Vector spaces of countable dimension over algebraic number fields
by Leon Eugene Mattics

A thesis submitted to the Graduate Faculty in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY in Mathematics
Montana State University
© Copyright by Leon Eugene Mattics (1967)

Abstract:
An investigation of denumerably infinite dimensional vector spaces over algebraic number fields
supplied with non-degenerate Hermitian forms is undertaken. The Hermitian forms are divided into
Glasses according to the underlying field automorphisms. If K is a field and ζ is an automorphism such
that (Formula not captured by OCR) then &sigma; is called weakly orthonormal (orthonormal) if and
only if every denumerably infinite-dimensional K -vector space supplied by a non-degenerate form out
of the class of Hermitian forms of ζ has a (Formula not captured by OCR) orthogonal basis (an
orthonormal basis). A field &Kappa; is called weakly orthonormal (orthonormal) if and only if
(Formula not captured by OCR) is weakly orthonormal (orthonormal). Finite extensions of orthonormal
fields are orthonormal fields.

By the Hasse-Minkowski theory of quadratic forms, the algebraic extensions of the rationale which are
orthonormal are precisely the non-formally real algebraic extensions. The weakly orthonormal
algebraic extensions of the nationals are precisely the algebraic extensions with at most one ordering.
Over algebraic extensions of the nationals with precisely one ordering, Sylvester's theorem holds for
denumerably infinite-dimensional vector spaces supplied with symmetric non-degenerate bilinear
forms; so, such spaces are characterized by a complete set of two cardinal invariants.

Let ζ be an arbitrary automorphism over algebraic number field K with (Formula not captured by OCR)
Criteria, depending on the fixed field of ζ in K and the generator of KL over the fixed field of ζ, are
given to determine whether or not ζ is orthonormal (weakly orthonormal).
VECTOR SPACES OF COUNTABLE DIMENSION
OVER ALGEBRAIC NUMBER FIELDS

by

LEON EUGENE MATTICS

A thesis submitted to the Graduate Faculty in partial
fulfillment of the requirements for the degree

of

DOCTOR OF PHILOSOPHY

in

Mathematics

Approved:

Louis C. Barrett
Head, Major Department

Herbert Gross
Chairman, Examining Committee

Louis D. Fennell
Dean, Graduate Division

MONTANA STATE UNIVERSITY
Bozeman, Montana

June, 1967
ACKNOWLEDGMENT

The author is deeply indebted to his teacher and thesis advisor, Dr. Herbert Gross.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. ORTHONORMAL FIELDS</td>
<td>5</td>
</tr>
<tr>
<td>III. ORTHONORMAL ALGEBRAIC NUMBER FIELDS</td>
<td>10</td>
</tr>
<tr>
<td>IV. HERMITIAN FORMS</td>
<td>22</td>
</tr>
<tr>
<td>LITERATURE CITED</td>
<td>30</td>
</tr>
</tbody>
</table>
ABSTRACT

An investigation of denumerably infinite dimensional vector spaces over algebraic number fields supplied with non-degenerate Hermitian forms is undertaken. The Hermitian forms are divided into classes according to the underlying field automorphisms. If \( \mathbb{K} \) is a field and \( \sigma \) is an automorphism such that \( \sigma \circ \sigma = 1_{\mathbb{K}} \), then \( \sigma \) is called weakly orthonormal (orthonormal) if and only if every denumerably infinite-dimensional \( \mathbb{K} \)-vector space supplied by a non-degenerate form out of the class of Hermitian forms of \( \sigma \) has a orthogonal basis (an orthonormal basis). A field \( \mathbb{K} \) is called weakly orthonormal (orthonormal) if and only if \( \mathbb{K} \) is weakly orthonormal (orthonormal). Finite extensions of orthonormal fields are orthonormal fields.

By the Hasse-Minkowski theory of quadratic forms, the algebraic extensions of the rationals which are orthonormal are precisely the non-formally real algebraic extensions. The weakly orthonormal algebraic extensions of the rationals are precisely the algebraic extensions with at most one ordering. Over algebraic extensions of the rationals with precisely one ordering, Sylvester's theorem holds for denumerably infinite-dimensional vector spaces supplied with symmetric non-degenerate bilinear forms; so, such spaces are characterized by a complete set of two cardinal invariants.

Let \( \sigma \) be an arbitrary automorphism over algebraic number field \( \mathbb{K} \) with \( \sigma \circ \sigma = 1_{\mathbb{K}} \). Criteria, depending on the fixed field of \( \sigma \) in \( \mathbb{K} \) and the generator of \( \mathbb{K} \) over the fixed field of \( \sigma \), are given to determine whether or not \( \sigma \) is orthonormal (weakly orthonormal).
CHAPTER I

INTRODUCTION

Let $K$ be a commutative field and $\sigma$ an automorphism of $K$ such that the composite map $\sigma \circ \sigma$ is the identity automorphism, $1_K$, on $K$. If $\alpha$ is any element of $K$ we shall write $\sigma(\alpha) = \overline{\alpha}$. By a $(K, \sigma)$-vector space $(E, H)$ over $K$ we shall mean a vector space $E$ together with a bilinear form $H : E \times E \rightarrow K$ such that

$$H(\alpha x, \beta y) = \alpha \overline{\beta} H(x, y), \forall x, y \in E; \forall \alpha, \beta \in K; \forall x, y \in E,$$

$$H(x, y) = H(y, x), \forall x, y \in E.$$

We shall call such a form a Hermitian form over $K$ with respect to $\sigma$ and denote the class of all such $H$ by $(K, \sigma)$. If $F$ is a linear subspace of $E$, by $(F, H)$ we shall mean the subspace $F$ together with the form $H$ restricted to $F \times F$. If there is no risk of confusion, we shall write $E$ instead of $(E, H)$. It is easy to show that any automorphism $\sigma$ with $\sigma \circ \sigma = 1_K$ defines at least one Hermitian form over a $K$-vector space $E$.

A $(K, \sigma)$-vector space $(E, H)$ is called semisimple if and only if the form $H$ is non-degenerate. Given $(E, H)$ and $x \in E$ then we shall write $\|x\| = H(x, x)$ and call $\|x\|$ the length of the vector $x$. Two vectors $x$ and $y$ in a space $(E, H)$ are orthogonal if and only if $H(x, y) = 0$. We shall take the usual meanings for orthogonal basis and orthonormal basis.

If the (algebraic) dimension of $(E, H)$ is denumerably infinite, we shall write $\dim E = \aleph_0$ or $\dim (E, H) = \aleph_0$. If the dimension of $(E, H)$ is at most countable, then we know that $E$ has an orthogonal
basis with respect to $\mathcal{H}$. Attempts to classify spaces $(E, \mathcal{H})$ up to orthogonal automorphism have, for this reason, been restricted to the cases of finite and denumerable dimensions.

Again let $\sigma$ be an automorphism of a commutative field $K$ with $\sigma \circ \sigma = 1_K$. We shall say that $\sigma$ is \textit{orthonormal} if and only if every $\mathcal{N}_o$-dimensional semisimple $K$-vector space with $\mathcal{H} \in (K, \rho)$ has an orthonormal basis. If $1_K$ is orthonormal then we shall say that the field $K$ is \textit{orthonormal} (i.e., $K$ is orthonormal if and only if every $\mathcal{N}_o$-dimensional vector space $(E, \rho)$ over $K$ with a symmetric bilinear form has an orthonormal basis). We shall say that $\sigma$ is \textit{weakly orthonormal} if and only if every $\mathcal{N}_o$-dimensional semisimple vector space $(E, \mathcal{H})$ with $\mathcal{H} \in (K, \sigma)$ admits of an orthogonal decomposition, $E = F \oplus G$, such that $F$ has an orthonormal basis and $G$ has a negative orthonormal basis (i.e., an orthogonal basis $\{q_i\}$ with $\|q_i\|_2 = 1$ for all $i$). If $1_K$ is weakly orthonormal, then we shall say that $K$ is \textit{weakly orthonormal}.

In this paper we shall investigate the problem of determining the orthonormal and weakly orthonormal automorphisms of algebraic number fields. This investigation is initiated in Chapters II and III with the study of orthonormal and weakly orthonormal fields. In Chapter III we shall find a surprisingly easy answer (Theorem 3 and Corollary 8) to the classification problem for orthonormal and weakly orthonormal algebraic number fields (a problem proposed by Kaplansky) and we shall even be able to extend the classification, by the Hasse-Minkowski theory of quadratic forms, to all algebraic extensions of the rationals.
In Chapter II we shall show that finite algebraic extensions of orthonormal fields are also, orthonormal fields (Theorem 1) by use of the following theorem of Fischer and Gross:

**Theorem G:** ([27], Corollary 4, pp. 29-30) Let $K$ be a not formally real field with $\text{char } K \neq 2$. If $(E, \phi)$ is an $N_0$-dimensional $K$-vector space with a non-degenerate, symmetric bilinear form $\phi$ then $(E, \phi)$ admits of an orthonormal basis if and only if there is an $N_0$-dimensional linear subspace $F$ of $E$ such that $\phi(F \times F) = \{0\}$.

