Algebraic Number Theory

[Handwritten Study Material]

[Part of advance study in Algebraic Number Theory]

✍

P. Kalika

PhD (NET(JRF), GATE, SET)

Email: maths.whisperer@gmail.com

No. of Pages: 51

Algebraic Number Theory

Integral domain: Basic Properties of Integral Domain, Units in ID, Properties of Units, Associates in Integral Domain, Divisibility in Integral Domain, Prime and Irreducible Elements in Integral Domain, GCD and HCF of two Elements in ID, Relation between Primes and Prime Ideals, Irreducible Element end Maximal Ideals, Noetherian Domain, PID,UFD, ED, Field Extensions, Finite extension, Algebraic and Transcendental Extension, Algebraic and Transcendental Number, algebraic integers, Algebraic Number Field, Ring of Integers in Algebraic Number Field, Ring of Gaussian Integers.

Bases: Bases and finite extensions, Properties of finite extensions, Conjugates and discriminants, The cyclotomic field.

Arithmetic in Algebraic Number Fields: Units and primes, Units in a quadratic field, the uniqueness of factorization, Ideals in an algebraic number field.

The Fundamental Theorem of Ideal Theory: Basic properties of ideals, the classical proof of the unique factorization theorem.

Consequences of the Fundamental Theorem: The highest common factor of two ideals, Unique factorization of integers, The problem of ramification, Congruences and norms, Further properties of norms

Next **Class-Numbers and Fermat's Problem:** Class numbers, The Fermat conjecture.

Texts/References

1 . Harry Pollard, Harold G. Diamond: The Theory of Algebraic Numbers, 3Ed, Dover,2010.
2. S. Alaca, K. S. Williams: Introductory Algebraic Number Theory, CUP, 2003.
3. E. Weiss: Algebraic Number Theory, Dover, 1998.
4. I. Stewart, D. Tall: Algebraic Number Theory and Fermat's Last Theorem, 3rd edition, A K Peters/CRC Press, 2001 .
5. G.J. Janusz: Algebraic Number Fields, 2nd edition, 1996.

(3)

Topics covered

By :- P. Kalika
Research Scholar
Dept. of Mathematics

- Rings
- Operations in Rings
- Units & Non-Units
- Zero divisor
- Non-zero divisor
- Nilpotent elt.
- Reducible / Irreducible elt.
- Prime element
- UFD

→ In $\mathbb{Z}$, Prime elts & irreducible elements are same, because $\mathbb{Z}$ is an UFD.

Que(1) $\boxed{\text{Check, 2 is irreducible in } \mathbb{Z}[\sqrt{-5}]}$

sol^n : Here, ∵ 2 is non-unit & non-zero

Now, to check inverse of 2 exist or not.
So, we have

$$2 \times (a + b\sqrt{-5}) = 1 \quad \text{where } a, b \in \mathbb{Z}$$

$$\Rightarrow 2a + 2b\sqrt{-5} = 1 = 1.1 + 0.\sqrt{-5}$$

on comparing $2a = 1$ & $2b = 0$

$$\Rightarrow a = 1/2 \text{ and } b = 0$$

So, clearly $1/2 \notin \mathbb{Z}$ ⇒ 2 is non-unit.

So, 2 is ~~irreducible~~ n.z, n.u.

4

Another way

Let $2 = (a+b\sqrt{-5})(x+y\sqrt{-5})$, $a, b, x, y \in \mathbb{Z}$

$\because$ Norm $\rightarrow$ products of conjugates
Trace $\rightarrow$ sum of conjugates

$\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{Q}(\sqrt{-5})$ $\xrightarrow{\sigma_1}$ $\sqrt{-5}$, $\xrightarrow{\sigma_2}$ $-\sqrt{-5}$

$\sigma_1(x+y\sqrt{-5}) = x+y\sqrt{-5}$

$\sigma_2(x+y\sqrt{-5}) = x-y\sqrt{-5}$

Now taking conjugates on both sides —

$$2.2 = (a+b\sqrt{-5})(a-b\sqrt{-5})(x+y\sqrt{-5})(x-y\sqrt{-5})$$

$$4 = (a^2+5b^2)(x^2+5y^2)$$

$\because$ 4 can be written as $4 = 1 \times 4$
2×2
4×1

Case-I $4 = 1 \times 4$

In this case, $a+b\sqrt{-5} = 1$ which then becomes unit. So, 2 is irreducible.

Case-II $4 = 2 \times 2$. $x^2+5y^2 = 2$

If $y=1$, & $x=0$, then eq^n doesn't holds

If $y=0$ & $x \neq 0$, then also. eq^n doesn't hold

i.e $\nexists$ $x, y \in \mathbb{Z}$ s.t $x^2+5y^2=2$ holds

thus case-II, doesn't exist.

Case-III $4 = 4 \times 1$

In this case $(x+y\sqrt{-5}) = 1$, which is a unit.

(5)

So, 2 is irreducible.

So. only two cases exist i.e $4 = 1 \times 4$
$4 = 4 \times 1$

So, 2 is irreducible.

---

* In $\mathbb{Z}[\sqrt{-5}]$ (To show, NOT UFD we proceed like this)

$2 \times 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$

so, 6 can be expressed in two ways

So, $\mathbb{Z}[\sqrt{-5}]$ is NOT UFD

NET (v.v.)

NB! $\mathbb{Z}[\sqrt{-d}]$ is UFD $\Leftrightarrow$ $d = 1$ or 2

\#

$\alpha \in \mathbb{Q}\sqrt[3]{2}$ $\xrightarrow{\sigma_1} \sqrt[3]{2}$, $\xrightarrow{\sigma_2} \sqrt[3]{2}\omega$, $\xrightarrow{\sigma_3} \sqrt[3]{2}\omega^2$, ω is cube root of unity

Norm - $N(\alpha) = \sigma_1(\alpha) * \sigma_2(\alpha) * \sigma_3(\alpha)$

Trace - $Tr(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha)$.

G: region (open & Connected subset of $\mathbb{C}$).

$H(G) = \{f \mid f: G \to \mathbb{C}$ analytic$\}$

Now, let $f, g \in H(G)$, then

$(f+g)(z) = f(z) + g(z) = g(z) + f(z) = (g+f)(z)$

$(f*g)(z) = f(z)\, g(z) = g(z) f(z) = (g*f)(z)$

$f(z) = u + iv$, $\left.\begin{array}{l} u_x = v_y \\ v_x = -u_y \end{array}\right\}$ Cauchy Riemann eq^n.

(If at least one of them is cts, then analytic)

$H(G)$ is commutative ring.

Rings

Definition : Suppose R is a n-e set equipped with two binary operations called add^n & mult^n & denoted by '+' and '.' respectively.
i-e $\forall a, b \in R$, we have $a+b \in R$ and $a.b \in R$.
Then this algebraic str. $(R,+,\cdot)$ is called Ring, if following properties are satisfied —

(i). Add^n is associative i-e
$$a+(b+c) = (a+b)+c \quad \forall a,b,c \in R.$$

(ii). Add^n is Commutative i-e
$$a+b = b+a \quad \forall a,b \in R$$

(iii). Is an elt., denoted by 0 in R s.t
$$0+a = a \quad \forall a \in R.$$

(iv). To each elt. in R, Is an elt. a in R s.t
$$a+(-a) = 0$$

(v). Multiplication is Associative i.e
$$a.(b.c) = (a.b).c \quad \forall a,b \in R.$$

(vi). Multiplication is distributive w.r.t add^n.
$\forall a,b,c \in R$
$$a.(b+c) = a.b + a.c \leftarrow \text{Left distributive law}$$
$$(b+c).a = ba + c.a \leftarrow \text{Right distributive law}$$

Here, R will be an abelian grp. under addition, the element $0 \in R$, will be the additive identity. It is called the zero elt. of the ring.

Operations in Rings

(7)

Two operations in rings —
(i). Modulo addition.
(ii). Modulo multiplication.

General operations $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, 3, \ldots, p-1\}$

$$(a + p\mathbb{Z}) + (b + p\mathbb{Z}) = (a+b) + p\mathbb{Z}$$
$$(a + p\mathbb{Z}) \cdot (b + p\mathbb{Z}) = ab + p\mathbb{Z}$$

2. Units

An elt. $a \overset{\neq 0}{\in} A$ (CRU) is called a unit if $\exists$ $b \in A$ s.t $ab = ba = I$

Comm. Ring : Ring + Commutative w.r.t mult^n.

CRU : Com. Ring + existence of Id. w.r.t. mult^n

Non-Units : An elt $a \in A$, which is not an unit, (means $\nexists$ an $b \in A$ s.t $ab = ba = I$)

Zero-divisor: A n.z elt. $a \in A$ is called zero divisor if $\exists$ $b\,(\neq 0) \in A$ s.t $ab = 0$

ie of $a \cdot b = 0 \nRightarrow a \neq 0,\ b \neq 0$

Nilpotent : An elt. $a(\neq 0) \in A$ is called Nilpotent elt. if $\exists$ $n \in \mathbb{Z}^+$ s.t $\boxed{a^n = 0}$

Remarks: Every nilpotent elt. is a zero divisor But not vice versa.

example: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Now $\bar{2} \times \bar{3} = \bar{6} = 0$ But $2 \neq 0, 3 \neq 0$

Also, but $\nexists\, n \in \mathbb{N}$ s.t $2^n = 0$

so, $\bar{2}$ is zero divisor but not nilpotent.

Irreducible

A n.z, non-unit elt. $x \in A$ is called ~~irredu~~ irreducible if whenever $x = ab$ for $a, b \in A$ then either a is a unit or b is a unit.

Que: Calculate the irreducibles, units and zero-divisors in $\mathbb{Z}/20\mathbb{Z}$

Sol^n :- $\because \mathbb{Z}/20\mathbb{Z} = \mathbb{Z}_{20} = \{0, 1, 2, \ldots, 19\}$ - Ring

$\because$ Invertible elt.s $= \{1, 3, 7, 9, 11, 13, 17, 19\}$ w.r.t multi^n.

$\therefore$ Units of $\mathbb{Z}_{20} = \{1, 3, 7, 9, 13, 17, 19\}$

Now,
$$2 = 1 \times 2 = 2 \times 1$$
1 is a unit.
So, 2 is irreducible

$$4 = 1 \times 4 \checkmark$$
$$= 2 \times 2 \times$$
$$= 4 \times 1 \checkmark$$
But, 2 is a non-unit
So, 4 is reducible.

Prime element (If A is CRU & $x \in A$ is n.z, non-unit)

An elt. $x (\neq 0) \in A$ is called Prime element if whenever $x | ab$ for $a, b \in A$ either $x | a$ or $x | b$

NB: In $\mathbb{Z}$, All prime elt.s & irreducible elt.s are same because $\mathbb{Z}$ is UFD.

(9)

$\boxed{\text{Integral Domain}}$ A ring is called an integral domain, if it is commutative.

(i). has unit elt. &

(ii). without zero divisor.

i-e A ring (CRU) without zero divisor is ID.

Unique Factorization Domain (UFD)

A unique factorization domain is an ID R in which every n.z elt. can be written as a product of a finite no. of irreducible ~~prime~~ elts of R.

Prime element:

An elt. p of a C.R (Comm. Ring) R is s.t.b prime if it is not zero or a unit & whenever p divides ab for some a & b in R, then

$p | a$ or $p | b$.

Algebraic Numbers

A: set of algebraic no.

$$= \{\alpha \in \mathbb{C} : \exists\, 0 \neq p(x) \in \underset{\text{Poly. Rings}}{\mathbb{Q}[x]} \text{ s.t } p(\alpha) = 0\}$$

1. Whether A is a ring (Comm.) ?
2. Whether A is a field ?
3. Whether $[A : \mathbb{Q}] < \infty$?

$\because \mathbb{Q}(\sqrt[3]{2}) \subseteq A$ (True) (taking in particular $a + b\sqrt[3]{2}$, $a = 1, b = 1$)

$\because 1 + \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$

Let $x = 1 + \sqrt[3]{2} \Rightarrow x - 1 = \sqrt[3]{2}$

(10).

