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

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 ς is an automorphism such that(Formula not captured by OCR)then &sigman; 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 ς 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 ς be an arbitrary automorphism over algebraic number field K with(Formula not captured by OCR) Criteria, depending on the fixed field of ς in K and the generator of KL over the fixed field of ς, are given to determine whether or not ς 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. Ames
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.

1098m

TABLE OF CONTENTS

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 K is a field and σ is an automorphism such that $\sigma \circ \sigma = \mathbb{1}_K$ then σ 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 σ has a ± 1 orthogonal basis (an orthonormal basis). A field K is called weakly orthonormal (orthonormal) if and only if $\mathbb{1}_K$ 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 σ be an arbitrary automorphism over algebraic number field K with $\sigma \circ \sigma = \mathbb{1}_K$. Criteria, depending on the fixed field of σ in K and the generator of K over the fixed field of σ, are given to determine whether or not σ is orthonormal (weakly orthonormal).

CHAPTER I

INTRODUCTION

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

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

$$H(x,y) = \overline{H(y,x)}, \quad \forall x,y\in E.$$

We shall call such a form a Hermitian form over K with respect to σ and denote the class of all such H by (K,σ). 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 σ with $\sigma\circ\sigma = 1_K$ defines at least one Hermitian form over a K-vector space E.

A (K,σ)-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 H. Attempts to classify spaces (E, H) up to orthogonal automorphism have, for this reason, been restricted to the cases of finite and denumerable dimensions.

Again let σ be an automorphism of a commutative field K with $\sigma \circ \sigma = 1_K$. We shall say that σ is orthonormal if and only if every $\aleph_0$-dimensional semisimple K-vector space with $H \in (K, \sigma)$ has an orthonormal basis. If 1_K is orthonormal then we shall say that the field K is orthonormal (i.e., K is orthonormal if and only if every $\aleph_0$-dimensional vector space (E, ϕ) over K with a symmetric bilinear form has an orthonormal basis). We shall say that σ is weakly orthonormal is and only if every $\aleph_0$-dimensional semisimple vector space (E, H) with $H \in (K, \sigma)$ admits of an orthogonal decomposition, $E = F \dotplus G$, such that F has an orthonormal basis and G has a negative orthonormal basis (i.e., an orthogonal basis $\{g_i\}$ with $\|g_i\| = -1$ for all i). If 1_K is weakly orthonormal, then we shall say that K is 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: ([2], Corollary 4, pp.290) Let K be a not formally real field with char $K \neq 2$. If (E, ϕ) is an $\aleph_0$-dimensional K-vector space with a non-degenerate, symmetric bilinear form ϕ then (E, ϕ) admits of an orthonormal basis if and only if there is an $\aleph_0$-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, ϕ) with $\phi \in (K, 1_K)$ 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 rôle 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, ϕ) 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,ϕ) we shall automatically mean that the form ϕ is symmetric. If we write (E,H) we shall mean that H is an arbitrary Hermitian form.

If Λ 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 $E = \overset{\perp}{\bigoplus}_{t\in\Lambda} F_t$ 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 Q. If $K(\theta)$ is a simple algebraic extension of K with $[K(\theta):K] = n$ and $x \in K(\theta)$ then x has a unique representation as a polynomial in θ of degree less than n. We denote the degree of this polynomial by $\partial_\theta(x)$. All field theoretic notation is consistent with [10].

CHAPTER II

ORTHONORMAL FIELDS

Some examples of orthonormal fields are the complex numbers C, the algebraic closure of the rationals Q in 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 such that the equation $\sum_1^q (-1)X_i^2 = 1$ 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 $\aleph_0$-dimensional K-vector space possesses an infinite dimensional totally isotropic subspace.

Corollary 3: A field K is orthonormal if and only if every semisimple $\aleph_0$-dimensional K-vector space has a non zero isotropic vector.

Corollary 4: Let K be an orthonormal field and $\{a_i\}_{i\geq 1}$ be a sequence of non zero elements of K. Then there are elements $a_2, \cdots, a_m$ in the sequence and elements $\alpha_1, \cdots, \alpha_m$ in the field K with $\alpha_1 \neq 0$ such that $\sum_1^m a_i \alpha_i^2 = 1$.

Corollary 5: Let K be an orthonormal field and $\{a_i\}_{i\geq 1}$ be a sequence of non zero elements of K. Then there are elements $a_2, \cdots, a_q$ in the sequence and elements $\alpha_1, \cdots, \alpha_q$ in the field K with $\alpha_1 \neq 0$ such that $\sum_1^q a_i \alpha_i^2 = 0$.

Corollary 6: Let K be a field then K is an orthonormal field if and only if for every sequence $\{a_i\}_{i\geq 1}$ of non zero elements of K there are elements $a_2, \cdots a_m$ in the sequence and elements $\alpha_1, \cdots, \alpha_m$ in the field K with $\alpha_1 \neq 0$ such that $\sum_1^m a_i \alpha_i^2 = 1$.

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 $\{-1, -1, \cdots\}$ there exists $\alpha_1, \cdots \alpha_m$ in the field with $\alpha_1 \neq 0$ and such that $\sum_1^m (-1)\alpha_i^2 = 1$, i.e. $\sum_1^m \alpha_i^2 = -1$. Let (E, ϕ) be an $\aleph_0$-dimensional semisimple K-vector space then (E, ϕ) has an orthogonal basis, say $\{e_i\}_{i\geq 1}$. Since (E, ϕ) 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 $\|e_2\|, \cdots, \|e_m\|$ in the sequence and elements $\alpha_1, \cdots, \alpha_m$ in the field such that $\sum_1^m \|e_i\| \alpha_i^2 = 1$. We now consider the sequence $\{-\|e_i\|\}_{i \geq m+1}$. By hypothesis we find $-\|e_{m+2}\|, \cdots, -\|e_{m+q}\|$ and elements of the field $\alpha_{m+1}, \cdots, \alpha_{m+q}$

such that $\sum_{m+1}^{m+q} \|e_i\| \alpha_i^2 = 1$ or $\sum_{m+1}^{m+b} \|e_i\| \alpha_i^2 = -1$. We now have that the non zero vector $\sum_1^{m+b} \alpha_i e_i$ 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 K be an orthonormal field and $K(\theta)$ a simple algebraic extension then $K(\theta)$ is orthonormal.

