Total Marks: 100 Theory: 80 Sessional: 20

Unit 5: Algebraic numbers, number fields, norm, trace, discriminants. Valuations, algebraic integers and integral bases. 20 marks

Text Books:

1. David M. Burton, Elementary Number Theory (Unit 1, 2, 3), McGraw Hill Education, 2017
2. G. E. Andrews, Number Theory (Unit 4), Dover Publications, 2012
3. Richard A Molin, Algebraic number theory, Chapman and Hall/CRC, 2011

Reference Books: 1. I. Niven, H. S. Zuckerman and H. L. Montgomery, Introduction to Theory of Numbers, Wiley, 2008

Algebraic Number: The number $\alpha \in C$ is said to be algebraic if it satisfies a polynomial equation $x^n + a_1x^{n-1} + \cdots + a_n$ with rational coefficients $a_i \in Q$.

We denote the set of algebraic numbers by $\overline{Q}$.

Examples:

1. $\alpha = \sqrt{2}$ is algebraic, since it satisfies the equation $x^2 - 2 = 0$.
2. $\alpha = \sqrt[3]{2} + 1$ is algebraic, since it satisfies the equation $(x - 1)^3 = 2$,

   ie $x^3 - 3x^2 + 3x - 3 = 0$.

Monic Polynomial: A polynomial $f(x) \in k[x]$ is said to be monic if its leading coefficient is 1.

$f(x) = x^n + a_1x^{n-1} + \cdots + a_n$.

is a monic polynomial, as the coefficient of the highest power (leading coefficient) term is 1.

Theorem: An algebraic number $\alpha \in \overline{Q}$ satisfies a unique monic polynomial $m(x) \in Q[x]$ of minimal degree; and if $f(x) \in Q[x]$ then $f(\alpha) = 0 \Leftrightarrow m(x) \mid f(x)$.

Proof : If α satisfies two monic polynomials $m_1(x)$, $m_2(x)$ of the same degree, then it satisfies the polynomial $m_1(x) - m_2(x)$ of lower degree.

If $f(\alpha) = 0$, divide $f(x)$ by $m(x)$, say $f(x) = m(x)q(x) + r(x)$, where deg $r(x) <$ deg $m(x)$.

Then $r(\alpha) = f(\alpha) - m(\alpha)q(\alpha) = 0$, contradicting the minimality of $m(x)$ unless $r(x) = 0$,

ie $m(x) \mid f(x)$.

Algebraic Integer : The number $\alpha \in C$ is said to be an algebraic integer if it satisfies a polynomial equation $x^n + a_1x^{n-1} + \cdots + a_n$ with integer coefficients $a_i \in Z$. We denote the set of algebraic integers by $\overline{Z}$.

Note: In algebraic number theory, an algebraic integer is often just called an integer, while the ordinary integers (the elements of Z) are called rational integers.

Examples:

1. $\alpha = 3\sqrt{2} + 1 \in \overline{Z}$, since α satisfies $(x - 1)^2 = 18$,

   ie $x^2 - 2x - 17 = 0$.

2. $\alpha = \sqrt{2} + \sqrt{3} \in \overline{Z}$, since α satisfies $(x - \sqrt{3})^2 = 2$ or $x^2 - 2x\sqrt{3} + 3 = 2$,

   ie $x^2 - 2\sqrt{3}x + 1 = 0$.

Hence $(x^2 + 1)^2 = 12x^2$,

ie $x^4 - 10x^2 + 1 = 0$.

Some Important Results:

1. $Z \subset \overline{Z}$

2. $\overline{Z} \cap Q = Z$

3. If $\alpha \in \overline{Q}$ then $n\alpha \in \overline{Z}$ for some non-zero $n \in Z$.

4. $\overline{Z}$ is a subring of C.

5. The number $\alpha \in C$ is an algebraic integer if and only if the Abelian group $B = <1, \alpha, \alpha^2, \ldots> \subset C$ is finitely-generated.

6. The number $\alpha \in C$ is an algebraic integer if and only if there exists a finitely-generated (but non-zero) Abelian group $B \subset C$ such that $\alpha B \subset B$.

