Algebraic Number Theory: Notes

by

Anwar Khan

Partial Contents

These are handwritten notes. We are very thankful to Mr. Anwar Khan for providing these notes.

Algebraic Number Theory

A Integral Domain and Fields.

of the set of rational integers has certian properties.

1. The Sum of two elements. in a certian order is unique element of the set.
2. Addition is Comutative.
3. Addition is an associative.
4. Each element has an inverse w.r.t addition i.e $a+(-a)=(-a)+a=0$
5. The multiplication of two elements in a certian order is unique element of the set
6. Multiplication is an associative.
7. Multiplication is commutative
8. Left and Right Distribution laws of $\times$ over + is hold.
9. There is an element '1' called 'unity' element or unity such that $a \cdot 1 = a$ for any a.
10. The element obeys cansalation laws so that $ac = ab$ and $a \neq 0$ Then $c = b$.

Any set of elements that fulfills these 10 axioms is called "Integral domain". when the set has at least two element and in addition to above property each element of set except zero has inverse element with respect multiplication. The set so defined is called field. smallest number of field is the set of rational number, of real number and the set of Complex number.

Diophantion Equation and Fermat's Conjecture (1601-1665)

The Equation

$$x^n + y^n = z^n \quad \text{--- (1)}$$

is not solvable in non-vanishing integer x, y, z for any integer $n \geq 3$.

Note: If x, y, z are integers satisfying (1) and two of them are divisible by 'd' Then 'd' ~~df~~ divides third one.

let $x = dx_1$, $y = dy_1$

Then $z = dz_1$

Then eqn (1) becomes

$$(dx_1)^n + (dy_1)^n = (dz_1)^n$$

$$d^n(x_1^n + y_1^n) = d^n z_1^n$$

$$x_1^n + y_1^n = z_1^n$$

$\Rightarrow x_1, y_1, z_1$ is an integral solution of ~~integral solution of~~ the given eqn.

It is sufficient to prove that eqn ① does not have primitive solution.

Primitive Solution:-

The solution of eqn ① in integer x, y, z that are co-prime in pair is called primitive solution.

Theorem:

The primitive sol of Eqn

$$x^2 + y^2 = z^2 \text{ —— } ①$$

are of the form $x = a^2 - b^2$, $y = 2ab$ and $z = a^2 + b^2$ where $(a, b) = 1$ and exactly one of 'a' and 'b' is even.

Proof:- i) Since we are interested in primitive solutions only therefore at most one of x, y, z is even. also if x & y are odd then z is even.

i.e

$x = 2m+1$, $y = 2n+1$ where $m, n \in \mathbb{Z}$

$$x^2 + y^2 = (2m+1)^2 + (2n+1)^2$$

$$= 4m^2 + 1 + 4m + 4n^2 + 4n + 1$$

$$x^2 + y^2 \equiv 2 \pmod 4$$

$$z^2 \equiv 2 \pmod 4$$

odd sum → even
odd diff → even.

$2^2 \equiv 0 \pmod 4$
$4^2 \equiv 0 \pmod 4$
$6^2 \equiv 0 \pmod 4$

$\because z$ is even
$z^2 \equiv 0 \pmod 4$

4

i.e $z^2 \equiv 2 \pmod 4$

But This is not possible Since z is even and

$$z^2 \equiv 0 \pmod 4.$$

ii) Without any ~~any~~ loss of generality we assume that x and z are odd Then y is even.

$\Rightarrow$ $x+z$ and $\cancel{x-z}$ are even.

take

$y = 2q$ ~~then~~

also

$$z+x = 2m, \quad z-x = 2n.$$

and let $(m,n) = d$.

Then $d \mid m+n$

$\Rightarrow d \mid z \quad \because z = m+n$ from above

and

$d \mid m-n = x \quad \because d \mid m+n \Rightarrow d \mid m-n$

But

$(x,z) = 1$.

Hence $d = 1$

So $(m,n) = 1$

eq (1) $\Rightarrow$

$$x^2 + y^2 = z^2.$$

$$y^2 = z^2 - x^2$$

$$y^2 = (z+x)(z-x)$$

$36 = 9(4)$
$6^2 = 3^2 \cdot 2^2$

$(2q)^2 = (2m)(2n)$

$\cancel{4}q^2 = \cancel{4}mn$

$q^2 = mn.$

iii) Integers 'm' and 'n' are coprime in pair and their product is perfect square Therefore each of m and n is a perfect square.

take

$m = a^2, \ n = b^2$

$\Rightarrow (a, b) = 1 \quad \because (m, n) = 1$

Hence a and b both can not be odd and even either because then

$x = m - n = a^2 - b^2$

& $z = m + n = a^2 + b^2$

would become even. Then exactly one of 'a' and 'b' is even

$y^2 = 4q^2 = 4mn = 4a^2b^2$

$y = 2ab.$

&

$x = m - n$

$x = a^2 - b^2$

&

$z = m + n$

$z = a^2 + b^2$

and $(a, b) = 1$ also one of 'a' or 'b' is even.

Now Conversely if x, y, z are of the form

$$x = a^2 - b^2, \quad y = 2ab$$
$$\& \quad z = a^2 + b^2.$$

$$x^2 + y^2 = (a^2 - b^2)^2 + (2ab)^2$$
$$= a^4 + b^4 - 2a^2b^2 + 4a^2b^2$$
$$= a^4 + b^4 + 2a^2b^2$$
$$= (a^2 + b^2)^2$$
$$= (z)^2$$

Hence
$$x^2 + y^2 = z^2.$$

---x---x---x---x---

Theorem:

Prove that the equation $x^4 + y^4 = z^4$ has no-solution in the integers.

Proof :- we first prove that

$$x^4 + y^4 = z^2 \text{ ——— } (1)$$ has

no-solution in integers

i) Suppose that $\exists$ a primitive solution x, y, z of eqn (1) Then at most one of x, y, z is even.

Suppose that x, y are odd.

Then z is even.

let $x = 2m+1$, $y = 2n+1$

Then

$$x^4 + y^4 = (2m+1)^4 + (2n+1)^4$$

$$x^4 + y^4 \equiv 2 \pmod 4$$

$$\Rightarrow z^2 \equiv 2 \pmod 4 \quad \because x^4 + y^4 = z^2$$

which is not possible as z is even: and $z^2 \equiv 0 \pmod 4$

if z is even $(2)^2 \equiv 0 \pmod 4$, $(4)^2 \equiv 0 \pmod 4$

so 'z' is not even and one of 'x' and 'y' is even.

ii) Suppose 'x' is even then y and z are odd.

$$x^4 + y^4 = z^2$$

$$(x^2)^2 + (y^2)^2 = z^2$$

we have

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad z^2 = a^2 + b^2$$

where $(a, b) = 1$ and exactly one of a and b is even by previous problem.

iii) we note that if a is even Then b is odd.

$$y^2 = a^2 - b^2 \equiv 3 \pmod 4$$

which is not possible since y is odd and

$$y^2 \equiv 1 \pmod 4$$

$1, 2, 3, 4$

$2^2 - 3^2 = -5 \neq 0$

$2^2 - 1 \equiv 3 \pmod 4$

$4^2 - 1 \equiv 3 \pmod 4$

Hence 'a' must be odd and 'b' is even

$(3,4)=1$, Then $(3,2)=1$

8

If a is odd & b is even.

iv) Let $b = 2c$ $\because$ b is even

Then $(a,c) = 1$

Since $(a,b) = 1$

Now

$$x^2 = 2ab$$
$$= 2a(2c)$$
$$x^2 = 4ac \quad \text{and} \quad (a,c) = 1$$

$\Rightarrow$ Both 'a' and c are perfect square i.e

$a = z_1^2$ and $c = e^2$ $\because$ $(e, z_1) = 1$

Then

$$y^2 = a^2 - b^2$$
$$= z_1^4 - 4e^4 \quad \because b = 2c \text{ and } b^2 = 4c^2$$
$$y^2 = (z_1^2)^2 - (2e^2)^2$$
$$\Rightarrow (2e^2)^2 + y^2 = (z_1^2)^2$$

Thus $2e^2$, y, z_1^2 are co-prime in pairs. It follows that

$$2e^2 = 2ml$$

$y = m^2 - l^2$ and $z_1^2 = m^2 + l^2$

$\because (m,l) = 1$

Exactly one of 'm' and 'l' is even.

$$2e^2 = 2ml$$

$$\Rightarrow e^2 = ml$$

$\Rightarrow$ m & l are perfect squares

let $l = y_1^2$ and $m = x_1^2$

$z_1^4 \geq z_1$

(9)

$z_1^2 = m^2 + l^2$

$z_1^2 = x_1^4 + y_1^4$

$\Rightarrow \; x_1^4 + y_1^4 = z_1^2$

as

$z > a^2 \qquad \because z = a^2 + b^2$

& $a^2 = z_1^4$ By (*)

Therefore

$z > z_1^4$

or

$z_1^4 < z$

$\Rightarrow z_1 < z^{1/4}$

It follows that if one- non-zero solution of $x^4+y^4=z^2$ exists another solution x_1, y_1, z_1 could be found. for which

$1 \leq z_1 < z^{1/4}$

If it has again another solution r, s, t for which

$1 \leq t < z_1^{1/4}$ and so on.

But this would yield an infinit decreasing ~~solution~~ sequence of positive integers

$z, z_1, t, t', \ldots$

which is impossible.

So equation $x^4 + y^4 = z^2$ has no integral solution

let $z_1 = z^2$

Then the equation

$x^4 + y^4 = z^4 = z_1^2$ has no solution

because $x^4 + y^4 = z_1^2$ has no solution.

//.

$R[x]$ = The set of all polynomials whose cofficient are rational number and set of rational number.

* Polynomial over the Rationals

$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is called polynomial of 'x' over the set of rational numbers, if $a_0, a_1, a_2, \ldots a_n$ are all rational numbers and

$$n \in \{0, 1, 2, 3, \ldots\}$$

e.g

$$p(x) = \frac{3}{2}x^5 + 7x^4 + \frac{5}{9}x^3 + 9x + 7$$

or

$$p(x) = 2x^3 + 3x + 7.$$

$R[x]$ consists of Q (set of rational numbers) together with all polynomial in x with rational cofficient, the cofficient of highest exponent of being non-zero

i.e

$$a_n \neq 0$$

Degree of Polynomial:-

If a polynomial $P(x)$ is in $R[x]$ Then degree of $P(x)$ means the exponent of heighest power of x, occuring in $P(x)$ e.g

$1 + x + \frac{2}{3}x^2 + 6/5\, x^3$ is the polynomial of degree 3.

* If $a \in Q$ then $a = ax^0$ that is to say every non-zero element of Q is a polynomial of degree zero. If $a = 0$ then degree of zero element is not defined.

* Monic Polynomical

A polynomial $p(x)$ in $R[x]$ is said to be monic if its leading cofficient is 1. for e.g.

$$\frac{4}{3}x + \frac{5}{8}x^2 + 6x^3 + x^4$$

leading cofficient mean cofficient of exponent of highest power

* Division of Polynomial

If $P_1(x)$ and $P_2(x)$ are in $R[x]$ we say that $P_2(x) \mid P_1(x)$ if there exist $q(x) \in R[x]$ such that

$$P_1(x) = q(x) P_2(x).$$

✓ such polynomial whose roots are not rational number i.e its roots are irrational or complex Then $P(x)$ is irreducible.

(Imp Annual obj)

(12)

Irreducible Polynomial

A Polynomial $P(x)$ in $R[x]$ is called irreducible in $R[x]$ if it cannot be written as the product of two non-unit elements of $R[x]$.

e.g.

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

x^2+2x+4

is irreducible in $R[x]$

and

$$x^2-9 = (x-3)(x+3)$$

is not irreducible but reducible in $R[x]$.

Division Algorithem

If $P_1(x)$ and $P_2(x)$ are in $R[x]$ and $P_2(x) \neq 0$ Then $\exists$ $q(x)$ and $r(x)$ in

$$P_1(x) = q(x)P_2(x) + r(x)$$

$$\deg r(x) < \deg P_2(x).$$

or

$$\deg r(x) = 0$$

Greatest Common Divisor

The G.C.D $d(x)$ of $P_1(x)$ & $P_2(x)$ is defined as

1) If $d(x) | P_1(x)$ & $d(x) | P_2(x)$

If $d_1(x) \mid p_1(x)$ and $d_2(x) \mid p_2(x)$ Then $d_1(x) \mid d(x)$ Then $d(x)$ is called G.C.D of $p_1(x)$ & $p_2(x)$. and It is denoted as

Remark $(p_1(x), p_2(x)) = d(x)$.

If $(p_1(x), p_2(x)) = d(x)$ There are polynomial $q_1(x)$ and $q_2(x)$ in $R[x]$ such that.

$$d(x) = q_1(x)p_1(x) + q_2(x)p_2(x).$$

i.e to say $d(x)$ can be expressed as combination of $p_1(x)$ and $p_2(x)$.

Algebraic Number

If α is root (zero) of polynomial $p(x)$ is i.e

$$p(\alpha) = x^n + r_1 x^{n-1} + r_2 x^{n-2} + \cdots + r_n = 0$$

for $p(x) \in R[x]$ and $n > 0$ Then α is called algebraic number.

Note Algebraic number of constant polynomial in $R[x]$ does not exist.

Degree of Algebraic Number

If $p(x)$ is irreducible polynomial in $R[x]$ Then 'α' is said to be of degree n.

e.g

$$x^2-2=0 \Rightarrow (x-\sqrt{2})(x+\sqrt{2})=0$$

its roots are $x=\sqrt{2}, -\sqrt{2}$

So this is irreducible polynomial. $\sqrt{2}$ is of degree 2.

e.g

$$x^3-2=0$$

$$x=\sqrt[3]{2}$$

$\sqrt[3]{2}$ is of degree 3.

Note: All the rational number are of degree 1. i.e

$$x-r=0 \Rightarrow x=r\in \mathbb{Q}$$

Minimal Polynomial

A Polynomial $p(x)\in R[x]$ is called the minimal polynomial for an algebraic number "α". If $p(x)$ is unique irreducible, monic polynomial otherwise α should satisfying a polynomial of lower degree.

eg:- x^2-5 is a minimal polynomial of $\sqrt{5}$.

x^2-5 is monic & irreducible $\because$ its root is irrational number.

$\frac{1}{5}x^2 - 1$ is not defining polynomial of $\sqrt{5}$.