$\Rightarrow (x-1)^3 = 2$

$\Rightarrow (x-1)^3 - 2 = 0$

$\Rightarrow x^3 - 1 - 3x^2 + 3x - 2 = 0$

$\Rightarrow x^3 - 3x^2 + 3x - 3 = 0$

$1 + \sqrt[3]{2}$ satisfies the poly. $(x-1)^3 = 2$

So, $(x-1)^3 - 2 \in Q[x]$. So, $Q(\sqrt[3]{2}) \subseteq A$

General elt. of $Q(\sqrt[3]{2})$ are $a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$
here $a_0, a_1, a_2 \in Q$

Degree of $[Q(\sqrt[3]{2}) : Q]$

$\because$ Basis of $Q(\sqrt[3]{2})$ over $Q = \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$

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

$\because (\sqrt[3]{2})^3 = 2 \cdot 1 + 0 \cdot \sqrt[3]{2} + 0(\sqrt[3]{2})^2$

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

this holds only for algebraic no.s.

Here, $\sqrt[3]{2}$ is algebraic numbers,

So, $Q[\sqrt[3]{2}]$ is field

$\Rightarrow Q[\sqrt[3]{2}]$ is ring.

$\left(\because \frac{1}{\sqrt[3]{2}} \in Q[\sqrt[3]{2}]\right)$

For non-algebraic ($\pi, e, \ldots$ etc).

$Q(\pi) = Q[\pi]$ not possible

$\because$ clearly $\frac{1}{\pi} \in Q(\pi)$ $\left[\begin{array}{l}\because 1 \text{ is a constant poly.} \\ \text{and } \pi \text{ is also a poly.} \\ \text{and } \pi \neq 0\end{array}\right.$

So, $1/\pi \in Q(\pi)$

(11)

Now, if possible assume that $Q(\pi) = Q[\pi]$

then $\frac{1}{\pi} = P(\pi) \Rightarrow 1 = \pi P(\pi)$

Now, we get a poly,

$q(x) = x P(x) - 1$ for which $q(\pi) = 0$ → ⟵ as π is transcen-dental no.

So, $Q(\pi) \neq Q[\pi]$

Note :-

$Q[x]$ = Poly. ring.

$Q[x] = \{ P(x) = a_0 + a_1 x + \dots + a_n x^n : a_0, a_1, \dots a_n \in Q, n \in \mathbb{Z}^+ \cup \{0\} \}$

$Q(x) = \left\{ \frac{P(x)}{q(x)} : P(x), q(x) \in Q[x], q(x) \neq 0 \right\}$

is field

field of fractions and if $Q[x] = Q(x)$

then $Q[x]$ becomes field.

Que $\alpha = \frac{\sqrt{3}}{2}$,

Let $x = \frac{\sqrt{3}}{2} \Rightarrow 2x = \sqrt{3} \Rightarrow 4x^2 - 3 = 0$

$4x^2 - 3 \leftarrow$ Poly. with integer coeff.

$x^2 - 3/4 \leftarrow$ Poly. with rational Co.eff.

$\because \alpha = \frac{\sqrt{3}}{2}$ satisfies poly. with integer co.eff.s & poly. with rational co.efficients, but doesn't satisfy monic poly. over $\mathbb{Z}$. (So α is alg. no. but NOT alg. integer)

* A is a field

$\because$ A is field, so it is ring also,

$B_{\mathbb{C}} = \{ \alpha \in \mathbb{C} : \exists\, P(x) \in \mathbb{Z}[x]$ monic s.t $P(\alpha) = 0 \}$

Now, $B_{\mathbb{Q}} = \{ \alpha \in \mathbb{Q} : \exists\, P(x) \in \mathbb{Z}[x]$ monic s.t $P(\alpha) = 0 \}$

Pf: Let $\alpha = p/q$, $a_0 + a_1 x + \cdots + a_n x^n$, $a_0, a_1, \ldots a_n \in \mathbb{Z}$

So, $a_0 + a_1 (p/q) + \cdots + a_n (p/q)^n = 0$

$\Rightarrow \underbrace{q^n a_0 + a_1 p q^{n-1} + \cdots + a_{n-1} p^{n-1} q}_{} + a_n p^n = 0$

q divides this part (bcz q divides every elt) also $q \mid 0$

$\Rightarrow q \mid a_n$. and poly. is monic. so $a_n = 1$

$\Rightarrow \underline{q = \pm 1}$

$\Rightarrow \alpha = p/q \Rightarrow \alpha = \pm p$ which is an integer.

Associates

> Two elt. x and y are s.t.b an associates of each other if $\exists$ an elt. u s.t $y = ux$

unit

It is an equivalence relⁿ.

eg. 2 and -2 are associate as $-2 = (-1) \times 2$

Defⁿ:

> Let R be a Ring. Let x & y be two elts of R. Then x & y are associate of each other if $\exists$ an unit $u \in R$ s.t $y = ux$

(13)

Equivalence Rel^n

Reflexive: $a \sim a$, then $\exists$ a unit $u \in A$ s.t $a = ua$

So, Associates is an eq. Rel^n. Reflexive Rel^n

Symmetry: $a \sim b \Rightarrow \exists$ a unit $u \in A$ s.t $b = ua$

$\Rightarrow u^{-1}b = (u^{-1}u)a = a$

$\Rightarrow b \sim a$

Transitive

$a \sim b,\ b \sim c \Rightarrow \exists\ u \,\&\, v \in A$ s.t $b = ua$ & $c = v.b$

(Product of two unit is unit)

$\Rightarrow c = v(ua) = (vu)a = k.a$

$\Rightarrow c \sim a$

$\left[\because (uv)^{-1} = v^{-1}u^{-1},\ \because u^{-1}, v^{-1} \in A \text{ as } u \,\&\, v \text{ are unit} \right.$

$\left. \Rightarrow v^{-1}u^{-1} \in A \text{ (closure prop.)} \right]$

Equivalence class of associate

For, $a \in A$, the equivalence class

$[a] = \{ua : u \in A \text{ is a unit}\}$

Example $\mathbb{Z}$ $\quad$ ($\because$ units of $\mathbb{Z}$ are $1 \,\&\, -1$)

$[2] = \{2, -2\}$

$[0] = \{0\}$

$[1] = \{1, -1\}$

$\vdots$

H.W. $\frac{1}{\sqrt[3]{2}} = \frac{(\sqrt[3]{2})^2}{2} = \frac{1}{2}(\sqrt[3]{2})^2 = 0.1 + 0\sqrt[3]{2} + \frac{1}{2}(\sqrt[3]{2})^2$

* $A = \{\alpha \in \mathbb{C} : \exists\ p(x)(\neq 0) \in \mathbb{Q}[x] \text{ s.t } p(\alpha) = 0\}$

Prove that A is ring also field.

let $0 \neq \alpha, \beta \in A$

then if we show $\underbrace{\alpha+\beta,\ \alpha\beta}_{\text{Ring}}, \frac{1}{\alpha} \in A$, then A is ~~ring~~ field

$$\begin{tikzcd} \mathbb{Q}(\alpha,\beta) \subseteq A \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]}_{\deg(\text{irred}(\beta,\mathbb{Q}(\alpha)))}\underbrace{[\mathbb{Q}(\alpha):\mathbb{Q}]}_{\deg(\text{irred}(\alpha,\mathbb{Q}))}$$

$\because \alpha, \beta$ are algebraic no.

So, $[\mathbb{Q}(\alpha,\beta), \mathbb{Q}] < \infty$, so $\mathbb{Q}(\alpha,\beta)$ is algebraic as degree of extension is finite.

So; $\mathbb{Q}(\alpha,\beta) \subseteq A$ ← collection of alg. no.

So, $\mathbb{Q}(\alpha,\beta)$ is a field. (If $\alpha \in A$, then $\mathbb{Q}(\alpha)$ is field)

thus, $\alpha+\beta,\ \alpha\cdot\beta,\ 1/\alpha \in \mathbb{Q}(\alpha,\beta) \subseteq A$

$\Rightarrow \alpha+\beta,\ \alpha\cdot\beta,\ 1/\alpha \in A$

Also, $\because$ A is ring $\Rightarrow$ A is field.

Que

$$\begin{tikzcd} \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

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

So $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$

As

$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]$. ← finite

$\times [\mathbb{Q}(\alpha):\mathbb{Q}]$ ← finite

$= 2 \times 2 = 4$

and every finite extension is Algebraic.

So, $\mathbb{Q}(\alpha,\beta) \subseteq A$ & $\mathbb{Q}(\alpha,\beta)$ is a field.

So, $\alpha+\beta, \alpha\beta, 1/\alpha \in \mathbb{Q}(\alpha,\beta)$, clearly $\underbrace{\alpha+\beta,\ \alpha\beta}_{\text{for ring}},\ \underbrace{1/\alpha}_{\text{for field}} \in A$

So, A is ring & is field.

A : Set of algebraic no.s
A : field extension of $\mathbb{Q}$

$$\begin{tikzcd} B = \mathcal{O}_A \arrow[r, hook] \arrow[d, no head] & A \arrow[d, no head] \\ \mathbb{Z} \arrow[r, hook] & \mathbb{Q} \end{tikzcd}$$

Def^n : $\mathcal{O}_K$

If $K \supseteq \mathbb{Q}$ is field extension then define

$$\mathcal{O}_K = \{\alpha \in K : \exists\ p(x) \in \mathbb{Z}[x] \text{ monic with } p(\alpha) = 0\}$$
= Ring of integers

example $\mathbb{Q} \supseteq \mathbb{Q}$

$$\mathcal{O}_{\mathbb{Q}} = \{\tfrac{p}{q} \in \mathbb{Q} : \exists\ p(x) \in \mathbb{Z}[x] \text{ monic with } p(\tfrac{p}{q}) = 0\}$$
$$= \{\pm p : p \in \mathbb{Z}\} = \mathbb{Z}$$
($\because$ units of $\mathbb{Z} = \{-1, 1\}$ look at p-12)

→ **Algebraic integers ($\mathcal{O}_K$)** ← collection of alg. integ. or

A complex no. α is called an **algebraic integer** if $\exists$ monic $f(x) \in \mathbb{Z}[x]$ s.t $f(\alpha) = 0$

eg: $\alpha = 2, 3, 4, 5, \ldots, i, \sqrt{2}, \sqrt{2}i, 1+i \ldots$ etc.

for $\alpha = 2$

$\exists$ at least one poly. $(x-2)$ which is monic

* Eg. of no.s for which, we can't get any monic poly. over $\mathbb{Z}$.

→ $1/2$ can't satisfy any monic poly. over $\mathbb{Z}$

Result

denominator must divide the highest co-eff but $2 \nmid 1$
so, it can't satisfy monic poly.

$\mathbb{Z} \subseteq \mathbb{Q}$ but $\mathbb{Z}$ is not a field, $\mathbb{Z}$ has ring structure.

<u>Que</u> $\boxed{\text{Does } B \text{ also have field or ring structure ?}}$

$\because$ $\underset{\text{alg. integ.}}{\text{Set of}} = B \subseteq A = \underset{\text{alg. No.s}}{\text{set of}}$

$A \to \mathbb{Q}$ Always not a finite ext^n.

$\because O_A \subseteq A \subseteq \mathbb{C}$ $\therefore$ so $O_A \subseteq \mathbb{C}$

let $\alpha, \beta \in O_A$. For ring we have to prove that
$\alpha+\beta \in O_A$ & $\alpha\beta \in O_A$

- O_A is not a field as $2 \in O_A$ but $\frac{1}{2} \notin O_A$.

<u>Number field</u> :- A finite field ext^n of $\mathbb{Q}$ is called a no. field.

<u>example</u>: $\boxed{K = \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}}$

$\because [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so it is a no. field.

$\because O_K = O_{\mathbb{Q}(\sqrt{2})} = \{\alpha \in \mathbb{Q}(\sqrt{2}) : \exists\, p(x) \in \mathbb{Z}[x] \text{ monic with } p(\alpha) = 0\}$

$\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$

<u>Observation</u> :-
If $\alpha \in \mathbb{C}$ is an algebraic integer, then $\underline{\text{irred}(\alpha, \mathbb{Q})}$ (irred. poly. of α in $\mathbb{Q}$) is also monic over $\mathbb{Z}$.