Proof: Assume $[K(\theta) : K] = m$. Let (E, ϕ) be an arbitrary $\aleph_0$-dimensional $K(\theta)$-vector space. We must show that (E, ϕ) contains a non zero isotropic vector. Let $\{e_i\}_{i \geq 1}$ be an orthogonal basis of (E, ϕ). By relabeling the subscripts of the e_i's we decompose (E, ϕ) in the following manner:

1) Split (E, ϕ) into "packets": $(E, \phi) = {}^{\perp}\bigoplus_{1=i}^{\infty} (E_i, \phi)$ with the $\dim E_i = \aleph_0$ for $i \geq 1$. Note that (E_i, ϕ) is semisimple.

2) Split each (E_i, ϕ) into packets: $(E_i, \phi) = {}^{\perp}\bigoplus_{j=1}^{\infty} (E_{ij}, \phi)$ with the $\dim E_{ij} = \aleph_0$ for $j \geq 1$. Note that (E_{ij}, ϕ) is semisimple.

.
.
.

m) Split each $(E_{ijk\cdots s\ell}, \phi)$ ($m-1$ subscripts) into packets: $(E_{ijk\cdots s\ell}, \phi) = {}^{\perp}\bigoplus_{p=1}^{\infty} (E_{ijk\cdots s\ell p}, \phi)$ with the $\dim E_{ijk\cdots s\ell p} = \aleph_0$ for $p \geq 1$. Note that $(E_{ijk\cdots s\ell p}, \phi)$ is semisimple.

Fix an $ijk\cdots s\ell$.

Step 1) We assert that each vector space $(E_{ijk\cdots s\ell p}, \phi)$ contains a non zero vector X such that $\partial_0(\|X\|) \leq m-2$.

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 $(E_{ijk\cdots s\ell p'}, \phi)$ This space is semisimple and it has an orthogonal basis, say $\{f_i\}_{i\geq 1}$. Now $\|f_i\| = \sum_{j=0}^{j=m-1} a_{ij}\theta^j$ with $a_{ij} \in K$ and by supposition $\partial_0(\|f_i\|) = m-1$. 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 $a_{2,m-1}, \cdots, a_{q,m-1}$ in the sequence and $\alpha_1, \cdots, \alpha_q$ in K with $\alpha_1 \neq 0$ such that $\sum_1^q a_{i,m-1}\alpha_i^2 = 0$. Now $\sum_1^q \alpha_i f_i \neq 0$ since $\alpha_1 \neq 0$ and $f_1 \neq 0$. We have $\partial_0(\|\sum_1^q \alpha_i f_i\|) < m-1$ contrary to the supposition.

Therefore, for each $p \geq 1$, $(E_{ijk\cdots s\ell p}, \phi)$ has a non zero vector $e_{\ell p}$ such that $\partial_0(\|e_{\ell p}\|) \leq m-2$ and thus $(E_{ijk\cdots s\ell}, \phi)$ contains an infinite set of linearly independent mutually orthogonal vectors $\{e_{\ell p}\}_{p\geq 1}$:

Step 2) Now let $ijk\cdots s$ remain fixed but vary ℓ. We have from Step 1 that for each $\ell \geq 1$ there exists an infinite set of linearly independent mutually orthogonal vectors $\{e_{\ell p}\}_{p\geq 1}$ contained in $(E_{ijk\cdots s\ell}, \phi)$ such that $\partial_0(\|e_{\ell p}\|) \leq m-2$. We consider the following cases for each ℓ.

Case i) For one p, $\|e_{\ell p}\| = 0$ then we are done, since (E, ϕ) then contains a non zero isotropic vector.

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

Case iii) For every $e_{\ell p}$ we have that $\partial_0(\|e_{\ell p}\|) = m-2$. Reapply the method of Step 1) on the leading coefficients of $\{\|e_{\ell p}\|\}_{p\geq 1}$ to find a

non zero vector X in the space generated by $\{e_{sp}\}_{p\geq 1}$ (which is a subspace of $(E_{ij\ldots sr}, \phi)$) such that $\partial_0(\|X\|) < m-2$. We call this vector e_{sr}.

Therefore, from Cases i), ii) and iii) either (E, ϕ) has a non zero isotropic vector or $(E_{ij\ldots s}, \phi)$ has an infinite set of mutually orthogonal linearly independent vectors $\{e_{sr}\}_{r\geq 1}$ with $\partial_0(\|e_{sr}\|) < m-2$.

Continuing the process (if we don't find a non zero isotropic vector at one step) we find that (E, ϕ) has an infinite set of mutually orthogonal linearly independent vectors $\{u_i\}_{i\geq 1}$ such that $\partial_0(\|u_i\|) = 0$ (i.e. $\|u_i\| \in K$). Reapplying the method of Step 1 we find that (E, ϕ) has a non zero isotropic vector.

But (E, ϕ) 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, ϕ) with no non zero isotropic vectors and $N < \dim F < \aleph_0$?

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 Q then because Q is a perfect field, there is an element θ of K such that $K = Q(\theta)$. Furthermore, if $\bar{\theta} = \theta - p$ with $p \in Q$ then $Q(\theta) = Q(\bar{\theta})$.

Definition 1: Let N and n be two positive integers then we define

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

Theorem 2: Let $Q(\theta)$ be a finite algebraic extension of the rationals Q with $[Q(\theta):Q] = n$. Let N be an arbitrary positive integer then any semisimple $Q(\theta)$-vector space (E,ϕ) 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 $Q(\theta)$ is a finite algebraic extension of Q with $[Q(\theta):Q] = n$, then any element α of $Q(\theta)$ has a unique representation as a polynomial in θ of degree less than or equal to $n-1$ with coefficients in Q. We denote by $\partial_\theta(\alpha)$ the degree of this polynomial.