The classification problem (as regards orthonormal and weakly orthonormal fields) has a simple answer for large classes of underlying fields. This is best illustrated by a theorem of Kaplansky:

**Theorem K:** Let $K$ be a field (char $K \neq 2$) with the property that for some fixed $n$, every $n$-dimensional semisimple vector space $(E, \phi)$ with $\phi \in (K, I_K)$ has a vector of length $+1$ or $-1$ then $K$ is a weakly orthonormal field. Further, if $K$ is not formally real, then $K$ is an orthonormal field.

The proof of the theorem proceeds by inductive construction. A critical role is played by the fact that, under the conditions stated, one can find "enough" subspaces of finite dimension which are spanned by orthogonal bases with all basis vectors of the same length.

In Chapter III we shall prove a theorem (Theorem 2) which guarantees the existence of such subspaces in the case of an arbitrary (denumerable) space $(E, \phi)$ over an algebraic number field. For special choices of $K$ (such as $K$, not formally real) one obtains an elementary proof for the
existence of orthonormal bases; however, the Hasse-Minkowski theory of quadratic forms (see [7] for an exposition) yields much stronger results so the usefulness of Theorem 2 will not be demonstrated until the study of arbitrary Hermitian forms is undertaken in Chapter IV.

In Chapter IV necessary and sufficient conditions are given to determine whether or not an arbitrary automorphism of an algebraic number field is orthonormal or weakly orthonormal. Several examples are then given to demonstrate the use of this criteria.

**Notation:** In Chapters II and III, we shall study symmetric bilinear forms exclusively. Thus, if we write \((E, \phi)\) we shall automatically mean that the form \(\phi\) is symmetric. If we write \((E, H)\) we shall mean that \(H\) is an arbitrary Hermitian form.

If \(\Lambda\) is an index set and \(F_t\) is a subspace of \(E\) for each \(t \in \Lambda\) then by \(E = \bigoplus_{t \in \Lambda} F_t\) we mean that \(E\) is a direct sum of the \(F_t\)s. By \(E = \bigoplus_{t \in \Lambda} F_t\) we mean that \(E\) is an orthogonal decomposition of the spaces \(F_t\), \(t \in \Lambda\). This and all other vector space notation is consistent with [2].

We shall always denote the field of rational numbers by \(\mathbb{Q}\). If \(K(\Theta)\) is a simple algebraic extension of \(K\) with \([K(\Theta) : K] = \nu\) and \(\chi \in K(\Theta)\) then \(\chi\) has a unique representation as a polynomial in \(\Theta\) of degree less than \(\nu\). We denote the degree of this polynomial by \(d_\Theta(\chi)\). All field theoretic notation is consistent with [4].
CHAPTER II

ORTHONORMAL FIELDS

Some examples of orthonormal fields are the complex numbers $\mathbb{C}$, the algebraic closure of the rationals $\mathbb{Q}$ in $\mathbb{C}$, and any finite field. All of these fields have the property that the order of the multiplicative group of the field modulo square factors is finite. Such fields are called Kneser fields and were found to be orthonormal fields in [2].

It is quite obvious that all finite algebraic extensions of the fields in the examples are also orthonormal fields. In this section we shall show that any finite algebraic extension of an orthonormal field is orthonormal.

**Corollary 1:** (To definition) If a field $K$ is an orthonormal field, then $K$ is non-formally real.

**Proof:** By the definition of orthonormal there is at least one positive integer $q_x$ such that the equation $\sum_{x=1}^{q_x} (-1)X_x^2 = 1$ has a solution in $K$. Thus, $K$ is non-formally real.

We shall now list several corollaries of Theorem G. To avoid monotonous repetition of the same sort of argument, we shall only give the proof of Corollary 6.

**Corollary 2:** A field $K$ is orthonormal if and only if every semisimple $\mathcal{V}_0$-dimensional $K$-vector space possesses an infinite dimensional totally isotropic subspace.

**Corollary 3:** A field $K$ is orthonormal if and only if every semisimple $\mathcal{V}_0$-dimensional $K$-vector space has a non zero isotropic vector.
Corollary 4: Let \( K \) be an orthonormal field and \( \{ q_i \}_{i \geq 1} \) be a sequence of non-zero elements of \( K \). Then there are elements \( a_{2j}, \ldots, a_m \) in the sequence and elements \( \alpha_{k1}, \ldots, \alpha_{km} \) in the field \( K \) with \( \alpha_1 \neq 0 \) such that \( \sum_{i=1}^{m} a_i \alpha_i^2 = 1 \).

Corollary 5: Let \( K \) be an orthonormal field and \( \{ q_i \}_{i \geq 1} \) be a sequence of non-zero elements of \( K \). Then there are elements \( a_{2j}, \ldots, a_q \) in the sequence and elements \( \alpha_{k1}, \ldots, \alpha_{kq} \) in the field \( K \) with \( \alpha_1 \neq 0 \) such that \( \sum_{i=1}^{q} a_i \alpha_i^2 = 0 \).

Corollary 6: Let \( K \) be a field then \( K \) is an orthonormal field if and only if for every sequence \( \{ q_i \}_{i \geq 1} \) of non-zero elements of \( K \) there are elements \( a_{2j}, \ldots, a_m \) in the sequence and elements \( \alpha_{k1}, \ldots, \alpha_{km} \) in the field \( K \) with \( \alpha_1 \neq 0 \) such that \( \sum_{i=1}^{m} a_i \alpha_i^2 = 1 \).

Proof: The sufficiency follows from Corollary 4. It remains only to prove the necessity. We notice immediately that \( K \) is non-formally real, since for the sequence \( \{-1, -1, \ldots\} \) there exists \( \alpha_{k1}, \ldots, \alpha_{km} \) in the field with \( \alpha_1 \neq 0 \) and such that \( \sum_{i=1}^{m} (-1) \alpha_i^2 = 1 \), i.e. \( \sum_{i=1}^{m} \alpha_i^2 = -1 \).

Let \( (E, \phi) \) be an \( N \)-dimensional semisimple \( K \)-vector space then \( (E, \phi) \) has an orthogonal basis, say \( \{ e_i \}_{i \geq 1} \). Since \( (E, \phi) \) is semisimple, we have that \( \| e_i \| \neq 0 \) each \( i \). Therefore, consider the sequence \( \{ \| e_i \| \}_{i \geq 1} \). By hypothesis there are elements \( \| e_i \|, \ldots, \| e_m \| \) in the sequence and elements \( \alpha_{k1}, \ldots, \alpha_{km} \) in the field such that \( \sum_{i=1}^{m} \| e_i \| \alpha_i^2 = 1 \).

We now consider the sequence \( \{ \| e_i \| \}_{i \geq m+1} \). By hypothesis we find \( \| e_i \|, \ldots, \| e_m \| \) and elements of the field \( \alpha_{m+1}, \ldots, \alpha_{m+q} \).
such that \( \sum_{m+1}^{m+b+1} \| e_i \|^2 \alpha_i = 1 \) or \( \sum_{m+1}^{m+b+1} \| e_i \|^2 \alpha_i = -1 \). We now have that the non zero vector \( \sum_{i=1}^{m+b} \alpha_i e_i \) is isotropic. By Corollary 3 the assertion is proved.

We shall use the corollaries to obtain the main result of Chapter II.

**Theorem 1:** Let \( \mathcal{K} \) be an orthonormal field and \( \mathcal{K}(\Theta) \) a simple algebraic extension then \( \mathcal{K}(\Theta) \) is orthonormal.

**Proof:** Assume \( \mathcal{K}(\Theta) : \mathcal{K} = \mathcal{C} \). Let \( (E, \phi) \) be an arbitrary \( n_0 \)-dimensional \( \mathcal{K}(\Theta) \)-vector space. We must show that \( (E, \phi) \) contains a non zero isotropic vector. Let \( \{ e_i \}_{i=1}^{\mathcal{J}} \) be an orthogonal basis of \( (E, \phi) \). By relabeling the subscripts of the \( e_i \'s \) we decompose \( (E, \phi) \) in the following manner:

1) Split \( (E, \phi) \) into packets: \( (E, \phi) = \bigoplus_{i=1}^{\infty} (E_i, \phi) \) with the dimension \( E_i = n_0 \) for \( i \geq 1 \). Note that \( (E_i, \phi) \) is semisimple.