$\because \frac{1}{5}x^2 - 1$ is not definining polynomial

$\sqrt[3]{2}$, $\sqrt[3]{7}$.

i) $x^3 - 2 = 0 \Rightarrow \cancel{(x + 2^{1/3})(x - 2^{1/3}) = 0}$

ii) $x^3 - 7 = 0 \Rightarrow ((x)^3 - (\sqrt[3]{7})^3)$ $\quad \sqrt[3]{2} = (2^{1/3})$

$2x^3 - 4 = 0$ is not defining polynomial of $\sqrt[3]{2}$ $\because$ polynomial is not monic.

$2(\sqrt[3]{2})^3 - 4 = 2(2^{1/3})^3 - 4 = 4 - 4 = 0$

Conjugates of an Algebraic Number

If $p(x)$ is minimal polynomial of 'α' Then for

$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ has n-zeros (roots or Algebraic numbers) $\alpha = \alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n$ are called conjugates of α. for e.g

i) $x^2 - 2$ is defining polynomial of $\sqrt{2}$ so conjugates of $\sqrt{2}$ are $\sqrt{2}, -\sqrt{2}$.

Similarly conjugates of $-\sqrt{2}$ are $\sqrt{2}, -\sqrt{2}$.

ii) $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + 2^{2/3})$.

By cube formula.

$\Rightarrow x - \sqrt[3]{2} = 0$ or $x^2 + \sqrt[3]{2}x + 2^{2/3} = 0$

$x = \sqrt[3]{2}$

16

$x = \sqrt[3]{2}$, $x = \dfrac{-\sqrt[3]{2} \pm \sqrt{2^{2/3} - 4 \cdot 2^{2/3}}}{2}$

$$x = \frac{-\sqrt[3]{2} \pm 2^{1/3}\sqrt{3}\, i}{2}$$

$$x = \sqrt[3]{2}\left(\frac{-1 \pm \sqrt{3}\, i}{2}\right)$$

where

$$\omega = \frac{-1 + \sqrt{3}\, i}{2}, \quad \omega^2 = \frac{-1 - \sqrt{3}\, i}{2}$$

Hence

$x = \sqrt[3]{2}\,\omega, \ \sqrt[3]{2}\,\omega^2$

So we can write

i.e conjugates of $\sqrt[3]{2}$ are

$\sqrt[3]{2}, \ \sqrt[3]{2}\,\omega, \ \sqrt[3]{2}\,\omega^2$.

Primitive Polynomial

A Polynomial $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$.

is called Primitive Polynomial if G.C.D of $a_0, a_1, a_2, \ldots, a_n$ is 1.

i.e $(a_0, a_1, a_2, \ldots, a_n) = 1$.

i.e A polynomial is called Primitive polynomial if all of its cofficient are relatively prime. for e.g.

i) $2x^2+x-3=0 \in R[x]$
wher
$(2,3,1)=1.$

ii) $5x^3+2x^2-3x=0$
$(5,2,3)=1.$

Imp
* [redacted]
Theorem If 'θ' is an algebraic number over Q, it has a unique minimal polynomial. (monic and irreducible polynomial)

Proof:
let $p(x)$ and $q(x)$ be two minimal polynomials over Q. satisfied by 'θ'

$$q(x) = g(x)p(x) + r(x) \longrightarrow (1)$$
where $g(x), r(x) \in R[x]$
where
$\deg r(x) < \deg p(x)$ or $r(x)=0$

Put $x=\theta$ in Eq: (1)

$$q(\theta) = g(\theta)p(\theta) + r(\theta)$$
$$0 = 0 + r(\theta) \implies r(\theta)=0$$

$r(\theta) = 0$

This is not possible since $\deg r(x) < \deg p(x)$

$\because$ θ is root of $p(x)$ & $\deg r(x) < \deg p(x)$

$\Rightarrow r(x) = 0$

otherwise $r(x)$ will be minimal polynomial satisfied by θ.

Hence

$q(x) = g(x)\, p(x)$ ~~[illegible]~~

$\Rightarrow p(x) \mid q(x) \longrightarrow (2)$

Similarly we can show that

$q(x) \mid p(x) \longrightarrow (3)$

From eqn (2) and (3) we get

$p(x) = q(x)$

Hence Algebraic number 'θ' over Q has unique minimal polynomial.

$\cdot\!/\!\cdot$ ——— $\cdot\!/\!\cdot$ ——— $\cdot\!/\!\cdot$

03463985788

Product of Polynomial

let $p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n$.
and

$q(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots + b_m x^m$

Then

$p(x) \cdot q(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_i x^i + \cdots c_k x^k$.

where

$C_0 = a_0 b_0$

$C_1 = a_0 b_1 + a_1 b_0$

$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$C_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$

$\vdots$

$C_i = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_i b_0$

$\vdots$

$C_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0$

$p(x)\, q(x) = \sum_{i=0}^{k} c_i x^i$ where

$c_i = \sum_{j=0}^{i} a_j b_{i-j}$

20

Also

$$p(x)\,q(x) = \sum_{i=0}^{k} c_i x^i$$

$$= \sum_{i=0}^{k}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i$$

$$= \sum_{i=0}^{k} \sum_{j=0}^{i} a_j b_{i-j}\, x^i \quad \text{where } k = mn.$$

Ans 10 02/10

Symmetric Polynomial

✓ A Polynomial $p(x_1, x_2, ---, x_n)$ is said to be Symmetric in $x_1, x_2, x_3, ---, x_n$ if it remains unchanged by any number of permutations of its variables $x_1, x_2, x_3, ---, x_n$.

OR

A polynomial $p(x_1, x_2, x_3, ---, x_n)$ in 'n' variable is said to be Symmetric polynomial if any of the variables $x_1, x_2, ---, x_n$ are interchanged we obtained the same polynomial.

for e.g.

Symmetric polynomial in two variable

$$x_1^3 + x_2^3 = 7.$$

$x_1 \longrightarrow x_2$ Then we obtained

$$x_2^3 + x_1^3 = 7.$$

(21)

$$4x_1^2 x_2^2 + x_1^3 x_2 + x_1 x_2^3 + (x_1 + x_2)^4$$

if $x_1 \longrightarrow x_2$

$$4x_2^2 x_1^2 + x_2 x_1^3 + x_2 x_1^3 + (x_2 + x_1)^4$$

$\Rightarrow f(x_1, x_2)$ is Symmetric polynomial.

$$f_1(x_1) \cancel{x_2, x_3, \ldots, x_n} = x_1 + x_2 + x_3 + \cdots + x_n.$$

$$= \sum_{i=1}^{n} x_i$$

$$f_2(x) = x_1 x_2 + x_1 x_3 + x_1 x_4 + \cdots + x_1 x_n$$
$$+ x_2 x_3 + x_2 x_4 + x_2 x_5 + \cdots + x_2 x_n + \cdots + x_{n-1} x_n.$$

$$f_3(x) = x_1 x_2 x_3 \cdots x_n$$

Let $f(x) = x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$

$$= x^n - (\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_n) x^{n-1} +$$
$$(\alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \cdots + \alpha_n \alpha_1) x^{n-2}$$
$$+ \cdots + (\alpha_1 \alpha_2 \alpha_3 \cdots \alpha_n)(-1)^n.$$

e.g.

$$x^3 - 9x^2 + 26x - 24$$
$$= (x-2)(x-3)(x-4)$$
$$= \cancel{(x^2 - 3x - 2x + 6)(x-4)}$$
$$= x^3 - 3x^2 - 2x^2 + 6x - 4x^2 + 12x + 8x - 24$$
$$= x^3 - (2+3+4)x^2 + (2 \cdot 3 + 3 \cdot 4 + 4 \cdot 2)x$$
$$+ 2 \cdot 3 \cdot 4 (-1)^3.$$

$$x^2+6x+9 = (x+3)(x+3)$$

$$= x^2+3x+3x+9.$$

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

$$= x^2+6x+9$$

Note To prove that a set of real number, rational number and complex number as field it is enough to show

$a, b \in S$ The elements

$a \pm b,\ ab,\ \frac{a}{b}\ (b \neq 0).$

are also in S.

Annual 09 v. imp.

Theorem The set of algebraic number is a field.

Let $\alpha = \alpha_1, \beta = \beta_1$ be algebraic number having defining polynomial

$$P(x) = x^m + r_1 x^{m-1} + r_2 x^{m-2} + \cdots + r_m$$

$$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) + \cdots + (x-\alpha_m)$$

&

$g(x) = x^n + s_1 x^{n-1} + \cdots + s_n$

$= (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$

Let

$\gamma_{ij} = \alpha_i + \beta_j$ where $i = 1,2,3,\ldots,m$ & $j = 1,2,3,\ldots,n$

and define

$g(x) = (x-\gamma_{11})(x-\gamma_{12})\cdots(x-\gamma_{mn})$.

Then

$\gamma_{11} = \alpha_1 + \beta_1 = \alpha + \beta$ is root of $g(x)$

To prove that $\alpha+\beta$ is algebraic number we will prove $g(x) \in R[x]$. Cofficient of $g(x)$ are Symmetric polynomial in $\gamma_{11}, \gamma_{12}, \ldots, \gamma_{mn}$. and so they are symmetric polynomial in $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_n$. with rational cofficient. But a symmetric polynomial α_i & β_j is symmetric polynomial in γ_i with s_j. It follows cofficient of $g(x)$ are rational number. Hence $g(x) \in R[x]$ and $\alpha_i + \beta_j$ are algebric number. We can also similarly shows that $\alpha_i - \beta_j$ and $\alpha_i \beta_j$ are algebraic number. Now if

$\beta \neq 0$ is zero of the polynomial $x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n$ and ~~one~~ $1/\beta$ is zero of the polynomial

$\gamma_n x^n + \gamma_{n-1} x^{n-1} + \cdots + 1$

Thus β is not equal to zero i.e $\beta \neq 0$. as an algebric number Then $1/\beta$ is also an algebric number

$\alpha \cdot \frac{1}{\beta} = \frac{\alpha}{\beta}$ is an algebric number. Hence the set of all algebric number is a field.

— ✳ — ✳ — ✳ —

* Aternative Statment

"The sum, Difference and product of two algebraic number are algebric number is field and the Quotient of two algebraic number is also algebraic number if the denominator is non-zero.

(ii) Theorem Imp Annual 10

Let θ be an algebraic number of degree $n>1$. Prove That the set $R(\theta)$ of all numbers of the form

$$\alpha = \frac{q_1(\theta)}{q_2(\theta)}$$

where $q_1(x)$ and $q_2(x) \in R[x]$ and $q_2(\theta) \neq 0$ is a field. Also Show that every element of $R(\theta)$

Can be expressed uniquively in the form

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}.$$

where $a_0, a_1, a_2, \ldots, a_{n-1} \in R$.

Proof :-

The sum, difference, product and quotient ~~fun~~ of two rational function is again rational function Hence $R(\theta)$ is field.

let $p(x) = x^n + r_1 x^{n-1} + \cdots + r_n$ be the defining polynomial of 'θ'. and $p(\theta) = 0$ Then

$p(x)$ and $q_2(x)$ are relatively prime $\because$ $p(x)$ is monic, irreducible polynomial and $q_2(x) \neq 0$.

i.e

$$(p(x), q_2(x)) = 1.$$

Then There exist $t(x), s(x) \in R[x]$ such that

$$t(x)p(x) + s(x)q_2(x) = 1$$

Put $x = \theta$

$$t(\theta)p(\theta) + s(\theta)q_2(\theta) = 1$$

$$0 + s(\theta)q_2(\theta) = 1 \quad \because p(\theta) = 0$$

$$q_2(\theta) = \frac{1}{s(\theta)}.$$

Now as for $\alpha \in R(\theta)$

$$\alpha = \frac{q_1(\theta)}{q_2(\theta)} = \frac{q_1(\theta)}{1/S(\theta)}$$

$$\boxed{\alpha = q_1(\theta)\, S(\theta)}$$

$\Rightarrow$ 'α' is polynomial in 'θ'

Now

$$f(\theta) = 0$$

$$\theta^n + r_1\theta^{n-1} + \cdots + r_n = 0$$

$$\theta^n = -(r_1\theta^{n-1} + r_2\theta^{n-2} + \cdots + r_n)$$

It follows that every positive power of 'θ' can be written as polynomial in 'θ' of degree $n-1$ or less.

Hence 'α' can also be express as polynomial in 'θ' of degree $n-1$ or less.

i.e

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}.$$

where

$a_0, a_1, a_2, \ldots, a_{n-1}$ in R

Finally if we have two representation of 'α'

i.e

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$$

&

$$\alpha = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}$$

i.e

$$a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}$$

$$(a_0 - b_0) + (a_1 - b_1)\theta + (a_2 - b_2)\theta^2 + \cdots + (a_n - b_n)\theta^{n-1} = 0$$

which is not possible since 'θ' is of degree n. Therefore 'α' has unique representation.

— x —

Definition Let 'θ' be algebraic number $n > 1$. Then the set $R(\theta)$ of all number of the form $\alpha = \frac{q_1(\theta)}{q_2(\theta)}$ where $q_1(x), q_2(x) \in R[x]$ and $q_2(x) \neq 0$ is field. This field is called "algebraic number field"

$R(\theta)$ = Algebraic Number field

$R[x]$ = The set of all polynomial with rational coefficients.

$R[\theta]$ = Integral Domain.

— x — x —

Defintion let 'θ' be the algebraic number of degree $n \geq 1$ and let

$$\theta = \theta_1, \theta_2, \theta_3, \theta_4, \dots \theta_n$$

are conjugates of 'θ'. Then

$$\alpha = \frac{\varphi_1(\theta)}{\varphi_2(\theta)} = \varphi(\theta) = a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1} \in R(\theta).$$

The numbers

$$\alpha = \alpha' = \varphi(\theta) = \varphi(\theta_1),\ \alpha'' = \varphi(\theta_2), \dots, \alpha^{n} = \varphi(\theta_n)$$

are called the field conjugate of α.

e.g;- $\sqrt{2}$ is an algebraic number of degree 2 over R. The elements of $R(\sqrt{2})$ are of the form.

$\varphi(\sqrt{2}) = \alpha = a + b\sqrt{2}$. where $a, b \in R$.

The conjugates of $\sqrt{2}$ are $\pm\sqrt{2}$.

