FUNDAMENTAL UNITS IN QUADRATIC FIELDS

THESIS SUBMITTED IN PARTIAL
FULFILMENT OF THE REQUIREMENTS
FOR
THE AWARD OF THE M.SC. DEGREE

BY

EMIL SOBHY SAAD

SUBMITTED AT
AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE

AUGUST 1982

M.SC. COURSES

STUDIED BY THE AUTHOR (FEB, 1979-FEB, 1980)
(AT AIN SHAMS UNIVERSITY)

(i) Functional analysis I
2 hours weekly for one semister.

(ii) Functional analysis II
2 hours weekly for one semister.

(iii) Functional analysis III
2 hours weekly for one semister.

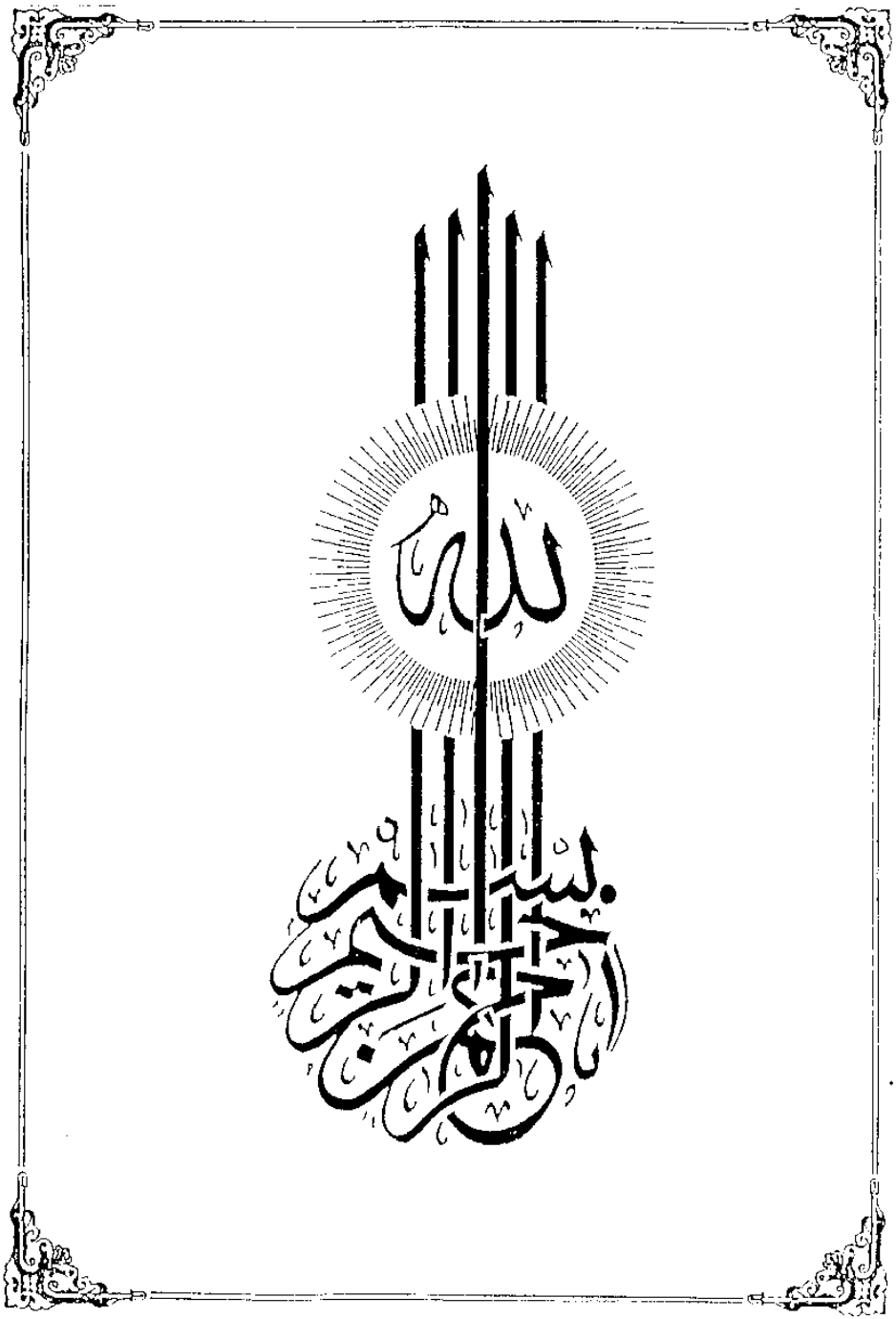
(iv) Algebraic topology
2 hours weekly for two semisters.