<u>OR</u>, If $\alpha \in \mathbb{C}$ is an algebraic integer then $\underline{\text{irred}(\alpha, \mathbb{Z})}$ is also monic.

Pf :-

Pf:- As α is an algebraic integer, so $\exists$ $f(x) \in \mathbb{Z}[x]$ monic s.t $f(\alpha) = 0$.

Let $p(x) = \text{irred}(\alpha; \mathbb{Q})$ ←

then $p(x) \mid f(x)$ [bcz irreducible poly. is also a minimal poly. so, it divides $f(x)$]

$\Rightarrow \underbrace{f(x)}_{\substack{\downarrow \\ f(x) \text{ is primitive}}} = p(x) \cdot q(x)$ for some $q(x) \in \mathbb{Q}$

$= \left(\frac{1}{cd}\right) p'(x) \, q'(x)$, $p'(x), q'(x) \in \mathbb{Z}[x]$

Gauss-lemma

If $f(x) \in \mathbb{Z}[x]$, then it can be factored as a product of primitive poly.

As, By Gauss-lemma,

$f(x) = g(x) \, h(x)$, $g(x)$ & $h(x)$ are monic

If $g(x)$ is not irreducible then, it can further be factored to monic poly.s. $(g(x) = g_1(x) \cdot h_1(x))$

$\Rightarrow f(x) = g_1(x) \cdot h_1(x)$ [$g_1(x)$ is the $\text{irred}(\alpha, \mathbb{Q})$, $h_1(x)$ is remaining poly.]

$\Rightarrow p(x) = g_1(x) \in \underset{\text{monic}}{\mathbb{Z}[x]}$ Hence $\text{irred}(\alpha, \mathbb{Z})$ is monic.

Find the O_K ?

$$\text{irred}((a+b\sqrt{2}) : \mathbb{Q}) = \begin{cases} x - a & : \text{if } b = 0 \\ x^2 - 2ax + a^2 - 2b^2 & : \text{o.w} \end{cases}$$

(18)

If $b=0$, then $\text{irred}((a+b\sqrt{2}):Q) = x-a \in \mathbb{Z}[x]$
$\Rightarrow a \in \mathbb{Z}$. $\Rightarrow \alpha = a \in \mathbb{Z}$

and if $b \neq 0$

$\left(\begin{array}{l} x = a+b\sqrt{2} \\ \Rightarrow (x-a)^2 = b^2 \cdot 2 \\ \Rightarrow x^2-2ax+a^2-2b^2=0 \end{array} \right)$

$x^2-2ax+a^2-2b^2 \in \mathbb{Z}[x]$

$\Rightarrow -2a \in \mathbb{Z} \Rightarrow a \in \mathbb{Z}$ $(\because 2,-2 \in \mathbb{Z})$

also, $a^2-2b^2 \in \mathbb{Z}$ $\quad [\because a \in \mathbb{Z} \Rightarrow a^2 \in \mathbb{Z}]$

$\Rightarrow -2b^2 \in \mathbb{Z} + a^2$ $\quad \Rightarrow \mathbb{Z}+a^2 \in \mathbb{Z}$

$\Rightarrow -2b^2 \in \mathbb{Z}$ $\quad (\because -2 \in \mathbb{Z})$

$\Rightarrow b^2 \in \mathbb{Z}$

$\Rightarrow b \in \mathbb{Z}$

H.W. 30/7/18

Que $\left(K = Q(\sqrt{2}) = Q[\sqrt{2}] \right)$ $Q(\alpha) = Q[\alpha]$

$(\mathbb{Z} \subseteq O_K)$

Sol^n $O_K = \{ \alpha \in K : \exists\, p(x) \in \mathbb{Z}[x] \text{ monic s.t. } p(\alpha)=0 \}$

$\Downarrow$

$a+b\sqrt{2}$, $a,b \in Q$

Now, $\text{irred}((a+b\sqrt{2}):Q) = \begin{cases} x-a & : b=0 \\ x^2-2ax+a^2-2b^2 & : b \neq 0 \end{cases}$

Case-I, $b=0$

$\text{irred}(a+b\sqrt{2}) = x-a \in \mathbb{Z}[x] \Rightarrow \alpha = a \in \mathbb{Z}$

Case-II, $b \neq 0$

$\text{irred}(a+b\sqrt{2}) = x^2-2ax+a^2-2b^2$ if $b \neq 0$

$\Rightarrow -2a \in \mathbb{Z} \Rightarrow 2a \in \mathbb{Z}$

let $2a = p$ for some $p \in \mathbb{Z}$

$\Rightarrow a = p/2$

Next, let $b = r/s$, $r,s \in \mathbb{Z}$

(19)

then $a^2 - 2b^2 = \left(\frac{p}{2}\right)^2 - 2\left(\frac{r}{s}\right)^2 \in \mathbb{Z}$

$= \frac{p^2}{4} - \frac{2r^2}{s^2} = \frac{p^2s^2 - 8r^2}{4s^2} \in \mathbb{Z}$

$\Rightarrow 4s^2 \mid p^2s^2 - 8r^2$ —— (*)

$\Rightarrow$ (If ~~$s^2 \nmid (p^2s^2 - 8r^2)$~~ $\Rightarrow 4 \mid (p^2s^2 - 8r^2)$)

$\Rightarrow 4 \mid p^2s^2 \Rightarrow 2 \mid p$ or $2 \mid s$

Subcase-I, if $2 \mid p \Rightarrow p/2 = a \in \mathbb{Z} \Rightarrow a^2 \in \mathbb{Z}$

$\Rightarrow a^2 - 2b^2 \in \mathbb{Z} \Rightarrow 2b^2 \in \mathbb{Z}$

$\Rightarrow 2\left(\frac{r}{s}\right)^2 \in \mathbb{Z} \Rightarrow s = \pm 1$ (r^2 should be divisible by s^2)

$\Rightarrow b = r \in \mathbb{Z}$

$\therefore \alpha = a + b\sqrt{2} = a + (\pm r)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

Subcase-II. If $2 \nmid p \Rightarrow 2 \mid s$?? $\Rightarrow s = 2s'$, $s' \in \mathbb{Z}$

$\therefore a^2 - 2b^2 = \frac{p^2}{4} - \frac{2r^2}{4s'^2} = \cancel{\frac{p^2s'^2 - 2r^2}{4s'^2}} \in \mathbb{Z}$

$= \frac{p^2}{4} - \frac{2r^2}{s^2} \in \mathbb{Z}$

$\Rightarrow 4s^2 \mid p^2s^2 - 8r^2$ —— (*) (If $p/ab \in \mathbb{Z} \Rightarrow p = kab$)

$\Rightarrow s^2 \mid p^2s^2 - 8r^2$ (from (*))

$\Rightarrow s^2 \mid 8r^2 \Rightarrow 4s'^2 \mid 8r^2$ ($s = 2s'$)

$\Rightarrow s'^2 \mid 2r^2$

$\therefore$ ~~s is rel~~ $(s, r) = 1 \Rightarrow (s', r) = 1$

$\Rightarrow s'^2 \mid 2 \Rightarrow s' = \pm 1$

$\Rightarrow s = \pm 2 \in \mathbb{Z}$

20

$\Rightarrow s = \pm 2 \in \mathbb{Z}$ $\qquad \left(a = p/2,\ b = r/s \right)$

As $\frac{p^2}{4} - \frac{2r^2}{4} \in \mathbb{Z}$ — $(*')$

$\Rightarrow 2 \mid p \Rightarrow a \in \mathbb{Z}$ $(\because a = p/2)$ $\qquad (\because 4 \mid p^2 \Rightarrow 2 \mid p^2 \Rightarrow 2 \mid p)$

$\Rightarrow p = 2k$ for some $k \in \mathbb{Z}$

$\Rightarrow \frac{4k^2}{4} - \frac{2r^2}{4} \in \mathbb{Z}$ (by $*'$)

$\Rightarrow \frac{r^2}{2} \in \mathbb{Z}$ $\qquad$ (As $k \in \mathbb{Z} \Rightarrow k^2 \in \mathbb{Z}$)

$\Rightarrow 2 \mid r$

$\Rightarrow b \in \mathbb{Z}$ $\qquad (\because b = r/s = \frac{r}{\pm 2} = \pm k \in \mathbb{Z})$

$\Rightarrow a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

$\boxed{\text{How to show } \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]}$ H.W

Que. let $K = \mathbb{Q}[\sqrt{3}]$ $\qquad$ (Q^n To show $\underset{\text{poly. Ring}}{\mathbb{Q}[\sqrt{3}]} = \underset{\text{field}}{\mathbb{Q}(\sqrt{3})}$)

H.W Show that $O_K = \mathbb{Z}[\sqrt{3}]$ = Ring of integers of $\mathbb{Q}(\sqrt{3})$

$\because O_K = \{ \alpha \in K : \exists\ p(x) \in \mathbb{Z}[x] \text{ monic s.t } p(\alpha) = 0 \}$
$= \mathbb{Z}[\sqrt{3}]$

$\because \alpha \in K = \mathbb{Q}[\sqrt{3}]$ so $\alpha = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$

(We show here ~~$\mathbb{Q}[\sqrt{3}]$~~ $O_K \subseteq \mathbb{Z}[\sqrt{3}]$)

$\therefore$ min. poly. $=$ irred$(a + b\sqrt{3}) = \begin{cases} x - a & \text{if } b = 0 \\ x^2 - 2ax + a^2 - 3b^2 & : \text{if } b \neq 0 \end{cases}$

- $\mathbb{Z} \hookrightarrow O_K$ (In general true)

As. $2a \in \mathbb{Z}$, let $2a = p$ for some $p \in \mathbb{Z} \Rightarrow a = p/2$

& $a^2 - 3b^2 \in \mathbb{Z}$, let $b = r/s$, $r, s \in \mathbb{Z}$, $(r, s) = 1$

$\therefore a^2 - 3b^2 = \frac{p^2}{4} - \frac{3r^2}{s^2} = \frac{p^2s^2 - 3 \cdot 4r^2}{4s^2} \in \mathbb{Z}$

$\Rightarrow 4s^2 \mid (p^2s^2 - 12r^2)$

$\because 4 \mid p^2s^2 - 12r^2$

$\because 4 \mid 12r^2 \Rightarrow 4 \mid p^2s^2 \Rightarrow 2 \mid p$ or $2 \mid s$

<u>Case-I</u>, If $2 \mid p$, then $a = p/2 \in \mathbb{Z}$

$a^2 - 3b^2 \in \mathbb{Z} \Rightarrow 3b^2 \in \mathbb{Z}$

$\Rightarrow 3 \cdot \left(\frac{r}{s}\right)^2 = \frac{3r^2}{s^2} \in \mathbb{Z} \Leftrightarrow s = \pm 1$ (bcz $(r,s) = 1$)

$\therefore b = \frac{r}{s} = \pm r$

$\therefore a + b\sqrt{3} = a + (\pm r)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

<u>Case-II</u>, If $2 \nmid p \Rightarrow 2 \mid s$

$\Rightarrow s = 2s'$ for some $s' \in \mathbb{Z}$

$\therefore \frac{p^2}{4} - \frac{3r^2}{(2s')^2} = \frac{p^2}{4} - \frac{3r^2}{4s'^2} = \frac{p^2s'^2 - 3r^2}{4s'^2} \in \mathbb{Z}$

$\Rightarrow 4s'^2 \mid p's'^2 - 3r^2$ — (A)

$\Rightarrow s'^2 \mid p's'^2 - 3r^2$ ($\because s'^2 \mid 4s'^2$)

$\Rightarrow s'^2 \mid 3r^2$

$\because (s, r) = 1 \Rightarrow (2s', r) = 1$ & $(s', r) = 1$

& $s'^2 \mid 3 \Rightarrow s'^2 = 1 \Rightarrow \boxed{s' = \pm 1}$

$\Rightarrow \underline{s = 2s' = \pm 2}$

Thus $\frac{p^2}{4} - \frac{3r^2}{4} = \frac{p^2 - 3r^2}{4} \in \mathbb{Z}$

$\Rightarrow 4 \mid p^2 - 3r^2 \Rightarrow 2 \mid p^2 - 3r^2 \Rightarrow 2 \nmid p^2$ & $2 \nmid r^2$

$\Rightarrow 2 \nmid p$ & $2 \nmid r \Rightarrow p = 2k_1$ & $r = 2k_2$, $k_1, k_2 \in \mathbb{Z}$

$$= \left(\frac{p^2}{4} - \frac{3r^2}{4} = \frac{(2k_1)^2}{4} - \frac{3\cdot(2k_2)^2}{4} \quad . \quad k_1, k_2 \in \mathbb{Z} \right.$$

$$\left. = k_1^2 - 3k_2^2 \in \mathbb{Z} \quad , \quad b(2\ k_1, k_2 \in \mathbb{Z} \right)$$

$$\therefore b = \frac{r}{s} = \frac{2k_2}{\pm 2} = \pm k_2 \in \mathbb{Z}$$

$$\Rightarrow b \in \mathbb{Z}$$

$$\Rightarrow a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

HW

$\mathbb{Q}(\sqrt{3}i)$ (or $\mathbb{Q}(\sqrt{-3})$)

$\boxed{\begin{array}{c} K = \mathbb{Q}(\sqrt{3}i) \\ \text{To show } O_K = K \end{array}}$

$\alpha \in \mathbb{Q}(\sqrt{3}i)$. $\alpha = a + ib\sqrt{3}$

If $b = 0$, $x - a$ is the irreducible poly.