Lemma 1: Let $Q(\theta)$ be a finite algebraic extension of Q and $[Q(\theta):Q] = n$. If $\sum_0^m a_i \theta^i \in Q(\theta)$ with $a_m \neq 0$

and $m<n$ then there is $\bar{\theta}$ in $Q(\theta)$ such that

1) $Q(\theta) = Q(\bar{\theta})$,

2) $\sum_0^m a_i \theta^i = \sum_0^m c_i \bar{\theta}^i$,

3) $c_i \neq 0$ and $\operatorname{sign} a_m = \operatorname{sign} c_i$; $0 \leq i \leq m$.

Proof of Lemma 1: If $m = 0$ we take $\theta = \bar{\theta}$.

If $m > 0$ then we set

$$\sum_0^m a_i \theta^i = \sum_0^m a_i (\theta - p + p)^i = \sum_0^m c_i (\theta - p)^i \text{ for } p \in Q,\ p > 0 \ ;$$

$$c_{m-q} = \sum_0^q \binom{m-i}{q-i} p^{q-i} a_{m-i} \ .$$

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, $\operatorname{sign} a_m = \operatorname{sign} c_i$. Further, $Q(\theta) = Q(\theta - p)$, i.e. we set $\bar{\theta} = \theta - p$.

Lemma 2: Let $Q(\theta)$ be an algebraic extension of Q with $[Q(\theta) : Q] = n$. Let $a_1, \cdots, a_\ell$ be elements of $Q(\theta)$ such that $a_i = \sum_{0=j}^{m=j} b_{ij} \theta^j$ for each i $(1 \leq i \leq \ell)$ and $m < n$. Furthermore, assume that $b_{im} \neq 0$ $(1 \leq i \leq \ell)$ and that $\operatorname{sign} b_{im} = \operatorname{sign} b_{jm}$ for $1 \leq i, j \leq \ell$; then there exists $\bar{\theta} \in Q(\theta)$ such that

1) $Q(\theta) = Q(\bar{\theta})$,

2) $\sum_{0=k}^{m=k} b_{ik} \theta^k = \sum_{0=k}^{m=k} c_{ik} \bar{\theta}^k$; $c_{ik} \neq 0$ all i, k,

3) $\operatorname{sign} b_{im} = \operatorname{sign} b_{jm}$ for all i, k.

Proof of Lemma 2: We set $\bar{\theta} = \theta - p$ 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 $\ell < \infty$.

Definition 2: Let $Q(\theta)$ be a finite algebraic extension of Q with $[Q(\theta):Q]=n$. Let $X\in Q(\theta)$, $X\neq 0$, and let m be an integer such that $0\leq m<n$. Then we shall say that X has an induced degree m (denoted $\bar{\partial}_\theta(X)=m$) if and only if there is an element $\alpha\in Q(\theta)$ such that $\partial_\theta(\alpha^2 X)=m$.

Remark: We note that X may admit various induced degrees.

Lemma 3: Let $Q(\theta)$ be a finite extension of the rationals with $[Q(\theta):Q]=n>1$. If $X\in Q(\theta)$ with $X\neq 0$ we may have either $\bar{\partial}_\theta(X)=n-1$ or $\bar{\partial}_\theta(X)=n-2$.

Proof of Lemma 3: We can always achieve this by multiplying X by a suitable power of θ.

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 proceeding lemmas to complete the proof of Theorem 2.

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

(E,ϕ) is semisimple, so it has an orthogonal basis $\{e_i\}_{1\leq i\leq g(N,n)}$ with $\|e_i\|\neq 0$. Therefore, by multiplying our basis vectors $\{e_i\}$ by suitable scalars $\gamma_i\in Q(\theta)$ we have by Lemma 3 that $\partial_\theta(\|\gamma_i e_i\|)>n-3$ for each i. Call this new basis $\{\bar{e}_i\}_{1\leq i\leq g(N,n)}$ $(\bar{e}_i=\gamma_i e_i)$.

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 $\{\bar{e}_i\}_{1 \le i \le g(N,n)}$ whose lengths have a degree in Θ over Q of $n-1$.

Case 2) There are at least $2 \cdot 4^{4(n-1)-3} \cdot N - 1$ vectors in the basis $\{\bar{e}_i\}_{1 \le i \le g(N,n)}$ whose lengths have a degree in Θ over 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 $\bar{e}$ in the basis $\{\bar{e}_i\}_{1 \le i \le g(N,n)}$ whose lengths (as minimal polynomials in Θ) have degree $n-1$ and positive leading coefficients.

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

Assume that Case 1a) holds; then we may choose vectors out of the basis $\{\bar{e}_i\}_{1 \le i \le g(N,n)}$ say $\{f_i\}_{1 \le i \le 4^{4n-3} \cdot N}$ with $\|f_i\| = \sum_{j=0}^{j=n-1} a_{ij} \Theta^j$ such that $a_{i,n-1} > 0$, $1 \le i \le 4^{4n-3} \cdot N$. Call

the subspace generated by these vectors F. Note that $\{f_i\}_{1 \le i \le 4^{4n-3} \cdot N}$ is an orthogonal basis and that (F, ϕ) is semisimple.

By Lemma 2 we may change to a new generator $\bar{\theta}$ of $Q(\theta)$ such that $\|f_i\| = \sum_{j=0}^{j=n-1} b_{ij} \bar{\theta}^j$ with $b_{ij} > 0$ for each i with $1 \le i \le 4^{4n-3} \cdot N$ and each j with $1 \le j \le n-1$.

