FINITE FIELDS

A THESIS

submitted by

PURNIMA SATAPATHY

in partial fulfillment of the requirements for the award of the degree

of

Master of Science in Mathematics

under the supervision

of

Dr. RAJA SEKHAR TUNGALA

DEPARTMENT OF MATHEMATICS

NIT ROURKELA

ROURKELA– 769 008

MAY 2012

DECLARATION

I declare that the topic '*Finite Fields*' for my M.Sc. degree has not been submitted in any other institution or university for the award of any other degree or diploma.

Place: Purnima Satapathy

Date: Roll No. 410MA2108

CERTIFICATE

This is to certify that the project report entitled **"Finite Fields"** submitted by **Purnima Satapathy** for the partial fulfilment of M.Sc. degree in Mathematics, National Institute of Technology Rourkela, Odisha is a bonafied record of review work carried out by her under my supervision and guidance. The content of this report, in full or in parts, has not been submitted to any other institute or university for the award of any degree or diploma.

(Raja Sekhar Tungala)
Assistant Professor
Department of Mathematics
NIT Rourkela -769 008

ACKNOWLEDGEMENTS

I would like to warmly acknowledge and express my deep sense of gratitude and indebtedness to my guide **Dr. Raja Sekhar Tungala**, Department of Mathematics, NIT Rourkela, Orissa, for his keen guidance, constant encouragement and prudent suggestions during the course of my study and preparation of the final manuscript of this Project.

I would like to thank the faculty members of Department of Mathematics for allowing me to work for this Project in the computer laboratory and for their cooperation. Also I am grateful to my senior Bibekananda Bira, research scholar, for his timely help during my work.

My heartfelt thanks to all my friends for their invaluable co-operation and constant inspiration during my Project work.

I owe a special debt gratitude to my revered parents, my brother, sister for their blessings and inspirations.

Rourkela,769008

May, 2012 **Purnima Satapathy**

ABSTRACT

In this report, we revised some important definitions with examples and results of ring theory such as ring homomorphism, Euclidean domain, principal ideal domain, unique factorization domain, polynomial rings, irreducibility criteria etc. Then, we discuss field theory. In field theory, we study the details of extension of fields, splitting fields, algebraic extensions etc. The most important field of abstract algebra is Galois theory. Here, we prove the fundamental theorem of Galois theory and the application of this result. Lastly, we discuss the structure and applications of finite fields.

Contents

NOTATIONS

English Symbols

$\mathbb{Z}$	Set of integers
$\mathbb{F}$	Field
$[\mathbb{E} : \mathbb{F}]$	Degree of extension
$Gal(\mathbb{E}/\mathbb{F})$	Galois group of $\mathbb{E}$ over $\mathbb{F}$
$\mathbb{E}_{\mathbb{H}}$	Fixed field of $\mathbb{H}$

CHAPTER 1

INTRODUCTION

The general solutions of linear and quadratic polynomials in one variable were known centuries before. For cubic and quadratic equations also the general solutions are provided by Cardano's and Ferrari's methods, respectively. In 19th century a great work has been done to find general solution of a general polynomial by radicals. However, there was no success even after efforts of many great mathematicians of that time. Eventually work by Able and Galois gives satisfactory solution and complete understanding of this problem. There are two important problems which provide some motivation for studying Galois Theory. Those problems are:

(1) The existence of polynomials which are not soluble by radicals.

(2) Some results about classical Euclidean Geometry. For example, we cannot trisect an angle using ruler and a compass and certain regular polygons cannot be constructed using ruler and compass.

Galois Theory provides a connection between Field theory and Group theory, which in turn useful to convert problems in field theory into Group theory, which are better understood and easy to handle. Galois theory not only provide answer to the problem discussed above but also explains why the general solution exists for polynomials with degree less than or equal to 4. In his original work, Galois used permutation groups to describe relations between roots of the polynomial. In modern approach, developed by Artin, Dedekind etc., involves study of automorphisms of field extensions.

In field theory the most beautiful and important area is finite fields. Finite fields were first introduced by Galois in 1830 in his proof of the un-solvability of the general quintic equation. When Cayley investigate groups of matrices over finite fields. In the past fifty years, there have been important application of finite fields in computer science, coding

theory, information theory, and cryptography. But, besides the many uses of finite fields in pure and applied mathematics. The important features of finite fields are the restricted nature of their order and structure.

CHAPTER 2

RING THEORY

Many sets associated with two binary operations addition and multiplication. When we considering these sets as groups then we consider either of binary operation addition or multiplication. But one may wish to take both the binary operations. So the ring concept comes into picture. This notion was originated in mid nineteenth century by Richard Dedekind, although its first formal abstract definition was not given until Abraham Fraenkel presented it in 1914. In this chapter, we give few definitions with examples and some results.

Definitions and theorems

Ring:

A non empty set R w.r.t binary operations addition and multiplication is called a ring when it satisfies below properties

1. It is an abelian group under addition.
2. It must satisfy associative property w.r.t multiplication.
3. Multiplication is distributive over addition.

$a(b+c)=ab+ac$

Commutative ring:

When R satisfies commutative property w.r.t multiplication then R is called commutative ring.

Unity:

When a ring other than $\{0\}$ has an identity under multiplication, we say that the ring has a unity.

Unit:

If $a \neq 0 \in R$ and a^{-1} exist then a is a unit of R.

Examples

(1) $\mathbb{Z}$ is a ring under addition and multiplication. It is a commutative ring with unity. The units of $\mathbb{Z}$ are 1 and -1.

(2)$M_3(\mathbb{Z}) = \Bigg\{$

$$A_{3\times 3} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$\mid a, b, c, d, e, f, g, h, i \in \mathbb{Z} \Bigg\}$
is a noncommutative ring with unity.

Subring:

A subset S of a ring R is a subring of R if S is itself a ring with same operations of R.

Examples

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

(2)For each positive integer n the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, ...\}$ is sub ring of $\mathbb{Z}$.

Zero Divisors:

A nonzero element a in a commutative ring R is called a zero divisor if there is a non zero element $b \in R$ such that $ab = 0$.

Examples

(1)

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

AB=0.

(2)$R = \{f | f : [0, 1] \to \mathbb{R}\}$. Units of $R = \{f | f(x) \neq 0 \ \forall x \ \in [0, 1]\}$. For such f inverse is $\frac{1}{f}$. f is a zero divisor because if we define

$$g(x) = \begin{cases} 0 & : f(x) \neq 0 \\ 1 & :\text{f(x)=0} \end{cases}$$

then $g(x)$ is not zero function. But $f(x)g(x) = 0$.

Integral domain:

A commutative ring with unity is said to be an integral domain if it has no zero divisor.

Examples

(1) The ring of integers $\mathbb{Z}$ is an integral domain.

(2) $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ is an integral domain.

Field:

A commutative ring with unity is called a field if every nonzero element is a unit.

Examples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$

Theorem: *A finite integral domain is a field.*

proof:

Let D be any finite integral domain. Let a $(\neq 0) \in D$. We have to show that a^{-1} exist or a is unit. If $a = 1$, a is its own inverse. If $a \neq 1$, then $a,\ a^2,\ a^3, ... \in D$. but D is finite. So there must be two positive integer i and j such that $i > j$ and $a^i = a^j \Rightarrow a^{i-j}$=1 $\Rightarrow a^{i-j-1}$=a^{-1}. So a^{-1} exists. $\square$

Characteristic of a ring:

The characteristic of a ring R is the least positive integer n such that $nx = 0\ \forall\ x \in R$. If no such n exists then Char R=0.

Examples

(1) $\mathbb{Q}$ has characteristic 0.

(2) $\mathbb{Z}_p$ has characteristic p.

Ideal:

A subring A of a ring R is called a (two sided) ideal of R if for every $r \in R$ and every $a\ \in A$ both ra and $ar \in A$.

Ideal test:

A non empty subset A of a ring R is an ideal of R if

(i) $a - b \in A$ whenever $a,\ b \in A$.

(ii) ra and $ar \in A$ whenever $a \in A$ and $r \in R$.

Examples

(1) Let R be a ring, $\{0\}$ and R are ideals of R. $\{0\}$ is called trivial ideal of R.

(2) $n\mathbb{Z} = \{0,\ \pm n,\ \pm 2n, ...\},\ n \in \mathbb{Z}^+$. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Homomorphism:

The word homomorphism comes from Greek words 'homo' means 'like' and 'morphe' means 'form'.

Similarity with photography:

A photograph of a person cannot tell us the person's exact height, weight and age. But it may be possible to decide from a photograph that the person is tall or short, heavy or thin, old or young, male or female. Like this a homomorphic image of a group gives us some information about the group not the exact property of the group.

Ring homomorphism:

A ring homomorphism is a map from one ring to another that preservers the binary operations addition and multiplication.

Let R and S be rings, $\phi : R \to S$ satisfying

(i)$\phi(a + b) = \phi(a) + \phi(b)\ \forall\ a, b\ \in R$.

(ii)$\phi(ab) = \phi(a)\phi(b)\ \forall\ a, b\ \in R$. Then ϕ is called a ring homomorphism.

Monomorphism:

If a ring homomorphism is one-one then it is called monomorphism.

Etimorphism:

If a ring homomorphism is onto then it is called etimorphism.

Isomorphism:

If a ring homomorphism is one-one and onto then it is called isomorphism.

Example

$\phi : \mathbb{Z} \to \mathbb{Z}_n$, defined by $k \to k \ mod \ n, n \ \in \mathbb{Z}^+ \ a, \ b \in \mathbb{Z}$

$\phi(a+b) = (a+b) \ mod \ n$

$= ((a \ mod \ n) + (b \ mod \ n)) \ mod \ n$

$= a \ mod \ n \ + \ b \ mod \ n$

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

Properties of homomorphism:

Let ϕ be a homomorphism from a ring R to a ring S. Let A be a subring of R and B an ideal of S.

(1) For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.

(2) If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.

(3) If R is commutative, then $\phi(R)$ is commutative.

(4) If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

(5) If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.

Quotient ring or factor ring:

Theorem: (Existence of factor ring) *Let R be a ring and let A be a subring of R. The set of all cosets $\{r + A | r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$, $(s + A)(t + A) = st + A$ iff A is an ideal of R.*

Example

$\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, \ 1 + 4\mathbb{Z}, \ 2 + 4\mathbb{Z}, \ 3 + 4\mathbb{Z}\}$

$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$ modulo arithmetic 4.

$(2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z}$ modulo arithmetic 4.

Prime ideal

A proper ideal A of a commutative ring R is said to be a prime ideal of R if $a, \ b \in R$ and $ab \in A$ then $a \in A$ or $b \in A$.

Examples

(1) $\mathbb{Z}$ is a ring. $n\mathbb{Z}$ is prime ideal iff n is prime.

$(2) < x^2+1 >$ is not a prime ideal of $\mathbb{Z}_2[x]$. $\mathbb{Z}_2[x]$=$\{a_0+a_1x+a_2x^2+....+a_nx^n|a_0, a_1, a_2, ..., a_n \in \mathbb{Z}_2\}$. Let $1+x \in \mathbb{Z}_2[x]$, $(1+x)^2 = 1+x^2+2x = 1+x^2 \in < x^2+1 >$, but $(1+x) \notin < x^2+1 >$ $< x^2 + 1 >$ is not a prime ideal of $\mathbb{Z}_2[x]$.