Therefore the field conjugate of

$$\alpha = a + b\sqrt{2} \in R(\sqrt{2}) \text{ are}$$

$$\alpha' = \alpha = a + b\sqrt{2} = \varphi(\sqrt{2})$$

&

$$\alpha'' = a - b\sqrt{2} = \varphi(-\sqrt{2}).$$

(27)

$\sqrt[3]{2}$ is an algebraic number of degree 3. over R.

The elements of $R(\sqrt[3]{2})$ are of the form.

$$\alpha = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2, \text{ where } a_0, a_1, a_2 \in R$$

The conjugae of '$\sqrt[3]{2}$' are $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$, $\sqrt[3]{2}\,\omega^2$

where

$$\omega = \frac{-1+\sqrt{3}\,i}{2}$$

$$\omega^2 = \frac{-1-\sqrt{3}\,i}{2}$$

Therefore the field conjugates of α are

$$q(\sqrt[3]{2}) \quad \alpha' = \alpha = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$$

$$q(\omega\sqrt[3]{2}) = \alpha'' = a_0 + a_1\omega\sqrt[3]{2} + a_2(\omega\sqrt[3]{2})^2$$

$$q(\omega^2 . \sqrt[3]{2}) = \alpha'' = a_0 + a_1(\sqrt[3]{2}\,\omega^2) + a_2(\omega^2\sqrt[3]{2}).$$

x ——— x

$\theta^n = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = \alpha.$
$\theta^n - \alpha = 0 \Rightarrow \alpha$ is an algebraic number.

Theorem Let $R(\theta)$ be an algebraic number field. Prove that every $\alpha \in R(\theta)$ is algebraic number. Every field conjugate of α is also a conjugate of α.

Proof: The set of all algebraic numbers is a field and any $\alpha \in R(\theta)$ can be uniquely expressed as

$$\varphi(\theta) = \alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$$
$a_0, a_1, a_2, a_3, \ldots, a_{n-1} \in R.$

Let $p(x)$ and $g(x)$ be the defining polynomial of θ and α respectively. also

$$\alpha = \varphi(\theta)$$

Now

$$g(\alpha) = 0$$

$$g(\varphi(\theta)) = 0 \Rightarrow \varphi(\theta) \text{ are conjugates of } g(x)$$

But $p(\theta) = 0$
every zero (root) of $p(x)$ is also zero of $g(\varphi(x))$.

$$\Rightarrow g(\varphi(\theta_i)) = 0$$
$i = 1, 2, 3, \ldots, n.$

Hence every field conjugate of of α is also a conjugate of α.

Theorem

i) The set of field conjugate of an element 'α' of $R(\theta)$ is either identical with set of conjugates or consist of several copies of the set of conjugates of 'α'

Proof

let

$$f(x) = (x-\alpha')(x-\alpha'')(x-\alpha''')\cdots(x-\alpha^{(n)})$$

Then the coefficient of $f(x)$ are symmetric polynomial in α^{i}'s and therefore symmetric polynomial in $\theta_1, \theta_2, \ldots, \theta_n$ which are rational number.

Hence $f(x) \in R[x]$

Factorize $f(x)$ into monic irreducible factors in $R[x]$. i.e

$$f(x) = f_1(x) f_2(x) f_3(x) \cdots$$

and suppose that $f_1(\alpha) = 0$

i.e

$f_1(x)$ is defining polynomial of 'α' also $f_1(\alpha) = 0 \Rightarrow f_1(\varphi(\theta)) = 0$

let $p(x)$ be the defining polynomial of 'θ' Then $p(x) \mid f_1(\varphi(x))$.

$\Rightarrow \theta, \theta', \theta'', \ldots, \theta^{(n)}$ are zeros of $f_1(x)$.

If all are distinct Then

$$f(x) = f_1(x)$$

If they are not distinct. Then let

$\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, ---, \alpha^{(t)}$ be the set of distinct $\alpha^{(k)}$'s. Now

$f_2(\alpha^k) = 0$ for some α^k.

$\Rightarrow f_1(x) \mid f_2(x)$

$\Rightarrow f_1(x) = f_2(x) \quad \because f_2(x)$ is irreducible.

If there are other factors of $f(x)$ The argument can be repeated until we obtain $f_1(x) = f_2(x) = f_3(x) = -- = f_m(x)$

where $\quad m = \frac{n}{t}$

$$f(x) = [f_1(x)]^m$$

$$= [f_1(x)]^{\frac{n}{t}}$$

Since the zeros of $f_1(x)$ are the field conjugates of α. Thus $f(x)$ consist of $\frac{n}{t}$ copies of α.

$$\alpha' = \alpha, \quad \theta = \theta'$$

$$f(x) = (x-\alpha')(x-\alpha'')(x-\alpha''') \cdots (x-\alpha^n)$$

$$f'(x) = (x-\alpha'')(x-\alpha''') \cdots (x-\alpha^n) + (x-\alpha')(x-\alpha'') \cdots (x-\alpha^n) + \cdots + (x-\alpha')(x-\alpha'') \cdots (x-\alpha^{n-1})$$

put $x = \alpha'$

33

ii) The polynomial whose zeros are field // conjugates of 'α' is a power of the defining polynomial of α. If it is equal to the defining polynomial Then

$$R(\alpha) = R(\theta).$$

Proof:

Suppose that

$f(x) = f_1(\alpha)$ and define

$$q(x) = f(x)\left\{ \frac{\theta'}{x-\alpha'} + \frac{\theta_2}{x-\alpha''} + \frac{\theta_3}{x-\alpha'''} + \cdots + \frac{\theta_n}{x-\alpha^n} \right.$$

where $f(x) = (x-\alpha')(x-\alpha'')(x-\alpha''') \cdots (x-\alpha^n)$

Then $q(x)$ is polynomial of degree $(n-1)$ with rational coefficient. that

$$q(x) = \theta_1\{(x-\alpha'')(x-\alpha''') \cdots (x-\alpha^n)\}$$

$$+ \theta_2\{(x-\alpha')(x-\alpha''') \cdots (x-\alpha^n)\}$$

put $x = \alpha$

$$+ \cdots + \theta_n\{(x-\alpha')(x-\alpha'') \cdots (x-\alpha^{n-1})\}$$

$$q(\alpha = \alpha') = \theta\,(\alpha-\alpha'')(\alpha-\alpha''') \cdots (\alpha-\alpha^n)$$

$$q(\alpha) = \theta f'(\alpha)$$

$$\theta = \frac{q(\alpha)}{f'(\alpha)}.$$

$$\Rightarrow \theta \in R(\alpha).$$

$\Rightarrow R(\theta) \subseteq R(\alpha)$ —— (1)

Also since

$\alpha \in R(\theta)$

$\Rightarrow R(\alpha) \subseteq R(\theta)$ —— (2)

From (1) & (2)

$R(\theta) = R(\alpha)$.

Definition Let 'θ' be an algraic number of degree n. Then algebraic number field $R(\theta)$ is called a simple extension of R we also say that $R(\theta)$ is obtained by adjoing 'θ' to R.

let θ and η be algebraic numbers Then the set $R(\theta)\eta$ which consist of all rational function of 'η' whose Coeffecient are elements of $R(\theta)$ is a field. This field is denoted by $R(\theta, \eta)$.

Theorem;- If θ and η are algebraic number Then the adjuction of η to $R(\theta)$ gives the same field $R(\theta,\eta)$ as the adjuction of 'θ' to $R(\eta)$. There exist an algebraic number ξ such that

$$R(\theta,\eta) = R(\xi)$$

Proof:- The 1st part is clear since both $R(\theta,\eta)$ and $R(\eta,\theta)$ are identical with field consisting of the number of the form

$$\frac{q_1(\theta,\eta)}{q_2(\theta,\eta)} \quad \text{where } q_2(\theta,\eta) \neq 0$$

where $q_1(x,y)$ and $q_2(x,y)$ polynomial in two variables with rational Co-efficient. ~~where~~

If $\eta \in R(\theta)$ Then

$$R(\theta,\eta) = R(\theta).$$

Similarly

if $\theta \in R(\eta)$ Then $R(\theta,\eta) = R(\eta)$

Then There is nothing to prove.

Assume that $\theta \notin R(\eta)$ and $\eta \notin R(\theta)$.

Let the defining polynomial of θ and η ~~are~~ be $P_1(x)$ and $P_2(x)$ and let Their conjugates be $\theta_1, \theta_2, \theta_3, \ldots, \theta_n$ and $\eta_1, \eta_2, \eta_3, \ldots \eta_m$ respectively we defined the number

ξ_{ij} as follow

$$\xi_{ij} = a\theta_i + b\eta_j \text{ where } i = 1,2,3,\dots,n \quad j = 1,2,3,\dots,m$$

and $a, b \in R$ and chosen so that all ξ_{ij} are distinct.

Now consider a polynomial

$$f(x) = (x-\xi_{11})(x-\xi_{12})(x-\xi_{13})\cdots(x-\xi_{nm})$$

Then the the coeffients of $f(x)$ being symmetric polynomials in ξ_{ij} will be symmetric polynomials in θ_i's and η_i's, so $f(x)$ has rational coefficients

$$\Rightarrow f(x) \in R[x]$$

we will prove $R(\theta, \eta) = R(\xi_1)$

where $\xi = \xi_{11} = a\theta_1 + b\eta_1$

i.e

$$\xi = a\theta + b\eta \in R(\theta, \eta)$$

$$R(\xi) \subseteq R(\theta, \eta) \quad \text{--- (1)}$$

Conversely consider

$\rho \in R(\theta, \eta)$

and let

$$\rho = \frac{q_1(\theta_i, \eta_j)}{q_2(\theta_i, \eta_j)}$$

where $i = 1, 2, \dots, n$. & $j = 1, 2, \dots, m$.

and

let

$$F(x) = f(x)\left\{\frac{\rho_{11}}{x-\xi_{11}} + \frac{\rho_{12}}{x-\xi_{12}} + \dots + \frac{\rho_{mn}}{x-\xi_{mn}}\right\}$$

"The co-efficients of $F(x)$ are rational numbers and it is of degree "$mn-1$""

$$F(x) = \rho_{11}(x-\xi_{12})(x-\xi_{13}) \dots (x-\xi_{mn}).$$
$$+ \rho_{12}(x-\xi_{11})(x-\xi_{13}) \dots (x-\xi_{mn}).$$
$$+ \dots + \rho_{mn}(x-\xi_{11})(x-\xi_{12}) \dots (x-\xi_{mn-1})$$

Put $x = \xi = \xi_{11}$

$$F(\xi) = \rho\underline{(\xi-\xi_{12})(\xi-\xi_{13}) \dots (\xi-\xi_{mn})}$$

$$F(\xi) = \rho F'(\xi). \text{ where}$$
$$F'(\xi) = (x-\xi_{12})(x-\xi_{13}) \dots (x-\xi_{mn}).$$

$$\rho = \frac{F(\xi)}{F'(\xi)} \in R(\xi)$$

38

$\Rightarrow R(\theta, \eta) \subseteq R(\xi)$ —— (2)

From (1) & (2) we have

$$R(\theta, \eta) = R(\xi).$$

—— x —— x ——

Definition

Primitive Element

If an element 'α' of $R(\theta)$ is such that

$$R(\alpha) = R(\theta)$$

Then α is called a primitive element ~~is called~~ of $R(\theta)$. It is clear that the degrees of any two primitive are same and both are equal to $R(\theta)$ or to degree of field.

—— x —— x ——

(39)

Question Show That

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

and find a rational function $\gamma(x)$ with rational coefficients such that

$$\gamma(\sqrt{2}+\sqrt{3}) = \sqrt{2}$$

Sol:-

Let $\theta = \sqrt{2}$, $\eta = \sqrt{3}$

Conjugates of $\theta = \pm\sqrt{2} \Rightarrow \theta_1 = \sqrt{2}, \theta_2 = -\sqrt{2}$.

Conjugates of $\eta = \pm\sqrt{3} \Rightarrow \eta_1 = \sqrt{3}, \eta_2 = -\sqrt{3}$.

Now

$$\xi_{11} = a\theta_1 + b\eta_1 = \theta + \eta \quad \text{where } a=b=1$$

$$\xi_{11} = \sqrt{2}+\sqrt{3}$$

$$\xi_{12} = \theta_1 + \eta_2$$

$$= \sqrt{2}-\sqrt{3}$$

$$\xi_{21} = -\sqrt{2}+\sqrt{3}.$$

$$\xi_{22} = \theta_2 + \eta_2 = -\sqrt{2}-\sqrt{3}$$

$$= -(\sqrt{2}+\sqrt{3})$$

when $\xi_{11}, \xi_{12}, \xi_{21}$ and ξ_{22} all are distinct it follows that algebraic number fields i.e

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

let $\xi = \sqrt{2} + \sqrt{3}$

$$\xi^2 = (\sqrt{2} + \sqrt{3})^2$$

$$= 2 + 3 + 2\sqrt{2}\cdot\sqrt{3}$$

$$\xi^2 = 5 + 2\sqrt{2}\cdot\sqrt{3}$$

$$\xi^2 - 1 = 4 + 2\sqrt{2}\cdot\sqrt{3}.$$

$$\frac{\xi^2 - 1}{2\xi} = \frac{4 + 2\sqrt{2}\cdot\sqrt{3}}{2(\sqrt{2}+\sqrt{3})}. = \frac{\cancel{2}(2+\sqrt{2}\cdot\sqrt{3})}{\cancel{2}(\sqrt{2}+\sqrt{3})}$$

$$\frac{\xi^2 - 1}{2\xi} = \frac{2 + \sqrt{2}\cdot\sqrt{3}}{\sqrt{2}+\sqrt{3}} \times \frac{\sqrt{2} - \sqrt{3}}{\sqrt{2} - \sqrt{3}}.$$

$$\frac{\xi^2 - 1}{2\xi} = \frac{2\sqrt{2} - \cancel{2\sqrt{3}} + \cancel{2\sqrt{3}} - 3\sqrt{2}}{2 - 3}$$

$$= \frac{\cancel{-}\sqrt{2}}{\cancel{-}1}$$

$$\frac{\xi^2 - 1}{2\xi} = \sqrt{2}$$

$$f(\xi) = \sqrt{2} \implies f(\sqrt{2}+\sqrt{3}) = \sqrt{2}$$

(41)

Q $R(\sqrt{2}, \sqrt[3]{5}) = R(\sqrt{2} + \sqrt[3]{5})$.

Sol:

let

$\theta = \sqrt{2}, \quad \eta = \sqrt[3]{5}$.