Algebraic Integers of degree m: If $\alpha \in C$ is a root of a monic integral polynomial of degree m but α is not a root of a polynomial of degree less than m, then α is called an algebraic integer of degree m.

Example : If $\alpha = \sqrt{-3}$, then α is a root of the polynomial $x^2 + 3$ but α does not satisfy a linear polynomial in x. Thus, $\alpha = \sqrt{-3}$ is an algebraic integer of degree 2.

Algebraic Number of degree m: If $\alpha \in C$ is a root of an integral polynomial of degree m but α is not a root of a polynomial of degree less than m, then α is called an algebraic number of degree m.

Note that, every algebraic integer is an algebraic number but the converse is not true.

Example : If $\alpha = \sqrt{(-3/2)}$, then α is a root of the polynomial $2x^2 + 3$ but α does not satisfy a linear polynomial in x. Thus, $\alpha = \sqrt{(-3/2)}$ is an algebraic number of degree 2.

Algebraic Number Field: If $\alpha \in C$ is an algebraic number of degree m, then the field $Q(\alpha)$ is called an algebraic number field of degree m over Q.

Note 1. Here α is a root of an integral polynomial of degree m but not less than m.

Note 2. $Q(\alpha)$ can be considered as a vector space over Q and so dimension of $Q(\alpha)$ over Q is m, that is, $[Q(\alpha) : Q] = m$.

Note 3. Q is the smallest algebraic number field as it is of degree 1 over itself.

Example 3: Let us consider the field $Q(\sqrt{-3})$. Since $\alpha = \sqrt{-3} \in C$ is a root of the polynomial $x^2 + 3$ but α is not a root of any linear polynomial in x. So, $\alpha = \sqrt{-3}$ is an algebraic number of degree 2. Thus, $Q(\sqrt{-3})$ is an algebraic number field of degree 2 over Q.

Algebraic Extension of a field: Let E be an extension of a field F. An element $\alpha \in E$ is said to be algebraic over F if $\exists$ a polynomial $f(x)(\neq 0) \in F[x]$ such that $f(\alpha) = 0$. An extension E of F is called an algebraic extension if every element of E is algebraic over F. Note that, an algebraic number is a complex number which is algebraic over Q.

A **number field** F is a finite field extension of Q. The dimension of F as a Q-vector space is called the degree of F. It is denoted by [F : Q].

Examples of number fields are Q, Q(i), Q($\sqrt[2]{4}$), Q($\sqrt[3]{3}$, $\sqrt{7}$) and Q($\sqrt{2}$, $\sqrt{[1+\sqrt{2}]}$) of degrees 1, 2, 4, 6 and 4 respectively. The following theorem says that every number field can be generated by one element only. This element is by no means unique

Minimal Polynomial: If α is algebraic over F, then $\exists$ a polynomial $f(x)(\neq 0) \in F[x]$ such that $f(\alpha) = 0$. We may assume f(x) has minimal degree. Then f(x) has to be irreducible, otherwise α would be a root of a polynomial of lower degree. Since F is a field we may assume f(x) is monic by dividing out by the leading co-efficient. The polynomial thus chosen is called the minimal polynomial of α over F and it is denoted by $m_{\alpha,F}(x)$. Thus, $m_{\alpha,F}(x)$ is monic and irreducible polynomial over F with lowest degree satisfied by α.

Eisenstein's Irreducibility Criterion: Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in Z[x]$ be a polynomial. If $\exists$ a prime p such that $p \mid a_i \ \forall i = 0, 1, 2, ..., n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$, then f(x) is irreducible over Q.

Example: Let us consider the polynomial $f(x) = x^3 + 6x^2 - 3x + 3 \in Z[x]$.

Then $3 \mid 3$, $3 \mid -3$, $3 \mid 6$ but 3 does not divide 1 and 3^2 does not divide 3.

Thus, f(x) is irreducible over Q.

Note: f(x) is irreducible $\Leftrightarrow$ f(x + a) is irreducible where $a \in Z$.

Theorem : Let F be an algebraic number field. If α is algebraic over F, then it has a unique minimal polynomial $m_{\alpha,F}(x)$ over F(called the minimal polynomial of α over F).