Theorem:

Let R be a commutative ring with unity and let A be an ideal of R.

Then R/A is an integral domain iff A is prime.

proof:

Given that R/A is an integral domain. We have to show that A is prime ideal. i.e, If $a,\ b \in R$ and $ab \in A$ then $a \in A$ *or* $b \in A$. Now, $a + A,\ b + A \in R/A$. $(a + A)(b + A) = ab + A \in A$. Since R/A is an integral domain, so either $a + A = 0 + A$ or $b + A = 0 + A$. $a \in A$ or $b \in A$. So A is prime ideal.

Conversely,

A is a prime ideal. We have to show that R/A is an integral domain. i.e, to show zero divisor does not exist in R/A. Let $a+A,\ b+A \in R/A$. $(a+A)(b+A) = 0+A = ab+A$, therefore $ab \in A \Rightarrow a \in A$ or $b \in A$ (since A is a prime ideal), $a+A$ or $b+A$ is zero coset of R/A. So, R/A is an integral domain. $\square$

Maximal ideal:

A proper ideal A of R is said to be a maximal ideal of R if B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$

Examples

1. $\mathbb{Z}$ is a ring. $p\mathbb{Z}$ is maximal ideal if p is prime.

2. $< x^2 + 1 >$ is maximal in $\mathbb{R}[x]$.

Theorem:

Let R be a commutative ring with unity and let A be an ideal of R.

Then R/A is a field iff A is maximal.

proof:

R is commutative ring with unity. A is an ideal of R.

Given that R/A is a field. We have to show that A is maximal. Let B be an ideal of R.

$A \subset B$

Let $b \in B$ but $b \notin A$. Therefore $b + A$ is a non-zero element of R/A. Since R/A is a field multiplicative inverse exist. i.e, $(b+A)(c+A) = 1+A$. Now, $1+A = (b+A)(c+A) = bc+A$. $b \in B$ and $bc \in B$, $1 - bc \in A \subset B$. Therefore, $1 = (1 - bc) + bc \in B$. So $B = R$. Hence A is maximal ideal.

Conversely, given that A is maximal ideal.We have to show that R/A is a field. i.e, to show any nonzero element of R/A has multiplicative inverse. Now, A is maximal ideal. Let $b \in R$ but $b \notin A$. $b + A$ is a nonzero element of R/A. We have to show $b + A$ has multiplicative inverse. Let us consider $B = \{br + A | r \in R, a \in A\}$. B is an ideal of R. Since A is maximal, so $B = R$. $1 \in B$, $1 = bc + a^{'}$, $a^{'} \in A$, $c \in R$. $1 + A = bc + a^{'} + A = bc + A = (b + A)(c + A)$. Therefore, $c + A$ is multiplicative inverse of $b + A$. So R/A is a field. $\square$

Corollary:

If R is commutative ring, every maximal ideal is prime ideal.

proof:

If A is a maximal ideal. R/A is a field. i.e, R/A is an integral domain.

So A is a prime ideal. $\square$

Factorization of polynomials:

Irreducible polynomial and reducible polynomial

A non-constant polynomial $f(x)$ is irreducible over $\mathbb{F}[x]$, if $f(x)$ cannot be expressed as a product of two polynomials $g(x)$ and $h(x)$ in $\mathbb{F}[x]$ both of lower degree than the degree of $f(x)$. If $f(x) \in \mathbb{F}[x]$ is a non-constant polynomial that is not irreducible over $\mathbb{F}$ then $f(x)$ is reducible over $\mathbb{F}$.

Example

$f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$, but $f(x)$ is reducible over $\mathbb{R}$.

Theorem:(Reducibility test for degree 2 and 3)

let $f(x) \in \mathbb{F}[x]$ *and let* $f(x)$ *be of degree* 2 *or* 3 *then* $f(x)$ *is reducible over* $\mathbb{F}$ *if and only if it has a zero in* $\mathbb{F}$.

proof:

Suppose $f(x)$ is reducible. So $deg\ f(x) = deg\ g(x) + deg\ h(x)$, degree of $f(x)$=2 or 3, so at least $g(x)$ or $h(x)$ has degree 1. $g(x) = ax + b$, therefore $ax + b = 0 \Longrightarrow x = -a^{-1}b$ is a zero of $g(x)$. $-a^{-1}b$ is a zero of $f(x)$. Conversely, suppose that $f(a) = 0,\ a \in \mathbb{F}$. So $x - a$ is a factor of $f(x)$. Therefore $f(x)$ is reducible over $\mathbb{F}$. $\square$

Application

For the field $\mathbb{Z}_p$ reducibility of $f(x)$ can be checked by $f(a) = 0$ for a= 0, 1, ...$p - 1$.

a is a root of $f(x)$ in $\mathbb{Z}_p$.

Only up to degree 3 we can use above theorem

If any polynomial has degree more than 3 we cannot apply the above theorem. See the below example.

In the polynomial ring $\mathbb{Q}[x]$, $p(x) = x^4 + 2x^2 + 1 \Rightarrow (x^2 + 1)(x^2 + 1)$, but $p(x)$ has no zero in $\mathbb{Q}[x]$. Hence $p(x)$ is reducible over $\mathbb{Q}[x]$, but $p(x)$ has no zero in $\mathbb{Q}[x]$. So it contradicts the above theorem.

Content of polynomial, primitive polynomial

The content of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, where the $a_i's$ are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, ..., a_0$. A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.

Gauss's Lemma : *The product of two primitive polynomials is primitive.*

proof:

let $f(x)$ and $g(x)$ be two primitive polynomials. We have to prove $f(x)g(x)$ is primitive. If possible, let $f(x)g(x)$ is not primitive. So let p be a primitive divisor of the content of $f(x)g(x)$, and let the polynomials $\overline{f}(x)$, $\overline{g}(x)$ and $\overline{(f(x)g(x))}$ obtained from $f(x)$, $g(x)$ and $f(x)g(x)$ respectively, by reducing the coefficients modulo p. Then $\overline{f}(x)$ and $\overline{g}(x)\ \in \mathbb{Z}_p[x]$ and $\overline{f}(x)\overline{g}(x) = \overline{(f(x)g(x))} = 0$, the zero elements of $\mathbb{Z}_p[x]$. So, either $\overline{f}(x) = 0$ or $\overline{g}(x) = 0$, (Since these are in integral domain). This means that either p divides every coefficient of $f(x)$ or p divides every coefficient of $g(x)$. Therefore, either

$f(x)$ is not primitive or $g(x)$ is not primitive, which is contradiction to the assumption. So $f(x)g(x)$ is primitive. $\square$

Theorem: *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*

Proof

Given that $f(x)$ is reducible over $\mathbb{Q}$. So we can write $f(x) = g(x)h(x)$, where $g(x)$ and $h(x) \in \mathbb{Q}[x]$. We may assume that $f(x)$ is primitive because we can divide both $f(x)$ and $g(x)h(x)$ by the content of $f(x)$. Let a be the least common multiple of the denominators of the coefficients of $g(x)$ and b be the least common multiple of the denominators of the coefficient of $h(x)$. Then $abf(x) = ag(x).bh(x)$, where $ag(x)$ and $bh(x) \in \mathbb{Z}[x]$. Let c_1 be the content of $ag(x)$ and c_2 be the content of $bh(x)$. Then $ag(x) = c_1g_1(x)$ and $bh(x) = c_2h_1(x)$, where $g_1(x)$ and $h_1(x)$ both are primitive and

$$abf(x) = c_1c_2g_1(x)h_1(x). \tag{2.1}$$

$f(x)$ is primitive so content of $abf(x)$ is ab and $g_1(x)h_1(x)$ is primitive since product of two primitive polynomials is primitive.

So content of $c_1c_2g_1(x)h_1(x)$ is c_1c_2. Thus from equation (2.1), $ab = c_1c_2$, $f(x) = g_1(x)h_1(x)$, where $g_1(x)$ and $h_1(x) \in \mathbb{Z}[x]$ and $deg\ g_1(x) = deg\ g(x)$ and $deg\ h_1(x) = deg\ h(x)$. $f(x)$ is reducible over $\mathbb{Z}$. $\square$

Irreducibility tests:

Theorem:(Mod p irreducibility test)

Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $degf(x) \geq 1$.

Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ modulo p.

If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $deg\bar{f}(x) = degf(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

proof

Let $f(x) \in \mathbb{Z}[x]$. If possible, let $f(x)$ be reducible over $\mathbb{Q}$, then we have $f(x) = g(x)h(x)$ with $g(x)$, $h(x) \in \mathbb{Z}[x]$ and both $g(x)$ and $h(x)$ have degree less than that of $f(x)$. Let $\bar{f}(x)$, $\bar{g}(x)$ and $\bar{h}(x)$ be the polynomials obtain from $f(x)$, $g(x)$ and $h(x)$ by reducing all the coefficient modulo p. Since $deg\ f(x) = deg\ \bar{f}(x)$, we have $deg\ \bar{g}(x) \leq deg\ g(x) < deg\bar{f}(x)$.

Again $deg\ \bar{h}(x) \leq deg\ h(x) < deg\ \bar{f}(x)$, but $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. $\bar{f}(x)$ is reducible over $\mathbb{Z}_p$, which is contradiction. Hence, $f(x)$ is irreducible over $\mathbb{Q}$. $\square$

Example

$f(x) = 9x^3 + 5x^2 + 5$.

Then in $\mathbb{Z}_2$, we have $\bar{f}(x) = x^3 + x^2 + 1$ and since $degf(x) = deg\ \bar{f}(x)$, $\bar{f}(0) = 1$and $\bar{f}(1) = 1 + 1 + 1 = 3 = 1$. $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2$. Therefore, so $f(x)$ is irreducible over $\mathbb{Q}$.

We found that $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2$. Thus $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem:(Eisenstein's Criterion)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Z}[x]$

If there is a prime p such that $p \nmid a_n$, $p \mid a_{n-1}$, $..., p \mid a_0$ *and* $p^2 \nmid a_0$, *then* $f(x)$ *is irreducible over* $\mathbb{Q}$

proof:

If possible let $f(x)$ be reducible over $\mathbb{Q}$. Then we know that $\exists$ elements $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$ and $deg\ g(x) \geq 1$, $deg\ h(x) < n$.

Say $g(x) = b_r x^r + b_{r-1}x^{r-1} + ... + b_0$ and $h(x) = c_s x^s + c_{s-1}x^{s-1} + ... + c_0$. Then since $p \mid a_0$ and $p^2 \nmid a_0$ and $a_0 = b_0 c_0$, so p divides one of b_0 and c_0 but not the both.