(v) Differential topology
2 hours weekly for one semister.

(vi) Ordinary differential equations
2 hours weekly for one semister.

(vii) Numerical treatment of matrices
2 hours weekly for one semister.

(viii) Theory of functions of matrices
2 hours weekly for one semister.



CONTENTS

Page

CHAPTER I

ALGEBRAIC NUMBER FIELDS

In this chapter we introduce the concept of an algebraic number field, and give some of its characteristics; in particular the ring of integers in an algebraic number field, the group of units in this ring, and Dirichlet's theorem concerning this group of units.

1. Finite extension fields

In this section we shall be concerned with the relation of one field to another. Let F be a field; a field K is said to be an extension of F if K contains F. Equivalently, K is an extension of F if F is a subfield of K, and we denote this by K/F.

If K is an extension of F, then under the ordinary field operations in K, K is a vector space over F.

Let $\phi_1, \phi_2, \ldots, \phi_r$ be elements of K, with the property that $A_1\phi_1 + A_2\phi_2 + \ldots + A_r\phi_r = 0$, $A_i \in F$ cannot hold, unless $A_1 = A_2 = \ldots = A_r = 0$; then the ϕ_i's are said to be linearly independent over F. If in addition to this property the ϕ_i's span the field K, that is, each element $\alpha \in K$ can be represented as a linear combination of the ϕ_i's, i.e., $\alpha = A_1\phi_1 + A_2\phi_2 + \ldots + A_r\phi_r$, $A_i \in F$, then the set $\{\phi_i, i = 1,2, \ldots, r\}$ is said to form a basis of K over F.

DEFINITION (1): The extension K/F is called finite if K considered as a vector space over F, is finite - dimensional, i.e., K has a finite number of elements as a basis over F. The degree of K/F is the dimension of K as a vector space over F, and is denoted by $[K:F]$.

2. Algebraic number fields

By an algebraic number field K, we shall mean a finite extension of Q, the field of rational numbers.

DEFINITION (2): A number θ is said to be an algebraic number if it is algebraic over Q, the field of rational numbers i.e., θ satisfies a non-zero polynomial equation $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_o = o$, with coefficients in Q.

THEOREM (1): An algebraic number θ satisfies a unique irreducible monic polynomial equation $g(x) = o$ over Q. Furthermore every polynomial equation over Q satisfied by θ is divisible by $g(x)$.

PROOF: From all polynomial equations over Q satisfied by θ, choose one of lowest degree, say $G(x) = o$. If the leading coefficient of $G(x)$ is c, define $g(x) = c^{-1} G(x)$, so that $g(\theta) = o$ and $g(x)$ is monic. The polynomial $g(x)$ is irreducible, for if $g(x) = h_1(x)h_2(x)$, then one at least of $h_1(x) = o$ and $h_2(x) = o$ would hold, contrary to the fact that $G(x) = o$ and $g(x) = o$ are polynomial equations over Q of least degree satisfied by θ.

Next let $f(x) = o$ be any polynomial equation over Q having θ as a root. Since we can get $f(x) = g(x)\ q(x) + r(x)$, the remainder $r(x)$ must be identically zero, for otherwise the degree of $r(x)$ would be less than that of $g(x)$, and θ would be a root of $r(x)$ since $f(\theta) = g(\theta) = 0$. Hence $g(x)$ is a divisor of $f(x)$.

Finally to prove that $g(x)$ is unique, suppose that $g_1(x)$ is an irreducible polynomial such that $g_1(\theta) = 0$. Then $g(x) \mid g_1(x)$, say, $g_1(x) = g(x)\ q(x)$. But the irreducibility of $g_1(x)$ then implies that $q(x)$ is a constant, in fact $q(x) = 1$ since $g_1(x)$ and $g(x)$ are monic. Thus we have $g_1(x) = g(x)$.