We divide the basis $\{f_i\}_{1 \le i \le 4^{4n-3} \cdot N}$ into $4^{4(n-1)} \cdot N$ disjoint packets $\{f_{4j+1}, f_{4j+2}, f_{4j+3}, f_{4j+4}\}$. For each packet, by Theorem M, there exist rationals $\alpha_{4j+1}, \alpha_{4j+2}, \alpha_{4j+3}, \alpha_{4j+4}$, not all zero such that

$$\sum_{t=1}^{t=4} b_{4j+t,n-1} \alpha_{4j+t}^2 = 1.$$

Then we define $\bar{f}_j = \sum_{t=1}^{t=4} \alpha_{4j+t} f_{4j+t}$ for each j with $1 \le j \le 4^{4(n-1)} \cdot N$.

Then $\{\bar{f}_j\}_{1 \le j \le 4^{4(n-1)} \cdot N}$ is a set of mutually orthogonal linearly independent vectors. Define F_{n-1} to be the space generated by $\{\bar{f}_j\}_{1 \le j \le 4^{4(n-1)} \cdot N}$. Then (F_{n-1}, ϕ) is semisimple with orthogonal basis $\{\bar{f}_j\}$. Also for each j we have that $\|\bar{f}_j\| = \sum_{k=0}^{k=n-1} h_{jk} \bar{\theta}^k$ with $h_{j,n-1} = 1$ and $h_{jk} > 0$ for $1 \le k \le n-1$.

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:

i) $\dim F_{n-K} = 4^{4(n-K)} \cdot N$ and (F_{n-K}, ϕ) is semisimple.

ii) (F_{n-K}, ϕ) has an orthogonal basis $\{U_i\}_{1 \le i \le 4^{4(n-K)} \cdot N}$ such that:

a) $\|U_i\| = \sum_{n-K}^{n-1} \lambda_j \bar{\theta}^j + \sum_{j < n-K} c_{ij} \bar{\theta}^j$ for all i; $1 \le i \le 4^{4(n-K)} \cdot N$,

b) $\lambda_j > 0$ for all j ; $n-K \le j \le n-1$,

c) $c_{ij} > 0$ for all i, j , $1 \le i \le 4^{4(n-K)} \cdot N$ and $j < n-K$.

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

Case 1aA). Suppose there exists a set

$$\{u_{i_\ell}\}_{1 \le \ell \le M} \subset \{u_i\}_{1 \le i \le 4^{4(n-K)} \cdot N}$$

such that $c_{i_\ell\, n-K-1} = c_{i_m\, n-K-1}$ for all m, ℓ with $1 \le m, \ell \le M$ and $M \ge 4^{4(n-K-1)} \cdot N$. Then select any $4^{4(n-K-1)} \cdot N$ of the u_{i_ℓ}'s, say $\{u_{i_\ell}\}_{1 \le \ell \le 4^{4(n-K-1)} \cdot N}$ and let them generate the F_{n-K-1} . F_{n-K-1} has the required properties; $\lambda_{n-K-1} = c_{i_\ell\, n-K-1}$ $(1 \le \ell \le 4^{4(n-K-1)} \cdot N)$.

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

Since we shall worry only about the coefficients $c_{i,\, n-K-1}$ ($n-K$ fixed) we shall put $c_{i,\, n-K-1} = c_i$. Clearly either (I) more than or exactly one half of the c_i's are greater than or equal to λ_{n-K} or (II) more than or exactly one half of the c_i's are less than or equal to λ_{n-K} ; $(1 \le i \le 4^{4(n-K)} \cdot N)$.

Without loss of generality, assume that (I) holds. We relabel the c_i's (and hence the corresponding u_i's), so that

$$0 < \lambda_{n-K} \le c_1 \le \cdots \le c_{(4^{4(n-K)} \cdot N)/2} .$$

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

$$2 \cdot 4^3 \cdot 4^{4(n-K-1)} \cdot N - 4 \cdot 4^{4(n-K-1)} \cdot N - 4^{4(n-K-1)} \cdot N > 20 \cdot 4^{4(n-K-1)} \cdot N,$$

there are at least $20 \cdot 4^{4(n-K-1)} \cdot N$ of the c_i's which are strictly greater than $c_{4 \cdot 4^{4(n-K-1)} \cdot N}$. Thus, we may construct a subsequence of the one above, relabeling c_i's is necessary (and hence the corresponding

u_i's), such that:

$$0<\lambda_{n-k}\leq c_1\cdots\leq c_{4\cdot 4^{4(n-k-1)}\cdot N}\leq c_{4\cdot 4^{4(n-k-1)}\cdot N+1}\leq\cdots\leq c_{20\cdot 4^{4(n-k-1)}\cdot N}.$$

By the Archimedian Property of the rationals, we choose a positive rational p such that:

$$0<c_1\leq\cdots\leq c_{4\cdot 4^{4(n-k-1)}\cdot N}\leq p\lambda_{n-k}\leq c_{4\cdot 4^{4(n-k-1)}\cdot N+1}\leq\cdots\leq c_{20\cdot 4^{4(n-k-1)}\cdot N}.$$

Now let $\bar{\bar{\theta}}=\bar{\theta}/p$ then $\sum_0^{n-1}a_i\bar{\theta}^i=\sum_0^{n-1}a_ip^i\bar{\bar{\theta}}^i$ in $Q(\theta)\left(=Q(\bar{\theta})=Q(\bar{\bar{\theta}})\right)$. We have

$$\|u_i\|=\sum_{j<n-k}c_{ij}p^j\bar{\bar{\theta}}^j+\sum_{n-k}^{n-1}\lambda_jp^j\bar{\bar{\theta}}^j.$$

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

For each u_i with $1\leq i\leq 4\cdot 4^{4(n-k-1)}\cdot N$ we choose four distinct u_j's with $4\cdot 4^{4(n-k-1)}\cdot N+1\leq j\leq 20\cdot 4^{4(n-k-1)}\cdot N$; call them u_{i1}, u_{i2}, u_{i3}, u_{i4}. In this way, we divide $\{u_i\}_{1\leq i\leq 20\cdot 4^{4(n-k-1)}\cdot N}$ into $4\cdot 4^{4(n-k-1)}\cdot N$ mutually disjoint packets $\{u_i,u_{i1},u_{i2},u_{i3},u_{i4}\}$.

