero commutative. Therefore, all element (nonzero element) has an own inverse. i.e., $Q, R, C, Fp = Z/pZ$ (p prime) are fields.

One of the most important and smallest field is $F_2 = Z/2Z = \{0,1\}$.

3.1.2. Subfield: If S ⊆ F and S itself a field then S is said to be subfield of F.

3.1.3. Extension Field: Let us assume a subfield F of field E then, E is called extension field of F. It is denoted as [E: F]. An extension field E of a field F then, F ⊆ E and all operations of F are those E restricted to F.



In practical: S ⊆ F ⊆ E

3.2. Characteristic of a field:

If F is a field, then its characteristic to be defined as a smallest positiveinteger p i.e., $p \cdot 1_F = 0$. It is denoted as char(F).

If such type of p exists then field is finite order and 0 otherwise if infinite order.

3.3. Proposition:

Characteristic of a field either zero or prime.

3.4. Corollary: If F is a field and exists an irreducible polynomial p(x) over F. Thus,

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

3.5. Theorem: Fundamental theorem of field theory (Kronecker's Theorem, 1887) 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:

Let us take a field F, hence as we know that if F is a field, then, F[x] is a unique factorization domain. Then, there exist an irreducible factor $p(x)$ (say), of $f(x)$.

Hence, it is sufficient to construct an extension E of F where $p(x)$ has a zero.

We consider a field E = F[x]/< $p(x)$ > {corollary 3.4.}

Now ψ: F → E given by ψ(k) = k + < $p(x)$ >. ψ is one-one, onto and preserves these operations.

Thus, E has a subfield which is isomorphic to F. Therefore, we find a unique coset k + p(x) representative k that belongs to F.

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

Let

$$p(x) = k_n x^n + k_{n-1} x^{n-1} + \ldots + a_0$$

$$p(x+ < p(x) >) = k_n(x+ < p(x) >)^n + k_{n-1}(x+ < p(x) >)^{n-1} + \ldots + k_0$$

$$= k_n(x^n + <p(x)>) + k_{n-1}(x^{n-1} + <p(x)>) + \ldots + k_0 + < p(x) >$$

$$= k_n x^n + k_{n-1} x^{n-1} + \ldots + k_0 + < p(x) >$$
$$= p(x) + < p(x) >$$
$$= 0 + < p(x) >$$

So, $x + < p(x) >$ is a zero of $p(x)$ in E.

3.5.1. Illustration: Let $f(x) = x^5 + 2x^2 + 2x + 2 \in Z_3\,[x]$.

There exits irreducible factorization of $f(x)$ over Z_3 is $(x^2 + 1)\,(x^3 + 2x + 2)$.

Hence, construct an extension field E (say) of $Z_{3,}$ where f(x) has a zero, we may let

E = $Z_3 / (x^2 + 1)$ of order 9 or E = $Z_3 / (x^3 + 2x + 2)$ of order 27.

3.5.2. Illustration: Let $f\,(y) = y^2 + 1 \in Q[y]$. Then E = $Q[y]/ < y^2 + 1 >$

We have,

$$f\,(y + < y^2 + 1 >) = (y + < y^2 + 1 >)^2 + 1$$
$$= y^2 + < y^2 + 1 > +1$$
$$= y^2 + 1 + < y^2 + 1 >$$
$$= 0 + < y^2 + 1 >$$

Hence, $y + < y^2 + 1 >$ is a zero of $f\,(y)$ in F.

4. Splitting Field

4.1. Definition: An extension field of K of F is said to be splitting field of $f(x) \in F[x]$ over F if;

(a) $f(x)$ can be factored in two linear factors over K[x].

(b) $f(x)$ can not be factored in two linear factors over any subfield of K containing F.

4.1.1. Illustration: Show that Q[i] is splitting field of $f(x) = x^2 + 1$ over Q but C is not splitting field of $f(x) = x^2 + 1$ over Q.

As given $f(x) = x^2 + 1 = (x+i)\,(x-i)$ over Q[i] and Q[i] is a smallest extension of Q then Q[i] is splitting field of $f(x) = x^2 + 1$ over Q.

But $f(x) = x^2 + 1 = (x+i)\,(x-i)$ over C and $Q \subseteq Q[i] \subseteq C$, such that $f(x) = x^2 + 1$ over q[i] then C is not splitting field $f(x) = x^2 + 1$ over Q

4.2. Theorem: For a field $\boldsymbol{F}$ and if a nonconstant element $\boldsymbol{f(x) \in F[x]}$. Then ∃ an extension $\boldsymbol{K}$ of $\boldsymbol{F}$ which is a splitting field for $\boldsymbol{f(x)}$.