The irreducible polynomial $g(x)$ is the minimal polynomial of θ and the degree of θ as an algebraic number is the degree of its minimal polynomial.

THEOREM (2): If θ is an algebraic number of degree n, then, the set $\left\{A_o + A_1\theta + A_2\theta^2 + \ldots + A_{n-1}\ \theta^{n-1};\ A_j \in Q\right\}$ forms a field denoted by $Q(\theta)$, whose degree over Q is n.

PROOF: Let the minimal polynomial of the algebraic number θ be $p(x) = x^n + B_{n-1}\ x^{n-1} + B_{n-2}x^{n-2} + \ldots + B_o;\ B_j \in Q$. Then $\theta^n = -(B_o + B_1\theta + B_2\theta^2 + \ldots + B_{n-1}\theta^{n-1})$. It follows that every polynomial in θ can be reduced to a polynomial of degree at most (n-1). The set $\left\{A_o + A_1\theta + A_2\theta^2 + \ldots + A_{n-1}\theta^{n-1};\ A_j \in Q\right\}$ forms a field usually denoted by $Q(\theta)$. All verifications that

$Q(\theta)$ is a field are trivial, except the existence of an inverse. Given $\alpha = \sum_{j=0}^{n-1} A_j \theta^j = g(\theta) \in Q(\theta)$, one has to show that $\alpha^{-1} \in Q(\theta)$. Since the degree of $g(x) \leq n-1$ and the degree of $p(x) = n$, then the irreducibility of $p(x)$ implies that $g(x)$ and $q(x)$ are coprime, i.e., $(g(x), q(x)) = 1$. Hence there exist polynomials $s(x)$ and $t(x)$ such that $s(x)p(x)+t(x)g(x) = 1$, (see [3], p/283) replacing here x by θ, $p(\theta) = o$, and we get $t(\theta)g(\theta) = 1$ or $\alpha^{-1} = \frac{1}{g(\theta)} = t(\theta) \in Q(\theta)$. The representation $\alpha = g(\theta)$ is unique, otherwise, $\alpha = g_1(\theta) = g_2(\theta)$ implies that $h(\theta) = g_1(\theta) - g_2(\theta) = 0$, i.e., θ satisfies the polynomial $h(x) = g_1(x) - g_2(x)$. But θ satisfies no polynomial of degree less than n. Then it follows that $h(x)$ is identically zero, $g_1(\theta) = g_2(\theta)$. This argument tells us that the set $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis of the field $Q(\theta)$ over Q where $[Q(\theta):Q] = n$.

One can see that $Q(\theta)$ is the smallest field containing both Q and θ. The field $Q(\theta)$ is called a simple extension of Q.

DEFINITION (3): Let $\theta_1, \theta_2, \ldots, \theta_n$ be the different roots of the minimal polynomial equation $p(x) = o$, satisfied by θ. These roots are called the conjugates of θ.

Since the coefficients of $p(x)$ are real then any imaginary root θ_i has paired with it a complex - conjugate root θ_j. Let s be the number of real roots and 2t the number of imaginary

roots. Since the degree of $Q(\theta)$ is n, then $n=s+2t$.

3. The ring of algebraic integers $Z[Q(\theta)]$

An algebraic number θ is an algebraic integer if it satisfies some monic polynomial equation

$$f(x) = x^n + b_1 x^{n-1} + \ldots + b_n = o,$$

with its coefficients belonging to Z, the ring of rational integers. It is easily seen that the roots $\theta = \theta_1, \theta_2, \ldots, \theta_n$ of $f(x) = o$ are algebraic integers.

THEOREM (3): In the set of rational numbers Q, the only ones that are algebraic integers are the rational integers $\{0, \pm 1, \pm 2, \ldots\}$.