2) Split each \( (E_i, \phi) \) into packets: \( (E_i, \phi) = \bigoplus_{i=1}^{\infty} (E_{ij}, \phi) \) with the dimension \( E_{ij} = n_0 \) for \( i \geq 1 \). Note that \( (E_{ij}, \phi) \) is semisimple.

... 

m) Split each \( (E_{ij}, \phi) \) (m-1 subscripts) into packets: \( (E_{ij}, \phi) = \bigoplus_{p=1}^{\infty} (E_{ijk}, \phi) \) with the dimension \( E_{ijk} = n_0 \) for \( p \geq 1 \). Note that \( (E_{ijk}, \phi) \) is semisimple.

**Fix an** \( i, j, k \).

**Step 1)** We assert that each vector space \((E_{ij}, \phi)\) contains a non zero vector \( \chi \) such that \( \mathcal{D}_\phi (\| \chi \|, n) \leq m - 2 \).
Suppose that this is not the case. Then there is a \( p' \geq 1 \) such that \( \partial_0(\|x\|) = m - 1 \) for any non zero vector \( x \) in \( (E_i^j, \ldots, s_{\Phi}, \Phi) \). This space is semisimple and it has an orthogonal basis, say \( \{e_i, i \geq 1\} \).

Now \( \|x\| = \sum_{j=0}^{\infty} a_{ij} \theta^j \) with \( a_{ij} \in K \) and by supposition \( \partial_0(\|e_i\|) = m - 1 \). Thus, \( a_{m-1, i} \neq 0 \) for each \( i \geq 1 \).

Therefore, \( \{a_{i, m-1}, i \geq 1\} \) is a sequence of non zero elements in \( K \). By Corollary 5 there exists a sequence \( \alpha_{1}, \ldots, \alpha_{q} \) in \( K \) with \( \alpha_{1} \neq 0 \) such that \( \sum_{i=1}^{q} a_{i, m-1} \alpha = 0 \). Now \( \sum_{i=1}^{q} \alpha \neq 0 \) since \( \alpha_{1} \neq 0 \) and \( \alpha_{1} \neq 0 \). We have \( \partial_0(\|\sum_{i=1}^{q} \alpha \|) < m - 1 \) contrary to the supposition.

Therefore, for each \( p \geq 1 \), \( (E_i^j, \ldots, s_{\Phi}, \Phi) \) has a non zero vector \( e_{2p} \) such that \( \partial_0(\|e_{2p}\|) \leq m - 2 \) and thus \( (E_i^j, \ldots, s_{\Phi}, \Phi) \) contains an infinite set of linearly independent mutually orthogonal vectors \( \{e_{2p}\}_{p \geq 1} \).

Step 2) Now let \( i, j, \ldots, s \) remain fixed but vary \( \lambda \). We have from Step 1 that for each \( \lambda \geq 1 \) there exists an infinite set of linearly independent mutually orthogonal vectors \( \{e_{2p}\}_{p \geq 1} \) contained in \( (E_i^j, \ldots, s_{\Phi}, \Phi) \) such that \( \partial_0(\|e_{2p}\|) \leq m - 2 \). We consider the following cases for each \( \lambda \).

Case i) For one \( p \), \( \|e_{2p}\| = 0 \) then we are done, since \( (E_i^j, \Phi) \) then contains a non zero isotropic vector.

Case ii) One of the \( e_{2p} \) is such that \( \partial_0(\|e_{2p}\|) < m - 2 \). Choose this vector and call it \( e_{s2} \).

Case iii) For every \( e_{2p} \) we have that \( \partial_0(\|e_{2p}\|) = m - 2 \). Reapply the method of Step 1) on the leading coefficients of \( \left\{\|e_{2p}\|\right\}_{p \geq 1} \) to find a
non zero vector \( X \) in the space generated by \( \sum_{i} \epsilon_{\alpha, p} \bar{z}_{p} \) (which is a subspace of \( (E_{\alpha}) \)) such that \( d_{\alpha}(\|X\|) < m-2 \). We call this vector \( E_{\alpha} \).

Therefore, from Cases i), ii) and iii) either \( (E, \phi) \) has a non zero isotropic vector or \( (E_{\alpha}) \) has an infinite set of mutually orthogonal linearly independent vectors \( \{E_{\alpha}\} \) with \( d_{\alpha}(\|E_{\alpha}\|) < m-2 \).

Continuing the process (if we don't find a non zero isotropic vector at one step) we find that \( (E, \phi) \) has an infinite set of mutually orthogonal linearly independent vectors \( \{E_{\alpha}\} \) such that \( d_{\alpha}(\|E_{\alpha}\|) = 0 \) (i.e. \( \|E_{\alpha}\| \in K \)). Reapplying the method of Step 1 we find that \( (E, \phi) \) has a non zero isotropic vector.

But \( (E, \phi) \) was arbitrary, therefore the theorem is proved by Corollary 3.

Theorem 1 immediately leads to:

**Corollary 7**: If \( K \) is an orthonormal field and \( \overline{K} \) is a finite algebraic extension of \( K \), then \( \overline{K} \) is orthonormal.

**Remark**: Gross has asked the following question: Does there exist an orthonormal field \( K \) such that for any integer \( N > 0 \) there is a \( P \)-dimensional semisimple \( K \)-vector space \( (F, \phi) \) with no non zero isotropic vectors and \( N \leq \dim F < \aleph_{0} \)?

If the answer is in the negative, then Theorem 1 has a much simpler proof.
CHAPTER III
ORTHONORMAL ALGEBRAIC NUMBER FIELDS.

In Chapter II we studied fields in general; in this chapter we turn our attention to algebraic number fields.

If $K$ is a finite algebraic extension of $\mathbb{Q}$ then because $\mathbb{Q}$ is a perfect field, there is an element $\alpha$ of $K$ such that $K = \mathbb{Q}(\alpha)$. Furthermore, if $\overline{\alpha} = \alpha - p$ with $p \in \mathbb{Q}$ then $\mathbb{Q}(\alpha) = \mathbb{Q}(\overline{\alpha})$.

**Definition 1:** Let $N$ and $\eta$ be two positive integers then we define

$$
g(N, \eta) = 2 \cdot \frac{4^{(n-1)} - 3}{4^n + 1} \cdot N - 3 \quad ; \quad n > 1,
g(N, 1) = 8(N-1) + 1
$$

**Theorem 2:** Let $\mathbb{Q}(\Theta)$ be a finite algebraic extension of the rationals $\mathbb{Q}$ with $[\mathbb{Q}(\Theta) : \mathbb{Q}] = n$. Let $N$ be an arbitrary positive integer then any semisimple $\mathbb{Q}(\Theta)$-vector space $(E, \phi)$ of dimension at least $g(N, n)$ contains $N$ linearly independent mutually orthogonal vectors of the same length.

Furthermore, the proof of the theorem will show that we may select the $N$ mutually orthogonal vectors such that their lengths are not zero. Before proving this theorem, we list several lemmas.

If $\mathbb{Q}(\Theta)$ is a finite algebraic extension of $\mathbb{Q}$ with $[\mathbb{Q}(\Theta) : \mathbb{Q}] = n$, then any element $\alpha$ of $\mathbb{Q}(\Theta)$ has a unique representation as a polynomial in $\Theta$ of degree less than or equal to $n-1$ with coefficients in $\mathbb{Q}$. We denote by $\deg_\Theta(\alpha)$ the degree of this polynomial.

**Lemma 1:** Let $\mathbb{Q}(\Theta)$ be a finite algebraic extension of $\mathbb{Q}$ and $[\mathbb{Q}(\Theta) : \mathbb{Q}] = n$. If $\sum_{i=0}^{m} a_i \Theta^i \in \mathbb{Q}(\Theta)$ with $a_m \neq 0$
and \( m < n \) then there is \( \overline{e} \) in \( Q(\overline{e}) \) such that

1) \( Q(\overline{e}) = Q(\overline{e}) \),
2) \( \sum_{i=0}^{m} a_i \Theta^i = \sum_{i=0}^{m} c_i \Theta^i \),
3) \( c_i \neq 0 \) and \( \text{sign} a_m = \text{sign} c_i \), \( 0 \leq i \leq m \).

Proof of Lemma 1: If \( m = 0 \) we take \( \Theta = \overline{e} \).

If \( m > 0 \) then we set

\[
\sum_{i=0}^{m} a_i \Theta^i = \sum_{i=0}^{m} c_i (\Theta - p)^i = \sum_{i=0}^{m} c_i (\Theta - p)^i \text{ for } p \in \Phi, p > 0 ;
\]

\[
C_m - q = \sum_{i=0}^{m} (m-i) p^{q-i} a_{m-i}.
\]

Thus, the coefficients \( c_i \) are polynomials in \( p \) with leading coefficients of the same sign as \( a_m \). We take \( p \) large enough so that the first terms of each polynomial in \( p \) are dominate. Then for such a \( p \), \( \text{sign} a_m = \text{sign} c_i \). Further, \( Q(\overline{e}) = Q(\overline{e} - p) \), i.e. we set \( \overline{e} = \overline{e} - p \).