Proof: To show first that, an extension K of F and $f(x)$ is splits completely into linear factors through induction on degree n of $f(x)$.

Let degree of $f(x)$ is one, then $f(x)$ will be already in linear in this case $K = F$.

Now,

Let us consider that the statement is true for all field, all polynomials degree less than that of $f(x)$.

Hence, as per fundamental theorem of field theory that, an extension K of F in which has a zero (say) a_1.

So, $f(x)$ has the linear factors $(x - \alpha)$ and we write $f(x) = (x - \alpha)g(x), where\ g(x) \in E[x]$. Since, $deg\ g(x) < deg\ f(x)$, by induction there is an extension $E\ of\ E1$ containing all the zeros of $g(x), say, \alpha_1, \alpha_2, . . ., \alpha_n.$

Since, $\alpha \in E$, E is an extension of F containing all the zeros of *f(x)*. Now assume K be the intersection of all the subfields of E containing F and also contain all zeros of *f(x)*. So, it is clearly, then a splitting field for $f(x)$ over F is $F(\alpha_1, \alpha_2, . . ., \alpha_n)$.

4.2.1. Corollary: If K is an algebraic extension of F while is the splitting filed over F for a collection of polynomials *f(x)* $\in$ *F[x]*, then K is a normal extension of F.

4.2.2. Illustration: The splitting field fir $(x^2 – 2)(x^2 – 3)$ is the field Q($\sqrt{2}$, $\sqrt{3}$) generated over Q by $\sqrt{2}$ and $\sqrt{3}$ since the zeros of the polynomial are $\pm\sqrt{2}$,$\pm \sqrt{3}$. Hence, we seen that it is an extension of degree 4 over Q. we can know subfields by following diagram:

$$\begin{tikzcd}
 & Q\,[\sqrt{2}, \sqrt{3}\,] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
Q\,[\sqrt{2}\,] \arrow[dr, dash, "2"'] & Q\,[\sqrt{6}\,] \arrow[d, dash, "2"] & Q\,[\sqrt{3}\,] \arrow[dl, dash, "2"] \\
 & Q &
\end{tikzcd}$$

(Source: Dummit Foote, Abstract Algebra, Page No. 568, Third Edition 2011, Wiley India Pvt. Ltd.)

5. Zeros of Irreducible Polynomial

5.1. Definition (Derivative of polynomials)

Let *f(x)* = $k_n x^n + k_{n-1}x^{n-1} + . . . + k_1 x + k_0$ belong to $F[x]$. then derivative of *f(x)*, is denoted by $f^{''}(x)$ = $nk_n x^{n-1} + (n-1)k_{n-1}x^{n-2} + . . . + k_1$in $F[x]$.

5.2. Lemma: [Algebraic laws of derivative]

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

(b) $[a\,f(x)]' = a\,f'(x)$

(c) $[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$.

5.3. Definition (Multiple zeros): Zeros of multiplicity greater than 1, such are called multiple zeros.

5.4. Definition (Perfect field): A field $\boldsymbol{F}$ is said to be perfect if its characteristic 0 or $\boldsymbol{p}$ and $\boldsymbol{F^p} = \{\boldsymbol{a^p} \mid \boldsymbol{a} \in \boldsymbol{F}\} = \boldsymbol{F}$.

5.5. Theorem: Let a nonconstant polynomial $f(x) \in F$, has multiple zeros in some extension K if and only if $f(x)\ and\ f'(x)$ have a common factor of positive degree in $F[x]$.

Proof. *Let* $f(x) = (x - a)^2\,g(x) \in E[x]$, then $f'(x) = 2(x-a)(-a)g(x) + (x - a)^2\ g'(x)$. So, that $f\ (x)\ and\ f'(x)\ have\ (x-a)$ common factor in K.

Now we suppose that, if $f(x)$ *and* $f'(x)$ have not any common factors in $F[x]$.

Therefore, all these are relatively prime.

Hence, there exist $g(x), h(x) \in F[x]$, such that, $g(x)f(x) + h(x)f'(x) = 1$, and $(x - a)$ is a factor of $1 \in K[x]$.

Conversely, we suppose $f(x)$ *and* $f'(x)$ have a common factor $(x - a)$, *then* $f(x) = (x - a)g(x)$ *and* $f'(x) = g(x) + (x - a)g'(x)$, *this emlise* $g(x) = (x - a)h(x)$.

Hence, $f(x) = (x - a)^2 h(x)$ *in* $K[x]$.

5.6. Theorem: An irreducible polynomial $f(x)$ over a field F;

(1) and F has characteristic 0. Then, $f(x)$ has no multiple zeros.

