GENERALIZED QUATERNION ALGEBRAS OVER ALGEBRAIC NUMBER FIELDS

by

Robert C. Irwin

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

1 9 6 3

THE UNIVERSITY OF ARIZONA

GRADUATE COLLEGE

I hereby recommend that this dissertation prepared under my direction by Robert C. Irwin

entitled GENERALIZED QUATERNION ALGEBRAS OVER ALGEBRAIC NUMBER FIELDS

be accepted as fulfilling the dissertation requirement of the degree of Doctor of Philosophy

Gordon Pall — Dissertation Director — 4/29/63 — Date

After inspection of the dissertation, the following members of the Final Examination Committee concur in its approval and recommend its acceptance:*

Gordon Pall	4/29/63
D. S. Myers	4/24/63
Harry Cole	4/29/63
DP Squires	4/29/63
B Schweizer	4/29/63

*This approval and acceptance is contingent on the candidate's adequate performance and defense of this dissertation at the final oral examination. The inclusion of this sheet bound into the library copy of the dissertation is evidence of satisfactory performance at the final examination.

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in The University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in their judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Robert C. Irwin

ACKNOWLEDGMENT

I wish to express my thanks to Professor Gordon Pall for his assistance, encouragement, and patience during the writing of this dissertation.

CONTENTS

ABSTRACT

GENERALIZED QUATERNION ALGEBRAS
OVER ALGEBRAIC NUMBER FIELDS

Let K be an algebraic number field, R the ring of all algebraic integers of K, and Q a central simple algebra over K of degree n, containing an identity element. K can be identified with a subfield of Q. The dimension of Q as a vector space over K is n^2.

An order is a subring of Q which is a finitely generated R-module of rank n^2 and which contains the identity. A lattice is a subset of Q which is a free R-module of rank n^2 and which contains the identity. If R is a principal ideal ring, then every order is a lattice. In general, orders are projective R-modules. The usual notion of integrality applies to elements of an order, i.e., they are roots of monic polynomials with coefficients in R. Thus an order is a natural object in which to study arithmetic. To simplify certain arithmetical considerations, it is often assumed that an order is maximal. Maximal orders exist, and every order is contained in a maximal order. Orders and lattices in Q can also be defined with respect to R_p, the local ring of p-adic integers of K at the prime ideal p.

The elementary properties are analogous.

The main concern of this paper is with lattices, and the conditions under which a lattice is an order. Only the case n=2 is considered. In this case, Q is called a (generalized) quaternion algebra. The main advantage of this restriction is that the form which expresses the norm of an element of Q in terms of its coordinates with respect to any abasis is a quaternary quadratic form, called the norm-form of the basis, and the machinery of quadratic form theory can be applied. Furthermore, there exists a conjugation with the usual properties (anti-automorphic involution), and the coefficients of the norm-form can be expressed in terms of the basis elements and their conjugates.

Instead of dealing with the standard canonical basis of Q, it is possible to construct a quaternion algebra whose multiplication is expressed in terms of the matrix and adjoint matrix of an arbitrary non-singular ternary quadratic form f over K. In case f is integral, a canonical lattice L can be associated with f, in such a way that L is an order.

For the purposes of this paper, however, it is more important to show that it is possible to go the other way:

given a lattice L, which has an R-basis in which one element is the identity, the norm-form is used to "recover" a ternary form f, which is unique except for sign. Moreover, if L consists of integral elements, then it is shown that L is an order if and only if f is integral. The proof is an application of the associativity equations in Q, and makes essential use of the fact that Q is semi-simple.

Next, we consider maximal integral lattices. Because of their connection with the fundamentalness of the norm-forms, such lattices are called <u>fundamental</u>. Fundamental lattices exist, and every integral lattice with respect to R is contained in a fundamental lattice. Using the characterization of orders in terms of the integrality of f, we arrive at the result that if R is a principal ideal ring, then the maximality of an integral lattice implies that it is closed under multiplication, i.e., every fundamental lattice is an order. The proof is accomplished by considering the local behavior of the norm-form at each prime ideal. We do not know whether this is true without the assumption that R is a principal ideal ring.

It is now an easy step to show that if R is a principal ideal ring, then the concepts of maximal order and fundamental lattice coincide.