Let us consider the case $p \mid b_0$ and $p \nmid c_0$, since $p \nmid a_n \Rightarrow p \nmid b_r c_s \Rightarrow p \nmid b_r$ or $p \nmid c_s$. If $p \nmid b_r$ so there exist a least integer t such that $p \nmid b_t$. Now consider $a_t = b_t c_0 + b_{t-1}c_1 + ... + b_0 c_t$. By assumption, $p|a_t$ and by choice of t every summand on the right hand side after the first one is divisible by p .

Then it is true that p to divides $b_t c_0$, this is impossible.

p is prime and p divides neither b_t nor c_0, which gives contradiction.

Hence the statement. $\square$

Example

$f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ is irreducible over $\mathbb{Q}$ because $5 \nmid 3$ and $25 \nmid 20$ but 5 divides 15, -20, 10 and 20. So by Eisenstein's Criterion $f(x)$ is irreducible over $\mathbb{Q}$.

Euclidean domains (ED)

Norm

Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called norm on the integral domain R. If $N(a) > 0$ for $a \neq 0$ is called positive norm.

Division Algorithm

If $a, b \in \mathbb{Z} - \{0\}$, then there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r \leq |b|$, where q is quotient and r is the remainder.

Euclidean Domain The integral domain R is said to be a Euclidean domain, if there is a norm N on R such that for any two element a and b of R with $b \neq 0$ there exists unique elements q and r in R with $a = bq + r$, where $r = 0$ *or* $N(r) < N(b)$. The element q is called quotient and the element r is called remainder.

Examples

(1) Any Field is a trivial example of Euclidean domain. $a, b \neq 0 \in \mathbb{F}$. $a = qb + 0$, $r = 0 \Rightarrow q = ab^{-1}$.

(2) The ring $\mathbb{Z}$ is an Euclidean domain. $N : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ defined by $N(a) = |a|$. $a, b(\neq 0) \in \mathbb{Z}$. $a = bq + r$, $N(r) < N(b)$, $|r| < |b|$, for $b = 0$, $N(b) = 0$. Therefore $\mathbb{Z}$ is an Euclidean domain.

(3) If $\mathbb{F}$ is a field then the polynomial ring $\mathbb{F}[x]$ is a Euclidean domain with norm given by $N(p(x)) = deg\ p(x)$.

(4) The ring of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain with the norm given by $N(a + ib) = a^2 + b^2$.

Proposition:

Every ideal in a Euclidean domain is principal. More precisely, if I is any nonzero ideal in the Euclidean domain R then $I =< d >$, where d is any nonzero element of I with minimum norm.

Application

By using the above proposition we can know whether an Integral domain is Euclidean domain or not.

(1) $\mathbb{Z}$ is Euclidean domain. Every ideal in $\mathbb{Z}$ is principal ideal.

(2) $\mathbb{Z}[x]$ in not a ED because I$=< 2, x >$ is an ideal of $\mathbb{Z}[x]$ but I is not a principal ideal.

Principal ideal domains (PID)

A principal ideal domain is an integral domain in which every ideal is principal. i.e, every ideal has the form $< a >= \{ra | r \in R\}$ for some $a \in R$

Examples

(1) The ring of integer $\mathbb{Z}$ is a principal ideal domain generated by $< n >$.

(2) A field $\mathbb{F}$ is PID. The only ideals of $\mathbb{F}$ are 0 and $\mathbb{F}$ itself.

(3) If $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a principal ideal domain.

Unique factorization domains(UFD)

Associates

Elements a and b of an integral domain D are called associates if $a = ub$, where u is unit of D.

Irreducibles

A nonzero element a of an integral domain D is called an irreducible if a is not a unit and, whenever $b,\ c \in\ D$ with $a = bc$, then b or c is a unit.

Primes

A nonzero element a of an integral domain D is called prime, if a is not a unit and $a|bc \Rightarrow a|b$ or $a|c$.

Unique factorization domain

A Unique factorization domain (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

(i) r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 ... p_n$ and

(ii) the decomposition in (i) is unique up to associates namely if $r = q_1 q_2 ... q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i =\ 1,\ 2,\ ..., n$.

Examples

(1) A field $\mathbb{F}$ is trivially a unique factorization domain since every nonzero element is a unit. So there are no elements for which properties (i) and (ii) must be verified.

(2) The subring of the Gaussian integers $R = \mathbb{Z}[2i] = \{a+2bi \mid a, b \in \mathbb{Z}\}$, where $i^2 = -1$ is an integral domain but not a unique factorization domain because 4=2.2=(-2i)(2i).

(3)The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not an unique factorization domain,

since $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives two distinct factorizations of 6 into irreducibles.

Note

(1) FIELD $\Rightarrow$ ED $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ ID .

(2) ID$\not\Rightarrow$ UFD $\not\Rightarrow$ PID $\not\Rightarrow$ ED $\not\Rightarrow$ FIELD.

Counter examples of note (2)

(i) ID $\not\Rightarrow$ UFD

$\mathbb{Z}[\sqrt{-5}]$ is ID, but not UFD.

Explanation: We know every Euclidean domain is integral domain. $\mathbb{Z}[\sqrt{-5}] = \{a + b(\sqrt{-5})| \ a, \ b \in \mathbb{Z}\}$. $\mathbb{Z}[\sqrt{-5}]$ is an Euclidean domain with respect to the norm $N(a + b\ sqrt{-5}) = a^2+5b^2$. Hence, $\mathbb{Z}[\sqrt{-5}]$ is an integral domain. But, $\mathbb{Z}[\sqrt{-5}]$ is not an unique factorization domain, since $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives two distinct factorization of 6 into irreducibles.

(ii) UFD $\not\Rightarrow$ PID

$\mathbb{Z}[x]$ is UFD, but not PID.

According to one result, *R is unique factorization domain if and only if $R[x]$ is unique factorization domain.* Since $\mathbb{Z}$ is unique factorization domain so, $\mathbb{Z}[x]$ is unique factorization domain. But, $\mathbb{Z}[x]$ is not a principal ideal domain, since $< x, 2 >$ is an ideal of $\mathbb{Z}[x]$ but this not the principal ideal. So $\mathbb{Z}[x]$ is not a principal ideal domain.

(iii) PID $\not\Rightarrow$ ED

$\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a principal ideal domain, but not Euclidean domain.

$\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a principal ideal domain. Since, every ideal of this ring is principal.

We cannot find any ideal which is not principal in this ring. But, $\mathbb{Z}[(1+\sqrt{-19})/2]$ is not an Euclidean domain. To prove this we have to know about universal side divisor.

Universal side divisor

For any integral domain, let $\widetilde{R} = R^{\star} \cup \{0\}$ denote the collection of units of R together with 0. An element $u \in R - \widetilde{R}$ is called a universal side divisor if for every $x \in R$ there is some $z \in \widetilde{R}$ such that u divides $x - z$ in R.

Proposition: *Let R be an integral domain that is not a field. If R is a Euclidean domain then there are universal side divisor in R.*

Here in this example we will show that in $\mathbb{Z}[(1+\sqrt{-19})/2]$ there does not exist any universal side divisor. So this is not an Euclidean domain. Now only we have to show that $R = \mathbb{Z}[(1+\sqrt{-19})/2]$, does not contain any universal side divisor.

The units of $\mathbb{Z}[(1+\sqrt{-19})/2]$ are ± 1. Therefore $\widetilde{R} = \{0, \pm 1\}$. Suppose $u \in R$ is a universal side divisor and let $N(a + b(1+\sqrt{-19})/2) = a^2 + ab + 5b^2$ is the norm. If $a, b \in \mathbb{Z}$ and $b \neq 0$ then $a^2 + ab + 5b^2 = (a + b/2)^2 + 19/4b^2 \geq 5$ and so the smallest nonzero values of N on R are 1(for units ± 1) and 4(for ± 2). For $x = 2$, according to definition of universal side divisor, u must divide one of $2 - 0$ or $2 - (\pm)1$ in R, i.e, u is a nonunit divisor of 2 or 3 in R. Hence the only divisors of 2 in R are $\{\pm 1, \pm 2\}$. Similarly, the only divisors of 3 in R are $\{\pm 1, \pm 3\}$, so the only possible values for u are ± 2 or ± 3. By taking $x = (1+\sqrt{-19})/2$, none of x, $x \pm 1$ are divisible by ± 2 or ± 3 in R, so none of these is a universal side divisor. Hence, $\mathbb{Z}[(1+\sqrt{-19})/2]$ is not an Euclidean domain.

(iv) ED $\nRightarrow$ FIELD

$\mathbb{Z}$ is a Euclidean domain, but not a field.

$\mathbb{Z}$ is Euclidean domain with norm given by $N(a) = |a|$. But, $\mathbb{Z}$ is not a field because $\mathbb{Z}$ has no multiplicative inverse.

CHAPTER 3

FIELDS AND THEIR EXTENSIONS

An archaic name for field is rational domain. Fields have been used implicity ever since the discovery of addition, subtraction, multiplication and division. Cardan's formula dating from 16^{th} century used $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Lagrange used the field of rational functions in n-variable in his 1770 study of roots of polynomials. The first truely abstract notion of field is due to Dedekind. In 1877, he gave the following definition:

"I call a system A of numbers (not all zero) a field when the sum, difference, product and quotient of any two numbers except 0 in denominator in A also belongs to A. "
This is not completely general for the numbers. Taking into account ring definition, a field can be defined as
"A commutative ring with unity in which every nonzero element has a multiplicative inverse."
OR, " A field is a commutative ring in which we can divide by any nonzero element."
In fact in 1893, Dedekind's student Weber gave the first fully abstract definition of field which we use today. The definition as follows:

Field:

$\mathbb{F}$ is a field if

(1)$\mathbb{F}$ is an abelian group under addition.

(2)$\mathbb{F}/\{0\}$ is an abelian group under multiplication.

(3)Multiplication distributes over addition.

In other words, A nonempty set $\mathbb{F}$ with two binary operations addition and multiplication is a field if,

(1)For any $a, b \in \mathbb{F},\ a + b \in \mathbb{F}$.

(2)For any $a,\ b \in \mathbb{F},\ a+b=b+a$.

(3)For any $a,\ b,\ c \in \mathbb{F},\ (a+b)+c\ =\ a+(b+c)$.

(4)There is $a,\ 0 \in \mathbb{F}$ such that $a+0\ =\ 0+a\ =\ 0$ for every $a \in \mathbb{F}$.

(5)For every $a \in \mathbb{F}$ there is an element $-a,\ \mathbb{F}$ with $a+(-a)=(-a)+a=0$.

(6)For any $a,\ b \in \mathbb{F},\ ab \in \mathbb{F}$.

(7)For any $a,\ b \in \mathbb{F},\ ab=ba$.

(8)For any $a,\ b,\ c \in \mathbb{F},\ (ab)c=a(bc)$.

(9)There is $a,\ 1\ \in \mathbb{F}$ such that $a.1=1.a=a$, for every $a \in \mathbb{F}$.

(10)For every $a(\neq 0) \in \mathbb{F}$ there is an element $a^{-1} \in \mathbb{F}$ with $aa^{-1}\ =\ a^{-1}a\ =\ 1$.

(11)For every $a,\ b,\ c \in \mathbb{F}$

$(a+b)c=ac+bc$

$c(a+b)=ca+cb$.