Proof : Let us assume that α is algebraic over F. So, $\exists$ a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Let $t(x) \in F[x]$ be the non-zero polynomial of smallest degree over F such that $t(\alpha) = 0$.

Let $t(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m \in F[x]$.

If t(x) is not monic then we put $p(x) = a_m^{-1}t(x) = a_m^{-1}(a_0 + a_1x + a_2x^2 + ... + a_mx^m)$

$= b_0 + b_1x + b_2x^2 + ... + x^m \in F[x]$.

Now, deg p(x) =deg t(x) and $p(\alpha) = 0$

$\Rightarrow$ p(x) is a monic polynomial of lowest degree such that $p(\alpha) = 0$.

Now, p(x) is obviously irreducible, for otherwise, we will get a polynomial h(x) of lower degree such that $h(\alpha) = 0$.

Uniqueness Let $q(x) \in F[x]$ be a monic irreducible polynomial such that $q(\alpha) = 0$.

Since F is a field, so F[x] is an Euclidean domain.

Therefore, $\exists$ unique $h(x), r(x) \in F[x]$ such that $q(x) = p(x)h(x) + r(x)$ where either deg r(x) < deg p(x) or $r(x) \equiv 0$.

Now, $r(\alpha) = 0$

If deg r(x) < deg p(x) then it contradicts the fact that p(x) is a polynomial of lowest degree satisfying $p(\alpha) = 0$.

$\Rightarrow r(x) \equiv 0$.

Thus, $q(x) = p(x)h(x)$.

As q(x) is irreducible, we have h(x) is a constant polynomial over F, say, $h(x) = a \in F$.

$\Rightarrow q(x) = ap(x)$.

Again, as q(x) is monic, we have a = 1. Thus, q(x) = p(x). This shows the uniqueness.

Theorem : Let F be an algebraic number field. If α is a root of an irreducible monic polynomial f(x) ∈ F[x], then f(x) is its minimal polynomial over F. Moreover, every polynomial in F[x] for which α is a root is divisible by $m_{\alpha,F}(x)$.

Proof.: Let us assume that α is a root of an irreducible monic polynomial f(x) over F.

To show that f(x) is the minimal polynomial of α over F.

If f(x) is not the minimal polynomial, then ∃ a polynomial g(x) over F of lowest degree such that g(α) = 0.

Now, ∃ unique polynomials h(x) and r(x) over F such that f(x) = h(x)g(x) + r(x) where either deg r(x) < deg p(x) or r(x) ≡ 0.

Since f(α) = 0 and g(α) = 0, so r(α) = 0.

If deg r(x) < deg p(x), then it contradicts the minimality of g(x). So r(x) ≡ 0.

Thus, f(x) = h(x)g(x)

As f(x) is irreducible, we have h(x) is a constant polynomial over F, say, h(x) = c ∈ F.

⇒ f(x) = cg(x).

Again, as f(x) is monic, we have c = 1.

Thus, f(x) = g(x).

Hence, f(x) is the minimal polynomial of α over F.

Moreover, if k(x) is another polynomial over F such that k(α) = 0, then we will show that k(x) is divisible by the minimal polynomial.

Let $m_{\alpha,F}(x)$ be the minimal polynomial of α over F.

Then ∃ unique polynomials $h_1(x)$ and $r_1(x)$ over F such that $k(x) = h_1(x)m_{\alpha,F}(x)+r_1(x)$ where either deg $r_1(x)$ < deg $m_{\alpha,F}(x)$ or $r_1(x) \equiv 0$.

Since k(α) = 0 and $m_{\alpha,F}(\alpha) = 0$, so $r_1(\alpha) = 0$.

If deg $r_1(x)$ < deg $m_{\alpha,F}(x)$, then it contradicts the minimality of $m_{\alpha,F}(x)$.

So, $r_1(x) \equiv 0$.

⇒ $k(x) = h_1(x)m_{\alpha,F}(x)$.

⇒ $m_{\alpha,F}(x) \mid k(x)$.

Theorem: An irreducible polynomial over an algebraic number field has no repeated root in C.

Proof: Let F be an algebraic number field and let f be an irreducible polynomial over F. If possible we consider f as $f(x) = a(x-\alpha)^2 g(x)$ where α ∈ C, a ∈ F and g(x) ∈ F[x].