Lemma 2: Let \( Q(\overline{e}) \) be an algebraic extension of \( Q \) with \( [Q(\overline{e}) : Q] = n \).

Let \( a_1, \ldots, a_l \) be elements of \( Q(\overline{e}) \) such that

\[
a_i = \sum_{i=0}^{m} b_i \Theta^i \text{ for each } i (1 \leq i \leq l) \text{ and } m < n.
\]

Furthermore, assume that \( b_{lm} \neq 0 \) (1 \( \leq i \leq l \)) and that \( \text{sign} b_{lm} = \text{sign} b_{j,m} \) for 1 \( \leq i, j \leq l \); then there exists \( \overline{e} \in Q(\overline{e}) \) such that

1) \( Q(\overline{e}) = Q(\overline{e}) \),
2) \( \sum_{i=0}^{m} b_i k_i \Theta^k_i = \sum_{i=0}^{m} c_i k_i \Theta^k_i \text{ for all } i, k \),
3) \( \text{sign} b_{im} = \text{sign} b_{j,m} \) for all \( i, j \).

Proof of Lemma 2: We set \( \overline{e} = \overline{e} - p \) as in the proof of Lemma 1. It follows from that proof that we merely have to choose \( p \) large enough.

It is, of course, essential that \( k < \infty \).
Definition 2: Let \( \mathbb{Q}(\Theta) \) be a finite algebraic extension of \( \mathbb{Q} \) with \( [\mathbb{Q}(\Theta) : \mathbb{Q}] = n \). Let \( x \in \mathbb{Q}(\Theta) \), \( x \neq 0 \), and let \( m \) be an integer such that \( 0 \leq m < n \). Then we shall say that \( x \) has an induced degree \( \nu \) (denoted \( \nu(x) = m \)) if and only if there is an element \( \gamma \in \mathbb{Q}(\Theta) \) such that \( \nu(x) = m \).

Remark: We note that \( x \) may admit various induced degrees.

Lemma 3: Let \( \mathbb{Q}(\Theta) \) be a finite extension of the rationals with \( [\mathbb{Q}(\Theta) : \mathbb{Q}] = n > 1 \). If \( x \in \mathbb{Q}(\Theta) \) with \( x \neq 0 \) we may have either \( \nu(x) = n - 1 \) or \( \nu(x) = n - 2 \).

Proof of Lemma 3: We can always achieve this by multiplying \( x \) by a suitable power of \( \Theta \).

We now state a theorem proved by Minkowski (See [1], p. 433).

Theorem M: Given rationals \( a \neq 0 \), \( b \neq 0 \), \( c \neq 0 \), \( d \neq 0 \), \( e \neq 0 \), such that the form \( ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2 + ex_5^2 \) is indefinite, then the form has a non-trivial zero in the rationals.

We now use Theorem M and the preceding lemmas to complete the proof of Theorem 2.

Proof of the Theorem: If \( n = 1 \) then by Theorem M \( \mathfrak{g}(N, 1) \) is indeed sufficient, so let us assume that \( n > 1 \).

\((E, \phi)\) is semisimple, so it has an orthogonal basis
\[ \{ \ell_{i} \}_{1 \leq i \leq q(n, n)} \]
with \( \| \ell_{i} \| \neq 0 \). Therefore, by multiplying our basis vectors \( \{ \ell_{i} \}_{1 \leq i \leq q(n, n)} \) by suitable scalars \( \gamma_{i} \in \mathbb{Q}(\Theta) \) we have by Lemma 3 that
\[ \nu_{\phi}(\| \gamma_{i} \ell_{i} \|) > n - 3 \]
for each \( i \). Call this new basis
\[ \{ \tilde{\ell}_{i} \}_{1 \leq i \leq q(n, n)} \quad (\tilde{\ell}_{i} = \gamma_{i} \ell_{i}) \].
We note that:

\[ g(N,n) = (2 \cdot 4^{4n-3} \cdot n - 2) + (2 \cdot 4^{4(n-1)-3} \cdot n - 2) + 1. \]

From this we deduce that at least one of the following cases must hold:

Case 1) There are at least \( 2 \cdot 4^{4n-3} \cdot n - 1 \) vectors in the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) whose lengths have a degree in \( \Theta \) over \( \mathbb{Q} \) of \( n - 1 \).

Case 2) There are at least \( 2 \cdot 4^{4(n-1)-3} \cdot n - 1 \) vectors in the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) whose lengths have a degree in \( \Theta \) over \( \mathbb{Q} \) of \( n - 2 \).

From this we may deduce that at least one of the four following cases must hold:

Case 1a) There are at least \( 4^{4n-3} \cdot n \) vectors \( \vec{e} \) in the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) whose lengths (as minimal polynomials in \( \Theta \)) have degree \( n - 1 \) and positive leading coefficients.

Case 1b) There are at least \( 4^{4n-3} \cdot n \) vectors in the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) whose lengths have degree \( n - 1 \) and negative leading coefficients.

Case 2a) There are at least \( 4^{4(n-1)-3} \cdot n \) vectors in the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) whose lengths have degree \( n - 2 \) and positive leading coefficients.

Case 2b) There are at least \( 4^{4(n-1)-3} \cdot n \) vectors in the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) whose lengths have degree \( n - 2 \) and negative leading coefficients.

Assume that Case 1a) holds; then we may choose vectors out of the basis \( \{ \vec{e} \}_{1 \leq i \leq g(N,n)} \) say \( \{ \vec{e}_i \}_{1 \leq i \leq 4^{4n-3} \cdot n} \) with

\[ \| \vec{e}_i \| = \sum_{j=0}^{4n-1} q_{ij} \Theta^j \]

such that \( q_{i,n-1} > 0 \), \( 1 \leq i \leq 4^{4n-3} \cdot n \). Call
the subspace generated by these vectors \( F \). Note that the \( \{\phi_i\} \) is an orthogonal basis and that \( (\phi, \phi) \) is semisimple.

By Lemma 2 we may change to a new generator \( \tilde{\phi} \) of \( Q(\theta) \) such that \( \|\tilde{\phi}\| = \sum_{j=0}^{n-2} \sum_{i<j} b_{ij} \tilde{\phi}^j \tilde{\phi}^i \) with \( b_{ij} > 0 \) for each \( i \) with \( 1 \leq i \leq 4^{n-2} \cdot N \) and each \( j \) with \( 1 \leq j \leq n-1 \).

We divide the basis \( \{\phi_i\} \) into \( 4(n-2) \cdot N \) disjoint packets \( \{\phi_{ij+1}, \phi_{ij+2}, \phi_{ij+3}, \phi_{ij+4}\} \). For each packet, by Theorem M, there exist rationals \( \alpha_{ij+1}, \alpha_{ij+2}, \alpha_{ij+3}, \alpha_{ij+4} \), not all zero such that:

\[
\sum_{t=1}^{T} \phi_{ij+t}, n-1 \alpha_{ij+t} = 1.
\]

Then we define \( \tilde{\phi} = \sum_{t=1}^{T} \alpha_{ij+t} \phi_{ij+t} \) for each \( j \) with \( 1 \leq j \leq 4^{n-2} \cdot N \).

Then \( \{\tilde{\phi}\} \) is a set of mutually orthogonal linearly independent vectors. Define \( F_{n-1} \) to be the space generated by 
\[
\{\tilde{\phi}\} \quad 1 \leq j \leq 4^{n-2} \cdot N.
\]

Then \( F_{n-1} \) is semisimple with orthogonal basis \( \{\tilde{\phi}\} \). Also for each \( j \), we have that \( \|\tilde{\phi}\| = \sum_{k=0}^{n-1} h_{jk} \tilde{\phi}^k \) with \( h_{jk} = 1 \) and \( h_{jk} > 0 \) for \( 1 \leq k \leq n-1 \).

Now we try to continue the process. Suppose we have already found vector spaces

\[
F_{n-k} \subset F_{n-k+1} \subset \cdots \subset F_{n-1} \subset F \subset E
\]

and \( F_{n-k} \) has the following properties:

\begin{enumerate}
\item \( \dim F_{n-k} = 4^{(n-k)} \cdot N \) and \( (F_{n-k}, \phi) \) is semisimple.
\item \( (F_{n-k}, \phi) \) has an orthogonal basis \( \{\phi_i\} \) such that:
\end{enumerate}

\begin{enumerate}
\item \( \|\phi_i\| = \sum_{j=n-k}^{n-1} \lambda_i \tilde{\phi}^j \sum_c \sum_{j<n-k} \phi_i \tilde{\phi}^j \) for all \( i, j \) with \( 1 \leq i \leq 4^{(n-k)} \cdot N \).
\end{enumerate}
b) \( \lambda_j^j > 0 \) for all \( j : n - \kappa \leq j \leq n - 1 \),

c) \( C_i > 0 \) for all \( i, j : 1 \leq i \leq 4^{(n - \kappa)} \cdot N \), and \( i \leq n - \kappa \).