Now

$$\|u_i\|=\sum_{n-k}^{n-1}\lambda_jp^j\bar{\bar{\theta}}^j+c_ip^{n-k-1}\bar{\bar{\theta}}^{n-k-1}+\sum_{j<n-k-1}c_{ij}p^j\bar{\bar{\theta}}^j,$$

$$\|u_{it}\|=\sum_{n-k}^{n-1}\lambda_jp^j\bar{\bar{\theta}}^j+c_{it}p^{n-k-1}\bar{\bar{\theta}}^{n-k-1}+\sum_{j<n-k-1}c_{itj}p^j\bar{\bar{\theta}}^j$$

with $c_ip^{n-k-1}<p^{n-k}\lambda_{n-k}$ 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:

$$p^{n-k}\lambda_{n-k}-c_ip^{n-k-1}>0,$$
$$p^{n-k}\lambda_{n-k}-c_{it}p^{n-k-1}<0\ ;\ (1\leq t\leq 4).$$

Therefore, by Theorem M the quadratic form

$$(p\lambda_{n-k} - c_i)X_0^2 + \sum_{t=0}^{t=4} (p\lambda_{n-k} - c_{it})X_t^2$$

has a non-trivial zero in the rationals; say $(\alpha_{i0}, \alpha_{i1}, \alpha_{i2}, \alpha_{i3}, \alpha_{i4})$. Let $\alpha_i = \sum_{t=0}^{t=4} \alpha_{it}^2$ then we have that

$$\alpha_i(p\lambda_{n-k}) = (c_i\alpha_{i0}^2 + \sum_{t=1}^{t=4} \alpha_{it}^2 c_{it}).$$

We define $\bar{u}_i = \alpha_{i0}u_i + \sum_{t=1}^{t=4} \alpha_{it}u_{it}$ for each i. Then $\{\bar{u}_i\}_{1 \le i \le 4\cdot 4^{4(n-k-1)}\cdot N}$ is a mutually orthogonal set of linearly independent vectors out of F_{n-k} and

$$\|\bar{u}_i\| = \alpha_i\left(\sum_{n-k}^{h-1} \lambda_j p^j \bar{\Theta}^j + p^{n-k-1}(p\lambda_{n-k})\bar{\Theta}^{n-k-1}\right) + \sum_{j<n-k-1} p^j d_{ij} \bar{\Theta}^j$$

with $1 \le i \le 4\cdot 4^{4(n-k-1)}\cdot N$ and $d_{ij} = \alpha_{i0}^2 c_{ij} + \sum_{t=1}^{t=4} \alpha_{it}^2 c_{it,j}$.

Changing back to the generator $\bar{\Theta}$ of $Q(\Theta)$ we have that

$$\|\bar{u}_i\| = \alpha_i\left(\sum_{n-k}^{n-1} \lambda_j \bar{\Theta}^j + p\lambda_{n-k}\bar{\Theta}^{n-k-1}\right) + \sum_{j<n-k-1} d_{ij} \bar{\Theta}^j.$$

Define λ_{n-k-1} to be $p\lambda_{n-k}$; by our induction assumption c) we have $d_{ij} > 0$ for all i, j. Therefore

$$\|\bar{u}_i\| = \alpha_i \sum_{n-k-1}^{n-1} \lambda_j \bar{\Theta}^j + \sum_{j<n-k-1} d_{ij} \bar{\Theta}^j, \quad (1 \le i \le 4\cdot 4^{4(n-k-1)}\cdot N.$$

We finally split $\{\bar{u}_i\}_{1 \le i \le 4\cdot 4^{4(n-k-1)}\cdot N}$ into $4^{4(n-k-1)}\cdot N$ packets of four, $\{\bar{u}_{(4i)+1}, \bar{u}_{(4i)+2}, \bar{u}_{(4i)+3}, \bar{u}_{(4i)+4}\}$.

We have:

$$\|\bar{u}_{(4i)+t}\| = \alpha_{(4i)+t} \sum_{n-k-1}^{n-k} \lambda_j \bar{\Theta}^j + \sum_{j<n-k-1} d_{(4i)+t,j} \bar{\Theta}^j, \quad (1 \le t \le 4).$$

Now $\alpha_{(4i)+t} > 0$ for $1 \le t \le 4$ so by Theorem M there is a non-trivial solution $(\beta_{i1}, \beta_{i2}, \beta_{i3}, \beta_{i4})$ in the rationals to the equation

$$1 = \sum_{t=1}^{t=4} \alpha_{(4i)+t} X_t^2$$

Let $\bar{\bar{u}}_i = \sum_{t=1}^{t=4} \beta_{it} \bar{u}_{(4i)+t}$ then

$\| \bar{\bar{u}}_i \| = \sum_{n-k-1}^{n-1} \lambda_j \bar{\theta}^j + \sum_{j<n-k-1} m_{ij} \bar{\theta}^j$ with $m_{ij} > 0$.

Denote the space generated by the $\{\bar{\bar{u}}_i\}_{1 \le i \le 4^{4(n-k-1)}}$ by F_{n-k-1}. Then $F_{n-k-1} \subset F_{n-k}$ and (F_{n-k-1}, ϕ) with basis $\{\bar{\bar{u}}_i\}$ satisfies properties i) and ii) with $k+1$ in lieu of k.