Then f(α) = 0

⇒ $m_{\alpha,F}(x) \mid f(x)$

⇒ $f(x) = bm_{\alpha,F}(x)$ (since f is irreducible).

Thus, $\deg f(x) = \deg m_{\alpha,F}(x)$.

Now, $f'(x) = 2a(x-\alpha)g(x) + a(x-\alpha)^2 g'(x)$

⇒ $f'(\alpha) = 0$ ⇒ $m_{\alpha,F}(x) \mid f'(x)$ ⇒ $f(x) \mid f'(x)$ and deg $m_{\alpha,F}(x)$

Embedding and Point-wise fixing

Let F is a number field. Then an embedding $\Theta : F \to C$ be a ring monomorphism. If $L \subseteq F$ be an extension of Q and $\Theta : F \to C$ is an embedding such that $\Theta(l) = l$ for all $l \in L$, then Θ fixes L pointwise.

In this case Θ is called an L – isomorphism.

Note: If F is an algebraic number field and $\Theta : F \to C$ is an embedding then $\Theta(q) = q$ for all $q \in Q$. That is Θ fixes Q point wise .

Theorem: (The number of Embeddings of number fields)

If $F = Q(\alpha)$ is an algebraic number field of degree d over Q, then there exists exactly d embeddings Θ_j for j = 1, 2, ……, d of F in C.

Furthermore, all of the conjugates of α over Q are the $\Theta_j(\alpha) = \alpha_j$ with $\alpha_1 = \alpha$, and these are precisely the roots of the minimal polynomial $m_{\alpha,Q(x)}$ of α over Q.

Proof: Let $\Theta : F \to C$ be an embedding such that $\Theta(\alpha) = \beta$.

Let $m_{\alpha,Q}(x) = q_0 + q_1x + q_2x^2+\ldots\ldots+x^d \in [x]$.

Then $m_{\alpha,Q}(\alpha) = q_0 + q_1\alpha + q_2\alpha^2+\ldots\ldots+\alpha^d = 0$ ……(1)

Now since Θ is an embedding so we have $\Theta(0) = 0$.

Now, since Θ is an embedding so we have $\Theta(0) = 0$.

- ⇨ $0 = \Theta(0) = \Theta(q_0 + q_1\alpha + q_2\alpha^2+\ldots\ldots+\alpha^d)$
- ⇨ $0 = q_0 + q_1\,\Theta(\alpha) + q_2\,\Theta(\alpha^2)+\ldots\ldots+\Theta(\alpha^d)$
- ⇨ $0 = q_0 + q_1\beta + q_2\beta^2+\ldots\ldots+\beta^d$
- ⇨ $\beta = \alpha_j$, for some j, where $1 \leq j \leq d$

where $\alpha1\ (\alpha)$, $\alpha2$, $\alpha3$, ……., αj are positive roots of $m_{\alpha,Q}(x)$.

Thus there are at most d emdeddings of F in C.

Next, let $\Theta_j : F \to C$ be defined as

$\Theta_j(f(\alpha)) = f(\alpha_j)$, j = 1, 2, …., d where $f(x) \in F[x]$.

Now, let $f(\alpha) = g(\alpha)$ for

§ NUMBER FIELDS

Definition. A number field F is a finite field extension of Q. The dimension of F as a Q-vector space is called the degree of F. It is denoted by [F : Q].

For example

$$\mathbf{Q}, \mathbf{Q}(i), \mathbf{Q}(\sqrt[4]{2}), \mathbf{Q}(\sqrt[3]{3}, \sqrt{7}) \text{ and } \mathbf{Q}(\sqrt{2}, \sqrt{1+\sqrt{2}})$$

Are number fields of degrees 1, 2, 4, 6 and 4 respectively. The following theorem says that every number field can be generated by one element only. This element is by no means unique.

So an algebraic number field (or just number field) is a subfield $K \subset C$ which is of finite dimension as a vector space over Q.

This dimension is called the degree of the number field: deg K = dim [K:Q] = $\dim_Q$ K.

Proposition: If K is a number field then each $\alpha \in K$ is an algebraic number of degree $\leq$ deg K.