Assuming that \( \kappa < n \), we shall construct \( F_{n - \kappa - 1} \subset F_{n - \kappa} \) with the same properties as \( F_{n - \kappa} \). We study first the

Case 1aA). Suppose there exists a set

\( \{ U_{i, 2} \} \) \( i \leq 2 \leq M \subset \sum_{i = 1}^{2} \sum_{l = 4^{(n - \kappa)} \cdot N} \)

such that \( C_{i, n - \kappa - 1} = C_{i, n - \kappa} \cdot \frac{1}{2} \) for all \( m, l \) with \( 1 \leq m, l \leq M \) and \( M \geq 4^{4(n - \kappa - 2)} \cdot N \). Then select any \( 4^{4(n - \kappa - 2)} \cdot N \) of the \( U_{i, 2} \)s, say \( \{ U_{i, 2} \} \) \( 1 \leq i \leq 4^{(n - \kappa - 2)} \cdot N \), and let them generate the \( F_{n - \kappa - 1} \). 

\( F_{n - \kappa - 1} \) has the required properties; \( \lambda_{n - \kappa - 1} = C_{i, n - \kappa - 1} (1 \leq i \leq \frac{1}{2} \cdot N) \).

If not Case 1aA), then Case 1aB).

Since we shall worry only about the coefficients \( C_i, n - \kappa - 1 \)

(\( n - \kappa \) fixed) we shall put \( C_{i, n - \kappa - 1} = C_i \). Clearly either (I) more than or exactly one half of the \( C_i \)s are greater than or equal to \( \lambda_{n - \kappa} \) or (II) more than or exactly one half of the \( C_i \)s are less than or equal to \( \lambda_{n - \kappa} \cdot \frac{1}{2} \cdot N \).

Without loss of generality, assume that (I) holds. We relabel the \( C_i \)s (and hence the corresponding \( U_i \)s), so that

\( 0 < \lambda_{n - \kappa} = C_1 \leq \ldots \leq C_i (4^{(n - \kappa)} \cdot N) / 2 \cdot N \).

Since we are not in case 1aA), and since

\( 2 \cdot 4^3 \cdot 4^{4(n - \kappa - 2)} \cdot N - 4 \cdot 4^{(n - \kappa - 2)} \cdot N = 4^4 \cdot 4^{(n - \kappa - 2)} \cdot N \),

there are at least \( 2 \cdot 4^4 \cdot 4^{(n - \kappa - 2)} \cdot N \) of the \( C_i \)s which are strictly greater than \( C_4 \cdot 4^{4(n - \kappa - 1)} \). Thus, we may construct a subsequence of the one above, relabeling \( C_i \)s is necessary (and hence the corresponding
\( \sum_{i=1}^{n-1} c_i \theta^i = \sum_{i=1}^{n-1} a_i \theta^i \) in \( Q(\theta) = Q(\theta^i) \). We have
\[
\| U_i \| = \sum_{j=1}^{n-1} c_{ij} p_j \theta^j + \sum_{j=1}^{n-1} \alpha_j p_j \theta^j.
\]

We now form five-tuples of elements of \( \{ U_i \}_{1 \leq i \leq 20, 4^{4(n-k-1)}, N} \) in the following special way.

For each \( U_i \) with \( 1 \leq i \leq 44^{4(n-k-1)} \) \( N \) we choose four distinct \( U_j \) with \( 4^{4(n-k-1)} \leq j \leq 20 \cdot 4^{4(n-k-1)}, N \); call them \( U_{i1}, U_{i2}, U_{i3}, U_{i4} \). In this way, we divide \( \{ U_i \}_{1 \leq i \leq 20, 4^{4(n-k-1)}, N} \) into
\( 4^{4(n-k-1)} \) \( N \) mutually disjoint packets \( \{ U_i, U_{i1}, U_{i2}, U_{i3}, U_{i4} \} \).

Now
\[
\| U_i \| = \sum_{j=1}^{n-1} \gamma_j p_j \theta^j + c_i p^{n-k-1} \theta^{n-k-1} + \sum_{j=n-k+1}^{n-1} c_{ij} p^j \theta^j,
\]
\[
\| U_{i1} \| = \sum_{j=1}^{n-1} \gamma_j p_j \theta^j + c_{i1} p^{n-k-1} \theta^{n-k-1} + \sum_{j=n-k+1}^{n-1} c_{i1j} p^j \theta^j
\]
with \( c_i p^{n-k-1} < p^{n-k} \lambda_{n-k} \) and \( c_{it} p^{n-k-1} > p^{n-k} \lambda_{n-k} \) \( (1 \leq t \leq 4) \) by our construction. So we now have that:
\[
p^{n-k} \lambda_{n-k} - c_i p^{n-k-1} > 0,
\]
\[
p^{n-k} \lambda_{n-k} - c_{it} p^{n-k-1} < 0; \ (1 \leq t \leq 4).
\]
Therefore, by Theorem M the quadratic form
\[ (p_1 \eta_{1-N} - c_1)X_0^2 + \sum_{t=0}^{t=4} (p_1 \eta_{1-N} - c_1)X_t^2 \]
has a non-trivial zero in the rationals; say \((p_1, c_1, p_2, c_2, p_3, c_3, p_4, c_4)\).

Let \(\alpha_i = \sum_{t=0}^{t=4} \alpha_i \kappa_t\) then we have that
\[ \alpha_i (p_1 \eta_{1-N}) = (c_1 \alpha_i \kappa_0 + \sum_{t=1}^{t=4} \alpha_i \kappa_t c_1 \kappa_t) \]

We define \(U_i = \alpha_i \kappa_0 U_i + \sum_{t=1}^{t=4} \alpha_i \kappa_t U_{i-t}\) for each \(i\). Then
\[ \{U_i\} \subseteq [4, 4^{(1-N-1)}] \]
is a mutually orthogonal set of linearly independent vectors out of \(F_{1-N}\) and
\[ \|U_i\| = \alpha_i (\sum_{t=1}^{t=4} \alpha_i \kappa_t + p_1 \eta_{1-N} \kappa_0 \kappa_{1-N-1}) + \sum_{t=1}^{t=4} p \kappa_{1-t} \kappa_i \kappa_t \]
with \(1 \leq i \leq 4 \cdot 4^{(1-N-1)}\) and \(d_{i, j} = \alpha_i \kappa_0 \kappa_j + \sum_{t=1}^{t=4} \alpha_i \kappa_t c_1 \kappa_t, j\).

Changing back to the generator \(\kappa\) of \(Q(\kappa)\) we have that
\[ \|U_i\| = \alpha_i \sum_{t=1}^{t=4} \kappa_0 \kappa_t \kappa_{1-N-1} + \sum_{j=1-N-1}^{j=4} \kappa_t \kappa_j \kappa_{1-N-1} \]

Define \(\kappa_{1-N-1}\) to be \(p_1 \eta_{1-N}\) by our induction assumption \(c)\) we have \(d_{i, j} > 0\) for all \(i, j\). Therefore
\[ \|U_i\| = \alpha_i \sum_{t=1}^{t=4} \kappa_0 \kappa_t \kappa_{1-N-1} + \sum_{j=1-N-1}^{j=4} d_{i, j} \kappa_j \kappa_{1-N-1}, (1 \leq i \leq 4 \cdot 4^{(1-N-1)}) \]

We finally split \(U_i\) into \(4^{(1-N-1)}\) packets of four, \(\{U_{(i_1) + 1}, U_{(i_1) + 2}, U_{(i_1) + 3}, U_{(i_1) + 4}\}\). We have:
\[ \|U_{(i_1) + t}\| = \alpha_{(i_1) + t} \sum_{t=1}^{t=4} \kappa_0 \kappa_t \kappa_{1-N-1} + \sum_{j=1-N-1}^{j=4} d_{(i_1) + t, j} \kappa_j \kappa_{1-N-1}, (1 \leq t \leq 4) \]

Now \(\alpha_{(i_1) + t} > 0\) for \(1 \leq t \leq 4\) so by Theorem M there is a non-trivial solution \((p_{1,1}, p_{1,2}, p_{1,3}, p_{1,4})\) in the rationals to the equation
$1 = \sum_{t=1}^{t^2} \alpha^t + \chi^2$

Let $\tilde{U}_i = \sum_{t=1}^{t^2} \beta_{lt} \tilde{U}_{( \alpha^t )}$. Then

$|| \tilde{U}_i || = \sum_{n-1}^{t^2} \gamma_j \delta^j + \sum_{j=n-k-2}^{t^2} m_{ij} \delta^j$ with $m_{ij} > 0$.