1

INTRODUCTION

The theory of associative algebras has received considerable attention since about the beginning of the twentieth century, and the modern theory can probably be said to have begun with the basic structure theorems of Wedderburn. Probably the first to give a systematic account of this theory, including a theory of arithmetic, was Dickson [8] , although many of the number-theoretic results were limited to algebras over the rational field, and to quaternion algebras in particular. The book of Albert [1] contains a more recent and somewhat simplified exposition of the structure theory. Deuring [7, Chapter 6] considered arithmetic in algebras over the quotient field of a Dedekind ring, and Schilling [14, Chapter 5] treated arithmetic in simple algebras using the language of valuation theory.

Arithmetical properties of rational quaternion algebras have been dealt with by Brandt [4] , Pall [11;12] , and others. Concerning the ideal class structure of algebras over number fields and its relation to the class structure of the fields, one may refer, for example, to papers of

Artin [2] and Schilling [13] .

The study of arithmetic in associative algebras can be reduced, by the classical structure theory, to that of simple algebras [8, Chapter 10] . It is usually assumed that the algebra contains an identity element and that its center coincides with its coefficient field. Thus a natural setting in which to study non-commutative arithmetic is a central simple associative algebra with identity, over an algebraic number field K whose ring of integers is R. One of the difficulties here is that the set of integral elements of the algebra, i.e., those which are roots of monic polynomials over R, is not generally closed under addition and multiplication. If we define an order as a subring of the algebra which contains the identity and which is a finitely generated R-module whose rank is the same as the dimension of the algebra, then the usual notion of integrality applies to the elements of an order, and orders are natural objects in which to carry on number-theortic investigations.

As pointed out by Dickson [8] , certain arithmetical questions are considerably simplified if it is assumed that the order is maximal. A maximal order is what Dickson called an "integral set". Maximal orders exist, and every order is contained in a maximal order. However, there may be many maximal orders in an algebra.

In addition to their importance in the arithmetic of algebras, orders also play a role in the integral representation theory of finite groups, in which the concept of order is a natural generalization of the concept of "group ring". By studying modules over orders, one obtains results in the integral representation theory. A recent treatment of this theory is given in Chapter 11 of [6] .

We define a lattice in a central simple algebra over K to be a subset of the algebra which is a free R-module whose rank is the dimension of the algebra, and which contains the identity. The main concern of this paper is with lattices, and the conditions under which a lattice is an order. If R is a principal ideal ring, then every order is a lattice. In general, an order is a projective R-module, i.e., a direct summand of a free R-module.

We will also have occasion to consider orders and lattices with respect to R_p, the local ring of p-adic integers of K at the prime ideal p. Since the definitions and some of the elementary properties are the same for this case, they will be combined, for purposes of brevity, under a single notation (see section 2).

To obtain a useful tool for the study of lattices, it will always be assumed that the algebra under consideration has dimension four over K. It will then be denoted by Q, and called a generalized quaternion algebra, or simply a

quaternion algebra. (The term "generalized" is a result of the departure from the ordinary Hamiltonian quaternions). This restriction has the advantage that the form which expresses the norm of an element $x = \sum x_i u_i$ of Q, where the x_i are in K and (u_0, u_1, u_2, u_3) is a K-basis of Q, in terms of the x_i as variables, is a quaternary quadratic form, called the norm-form of the basis, and the machinery of quadratic form theory can be applied. Furthermore, there exists a conjugation with the usual properties, i.e., an anti-automorphic involution on Q, and the coefficients of the norm-form can be expressed in terms of the basis elements and their conjugates.

In the case where K is the field of rational numbers, Pall [12] constructed a quaternion algebra Q whose multiplication is expressed in terms of the matrix and adjoint matrix of an arbitrary non-singular ternary quadratic form f over K, and, in case f is integral, constructed a lattice L in Q in such a way that L is an order. He then used the arithmetic of L to study certain properties of f and the associated norm-form. We will show that it is possible to extend this construction to the case where K is an arbitrary algebraic number field. (section 4).

For our study of lattices, however, it is more important to show that it is possible to go the other way: Given a lattice L which has an R-basis in which one element

is the identity, the norm-form is used to "recover" a ternary form f, which is unique except for sign. It is then shown that if L consists of integral elements, then L is an order if and only if f is integral.