Again $x = a + bi\sqrt{3}$

$$\Rightarrow (x-a)^2 = (ib\sqrt{3})^2 = -3b^2$$

$$\Rightarrow x^2 - 2ax + a^2 + 3b^2 = 0 \quad \left(\text{or } x^2 - (\alpha+\beta)x + \alpha\beta = 0 \right)$$

$$\therefore \phi(x) = x^2 - 2ax + a^2 + 3b^2$$

$$\therefore \text{irred.}(\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}) = \begin{cases} x - a & \text{if } b \neq 0 \\ x^2 - 2ax + a^2 + 3b^2 & \text{if } b \neq 0 \end{cases}$$

Case-I If $b = 0$

$$\text{irred}(\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}) = x - a \in \mathbb{Z}[x]$$

$$\alpha = a \in \mathbb{Z}$$

Case-2 If $b \neq 0$

$$\text{irred}\,(\mathbb{Q}(\sqrt{3}i) ; \mathbb{Q}) = x^2 - 2ax + (a^2 + 3b^2)$$

where $-2a \in \mathbb{Z}$ & $(a^2+3b^2) \in \mathbb{Z}$

$2a \in \mathbb{Z}$ let $p = 2a \ni a = p/2$

& let $b = \frac{r}{s}$, $r, s \in \mathbb{Z}$, $(r,s) = 1$

$\therefore a^2 + 3b^2 = \left(\frac{p}{2}\right)^2 + 3\left(\frac{r}{s}\right)^2$

$$= \frac{p^2}{4} + \frac{3r^2}{s^2} \in \mathbb{Z}$$

$\cancel{\frac{p^2}{4} + \frac{3r^2}{s^2} \Rightarrow \frac{3r^2}{s^2} \in \mathbb{Z}}$ $\Rightarrow \frac{s^2p^2 + 4 \cdot 3r^2}{4s^2} \in \mathbb{Z}$

$\Rightarrow 4s^2 \mid (p^2s^2 + 12r^2)$

$\Rightarrow 4 \mid (p^2s^2 + 12r^2) \Rightarrow 4 \mid p^2s^2 \Rightarrow 2 \mid p$ or $2 \mid s$

Subcase-I If $2 \mid p$

then $a = p/2 \in \mathbb{Z}$

& $a^2 + 3b^2 \in \mathbb{Z} \Rightarrow 3b^2 \in \mathbb{Z}$ (let $b = r/s$)

$\Rightarrow 3 \cdot \left(\frac{r}{s}\right)^2 \in \mathbb{Z} \Rightarrow s^2 = 1$

$\Rightarrow s = \pm 1$

$\therefore b = \frac{r}{s} = \pm r \in \mathbb{Z}$

$\therefore \alpha = a + b\sqrt{3}\,i = a \pm i r\sqrt{3} \in \mathbb{Z}[\sqrt{3}i]$

Subcase-II If $2 \mid s \Rightarrow s = 2k_1$, $k_1 \in \mathbb{Z}$

$\Rightarrow \frac{p^2}{4} + \frac{3r^2}{(2k)^2} = \frac{k^2p^2 + 3r^2}{4k^2} \in \mathbb{Z}$

24

$\Rightarrow 4k^2 \mid k^2p^2 + 3r^2$

$\Rightarrow k^2 \mid k^2p^2 + 3r^2$ $\quad (\because k^2 \mid 4k^2)$

$\Rightarrow k^2 \mid 3r^2$ $\quad (\because (s, r) = 1 \Rightarrow (2k, r) = 1 \Rightarrow (k, r) = 1$

$\Rightarrow k^2 \mid 3$

$\Rightarrow k = \pm 1 \Rightarrow s = \pm 2$

$\therefore \frac{p^2}{4} + \frac{3r^2}{4} \in \mathbb{Z}$

$\Rightarrow 4 \mid p^2 + 3r^2 \Rightarrow 2 \mid p^2 + 3r^2$

$\Rightarrow 2 \mid p^2 \Rightarrow 2 \mid p \Rightarrow \boxed{p = 2k_1}$

$2 \mid 3r^2 \Rightarrow 2 \mid r^2 \Rightarrow 2 \mid r \Rightarrow \boxed{r = 2k_2}$

$\cancel{\therefore \frac{p^2}{4} + \frac{3r^2}{4} = 2k_1}$ $\therefore b = \frac{r}{s} = \frac{2k_2}{\pm 2} = \pm k_2 \in \mathbb{Z}$

$\Rightarrow b \in \mathbb{Z}$

$\therefore a + i\sqrt{3}\, b \in \mathbb{Z}[\sqrt{3} i]$

Primitive element theorem (25)

$\boxed{\text{Every finite \& separable ext}^n \text{ is primitive}}$

ⓐ No. field

$$K = Q(\theta) \quad \left[K = \text{Number field for some algebraic number } \theta \right]$$

finite | Q

↳ By primitive element theorem

ⓑ Alg. No.

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

4 deg. | Q

$\because \frac{1}{2}(\sqrt{2}+\sqrt{3}) \in Q(\sqrt{2}+\sqrt{3})$ $\quad = Q\left(\frac{1}{2}(\sqrt{2}+\sqrt{3})\right)$

Not an alg. integer

$\sqrt{2}+\sqrt{3} \in Q\left(\frac{1}{2}(\sqrt{2}+\sqrt{3})\right)$

$\sqrt{2}+\sqrt{3} = 2 \times \frac{1}{2}(\sqrt{2}+\sqrt{3})$

Que: Can we choose an algebraic integer α in place of θ to assume that $K = Q(\alpha)$?

Sol^n Observation: $\boxed{\text{If } \theta \text{ is an algebraic no., then } \exists \text{ +ve integer } m \text{ s.t } m\theta \text{ is an alg. integer}}$

Pf: As θ is an alg. no., so $\exists$ $P(x)(\neq 0) \in Q[x]$ s.t $P(\theta) = 0$

W.L.O.G, assume that $p(x) = \text{irred}(\theta; Q)$

i.e $\quad p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0, \quad a_0, a_1, \dots a_{n-1} \in Q$

let $\quad a_i = \frac{p_i}{q_i}, \quad p_i, q_i \in \mathbb{Z}$ & $(p_i, q_i) = 1$

$x = \theta$

$$\Rightarrow \theta^n + \frac{p_{n-1}}{q_{n-1}}\theta^{n-1} + \dots + \frac{p_0}{q_0} = 0$$

Let $m = q_{n-1} q_{n-2} \dots q_1 q_0$

$$\Rightarrow m^n\theta^n + \left(\frac{m\, p_{n-1}}{q_{n-1}}\right)(m\theta)^{n-1} + \dots + \frac{m^n p_0}{q_0} = 0 \leftarrow \text{multiplying by } m^n.$$

(26)

$\Rightarrow (m\theta)^n + \left(\frac{m\,p_{n-1}}{q_{n-1}}\right)(m\theta)^{n-1} + \cdots + \left(\frac{m^n}{q_0}\right)p_0 = 0$

$\Rightarrow \alpha^n + \left(\frac{m\,p_{n-1}}{q_{n-1}}\right)\alpha^{n-1} + \cdots + \frac{m^n}{q_0}\cdot p_0 = 0$ (let $m\theta = \alpha$)

$\Rightarrow \alpha = m\theta$ is an algebraic integer. Proved

Que: Can $Q(\theta) = Q(m\theta)$? (yes)

Sol^n It is obviously $Q(\theta) \subseteq Q(m\theta)$

we have to show $Q(m\theta) \subseteq Q(\theta)$

as $\beta = f(\theta)$ for some $f(x) \in Q[x]$

$$a_0 + a_1\theta + \cdots + a_k\theta^k = a_0 + a_1\cdot\frac{m\theta}{m} + \cdots + a_k\left(\frac{m\theta}{m}\right)^k$$
$$= \frac{1}{m^k}\left(a_0 m^k + a_1 m^{k-1}(m\theta) + \cdots + a_k(m\theta)^k\right)$$
$$\in Q(m\theta)$$

$\Rightarrow Q(\theta) \subseteq Q(m\theta)$

It is obvious that $Q(m\theta) \subseteq Q(\theta)$ verify

so, from both above $Q(\theta) = Q(m\theta)$

$K = Q(\theta)$: θ algebraic integer

$p_0(x) = \text{irred}(\theta, Q)$ (= minimal poly.)

(assume that $p_0(x)$ is of r. deg. poly, so $\exists$ r roots)

$\theta_1, \theta_2, \theta_3, \ldots, \theta_r$

$\theta_1 = \theta$ (say), $\theta_1, \theta_2, \ldots \theta_r$ are conjugates of θ

For any embedding σ

$$\sigma(\theta) \in \{\theta_1, \theta_2, \cdots \theta_r\}$$

$\underline{\underline{NB}}$: $\boxed{\text{Roots of minimal poly.s are conjugates}}$

$$
\begin{aligned}
&Q(\theta_1) \xrightarrow{\sigma_1 = Id_1} \theta \\
&Q(\theta_1) \xrightarrow{\sigma_2} \theta_1 \\
&Q(\theta_1) \xrightarrow{\sigma_3} \theta_2 \\
&\quad \vdots \\
&Q(\theta_1) \xrightarrow{\sigma_r} \theta_r
\end{aligned}
$$

($*$ $\because$ θ is an alg. int., so its other conjugates $\theta_1, \theta_2, \cdots \theta_r$ are also algebraic integ.)

eg

$K = Q(\sqrt[5]{2})$, $\rho = e^{\frac{2\pi i}{5}}$

$p(x) = \text{irred}(\sqrt[5]{2}, Q)$

$= x^5 - 2$

roots : $\sqrt[5]{2}, (\sqrt[5]{2})^2, (\sqrt[5]{2})^3, \cdots (\sqrt[5]{2})^5$

or : $\sqrt[5]{2}, \sqrt[5]{2}\rho, \sqrt[5]{2}\rho^3, \cdots \sqrt[5]{2}\rho^5$

ρ = 5th root of unity

$\because$ $\sqrt[5]{2}$ is a no. field & deg. $p(x) = 5$ which is finite so, others are also no. field.

$O \to$ Collection of alg. integers

$$
\begin{tikzcd}
O \arrow[r, hook] \arrow[d, dash] & A \arrow[d, dash] \\
\mathbb{Z} \arrow[r, hook] & Q
\end{tikzcd}
$$

Prove that O is ring

{ To prove O is ring : we do, for $\alpha, \beta \in O$
$\alpha + \beta, \ \alpha \cdot \beta \in O$ }

Observation

$\boxed{\text{Let } \alpha \in A. \text{ Then } \alpha \text{ is an algebraic integer iff } \mathbb{Z}[\alpha] \text{ is finitely generated.}}$

Proof : Let $\alpha \in A$, $\exists$ $0 \neq P(x) \in Q[x]$ s.t $P(\alpha) = 0$

$P(x) = \text{irred}(\alpha; Q)$ = minimal Poly.