The conjugates of $\theta = \pm\sqrt{2}$,

&

Conjugates of $\eta = \sqrt[3]{5}, \ \sqrt[3]{5}\,\omega, \ \sqrt[3]{5}\,\omega^2$.

let

$\xi_{ij} = a\theta_i + b\eta_j \qquad$ put $a = b = 1$

$\xi_{11} = \sqrt{2} + \sqrt[3]{5}, \quad \xi_{12} = \theta_1 + \eta_2$.

$= +\sqrt{2} + \sqrt[3]{5}\,\omega$.

$\xi_{21} = -\sqrt{2} + \sqrt[3]{5}\,\omega^2$

$\xi_{22} = -\sqrt{2} + \sqrt[3]{5}\,\omega^2$.

all the root of ξ_{ij} are different

so

$R(\sqrt{2}, \sqrt[3]{5}) = R(\sqrt{2} + \sqrt[3]{5})$.

let

$\xi = \sqrt{2} + \sqrt[3]{5}$

$\xi^2 =$

2nd Annual 10

(42)

Eienstein's Irreduciblity Eriterion

Let p be a prime and
$f(x) = a_0 + a_1x + \dots + a_nx^n$
be a polynomial of degree n with integral coefficients such that

$$p \nmid a_n,\ p^2 \nmid a_0,\ p \mid a_i \text{ for } i < n$$

Then $f(x)$ is irreducible.

for e.g.

$-18 + 4x + 6x^2 + 7x^3 = 0$

$$7x^3 + 6x^2 + 4x - 18 = 0$$

take prime, $p = 2$.

$2 \nmid 7,\ 4 \nmid 18$ but $2 \mid 6,\ 2 \mid 4,\ 2 \mid 18$

Proof

Assume that $f(x)$ is reducible

Then

$$f(x) = g(x)h(x)$$

where $g(x) = b_0 + b_1x + \dots + b_mx^m$

and

$h(x) = c_0 + c_1x + \dots + c_kx^k$

and b_i's and c_i's are integers.

and $m + k = n$.

Now

$p \mid a_0$

$\Rightarrow p \mid b_0c_0$

where $p^2 \nmid a_0$

$\Rightarrow p \mid b_0$ or $p \mid c_0$

Suppose

$p \mid b_0$ and $p \nmid c_0$

Since

$p \nmid a_n$ ..

$\Rightarrow p \nmid b_m c_k$

$\Rightarrow p \nmid b_m$ and $p \nmid c_k$.

Thus

$p \mid b_0$ but $p \nmid b_m$.

Let 'r' be the smallest +ve integer such that

$p \nmid b_r$ where $0 \leq i < r \leq m$

Consider coeffients of x^r

$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0$

$a_r - b_r c_0 = b_0 c_r + b_1 c_{r-1} + \cdots + b_{r-1} c_1$

since

$p \mid b_i \quad 0 \leq i < r$

$\Rightarrow p \mid a_r - b_r c_0 \quad \because$ $p \mid a+c$ & $p \mid a$ $\Rightarrow p \mid c$.

$\Rightarrow p \mid a_r$ and $p \mid b_r c_0 \quad \because p \mid a_i$; $r < n$. $i < n$.

$\Rightarrow p \mid b_r$ or $p \mid c_0$

$\Rightarrow$ ~~as~~ $p \nmid b_r$ Then $p \mid c_0$

This is contradiction. Since

$p \nmid c_0$ so consequently

$f(x)$ is irreducible.

[redacted]

Algebraic Integer :-

defining polynomial of the an algebraic number 'θ' has the integral coefficients Then algebraic number 'θ' is called algebraic integer. i.e

$$f(x) = x^n + a_0 x^{n-1} + a_1 x^{n-2} + \dots + a_n$$

be the defining polynomial of θ and

$$a_0, a_1, \dots, a_n \in \mathbb{Z}.$$

Then

$$f(x) \in \mathbb{Z}[x]$$

NOTE: Every algebraic integer is an algebraic number but converse may or may not be hold.

Eg :- The defining polynomial of $\sqrt{2}$ is x^2-1 which has integral coefficient so '$\sqrt{2}$' is an algebraic integer.

ordinary integer 'r' the zeros of the monic polynomial with integral coefficient. The set of all algebraic integer is the extension of ordinary integers.

Theorem;- If 'θ' is an algebraic integer Then $R[\theta]$ is an integral domain.

Proof: The sum, difference, and Product of two algebraic integers is an algebraic integer.

let $\alpha = \alpha_1$ and $\beta = \beta_1$ be two algebraic integer having defining polynomial

$$f(x) = x^n + r_1 x^{n-1} + \cdots + r_n$$
$$= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

&

$$q(x) = x^n + S_1 x^{n-1} + \cdots + S_n.$$
$$= (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n).$$

and let $r_{ij} = \alpha_i + \beta_j$ for $i = 1,2,3,\ldots,n$
$j = 1,2,3,\ldots,m$.

and define

$$g(x) = (x - r_{11})(x - r_{12})\cdots(x - r_{mn}).$$

Then $r_{11} = \alpha_1 + \beta_1 = \alpha + \beta$.

is a root of $g(x)$. To prove that $\alpha+\beta$ is an algebraic integer, we will prove that

$$g(x) \in Z[x]$$

Cofficients of $g(x)$ are symmetric polynomials in $r_{11}, r_{12}, r_{13}, \dots, r_{mn}$. and r_{ij} are symmetric polynomials in α_i's and β_j's where $i=1,2,3,\dots n$ ~~with integra~~ and the $j=1,2,3,\dots m$ cofficients of α_i's & β_j's are integers so the coeffient of $g(x)$ are integers and hence

$$g(x) \in Z[x]$$

so

$r_{11} = \alpha+\beta$ is an algebraic integers. Similarly we can prove that $\alpha-\beta$ and $\alpha\cdot\beta$ are an algebraic integers. Hence

$R(\theta)$ is an integral domain.

— x — x — x —

Dr. Farmulos

(47)

Remark: If α is a root of an eqn $f(x) = x^n + \beta_1 x^{n-1} + \beta_2 x^{n-2} + \cdots + \beta_n = 0$ in which $\beta_1, \beta_2, \ldots, \beta_n$ are algebraic integers then 'α' is an algebraic integer.

Theorem: If 'θ' is an algebraic number then there exist some rational integer 'a', $(a \neq 0)$ such that $a(\theta)$ is an algebraic integer.

Proof: Let the defining polynomial of θ be

$$P(x) = x^n + r_1 x^{n-1} + \cdots + r_n.$$

and let L.C.M of denominators of reduced fraction $r_1, r_2, \ldots, r_n$ be 'a'.

Now consider

$$P\left(\frac{x}{a}\right) = \left(\frac{x}{a}\right)^n + r_1\left(\frac{x}{a}\right)^{n-1} + \cdots + r_n.$$

$$\Rightarrow a^n P\left(\frac{x}{a}\right) = x^n + a r_1 x^{n-1} + a^2 r_2 x^{n-2} + \cdots + a^n r_n = q(x)$$

Then '$a\theta$' is the zero of $q(x)$, a monic irreducible polynomial with integral coefficient. Hence $a(\theta)$ is an algebraic ~~number~~ integer.

—— x —— x —— x ——

NOTE:- $R(\theta) = R(a\theta)$; a belonged to $\mathbb{Z}$.
Therefore any algebraic number field can be considered as the result of adjoining an algebraic integer to R.

Theorem:-
If an algebraic number 'θ' satisfies an equation
$$\beta_0 x^n + \beta_1 x^{n-1} + \cdots + \beta_n = 0$$
in which $\beta_0, \beta_1, \cdots, \beta_n$ are algebraic integer's Then $\beta_0(\theta)$ is an algebraic integer.

Proof
Let
$$f(x) = \beta_0 x^n + \beta_1 x^{n-1} + \cdots + \beta_n.$$
$$\Rightarrow f\left(\frac{x}{\beta_0}\right) = \beta_0\left(\frac{x}{\beta_0}\right)^n + \beta_1\left(\frac{x}{\beta_0}\right)^{n-1} + \cdots + \beta_n$$
$$= \frac{\beta_0}{\beta_0^n} x^n + \frac{\beta_1}{\beta_0^{n-1}} x^{n-1} + \cdots + \beta_n$$
$$f\left(\frac{x}{\beta_0}\right) = \frac{x^n}{\beta_0^{n-1}} + \frac{\beta_1}{\beta_0^{n-1}} x^{n-1} + \cdots + \beta_n.$$

$$\left.\begin{aligned}\alpha &= a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \\ \beta &= b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}\end{aligned}\right\} \text{— } ①$$

Then in the product $\alpha\beta$ power of θ are greater than $(n-1)^{th}$ power ~~so~~ so it can be reduced to $(n-1)$ by using the equation

$$\theta^{n+j} = \theta^{j}(r_1\theta^{n-1} + \cdots + r_n) \text{ — } ②$$

Also α^{k} and β^{k} can be obtained from ① by replacing θ by θ_k. and in the product α^{k}, β^{k} highers powers of θ_k can be reducing by using ②.

Hence the field conjugate $(\alpha\beta), (\alpha\beta)', (\alpha\beta)''$ --- $(\alpha\beta)^{n}$. of $\alpha\beta$ are simply $\alpha\beta, \alpha''\beta''$, ---, $\alpha^{(n)}\beta^{(n)}$. Thus.

$(\alpha\beta)^{k} = \alpha^{k}\beta^{k}$

$$N_{\alpha\beta} = (\alpha\beta)(\alpha\beta)'' \cdots (\alpha\beta)^{n} \quad ?$$

$$= \alpha\beta\, \alpha''\beta'' \cdots \alpha^{n}\beta^{n}$$

$$= \alpha\alpha'' \cdots \alpha^{n}\, \beta\cdot\beta'' \cdots \beta^{n}$$

$$N_{\alpha\beta} = N_{\alpha}\cdot N_{\beta}.$$

//

— x — x —

Annual 10 / 2nd

(56)

Ex:

Let $\theta', \theta'', \theta'''$ be the root
$x^3+2x+6=0$
Compute The Number $N_{R(\theta)}(3\theta-2)$

Sol:-

$$x^3+2x+6 = (x-\theta')(x-\theta'')(x-\theta''')$$

$$= x^3-(\theta'+\theta''+\theta''')x^2+(\theta'\theta''+\theta''\theta'''+\theta'\theta''')x - \theta'\theta''\theta''.$$

Comparing the Coeffieni on both sides

for

x^2 $\quad \theta'+\theta''+\theta''' = 0$

x $\quad \theta'\theta''+\theta''\theta'''+\theta'''\theta' = 2$ — (1)

Const $\quad \theta'\theta''\theta''' = -6$

$$N(3\theta-2) = (3\theta-2)'(3\theta-2)''(3\theta-2)'''$$

$$= (3\theta'-2)(3\theta''-2)(3\theta'''-2)$$

$$= (9\theta'\theta''-6\theta'-6\theta''+4)(3\theta''-2)$$

$$= 27\theta'\theta''\theta''-18\theta'\theta''-18\theta'\theta'''+12\theta' - 18\theta'\theta'''+12\theta''+12\theta'''-8$$

$$= 27\theta'\theta''\theta'''-18(\theta'\theta''+\theta''\theta'''+\theta'\theta''') + 12(\theta'+\theta''+\theta''')-8$$

Using (1)

$$N(3\theta-2) = 27(-6)-18(2)+12(0)-8 = -206$$

Definition:

The determinent

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le j < i \le n} (x_i - x_j)$$

is called vendermende determinent.

Ex:-

Let $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ be irreducible over R and let $\theta, \theta', \theta'', \ldots, \theta^{(n)}$ be the zeros of $f(x)$ show that in $R(\theta)$

$$a_0^n \, \Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\theta^{(i)})$$

Sol:

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \prod_{1 \le j < i \le n} (\theta^{(i)} - \theta^{(j)}) \quad \text{--- (1)}$$

Now $f(x) = a_0 (x - \theta^{1})(x - \theta^{(2)})(x - \theta^{3}) \cdots (x - \theta^{n})$.

$$f(x) = a_0 \prod_{i=1}^{n} (x - \theta^{i})$$

$$f'(x) = a_0 \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \ne j}}^{n} (x - \theta^{i})$$

It follows that

$$f'(\theta) = a_0 \prod_{i=2}^{n} (\theta - \theta^{i})$$

$$f''(\theta) = a_0 \prod_{\substack{i \ge 1 \\ i \ne 2}}^{n} (\theta^{2} - \theta^{i})$$

$\vdots$

$$f'(\theta^n) = a_0 \prod_{i=1}^{n-1} (\theta^n - \theta^i)$$

Multiplying these equations

$$\prod_{i=1}^{n} f'(\theta^i) = a_0^n \prod_{i,j=1}^{n} (\theta^i - \theta^j)$$

$n = 3, \quad i = 1, 2, 3, \quad j = 1, 2, 3.$

$$\prod_{i=1}^{n} f'(\theta^i) = a_0^n (-1)^{\frac{n(n-1)}{2}} \prod (\theta^i - \theta^j)^2$$

$$\prod_{i=1}^{n} f'(\theta^i) = a_0^n (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le j < i < n} (\theta^i - \theta^j)^2$$

$$\prod_{i=1}^{n} f'(\theta^i) = a_0^n (-1)^{\frac{n(n-1)}{2}} \Delta(1, \theta, \ldots, \theta^{n-1})$$

$$a^0 \Delta(1, \theta, \ldots, \theta^{n-1}) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\theta^i).$$

(S3)

1- Basis of $R(\theta)$.

2- Integral Basis Of $R[\theta]$.

3- Every ingral base is a base for $R(\theta)$.

~~M Awad~~ obj.

Units and Primes in $R[\theta]$

Definition:-

i) If $\alpha, \beta \in R[\theta]$ we say $\beta | \alpha$ if $\exists$ another $r \in R[\theta]$ s.t $\alpha = \beta r$.

ii) An ~~int~~ integer ε s.t $\varepsilon | 1$ is called unit of $R[\theta]$.

iii) we say α, β are associate if $\alpha = \varepsilon \beta$. where ε is a unite.

NOTE:

The only unit in $R[\theta]$ are only $+1, -1$ i.e $\varepsilon | 1 \Rightarrow \varepsilon = \pm 1$.

ii) $R[i] \rightarrow$ Gussian domain if $\varepsilon = +i, -i$.

iii) If ε is unite then $\frac{1}{\varepsilon}$ is also unite. $\varepsilon \in R[\theta]$ form multipliate group.