Examples

(1)The set of rational numbers($\mathbb{Q}$).

(2)The set of real numbers ($\mathbb{R}$).

(3)The set of complex numbers($\mathbb{C}$).

(4)The field $\mathbb{F}$=$\mathbb{Q}(\sqrt{D})$ where D is not a perfect square.

$\mathbb{F}=\{a+b\sqrt{D}|a,b \in \mathbb{Q}\}$ where addition and multiplication is as usual.

(5)The field $\mathbb{F}=\mathbb{F}_p$ of integers modulo p,where p is a prime.

$\mathbb{F}_p=\{0,1,...p-1\}$ with addition and multiplication defined by mod p i.e, $i+j=k(mod\ p)$ and $ij=k(mod\ p)$.

Sub field:

A non-empty subset $\mathbb{E}$ of a field $\mathbb{F}$ is said to be a subfield of $\mathbb{F}$ if $\mathbb{E}$ is a field under the induced addition and multiplication. If a subfield $\mathbb{E}$ is not equal to $\mathbb{F}$ we shall say that $\mathbb{E}$ is proper subfield of $\mathbb{F}$.

Prime subfield

Let $\mathbb{F}$ be a field. By the prime subfield of $\mathbb{F}$ we mean the smallest subfield of $\mathbb{F}$.

Characteristic of a field

The characteristic of a field $\mathbb{F}$, denoted by char($\mathbb{F}$), is defined to be the smallest positive integer p such that $p \cdot 1_F = 0$ if such a p exists and is defined to be 0 otherwise.

Proposition:

Characteristic of a field either zero or prime.

proof:

According to the definition of characteristic of field, it is the smallest positive integer n such that $n \cdot 1_F = 0$ otherwise 0.

We have to show characteristics of field is prime.

Let n be the composite number such that

$n \cdot 1_{\mathbb{F}} = 0$

$\Rightarrow (a.b).1_{\mathbb{F}} = 0$

$\Rightarrow (a.1_{\mathbb{F}})(b.1_{\mathbb{F}}) = 0$

$\Rightarrow (a.1_{\mathbb{F}}) = 0 or\ (b.1_{\mathbb{F}}) = 0$, (since there exist no zero divisor).

Which is a contradiction that n is the smallest positive integer such that $n \cdot 1_F = 0$. So, the smallest integer must be prime. $\square$

Examples

(1) The fields $\mathbb{Q}$, $\mathbb{R}$ have characteristic 0.

(2) $F_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p.

Field isomorphism

Let $\mathbb{F}$ and $\mathbb{F}'$ be fields. A mapping $f : \mathbb{F} \to \mathbb{F}'$ is called an isomorphism if

(1) f is one-one and onto.

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

(3) $f(ab) = f(a)f(b)$.

Two fields $\mathbb{F}$ and $\mathbb{F}'$ are said to be isomorphic if there exists an isomorphism from one onto other.

Proposition:

Let $\phi : \mathbb{F} \to \mathbb{F}'$ be a homomorphism of fields. Then ϕ is either identically 0 or is injective,

so that the image of ϕ is either 0 or isomorphic to $\mathbb{F}$.

Extension Field:

Idea behind to develop extension fields

Some polynomials don't have zeros in the base field. The zeros of those polynomials are exist in some other field which is lager than the base field. Those fields are called extension fields.

Extension fields

Let $\mathbb{F}$ be a field and $\mathbb{E}$ be a field containing $\mathbb{F}$ as a subfield. Then $\mathbb{E}$ is called an extension of $\mathbb{F}$ and can be regarded as vector space over $\mathbb{F}$. $\mathbb{F}$ is called base field of the extension $\mathbb{E}$.

Examples

The extension field of $\mathbb{Q}$ is $\mathbb{R}$ and extension field of $\mathbb{R}$ is $\mathbb{C}$.

Theorem:

Fundamental theorem of field theory (Kronecker's Theorem, 1887) *Let F be a field and f(x) a non-constant polynomial in* $\mathbb{F}[x]$*, then there is an extension field* $\mathbb{E}$ *of* $\mathbb{F}$ *in which f(x) has a zero.*

proof:

$\mathbb{F}[x]$ is a principal ideal domain. So $\mathbb{F}[x]$ is unique factorization domain. So, $f(x)$ has an irreducible factor $p(x)$. We have to construct an extension field $\mathbb{E}[x]$ of $\mathbb{F}[x]$ in which $p(x)$ has a zero.

Let's consider the field $\mathbb{E} = \mathbb{F}[x]/< p(x) >$

Now $\phi : \mathbb{F} \to \mathbb{E}$ given by $\phi(a) = a+ < p(x) >$. ϕ is one-one, onto and preserves both the operations, so $\mathbb{E}$ has a sub filed isomorphic to $\mathbb{F}$.

Now we have to show $p(x)$ has a zero in $\mathbb{E}$.

Let

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \\ p(x+ < p(x) >) &= a_n(x+ < p(x) >)^n + a_{n-1}(x+ < p(x) >)^{n-1} + ... + a_0 \\ &= a_n(x^n+ < p(x) >) + a_{n-1}(x^{n-1}+ < p(x) >) + ... + a_0+ < p(x) > \\ &= a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \\ &= p(x)+ < p(x) > \\ &= 0+ < p(x) > \end{aligned}$$

So $x+ < p(x) >$ is a zero of $p(x)$ in $\mathbb{E}$. $\square$

Application

Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$

Then $\mathbb{E} = \mathbb{Q}[x]/ < x^2 + 1 >$

$$\begin{aligned} f(x+ < x^2 + 1 >) &= (x+ < x^2 + 1 >)^2 + 1 \\ &= x^2+ < x^2 + 1 > +1 \\ &= x^2 + 1+ < x^2 + 1 > \\ &= 0+ < x^2 + 1 > \end{aligned}$$

$x+ < x^2 + 1 >$ is a zero of $f(x)$ in $\mathbb{F}$.

Basic properties of field extensions

(1) Let $\mathbb{F}$, $\mathbb{B}$ and $\mathbb{E}$ be fields with $\mathbb{F} \subseteq \mathbb{B} \subseteq \mathbb{E}$. Then as $\mathbb{F}$-vector spaces, $\mathbb{B}$ is a subspace of $\mathbb{E}$, so $(\mathbb{B}/\mathbb{F}) \leq (\mathbb{E}/\mathbb{F})$.

(2) In 1894, Dedekind developed the theory of field extension that included the concept of degree. He formulated the proof of *Tower Theorem* stated below:

Tower Theorem:

If $\mathbb{B}$ is the finite extension of $\mathbb{F}$ and $\mathbb{E}$ is the finite extension of $\mathbb{B}$, then $\mathbb{E}$ is the finite extension of $\mathbb{F}$ and ($\mathbb{E}/\mathbb{F}$)= ($\mathbb{E}/\mathbb{B}$)($\mathbb{B}/\mathbb{F}$).

proof:

Let $\{e_1,\ e_2,\ ..., e_n\}$ be a basis of ($\mathbb{B}$/ $\mathbb{F}$) and $\{f_1, f_2, ...f_m\}$ a basis of ($\mathbb{E}$/ $\mathbb{B}$)

We have to show that $\{e_i f_j | 1 \leq i \leq n,\ 1 \leq j \leq m\}$ is a basis of $\mathbb{E}$/ $\mathbb{F}$. Let α be any element of $\mathbb{E}$.

Therefore, $\alpha = \sum_{j=1}^{m} b_j f_j$ where $b_j \in \mathbb{B}$ and $b_j = \sum_{i=1}^{n} \lambda_{ij} e_i$ where $\lambda_{ij} \in \mathbb{F}$

Then $\alpha = \sum_{j=1}^{m} (\sum_{i=1}^{n} \lambda_{ij} e_i) f_j$

$= \sum_{j=1}^{m} \sum_{i=1}^{n} \lambda_{ij} e_i f_j$

This shows that $\{e_i f_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ generates $\mathbb{E}$ over $\mathbb{F}$.

Now to show linear independence.

Let $\sum_{j=1}^{m} (\sum_{i=1}^{n} \mu_{ij} e_i) f_j = 0$

Since, $\{f_1, f_2, ..., f_m\}$ is linear independent over $\mathbb{B}$ so $\sum_{i=1}^{n} \mu_{ij} e_i = 0\ \forall\ j$,

Since $\{e_1, e_2, ...e_n\}$ are linear independent over $\mathbb{F}$ so $\mu_{ij} = 0\ \forall\ i$ and j.

Hence $\{e_i f_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of $\mathbb{E}$/ $\mathbb{F}$ consisting of mn elements. □

(3) Let $\mathbb{E}$ be an extension of $\mathbb{F}$, let $\mathbb{B}$ and $\mathbb{D}$ be subfields of $\mathbb{E}$, both of which are extension of $\mathbb{F}$. Then $\mathbb{B} \cap \mathbb{D}$ is a subfield of $\mathbb{E}$ which is also an extension of $\mathbb{F}$.

(4) Let $\mathbb{E}$ be an extension of $\mathbb{F}$ and let $\mathbb{B}$ and $\mathbb{D}$ be subfields of $\mathbb{E}$, both of which are extension of $\mathbb{F}$. Then $\mathbb{BD}$, the composite of $\mathbb{B}$ and $\mathbb{D}$ is the smallest subfield of $\mathbb{E}$ that contains $\mathbb{B}$ and $\mathbb{D}$ also an extension of $\mathbb{F}$.

(5)Let $\mathbb{E}$ be an extension of $\mathbb{F}$, and let $\{\alpha_i\}$ be a set of elements of $\mathbb{E}$. Then $\mathbb{F}(\{\alpha_i\})$. This is the field obtained by adjoining $\{\alpha_i\}$.

(6)**Simple extension**

An extension $\mathbb{E}/\mathbb{F}$ is called a simple extension if, $\mathbb{E}/\mathbb{F}$ is generated by a single element. i.e, if $\mathbb{E}$=$\mathbb{F}(a)$ for some $a \in \mathbb{E}$ such an element is called a primitive element for the extension $\mathbb{E}/\mathbb{F}$.

Example

$(\mathbb{Q}(\sqrt{2}))|\mathbb{Q}$ is a simple extension.

Splitting Field:

Splitting Field:

Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ and let $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ can be factored as a product of linear factors in $\mathbb{E}[x]$. We call $\mathbb{E}$ a splitting field for $f(x)$ over $\mathbb{F}$ if $f(x)$ splits in $\mathbb{E}$ but in no proper subfield of $\mathbb{E}$.

Note:

(1) $(x - \alpha)$ is a factor of $f(x)$ iff $f(\alpha) = 0$. i.e, α is a root of $f(x)$. We say $f(x)$ splits in $\mathbb{E}$ if all the roots of $f(x)$ are in $\mathbb{E}$. We say $\mathbb{E}$ as a splitting field if all the roots of $f(x)$ lie in $\mathbb{E}$ but not in any proper subfield of $\mathbb{E}$.

(2) Splitting field of a polynomial over a field depends not only on the polynomial but the field as well.