$(\Rightarrow)$. Let α is an algebraic integer

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

$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$; $a_{n-1}, \cdots, a_0 \in \mathbb{Z}$

If $\beta \in \mathbb{Z}[\alpha] \Rightarrow \beta = f(\alpha)$ for some $f(x) \in \mathbb{Z}[x]$

$\therefore f(x) = p(x).q(x) + r(x)$ (By division algorithm)

where $q(x), r(x) \in \mathbb{Z}[x]$

& either $r(x) = 0$ or $\deg r(x) < \deg p(x) = n$

$\therefore \beta = \underbrace{p(\alpha).q(\alpha)}_{=0} + r(\alpha)$ $\quad (\because p(\alpha) = 0)$

$\Rightarrow \beta = r(\alpha)$

if $\beta = 0 \Rightarrow r(\alpha) = 0$, then $f(x) = p(x)\, q(x)$

thus result holds.

<u>If $\beta \neq 0$</u>, then

$\beta = r(\alpha) = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$ —— $(*)$

Let $\Gamma_\alpha = \mathbb{Z}\langle 1, \alpha, \ldots \alpha^{n-1} \rangle$ ← finitely generated (i.e. generated by finite elt.s $1, \alpha, \ldots \alpha^{n-1}$)

$$\boxed{\begin{array}{l}\text{let } \gamma \in \Gamma_\alpha \text{, then} \\ \gamma = b_0.1 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \quad b_0, b_1, \ldots b_{n-1} \in \mathbb{Z}\end{array}}$$

then by $(*)$, we have –

$\mathbb{Z}[\alpha] \subseteq \Gamma_\alpha$

and by definition of Γ_α, $\Gamma_\alpha \subseteq \mathbb{Z}[\alpha]$

thus $\boxed{\mathbb{Z}[\alpha] = \Gamma_\alpha}$ ← (req. Result)

($\Leftarrow$). Let $\mathbb{Z}[\alpha]$ is finitely generated

claim: α is an algebraic integer.

(29)

$\because \mathbb{Z}[\alpha]$ is finitely generated, so $\exists\ v_1, v_2, \dots v_k \in \mathbb{Z}[\alpha]$ s.t $\mathbb{Z}[\alpha] = \mathbb{Z}\langle v_1, v_2, \dots v_k \rangle$

$\because \mathbb{Z}[\alpha]$ is a ring $\forall\ \alpha \in \mathbb{Z}[\alpha], v_1 \in \mathbb{Z}[\alpha]$

$\Rightarrow \alpha v_1 \in \mathbb{Z}[\alpha]$

$$\Rightarrow \alpha v_1 = a_{11}v_1 + \dots + a_{1k}v_k$$

lly

$$\alpha v_2 = a_{21}v_1 + \dots + a_{2k}v_k$$
$$\vdots$$
$$\alpha v_k = a_{k1}v_1 + \dots + a_{kk}v_k$$

$$\Rightarrow (\alpha - a_{11})v_1 - \dots - a_{1k}v_k = 0$$

$$\Rightarrow -a_{21}v_1 + (\alpha - a_{22})v_2 - \dots - a_{2k}v_k = 0$$
$$\vdots$$
$$-a_{k1}v_1 - a_{k2}v_2 + \dots + (\alpha - a_{kk})v_k = 0$$

$\because$ this system has a non-zero solⁿ $(v_1, \dots, v_k)$

$$\therefore \det \begin{pmatrix} \alpha - a_{11}, & -a_{12} & \dots & -a_{1k} \\ -a_{21} & \alpha - a_{22} & \dots & -a_{2k} \\ \vdots & \vdots & \ddots & \\ -a_{k1} & -a_{k2} & \dots & (\alpha - a_{kk}) \end{pmatrix} = 0$$

which gives a monic poly. with powers of α and integer co-efficients.

$\Rightarrow \alpha$ satisfies a monic poly. with integer co.eff.

$\Rightarrow \alpha$ is an algebraic integer.

Lemma:-

$\boxed{\text{If } \phi \text{ \& } \psi \text{ are alg. integers then } \phi+\psi \text{ \& } \phi\psi \text{ are also}}$

$\Gamma_\phi = \mathbb{Z}[\phi]$ is finitely generated

$\Gamma_\psi = \mathbb{Z}[\psi]$ is finitely generated.

Claim: (i) $\Gamma_{\phi+\psi} = \mathbb{Z}[\phi+\psi]$ is finitely generated

(ii) $\Gamma_{\phi\psi} = \mathbb{Z}[\phi\psi]$ is finitely generated

Pf: $\Gamma_\phi = \mathbb{Z}[\phi]$ is finitely generated

$\Rightarrow \Gamma_\phi = \mathbb{Z}\langle v_1, v_2, \dots, v_n \rangle$ for some $v_1, v_2, \dots v_n \in \Gamma_\phi$

and $\Gamma_\psi = \mathbb{Z}[\psi]$ is finitely generated

$\Rightarrow \Gamma_\psi = \mathbb{Z}\langle u_1, u_2, \dots u_m \rangle$ for some $u_1, u_2, \dots u_m \in \Gamma_\psi$

<u>For $\Gamma_{\phi+\psi}$</u>

Let $\alpha \in \Gamma_{\phi+\psi}$ then

$$\alpha = a_0 + a_1(\phi+\psi) + a_2(\phi+\psi)^2 + \dots + a_k(\phi+\psi)^k$$
$$= a_0 + a_1(\phi+\psi) + a_2(\phi^2+2\phi\psi+\psi^2) + \dots + \dots$$

?? α is a poly. in $\underset{(\phi+\psi)^i}{\phi^i\psi^j}$ $0 \le i,j$, but $\phi^i\psi^j \in \Gamma_\phi\Gamma_\psi$

$\therefore \Gamma_{\phi+\psi} \subseteq \Gamma_\phi\Gamma_\psi = \mathbb{Z}\langle v_1, \dots v_n\rangle \, \mathbb{Z}\langle u_1, \dots, u_m\rangle$

$= \mathbb{Z}\langle v_i u_j : 1 \le i \le n, 1 \le j \le m \rangle$

$\Rightarrow \Gamma_\phi\Gamma_\psi$ is finitely generated

& $\Gamma_{\phi+\psi} \subseteq$ finitely generated as a group.

So $\Gamma_{\phi+\psi}$ is also finitely generated

$\Rightarrow \phi+\psi$ is an algebraic integer.

~~and~~ <u>For $\Gamma_{\phi\psi}$</u>

Let $\alpha \in \Gamma_{\phi\psi}$

$$\alpha = a_0 + a_1\phi\psi + a_2(\phi\psi)^2 + \dots + a_k(\phi\psi)^k$$
$$= a_0 + a_1\phi\psi + a_2\phi^2\psi^2 + \dots + a_k\phi^k\psi^k$$

α is a poly. in $\phi^i\psi^j$, $0 \le i, j$

$\because$ ~~$\Gamma_\phi \Gamma_\psi \subseteq$~~ $\Gamma_{\phi\psi} \subseteq \Gamma_\phi . \Gamma_\psi$ & $\Gamma_\phi \Gamma_\psi$ is finitely generated

$\Rightarrow$ $\Gamma_{\phi\psi}$ is also finitely generated

$\Rightarrow$ $\phi\psi$ is an algebraic integer.

Thus, Collection B of algebraic integer in $\mathbb{C}$ forms a Ring

This B is called a Ring of integers.

* $\{\alpha \in K : \alpha \text{ is an alg. integ.}\} = O_K$

$$\begin{tikzcd} O_K \arrow[r, hook] \arrow[d, leftrightarrow] & K \arrow[d, dash] \\ \mathbb{Z} \arrow[r, hook] & Q \end{tikzcd}$$

$B \cap Q = \mathbb{Z} = O_K \cap Q$

Now we have to show that O_K is Ring

Exercise : Show that O_K is a ring

Result Let $m \in \mathbb{Z}$ be a sq. free integ. $K = Q(\sqrt{m})$

then $O_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & : m \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & : m \equiv 1 \pmod 4 \end{cases}$

example $K = Q(\sqrt{5})$, then $O_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

this eg. show that $\mathbb{Z}[\sqrt{5}] \neq O_K$ but $\mathbb{Z}[\sqrt{5}] \subseteq O_K$

proof

Let $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

$\Rightarrow \alpha = a + b\left(\frac{1+\sqrt{5}}{2}\right)$, $a, b \in \mathbb{Z}$

take $a = -1$ & $b = 2$ then $\alpha = -1 + 2\left(\frac{1+\sqrt{5}}{2}\right) = \sqrt{5}$

$\Rightarrow \alpha \in \mathbb{Z}[\sqrt{5}]$.

$O_K \neq \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{5}] \leftarrow a+b\sqrt{5}$

$c+d\left(\frac{1+\sqrt{5}}{2}\right)$. But take $c=0$, $d=1 \Rightarrow \frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$

$\Rightarrow O_K \supsetneq \mathbb{Z}[\sqrt{5}]$

• Results B: Collection of algebraic integers.

$\alpha \in \mathbb{C}$ s.t $\exists$ a monic poly. $p(x) \in \mathbb{B}[x]$, then $\alpha \in B$.
$p(\alpha)=0$

Let $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$; $a_0, \dots a_{n-1} \in B$

for $0 \le i \le n-1$, $\Gamma_{a_i} = \mathbb{Z}[a_i]$ is finitely generated.

$= \mathbb{Z}\langle\{ \gamma_{i j_i} : i \le j_i \le n_i \}\rangle$

Claim $\Gamma_\alpha = \mathbb{Z}[\alpha]$ is finitely generated.

let $\alpha \in \mathbb{Z}[\alpha]$

then $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$

$\Rightarrow \alpha^n = -a_0 - a_1\alpha - \dots - a_{n-1}\alpha^{n-1}$, $a_0, \dots a_{n-1} \in \mathbb{Z}$

$\Rightarrow \alpha^n \in \Gamma_\alpha$

A subset of O_K, which generates O_K are ______ is called free generator of O_K over $\mathbb{Z}$.

9/8/18. (33)

A: Algebraic number
B: algebraic integer.

$\boxed{A \supseteq B}$

let $\alpha \in \mathbb{C}$,
if α satisfies a monic polynomial $p(x) \in B[x]$

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \quad , \quad a_0, \dots a_{n-1} \in \mathbb{Z}$$

<u>Claim</u>: $\alpha \in B$

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0 \quad \text{———} (*)$$

let $C = \mathbb{Z}[a_0, a_1, \dots, a_{n-1}]$ be a poly. ring

Now, from $(*)$, We see that —

$$C[\alpha] = C\langle 1, \alpha, \dots, \alpha^{n-1} \rangle$$
$$\shortparallel$$
$$\mathbb{Z}[a_0, a_1, \dots, a_{n-1}][\alpha] = \mathbb{Z}[a_0, a_1, \dots, a_{n-1}, \alpha]$$

If we can show that $C[\alpha]$ is finitely generated then we are done

$\mathbb{Z}[x]$
$\mathbb{Z}[x,y] = \mathbb{Z}[x][y]$
$\mathbb{Z}[x_0, \dots, x_{n-1}] =$
$\mathbb{Z}[x,y] = \mathbb{Z}[x] \cdot \mathbb{Z}[y]$

$$\therefore \mathbb{Z}[a_0, a_1, \dots a_{n-1}][\alpha] = \mathbb{Z}[a_0]\,\mathbb{Z}[a_1] \dots \mathbb{Z}[a_{n-1}].[\alpha]$$
$$= \Gamma_{a_0} \cdot \Gamma_{a_1} \cdot \dots \Gamma_{a_{n-1}} \cdot [\alpha]$$

$$\Gamma_{a_i} = \mathbb{Z}\langle a_{i_1}, a_{i_2}, \dots, a_{i n_i} \rangle \quad \forall\ 0 \le i \le n-1.$$

$$\therefore \Gamma_{a_1}\Gamma_{a_2} \dots \Gamma_{a_{n-1}} = \mathbb{Z}\langle \{ a_{0 j_0}, a_{1 j_1}, \dots, a_{n-1\, j_{n-1}} : 1 \le j_0 < n_0,\ 1 \le j_1 \le n_1, \dots 1 \le j_{n-1} \le n_{n-1} \} \rangle$$