Denote the space generated by the $\{ \tilde{U}_i \} : 1 \leq i \leq A^{(n-k-2)}$ by $F_{n-k-2}$.

Then $F_{n-k-2} \subset F_{n-k}$ and $(F_{n-k-1})^\perp$ with basis $\{ \tilde{U}_i \}$ satisfies properties $i)$ and $ii)$ with $\kappa + 1$ in lieu of $\kappa$.

By this construction we have proved the theorem for Case 1a). The proofs for Cases 1b), 2a) and 2b) are nearly the same, word for word, and are omitted here. This concludes the proof of the theorem.

Remark: A theorem of the same nature as Theorem 2 can be derived from the results of the Hasse-Minkowski theory. With Theorem 2 we could classify all orthonormal and weakly orthonormal algebraic number fields. However, we shall use the results of the Hasse-Minkowski theory to classify all orthonormal and weakly orthonormal algebraic extensions of the rationals $\mathbb{Q}$.

An element of a field is said to be totally positive if and only if it is positive under every ordering of the field. Under this definition, all non-zero elements of a not formally real field are totally positive. It can be shown that a non zero element of a field is totally positive if and only if it is a sum of squares.

Lemma 4: If a field $K$ is weakly orthonormal then $K$ admits at most one ordering.

Proof: Let $\alpha$ be an arbitrary element of $K$ then for some integer $q$, either the equation $\sum_{1}^{q} \alpha^{-1} \chi^2 + 1 = 0$ or $\sum_{1}^{q} \alpha^{-1} \chi^2 - 1 = 0$. 


has a solution in $K$. Thus, either $\preceq$ or $\succeq$ is a sum of squares.

**Theorem 3:** The weakly orthonormal algebraic extensions of the rationals are precisely those algebraic extensions of the rationals which have at most one ordering.

**Proof:** By Lemma 4, the only algebraic extensions of the rationals which are weakly orthonormal are those which have at most one ordering. Let $K$ be an algebraic extension of the rationals $\mathbb{Q}$ such that $K$ admits at most one ordering. First suppose that $K$ is not formally real. By a result of Siegel ([\textit{K}], Satz 1, p. 259) there are $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in K$ such that $\sum_{i=1}^{4} \alpha_i^2 = -1$. Let $(F, \phi)$ be an arbitrary semisimple four-dimensional space over $K$. Then $F$ has an orthogonal basis $\{e_i\}_{1 \leq i \leq 4}$ and $\phi_i = \|e_i\|$, $1 \leq i \leq 4$. Now the field $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \phi_1, \phi_2, \phi_3, \phi_4)$ is not formally real, thus every five-dimensional quadratic form in five variables with coefficients in $\mathbb{Q}(\alpha_1, \ldots, \alpha_4, \phi_1, \ldots, \phi_4)$ has a non trivial zero in $\mathbb{Q}(\alpha_1, \ldots, \phi_4)$ by the results of the Hasse-Minkowski theory. Thus the quadratic form $\sum_{i=1}^{4} \phi_i x_i^2 + x_5^2$ has a non trivial zero in $\mathbb{Q}(\alpha_1, \ldots, \phi_4)$ and so in $K$. Thus, either the vector space $(F, \phi)$ has a vector of length $-1$ or an isotropic vector in which case $(F, \phi)$ contains a hyperbolic plane and so also a vector of length $-1$. Therefore, since $(F, \phi)$ was arbitrary, we may choose $n = 4$ in Theorem K of Chapter I to show that $K$ is weakly orthonormal. Now suppose that $K$ admits exactly one ordering. Let $(F, \phi)$ again be an arbitrary semisimple four-dimensional vector space with orthogonal basis $\{e_i\}_{1 \leq i \leq 4}$ and $\|e_i\| = \phi_i$, $1 \leq i \leq 4$. Now every element in $K$ is either a sum of squares or its negative is the sum of squares.
Thus, for each $L$, there are $x_{11}, \ldots, x_{4,4}$ in $K$ such that either $\beta_1 = \frac{p}{2} x_{11}^2$ or $-\beta_1 = \frac{p}{2} x_{4,4}^2$. We now observe that either the quadratic form $\sum\beta_1 x_i^2 + x_5^2$ or the quadratic form $\sum\beta_1 y_i^2 - y_5^2$ is indefinite at every archimedian completion of the global field $Q(\alpha_{11}, \ldots, \alpha_{4,4})$, and so at least one of the forms has a non trivial zero in $Q(\alpha_{11}, \ldots, \alpha_{4,4})$ and so in $K$. Hence, by the same argument as for the not formally real case, every semisimple four-dimensional space over $K$ contains a vector of length $1$ or $-1$, so we can take $\eta = 4$ in Theorem $K$ to show that $K$ is weakly orthonormal.

**Corollary 8:** The orthonormal algebraic extension fields of the rationals are precisely the not formally real ones.

**Proof:** Use Theorem 3, Theorem G and Corollary 1.

**Remark:** Let $K$ be a formally real algebraic extension of the rational numbers with exactly one ordering. Let $(E, \phi)$ be a $N$-dimensional semisimple vector space over $K$. By Theorem 3, $K$ is weakly orthonormal, so $E$ admits an orthogonal decomposition, $E = E^+ \oplus E^-$, where $E^+$ has an orthonormal basis and $E^-$ has a negative orthonormal basis. We shall show that Sylvester's theorem holds in this case (See [8]).

**Theorem 2.2, p. 524.** Indeed, if $E$ admits of two decompositions $E = E^+ \oplus E^- = F^+ \oplus F^-$ then every vector $e^+ \in F^+$ can be written as the sum $e^+ = e^+ + e^-$ with $e^+ \in E^+$ and $e^- \in E^-$. If the dimension of $E^+$ were less than the dimension of $F^+$ then there is at least one non zero vector $x_0$ in $F^+ \cap E^-$; $x_0$ would therefore be of positive and negative length, a contradiction. Thus, the dimensions of $E^+$ and $E^-$ are unique ($E^+$ and $E^-$ are not) and so we see that the two
(cardinal) numbers are a complete set of invariants for non-degenerate \( N^0 \)-dimensional forms over \( K \).

Remark: We end this chapter by indicating an example of an extension field of the Gaussian numbers \( Q(\sqrt{-1}) \) which is not orthonormal.

Consider the polynomial ring \( Q(\sqrt{-1})[X_0, X_1, X_2, \ldots] \).

It is easy to show by induction that the quadratic form

\[
\sum_{i=1}^{n} \left( \prod_{j \neq i} (X_j - X_0) \right) P_i^2 \quad \text{and} \quad \prod_{i=1}^{n} (X_i - X_0) = 1,
\]

has no non-trivial zero for any \( n \geq 1 \) in \( Q(\sqrt{-1})[X_0, X_1, \ldots] \).

Thus, the vector space \( (E, \phi) \) over the quotient field of \( Q(\sqrt{-1})[X_0, X_1, X_2, \ldots] \) with orthogonal basis \( \{e_i\}_{i=1}^{n} \) and \( \phi(e_i, e_j) = \prod_{1 \neq j \neq i} (X_i - X_0) \) has no orthonormal basis. Therefore, the quotient field of \( Q(\sqrt{-1})[X_0, X_1, X_2, \ldots] \) is not orthonormal.
CHAPTER IV

HERMITIAN FORMS

Let $K$ be a commutative field and let $\sigma$ be an automorphism of $K$ such that $\sigma \circ \sigma = \mathbb{1}_K$. Let $K_\sigma$ be the fixed field of $\sigma$ in $K$.

If $(E, H)$ is a semisimple $\sigma$-dimensional vector space with $H \in \langle K, \sigma \rangle$ then $E$ has an orthogonal basis $\{\varepsilon_i, \ldots, \varepsilon_n\}$. Now for any $x \in E$, by the definition of a Hermitian form, $H(x, x) = \overline{H(x, x)}$ where $\sigma(H(x, x)) = H(x, x)$. Thus, the lengths of all basis vectors $\varepsilon_i$ of $E$ are in the fixed field $K_\sigma$. By restricting the scalars of $E$ to the fixed $K_\sigma$ we may induce a vector space $(E, \overline{H})$ in the natural way that $E$ is a $K_\sigma$-vector space with $x \in E$ if and only if $x = \sum \lambda_i \varepsilon_i$ with $\lambda_i \in K_\sigma$; and the form $\overline{H} = H|_{E \times E}$ is a symmetric non-degenerate bilinear form. Transition from $E$ to $K \otimes _{K_\sigma} E$ gives us $E$ back again.