PROOF: Any integer m is an algebraic integer because f(x) can be taken as x-m. On the otherhand, if any rational number m/q is an algebraic integer, then we may suppose (m,q) = 1, and we have

$$\left(\frac{m}{q}\right)^n + b_1\left(\frac{m}{q}\right)^{n-1} + \ldots + b_n = o,$$

$$m^n + b_1 q m^{n-1} + \ldots + b_n q^n = o,$$

$$\frac{m^n}{q} = -\left(b_1 m^{n-1} + b_2 q m^{n-2} + \ldots + b_n q^{n-1}\right).$$

Thus $q \mid m^n$, so that $q = \pm 1$, and m is an integer.

THEOREM (4): The minimal equation of an algebraic integer is monic with integral coefficients.

PROOF: The minimal equation is monic by definition, so we need to prove that the coefficients are integers. Let the algebraic integer θ satisfy $f(x) = o$, where $f(x)=x^n+b_1x^{n-1}+ \ldots + b_n$, $b_i \in Z$, and let its minimal equation be $g(x) = o$, monic and irreducible over Q. By theorem (1) $g(x)$ is a divisor of $f(x)$, say, $f(x) = g(x)\, h(x)$, and $h(x)$ is monic and has coefficients in Q. Let c,c' be the least positive integers such that $cg(x)$ and $c'h(x)$ have integral coefficients. Then $cg(x)$ and $c'h(x)$ are primitive polynomials, i.e., the coefficients have no common factors other than 1. Thus $cc'g(x)h(x)$ is primitive, (see [5], p/59) and hence $cc'f(x)$ is primitive. Since $f(x)$ is primitive, then $cc'=1$ and $c=c'=1$ which implies that $g(x)$ has integral coefficients.

DEFINITION (4): Let α be an integer in $Q(\theta)$, and $Q(\theta)$ be of degree n over Q. Then α has the form

$$\alpha = a_o + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1} = r(\theta).$$

If $\theta = \theta_1, \theta_2, \ldots, \theta_n$ are the conjugates of θ over Q, then the numbers:

$$\alpha_i = r(\theta_i) \quad , \quad i = 1,2, \ldots , n$$

are called the field conjugates of α for the field $Q(\theta)$.

THEOREM (5): The algebraic integers of the algebraic number field $Q(\theta)$ form a ring denoted by $Z[Q(\theta)]$.

PROOF: Let α and β be algebraic integers whose field conjugates are $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_n$ respectively, and consider the polynomials $f(x)$ and $g(x)$ such that

$$f(x) = \prod_{j=1}^{n} (x - \alpha_j \beta_j) \quad \text{and} \quad g(x) = \prod_{j=1}^{n} (x - (\alpha_j + \beta_j)).$$

The coefficients of both, $f(x)$ and $g(x)$, are symmetric polynomials with integral coefficients in the conjugates of both, α and β, and hence, by the theorem on symmetric functions (see [3], p/78), in the coefficients of the field polynomials for α and β. Consequently, they are rational, and being also integers, are rational integers, so that $f(x)$, $g(x)$ are polynomials with integral coefficients. Also $f(x)$ and $g(x)$ are both monic, so that $\alpha + \beta$ (and its conjugates) and $\alpha\beta$ (and its conjugates) are algebraic integers. In fact, this ring of integers, $Z[Q(\theta)]$, is the maximal ring of integers in $Q(\theta)$.

4. The units of the ring of integers $Z[Q(\theta)]$

Let α and $\beta \neq o$ be two elements of $Z[Q(\theta)]$ in the algebraic number field $Q(\theta)$. Then we say that α divides β, and write $\alpha \mid \beta$, if β/α is an integer of $Z[Q(\theta)]$. An element $\xi \in Z[Q(\theta)]$, is a unit if it divides the integer 1, which means that the multiplication inverse $1/\xi$ of ξ belongs to $Z[Q(\theta)]$. Two integers α and β are associates if α/β is a unit.

Let α be an integer in $Q(\theta)$ which is of degree n over Q, and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the field conjugates of α for $Q(\theta)$. We define the norm of α, written $N(\alpha)$, by

$$N(\alpha) = \alpha_1 \ldots \alpha_n .$$

Note that $N(\alpha)$ depends on the field $Q(\theta)$. For example $N(2) = 2$ in Q, but $N(2) = 4$ in $Q(i)$.