Basis of $R(\theta)$ is $\{\theta^1, \theta^2, ---, \theta^{n-1}\}$ since each $\alpha \in R(\theta)$ can be expressed as linear combination of $\theta^1, \theta^2, ---, \theta^{n-1}$

Imp Annual 10

(54)

Theorem An element of $R[\theta]$ is a unit iff its norm is ± 1.

Proof :- Suppose that α is a unit. There exist an integer β such that

$\alpha | 1$

$1 = \alpha\beta$

$$\alpha\beta = 1.$$

Hence

$$N\alpha\beta = N_1$$

$$\cancel{N\alpha \cdot N\beta = N_1}$$

$$N\alpha \cdot N\beta = 1$$

$$\Rightarrow \quad N\alpha = \pm 1$$

Since norm of an integer is a rational integer so $N\alpha = \pm 1$.

Conversely suppose that the norm of an element $\alpha \in R[\theta]$ is ± 1

i.e

$$N\alpha = \pm 1$$

and let

$x^m + a_1 x^{m-1} + \cdots + a_m = 0$ be the defining polynomial of α.
Then defining polynomial of $\frac{1}{\alpha}$ is

$$a_m x^m + a_{m-1} x^{m-1} + \cdots + 1 = 0$$

$$x^m + \frac{a_{m-1}}{a_m} x^{m-1} + \cdots + \frac{1}{a_m} = 0$$

Now $N\alpha$ is a power of the constant term a_m in its defining polynomial.
Therefore $a_m = \pm 1$.
(It follows that $\frac{1}{\alpha} \in R[\theta]$ and α is unit function) *

Ex. Find the units of $R(\sqrt{-5})$ and $R(\sqrt{-3})$.

Since

$-5 \equiv 3 \pmod 4$

$\therefore$ units of $R(\sqrt{-5})$ are of the form

$a + b\sqrt{-5}$

and which are given by the solution

$a^2 + 5b^2 = \pm 1$

The only solution is given to this are

$(\pm 1, 0)$. So its solution are $\pm 1 + 0\sqrt{-5}$
$\Rightarrow \pm 1$.

x ——— x ——— x

NOTE: To find the units of $R(\sqrt{d})$.

i) if $d \equiv 1 \pmod 4$ Then members of $R(\sqrt{d})$ is of the form $\frac{x + y\sqrt{d}}{2}$ and units are find by the solution

$$\left(\frac{x + y\sqrt{d}}{2}\right)\left(\frac{x - y\sqrt{d}}{2}\right) = \pm 1.$$

ii) if $d \equiv 3 \pmod 4$.
Then units are given by the solution $(x + y\sqrt{d})(x - y\sqrt{d}) = \pm 1$.

Euclidean Domain: (56)

A domain $R[\theta]$ is Called Euclidian domain if for any pair $\alpha, \beta \in R[\theta]$ s.t $\alpha, \beta \neq 0$. There is an element $\gamma \in R[\theta]$

$$|N(\alpha - \beta\gamma)| < |N(\beta)|$$

Quardratic Field:

$R(\theta)$ is quardratic field if degree of θ is 2. and $R(\sqrt{d})$ is Called quardratic field and $R[\sqrt{d}]$ is called quardratic domain.

$R[\sqrt{d}]$ is called quardratic Euclidian domain if 'd' has one of the 21 values.

$-11, -7, -3, -2, 2, 3, 5, 6, 7, 11, 13$
$17, 19, 21, 29, 33, 37, 41, 57, 73.$

The Q.E.D is completly known.

Squere Free rational integer.

let d be squere free rational integer if $d \equiv 1 \pmod 4$. Then discrement of $R[\sqrt{d}]$ is

$$\Delta = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d.$$

if $d \equiv 2 \pmod 4$

Then $\Delta = 4d$.

Prime An element δ of $R[\theta]$ is said to be prime If It is not unit and has no factor other Then its associate and units.

i.e

$$\delta \neq \varepsilon = \pm 1$$

only $\delta = \beta\varepsilon$.

Theorem: Every non-unit element of $R[\theta]$ can be written as a finite product of primes.

Proof; we know that every non-unit element $\alpha \in R[\theta]$ has $|N\alpha| = 1$.

Suppose α is not a prime Then $\alpha = \beta r$.

$N\alpha = N\beta \cdot Nr$.

$1 < |N\beta| < |N\alpha|$, $1 < |Nr| < |N\alpha|$.

If either β or p is not prime then It may be factor more but this process must be terminated

$\because$ rational integer $N\alpha$ has finite number of ~~integers~~ divisor of absolute value greater then 1.

Unique Factorization Domain:-

An integral Domain $R[\theta]$ is said to be unique Factorization domain if

i) every $\alpha \in R[\theta]$ such that $\alpha \neq \pm 1$ is the product of finite number of irreducible elements.

ii) The factorization is unique upto the order of factors and to the associate of irreducible element.

Imp Annual 09 (58)

Ex: Prove that $R[\sqrt{-5}]$ is not a unique Factorization domain.

Sol:

$$-5 \equiv 3 \pmod 4$$

Therefore all the elements of $R(\sqrt{-5})$ are of the form.

$$a + b\sqrt{-5} \quad a, b \in \mathbb{Z}.$$

Consider the two representation of

$$21 = 3 \cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5}).$$

It is clear that no two of the number $3, 7, 4+\sqrt{-5}, 4-\sqrt{-5}$, are associate. Now we show that all of them are prime. Suppose that 3 is not prime. Then it is product of two numbers.

$$3 = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5}).$$

$$N_3 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b\sqrt{-5}}$$

$$9 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b\sqrt{-5}}$$

$$N_{a_1+b_1\sqrt{-5}} = 3$$

$$a_1^2 + 5b_1^2 = 3.$$

$a_1^2 + 5b_1^2 = 3$ has no integral solutions so this not true and our supposition is wrong and 3 is prime.

59

Suppose 7 is not a prime. Then

$7 = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5})$.

$N7 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b_2\sqrt{-5}}$

$49 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b_2\sqrt{-5}}$

Then

$N_{a_1+b_1\sqrt{-5}} = 7$.

$a_1^2 + 5b_1^2 = 7$ has no integral solution so this is not true so our supposition is wrong. Hence 7 is prime

now

Suppose that $4+\sqrt{-5}$ is not prime

$4+\sqrt{-5} = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5})$

~~$N_{4+\sqrt{-5}} = (N_{a_1+b_1\sqrt{-5}})(N_{a_2+b_2\sqrt{-5}})$~~

$21 = (N_{a_1+b_1\sqrt{-5}})(N_{a_2+b_2\sqrt{-5}})$.

If neither factor is unit

Then

$N_{a_1+b_1\sqrt{-5}} = 3$, $N_{a_1+b_1\sqrt{-5}} = 7$.

$a_1^2 + 5b_1^2 = 3$, $a_1^2 + 5b_1^2 = 7$.

Non of these is solvable that $4+\sqrt{-5}$ is prime similarly $4-\sqrt{-5}$ is prime

$\Rightarrow R[\sqrt{-5}]$ is not unique factorization

60

Ideal A subset of an integral domain which is group under addition and closed under multiplication is called ideal in R.

OR

$\{0, \alpha\} \subseteq R[\theta]$ is an ideal

if $\alpha, \beta \in R[\theta]$ also $\alpha, \beta \in A$.

$a\alpha + b\beta \in A$ where $a, b \in R[\theta]$.

NOTATION:

if $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ be finite subset of $R[\theta]$ Then the set of all expression

$d_1\alpha_1 + d_2\alpha_2 + \cdots + d_n\alpha_n \in A$ where

$d_1, d_2, \ldots, d_n \in R[\theta]$. is an ideal and is designated by

$\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ or $[\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n]$.

Principal Ideal. (def of principal ideal)

An ideal of $R[\theta]$ is said to principal ideal if it contains of all multiples of α of the domain and is designated by $[\alpha]$ or $\langle \alpha \rangle$

$\langle 1, 2, 3 \rangle$

$\alpha \langle d_1\alpha_1 + d_2\alpha_2 + \cdots + d_n\alpha_n \rangle$ $\qquad \langle 2, 4, 6 \rangle$ $\quad 2\langle 1, 2, 3 \rangle$

Every ideal is a principal ideal.

Theorem: $A \mid C \iff C \subseteq A$ where A and C are ideals.

Proof:- Suppose that $A \mid C$ Then for Some ideal B

$$C = AB.$$

let $A = \langle \alpha_1, \alpha_2, \ldots, \alpha_r \rangle$, $B = \langle \beta_1, \beta_2, \ldots, \beta_s \rangle$.

Then $C = AB = \langle \alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_1\beta_s, \alpha_2\beta_1, \ldots, \alpha_r\beta_s \rangle$ so that every element of C in A so that and also is B.

$$C \subseteq A.$$

Conversely suppose that

$C \subseteq A$ Then for any ideal D.

$$CD \subseteq AD \text{ —— (1)}$$

Choose D so that $AD = \langle e \rangle$ is a principle ideal. let

$$CD = \langle \gamma_1, \gamma_2, \ldots, \gamma_t \rangle$$

~~CD~~ eq(1) $\Rightarrow$

eq(1) $\Rightarrow$ $\gamma_i = e\mu_i$ $\quad i = 1, 2, 3, \ldots, t$

for some integer μ_i

So that

$$CD = \langle e\mu_1, e\mu_2, \ldots, e\mu_t \rangle.$$
$$= \langle e \rangle \langle u_1, \ldots, u_t \rangle.$$

by the above ther $= AD \langle u_1, \ldots, u_t \rangle$

~~$CD =$~~ $C = AF$. $\Rightarrow A \mid C$. //

Congruence of an ideal:-

Two elements $\alpha, \beta \in R[\theta]$ are said to be congruence (mod A) if these difference lies in A, i.e $(\alpha-\beta) \in A$. A divides the ideal $\langle \alpha-\beta \rangle$.

For a fixed α (the set of all elements of $R[\theta]$ which are congruent to α (mod A) is called residue class of α (mod A).

Norm of an ideal:-

The number of residue classes of (mod A) is called the norm of A and is written as NA.

Theorem;

i) All principle ideal are equivalent.

ii) Any ideal equivelent to principle ideal is principle.

Proof i) Consider $\langle \alpha \rangle$ and $\langle \beta \rangle$ are principle ideal Then There exist two non-zero elements γ and δ of $R[\theta]$ such that

$$\langle \gamma \rangle \langle \alpha \rangle = \langle \delta \rangle \langle \beta \rangle$$

$$\Rightarrow \langle \alpha \rangle \sim \langle \beta \rangle$$

and

$$\langle \gamma \rangle \sim \langle \delta \rangle.$$

ii) let A be an ideal and $\langle \alpha \rangle$ be a principle ideal and also

$$A \sim \langle \alpha \rangle$$

Then for some $\beta, r \in R[\theta]$

$$\langle \beta \rangle A = \langle \alpha \rangle \langle r \rangle.$$

$$\langle \beta \rangle A = \langle \alpha r \rangle \quad \text{---} (1)$$

$$\Rightarrow \langle \beta \rangle \mid \langle \alpha r \rangle$$

$$\Rightarrow \beta \mid r\alpha.$$

$$\Rightarrow r\alpha = \beta \delta$$

using in eqn (1)

$$\langle \beta \rangle A = \langle \beta \delta \rangle.$$

$$\langle \beta \rangle A = \langle \beta \rangle \langle \delta \rangle$$

$$A = \langle \delta \rangle.$$

Hence A is principle ideal.

— x — x — x — x —

$\mathcal{A} = \{ A :$ where A is an ideal of $R[\theta]\}$

Class number of the field $R[\theta]$:-

The set of ideal can be partitioned into equivelence classes s.t two ~~elements~~ ideals belong to same class iff they are equivelent.

The number (h) of such classes is called the class number of the field $R[\theta]$.

class number of $R[\theta]$ is 1 $\Leftrightarrow$ every ideal is principle ideal.

Q. Theorem. If A is non-zero ideal in $R[\theta]$ Then There exist $\alpha \in A$ such that

$N\alpha < NA\sqrt{\Delta}$ where Δ descriminent of $R[\theta]$.

Q.

Theorem

Prove That class number h of a field is finite:

Proof: If every ideal is principle ideal (if R is the field) Then class number is one.

If R is not the field. Then it is sufficient to show That for each class There exist an ideal $B \subseteq R[\theta]$ such that

$$N_B < \sqrt{\Delta}$$

let C be a such ideal in given class $\mathcal{C}$.

Choose an ideal A such that AC is principle ideal Then.

$AC \sim \langle 1 \rangle$ Since all Principle ideals are equivelent.

Now by Theorem There exist $\alpha \in A$. Such that

$$N\alpha < NA\sqrt{\Delta} \longrightarrow (1)$$

Also

$$\alpha \in A \Rightarrow \langle \alpha \rangle \subseteq A$$

$$\Rightarrow A \mid \langle \alpha \rangle$$

$$\Rightarrow \langle \alpha \rangle = AB$$

$$N\alpha = NA \cdot NB$$

eqn (1) $\Rightarrow$

$$\cancel{NA}\,NB < \cancel{NA}\sqrt{\Delta}$$

$$NB < \sqrt{\Delta}.$$

Now we are to show that

$$B \in \ell$$

$$AC \sim \langle 1 \rangle$$

and

$$AB \sim \langle \alpha \rangle$$

$$AB \sim AC$$

$$\Rightarrow B \sim C$$

$$\Rightarrow B \in \ell$$ Hence proved.