If $K_\sigma$ is an orthonormal field then $(E, H)$ has an orthonormal basis and so $(E, H)$ has an orthonormal basis; likewise, if $K_\sigma$ is weakly orthonormal, then $(E, H)$ has a $+1, -1$ orthogonal basis. We have proved

Theorem 4: Let $K$ be a commutative field and $\sigma$ an automorphism of $K$ such that $\sigma \circ \sigma = \mathbb{1}_K$. Then

1) if the fixed field of $\sigma$ in $K$ is orthonormal then $\sigma$ is orthonormal.

2) if the fixed field of $\sigma$ in $K$ is weakly orthonormal, then $\sigma$ is weakly orthonormal.

We now turn our attention to the problem of determining the orthonormal and weakly orthonormal automorphisms of an algebraic number field.
In Example 2 below we shall show that an algebraic number field may admit an orthonormal automorphism and an automorphism whose square is the identity automorphism, but which is not even weakly orthonormal. This example indicates that not only the field, but the individual automorphisms of the field must be taken into consideration. Thus, it seems more profitable to give a classification criteria which can be applied to special cases. Theorem 5 and Corollary 9 below will give necessary and sufficient conditions for classifying an automorphism over an algebraic number field.

Lemma 5: Let \( K \) be an algebraic field and \( \sigma \) an automorphism of \( K \) such that \( \sigma \circ \sigma = 1 \). If \( K_\sigma \) is the fixed field of \( \sigma \) in \( K \) then either 1) \( K_\sigma = K \) or 2) \( K_\sigma \neq K \) and there exists \( a \in K_\sigma \) such that \( K_\sigma (\sqrt{a}) = K \).

Proof: If \( K_\sigma \neq K \) then \( K_\sigma \subsetneq K \) and \( Q \subset K_\sigma \subsetneq K \) with \( [K : Q] \leq \aleph_0 \). Hence, \( [K : K_\sigma] \leq \aleph_0 \) and so \( K_\sigma (\Theta) = K \). But both \( \sigma(\Theta) \cdot \Theta \) and \( \sigma(\Theta) + \Theta \) are in \( K_\sigma \). Thus, \( x^2 - (\sigma(\Theta) + \Theta)x + \sigma(\Theta) \cdot \Theta \) is the minimal monic polynomial of \( \Theta \) over \( K_\sigma \).

Theorem 5: Let \( K \) be an algebraic number field and \( \sigma \) an automorphism of \( K \) such that \( \sigma \circ \sigma = 1 \). Then \( \sigma \) is orthonormal if and only if either \( K_\sigma \) is orthonormal or there is \( \beta \in K - K_\sigma \) and \( \beta \) is a square root of a totally positive element of \( K_\sigma \).

Proof: We first prove the sufficiency. If \( K_\sigma \) is orthonormal then we
are done by Theorem 4. So suppose $K_{c}(\beta) = K$. Then the norm of any element $x \in K$ is of the form $N_{K_{c}}(x) = x^{2} - \lambda \cdot x \cdot \beta \in K_{c}$, where $\lambda = \beta^{2}$. We have by hypothesis that $\lambda$ is totally positive in $K_{c}$.

Now let $(E, H)$ be an arbitrary semisimple $N_{c}$-dimensional vector space with $H \in (K, c)$. We want to show that $(E, H)$ has an orthonormal basis and we shall do this by the methods used by Fischer and Gross in the proof of Theorem 1 (2, pp. 287-288). We shall show first that $(E, H)$ has an orthogonal decomposition into hyperbolic planes. Let $\{e_{i}\}_{i = 1}^{3} \subseteq E$ be a fixed but arbitrary basis of $E$. Suppose that we have found $E_{p} \subseteq E$ such that $E_{p} = \bigoplus_{i \leq p} P_{i}$ where $P_{i}$'s are hyperbolic planes, and $e_{i} \in E_{p}$ for $i \leq p$. Suppose that $n$ is the smallest integer such that $e_{n} \not\in E_{p}$. If we can find a hyperplane $P_{p+1} \subseteq E_{p}$ such that $e_{n} \in E_{p+1} = \bigoplus_{i \leq p} P_{i} \bigoplus P_{p+1}$ then we have proved the assertion. Now $E_{n} = E_{n} + \overline{E_{n}}$ where $\overline{E_{n}} \subseteq E_{p}$ and $\overline{E_{n}} \subseteq E_{p}$; assume without loss of generality that $\overline{E_{n}} = 0$.

Case 1) Suppose $\|e_{n}\| = 0$. Since $e_{n} \in E_{p}$ and $E_{p}$ is semisimple, then there is $y \in E_{p}$ such that $H(e_{n}, y) = 0$. Hence, $e_{n}$ and $y$ generate a hyperbolic plane in $E_{p}$ and this may be used as the $P_{p+1}$ desired.

Case 2) Suppose $\|e_{n}\| = \beta_{n} \neq 0$. Let $K \subseteq e_{n}$ be the one-dimensional subspace of $E_{p}^{\perp}$ generated by $e_{n}$, then $E_{p}^{\perp} = K \subseteq e_{n} \bigoplus F$ where $F$ is semisimple. Restricting the scalars of $F$ to $K_{c}$ we define the vector space $\overline{F}$ with symmetric
form $\overline{\mathbf{H}} = H|_{E^-}$. Using Theorem 2 of Chapter III we find five mutually orthogonal, linearly independent vectors $\xi_1, \xi_2, \xi_3, \xi_4, \xi_5$ in $\overline{E}$ (and thus in $E$) such that $\|\xi_1\| = \|\xi_2\| = \|\xi_3\| = \|\xi_4\| = \|\xi_5\| \neq 0$.

We multiply $\xi_5$ by $\beta$. Since $\beta \cdot \sigma(\beta)$ is the additive inverse of a totally positive element, the quadratic form

$$\sum_i x_i + \sigma(\beta) \cdot \beta \cdot x_5^2$$

has a non-trivial zero in $K_{\sigma}$ by the Hasse-Minkowski theory. We shall call this zero $\left(\alpha_{\xi_1}, \alpha_{\xi_2}, \alpha_{\xi_3}, \alpha_{\xi_4}, \alpha_{\xi_5}\right)$. Since $\xi_1, \xi_2, \xi_3, \xi_4, \xi_5$ are linearly independent, then $z = \sum_i \alpha_i \xi_i + \alpha_5 \beta \xi_5$ is a non-zero isotropic vector in $F$. But $F$ is semisimple so there is $\lambda \in F^*$ such that $\lambda (x_j, z) \neq 0$. Now $x$ and $z$ generate a hyperbolic plane in $F$ and a hyperbolic plane contains a vector of any length; thus, there is $w \in F$ such that $\|w\| = -\beta \lambda$. Hence, $w$ and $e_n$ will generate the hyperbolic plane $P_{p+1}$ in $E_{\sigma}$ which is desired. By Case 1 and Case 2 we have shown that $E = E^+ \oplus E^-$ where $E^+$ has an orthonormal basis and $E^-$ has a negative orthonormal basis with $\dim E^- = \lambda_0$. We shall now complete the proof of the sufficiency by showing that $E^-$ has an orthonormal basis. Let $\{\xi_i\}$ be the negative orthonormal basis of $E^-$. Then define $\overline{\xi}_i = \beta \xi_i$, each $i$. Then $\{\overline{\xi}_i\}$ is a basis of $E^-$ and $\|\overline{\xi}_i\| = \lambda$, each $i$, where $\lambda$ is totally positive by hypothesis. We restrict ourselves to the scalars of $K_{\sigma}$ then $E^- = \{x \in E^- | x = \sum_i \lambda_i \overline{\xi}_i, \lambda_i \in K_{\sigma}\}$ is a vector space over $K_{\sigma}$ with non-degenerate bilinear form $\overline{H} = H|_{E^-} \cdot \overline{E}$. We note that $\overline{H}$ is symmetric. Now the
length of every non zero vector in \((\mathbb{E}^-, \mathbb{H})\) is totally positive; thus, by the Hasse-Minkowski theory, every five-dimensional semisimple subspace of \(\mathbb{E}^-\) has a vector of length 1. Suppose we have been able to find a subspace of \(\mathbb{E}^-\) say \(\mathbb{E}_p\), such that \(\mathbb{E}_p = \bigoplus G_i \mathbb{C}\), where the \(G_i\) are four-dimensional vector spaces with orthonormal bases and such that \(\mathbb{E}_i \in \mathbb{E}_p\) for \(i \leq p\). Let \(\mathbb{H}\) be the smallest integer such that \(\mathbb{E}_n\) is not in \(\mathbb{E}_p\); if we can find a space \(\mathbb{G}_{p+1}\) of dimension four with an orthonormal basis such that \(\mathbb{E}_n \in \bigoplus \mathbb{G}_{p} \mathbb{C}\), then we have shown that \(\mathbb{E}^-\) has an orthonormal basis. Assume, without loss of generality, that \(\mathbb{E}_n \in \mathbb{E}_p\).