Examples

(1)$f(x) = x^2 + 1 \in \mathbb{Q}[x],\ x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$. So $f(x)$ splits over $\mathbb{C}$, but splitting field over $\mathbb{Q}$ is $\mathbb{Q}[i] = \{r + si | r, s \in \mathbb{Q}\}$ and splitting field over $\mathbb{R}$ is $\mathbb{C}$.

(2)$f(x) = x^2 - 2 \in \mathbb{Q}[x]$ splits in R but a splitting field of $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2} | r, s \in \mathbb{Q}\}$.

Note:

There is a useful analogy between the definition of splitting field and the definition of an irreducible of polynomial. i.e, $f(x)$ is irreducible over filed similarly $\mathbb{E}$ is a splitting field for $f(x)$ over field.

Existence of splitting field

Theorem:

Let $\mathbb{F}$ be a field and let $f(x)$ be a non-constant element of $\mathbb{F}[x]$. Then there exists a splitting field $\mathbb{E}$ for $f(x)$ over $\mathbb{F}$.

proof:

Let's prove it by induction on *deg* $f(x)$. If *deg* $f(x) = 1$, then is already linear and $\mathbb{E} = \mathbb{F}$.

Now suppose that the statement is true for all fields and all polynomial of degree less than that of $f(x) = 1$.

Hence by fundamental theorem of field theory, there is an extension $\mathbb{E}$ of $\mathbb{F}$ in which $f(x)$ has a zero, (say a_1). $f(x) = (x - a_1)g(x)$, where $g(x) \in \mathbb{F}[x]$.

since $deg\ g(x) < deg\ f(x)$, by induction, there is a field $\mathbb{M}$ that contains $\mathbb{E}$ and all the zeros of $deg\ g(x)$ say $a_2,\ a_3,\ ..., a_n$. A splitting field for $f(x)$ over $\mathbb{F}$ is $\mathbb{F}(a_1, a_2, ..., a_n)$. □

Example

Let's consider polynomial $f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$ over $\mathbb{Q}$. Zeros of $f(x) = \pm\sqrt{2}$ and $\pm i$ so the splitting field for $f(x)$ over $\mathbb{Q}$ is

$\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$

$= \{\alpha + \beta i | \alpha,\ \beta \in \mathbb{Q}(\sqrt{2})\}$

$= \{(a + b\sqrt{2}) + (c + d\sqrt{2})i | a,\ b,\ c,\ d \in \mathbb{Q}\}$

Theorem:

Let $\mathbb{F}$ be a field and $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$. If a is a zero of $p(x)$ in some extension $\mathbb{E}$ of $\mathbb{F}$, then $\mathbb{F}(a)$ is isomorphic to $\mathbb{F}[x]/ < p(x) >$. Furthermore, if deg p(x)=n, then every member of $\mathbb{F}(a)$ can be uniquely expressed in the form $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + ... + c_1 a + c_0$, where $c_0, c_1, ..., c_{n-1} \in \mathbb{F}$.

Example

$f(x) = x^6 - 2$ over $\mathbb{Q}$. So $x = \sqrt[6]{2}$ is the zero of $f(x)$.

Therefore, $\{1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6}\}$ is a basis for $\mathbb{Q}(\sqrt[6]{2})$ over $\mathbb{Q}$.

Thus $\mathbb{Q}(\sqrt[6]{2}) = \{a_0 + a_1 2^{1/6} + a_2 2^{2/6} + a_3 2^{3/6} + a_4 2^{4/6} + a_5 2^{5/6}\ | a_i \in \mathbb{Q},\ i = 0, 1, ...5\}$

This field is isomorphic to $\mathbb{Q}[x]/ < x^6 - 2 >$.

Splitting fields are unique

Lemma:

Let $\mathbb{F}$ be a field,let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$, and let a be a zero of $p(x)$ in some extension of $\mathbb{F}$. If ϕ is a field isomorphism from $\mathbb{F}$ to $\mathbb{F}'$ and b is a zero of $\phi(p(x))$ in some extension of $\mathbb{F}'$, then there is an isomorphism from $\mathbb{F}(a)$ to $\mathbb{F}'(b)$ that agrees with ϕ on $\mathbb{F}$ and carries a to b.

Theorem:

Let ϕ be an isomorphism from a field $\mathbb{F}$ to $\mathbb{F}'$ and let $f(x) \in \mathbb{F}[x]$. If $\mathbb{E}$ is a splitting field for $f(x)$ over $\mathbb{F}$ and $\mathbb{E}'$ is a splitting field for $\phi(f(x))$ over $\mathbb{F}'$, then there is an isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ that agrees with ϕ on $\mathbb{F}$.

proof:

Let's prove it by induction on *deg* $f(x)$. If *deg* $f(x) = 1$, then $\mathbb{E}$=$\mathbb{F}$ and $\mathbb{E}' = \mathbb{F}'$. So that ϕ is itself the required mapping.

If $degf(x) > 1$, let $p(x)$ be an irreducible factor of $f(x)$, let a be a zero of $p(x)$ in $\mathbb{E}$, and let b be a zero of $\phi(p(x))$ in $\mathbb{E}'$. By the above lemma, there is an isomorphism ψ from $\mathbb{F}(a)$ to $\mathbb{F}'(b)$ that agrees with ϕ on $\mathbb{F}$ and carries a to b. Now, $f(x) = (x-a)g(x)$, where $g(x) \in \mathbb{F}(a)[x]$. Then $\mathbb{E}$ be a splitting field of $g(x)$ over $\mathbb{F}(a)$.

$\mathbb{E}'$ be a splitting field of $\psi(g(x))$ over $\mathbb{F}'(b)$, since *deg* $g(x) <$ *deg* $f(x)$, there is an isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ that agrees with ψ on $\mathbb{F}(a)$ and therefore with ϕ on $\mathbb{F}$. □

Corollary:

Splitting field are unique

Let $\mathbb{F}$ be a field and let$f(x) \in \mathbb{F}[x]$. Then any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic.

proof:

Let $\mathbb{E}$ and $\mathbb{E}'$ are splitting fields of $f(x)$ over $\mathbb{F}$. By the previous theorem, ϕ be the identity from $\mathbb{F}$ to $\mathbb{F}$. So splitting fields are unique. □

Algebraic extension

Algebraic extension

Let $\mathbb{E}$ be an extension field of a field $\mathbb{F}$ and let $a \in \mathbb{E}$. We call a algebraic over $\mathbb{F}$ if a is the zero of some nonzero polynomial in $\mathbb{F}[x]$. An extension $\mathbb{E}$ of $\mathbb{F}$ is called an algebraic extension of $\mathbb{F}$ if every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$.

Transcendental extension

If a is not algebraic over $\mathbb{F}$, then it is transcendental over $\mathbb{F}$. If $\mathbb{E}$ is not an algebraic extension, then it is a transcendental extension.

Examples

(1) e is transcendental over $\mathbb{Q}$.

(2) π is transcendental over $\mathbb{Q}$.

(3) It is still unknown that $e + \pi$ is transcendental or not.

Characterization of extensions

Theorem: *Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$ and let $a \in \mathbb{E}$. If a is algebraic over $\mathbb{F}$, let $p(x) \in \mathbb{F}[x]$ be a polynomial of least degree such that $p(a) = 0$, then $p(x)$ is irreducible over $\mathbb{F}$.*

proof:

Let $p(x)$ be reducible over $\mathbb{F}$. So $p(x) = p_1(x)p_2(x)$ and $deg\ p_1(x) < p(x)$ and $deg\ p_2(x) < p(x)$.

Now $p(a) = 0$.

$\Rightarrow p(a) = p_1(a)p_2(a) = 0$.

$\Rightarrow p_1(a) = 0$ or $p_2(a) = 0$.

i.e, a satisfies a polynomial of degree less than $p(x)$ which is a contradiction.

So $p(x)$ is irreducible over $\mathbb{F}$. $\square$

Divisibility property

Theorem: *If a is algebraic over $\mathbb{F}$. Let $p(x) \in \mathbb{F}[x]$ be a polynomial of least degree such that $p(a) = 0$. If $f(x) \in \mathbb{F}[x]$ and $f(a) = 0$ then $p(x) \mid f(x)$ in $\mathbb{F}[x]$.*

proof:

Let $f(x) \in \mathbb{F}[x]$, by division algorithm $f(x) = p(x)q(x) + r(x)$ where $r(x) = 0$ or $deg\ r(x) < deg\ p(x)$.

Then $f(a) = 0 \Rightarrow p(a)q(a) + r(a) = 0 \Rightarrow r(a) = 0$, since $p(a) = 0$ Thus $p(x) \mid f(x)$. $\square$

Degree of an extension

Let $\mathbb{E}$ be an extension of a field $\mathbb{F}$. We say that $\mathbb{E}$ has degree n over $\mathbb{F}$ if $\mathbb{E}$ has dimension n as a vector space over $\mathbb{F}$. It is denoted as $[\mathbb{E} : \mathbb{F}]$. If $[\mathbb{E} : \mathbb{F}]$ is finite, then $\mathbb{E}$ is called a finite extension of $\mathbb{F}$; otherwise $\mathbb{E}$ is an infinite extension of $\mathbb{F}$.

Example

(1) The field of complex numbers has degree 2 over the reals since $\{1, i\}$ is a basis.

(2) If a is algebraic over $\mathbb{F}$ and its minimal polynomial over $\mathbb{F}$ has degree n, then we have $\{1, a, ...a^{n-1}\}$ is a basis for $\mathbb{F}(a)$ over $\mathbb{F}$ and therefore $[F(a) : F] = n$. So a has degree n over $\mathbb{F}$.

Finite implies algebraic

Theorem: *If* $\mathbb{E}$ *is a finite extension of* $\mathbb{F}$*, then* $\mathbb{E}$ *is an algebraic extension of* $\mathbb{F}$*.*

proof:

Suppose that $[\mathbb{E} : \mathbb{F}] = n$ and $a \in \mathbb{E}$. Then the set $\{1, a, ..., a^n\}$ is linearly dependent over $\mathbb{F}$, i.e, there are elements $c_0, c_1, ..., c_n$ in $\mathbb{F}$ not all zero, such that $c_n a^n + c_{n-1} a^{n-1} + ... + c_1 a + c_0$.

Then a is a zero of the nonzero polynomial, $f(x) = c_n x^n + c_{n-1} x^{n-1} + ... + c_1 x + c_0$.

Hence a is algebraic over $\mathbb{F}$. $\square$

Converse

The converse of the above theorem need not be true.

Counter example

$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}.....)$ is an algebraic extension of $\mathbb{Q}$ that contains elements of every degree over $\mathbb{Q}$ but clearly this is not a finite extension.