Theorem: If p is a rational prime and $p \nmid h$ Then
$$A^p \sim B^p \Rightarrow A \sim B.$$

Proof:- Since p and h are relatively prime i.e $(p,h)=1$. $\exists$ +ve rational integers x and y in $\mathbb{Z}$ s.t

$$px - hy = 1 \quad \text{—— (1)}$$

$$A^p \sim B^p \Rightarrow \langle \alpha \rangle A^p = \langle \beta \rangle B^p.$$

$$\langle \alpha \rangle^x A^{px} = \langle \beta \rangle^x \cdot B^{px}.$$

by eqn (1)

$$\langle \alpha \rangle^x A^{1+hy} = \langle \beta \rangle^x B^{1+hy}.$$

$$\langle \alpha \rangle^x \cdot A \cdot A^{hy} = \langle \beta \rangle^x B \cdot B^{hy}.$$

But A^h and B^h are principle ideals

Hence so are

$$\langle \alpha \rangle^x A^{hy} \text{ and } \langle \beta \rangle^x B^{hy}$$

$$\langle \alpha \rangle^x A^{hy} = \langle \gamma \rangle \text{ and } \langle \beta \rangle^x B^{hy} = \langle \delta \rangle$$

$$\Rightarrow \langle \gamma \rangle A = \langle \delta \rangle B$$

$$\Rightarrow A \sim B$$

//

Theorem. If $\alpha, \beta \in R(\theta)$ Then show that

$$N\alpha\beta = N\alpha \cdot N\beta$$

Proof: Since $\alpha, \beta \in R(\theta)$ There α, β can be expressed in θ.

$$\left.\begin{aligned} \alpha &= a_0 + a_1\theta + a_2\theta + \dots + a_n\theta. \\ \beta &= b_0 + b_1\theta + b_2\theta + \dots + b_m\theta. \end{aligned}\right\} \longrightarrow (1)$$

Then in the product of $\alpha\beta$ power of θ higher then $(n-1)$ can be reduced using

$$\theta^{n+j} = -\theta^j\left[r_1\theta^{n-1} + \dots + r_n\right] \quad -(2)$$

Also α^k and β^k can be obtained from (1) by replacing θ by θ_k and in the product $\alpha^k\beta^k$ higher powers of θ can be reduced using eqn (2). Hence the field conjugate

$\alpha\beta, (\alpha\beta)', (\alpha\beta)'' \dots, (\alpha\beta)^n$ of $\alpha\beta$ are of the form $\alpha\beta, \alpha'\beta', \alpha''\beta'', \dots, \alpha^n\beta^n$

so

$$N\alpha\beta = \alpha\beta\,\alpha'\beta'\,\alpha''\beta'' \dots \alpha^n\beta^n$$

$$= \alpha\alpha' \dots \alpha^n \cdot \beta \cdot \beta' \dots \beta^n$$

$$N\alpha\beta = N\alpha \cdot N\beta$$

Hence the proof.

Theorem: The norm of an algebraic integer is ~~a~~ rational integer

Proof let α be an algebraic integer corresponding defining polynomial is

$$f(x) = x^m + S_1 x^{m-1} + \cdots + S_m.$$

and let

$$f(x) = (x-\alpha')(x-\alpha'')\cdots(x-\alpha^n).$$

where $\alpha', \alpha'', \ldots, \alpha^n$ are field conjugate of α.

Since the set of field conjugate of α contains a several copy of conjugate of α. so

$$f(x) = [f(x)]^{n/m}.$$

$$(x-\alpha')(x-\alpha'')\cdots(x-\alpha^n) = [f(x)]^{n/m}.$$

Comparing the constant term of both polynomial we have

$$\alpha' \cdot \alpha'' \cdots \alpha^n = (S_m)^{n/m}$$

$$N\alpha = (S_m)^{n/m}$$

Norm of α is power of S_m where S_m is an integer. Hence $N\alpha$ is a rational integers.

Deserment.

If $\alpha, \beta, --, \gamma$ n element belongs to $R(\theta)$ Then the determinent

$$\Delta(\alpha,\beta,--,\gamma) = \begin{vmatrix} \alpha & \alpha' & \alpha'' & --- & \alpha^n \\ \beta & \beta' & \beta'' & --- & \beta^n \\ \vdots & \vdots & \vdots & & \vdots \\ \gamma & \gamma' & \gamma'' & --- & \gamma^n \end{vmatrix}^2.$$

$\alpha^k, \beta^k, \gamma^k$ are Conjugate of α, β, γ respectively.

Theorem: If $\alpha, \beta, --, \gamma$ are in $R[\theta]$ Then $\Delta(\alpha,\beta, - \gamma)$ is a rational integer.

Proof: If we take the row by Column product.

$$\Delta(\alpha,\beta,--\gamma) = \begin{vmatrix} \alpha & --- & \alpha^n \\ \vdots & & \vdots \\ \gamma & --- & \gamma^n \end{vmatrix} \begin{vmatrix} \alpha & --- & \gamma \\ \vdots & & \vdots \\ \alpha^n & --- & \gamma^n \end{vmatrix}$$

$$= \begin{vmatrix} \alpha^2 + --- + (\alpha^n)^2 + --- + \alpha\gamma + --- + \alpha^n\gamma^n \\ \vdots \\ \alpha\gamma + --- + \alpha^n\gamma^n + --- + \gamma^2 + --- + (\gamma^n)^2 \end{vmatrix}$$

Now from previous Theorem

$$\alpha\beta + \alpha''\beta'' + --- + \alpha^n\beta^n = \alpha\beta + (\alpha\beta)' + --- + (\alpha\beta)^n.$$

and the sum of the field conjugates of an integer is itself a rational

integer. Hence $\Delta(\alpha, \beta, \ldots, \nu)$ can be written as the integers entries. Hence
$\Delta(\alpha, \beta, \ldots, \nu)$ is an rational integer.

Theorem:

If $\omega_1, \omega_2, \ldots, \omega_n$ are any n integer of $R[\theta]$ for which
$|\Delta(\omega_1, \omega_2, \omega_3, \ldots, \omega_n)|$ has smallest possible value different from zero form a basis of $R[\theta]$

Proof:

Let

$$\omega_i = \sum_{j=0}^{n-1} a_{ij}\theta^j \quad i = 1, 2, \ldots, n. \qquad (1)$$

where the $a_{ij} \in R$. Then

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \begin{vmatrix} \omega_1 & \cdots & \omega_n \\ \vdots & & \vdots \\ \omega_1^{n} & \cdots & \omega_n^{(n)} \end{vmatrix}^2$$

$$= \begin{vmatrix} \sum_{j=0}^{n-1} a_{1j}\theta^j & \cdots & \sum_{j=0}^{n-1} a_{nj}\theta^j \\ \vdots & & \vdots \\ \sum_{j=0}^{n-1} a_{1j}\theta_n^j & \cdots & \sum_{j=0}^{n-1} a_{nj}\theta_n^j \end{vmatrix}^2$$

and this can be factored.

$$\Delta(w_1, w_2, \ldots, w_n) = \left\{ \begin{vmatrix} 1 & \theta & \cdots & \theta^{n-1} \\ \vdots & & & \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{vmatrix} \begin{vmatrix} a_{10} & \cdots & a_{n0} \\ \vdots & & \\ a_{1,n-1} & \cdots & a_{n,n-1} \end{vmatrix} \right\}^2$$

$$= \Delta(1, \theta, \ldots, \theta^{n-1}) \det|a_{ij}|^2 \quad (2)$$

where $\theta_1, \theta_2, \ldots, \theta_n$ are conjugate of θ.

Since $\Delta(w_1, w_2, \ldots, w_n) \neq 0$ also $\det|a_{ij}| \neq 0$ and the system of eqn (1) can be solved for the number $1, \theta_1, \ldots, \theta_{n-1}$ giving linear expression in $w_1, \ldots, w_n$. Thus every number $f \in R[\theta]$ can be written in the form.

$$f = b_1w_1 + b_2w_2 + \cdots + b_3w_3 \quad (3)$$

where b_i's are rational. we must show that they are rational integer. If this not the case of (3), then some b_i's has non-zero fractional part. i.e

$$b_i = [b_i] + c, \quad 0 < c < 1$$

Put.

$$f_i = f - [b_i]w_i$$
$$= b_1w_1 + \cdots + cw_i + \cdots + b_nw_n$$

Just the same way that (2) Deduce from (1), we can deduce from the system of equation.

$$\omega_1 = \omega_1$$
$$\omega_2 = \omega_2$$
$$\vdots$$
$$\omega_{i-1} = \omega_{i-1}$$
$$g_i = b_1\omega_1 + b_2\omega_2 + \cdots + c\omega_i + \cdots + b_n\omega_n$$
$$\omega_{i+1} = \omega_{i+1}$$
$$\vdots$$
$$\omega_n = \omega_n.$$

The relation.

$$\Delta(\omega_1, \ldots, g_i, \ldots, \omega_n) = \begin{vmatrix} 1 & 0 & \cdots & & 0 \\ 0 & 1 & \cdots & \vdots & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ b_1 & b_2 & \cdots c & \cdots & b_n \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 \end{vmatrix} \times \Delta(\omega_1, \omega_2, \ldots, \omega_n)$$

$$= c^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

But This implies that

$\Delta(w_1, w_2, \ldots, \delta_i, \ldots w_n)$ is numerically smaller than $\Delta(w_1, w_2, \ldots, w_n)$. and is not zero. which is contradiction to given Hypothesis. Hence each b_i's is a rational integer.

— x — x — x — x —

Definition. The Discomenent.

$$\Delta(1, x_1, x_2, x_3, \ldots, x_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & & & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

$$= \prod_{1 \le j < i \le n} (x_i - x_j)$$

is called vendrvall determinant

Theorem:-

4. Let $f(x) = a_0 x^n + \cdots + a_n$ be irreducible over R and let $\theta, \theta'', \theta''', \ldots, \theta^n$ be zero of $f(x)$ show that in $R(\theta)$.

$$a_0^n \Delta(1, \theta, \cdots, \theta^n) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f(\theta^i)$$

Proof:

Sn:

$$\Delta(1, \theta, \theta^2, \cdots, \theta^n) = \prod_{1 \le j < i \le n} (\theta^{(i)} - \theta^{(j)}) \quad (1)$$

$$f(x) = a_0 (x - \theta^{(1)})(x - \theta^{(2)}) \cdots (x - \theta^n).$$

Now
$$f(x) = a_0 \prod_{i=1}^{n} (x - \theta^i)$$

$$f'(x) = a_0 \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \ne 0}}^{n} (x - \theta^i)$$

It follow that put $x = \theta$.

$$f'(\theta) = a_0 \prod_{i=2}^{n} (\theta' - \theta^i) \quad \because \theta = \theta'$$

Similarly.

$$f'(\theta'') = a_0 \prod_{\substack{i=1 \\ i \ne 2}}^{n} (\theta'' - \theta^{(i)})$$

$$f'(\theta''') = a_0 \prod_{\substack{i=1 \\ i \ne 3}}^{n} (\theta''' - \theta^i)$$

$$f'(\theta^{n}) = a_0 \prod_{i=1}^{n} (\theta^{(n)} - \theta^{i})$$

Multiplying of all these equations

$$\prod_{i=1}^{n} f'(\theta^{i}) = a_0^{n} \prod_{i,j=1}^{n} (\theta^{(i)} - \theta^{j})$$

$j < i$

$$\prod_{i=1}^{n} f'(\theta^{i}) = a_0^{n} (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le j < i < n} (\theta^{(i)} - \theta^{(j)})$$

By (1)

$$\prod_{i=1}^{n} f'(\theta^{i}) = a_0^{n} (-1)^{\frac{n(n-1)}{2}} \Delta(1, \theta, \ldots, \theta^{n-1})$$

$$\rightarrow a_0^{n} \Delta(1, \theta, \ldots \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\theta^{i})$$

Units and Primes in $R[\theta]$:-

If $\alpha, \beta \in R[\theta]$, we say.

$\beta \mid \alpha$ if There exist another $\gamma \in R[\theta]$

Such that $\alpha = \gamma\beta$. An integer ε such that $\varepsilon \mid 1$ is called a unit of $R[\theta]$.

α & β are associate if $\alpha = \varepsilon\beta$. where ε is unit.

NOTE:- Every integral Basis is Basis of $R(\theta)$.

Theorem.

Any two integral Basis of an algraic number field have the same Discriment.

Proof; Let $\alpha_1, \alpha_2, \dots, \alpha_n$ and $\beta_1, \beta_2, \dots, \beta_n$ be two basis of $R[\theta]$

Then

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = (\det|a_{ij}|)^2 \, \Delta(\beta_1, \beta_2, \dots, \beta_n) \quad (1)$$

and

$$\Delta(\beta_1, \beta_2, \dots, \beta_n) = (\det|a_{ij}|)^2 \, \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \quad (2)$$

eq (1) $\Rightarrow$ $\Delta(\beta_1, \dots, \beta_n) \mid \Delta(\alpha_1, \dots, \alpha_n)$

& eq (2) $\Rightarrow$ $\Delta(\alpha_1, \dots, \alpha_n) \mid \Delta(\beta_1, \dots, \beta_n)$

$\Rightarrow \Delta(\alpha_1, \dots, \alpha_n) = \Delta(\beta_1, \dots, \beta_n)$.

Prove of $f(x) = x^3 + px + q$.
is irreducible over R and a is one of its zero Then show that.

$$\Delta(1, \alpha, \alpha^2) = -27q^2 - 4p^2.$$

Ex: 1) The only integral Domain in $R[O]$ are $+1$ & -1

2) $R[i]$ is Called Gussian Domain

i. i & $-i$ are the only units in Gussian Domain.

NOTE: These units i.e $\{-1, 1\}$ form a multiplicative group.

If ε is a unit Then $\frac{1}{\varepsilon}$ is also unit

$$\varepsilon . \varepsilon^{-1} = 1$$

Theorem: An element of $R[\theta]$ is unit iff its norm is ± 1.

Proof Suppose that $\alpha \in R[\theta]$ is a unit. Then exist an integer β such that

$$\alpha\beta = 1.$$

Hence

$$N\alpha\beta = N_1.$$

$$N\alpha \cdot N\beta = N_1$$

$$\Rightarrow N\alpha \text{ is } \pm 1.$$

Since Norm of an integer is a rational integer so

$$N\alpha = \pm 1$$

Conversely Suppose that.

$$N\alpha = \pm 1 \text{ and}$$

Let

$$x^m + a x^{m-1} + \cdots + a_m = 0$$

be the defining polynomial of α.

Then the defining eqn of $\frac{1}{\alpha}$ is

$$a_m x^m + a_{m-1} x^{m-1} + \cdots + 1 = 0$$

Now $N\alpha$ is the power of the constant term a_m in its defining polynomial. Therefore $a_m = \pm 1$

$$\Rightarrow \frac{1}{\alpha} \in R[\theta]$$

and hence α is unit.