If $\beta \in C[\alpha]$, then

$$\beta = \beta_0 + \beta_1\alpha + \cdots + \beta_{n-1}\alpha^{n-1}.$$

where $\beta_0, \beta_1, \ldots, \beta_{n-1} \in \overset{\Gamma_{a_0}\Gamma_{a_1}\cdots\Gamma_{a_{n-1}}}{\overset{\|}{C}}$

Then, we see that –

$$\beta_i = \sum_{\substack{1 \le j_0 \le n_0 \\ 1 \le j_1 \le n_1 \\ \vdots \\ 1 \le j_{n-1} \le n_{n-1}}} \gamma^{(i)}_{j_0 j_1 \cdots j_{n-1}} \, a_{0j_0} a_{1j_1} \cdots a_{n-1\, j_{n-1}} \quad \text{with } \gamma^{(i)}_{j_0 \cdots j_{n-1}} \in \mathbb{Z}$$

Then it is easy to see that

$$\beta \in \mathbb{Z}\langle \{ a_{0j_0} a_{1j_1} \cdots a_{n-1\, j_{n-1}} : 1 \le j_0 \le n_0, \ldots, 1 \le j_{n-1} \le n_{n-1}, \ 0 \le k \le n-1 \} \rangle$$

$$\Rightarrow C[\alpha] \subseteq \mathbb{Z}\langle \{ a_{0j_0} a_{1j_1} \cdots a_{n-1\, j_{n-1}} \alpha^k : 1 \le j_0 \le n_0, \ldots, 1 \le j_{n-1} \le n_{-1}, \ 0 \le k \le n-1 \} \rangle$$

and also

$$\mathbb{Z}\langle \{ a_{0j_0} a_{1j_1} \cdots a_{n-1\, j_{n-1}} \alpha^k : 1 \le j_0 \le n_0, \ldots, 1 \le j_{n-1} \le n-1, \ 0 \le k \le n-1 \} \rangle \le C[\alpha]$$

$$\therefore C[\alpha] = \mathbb{Z}\langle \{ a_{0j_0} a_{1j_1} \cdots a_{n-1\, j_{n-1}} \alpha^k : 1 \le j_0 \le n_0, \ldots, 1 \le j_{n-1} \le n_{n-1}, \ 0 \le k \le n-1 \} \rangle$$

$\Rightarrow \alpha$ is an algebraic

$\Rightarrow \alpha \in B.$

(35)

Que: K = number field.

O_K = Ring of integer in K.

($\alpha, \beta \in O_K$, $\alpha+\beta \in O_K$??) Prove O_K is Ring.

$\because \alpha, \beta \in O_K \Rightarrow \alpha, \beta \in B$ $\quad (O_K = K \cap B)$ $\Rightarrow O_K \subseteq B$

$\Rightarrow \alpha+\beta \in B$ ($\because B$ is a ring)

$\because K$ is field

$\therefore \alpha+\beta \in K$ ($\because \alpha, \beta \in O_K$ & $O_K \subseteq K$)

$\Rightarrow \alpha+\beta \in B \cap K = O_K$

and also $\alpha, \beta \in O_K \Rightarrow \alpha, \beta \in B$

$\Rightarrow \alpha\beta \in B$ ($\because B$ is ring)

$\because K$ is a field $\Rightarrow \alpha\beta \in K$

$\Rightarrow \alpha\beta \in B \cap K = O_K$

$\therefore O_K$ is a ring.

$K = \mathbb{Q}(\sqrt{2})$, $O_K = \mathbb{Z}[\sqrt{2}]$

$z \in \mathbb{Z}\langle\{1, \sqrt{2}\}\rangle$

$= \mathbb{Z} \oplus \mathbb{Z}\{\sqrt{2}\} \simeq \mathbb{Z} \times \mathbb{Z}\langle\{\sqrt{2}\}\rangle$

$z = z_1 + z_2\sqrt{2}$ with $z_1, z_2 \in \mathbb{Z}$

$= (z_1, z_2)$

$a \cdot 1 + b\sqrt{2} = 0 = 0 + 0\sqrt{2} \Rightarrow a = 0 = b$

(36)

An abelian group G is called free of Rank K if $G \xrightarrow{\sim} \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{k\text{-copies}} = \mathbb{Z}^k$

Eg. $K = \mathbb{Q}[i]$, $O_K = \mathbb{Z}[i] \supseteq \mathbb{Z}$

$= \mathbb{Z} \oplus \mathbb{Z}\langle\{i\}\rangle \longrightarrow \mathbb{Z} \times \mathbb{Z}$

$(a + ib) \xrightarrow{\Psi} (a, b)$

Here $\{1, i\}$ are free w.r.t each other

$\{1, i\}$ are free generator

$\therefore \{1, i\}$ are also basis for $\mathbb{Q}(i)$.

every ~~elt~~. primitive elt. is an alg. integer which acts as free generator of the primitive element.

But every algebraic integer cannot be a primitive elt.s whose basis does not act as free generator.

Eg. $K = \mathbb{Q}(\sqrt{5})$ → Basis $= \{1, \sqrt{5}\}$

$\sqrt{5}$ is an algebraic integer but $\{1, \sqrt{5}\}$ is not the basis of O_K.

$$O_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$$

$$\therefore \sqrt{5} = 2 \times \left(\frac{1+\sqrt{5}}{2}\right) - 1$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1}{4}(1+5+2\sqrt{5}) = \frac{3+\sqrt{5}}{2} = 1.1 + \frac{1+\sqrt{5}}{2}$$

$$= a + b\left(\frac{1+\sqrt{5}}{2}\right) \quad , \ a = 1, \ b = 1$$

(37)

Que: Show that $\{1, \frac{1+\sqrt{5}}{2}\}$ are free generator!

Ans: $a.1 + b.\left(\frac{1+\sqrt{5}}{2}\right) = 0$ where $a, b \in \mathbb{Z}$

$\Rightarrow \left(a + \frac{b}{2}\right) + \frac{b\sqrt{5}}{2} = 0$

$\Rightarrow (2a+b).1 + b\sqrt{5} = 0$

$\because \{1, \sqrt{5}\}$ are the basis of K over Q.

so $2a + b = 0$ ($\because \{1, \sqrt{5}\}$ are L.I)

& $b = 0$

$\Rightarrow$

$2a + 0 = 0 \Rightarrow a = 0 \rightarrow \Rightarrow 1, \frac{1+\sqrt{5}}{2}$ are L.I

$\therefore \{1, \frac{1+\sqrt{5}}{2}\}$ are free generator.

Fact: If K is no. field, then $K = Q(\theta)$ for some $\theta \in \mathbb{B}$, the no. of basis elt.s of $\frac{K}{Q} = [K : Q]$

$= \deg(\text{irred}(\theta, Q)) = n$

$O_K \rightarrow v_1, v_2, \ldots v_n$ generator over $\mathbb{Z}$.

* Every elements of $Q(\sqrt{5})$ can be expressible in the $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

for eg: Let ~~a+b~~ $\alpha \in Q(\sqrt{5})$, then $a, b \in Q$

$\alpha = a + b\sqrt{5} = a + \frac{2(b\sqrt{5} + b)}{2} - b$

$= (a-b).1 + 2b\left(\frac{1+\sqrt{5}}{2}\right)$

Now, to show $\{1, \frac{1+\sqrt{5}}{2}\}$ are also the basis of $Q(\sqrt{5})$.

$\because x \cdot 1 + y\left(\frac{1+\sqrt{5}}{2}\right) = 0, \quad x, y \in \mathbb{Q}$

$\Rightarrow x + \frac{y}{2} + \frac{y\sqrt{5}}{2} = 0$

$\Rightarrow (2x+y)\cdot 1 + y\cdot\sqrt{5} = 0$

$\because \{1, \sqrt{5}\}$ are L.I as they are basis of $\mathbb{Q}(\sqrt{5})$.

$2x+y = 0$ & $y = 0$ $\Rightarrow 2x = 0 \Rightarrow x = 0$

O_K, $v_1, v_2, \ldots v_n$ generators over $\mathbb{Z}$

$\alpha \in K \Rightarrow \exists\, m \in \mathbb{Z}$ s.t $m\alpha \in O_K$.

$\Rightarrow m\alpha = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ for some $a_1 \ldots a_n \in \mathbb{Z}$

$\Rightarrow \alpha = \frac{a_1}{m}v_1 + \frac{a_2}{m}v_2 + \cdots \frac{a_n}{m}v_n$

$\Rightarrow \{v_1, v_2, \ldots v_n\}$ is a maximal spanning set of K over $\mathbb{Q}$,

$\Rightarrow \{v_1, v_2, \ldots v_n\}$ is basis for K.

$\Rightarrow \{v_1, v_2, \ldots v_n\}$ is L.I over $\mathbb{Q}$,

Que: Whether $\{v_1, v_2, \ldots v_n\}$ is a free generator of O_K?

Now, $z_1v_1 + z_2v_2 + \cdots + z_nv_n = 0$

$\because \{v_1, v_2, \ldots v_n\}$ are L.I over $\mathbb{Q}$, $z_1, z_2, \ldots z_n \in \mathbb{Z}$

So, $z_1, z_2, \ldots z_n \in \mathbb{Q}$

So $z_1v_1 + z_2v_2 + \cdots + z_nv_n = 0$

$\Rightarrow z_1 = z_2 = \cdots = z_n = 0$

So $\{v_1, v_2, \ldots v_n\}$ are L.I over $\mathbb{Z}$.

So, O_K is a free abelian group.

K = number field, then

$K = \mathbb{Q}(\theta)$ for some algebraic integer θ

$[K:Q] = n = (\text{irred}(\theta; Q))$

$\because$ θ is an algebraic integer.

$\therefore \text{irred}(\theta, Q) \in \mathbb{Z}[x]$

$1, \theta, \dots \theta^{k-1} \in O_K$

and are basis elts for K over Q

Are they free generator always ? — NO

Eg. $K = Q(\sqrt{5})$, $\{1, \sqrt{5}\}$ are basis of $Q(\sqrt{5})$

$\downarrow$ Not free generators for O_K

To show free generator exists sometime —

Consider a collection

$S = \{(\omega_1, \dots, \omega_n) : \omega_i \in O_K$ & $\omega_1, \omega_2 \dots \omega_n$ forms a Q-basis for $K\}$

Discriminant of a Q-basis on K

Let $\omega = \{\omega_1, \dots, \omega_n\}$ be a Q-basis of K then discriminant of ω is defined as —

$$\Delta(\omega_1, \dots \omega_n) = \det{}^2(\sigma_i(\omega_j))$$

, where $\sigma_i : K \to \mathbb{C}$ is a Q-embedding.

Eg. $K = Q(\sqrt{5})$

Basis of $Q(\sqrt{5})$ is $\{1, \sqrt{5}\}$

embeddings of $Q(\sqrt{5})$ are

$Q(\sqrt{5}) \xrightarrow{\sigma_1 = \text{id}} \sqrt{5} \to \sqrt{5}$

$Q(\sqrt{5}) \xrightarrow{\sigma_2} \sqrt{5} \to -\sqrt{5}$

$$\therefore \Delta(1, \sqrt{5}) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{5}) \\ \sigma_2(1) & \sigma_2(\sqrt{5}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{vmatrix}^2 = (-2\sqrt{5})^2 = 20$$

(40)

* $\{1, \frac{1+\sqrt5}{2}\}$ is also a Basis of $Q(\sqrt5)$ then

$$\Delta\left(1, \frac{1+\sqrt5}{2}\right) = \begin{vmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt5}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt5}{2}\right) \end{vmatrix}^2 = \begin{vmatrix} 1 & \frac{1+\sqrt5}{2} \\ 1 & \frac{1-\sqrt5}{2} \end{vmatrix}^2$$

$$= \left(\frac{1-\sqrt5}{2} - \frac{1+\sqrt5}{2}\right)^2 = (-\sqrt5)^2 = 5$$

So, for different basis, we have different values of ~~determinant~~ discriminant.