Proof: Consider the d + 1 elements 1, $\alpha, \ldots, \alpha^d$. where d = deg K.

These elements must be linearly dependent over Q, say $a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0$, with $a_i \in Q$. Thus α satisfies an equation of degree $\leq d$ over Q.

It follows that any number field K is sandwiched between Q and $\overline{Q}$: $Q \subset K \subset \overline{Q}$.

Proposition: Suppose α is an algebraic number of degree d. Then the elements $\beta = f(\alpha)$, where $f(x) \in Q[x]$, form a number field K of degree d, with basis $1, \alpha, \ldots, \alpha^{d-1}$.

Proof . It is clear that K is closed under addition and multiplication.

To see that it is closed under inversion, suppose $\beta \in K$, $\beta \neq 0$.

Consider the map $\theta : \gamma \to \beta\gamma : k \to k$.

This is a linear map over Q.

Moreover it is injective since $\theta(\gamma) = 0 \Rightarrow \beta\gamma = 0 \Rightarrow \gamma = 0$.

But a linear transformation $\varphi : V \to V$ of a finite-dimensional vector space V is surjective if and only if it is injective.

Thus $\theta : k \to k$ is surjective; and in particular $\beta\gamma = 1$ for some $\gamma \in K$, ie $\beta - 1 \in K$.

Suppose $\beta = f(\alpha)$, where $f(x) \in Q[x]$. Divide f(x) by the minimal polynomial m(x) of α, say f(x) = m(x)q(x) + r(x), where deg r(x) $\leq$ d = deg m(x).

Then $\beta = f(\alpha) = r(\alpha)$

Thus $\beta = c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}$.

Hence the d elements $1, \alpha, \ldots, \alpha^{d-1}$ span k;

and they are linearly independent since otherwise α would satisfy an equation of degree < d.

So these elements form a basis for K; and consequently deg k = d. ■

It is evident that this is the smallest number field containing α, since such a field must contain all numbers of the form $f(\alpha)$.

Definition : We say that the field K is generated by α, and denote it by $Q(\alpha)$.

A number field of the form $K = Q(\alpha)$ is sometimes said to be simple, although the Theorem below makes this definition somewhat superfluous. But first we note that the notion of extending Q to the number field $Q(\alpha)$ applies equally with any number field k in place of Q

Proposition: Suppose K is a number field of degree d; and suppose $\beta \in \overline{Q}$. Then β satisfies an equation $m(x) \in K[x]$ of minimal degree e, and the numbers $\gamma = f(\beta)$, with $f(x) \in K[x]$, form a number field K of degree deg K = de.

Lemma: Suppose $K = Q(\alpha)$. Then the de elements $\alpha_i\beta_j$ $(0 \leq i < d, 0 \leq j < e)$ form a basis for K over Q.

Proof : Each element $\gamma \in K$ is uniquely expressible in the form $\gamma = \alpha_0 + \alpha_1\beta + \cdots + \alpha_{d-1}\beta_{e-1}$, with $\alpha_i \in K = Q(\alpha)$.

But each α_i is uniquely expressible as a polynomial $f_i(\alpha)$, where $f_i(x) \in Q[x]$ is of degree < d.

It follows that γ is uniquely expressible as a linear combination of the de elements $\alpha_i\beta_j$.

Corollary: If L ⊂ K is a subfield of the number field K, then L is a number field, and deg L | deg K.

Theorem. (Theorem of the primitive element.) Let F be a finite extension of Q. Then there exists α ∈ F such that F = Q(α).

Proof. It suffices to consider the case where F = Q(α, β). The general case follows by induction. We must show that there is an element θ ∈ F such that Q(α, β) = Q(θ). We will take for θ a suitable linear combination of α and β: let $f(T) = f_{min}^{\alpha}(T)$ the minimum polynomial of α over Q. Let n = deg(f) and let α = α1, α2, . . . , αn be the zeroes of f in C. The αi are all distinct. Similarly we let g(T) = f β min(T) the minimum polynomial of β over Q. Let m = deg(g) and let β = β1, β2, . . . , βm be the zeroes of g in C. Since Q is an infinite field, we can find λ ∈ Q∗ such that

$$\lambda \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$
$$\text{for } 1 \leq i \leq n \text{ and for } 2 \leq j \leq m\,,$$

Or equivalently

$$\alpha + \lambda\beta \neq \alpha_i + \lambda\beta_j \text{ for } 1 \leq i \leq n \text{ and for } 2 \leq j \leq m$$

Put θ = α + λβ.