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 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 α be an arbitrary element of K then for some integer q either the equation $\sum_1^q \alpha^{-1} X_i^2 + 1 = 0$ or $\sum_1^q \alpha^{-1} Y_i^2 - 1 = 0$

has a solution in K. Thus, either α or $-\alpha$ 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 Q such that K admits at most one ordering. First suppose that K is not formally real. By a result of Siegel ([9], Satz 1, p. 259) there are $\alpha_1, \alpha_2, \alpha_3$ $\alpha_4 \in K$ such that $\sum_1^4 \alpha_i^2 = -1$. Let (F, ϕ) be an arbitrary semi-simple four-dimensional space over K. Then F has an orthogonal basis $\{e_i\}_{1 \le i \le 4}$ and $\beta_i = \|e_i\|$, $1 \le i \le 4$. Now the field $Q(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2, \beta_3, \beta_4)$ is not formally real, thus every five-dimensional quadratic form in five variables with coefficients in $Q(\alpha_1, \cdots, \alpha_4, \beta_1, \cdots, \beta_4)$ has a non trivial zero in $Q(\alpha_1, \cdots, \beta_4)$ by the results of the Hasse-Minkowski theory. Thus the quadratic form $\sum_1^4 \beta_i X_i^2 + X_5^2$ has a non trivial zero in $Q(\alpha_1, \cdots, \beta_4)$ and so in K. Thus, either the vector space (F, ϕ) has a vector of length -1 or an isotropic vector in which case (F, ϕ) contains a hyperbolic plane and so also a vector of length -1. Therefore, since (F, ϕ) 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, ϕ) again be an arbitrary semisimple four-dimensional vector space with orthogonal basis $\{e_i\}_{1 \le i \le 4}$ and $\|e_i\| = \beta_i$, $1 \le i \le 4$. Now every element in K is either a sum of squares or its negative is the sum of squares.

Thus, for each i, there are $\alpha_{i1}, \cdots, \alpha_{iP_i}$ in K such that either $\beta_i = \sum_1^{P_i} \alpha_{ij}^2$ or $-\beta_i = \sum_1^{P_i} \alpha_{ij}^2$. We now observe that either the quadratic form $\sum_1^4 \beta_i X_i^2 + X_5^2$ or the quadratic form $\sum_1^4 \beta_i Y_i^2 - Y_5^2$ is indefinite at every archimedian completion of the global field $Q(\alpha_{11}, \cdots, \alpha_{1P_1}, \cdots, \alpha_{41}, \cdots, \alpha_{4P_4})$, and so at least one of the forms has a non trivial zero in $Q(\alpha_{11}, \cdots, \alpha_{4P_4})$ 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 $n = 4$ 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, ϕ) be a $\aleph_0$-dimensional semisimple vector space over K. By Theorem 3, K is weakly orthonormal, so E admits an orthogonal decomposition, $E = E^+ \dot{\oplus} E^-$, 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. 522). Indeed, if E admits of two decompositions $E = E^+ \dot{\oplus} E^- = F^+ \dot{\oplus} F^-$ then every vector $f^+ \in F^+$ can be written as the sum $f^+ = e^+ + e^-$ 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 $\aleph_0$ -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 $Q(\sqrt{-1})[X_0, X_1, X_2, \cdots]$. It is easy to show by induction that the quadratic form

$$\sum_{i=1}^{i=n} \prod_{1}^{i} (X_j - X_0) P_j^2 \quad ; \quad \prod_{1}^{0} (X_j - X_0) = 1,$$

has no non trivial zero for any $n \geq 1$ in $Q(\sqrt{-1})[X_0, X_1, \cdots]$. Thus, the vector space (E, ϕ) over the quotient field of $Q(\sqrt{-1})[X_0, X_1, X_2, \cdots]$ with orthogonal basis $\{e_i\}_{i \geq 1}$ and $\phi(e_i, e_i) = \prod_{1=j}^{i=j} (X_j - X_0)$ has no orthonormal basis. Therefore, the quotient field of $Q(\sqrt{-1})[X_0, X_1, X_2, \cdots]$ is not orthonormal.

CHAPTER IV

HERMITIAN FORMS

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

If (E, H) is a semisimple $\aleph_0$-dimensional vector space with $H \in (K, \sigma)$ then E has an orthogonal basis $\{e_i\}_{i \geq 1}$. Now for any $x \in E$, by the definition of a Hermitian form, $H(x,x) = \overline{H(x,x)}$ where $\sigma(H(x,x)) = \overline{H(x,x)}$. Thus, the lengths of all basis vectors e_i of E are in the fixed field K_σ. By restricting the scalars of E to the fixed K_σ we may induce a vector space $(\bar{E}, \bar{H})$ in the natural way that $\bar{E}$ is a K_σ-vector space with $x \in \bar{E}$ if and only if $x = \sum_1^\rho \lambda_i e_i$ with $\lambda_i \in K_\sigma$; and the form $\bar{H} = H|_{\bar{E} \times \bar{E}}$ is a symmetric non-degenerate bilinear form. Transition from $\bar{E}$ to $K \otimes_{K_\sigma} \bar{E}$ gives us E back again.

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

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

1) if the fixed field of σ in K is orthonormal then σ is orthonormal.
2) if the fixed field of σ in K is weakly orthonormal, then σ 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 σ an automorphism of K such that $\sigma \circ \sigma = \mathbb{1}$. If K_σ is the fixed field of σ 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 $Q \subset K_\sigma \subset K$ with $[K : Q] < \aleph_0$. Hence, $[K : K_\sigma] < \aleph_0$ and so $K_\sigma(\theta) = K$. But both $\sigma(\theta)\cdot\theta$ and $\sigma(\theta)+\theta$ are in K_σ. Thus, $X^2 - (\sigma(\theta)+\theta)X + \sigma(\theta)\cdot\theta$ is the minimal monic polynomial of θ over K_σ.

Theorem 5: Let K be an algebraic number field and σ an automorphism of K such that $\sigma \circ \sigma = \mathbb{1}_K$. Then σ is orthonormal if and only if either K_σ is orthonormal or there is $\beta \in K - K_\sigma$ and β is a square root of a totally positive element of K_σ.