Now let \((\mathbb{V}, \phi)\) be an arbitrary four-dimensional vector space over \(k\) with an orthonormal basis (the form \(\phi\) is a symmetric bilinear form). Since \(\|\mathbb{E}_n\|\) is totally positive, then \(\mathbb{V}\) has an orthogonal basis \(\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4\}\) with \(\|\mathbf{u}_1\| = \|\mathbb{E}_n\|\).

We let \(K=\mathbb{E}_n\bigoplus \mathbb{W}\) be the one-dimensional subspace of \(\mathbb{E}_n\), then \(\mathbb{E}_n = K \bigoplus \mathbb{W}\). Now \(\mathbb{W}\) is semisimple and the lengths of all non zero vectors in \(\mathbb{W}\) are totally positive. Thus, we can find three mutually orthogonal, linearly independent vectors \(\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_3 \) in \(\mathbb{W}\) such that \(\|\mathbf{v}_2\| = \|\mathbf{u}_2\|\), \(\|\mathbf{v}_3\| = \|\mathbf{u}_3\|\), \(\|\mathbf{v}_4\| = \|\mathbf{u}_4\|\). Thus, the subspace \(\mathbb{G}\) generated by \(\{\mathbb{E}_n, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}\) is orthogonally isomorphic to \((\mathbb{V}, \phi)\) so \(\mathbb{G}\) has an orthonormal basis. Hence, \(\mathbb{G}\) is the \(\mathbb{G}_{p+1}\) desired and so \(\mathbb{E}^-\) has an orthonormal basis. Hence, \(\mathbb{E}^-\) has an orthonormal basis. This concludes the proof of the sufficiency.
It remains to prove the necessity. So suppose \( \sigma \) is orthonormal. If \( \sigma = \mathbb{1}_K \) then by definition \( K = K_\sigma \) and \( K_\sigma \) is orthonormal. If \( \sigma \neq \mathbb{1}_K \) then \( K_\sigma \leq K \) and, by Lemma 5,

\[ K_\sigma(\sqrt{a}) = K \]

where \( a \in K_\sigma \). Hence, \( \sqrt{a} \in K - K_\sigma \).

Now let \( \mathbb{E} \) be a \( K \)-vector space with basis \( \{e_i\}_{i \geq 1} \) supplied with the form \( H \in (K_\sigma) \) such that \( \{e_i\}_{i \geq 1} \) is an orthogonal basis and \( H(e_i, e_i) = -1 \) all \( i \geq 1 \). Since \( \sigma \) is orthonormal there exist \( \alpha_1, \alpha_2, \ldots, \alpha_q \) in \( K \) for some \( q \), such that

\[ \sum \alpha_i^2 N_{K:K_\sigma}(\alpha_i) = -1 \].

But \( N_{K:K_\sigma}(\alpha_i) = \prod_{j}^{2} - \omega_j^2 a \) for some \( \prod_{j}^{2} \omega_j \in K_\sigma \); each \( j \). Thus, we have that

\[ \sum \alpha_i^2 \prod_{j}^{2} + 1 - a \sum \omega_j^2 = 0. \]

Now if \( a \) is not positive under some ordering of \( K_\sigma \) the above equation can have no solution. (We can assume that \( K_\sigma \) is formally real, for if not, then \( a \) is totally positive to start with.) So we must have \( a \) totally positive in \( K_\sigma \), which was to be shown. This concludes the proof of Theorem 5.

Remark: We have seen by the proof of Theorem 5 that the property 'there are \( x_1, \ldots, x_n \) in the field \( K \) such that \( \sum_{i} x_i^2 = -1 \)' in the case of classifying orthonormal algebraic number fields is equivalent in the classification of arbitrary automorphisms \( \langle \sigma \circ \sigma = \mathbb{1}_{K_\sigma} \rangle \) to the property 'there exist \( x_1, \ldots, x_n \) in the field such that \( \sum_{i} x_i^2 \leq \langle x_i \rangle = -1 \)'.

We see by the proof of Theorem 5 that we may state the following corollary:
Corollary 2: Let $K$ be an algebraic number field and $\sigma$ an automorphism of $K$ such that $\sigma \circ \sigma = \mathbb{I}_K$. Then $\sigma$ is weakly orthonormal if and only if either $K_{\sigma}$ is weakly orthonormal or there is $\beta \in K - K_{\sigma}$ and $\beta$ is a square root of a totally positive element in $K_{\sigma}$.

We shall end this paper with several examples illustrating the above classification criteria.

Example 1: Consider the field $K = \mathbb{Q}(\sqrt{3}, \sqrt{7}, \sqrt{11})$. The four automorphisms of $K$ are

- $\sigma_1 = \mathbb{I}_K$ and $K_{\sigma_1} = K$,
- $\sigma_2$ which sends $\sqrt{7}$ into $-\sqrt{7}$ and has fixed field $K_{\sigma_2} = \mathbb{Q}(\sqrt{3}, \sqrt{11})$,
- $\sigma_3$ which sends $\sqrt{2}$ into $-\sqrt{2}$ and has fixed field $K_{\sigma_3} = \mathbb{Q}(\sqrt{3}, \sqrt{7})$,
- $\sigma_4$ which sends $\sqrt{2}$ into $-\sqrt{2}$ and $\sqrt{7}$ into $-\sqrt{7}$, $K_{\sigma_4} = \mathbb{Q}(\sqrt{3}, \sqrt{11})$.

Note that $\sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = \sigma_3 \circ \sigma_3 = \sigma_4 \circ \sigma_4 = \mathbb{I}_K$.

By Theorem 3, $\sigma_1$ is not even weakly orthonormal.

But, since $2$, $7$ and $11$ are totally positive elements, by Theorem 5 $\sigma_2$, $\sigma_3$ and $\sigma_4$ are all orthonormal. Thus, over this field, there are essentially only three distinct $\mathbb{V}$-dimensional semisimple vector space with non symmetric Hermitian forms. (Each of these admit of an orthonormal basis.)

Example 2: Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$. The automorphisms of $K$ are
- 29 -

\[ \sigma_1 = 1_K \; ; \; \mathbb{K}_{\sigma_1} = \mathbb{K} \, , \]
\[ \sigma_2 : \sqrt{2} \to -\sqrt{2} \; ; \; \mathbb{K}_{\sigma_2} = \mathbb{Q}(\sqrt{2}) \, , \]
\[ \sigma_3 : \sqrt{1} \to -\sqrt{1} \; ; \; \mathbb{K}_{\sigma_3} = \mathbb{Q}(\sqrt{-1}) \, , \]
\[ \left\{ \begin{array}{l}
\sigma_4 : \sqrt{1} \to -\sqrt{1} \; ; \; \mathbb{K}_{\sigma_4} = \mathbb{Q}(\sqrt{-1}) \\
\sigma_4 : \sqrt{2} \to -\sqrt{2} \; ; \; \mathbb{K}_{\sigma_4} = \mathbb{Q}(\sqrt{-2}) \end{array} \right. \]

Note that: \( \sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = \sigma_3 \circ \sigma_3 = \sigma_4 \circ \sigma_4 = 1_K \)

\( \sigma_1 \) is an orthonormal field by Theorem 3.

\( \sigma_2 \) is orthonormal by either Theorem 4 or Theorem 5.

\( \sigma_3 \) is not even weakly orthonormal by Theorem 5 and Corollary 9.

\( \sigma_4 \) is orthonormal by Theorem 5.

Example 3: The field \( \mathbb{Q}(\sqrt{-1}) \) has one weakly orthonormal automorphism which is not orthonormal and one orthonormal automorphism \( (1_\mathbb{K}) \).

Example 4: Let \( \mathbb{K} \) be a splitting field of \( X^3 - 3 \) over \( \mathbb{Q} \). The Galois group \( \mathbb{G}(\mathbb{K} \mid \mathbb{Q}) \) is of order 6. Corollary 8 of Chapter III gives that \( 1_\mathbb{K} \) is orthonormal. The two automorphisms which move all three roots of \( X^3 - 3 \) in \( \mathbb{K} \) are not of order 2 in the Galois group so there are no Hermitian forms connected to them. The three automorphisms which move exactly two conjugates are of order 2 in \( \mathbb{G}(\mathbb{K} \mid \mathbb{Q}) \) and have fixed fields isomorphic to \( \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3}^{1/3}) \). Hence, by Theorem 4, these automorphisms are weakly orthonormal. The square roots which give \( \mathbb{K} \) when adjoined to the fixed fields are all of the form \( \sqrt{-3X^2} \) with \( X \) in the fixed field; thus, by Theorem 5, these three automorphisms are not orthonormal.
LITERATURE CITED


Vector spaces of countable dimension over algebraic number fields.