$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$

Theorem:

Let $\mathbb{K}$ *be a finite extension field of the field* $\mathbb{E}$ *and* $\mathbb{E}$ *be a finite extension field of the field* $\mathbb{F}$*. Then* $\mathbb{K}$ *is a finite extension field of* $\mathbb{F}$ *and* $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$

Example

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$

$= 2.2 = 4$

Kronecker Theorem

Theorem:

If $g(x)$ is a polynomial in $\mathbb{F}[x]$ of degreen ≥ 1 and is irreducible over $\mathbb{F}$, then there is an extension $\mathbb{K}$ of $\mathbb{F}$ with [$\mathbb{K}$:$\mathbb{F}$]=n in which $g(x)$ has a root.

proof:

Let $g(x)$ is irreducible over $\mathbb{F}[x]$. So the ideal $I =< g(x) >$ in $\mathbb{F}[x]$ is a maximal ideal. Since, R/A is a field iff A is maximal ideal. $\mathbb{K} = \mathbb{F}[x]/I$ is a field. The mapping $f : \mathbb{F} \to \mathbb{K}$ given by $a \to a + I$ is an isomorphism of $\mathbb{F}$ onto its image $\mathbb{F}' \subset \mathbb{K}$. Identifying $\mathbb{F}$ with $\mathbb{F}'$, $\mathbb{K}$ as an extension of $\mathbb{F}$.

We have to show that $x + I$ is a root of the polynomial $g(x)$. Now $g(x + I) = g(x) + I = 0 + I$ as $g(x) \in I$

So $x + I$ is a root of $g(x)$, and $\{1 + I, x + I, ..., x^{n-1} + I\}$ is a basis of $\mathbb{F}[x]/I$ over $\mathbb{F}$.

So $[\mathbb{K} : \mathbb{F}] = n$. $\square$

Properties of algebraic extensions:

Theorem:(Algebraic over algebraic is algebraic)

If $\mathbb{K}$ is an algebraic extension of $\mathbb{E}$ and $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$.

proof:

Let $a \in \mathbb{K}$, as $\mathbb{K}$ is algebraic over $\mathbb{E}$ so there is $b_0,\ b_1,\ ..., b_n \in \mathbb{E}$ such that $b_0 + b_0 a + ... + b_n a^n = 0$.

Again $\mathbb{E}$ is algebraic over $\mathbb{F}$ and $b_0, b_1, ..., b_n \in \mathbb{E}$ so $b_0, b_1, ..., b_n$ algebraic over $\mathbb{F}$.

$\mathbb{E}|\mathbb{F}$ is finite and $\mathbb{E}$ is isomorphic to $\mathbb{F}(b_0, b_1, ..., b_n)$.

So $[\mathbb{F}(b_0, b_1, ..., b_n) : \mathbb{F}]$=finite. Let's take $\mathbb{M} = \mathbb{F}(b_0, b_1, ..., b_n)$. Therefore $[\mathbb{M} : \mathbb{F}]$=finite

a satisfies the equation $b_0 + b_0 a + ... + b_n a^n = 0$

So a is algebraic over $\mathbb{M}$

$\Rightarrow [\mathbb{M}(a) : \mathbb{M}]$ =finite

Now, $[\mathbb{M}(a) : \mathbb{F}] = [\mathbb{M}(a) : \mathbb{M}][\mathbb{M} : \mathbb{F}]$ =finite

So $\mathbb{M}(a)$ is algebraic over $\mathbb{F}$. Thus a is algebraic over $\mathbb{F}$. Hence, $\mathbb{K}$ is algebraic over $\mathbb{F}$. $\square$

Corollary:(Subfield of Algebraic Elements)

Let $\mathbb{E}$ *be an extension field of the field* $\mathbb{F}$*. Then the set of all elements of* $\mathbb{E}$ *that are algebraic over* $\mathbb{F}$ *is a subfield of* $\mathbb{E}$*.*

proof:

Suppose that $a, b \in \mathbb{E}$ are algebraic over $\mathbb{F}$ and $b \neq 0$.

We have to show $a + b, a - b, ab, a/b$ are algebraic over $\mathbb{F}$. i.e, to show $[\mathbb{F}(a, b) : \mathbb{F}]$ is algebraic. Now, $[\mathbb{F}(a, b) : \mathbb{F}]$=$[\mathbb{F}(a, b) : \mathbb{F}(b)][\mathbb{F}(b) : \mathbb{F}]$.

Since a is algebraic over $\mathbb{F}$, it is certainly algebraic over $\mathbb{F}(b)$

$[\mathbb{F}(a, b) : \mathbb{F}(b)]$ and $[\mathbb{F}(b) : \mathbb{F}]$ are finite.

So, $[\mathbb{F}(a, b) : \mathbb{F}]$=finite. $\square$

CHAPTER 4

AN INTRODUCTION TO GALOIS THEORY

Motivation

Galois theory is a big subject. However, there are two important problems which provide some motivation for studying Galois Theory. The problems are:

(1) The existence of polynomials which are not soluble by radicals.

(2) Some results about classical Euclidean Geometry. For example we cannot trisect an angle using ruler and a compass and certain regular polygons cannot be constructed using ruler and compass.

Soluble by radicals

When we can find the solution for a polynomial with rational coefficients using only rational numbers and operations of addition, subtraction, multiplication, division and finding the n^{th} roots, we say that polynomial is soluble by radicals.

Remark:

Using Galois Theory we can prove that if the degree of polynomial is less that 5 then the polynomials is soluble by radicals but the polynomials of degree 5 and higher not soluble by radicals.

History

Galois Theory is named after a French Mathematician *Evariste Galois* (1811-1832) who did some very important work in this area. He had a very dramatic and difficult life.

Galois introduced many important topics in algebra i.e, normal subgroups, isomorphisms, simple groups, finite fields, Galois theory etc. His work provides a method for disposing of several famous constructibility problems, such as trisecting an arbitrary angle and doubling a cube.

Basic definitions

Automorphism

Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$. An automorphism of $\mathbb{E}$ is a ring isomorphism form $\mathbb{E}$ onto $\mathbb{E}$, denoted by Aut($\mathbb{F}$). Any field has at least one automorphism, the identity map(trivial automorphism).

Group fixing $\mathbb{F}$

An automorphism $\phi \in Aut(\mathbb{F})$ is said to fix an element $a \in \mathbb{E}$ if $\phi a = a$. If $\mathbb{F}$ is subfield of $\mathbb{E}$ then automorphism ϕ is said to be fix $\mathbb{F}$ if ϕa=$a \ \ \forall \ a \in \mathbb{F}$.

Galois group of $\mathbb{E}$ over $\mathbb{F}$

Galois group of $\mathbb{E}$ over $\mathbb{F}$ is the set of all automorphism of $\mathbb{E}$ that take every element of $\mathbb{F}$ to itself. It is denoted as Gal($\mathbb{E}/\mathbb{F}$).

Fixed field of $\mathbb{H}$

If $\mathbb{H}$ is a subgroup of Gal($\mathbb{E}/\mathbb{F}$), the set $\mathbb{E}_{\mathbb{H}} = \{x \in \mathbb{E} | \phi(x) = x \forall \phi \in \mathbb{H}\}$ is called the fixed field of $\mathbb{H}$.

Conjugate element

Let $\mathbb{E}$ be a finite extension of a field $\mathbb{F}$, then two element α and β of a field $\mathbb{E}$ are said to be conjugate over $\mathbb{F}$ if they have the same minimal polynomial over $\mathbb{F}$.

Examples:

(1) Let's consider the extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$

$\phi(\mathbb{Q}(\sqrt{2})) \to \mathbb{Q}(\sqrt{2})$ such that $\phi(a) = a \ , \forall \ a \in \mathbb{Q}$

$$\begin{aligned} \phi(a + b\sqrt{2}) &= \phi(a) + \phi(b\sqrt{2}) \\ &= a + \phi(b)\phi(\sqrt{2}) \\ &= a + b\phi(\sqrt{2}) \end{aligned}$$

An auto morphism $\phi(\mathbb{Q}(\sqrt{2}))$ is determine if $\mathbb{Q}(\sqrt{2})$ is known.

$2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \phi(\sqrt{2})\phi(\sqrt{2}) = (\phi(\sqrt{2}))^2$

Therefore $\phi(\sqrt{2}) = \pm\sqrt{2}$

so$\left|Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})\right| = 2$ i.e, the identity map and the mapping $a + b\sqrt{2} \to a - b\sqrt{2}$ are the two required mappings.

The Fixed Field $Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ is $\mathbb{Q}$ as everything is fixed by the automorphism defined by $a + b\sqrt{2} \to a - b\sqrt{2}$ and $a + b\sqrt{2} \to a + b\sqrt{2}$ which is equivalent to $a + b\sqrt{2} = a - b\sqrt{2} \Rightarrow b = 0$

(2) Let's consider the extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$ similarly as above example an automorphism ϕ of $\mathbb{Q}(\sqrt[3]{2})$ is completely determines by $\phi(\sqrt[3]{2})$.

$\phi(\sqrt[3]{2})$ is a cube root of 2, therefore $\phi(\sqrt[3]{2}) = \sqrt[3]{2},\ \sqrt[3]{2}\omega$ *or* $\sqrt[3]{2}\omega^2$, where $\omega^3 = 1$ and $\omega \neq 1$.

Since, $\phi(\sqrt[3]{2})$ is real, the only possibility is $\mathbb{Q}(\sqrt[3]{2}) = \sqrt[3]{2}$. Hence the automorphism is $a + b\sqrt[3]{2} \to a + b\sqrt[3]{2}$

$\left|Gal(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})\right| = 1$ and Fixed Field $Gal(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$ is $\mathbb{Q}(\sqrt[3]{2})$.

Galois extension

A finite extension $\mathbb{E}/\mathbb{F}$ is said to be Galois extension if $|Gal(\mathbb{E}|\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$

where $[\mathbb{E} : \mathbb{F}]$ is the degree of extension $\mathbb{E}/\mathbb{F}$.

Examples

(1) Let's consider the extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}|a, b \in \mathbb{Q}\}$

$\phi(\mathbb{Q}(\sqrt{2})) \to \mathbb{Q}(\sqrt{2})$ such that $\phi(a) = a\ \forall\ a \in \mathbb{Q}$

$$\begin{aligned} \phi(a + b\sqrt{2}) &= \phi(a) + \phi(b\sqrt{2}) \\ &= a + \phi(b)\phi(\sqrt{2}) \\ &= a + b\phi(\sqrt{2}) \end{aligned}$$

An auto morphism $\phi(\mathbb{Q}(\sqrt{2}))$ is determine if $\mathbb{Q}(\sqrt{2})$ is known.

$2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \phi(\sqrt{2})\phi(\sqrt{2}) = (\phi(\sqrt{2}))^2$

Therefore $\phi(\sqrt{2}) = \pm\sqrt{2}$

so$\left|Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})\right| = 2$ i.e, the identity map and the mapping $a + b\sqrt{2} \to a - b\sqrt{2}$ are

the two required mappings.

The Fixed field $Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ is $\mathbb{Q}$ as everything is fixed by the automorphism defined by $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$ and $a + b\sqrt{2} \rightarrow a + b\sqrt{2}$ which is equivalent to $a + b\sqrt{2} = a - b\sqrt{2} \Rightarrow b = 0$. Here, $Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$=2. So this extension is Galois Extension.

(2) Let's consider the extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$ similarly as above example an automorphism ϕ of $\mathbb{Q}(\sqrt[3]{2})$ is completely determines by $\phi(\sqrt[3]{2})$.