<u>Que</u> Can we see any isomorphism b/w $\{1, \sqrt5\} \to \{1, \frac{1+\sqrt5}{2}\}$

<u>Ans</u> $1, \frac{1+\sqrt5}{2}$

$\Rightarrow 1 = 1.1 + 0.\sqrt5$ (in combination of $1, \sqrt5$)

& $\frac{1+\sqrt5}{2} = \frac{1}{2}.1 + \frac{1}{2}.\sqrt5$

Then $\begin{pmatrix} 1 \\ \frac{1+\sqrt5}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac12 & \frac12 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt5 \end{pmatrix}$

$$\therefore \Delta\left(1, \frac{1+\sqrt5}{2}\right) = \Delta\left(1, \frac{\sqrt5+1}{2}\right) = \det\begin{bmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt5}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt5}{2}\right) \end{bmatrix}^2$$

$$= \det{}^2\begin{pmatrix} 1 & \frac12\cdot1 + \frac12\cdot\sqrt5 \\ 1 & \frac12\cdot1 - \frac12\sqrt5 \end{pmatrix} = [-\sqrt5]^2 = 5$$

Now consider the matrix

$$\begin{pmatrix} 1 & \frac12\sigma_1(1) + \frac12\sigma_1(\sqrt5) \\ 1 & \frac12\sigma_2(1) + \frac12\sigma_2(\sqrt5) \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & \sigma_1(\sqrt5) \\ 1 & \sigma_2(\sqrt5) \end{pmatrix}$$

$$= \begin{pmatrix} x+y & x\sigma_1(\sqrt5) + y\sigma_2(\sqrt5) \\ z+w & z\sigma_1(\sqrt5) + w\sigma_2(\sqrt5) \end{pmatrix}$$

So, on comparing the corresponding element, we get —

$x+y = 1$, $z+w = 1$, $x = \frac12 = y$ & $z = \frac12$, $w = \frac12$

(41)

$\{\alpha_1, \dots \alpha_n\}$ $\mathbb{Q}$-basis for K and $\{\beta_1 \dots \beta_n\}$ is another $\mathbb{Q}$-basis for K, then $\beta_i = c_{i1}\alpha_1 + \dots + c_{in}\alpha_n$ for some $c_{ij} \in \mathbb{Q}$, $i \le j \le n$

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ \vdots & & & \\ c_{i1} & c_{i2} & \dots & c_{in} \\ \vdots & & & \\ c_{n1} & \dots & & c_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$\Delta(\beta_1 \dots \beta_n) = \det{}^2(\sigma_i(\beta_j))$$

where
$$\sigma_i(\beta_j) = \begin{pmatrix} \sigma_1(\beta_1) & \dots & \sigma_1(\beta_n) \\ \sigma_2(\beta_2) & \dots & \sigma_2(\beta_n) \\ \vdots & & \\ \sigma_i(\beta_1) & \dots & \sigma_i(\beta_n) \\ \vdots & & \\ \sigma_n(\beta_n) & \dots & \sigma_n(\beta_n) \end{pmatrix}$$

$$= \begin{pmatrix} c_{11}\sigma_1(\alpha_1) + \dots + c_{1n}\sigma_1(\alpha_n) & \dots & c_{n1}\sigma_1(\alpha_1) + \dots + c_{nn}\sigma_1(\alpha_n) \\ \vdots & & \\ c_{i1}\sigma_i(\alpha_1) + \dots + c_{in}\sigma_i(\alpha_n) & \dots & c_{n1}\sigma_i(\alpha_1) + \dots + c_{nn}\sigma_i(\alpha_n) \\ \vdots & & \\ c_{n1}\sigma_n(\alpha_1) + \dots + c_{1n}\sigma_n(\alpha_n) & \dots & c_{n1}\sigma_n(\alpha_1) + \dots + c_{nn}\sigma_n(\alpha_n) \end{pmatrix}$$

$$= \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ \vdots & & & \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \dots & \sigma_n(\alpha_2) \\ \vdots & & & \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{pmatrix}$$

$$\therefore \Delta(\beta_1, \beta_2, \dots \beta_n) = \det{}^2(\sigma_i(\beta_j)) = \det{}^2(c_{ij}) \cdot \det{}^2 \begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{vmatrix}$$

$$= \det{}^2(c_{ij})^T . \Delta(\alpha_1, \dots \alpha_n) \qquad (\because |A| = |A^T|)$$

$\because c_{ij} \in \mathbb{Q}$

$\therefore \det{}^2(c_{ij}) \in \mathbb{Z}$

$$\therefore \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$\Delta(\beta_1 \dots \beta_n) = (\det A)^2 \Delta(\alpha_1 \dots \alpha_n)$$

(42)

Result: Let K be a quadratic field & m be a square free integer s.t $K = \mathbb{Q}[\sqrt{m}]$. then the set O_K of algebraic integers in K is given by

$$K = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

(P-31)

Sq. free integer.
def^n if $a|b$ then $a^2 \nmid b$ or $a^k \nmid b$; $k = 2, 3 \ldots$

Pf: Let $\alpha \in O_K$ & $O_K \subseteq K$

then $\alpha = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$

So, let $a = p/q$ & $b = r/s$

with $(p,q) = 1$, $(r,s) = 1$ & $p, q, r, s \in \mathbb{Z}$

$\therefore Tr_{\mathbb{Q}}(\alpha) = (a + b\sqrt{m}) + (a - b\sqrt{m}) = 2a$

$N_{\mathbb{Q}}(\alpha) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2 m$

We know that

$Tr_{\mathbb{Q}}(\alpha), \; N_{\mathbb{Q}}(\alpha) \in \mathbb{Z}$

So, $Tr_{\mathbb{Q}}(\alpha) = 2a = 2 \cdot (p/q) \in \mathbb{Z}$ & $(p,q) = 1$

So, $q | 2 \Rightarrow q = 1, 2$

Case-I, $q = 1$

$N_{\mathbb{Q}}(\alpha) = a^2 - mb^2 = \left(\frac{p}{q}\right)^2 - m\left(\frac{r}{s}\right)^2 = p^2 - \frac{mr^2}{s^2}$

$\because N_{\mathbb{Q}}(\alpha) \in \mathbb{Z} \Rightarrow p^2 - \frac{mr^2}{s^2} \in \mathbb{Z}$ $(\because p \in \mathbb{Z} \Rightarrow p^2 \in \mathbb{Z})$

$\Rightarrow \frac{mr^2}{s^2} \in \mathbb{Z} \Rightarrow s^2 | m$ $(\because (r,s) = 1)$

$\Rightarrow m = ks^2$ for some $k \in \mathbb{Z}$

If ~~m≠1~~, $s \neq 1$, $\longrightarrow \longleftarrow$ (as m is sq. free integ.)

So, $s = 1$

$\Rightarrow \alpha = p + r\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$

Case-II $\rightarrow$ for $q = 2$

$N_Q(\alpha) = \left(\frac{p}{2}\right)^2 - \left(\frac{r}{s}\right)^2 m \in \mathbb{Z}$

$\Rightarrow \frac{p^2}{4} - \frac{r^2}{s^2} m = \frac{p^2 s^2 - 4r^2 m}{4s^2} \in \mathbb{Z}$

$\Rightarrow 4s^2 \mid (p^2 s^2 - 4r^2 m)$ & $s^2 \mid (p^2 s^2 - 4r^2 m)$

$\Rightarrow 4 \mid p^2 s^2$

$\Rightarrow 4 \mid s^2$ $[\because (p, q) = 1, (p, 2) = 1]$ — ⓐ

& $s^2 \mid p^2 s^2 - 4r^2 m \Rightarrow s^2 \mid 4r^2 m$

$\Rightarrow s^2 \mid 4$ $(\because (r, s) = 1$, and m is a sqare free integer$)$ — ⓑ

$\therefore$ (a) & (b) $\Rightarrow s^2 = 4 \Rightarrow s = 2$

$\therefore \alpha = \frac{p}{2} + \frac{r}{2}\sqrt{m}$

$\therefore N_Q(\alpha) = \frac{p^2}{4} - \frac{mr^2}{4} = \frac{p^2 - mr^2}{4}$

$4 \mid (p^2 - mr^2) \Rightarrow p^2 - mr^2 \equiv 0 \pmod 4$

$1 - m \cdot 1 \equiv 0 \pmod 4$
as $(p, q) = 1$ & $(r, s) = 1$

$\Rightarrow m \equiv 1 \pmod 4$

$p = 2k + 1$ $(\because 2 \nmid p$ & $2 \nmid r)$

$r = 2k' + 1$

then $\alpha = \frac{2k+1}{2} + \frac{2k'+1}{2}\sqrt{m} = \left(k + \frac{1}{2}\right) + \left(k' + \frac{1}{2}\right)\sqrt{m}$

$= (k + k'\sqrt{m}) + \left(\frac{1}{2} + \frac{1}{2}\sqrt{m}\right)$

$$= k - k' + k'(1+\sqrt{m}) + \left(\frac{1+\sqrt{m}}{2}\right)$$

$$= (k-k') + (2k'+1)\left(\frac{1+\sqrt{m}}{2}\right)$$

$$= b_0 + b_1\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$$

$K = \mathbb{Q}(\theta)$, θ alg. integ. i.e $\theta \in O_K$

$\{1, \theta, \theta^2, \ldots \theta^{n-1}\}$ is basis for K over $\mathbb{Q}$.

$$[K:\mathbb{Q}] = n = \deg.(\operatorname{irred}(\theta;\mathbb{Q})) \subseteq \mathbb{Z}[x]$$

$$\begin{array}{c} K \; \xrightarrow{\sigma_1,\ \sigma_2,\ \sigma_3} \\ | \\ \mathbb{Q} \end{array}$$

Conjugates of θ are

$$\begin{array}{cccc} \sigma_1(\theta), & \sigma_2(\theta), & \ldots & \sigma_n(\theta) \\ \shortparallel & \shortparallel & & \shortparallel \\ \theta_1 & \theta_2 & & \theta_n \end{array}$$

$$\Delta(1, \theta, \theta^2, \ldots \theta^{n-1}) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\theta) & \ldots & \sigma_1(\theta^{n-1}) \\ \sigma_2(1) & \sigma_2(\theta) & \ldots & \sigma_2(\theta^{n-1}) \\ \vdots & & & \\ \sigma_n(1) & \sigma_n(\theta) & \ldots & \sigma_n(\theta^{n-1}) \end{vmatrix}^2$$

$$= \begin{vmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ \vdots & \vdots & & & \vdots \\ 1 & \theta_n & \theta_n^2 & & \theta_n^{n-1} \end{vmatrix}^2$$

Vandermonde matrix

$$= \left(\prod_{1 \le i,j \le n} (\theta_i - \theta_j)\right)^2, \quad i \ne j$$

$$= \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2 \in \mathbb{Q}^* \cap B = \mathbb{Z}^*$$

Algebraic No.

For $\theta \in O_K$

$$\Delta(1, \theta, \ldots \theta^{n-1}) \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$$

Observation

If $\{\beta_1, \beta_2, \ldots \beta_n\}$ is any other $\mathbb{Q}$-basis of K with $\beta_i \in O_K$ then $\Delta(\beta_1, \ldots \beta_n) \in \mathbb{Q}^* \cap B = \mathbb{Z}^*$

Further, if all conjugates of θ are real then

$$\Delta(1, \ldots \theta^{n-1}) \in \mathbb{Z}^+ \text{ and so } \Delta(\beta_1 \ldots \beta_n) \in \mathbb{Q}^+$$

Existence of Integral basis

Integral Basis — Basis of O_K — free generators of O_K

OR Integral Basis of K = Free generating subset of O_K as an abelian group.

free generator : Independent over $\mathbb{Z}$.

* n-generator of O_K are free generator.

Integral Basis of K

= Free generating subset of O_K as an abelian group.

$[K : \mathbb{Q}] = n$

$K = \mathbb{Q}[\theta]$ for some $\theta \in O_K$

$\{1, \theta, \ldots \theta^{n-1}\}$ is a basis ~~for~~ K over $\mathbb{Q}$.

$$\Delta(1, \theta, \ldots \theta^{n-1}) \in \mathbb{Z}^* \Rightarrow |\Delta(1, \theta, \ldots \theta^{n-1})| \in \mathbb{Z}^+$$

Consider a collection $\Sigma = \{ |\Delta(w_1 \ldots w_n)| : \{w_1, \ldots w_n\} \subseteq O_K$ is a $\mathbb{Q}$-basis of $K \}$

then Σ is non-empty.