Theorem:

let d be square free rational integer

i) If $d \equiv 1 \pmod 4$ Then the element of $R(\sqrt{d})$ are either of the form

$$a + b\sqrt{d} \quad a \,\&\, b \in \mathbb{Z}$$

$$\text{or} \quad \frac{a+b\sqrt{d}}{2}, \ a \,\&\, b \text{ are in } \mathbb{Z}, \ a \equiv b \equiv 1 \pmod 2)$$

ii) $d \equiv 2$ or $3 \pmod 4$. Then all the elements of $R(\sqrt{d})$ are of the form

$$a + b\sqrt{d} \quad a, b \in \mathbb{Z}.$$

Proof we take $1, \sqrt{d}$ as basis of $R[\sqrt{d}]$ so The every element of $R[\sqrt{d}]$ can be uniquely expressed as $a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$.

If $b = 0$ Then $a + b\sqrt{d} = a$ is an rational integer.

If $b \neq 0$ Then the following defining polynomial of $a + b\sqrt{d}$

is $f(x) = (x - (a+b\sqrt{d}))(x - (a - b\sqrt{d}))$
$= (x - a - b\sqrt{d})(x - a + b\sqrt{d})$.

$= (x-a)^2 - (b\sqrt{d})^2$

$= x^2 + a^2 - 2ax - b^2 d$

$f(x) = x^2 - 2ax + a^2 - b^2 d$

we assume that

$a + b\sqrt{d} \in R[\sqrt{d}]$

A) $2a$ & $a^2 - b^2 d$ both are rational integer

$\Rightarrow (2a)^2 - 4(a^2 - b^2 d) = 4b^2 d$
is a rational integer
$\Rightarrow$ $2b$ is also a rational integer
Since d is square free

B) Suppose $2a$ is odd and let

$a = k + 1/2$. where $k \in Z$

Then.
$4a^2 - 4b^2 d \equiv 0 \pmod 4$.

$(2k+1)^2 - 4b^2 d \equiv 0 \pmod 4$

$1 - 4b^2 d \equiv 0 \pmod 4$.

$4b^2 d \equiv 1 \pmod 4$

~~$2b \equiv 1 \pmod 4$~~
and ~~$d \equiv 1 \pmod 4$~~

Since d is square free
$\Rightarrow 2a$ is odd and $2b$ is odd.

c) If $2a$ is even and let.
$2a = 2k$
$\Rightarrow a = k$. $k \in \mathbb{Z}$.
Then.
$$4a^2 - 4b^2 d \equiv 0 \pmod 4.$$
$$(2k)^2 - 4b^2 d \equiv 0 \pmod 4.$$
$$4b^2 d \equiv 0 \pmod 4.$$
$$4b^2 \equiv 0 \pmod 4 \quad \because d \text{ is square free.}$$
$$2b \equiv 0 \pmod 4$$
$\Rightarrow 2b$ is even.
Both $2b$ & $2a$ are even.
It follows (A), (B) and (C) that

$a + b\sqrt{d} \in R(\sqrt{d})$. Then either both $2a$ and $2b$ are odd or both are even integers

Conversely if $2a$ & $2b$ are both Then clearly the poly $f(x)$ has Coefficient in $\mathbb{Z}$ and
$$a + b\sqrt{d} \in R(\sqrt{d}).$$

Now if $d \equiv 1 \pmod 4$ and
$2a$ & $2b$ are both odd

Then the polynomial $f(x)$ has coefficient in Z. It proves that elements of $f(x)$ has coefficient either of the form $a+b\sqrt{d}$, $a,b\in Z$.
or $\frac{a+b\sqrt{d}}{2}$, $a \equiv b$ (mod 4)
~~$a \equiv b \equiv 1$ (mod 4)~~.

ii) if $d \equiv 2$ or 3 (mod 4).
Then its element of the form $a+b\sqrt{d}$. Then
$a+b\sqrt{d}$ is an integer iff
a is rational integer and
$b=0$. If $b\neq 0$ then
as discussed in (i) That
$2a$ is even.
$\Rightarrow 2b$ is even.

a & b are in Z and all the element of $R(\sqrt{d})$ are of the form $a+b\sqrt{d}$.

$\propto$

Remarks. The unit of $R[\sqrt{d}]$ are the integers for which Norm is ± 1.

$x+y\sqrt{d}$, $x-y\sqrt{d}$.

So

$$(x+y\sqrt{d})(x-y\sqrt{d}) = \pm 1$$

$$x^2 - dy^2 = \pm 1$$

Not if

$d \equiv 1 \pmod 4$ Then elements of $R(\sqrt{d})$ are of the form

$$\frac{x+y\sqrt{d}}{2}$$

if

$d \equiv 3 \pmod 4$ Then elements of $R[\sqrt{d}]$ are of the form.

So $x+y\sqrt{d}$ =

its unit

$$(x+y\sqrt{d})(x-\sqrt{y}d) = \pm 1.$$

Euclidean Domain,

if $\alpha, \beta, \gamma \in R[\theta]$ such that
$|N(\alpha - \beta\gamma)| < |N(\beta)|$.

- $R(\sqrt{d})$ is quardratic field i.e
$R(\theta)$ is Quardratic if deg of θ is 2.
& $R[\sqrt{d}]$ is quardratic Integral
Domain.

NOTE: if $R[\sqrt{d}]$ and

$d \equiv 1 \pmod 4$ Then

$$\Delta = \begin{vmatrix} 1 & \frac{1}{2}(1+\sqrt{d}) \\ 1 & \frac{1}{2}(1-\sqrt{d}) \end{vmatrix}^2 = d.$$

and if $d \equiv 2$ or $3 \pmod 4$

$$\Delta = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d.$$

NOTE: Descriment of a field is the discriment of its integral basis.

Prime :- A non unit element of $R[\theta]$ whose factors only its associate.

— x — α — σ —

Theorem- Every non-unit element of R[θ] can as a finite product of primes.

Proof we know that every non-unit element of R[θ] has

$|N\alpha| > 1$.

Suppose α is not prime then

$\alpha = \beta\gamma$ where β, γ are non-unit of R[θ]

$N\alpha = N\beta \cdot N\gamma$

$1 < |N\beta| < |N\alpha|$, $1 < |N\gamma| < |N\alpha|$

If either β, γ are not prime it may be factored more but this process must be terminated ∵ rational integers $N\alpha$ has a finite number of divisor of absolute value greater than 1.

— α — α —— α —

Unique factorization Domain:-

$R[\theta]$ is called U.F.D if

i) every $\beta \neq 1 \in R[\theta]$ can be written in a product of irreducible elements.

ii) The factorization is unique up to the order of the factor and the to the associate of irreducible element.

Ex: Prove That $R(\sqrt{-5})$ is not a unique factorization domain.

Sol:-

$-5 \equiv 3 \pmod 4$ Therefore all the elements of $R(\sqrt{-5})$ are of the form

$$a + b\sqrt{-5} \; ; \; a, b \in \mathbb{Z}.$$

Consider The two representation of 21 is

$$21 = 7 \cdot 3.$$

&

$$21 = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

It is Clear that no two of them are associate. we show that all of them are prim in $R(\sqrt{-5})$.

Suppose That 3 is not prime

Then

$$3 = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{5})$$

$$N_3 = N_{a_1 + b_1\sqrt{-5}} \cdot N_{a_2 + b_2\sqrt{5}}.$$

$$9 = N_{a_1 + b_1\sqrt{-5}} \cdot N_{a_2 + b_2\sqrt{5}}.$$

Then

$$N_{a_1+b_1\sqrt{-5}} = 3$$

$$a_1^2+5b_1^2 = 3.$$

It has no integral solution so this not true. Hence 3 is prime

Suppose that 7 is not prime then it is product of two number of $R(\sqrt{-5})$

$$7 = (a_1+b_1\sqrt{-5})(a_2+b_2\sqrt{-5}).$$

$$N_7 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b_2\sqrt{-5}}.$$

$$49 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b_2\sqrt{-5}}.$$

$$7 = N_{a_1+b_1\sqrt{-5}}$$

$$\Rightarrow a_1^2+5b_1^2 = 7$$

It has integral solution Hence 7 is prime

Suppose that $4+\sqrt{-5}$ is not a prime Then

$$4+\sqrt{-5} = (a_1+b_1\sqrt{-5})(a_2+b_2\sqrt{-5}).$$

$$N_{4+\sqrt{-5}} = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b_2\sqrt{-5}}$$

$$21 = N_{a_1+b_1\sqrt{-5}} \cdot N_{a_2+b_2\sqrt{-5}}.$$

If neither factor is a unit

Then $7\times 3 = N_{a_1+b_1\sqrt{-5}}\, N_{a_2+b_2\sqrt{-5}}$

$N_{a_1+b_1\sqrt{-5}} = 3$.

or

$N_{a_1+b_1\sqrt{-5}} = 7$.

i.e

$a_1^2 + 5b_1^2 = 3$ or $a_1^2 + 5b_1^2 = 7$.

None of these is solvable in $R(\sqrt{-5})$

It follows that $4+\sqrt{-5}$ is prime

Similarly $4-\sqrt{-5}$ is ~~not~~ prime.

$\Rightarrow R[\sqrt{-5}]$ is not a unique factorization Domain.

NOTE: Every Euclidean domain is unique factorization Domain.

Domain in which we find G.C.D is called Euclidean Domain

$$|N(\alpha-\beta\gamma)| < |N\beta|.$$

— x ——— x ———

Ideal: A subset A of $R(\theta)$ containing atleast one element beside zero of an integral Domain $R[\theta]$ is called an ideal of $R[\theta]$ if for $\alpha, \beta \in A$.

$a\alpha + b\beta \in A$ where $a, b \in R[\theta]$.

NOTATION $[\alpha_1, \alpha_2, \ldots \alpha_n]$

Principal ideal

An ideal of the Domain $R[\theta]$ is called principal ideal if it consists of all multiples of α of the domain and is designated by $[\alpha]$, or $\langle\alpha\rangle$.

$\alpha\langle d_1\alpha_1 + d_2\alpha_2 + \cdots + d_n\alpha_n\rangle$.

" Every ideal is a principal ideal "

Basis of ideal

$\alpha_1, \alpha_2, \cdots, \alpha_n$.

Discriment of ideal Δ is

$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)$.

Theorem: The value of the discriment of an ideal is independent of the choice of the basis.

Arithmatic of ideal

Def: If $A = \langle\alpha_1, \alpha_2, \cdots, \alpha_n\rangle$
$B = \langle\beta_1, \beta_2, \cdots, \beta_s\rangle$
and ideal Then AB i.e product of ideal is again ideal.

$AB = \langle\alpha_1\beta_1, \alpha_1\beta_2, \cdots, \alpha_1\beta_s, \alpha_2\beta_1, \cdots, \alpha_n\beta_s$

Theorem: The product of ideal AB does not depends upon the representation choosen for the ideals A & B.

Proof: By taking two different representation for A & B.

$A = \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle$, $B = \langle \beta_1, \beta_2, \dots, \beta_s \rangle$
& $A = \langle \alpha_1', \alpha_2', \dots, \alpha_m' \rangle$, $B = \langle \beta_1', \beta_2', \dots, \beta_s' \rangle$

Then find
C & C'

(

Def: If A & B & C are ideal & AB = C Then we say A divides C That is

$A \mid C$. $C \subseteq AD$

we also $AD = \langle e \rangle$.

Theorem $A|C \Leftrightarrow C \subseteq A$ and A & C are ideal.

Proof.

Suppose that $A|C$ there is ideal B s.t.

$$C = AB$$

let

$A = \langle \alpha_1, \alpha_2, \cdots, \alpha_r \rangle$ and $B = \langle \beta_1, \beta_2, \cdots, \beta_s \rangle$

Then

$$C = \langle \alpha_1\beta_1, \alpha_1\beta_2, \cdots, \alpha_1\beta_s, \alpha_2\beta_1, \cdots, \alpha_r\beta_s \rangle.$$

so that every element of C is is in A and also in B.

$$\Rightarrow \quad C \subseteq A.$$

Conversely suppose that

$C \subseteq A$ Then for ideal

$$CD \subseteq AD \quad \text{—(1)}$$

Chose D so that

$AD = \langle e \rangle$ is principal ideal let.

$$CD = \langle \gamma_1, \gamma_2, \cdots, \gamma_t \rangle$$

eq (1) $\Rightarrow$

$\gamma_i = e\mu_i$. $i = 1, 2, 3, \cdots, t$.

for some integer μ_i

so that

$$CD = \langle e\mu_1, e\mu_2, \cdots, e\mu_t \rangle$$
$$= \langle e \rangle \langle \mu_1, \mu_2, \cdots \mu_t \rangle.$$

$$CD = AD\langle \mu_1, \mu_2, ---, \mu_t\rangle$$

$$C = A\langle u_1, u_2, ---, u_t\rangle$$

$$C = AF.$$

$$\Rightarrow A \mid C$$

— α — α — α — α —

NOTE: An ideal is divisible by only a finit number of ideal.

G. C. D of ideals.

A common Divisor of the ideals A & B which is divisible by every. Common divisor of A & B is called G.C.D of A & B and it is denoted as

$$(A, B) = D.$$

⇒ let C be common Divisor of A & B and D is greater then C.

$$C/A \ \& \ C/B.$$

$$\& \ D/A \ \& \ D/B$$

$$C/D.$$

↓

G.C.D.

— α — α —

Theorem.

Each pair of ideals A and B has a unique G.C.D. It is composed of number $\alpha+\beta$ where α runs ove A & β run over B.

Prime ideal

A & B are ideals they are relatively prim if $(A, B) = \alpha + \beta = \langle 1 \rangle$.

NOTE: if $(A, B) = \langle 1 \rangle$ then

There $\alpha \in A$ and $\beta \in B$.

s.t

$\alpha + \beta = 1$.

Congruence of an ideal:

two elements.

$\alpha, \beta \in R[\theta]$ s.t.

$\alpha \equiv \beta \pmod{A}$

if '$\alpha - \beta$' lies in A. A divides the ideal $\langle \alpha - \beta \rangle$.

Norm of an ideal:

The number of residue classes modulo 'A' is called the norm of A and it is denoted as

NA.

Equivelent Ideal:

Ideals A & B of $R[\theta]$ are said to equivelent if there are non-zero elements. α and $\beta \in R[\theta]$ Such that

$$\langle\alpha\rangle A = \langle\beta\rangle B.$$

Then we write

$$A \sim B.$$

NOTE: i) $\sim$ is an equivelence relation.

ii) $A \sim B$ and $C \sim D$
$\Rightarrow AC \sim BD$.

iii) $AC \sim BC \Rightarrow A \sim B$.