The polynomials h(T) = f(θ − λT) and g(T) are both in Q(θ)[T] and they both have β as a zero. The remaining zeroes of g(T) are $\beta_2, \ldots, \beta_m$ and those of h(T) are $(\theta - \alpha_i)/\lambda$ for $2 \leq i \leq n$. By our choice of λ, we have that $\beta_j \neq (\theta - \alpha_i)/\lambda$ for all $1 \leq i \leq n$ and $2 \leq j \leq m$. Therefore the gcd of h(T) and g(T) is T −β. Since g(T), h(T) are monic poynomials in Q(θ)[T] we have that T −β ∈ Q(θ)[T]. This implies that β ∈ Q(θ) and hence that α ∈ Q(θ). It follows that Q(α, β) = Q(θ) as required.

Corollary - Let F be a finite extension of degree n of Q. There are exactly n distinct field homomorphisms $\varphi : F \to C$.

Proof. We can write $F = \boldsymbol{Q(\alpha)}$ for some α. Let f be the minimum polynomial of α over Q.

A homomorphism φ from F to C induces the identity on Q . Therefore it is determined by the image $\varphi(\alpha)$ of α. We have that $0 = \varphi(f(\alpha)) = f(\varphi(\alpha))$. In other words, $\varphi(\alpha)$ is a zero of $f(T)$.

Conversely, every zero $\beta \in C$ of $f(T)$ gives rise to a homomorphism $\varphi : F \to C$ given by $\varphi(\alpha) = \beta$. This shows that there are exactly as many distinct homomorphism $F \longrightarrow C$ as the degree n of f, as required.

Proposition - Let F be a number field of degree n over Q. Let $\omega_1, \ldots, \omega_n \in F$.

Then $\omega_1, \ldots, \omega_n$ form a basis for F as a Q-vector space if and only if $\det(\varphi(\omega_i))_{\varphi,i} \neq 0$. Here i runs from 1 to n and φ runs over all homomorphisms $\varphi : F \to C$.

Proof. First of all, note that the matrix $(\varphi(\omega_i))_{\varphi,i}$ is a square matrix. Suppose that there exists a relation $\sum_i \lambda_i\omega_i = 0$ with $\lambda_i \in Q$ not all zero. Since $\varphi(\lambda) = \lambda$ for every $\lambda \in Q$, we see that $\sum_i \lambda_i\omega_i = 0$ for every $\varphi : F \to C$. This implies that $\det\left(\phi(\omega_i)\right)_{\phi,i} = 0$

To prove the converse, we write $F = Q(\alpha)$ for some α. Consider the Q-basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. For this basis the matrix $\left(\phi(\omega_i)\right)_{\phi,i} = \left(\phi(\alpha)^{i-1}\right)\Big)_{\phi,i}$ is a Vandermonde matrix with determinant equal to a product of terms of the form $(\varphi_1(\alpha) - \varphi_2(\alpha))$ with $\varphi_1 \neq \varphi_2$. Since the zeroes $\varphi(\alpha) \in C$ of the

minimum polynomial of α are all distinct, this determinant is not zero. So, for the basis 1, α, α^2 , . . . , α^{n-1} the theorem is valid. For an arbitrary Q-basis ω_1, . . . , ω_n there exists a matrix $M \in GL_n(Q)$ such that

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = M \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}$$

applying the homomorphisms $\varphi : F \to C$ one obtains the following equality of $n \times n$ matrices:

$$\left(\phi(\omega_i)\right)_{\phi,i} = M \cdot \left(\phi\left(\alpha^i\right)\right)_{\phi,i},$$

and therefore

$$\det\left(\left(\phi(\omega_i)\right)_{\phi,i}\right) = \det(M) \cdot \det\left(\left(\phi\left(\alpha^i\right)\right)_{\phi,i}\right) \neq 0$$

as required. This proves the proposition.