Well-Ordering Principle

Every +ve subset of the integer has a least element

By well-ordering principle, $\exists$ a $\mathbb{Q}$-basis $\{1, w_1, \ldots w_n\}$ of K with $w_i \in O_K$

(48)

Claim: $\{w_1, \dots w_n\}$ is an integral basis of K

i.e a free generating subset of O_K.

Let $w \in O_K \Rightarrow w = a_1w_1 + a_2w_2 + \dots + a_nw_n,\ a_i \in \mathbb{Q}$

[$\because w \in O_K \Rightarrow w \in K$ as $O_K \subseteq K$]

If all the co-eff are in $\mathbb{Z}$, then we done

So, assume that (w.L.O.G) $a_1 \notin \mathbb{Z}$

$$\Rightarrow a_1 = \underset{[a]}{a} + \underset{\{(a_1)\}}{r} \qquad \text{for some } a \in \mathbb{Z},\ 0 < r < 1$$

then $w = (a+r)w_1 + a_2w_2 + \dots + a_nw_n$

$\Rightarrow w - aw_1 = rw_1 + a_2w_2 + \dots + a_nw_n$

Now, define

$$\psi_1 = w - aw_1,\ \psi_2 = w_2, \dots, \psi_n = w_n$$

then —

$$\begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} = \begin{pmatrix} r & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

↳ Non-singular matrix

When, we apply non-sing. matrix with basis, we get another basis.

So $(\psi_1, \dots \psi_n)$ is also a $\mathbb{Q}$-basis.

$\Rightarrow (\psi_1, \psi_2, \dots \psi_n)$ is also a basis of K with $\psi_i \in O_K$.

$$|\Delta(\psi_1, \psi_2, \dots, \psi_n)| = (\det A)^2 |\Delta(w_1, \dots, w_n)|$$
$$= r^2 |\Delta(w_1, \dots w_n)| < |\Delta(w_1 \dots w_n)|$$

$\longrightarrow\ \longleftarrow$

So, $a_1 \in \mathbb{Z}$

$\Rightarrow a_1, a_2, \dots a_n \in \mathbb{Z}$

So, $\{w_1, \dots w_n\}$ is an integral basis of K.

Note 2 integral Basis

transforming matrix b/w 2-integral basis is an unimodular matrix.

* Let $(\beta_1, \beta_2 \ldots \beta_n)$ and $(\alpha_1, \alpha_2, \ldots \alpha_n)$ are two integral basis.

then $\Delta(\beta_1, \beta_2, \ldots \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots \alpha_n)$ — $(*)$

and we know that

$\Delta(\beta_1, \beta_2, \ldots \beta_n) = (\det A)^2 \, \Delta(\alpha_1, \alpha_2, \ldots \alpha_n)$ — $(*,*)$

$(*)$ & $(**)$ $\Rightarrow$ $(\det A)^2 = 1$

$\Rightarrow \det A = \pm 1$

the matrix whose determinant is either 1 or -1 is called uni-modular matrix.

Example : $K = Q(\sqrt{5})$ $\left(\because 5 \equiv 1 \pmod 4 \right.$ $\left. \Rightarrow O_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \right)$

$O_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

& $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ is integral basis O_K

$\therefore \Delta\left(1, \frac{1+\sqrt{5}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix}^2 = \left(\frac{1-\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}\right)^2$

$= (-\sqrt{5})^2 = 5$

and $\left\{1, \frac{1-\sqrt{5}}{2}\right\}$ is also integral basis O_K.

$\therefore \Delta\left(1, \frac{1-\sqrt{5}}{2}\right) = \begin{vmatrix} 1 & \frac{1-\sqrt{5}}{2} \\ 1 & \frac{1+\sqrt{5}}{2} \end{vmatrix}^2 = \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right)^2 = (\sqrt{5})^2 = 5$

$\because$ $(1, \sqrt{5})$ is basis of K

$\Delta(1, \sqrt{5}) = \begin{vmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{vmatrix}^2 = (-2\sqrt{5})^2 = 4 \times 5 = 20$

(48)

$$\Delta(1, \sqrt{5}) = 20 > \Delta\left(1, \frac{1+\sqrt{5}}{2}\right) = \Delta\left(1, \frac{1-\sqrt{5}}{2}\right)$$

H.W.
Example. $K = \mathbb{Q}(\sqrt{-3})$, $K = \mathbb{Q}(\sqrt{-5})$

Fact: K : Number field, $K = \mathbb{Q}(\theta)$ for some θ

If K' is any other number field isomorphic to K, then

$$\Delta_K = \Delta_{K'} \quad \text{(check it holds or NOT)}$$

i.e. check it

$$\boxed{\sigma : \underset{\mathbb{Q}(\theta)}{K} \longrightarrow K' = \underset{\sigma(\theta)}{\mathbb{Q}(\theta')}}$$

Que: O_K has integral basis $\{\alpha_1, \ldots, \alpha_n\}$

$\{\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)\}$ is an integral basis of K

then

$$\Delta(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) = \begin{vmatrix} \sigma_1(\sigma(\alpha_1)) & \cdots & \sigma_1(\sigma(\alpha_n)) \\ \sigma_2(\sigma(\alpha_1)) & \cdots & \sigma_2(\sigma(\alpha_n)) \\ \vdots & & \\ \sigma_n(\sigma(\alpha_1)) & \cdots & \sigma_n(\sigma(\alpha_n)) \end{vmatrix}^2$$

$$= \begin{vmatrix} \underbrace{\sigma_1 \circ \sigma}_{\tau_1}(\alpha_1) & \cdots & \sigma_1 \circ \sigma(\alpha_n) \\ \underbrace{\sigma_2 \circ \sigma}_{\tau_2}(\alpha_1) & \cdots & \sigma_2 \circ \sigma(\alpha_n) \\ \vdots & & \vdots \\ \underbrace{\sigma_n \circ \sigma}_{\tau_n}(\alpha_1) & \cdots & \sigma_n \circ \sigma(\alpha_n) \end{vmatrix}$$

$$\{\tau_1, \tau_2, \cdots \tau_n\} = \{\sigma_1, \sigma_2, \cdots \sigma_n\}$$

$$= \begin{vmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \vdots & & \vdots \\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_n) \end{vmatrix} = \Delta(\alpha_1 \ldots \alpha_n)$$

HW Check with the integral basis $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$

$K = \mathbb{Q}(\sqrt[3]{2})$, $K' = \mathbb{Q}(\sqrt[3]{2}\omega)$

then $\Delta O_K = \Delta O_{K'}$

Result: Let K be a no. field & $\{\alpha_1, \cdots \alpha_n\} \subseteq O_K$ be a $\mathbb{Q}$-basis of K. If $\Delta(\alpha_1, \cdots \alpha_n)$ is square free then $\{\alpha_1, \cdots \alpha_n\}$ is an integral basis.

Proof: Let $\{\beta_1, \cdots \beta_n\}$ be an integral basis of O_K.

Then $\alpha_1 = a_{11}\beta_1 + a_{12}\beta_2 + \cdots + a_{1n}\beta_n$, $a_{11}, a_{12}, \cdots a_{1n} \in \mathbb{Z}$

$\alpha_2 = a_{21}\beta_1 + a_{22}\beta_2 + \cdots + a_{2n}\beta_n$, $a_{21}, a_{22} \cdots a_{2n} \in \mathbb{Z}$

$\alpha_n = a_{n1}\beta_1 + a_{n2}\beta_2 + \cdots + a_{nn}\beta_n$, $a_{n1}, a_{n2} \cdots a_{nn} \in \mathbb{Z}$

$\Delta(\alpha_1, \alpha_2, \cdots \alpha_n) = (\det(A))^2 \Delta(\beta_1, \cdots \beta_n)$

where $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{n1} & a_{n2} & & a_{nn} \end{pmatrix}$

$\Rightarrow \det(A) = \pm 1$ as $\Delta(\alpha_1, \cdots \alpha_n)$ is sq. free

$\Rightarrow \Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = \Delta(\beta_1, \cdots \beta_n)$

$\Rightarrow \{\alpha_1, \cdots \alpha_n\}$ is also an integral basis of O_K.

Let G: free abelian group of rank n; H is a subgrp of G, then $\exists$ a set of free generator $\{\alpha_1, \alpha_2, \cdots \alpha_n\}$ of G & +ve integers $d_1, \cdots d_s$, $s \leq n$ s.t $\{d_1\alpha_1, \cdots, d_s\alpha_s\}$ is a free generating subset of H.

(50)

eg: $G = \mathbb{Z} \times \mathbb{Z}$

free generator of $\mathbb{Z}\times\mathbb{Z}$ is $\{(0,1),(1,0)\}$

So, $\mathbb{Z}\times\mathbb{Z}$ is free ab. grp of Rank 2.

$H = 2\mathbb{Z}\times\mathbb{Z}$, $d_1 = 2$, $d_2 = 1$ s.t $\{2(1,0), 1(0,1)\}$

>> 1st chapter of :-
↳ Algebraic number theory & farmats last theorem

Book

Result: Let K be a no. field, O_K ring of integer in K. If $G < O_K$ of α = rank = $[K:\mathbb{Q}]$ with a $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ then $[O_K / G]^2 \mid \Delta(\alpha_1, \ldots \alpha_n)$

Result: If G is a free grp. of rank n, $H < G$, then $\exists$ a subset $\{\alpha_1, \ldots \alpha_n\}$ of free generators of G and the integers $d_1, d_2, \ldots d_s$, $s \leq n$, s.t $\{d_1\alpha_1, \ldots, d_s\alpha_s\}$ is a set of free generators of H.

Mathematically

If $x \in G = \mathbb{Z}\{\alpha_1\} \oplus \mathbb{Z}\{\alpha_2\} \oplus \cdots \oplus \mathbb{Z}\{\alpha_n\}$

$x = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, $a_1, a_2, \ldots a_n \in \mathbb{Z}$

$H = \mathbb{Z}\{d_1\alpha_1\} \oplus \mathbb{Z}\{d_2\alpha_2\} \oplus \cdots \oplus \mathbb{Z}\{d_s\alpha_s\}$

$$G/H = \frac{\mathbb{Z}\{\alpha_1\} \oplus \cdots \oplus \mathbb{Z}\{\alpha_s\} \oplus \cdots \oplus \mathbb{Z}\{\alpha_n\}}{\mathbb{Z}\{d_1\alpha_1\} \oplus \cdots \oplus \mathbb{Z}\{d_s\alpha_s\}}$$

Observation :-

$G = G_1 \oplus G_2$ & $H \subseteq G$, $H = H_1 \oplus H_2$

then $\dfrac{G}{H} \xrightarrow{\sim} G_1/H_1 \oplus G_2/H_2$

Pf:

$$G \longrightarrow G_1/H_1 \oplus G_2/H_2$$

$G \cong G_1 \oplus G_2$

Some Useful Links:

1. Free Study Materials(By P Kalika) (https://pkalika.in/2019/10/14/study-material/**)**

2. Free Maths Study Materials(Donated) (https://pkalika.in/2020/04/06/free-maths-study-materials/**)**

3. MSc Entrance Exam Que. Paper: (https://pkalika.in/2020/04/03/msc-entrance-exam-paper/**)**
[JAM(MA), JAM(MS), BHU, CUCET, ...etc]

4. PhD Entrance Exam Que. Paper: (https://pkalika.in/que-papers-collection/**)**
[CSIR-NET, GATE(MA), BHU, CUCET,IIT, NBHM, ...etc]

5. CSIR-NET Maths Que. Paper: (https://pkalika.in/2020/03/30/csir-net-previous-yr-papers/**)**
[Upto 2019 Dec]

6. Practice Que. Paper: (https://pkalika.in/2019/02/10/practice-set-for-net-gate-set-jam/**)**
[Topic-wise/Subject-wise]

(Provide your Feedbacks/Comments at maths.whisperer@gmail.com)