$\phi(\sqrt[3]{2})$ is a cube root of 2, therefore $\phi(\sqrt[3]{2}) = \sqrt[3]{2},\ \sqrt[3]{2}\omega$ *or* $\sqrt[3]{2}\omega^2$, where $\omega^3 = 1$ and $\omega \neq 1$. Since, $\phi(\sqrt[3]{2})$ is real, the only possibility is $\mathbb{Q}(\sqrt[3]{2}) = \sqrt[3]{2}$. Hence the automorphism is $a + b\sqrt[3]{2} \rightarrow a + b\sqrt[3]{2}$. $\left|Gal(\mathbb{Q}(\sqrt[3]{2}|\mathbb{Q}))\right| = 1$ and Fixed field $Gal(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$ is $\mathbb{Q}(\sqrt[3]{2})$. This is not a Galois extension.

Normal Extension

Let $\mathbb{E}$ be a finite extension of a field $\mathbb{F}$. The extension $\mathbb{E}$ is said to be normal extension of $\mathbb{F}$ if the fixed field of $Gal(\mathbb{E}/\mathbb{F})$ is $\mathbb{F}$ itself.

Note:

The followings are equivalent statements.

(1) $\mathbb{E}$ is normal extension of $\mathbb{F}$.

(2) $\mathbb{F}$ is the fixed field of $Gal(\mathbb{E}/\mathbb{F})$.

(3) $[\mathbb{E} : \mathbb{F}] = |Gal(\mathbb{E}/\mathbb{F})|$.

Fundamental Theorem Of Galois Theory

Let $\mathbb{F}$ be field of characteristic 0 or a finite field. If $\mathbb{E}$ is the splitting field over $\mathbb{F}$ for some polynomial in $\mathbb{F}[x]$, then the mapping from the set of subfields of $\mathbb{E}$ containing $\mathbb{F}$ to the set of subgroups of $Gal(\mathbb{E}|\mathbb{F})$ given by $\mathbb{K} \rightarrow Gal(\mathbb{E}|\mathbb{K})$ is a one-to-one correspondence. Furthermore, for any subfield $\mathbb{K}$ of $\mathbb{E}$ containing $\mathbb{F}$,

(1) $[\mathbb{E} : \mathbb{K}] = |Gal(\mathbb{E}|\mathbb{K})|$ and $[\mathbb{K} : \mathbb{F}] = |Gal(\mathbb{E}|\mathbb{F})/\,|Gal(\mathbb{E}|\mathbb{K})||$. (The index of $Gal(\mathbb{E}|\mathbb{K})$ in $Gal(\mathbb{E}|\mathbb{F})$ equals the degree of $\mathbb{K}$ over $\mathbb{F}$.)

(2) If $\mathbb{K}$ is the splitting field of some polynomial in $\mathbb{F}[x]$, then $Gal(\mathbb{E}|\mathbb{K})$ is normal subgroup of $Gal(\mathbb{E}|\mathbb{F})$ and $Gal(\mathbb{E}|\mathbb{F})$ is isomorphic to $Gal(\mathbb{E}|\mathbb{F})/Gal(\mathbb{E}|\mathbb{K})$

(3) $\mathbb{K} = \mathbb{E}_{Gal(E|K)}$. *(The fixed field of* $Gal(\mathbb{E}|\mathbb{K})$ *is* $\mathbb{K}$*)*

(4) If $\mathbb{H}$ *is a subgroup of* $Gal(\mathbb{E}|\mathbb{F})$*, then* $\mathbb{H} = Gal(\mathbb{E}/\mathbb{E}_H)$*. (The automorphism group of* $\mathbb{E}$ *fixing* $\mathbb{E}_H$ *is* $\mathbb{H}$*)*

proof:

Let $S = \{\mathbb{K} : \mathbb{F} \subset \mathbb{K}$ and $\mathbb{K}$ is subfield of $\mathbb{E}\}$

$S' = \{\mathbb{H} : \mathbb{H}$ is subgroup of $Gal(\mathbb{E}|\mathbb{F})\}$

Claim-1

$\phi : S \to S'$ defined by $\mathbb{K} \to Gal(\mathbb{E}|\mathbb{K})$ where $\mathbb{K} \in S$ is bijective or there exists a one-to-one correspondence between S and S'.

$\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ so that $Gal(\mathbb{E}|\mathbb{K}) \subset Gal(\mathbb{E}|\mathbb{F})$.

Also $Gal(\mathbb{E}|\mathbb{K})$ and $Gal(\mathbb{E}|\mathbb{F})$ are the subgroups of the group of all automorphism of $\{\mathbb{E}\}$, therefore $Gal(\mathbb{E}|\mathbb{K})$ is a subgroup of $Gal(\mathbb{E}|\mathbb{F})$.

Thus for each subfield of $\mathbb{K}$ of $\mathbb{E}$ containing $\mathbb{F}$ we can find a subgroup $Gal(\mathbb{E}|\mathbb{K})$ of $Gal(\mathbb{E}|\mathbb{F})$.

ϕ is one − one

Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be any two subfields of $\mathbb{E}$ containing $\mathbb{F}$

$\phi(\mathbb{K}_1) = \phi(\mathbb{K}_2)$

$\Rightarrow Gal(\mathbb{E}/\mathbb{K}_1) = Gal(\mathbb{E}/\mathbb{K}_2)$

$\Rightarrow E_M = E_N$ (Where M=The fixed field of $Gal(\mathbb{E}/\mathbb{K}_1)$ Let N=The fixed field of $Gal(\mathbb{E}/\mathbb{K}_2)$)

$\Rightarrow \mathbb{K}_1 = \mathbb{K}_2$, (Since $\mathbb{E}$ is splitting field over $\mathbb{F}$ so $\mathbb{E}$ is normal extension of $\mathbb{F}$)

ϕ is onto

Let $\mathbb{H}$ be an arbitrary subgroup of $Gal(\mathbb{E}/\mathbb{F})$, then the fixed field of $\mathbb{H}$ is denoted by $\mathbb{E}_{\mathbb{H}}$ which is given by $\mathbb{E}_{\mathbb{H}} = \{a \in \mathbb{E} : \psi(a) = a \ \forall \ \psi \in \mathbb{H}\}$.

Then $\mathbb{H} = Gal(\mathbb{E}/\mathbb{E}_{\mathbb{H}})$.

This shows that each subgroup of $Gal(\mathbb{E}|\mathbb{F})$ is of the form $Gal(\mathbb{E}/\mathbb{E}_{\mathbb{H}})$ such that $\mathbb{F} \subseteq \mathbb{E}_{\mathbb{H}} \subseteq \mathbb{E}$ and corresponding to this subgroup $Gal(\mathbb{E}/\mathbb{E}_{\mathbb{H}})$ there exists a subfield $\mathbb{E}_{\mathbb{H}}$ of $\mathbb{E}$ containing $\mathbb{F}$ such that $\phi(\mathbb{E}_{\mathbb{H}}) = Gal(\mathbb{E}/\mathbb{E}_{\mathbb{H}})$.

(1) $\mathbb{E}$ is normal extension of $\mathbb{F}$ and $\mathbb{K}$ is subfield of $\mathbb{E}$ containing $\mathbb{F}$ such that $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$ then $\mathbb{E}$ is normal extension of $\mathbb{K}$ therefore we have $[\mathbb{E} : \mathbb{F}] = |Gal(\mathbb{E}/\mathbb{F})|$ and $[\mathbb{E} : \mathbb{K}] =$

$|Gal(\mathbb{E}/\mathbb{K})|$

Moreover $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$

$\Rightarrow |Gal(\mathbb{E}/\mathbb{F})| = |Gal(\mathbb{E}/\mathbb{K})|\,[\mathbb{K} : \mathbb{F}]$

$\Rightarrow [\mathbb{K} : \mathbb{F}] = |Gal(\mathbb{E}/\mathbb{F})|\,|Gal(\mathbb{E}/\mathbb{K})|$

(2) Given that $\mathbb{K}$ is the splitting field of some polynomial in $\mathbb{F}[x]$. i.e, $\mathbb{K}$ is normal extension of $\mathbb{F}$. We have to show $Gal(\mathbb{E}/\mathbb{K})$ is normal subgroup of $Gal(\mathbb{E}/\mathbb{F})$ i.e, to show for any $\sigma \in Gal(\mathbb{E}/\mathbb{F})$ and $\mu \in Gal(\mathbb{E}/\mathbb{K})$ then $\sigma^{-1}\mu\sigma \in Gal(\mathbb{E}/\mathbb{K})$. Let α be any arbitrary element of $\mathbb{K}$. Since $\mathbb{K}$ is normal extension of $\mathbb{F}$, so that the splitting field of the minimal polynomial of α over $\mathbb{F}$ is contained in $\mathbb{K}$ and every conjugate of α is therefore in $\mathbb{K}$. For any $\sigma \in Gal(\mathbb{E}/\mathbb{F})$ since $\sigma(\alpha)$ is conjugate of α so $\sigma(\alpha) \in \mathbb{K}$. Thus for any automorphism $\mu \in Gal(\mathbb{E}/\mathbb{K})$ such that $\mu(\sigma(\alpha)) = \sigma(\alpha)$.

Now $(\sigma^{-1}\mu\sigma)(\alpha) = \sigma^{-1}[\mu(\sigma(\alpha))]$

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

$= \alpha$

so $\sigma^{-1}\mu\sigma \in Gal(\mathbb{E}/\mathbb{K})\ \forall\ \sigma\ \in Gal(\mathbb{E}/\mathbb{F})$ and $\mu \in Gal(\mathbb{E}/\mathbb{K})$.

Therefore, $Gal(\mathbb{E}/\mathbb{K})$ is normal subgroup of $Gal(\mathbb{E}/\mathbb{F})$.

Now we have to show $Gal(\mathbb{E}|\mathbb{F})$ is isomorphic to $Gal(\mathbb{E}/\mathbb{F})/Gal(\mathbb{E}/\mathbb{K})$.

Let $\mathbb{K}$ is the normal extension of $\mathbb{F}$. Let σ be any element of $Gal(\mathbb{E}/\mathbb{F})$. A mapping $\sigma' : \mathbb{K} \to \mathbb{K}.\mathbb{E}$ be defined as $\sigma'(\alpha) = \sigma(\alpha)\ \forall\ \alpha\ \in \mathbb{K}$.

Since σ is an F-automorphism of $\mathbb{E}$ and $\mathbb{K}$ is a normal extension of $\mathbb{F}$

so that $\mathbb{K} = \mathbb{F}(\alpha)$, therefore σ' is F-automorphism of $\mathbb{K}$. i.e, $\sigma' \in Gal(\mathbb{K}/\mathbb{F})$. Thus $\sigma(\mathbb{K}) = \sigma'(\mathbb{K}) = \mathbb{K}$.

Now consider a mapping $\beta : Gal(\mathbb{E}|\mathbb{F}) \to Gal(\mathbb{K}|\mathbb{F})$ defined by $\beta(\sigma) = \sigma'\ \forall\ \sigma\ \in Gal(\mathbb{E}|\mathbb{F})$.