LEMMA (6): $N(\alpha)$ is a rational integer.

PROOF: Let $f(x)$ be the field polynomial of α; i.e., $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the field conjugates of α for $f(x)$. Since $f(x)$ is a power of the minimal polynomial (see [7], p/65) it has integral coefficients. Hence

$$f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_o$$

$$= (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

where b_o is a rational integer. Then

$$N(\alpha) = \alpha_1 \ldots \alpha_n$$

$$= (-1)^n b_o .$$

LEMMA (7): $N(\alpha\beta) = N(\alpha).N(\beta)$.

PROOF: If $\alpha_1, \alpha_2, \ldots, \alpha_n$; $\beta_1, \beta_2, \ldots, \beta_n$ are the field conjugates of α and β respectively for $Q(\theta)$, then

$$\alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_n\beta_n$$

are the conjugates of $\alpha\beta$ for $Q(\theta)$. Hence

$$N(\alpha\beta) = \alpha_1\beta_1 \cdot \alpha_2\beta_2 \cdot \ldots \cdot \alpha_n\beta_n$$

$$= \alpha_1\alpha_2 \ldots \alpha_n \cdot \beta_1\beta_2 \cdots \beta_n$$

$$= N(\alpha) \cdot N(\beta).$$

THEOREM(8): $\xi \in Z[Q(\theta)]$ is a unit if and only if $N(\xi) = \pm 1$.

PROOF: We first show that for any $\xi \neq o$ of $Z[Q(\theta)]$, the norm $N(\xi)$ is divisible by ξ. The minimal polynomial

$$f(x) = x^n + b_1x^{n-1} + \ldots + b_n$$

of ξ has integral coefficients. Since $f(\xi) = o$, then $N(\xi)/\xi$ lies in $Z[Q(\theta)]$, which means that $N(\xi)$ is divisible by ξ.

Now if $N(\xi) = \pm 1$, then 1 is divisible by ξ, that is ξ is a unit of $Z[Q(\theta)]$. Conversely, if ξ is a unit of $Z[Q(\theta)]$, so that $\xi\xi' = 1$ for some $\xi' \in Z[Q(\theta)]$, then since $N(\xi)$ and $N(\xi')$ are rational integers, the equation $N(\xi)\,N(\xi') = 1$ implies that $N(\xi) = \pm 1$.

THEOREM (9): The units of the ring $Z[Q(\theta)]$ form an Abelian group under multiplication.

PROOF: Let U be the set of all units of $Z[Q(\theta)]$. It is obvious that $1 \in U$ and is the identity element of U. Now if $\xi \in U$, this implies that there is $\xi' \in Z[Q(\theta)]$ such

that $\xi\xi' = 1$, hence $\xi' \in U$. Thus the inverse of a unit belongs to U. If $\xi \in U$ and $\eta \in U$, then $\xi\xi' = 1$ and $\eta\eta' = 1$ where $\xi', \eta' \in U$. But then $\xi\eta(\xi'\eta') = 1$, and this means that $\xi\eta \in U$, i.e., U is closed under multiplication. Associativity and commutativity are satisfied in U because, they are satisfied in $Z[Q(\theta)]$.

Dirichlet (1846) gave in his celebrated units theorem a complete description for the structure of the group of units in the algebraic number field.

5. Dirichlet's theorem

If the field $K = Q(\theta)$ is of degree n, where $n = s+2t$, then there exist units $\xi_1, \xi_2, \ldots, \xi_r$ where $r = s+t-1$, such that every unit $\xi \in Z[Q(\theta)]$ has a unique representation in the form

$$\xi = \gamma \xi_1^{\alpha_1} \xi_2^{\alpha_2} \ldots \xi_r^{\alpha_r}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are rational integers and γ is some root of 1 contained in $Z[Q(\theta)]$.

The units $\xi_1, \ldots, \xi_r$, whose existence is established by Dirichlet's theorem are called fundamental units for the algebraic number field. The proof of Dirichlet's theorem is not effective in that it does not give an algorithm for finding some set of fundamental units for the algebraic number field.