Proof: We first prove the sufficiency. If K_σ is orthonormal then we

are done by Theorem 4. So suppose $K_\sigma(\beta) = K$. Then the norm of any element $\alpha \in K$ is of the form $N_{K:K_\sigma}(\alpha) = \alpha^2 - \beta^2\lambda$; $\alpha, \beta \in K_\sigma$, where $\lambda = \beta^2$. We have by hypothesis that λ is totally positive in K_σ .

Now let (E, H) be an arbitrary semisimple n_σ -dimensional vector space with $H \in (K, \sigma)$. 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 $\{e_i\}_{i \geq 1}$ be a fixed but arbitrary basis of E . Suppose that we have found $E_p \subset E$ such that $E_p = \perp\bigoplus_1^p P_i$ 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 $e_n \notin E_p$. If we can find a hyperbolic plane $P_{p+1} \subset E_p^\perp$ such that $e_n \in E_{p+1} = \perp\bigoplus_1^p P_i \perp\oplus P_{p+1}$ then we have proved the assertion. Now $e_n = \bar{e}_n + \bar{\bar{e}}_n$ where $\bar{e}_n \in E_p$ and $\bar{\bar{e}}_n \in E_p^\perp$; assume without loss of generality that $\bar{e}_n = 0$.

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

Case 2) Suppose $\|e_n\| = \beta_n \neq 0$. Let $K\{e_n\}$ be the one-dimensional subspace of $E_p^\perp$ generated by e_n , then $E_p^\perp = K\{e_n\} \perp\oplus F$ where F is semisimple. Restricting the scalars of F to K_σ we define the vector space $\bar{F}$ with symmetric

form $\overline{H} = H|_{E \times E}$. Using Theorem 2 of Chapter III we find five mutually orthogonal, linearly independent vectors f_1, f_2, f_3, f_4, f_5 in E (and thus in F) such that $\|f_1\| = \|f_2\| = \|f_3\| = \|f_4\| = \|f_5\| \neq 0$. We multiply f_5 by β . Since $\beta \cdot \sigma(\beta)$ is the additive inverse of a totally positive element, the quadratic form

$$\sum_1^4 x_i^2 + \sigma(\beta) \cdot \beta x_5^2$$

has a non trivial zero in K_σ by the Hasse-Minkowski theory. We shall call this zero $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$. Since f_1, f_2, f_3, f_4, f_5 are linearly independent, then $Z = \sum_1^4 \alpha_i f_i + \alpha_5 \beta f_5$ is a non zero isotropic vector in F. But F is semisimple so there is $X \in F$ such that $H(X, Z) \neq 0$. 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 $\|w\| = -\beta_n$. Hence, w and e_n will generate the hyperbolic plane P_{p+1} in $E_p^{\perp}$ which is desired. By Case 1 and Case 2 we have shown that $E = E^+ \overset{\perp}{\oplus} E^-$ where E^+ has an orthonormal basis and E^- has a negative orthonormal basis with $\dim E^- = \aleph_0$. We shall now complete the proof of the sufficiency by showing that E^- has an orthonormal basis. Let $\{f_i\}$ be the negative orthonormal basis of E^- . Then define $\overline{f}_i = \beta f_i$, each i. Then $\{\overline{f}_i\}$ is a basis of E^- and $\|\overline{f}_i\| = \lambda$, each i, where λ is totally positive by hypothesis. We restrict ourselves to the scalars of K_σ then $\overline{E}^- = \{x \in E^- \mid x = \sum_1^p \lambda_i \overline{f}_i ; \lambda \in K_\sigma\}$. $(\overline{E}^-, \overline{H})$ is a vector space over K_σ with non-degenerate bilinear form $\overline{H} = H|_{\overline{E}^- \times \overline{E}^-}$. We note that $\overline{H}$ is symmetric. Now the

length of every non zero vector in $(\overline{E}^-, \overline{H})$ is totally positive; thus, by the Hasse-Minkowski theory, every five-dimensional semisimple subspace of $\overline{E}^-$ has a vector of length 1. Suppose we have been able to find a subspace of $\overline{E}^-$ say $\overline{E}_p$, such that $\overline{E}_p = \overset{\perp}{\oplus}_1^p G_i$ where the G_i's are four-dimensional vector spaces with orthonormal bases and such that $\overline{f}_i \in \overline{E}_p$ for $i \leq p$. Let n be the smallest integer such that e_n is not in $\overline{E}_p$; if we can find a space G_{p+1} of dimension four with an orthonormal basis such that $\overline{f}_n \in \overset{\perp}{\oplus}_1^p G_i \overset{\perp}{\oplus} G_{p+1}$ then we have shown that $\overline{E}^-$ has an orthonormal basis. Assume, without loss of generality, that $\overline{f}_n \in E_p^{\perp}$.

Now let (V, ϕ) be an arbitrary four-dimensional vector space over K_σ with an orthonormal basis (the form ϕ is a symmetric bilinear form). Since $\|\overline{f}_n\|$ is totally positive, then V has an orthogonal basis $\{u_1, u_2, u_3, u_4\}$ with $\|u_1\| = \|\overline{f}_n\|$.

We let $K_\sigma\{\overline{f}_n\}$ be the one-dimensional subspace of $\overline{E}_p^{\perp}$, then $\overline{E}_p^{\perp} = K\{\overline{f}_n\} \overset{\perp}{\oplus} W$. Now W is semisimple and the lengths of all non zero vectors in W are totally positive. Thus, we can find three mutually orthogonal, linearly independent vectors V_2, V_3, V_3 in W such that $\|V_2\| = \|u_2\|$, $\|V_3\| = \|u_3\|$, $\|V_4\| = \|u_4\|$. Thus, the subspace $\overline{G}$ generated by $\{\overline{f}_n, V_2, V_3, V_4\}$ is orthogonally isomorphic to (V, ϕ) so $\overline{G}$ has an orthonormal basis. Hence, $\overline{G}$ is the G_{p+1} desired and so $\overline{E}^-$ has an orthonormal basis. Hence, E^- has an orthonormal basis. This concludes the proof of the sufficiency.