(2) and F has characteristic $p \neq 0$. Then, $f(x)$ has a multiple zero,

If it is in the form of $f(x) = g(x^p)$ for some $g(x)$ in $f[x]$.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + . . . + a_1 x + a_0$ in $F[x]$.

So, $f''(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + . . . + a_1$ in $F[x]$.

Let $f(x)$ has a multiple zero then, $f(x)$ and $f'(x)$ have common factors $g(x)$ *(say)* of degree at list in $F[x]$.

Then, $g(x)/f(x)$ and $g(x)/f'(x)$,

$\Rightarrow g(x) = u\, f(x)$. Hence, we see $f\,'(x) = 0$ means only $ka_k = 0$ *for* $k = 1, 2, . . . n$.

Now, we can see two cases;

(a) If $char(F) = 0$, and $f(x) = a_0$, which is not irreducible. But it is a contradiction that $f(x)$ is an irreducible. Therefore, $f(x)$ has no multiple zeros.

(b) *If* $char(F) = p \neq 0$, *and* $a_k = 0$, where p does not divide k. Thus, the power of x that in the sum $a_n x^n + a_{n-1}x^{n-1} + . . . + a_0$, are these of the form $x^{pi} = (x^p)^i$. This follows $f(x) = g(x^p)$, for some $g(x) \in F[x]$.

5.6.1. Corollary: Every finite field is perfect**.**

IJCRT

5.7. Theorem: An irreducible polynomial $f(x)$ over a field F and splitting field K of $f(x)$ over F. Then the zeros of $f(x)$ in K having the similar multiplicity.

Proof: Suppose a, b are two zeros (distinct) of $f(x)$ in K.

Now we take multiplicity of a is n.

So, it may write as $f(x) = (x - a)$ then, it is written $f(x) = (x - a)^n h(x) \in K[x]$.

Now, we know a field isomorphism $\emptyset : K \rightarrow K$ leaving F invariant and brings a *to* b.

Therefore, $f(x) = \emptyset\{f(x)\} = (x - b)^n \emptyset\{h(x)\} = (x - a)^n \emptyset\{h(x)\} \in K[x]$.

Hence, we seen that, multiplicity of b is greater or equal to multiplicity of a and vice-versa.

Thus, a and b have the same multiplicity.

5.7.1. Corollary: An irreducible polynomial $\boldsymbol{f(x)}$ over a field $\boldsymbol{F}$ and splitting field $\boldsymbol{K}$ of $\boldsymbol{f(x)}$. Then, $\boldsymbol{f(x)}$ has the form $\boldsymbol{k(x - a_1)^n (x - a_2)^n . . . (x - a_i)^n}$ where $\boldsymbol{a_1, a_2, a_3, \; . . . ,}$ are distinct elements of $\boldsymbol{K}$ and $\boldsymbol{a} \in \boldsymbol{F}$.

6. Conclusions

In conclusion, the irreducible polynomial over any field which is contained all coefficient are absolutely irreducible. As per crucial hypothesis of algebra, a univariate polynomial is absolutely irreducible iff its degree is 1. Then again, with a few indeterminates, there are totally irreducible polynomials having any degree. Existing of splitting field over some field, multiplicity of zeros, common factors of positive degree polynomials over some extension field. Hence this article helps us to know the characteristics of irreducible polynomials over the fields and their extension.

7. References

a. A.K. Vasishtha & A.R. Vasishtha, Modern Algebra (Abstract Algebra), 3rd edition 2015, Krishna Publication.

b. S. K. Bhambri and V. K. Khanna, A Course in Abstract Algebra Book, 5th edition 2017, Vikas Publication House.

c. David S. Dummit and Richard M. Foote, Abstract Algebra, Third Edition 2011, Wiley India Pvt. Ltd.

d. Goyal Gupta, Advanced Course in Modern Algebra, 18th edition 2019, Pragati Prakashan.

e. M.L. Kanna, Modern Algebra, 20th edition 2012, Jai Prakash Nath & Co, meerut.

f. Serge Lang, Algebra, 3rd edition 2002, Springer-Verlag New York.

g. Joseph A. Gallian, Contemporary Abstract Algebra, 4th edition 1999, N. K. Mehra for Narosa Publishing House Pvt. Ltd.

h. Joseph J. Rotman, A first course in abstract algebra with applications, 3rd edition 2005, Pearson Education.

i. George, Abin, Mr Rakesh, and Mr Asokan. "The Role and Importance of Digitalization in Hospitality Sector to Ease Function." *Design Engineering* (2021): 13773-13779.

j. George, Abin, "Sustainable Developments of Hospitality and its Challenges in the Government Organizations." *Turkish Online Journal of Qualitative Inquiry| TOJQI* (2021): 6410 – 6416.