Note: The number field Q admits a unique embedding into the field of complex numbers C. The image of this embedding is contained in R. In general, a number field F admits several embeddings in C, and the images of these embeddings are not necessarily contained in R. We generalize the embedding $\Phi : Q \to R$ as follows.

Let F be a number field and let $\alpha \in F$ be such that $F = Q(\alpha)$. In other words $F = Q[T]/(f(T))$ where f(T) denotes the minimum polynomial of α. Let $n = \deg(f)$.

We put $F \otimes R = R[T]/(f(T))$.

In these notes, $F \otimes R$ is just our notation for the R-algebra R[T]/(f(T)). This algebra is actually the tensor product of F over Q with R and this also shows that the construction does not depend on the choice of α, but we will not use this interpretation. The natural map $Q[T]/(f(T)) \longrightarrow R[T]/(f(T))$ gives us a map $\Phi : F \to F \otimes R$.

We compute the ring $F \otimes R$ explicitly: since C is an algebraically closed field, the polynomial $f(T) \in Q[T]$ factors completely over C. Let's say it has precisely m real zeroes $\beta_1, \ldots, \beta_m$ and w pairs of complex conjugate zeroes $\gamma_1, \bar{\gamma_1}, \ldots, \gamma_w, \bar{\gamma_w}$.

We have $m + 2w = n$.

The numbers m and n depend only on the number field F and not on the choice of α. By the Chinese Remainder Theorem there is an isomorphism

$$F \otimes R \cong R^m \times C^w$$

given by $T \to (\beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_w)$. Identifying the spaces $F \otimes R$ and $R^m \times C^w$ by means of this isomorphism, we obtain an explicit description of the map Φ.

Definition. Let F be a number field. With the notation above, the map Φ

$\Phi : F \to R^m \times C^w$ is defined by $\Phi(x) = (\varphi_1(x), \ldots, \varphi_m(x), \varphi_{m+1}(x), \ldots, \varphi_{w+m}(x))$

where the $\varphi_i : F \to C$ are determined by $\varphi_i(\alpha) = \beta_i$ for $1 \le i \le m$ and $\varphi_{m+i}(\alpha) = \gamma_i$ for $1 \le i \le w$.

Example. Let $\alpha = 2^{\frac{1}{4}}$ be a zero of $T^4 - 2 \in Q[T]$ and let $F = Q(\alpha)$.

The minimum polynomial of α is $T^4 - 2$. It has two real roots $\pm 2^{\frac{1}{4}}$ and two complex conjugate roots $\pm i\, 2^{\frac{1}{4}}$. We conclude that m = 2 and w = 1. The homomorphisms $\varphi_i : F \to C$ are determined by

$\varphi_1(\alpha) = 2^{\frac{1}{4}}$, $\varphi_2(\alpha) = -2^{\frac{1}{4}}$, $\varphi_3(\alpha) = i\, 2^{\frac{1}{4}}$, $\varphi_4(\alpha) = -i\, 2^{\frac{1}{4}}$.

The map $\Phi : F \to F \otimes R = R \times R \times C$ is, given by $\Phi(x) = (\varphi_1(x), \varphi_2(x), \varphi_3(x))$.

§ Traces and norms:

Definition: Let L/K be a finite extension of fields, and $x \in L$. We view L as a finite dimensional K-vector space, and denote by $\varphi_x : L \to L$ the K-linear endomorphism on L defined by the multiplication by x.

We have $\varphi_x \in \mathrm{End}_K(L)$.

We put $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(\varphi_x)$, and call it the trace of x (relative to L/K);

put $N_{L/K}(x) = \det(\varphi_x)$, and call it the norm of x (relative to L/K).

We suppose that K is a number field.

Suppose $\beta \in K$. Let μ_β denote the map $\gamma \to \beta\gamma : K \to K$. This is a linear map over Q.

Let $A \subset B$ be rings such that B is a free A-module of rank n. Then every $\beta \in B$ defines an A-linear map from B to B as $x \to \beta x$; and the trace and norm (determinant) of this map are well-defined.