Theorem:

i) All principal ideals are equivelent.

ii) Any ideal equivelent to principal ideal is principal ideal.

Proof:- Consider the principal ideal $\langle\alpha\rangle$ and $\langle\beta\rangle$ Then There exist two non-zero elements γ & δ of $R[\theta]$ such that.

$$\langle\gamma\rangle\langle\alpha\rangle = \langle\delta\rangle\langle\beta\rangle.$$

$$\Rightarrow \langle\alpha\rangle \sim \langle\beta\rangle.$$

and

$$\langle\gamma\rangle \sim \langle\delta\rangle$$

ii) Suppose

$$A \sim \langle \alpha \rangle.$$

Then for som $\beta, \gamma \in R[\theta]$

$$\langle \beta \rangle A = \langle \gamma \rangle \langle \alpha \rangle$$

$$\langle \beta \rangle A = \langle \gamma \alpha \rangle \quad \text{---} (1)$$

$$\langle \beta \rangle \mid \langle \gamma \alpha \rangle$$

$$\beta \mid \gamma \alpha.$$

$\gamma \alpha = \beta \delta$ using in (1)

$$\langle \beta \rangle A = \langle \beta \delta \rangle$$

$$\langle \beta \rangle A = \langle \beta \rangle \langle \delta \rangle$$

$$A = \langle \delta \rangle$$

$\Rightarrow$ A is principal ideal

— α — α —

NOTE:: If A is non-zero ideal in $R[\theta] \neq R$ Then $\exists$ a number $\alpha \neq 0$ in A s.t

$$|N\alpha| \leq N_A \sqrt{\Delta}.$$

//

Theorem:-

The class number h of field is finite.

Proof:-

If the field is R Then h is one and there is nothing to proove. If the field is different from R then It is enough to show that in each class of ideals there is an ideal B such that

$$N_B < \sqrt{\Delta}$$

let 'C' b an ideal in the given class l of ideal.

Choose an ideal A so that AC is a principal ideal Then.

$AC \sim \langle 1 \rangle$ Since all the principal ideals are equivalent.

Now By theorem There exist an $\alpha \in A$, $\alpha \neq 0$. s.t

$$|N\alpha| < N_A \sqrt{\Delta} \longrightarrow (1)$$

Also $\alpha \in A \Rightarrow \langle \alpha \rangle \subset A$

$\Rightarrow A \mid \langle \alpha \rangle$

$\Rightarrow \langle \alpha \rangle = AB$ for some ideal B

$$N_{\langle \alpha \rangle} = N_{AB}.$$

$$|N_{\langle \alpha \rangle}| = N_A \cdot N_B \longrightarrow (2)$$

Equating ① & ②

$NA \cdot NB < NA \cdot \sqrt{\Delta}$

$\Rightarrow NB < \sqrt{\Delta}$

finally we show $B \in \mathcal{C}$

$AC \sim \langle 1 \rangle$ and $AB \sim \langle \alpha \rangle$

$\Rightarrow AB \sim AC$ ∵ all principal ideals are equivalent.

$\Rightarrow B \sim C$

$\Rightarrow B \in \mathcal{C}$

Since $C \in \mathcal{C}$. Hence proof.

Theorem

If h is a class numbers of a field then h^{th} power of any ideal is principal.

i.e $A^n \sim \langle 1 \rangle$

$\Rightarrow A^n$ is principal ideal.

Theorem :- If p is rational prime and $p \nmid h$ then

$$A^p \sim B^p \Rightarrow A \sim B.$$

Since

$(p, h) = 1$ i.e relatively prime.

Therefore $\exists$ +ve rational integer x & y such that

$$px - hy = 1 \longrightarrow (1)$$

$$A^p \sim B^p \Rightarrow \langle\alpha\rangle A^p = \langle\beta\rangle B^p \quad \text{By def.}$$

$$\Rightarrow \langle\alpha\rangle^x A^{px} = \langle\beta\rangle^x B^{px}$$

By eqn (1)

$$\langle\alpha\rangle^x A^{1+hy} = B^{1+hy}\langle\beta\rangle^x$$

$$\langle\alpha\rangle^x \cdot A\, A^{hy} = \langle\beta\rangle^x \cdot B \cdot B^{hy}$$

But A^h and B^h are principal ideals.

Hence

$$\langle\alpha\rangle^x A^{hy} = \langle\gamma\rangle$$

and

$$\langle\beta\rangle^x B^{hy} = \langle\delta\rangle.$$

$$\langle\gamma\rangle A = \langle\delta\rangle B$$

$$\Rightarrow A \sim B.$$

Cyclotomic Field Kp :-

Let p be an odd prime. Then Eisenteins irreducibility criterian the polynomial

$$\varphi(x) = x^{p-1} + x^{p-2} + \cdots + 1.$$

is irreducable over R. Hence for any root 'ξ' of $\varphi(x)$ The field $R(\xi)$ is of degree $p-1$

$R(\xi)$ is call the Cyclotomic field. and it is denoted by K_p.

NOTE The zero's of

i) $\varphi(x) = x^{p-1} + x^{p-2} + \cdots + 1 = \frac{x^p - 1}{x - 1}$ are the pth root of unity

ii) Then Conjugates of ξ are $\xi_1, \xi_1^2, \xi_1^3, \cdots$

iii) $1, \xi, \xi^2, \cdots, \xi^{p-2}$ are basis of K_p.

//.

Theorem:- The Discriment of the Cyclotomic field. K_p is

$$(-1)^{\frac{p-1}{2}} \cdot p^{p-2}$$

Proof: Since $1, \xi_2, \xi_2^2, \ldots, \xi_2^{p-2}$ form integral Basis for K_p. Therefore descriment of the field is

$$\Delta(1, \xi_2, \xi_2^2, \ldots, \xi_2^{p-2}) = \begin{vmatrix} 1 & \xi_2 & \cdots & \xi_2^{p-2} \\ 1 & \xi_2^2 & & \xi_2^{2(p-2)} \\ \vdots & \vdots & & \\ 1 & \xi_2^{p-1} & \cdots & \xi_2^{(p-1)(p-2)} \end{vmatrix}^2$$

$$= \prod_{1 \leq i \leq j \leq p-1} \left(\xi_2^i - \xi_2^j\right)^2 \quad \text{———} (1)$$

Step-I

Since $\xi_2, \ldots, \xi_2^{p-1}$ are all the primitive pth roots of unity of

$\varphi(x) = x^{p-1} + x^{p-2} + \cdots + 1$. So we have.

$$\frac{x^{p-1}}{x-1} = x^{p-1} + \cdots + x + 1 = \prod_{i=1}^{p-1} (x - \xi^i) \quad (2)$$

Differentiating both sides

$$\frac{(x-1)px^{p-1} - (x^p - 1)}{(x-1)^2} = \sum_{j=1}^{p-1} \prod_{\substack{i=1 \\ i \neq j}}^{p-1} \left(x - \xi_2^i\right)$$

taking $x = \xi^{i}$ and noting

that
$$\frac{(\xi^{j}-1)\,p\,\xi^{j(p-1)} - (1-1)}{(\xi^{j}-1)^2} = \prod_{\substack{i=1\\ i\neq j}}^{p-1} (\xi^{j}-\xi^{i})$$

$$\frac{p\,\xi^{j(p-1)}}{(\xi^{j}-1)} = \prod_{\substack{i=1\\ i\neq j}}^{p-1} (\xi^{(j)}-\xi^{(i)}) \rightarrow (3)$$

Step II taking $x=0$ in eq. (2)

$$1 = \prod_{i=1}^{p-1} (-\xi^{i}) = (-1)^{p-1}\,\xi\cdot\xi^{2}$$

$$= \prod_{j=1}^{p-1} \xi^{p-j} \longrightarrow (4)$$

and taking $x=1$ in eqn (2)

$$p = \prod_{i=1}^{p-1} (1-\xi^{i}) \longrightarrow (5)$$

Now from (3) we have

$$\prod_{j=1}^{p-1}\left(\frac{-p\,\zeta_q^{p-j}}{1-\zeta_q^{j}}\right) = \prod_{j=1}^{p-1}\prod_{\substack{i=1\\(\neq)}}^{p-1}\left(\zeta_q^{j}-\zeta_q^{i}\right)$$

$$(-1)^{p-1}\,p^{p-1}\cdot\frac{\prod_{j=1}^{p-1}\zeta_q^{p-j}}{\prod_{j=1}^{p-1}\left(1-\zeta_q^{j}\right)} = \prod_{j=1}^{p-1}\prod_{\substack{i=1\\(\neq)}}^{p-1}\left(\zeta_q^{j}-\zeta_q^{i}\right).$$

using (4) & (5)

$$(-1)^{p-1}p^{p-1}\frac{1}{p} = \prod_{j=1}^{p-1}\prod_{\substack{i=1\\(\neq)}}^{p-1}\left(\zeta_q^{j}-\zeta_q^{i}\right)$$

$$(-1)^{p-1}\cdot p^{p-2} = \prod_{j=1}^{p-1}\cdot\prod_{\substack{i=1\\(\neq)}}^{p-1}\left(\zeta_q^{j}-\zeta_q^{i}\right)$$

In the final product $i<j$ for half factors and $j<i$ for other half factor. Then.

$(p-1)(p-2)$ factors in all

hence last product is

$$(-1)^{p-1}\cdot p^{p-2} = (-1)^{\frac{(p-1)(p-2)}{2}}\prod\left(\zeta^{i}-\zeta^{j}\right)^{2}$$

Since p is odd prime

So

$$(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-1}{2}}.$$

So that

$$\prod_{1 \le i < j \le p-1} \left(\xi^i - \xi^j\right)^2 = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$$

$$\Delta(1, \xi, \dots, \xi^{p-1}) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$$

To find Discriminant following steps to be observed.

(i) $\Delta(1, \xi, \xi^2, \dots, \xi^{p-2})$ Def.

ii) $f(x) = x^{p-1} + x^{p-2} + \dots + 1 = \frac{x^p - 1}{x - 1} = \pi(x - \xi^i)$

Differentiating

Put $x = \xi^i$ and $\xi^p = 1$ —

iii) taking $x = 0$ in Def —

taking $x = 1$ in def.

Def. —

Riemann ζ - Function:-

Let $s = \sigma + it$ be complex variable for $\sigma > 1$ The function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

is called Riemann ζ - function.

— α — α — α —

Pure Cubic field:-

The field $L = R(\sqrt[3]{d})$ in which $d > 1$ is a cubic free rational integer and $\sqrt[3]{d}$ is real is called pure cubic ~~root~~ field. d can be written $d = ab^2$.

Kummer's Lemma: Let p be a regular prime. Then if ε is unit of K_p and a is rational integer such that

$$\varepsilon \equiv a \pmod{p^p}$$

Then ε is the pth power of another unit of K_p.

Theorem. Show that Euler's function is multiplicative

i.e $\varphi(mn) = \varphi(m)\,\varphi(n)$ if $(m,n)=1$

Proof, let

$A = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$ be R.R.S (mod m).

&

$B = \{b_1, b_2, \ldots, b_{\varphi(n)}\}$ be R.R.S (mod n).

Consider the following set of $\varphi(m)\cdot\varphi(n)$ integers.

$C = \{a_i n + b_j m,\ i = 1,2,3,\ldots,\varphi(m),\ j = 1,2,3,\ldots,\varphi(n)\}$

we prove that ~~...~~ C . R.R.S (mod mn).

we note the following properties

a) $(a_i n + b_j m, mn)$

$= (a_i n + b_j m, m)\cdot(a_i n + b_j m, n)$

~~$= (a_i n, m)\cdot(b_j m, n)$~~

$= (a_i, m)\cdot(b_j, n) = 1$

bcs $(a_i, m) = 1$ & $(b_j, n) = 1$

Thus all the integers of C are prime mn.

b) If $a_i n + b_j m \equiv a_l n + b_k m \pmod{mn}$

$n(a_i - a_l) \equiv m(b_k - b_j) \pmod{mn}$

$\Rightarrow n(a_i - a_l) \equiv 0 \pmod m$

$n a_i \equiv n a_l \pmod n$.

$a_i \equiv a_l \pmod{m}$ and Similarly

$b_u \equiv b_j \pmod{n}$.

which is contradiction Hence

C is C.R.S.

c) let $a \in \mathbb{Z}$ such that $(a, mn) = 1$.

Since $(m, n) = 1$ we can find integer

$$mx + ny = 1$$

$$amx + any = a.$$

Now $(x, n) = 1$, $(y, m) = 1$ because of otherwise any common divisor divides a which would mean that $(a, m) \neq 1$

Therefore $(ax, n) = 1$, and $(ay, m) = 1$

& so there exist $a_i \in A$ & $b_j \in B$.

$$ax \equiv b_j \pmod{n}$$

&

$$ay \equiv a_i \pmod{m}.$$

or

$$ax - b_j = nq_1 \text{ and}$$

$$ay - a_i = mq_2.$$

for $q_1, q_2 \in \mathbb{Z}$. This substituting the values of ax & ay in eqn ① we get

$$a \equiv mb_j + na \pmod{mn}.$$

Hence a is congruent $\pmod{mn}$

$\Rightarrow C$ is C.R.S.

Hence it has $\varphi(mn)$ ele $\Rightarrow$ q.m.d —

Theorem if $(a,m)=1$ and $=$

$$a^{m-1} \equiv 1 \pmod{m}$$

&

$$a^{d} \not\equiv 1 \pmod{m} \text{ where}$$

d is divisor of m other than '$m-1$'

Proof: Suppose that m is Composite. Then

$$\varphi(m) < m-1$$

let

$$(\varphi(m), m-1) = d$$

Since $\Rightarrow x\varphi(m) + y(m-1) = d$.

$$0 < d < m-1$$

$\Rightarrow$ one of x, y is positive & other negative. Let us suppose that $x<0$ and $y>0$

Now

$$a^{|x|\varphi(m)} \equiv \left(a^{\varphi(m)}\right)^{|x|} \equiv 1 \pmod{m}$$

& ~~Therefore~~

$$a^{y(m-1)} = \left(a^{m-1}\right)^{y} \equiv 1 \pmod{m}$$

Therefore,

$$a^{d} \equiv a^{x\varphi(m) + y(m-1)}$$

$$= a^{|x|\varphi(m) + y(m-1) - 2|x|\varphi(m)}$$

$$= a^{2|x|\varphi(m)} \pmod{m}.$$