It remains to prove the necessity. So suppose σ is orthonormal. If $\sigma = 1_K$ then by definition $K = K_\sigma$ and K_σ is orthonormal. If $\sigma \neq 1_K$ then $K_\sigma \subsetneq K$ and, by Lemma 5, $K_\sigma(\sqrt{a}) = K$ where $a \in K_\sigma$. Hence, $\sqrt{a} \in K - K_\sigma$. Now let 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 σ is orthonormal there exist $\alpha_1, \alpha_2, \ldots \alpha_q$ in K for some q, such that $\sum_1^q N_{K:K_\sigma}(\alpha_j) = -1$. But $N_{K:K_\sigma}(\alpha_j) = \pi_j^2 - w_j^2 a$ for some $\pi_j, w_j \in K_\sigma$; each j. Thus, we have that

$$\sum_1^q \pi_j^2 + 1 - a \sum_1^q w_j^2 = 0.$$

Now if a is not positive under some ordering of K_σ the above equation can have no solution. (We can assume that K_σ is formally real, for if not, then a is totally positive to start with.) So we must have a totally positive in K_σ, 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 $\sum_1^n x_i^2 = -1$' in the case of classifying orthonormal algebraic number fields is equivalent in the classification of arbitrary automorphisms σ ($\sigma \circ \sigma = 1_K$) to the property 'there exist $x_1, \ldots, x_n$ in the field such that $\sum_1^n x_i \cdot \sigma(x_i) = -1$'.

We see by the proof of Theorem 5 that we may state the following corollary:

Corollary 9: Let K be an algebraic number field and σ an automorphism of K such that $\sigma \circ \sigma = 1_K$. Then σ is weakly orthonormal if and only if either K_σ is weakly orthonormal or there is $\beta \in K - K_\sigma$ and β is a square root of a totally positive element in K_σ.

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

Example 1: Consider the field $K = Q(3^{1/3})(\sqrt{7})(\sqrt{2})$. The four automorphisms of K are

$\sigma_1 = 1_K$ and $K_\sigma = K$,

σ_2 which sends $\sqrt{7}$ into $-\sqrt{7}$ and has fixed field $K_{\sigma_2} = Q(3^{1/3})(\sqrt{2})$,

σ_3 which sends $\sqrt{2}$ into $-\sqrt{2}$ and has fixed field $K_{\sigma_3} = Q(3^{1/3})(\sqrt{7})$,

σ_4 which sends $\sqrt{2}$ into $-\sqrt{2}$ and $\sqrt{7}$ into $-\sqrt{7}$; $K_{\sigma_4} = Q(3^{1/3})(\sqrt{14})$.

Note that $\sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = \sigma_3 \circ \sigma_3 = \sigma_4 \circ \sigma_4 = 1_K$.

By Theorem 3, σ_1 is not even weakly orthonormal.

But, since 2, 7 and 14 are totally positive elements, by Theorem 5 σ_2, σ_3 and σ_4 are all orthonormal. Thus, over this field, there are essentially only three distinct $\aleph_0$-dimensional semisimple vector space with non symmetric Hermitian forms. (Each of these admit of an orthonormal basis.)

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

$\sigma_1 = 1\!\!1_K$; $K_{\sigma_1} = K$,

$\sigma_2 : \sqrt{2} \to -\sqrt{2}$; $K_{\sigma_2} = Q(\sqrt{-1})$,

$\sigma_3 : \sqrt{-1} \to -\sqrt{-1}$; $K_{\sigma_3} = Q(\sqrt{2})$,

$\begin{cases} \sigma_4 : \sqrt{-1} \to -\sqrt{-1} \\ \sigma_4 : \sqrt{2} \to -\sqrt{2} \end{cases}$; $K_{\sigma_4} = Q(\sqrt{-2})$,

Note that: $\sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = \sigma_3 \circ \sigma_3 = \sigma_4 \circ \sigma_4 = 1\!\!1_K$

σ_1 is an orthonormal field by Theorem 3.

σ_2 is orthonormal by either Theorem 4 or Theorem 5.

σ_3 is not even weakly orthonormal by Theorem 5 and Corollary 9.

σ_4 is orthonormal by Theorem 5.

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

Example 4: Let K be a splitting field of $X^3 - 3$ over Q . The Galois group $G(K|_Q)$ is of order 6. Corollary 8 of Chapter III gives that $1\!\!1_K$ is orthonormal. The two automorphisms which move all three roots of $X^3 - 3$ in 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 $G(K|_Q)$ and have fixed fields isomorphic to $Q(3^{1/3})$. Hence, by Theorem 4, these automorphisms are weakly orthonormal. The square roots which give 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

[1] L. E. Dickson, Theory of Numbers Vol. II, Chelsea, New York, (1952).

[2] H. R. Fischer and H. Gross, 'Quadratic Forms and Linear Topologies II', Math. Ann. 159, (1964), 296-325.

[3] N. Jacobson, Lectures in Abstract Algebra Vol. II, Van Nostrand, Princeton, (1953).

[4] N. Jacobson, Lectures in Abstract Algebra Vol. III, Van Nostrand, Princeton, (1964).

[5] I. Kaplansky, 'Forms in Infinite Dimensional Spaces', Annais Acad. Bras. Ci XXII, (1950).

[6] S. Lang, Algebra, Addison-Wesley, Reading, (1965).

[7] O. T. O'Meara, Introduction to Quadratic Forms, Academic Press, New York, (1963).

[8] L. J. Savage, 'The Application of Vectoral Methods to Metric Geometry', Duke Math. J. 13, (1946), 521-528.

[9] C. L. Siegel, 'Darstellung total Positiver Zahlen durch Quadrate', Math. Zeitschr. 11, (1921), 246-275.

[10] B. L. van der Waerden, Algebra I, Springer-Verlag, Berlin-Gottigen-Heidelberg, (1959).