We call them the trace $\mathrm{Tr}_{B/A}\,\beta$ and norm $N_{B/A}\,\beta$ of β in the extension B/A.

Thus if $\{e_1, \ldots, e_n\}$ is a basis for B over A, and $\beta e_i = \sum a_{ij} e_j$,

then $\mathrm{Tr}_{B/A}(\beta) = \sum a_{ii}$ and $N_{B/A}(\beta) = \det(a_{ij})$

When $B \supset A$ is a finite field extension, this agrees with the usual definition.

The following hold for $a \in A$, $\beta, \beta' \in B$

$\mathrm{Tr}_{B/A}(\beta + \beta') = \mathrm{Tr}_{B/A}(\beta) + \mathrm{Tr}_{B/A}(\beta')$ $\qquad$ $N_{B/A}(\beta\,\beta') = N_{B/A}(\beta)\, N_{B/A}(\beta')$

$\mathrm{Tr}_{B/A}(a\beta) = a\,\mathrm{Tr}_{B/A}(\beta)$ $\qquad$ $N_{B/A}(a) = a^n$

$\mathrm{Tr}_{B/A}(a) = na$

PROPOSITION : Let L/K be an extension of fields of degree n, and let $\beta \in L$.

Let f (X) be the minimal polynomial of β over K and let $\beta_1 = \beta, \beta_2, \ldots, \beta_m$, be the roots of f (X).

Then $\mathrm{Tr}_{L/K}(\beta) = r.(\beta_1 + \beta_2 + \ldots + \beta_m)$ and $N_{L/K}(\beta) = (\beta_1.\, \beta_2.\, \ldots.\, \beta_m)^r$;

where $r = [L : K[\beta]] = n/m$

We may set $\quad S(\beta) = \mathrm{tr}\ \mu_\beta$,

$N(\beta) = \det \mu_\beta$.

We call $S(\beta)$, $N(\beta)$ the trace and norm of $\beta \in K$.

Evidently, $S(\beta)$, $N(\beta) \in Q$.

The following results are immediate

Propositions:

1. $S(\beta + \gamma) = S(\beta) + S(\gamma)$;

2. $N(\beta\gamma) = N(\beta)\, N(\gamma)$;

3. if $c \in K$ then $S(c) = dc$, $N(c) = c^d$.

There is an alternative way of looking at the trace (or spur) and norm, in terms of conjugates.

If L, K are two fields then any ring homomorphism $\theta : L \to K$ is necessarily injective; for if $c \in L$ is non-zero then

$$c \in \ker \theta \Rightarrow f(c) = 0$$

$$\Rightarrow f(1) = f(cc^{-1}) = f(c)f(c^{-1}) = 0,$$

while $f(1) = 1$ by definition.

Suppose L is a number field, and K = C.

We may say that θ defines an embedding of L in C.

We want to see in how many ways the number field $L = Q(\alpha)$ can be embedded in C.

Suppose m(x) is the minimal polynomial of α.

Let the roots of m(x) be $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$, so that $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

Note that the roots are distinct, since m(x) is irreducible.

For if there was a multiple root it would also be a root of $m'(x)$, and then

$f(x) = \gcd(m(x), m'(x))$ would be a non-trivial factor of m(x).

Proposition :

Suppose $L = Q(\alpha)$ is a number field of degree d,

Then there are just d ring homomorphisms $\sigma_i : L \to C$, given by

$$\sigma_i : f(\alpha) \to f(\alpha_i) \quad (f(x) \in Q[x]) \text{ for } i = 1, \ldots, d.$$

Proof : If $\alpha \to \alpha'$ then $m(\alpha) = 0$

$$\Rightarrow m(\alpha') = 0.$$

Hence $\alpha' = \alpha_i$ for some i; and so

$$f(\alpha) \to f(\alpha_i).$$

This map is well-defined, since $f(\alpha) = g(\alpha) \Rightarrow m(x) \mid f(x) - g(x)$

$$\Rightarrow f(\alpha_i) = g(\alpha_i);$$

and it is evident that it is a ring-homomorphism. ■

In other words, there are just d = deg L embeddings of the number field L in C.

Note that this result is independent of the choice of generator α; it is a property of the field L itself.