Let us show that β is a group homomorphism.

Let σ_1 and σ_1 are any two element of $Gal(\mathbb{E}|\mathbb{F})$ and $\alpha\ \in\ \mathbb{K}$.

Now, $(\beta(\sigma_1\sigma_2))(\alpha) = (\sigma_1\sigma_2)'(\alpha)$

$= (\sigma_1\sigma_2)(\alpha)$

$= \sigma_1(\sigma_2(\alpha))$

$(\beta(\sigma_1)\beta(\sigma_2)(\alpha) \quad = \beta(\sigma_1)(\beta(\sigma_2)(\alpha))$

$= (\beta(\sigma_1))(\sigma_2^{'}(\alpha))$

$= (\beta(\sigma_1))(\sigma_2(\alpha))$

$= \sigma_1^{'}(\sigma_2(\alpha))$

$= \sigma_1^{'}(\sigma_2(\alpha))$

$= \sigma_1(\sigma_2(\alpha))$

So, $\beta(\sigma_1\sigma_2) = \beta(\sigma_1)\beta(\sigma_2)$

Consider any $\eta \in Gal(\mathbb{K}|\mathbb{F})$, then

$\eta(\alpha)$ is conjugate of α over $\mathbb{F}$, so there exists an F-automorphism σ of $\mathbb{E}$ such that $\sigma(\alpha) = \eta(\alpha)$, also σ and η are both identity of $\mathbb{F}$ and $\mathbb{K}$ and $\mathbb{K} = \mathbb{F}(\alpha)$, so that $\sigma(a) = \eta(a) \ \forall \ a \ \in \mathbb{F}(\alpha) = \mathbb{K}$, therefore $\eta = \sigma^{'} = \beta(\alpha)$. Hence β is onto.

$Kernel(\beta) = \{\sigma \ \in Gal(\mathbb{E}|\mathbb{F}) : \sigma = \text{I the identity of } Gal(\mathbb{E}|\mathbb{F})\} = \{\sigma \ \in Gal(\mathbb{E}|\mathbb{F}) : \sigma^{'} = \text{I}\}$.

Then by Fundamental theorem of homomorphism of groups $Gal(\mathbb{K}|\mathbb{F})$ is isomorphic to $Gal(\mathbb{E}|\mathbb{F})/Gal(\mathbb{E}|\mathbb{K})$

(3) $\mathbb{E}$ is normal extension of $\mathbb{K}$. So, by definition of normal extension the fixed field of $Gal(\mathbb{E}|\mathbb{K})$ is $\mathbb{K}$.

(4) Since $\mathbb{H}$ is a subgroup of $Gal(\mathbb{E}|\mathbb{F})\}$ so that $\mathbb{H} \subset Gal(\mathbb{E}|\mathbb{F})\}$,

also $\mathbb{E}_{\mathbb{H}} = \{a \ \in \ \mathbb{E} : \sigma(a) \ = a \ \forall \ \sigma \ \in \ \mathbb{H}\}$,since $\mathbb{E}_{\mathbb{H}}$ is subfield of $\mathbb{E}$.

$$|Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})| \leq [\mathbb{E} : \mathbb{E}_{\mathbb{H}}]. \tag{4.1}$$

Now,

$$Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}}) = \{\sigma \in Aut(\mathbb{K}) : \sigma(a) = a \ \forall \ a \ \in \mathbb{E}_{\mathbb{H}}\}. \tag{4.2}$$

Let $\sigma \ \in \ \mathbb{H} \Rightarrow \sigma(b) = b \ \forall \ b \ \in \ \mathbb{E}_{\mathbb{H}}$, (using (4.2))

$\Rightarrow \ \sigma \in Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})$. Therefore, $\mathbb{H} \subset \ Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})$

Therefore,

$$|\mathbb{H}| \leq |Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})| \tag{4.3}$$

From (4.1) and (4.3)$\Rightarrow$ $|\mathbb{H}| = |Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})|$. Also $\mathbb{H}$ is subgroup of $Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})$ Hence $\mathbb{H} = Gal(\mathbb{E}|\mathbb{E}_{\mathbb{H}})$. $\square$

CHAPTER 5

FINITE FIELDS

In field theory the most beautiful and important area is finite fields. Finite fields were first introduced by Galois in 1830 in his proof of the un-solvability of the general quintic equation. When Cayley investigate groups of matrices over finite fields. In the past fifty years there have been important application of finite fields in computer science,coding theory,information theory, and cryptography. But, besides the many uses of finite fields in pure and applied mathematics. The important features of finite fields is the restricted nature of their order and structure.

Classification of finite fields Theorem

For each prime p and each positive integer n there is, up to isomorphism, a unique finite field of order p^n.

Note

The finite field of order p^n is also known as *Galois field of order* p^n and is denoted as $GF(p^n)$.

Structure of finite fields

We will discuss the additive and multiplicative group structure of a field of order p^n.

Theorem:(Structure of finite fields)

As a group under addition, $GF(p^n)$ *is isomorphic to* $\mathbb{Z}_p \bigoplus \mathbb{Z}_p \bigoplus ... \bigoplus \mathbb{Z}_p$. *(n factors)*
As a group under multiplication, the set of nonzero elements of $GF(p^n)$ *is isomorphic to* $\mathbb{Z}_{p^n-1}$ *(and is therefore cyclic).*

proof:

We know $GF(p^n)$ has characteristic p. i.e, $p\ x = 0\ \forall\ x\ \in\ GF(p^n)$. Thus, every nonzero element of $GF(p^n)$ has additive order p. Then under addition $GF(p^n)$ is isomorphic to a direct product of n copies of $\mathbb{Z}_p$. Now we have to show that $GF(p^n)$ is isomorphic to

$\mathbb{Z}_{p^n-1}$. We know that every finite Abelian group can be expressed as the direct product of cyclic groups of order $n_1,\ n_2,\ ..., n_t$ where $n_{i+1}|n_i$ for $i = 1,\ 2,\ ..., t-1$. Therefore $GF(p^n)$ is isomorphic to a direct product of the form $\mathbb{Z}_{n_1} \bigoplus \mathbb{Z}_{n_2} \bigoplus ... \bigoplus \mathbb{Z}_{n_k}$ where $n_{i+1}|n_i$. So, for any element $a = (a_1, a_2, ..., a_k)$ in this product, we have $a^{n_1} = n_1a_1, n_1a_2, ..., n_1a_k = (0, 0, ..., 0)$. Thus,the polynomial $x^{n_1} - 1$ has $p^n - 1$ zeros in $GF(p^n)$. Since the number of zeros of a polynomial over a field cannot exceed the degree of the polynomial, so $p^n - 1 \ \leq \ n_1$. Since $GF(p^n)$ has a subgroup isomorphic to $\mathbb{Z}_{n_1}$ and $n_1 \leq p^n - 1$. Therefore $GF(p^n)$ is isomorphic to $\mathbb{Z}_{p^n-1}$. □

Corollary:

$[GF(p^n) : GF(p)] = n$

Corollary: $(GF(p^n))$ Contains an element of degree of n *Let a be a generator of the group of nonzero elements of $GF(p^n)$ under multiplication.Then a is algebraic over $GF(p)$ of degree n.*

proof:

$[GF(p)(a) : GF(p)] = [GF(p^n) : GF(p)] = n$. Therefore a is algebraic over $GF(p)$ of degree n

Example

Let us consider $GF(16)$. $16 = 2^4$. Since $x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$.

Therefore, $GF(16) \approx \{ax^3 + bx^2 + cx + d + < x^4 + x + 1 > | a, b, c, d \ \in \ \mathbb{Z}_2\}$

We may think the $GF(16)$ as the set $F = \{ax^3 + bx^2 + cx + d | a, b, c, d \ \in \ \mathbb{Z}_2\}$

Addition is done as in $\mathbb{Z}_2[x]$, but multiplication is done modulo $x^4 + x + 1$.

For example, for addition,

$x^4 + x + 1 = 0$

$\Rightarrow x^4 = -x - 1 = x + 1$

$\Rightarrow x^5 = x^2 + x$

$\Rightarrow x^6 = x^3 + x^2$

Thus $x^6 + x^5 + x^2 + x = (x^3 + x^2) + (x^2 + x) + x^2 + x = x^3 + x^2$

For multiplication,

$(x^3 + x^2 + x + 1)(x^3 + x) = x^6 + x^5 + x^2 + x = x^3 + x^2$. Since the remainder upon dividing $x^6 + x^5 + x^2 + x$ by $x^4 + x + 1$ in $\mathbb{Z}_2[x]$ is $x^3 + x^2$

Subfield of a finite field

The following theorem gives us a complete description of all the subfields of a finite field.

Theorem(Subfields of a finite field)

For each divisor m of n $GF(p^n)$ has a unique subfield of order p^m. Moreover, these are the only subfields of $GF(p^n)$.

proof:

Suppose that $m|n$. Then since, $p^n - 1 = (p^m - 1)(p^{n-m} + p^{n-2m} + ...p^m + 1)$,

$\Rightarrow (p^m - 1)|(p^n - 1)$

$\Rightarrow (x^{p^{m-1}-1})|(x^{p^{n-1}-1})$ in $\mathbb{Z}_p[x]$

Thus every zero of $x(x^{p^{m-1}-1})$ is also a zero of $x(x^{p^{n-1}-1})$. But according to a theorem stated above "For each prime p and each positive integer n there is, up to isomorphism, a unique finite field of order p^n." Therefore, the set of zeros of $x(x^{p^{m-1}-1})$in $GF(p^m)$ and the set of zeros of $x(x^{p^{n-1}-1})$ in $GF(p^n)$ is $GF(p^n)$. Hence, $GF(p^m)$ is a subfield of $GF(p^n)$ where $m|n$.

Uniqueness:

Let $GF(p^n)$ has two subfields of order (p^m), then the $x^{p^m} - x$ would have more than (p^m) zeros in $GF(p^n)$. This a contradiction that a polynomial of degree n over a field has at most n zeros.

Again suppose $\mathbb{F}$ is subfield of $GF(p^n)$. Then $\mathbb{F}$ is isomorphic to $GF(p^m)$ for some m.

Therefore, $n = [GF(p^n) : GF(p)]$

$= [GF(p^n) : GF(p^m][GF(p^m) : GF(p)]$

$= [GF(p^n) : GF(p^m)]m$

Thus, $m|n$. $\square$

Example

Let $\mathbb{F}$ be the field of order 16, i.e, $GF(16)$. Then there are exactly three subfields of $\mathbb{F}$, and their orders are 2, 4 and 16. This follows from the above theorem.

Bibliography

[1] David S. Dummit, Richard M. Foote : *Abstract Algebra*, Wiley Student edition, (2009).

[2] Joseph A. Gallan: *Contemporary Abstract Algebra*, Narosa Publishing House, 4th edition, (1999)

[3] I.B.S. Passi, I.S.Luthar: *Galois Theory*, Springer 2nd edition(2009).

[4] I.N. Herstein: *Topics in Algebra*, Wiley Student edition, (1999)