Section 5 is concerned with maximal integral lattices. Because of their connection with the fundamentalness of the associated norm-forms, such lattices are called <u>fundamental</u>. There exist fundamental lattices with respect to R, and every integral lattice is contained in a fundamental lattice. It is shown that if R is a principal ideal ring, then the maximality of an integral lattice implies that it is closed under multiplication, i.e., every fundamental lattice is an order. We do not know if this is true without the assumption that R is a principal ideal ring. An interesting question is whether a similar result can be stated in an arbitrary central simple algebra, where the theory of quadratic forms is no longer available.

From the last stated result it is an easy step to show that if R is a principal ideal ring, then the concepts of maximal order and fundamental lattice coincide.

NOTATIONS; BASIC PROPERTIES OF THE ALGEBRA

Throughout this paper, K will denote an algebraic number field (a finite extension of the field of rationals), R will denote the ring of all algebraic integers of K, and p a (proper) prime ideal of R. R_p will mean the ring of quotients consisting of those elements a/b of K such that a is in R and b is in R - p, where R - p is the set-theoretic difference. R_p is thus the valuation ring of the p-adic valuation of K [17, p.38] . To simplify the statements of some of the definitions and theorems, the letter S will be used to denote either R or any one of the local rings R_p.

Q will always mean a quaternion algebra over K, and u will denote a 4-tuple (u_0,u_1,u_2,u_3) of linearly independent elements of Q over K. Thus u is a K-basis of Q. Occasionally, primes will be attached to u to distinguish between bases. The structure constants of a basis u will be denoted by u_{ijk}. These are the elements of K which are uniquely defined by the equations $u_iu_j = \sum u_{ijk}u_k$.

If u is a K-basis of Q, then F_u is the norm-form of

u, and, in case $u_0 = 1$, f_u is the ternary form associated with u. These forms are defined in section 4. f_u is defined only up to its sign, but this will not matter.

We will not use the concept of tensor product in its full generality, but only in the form $M \otimes R_p$, where M is a finitely generated R-module, and $\otimes$ denotes the tensor product over R. Then $M \otimes R_p$ is a finitely generated R_p-module, and may be identified with the module whose set of R_p-generators is the same as the set of R-generators of M. For a discussion of tensor products and such identifications, we refer to [6, p.495] .

An associative algebra over K is called <u>central</u> if the set of elements which commute with all elements of K is exactly K. It is called <u>simple</u> if it contains no proper two-sided ideals. The dimension over K of a central simple algebra is the square of an integer n, called the <u>degree</u> of the algebra [1, p.43] . Thus we can define a <u>quaternion algebra</u> Q as a central simple algebra of degree 2 over K, with an identity element. Since Q has an identity, K can be identified with a subfield of Q. Thus it will always be assumed that K is contained in Q. The degree reflects the fact that every element of Q is a root of a quadratic polynomial over K (theorem 2.2).

We note here that the terminology in the literature is somewhat inconsistent. The degree of an algebra was

called its "rank" by Dickson [8] . The dimension of an algebra as a vector space over K has been called "order" [8;14] and also "rank" [7] , the latter referring to its rank as a K-module. We will reserve the term "rank" for R-modules. What we have called "central" is also called "normal" [1;7] , although the former terminology is more descriptive and currently more popular.

Since K has characteristic zero, we have the following theorem [1, p.146] .

THEOREM 2.1. Every quaternion algebra over K has a basis u such that $u_0 = 1$, $u_1^2 = a$, $u_2^2 = b$, $u_1u_2 = u_3$, and $u_2u_1 = -u_3$, for some non-zero elements a and b of K. Conversely, every algebra over K for which there exists such a basis u is a quaternion algebra.

Using the canonical basis of theorem 2.1, the conjugate, trace, and norm of an element of Q can be conveniently defined, and their elementary properties can be easily proved. If u is a K-basis of Q with the property of theorem 2.1, and if $x = x_0 + x_1u_1 + x_2u_2 + x_3u_3$ is an element of Q, where $x_i \in K$, the conjugate of x is $\bar{x} = x_0 - x_1u_1 - x_2u_2 - x_3u_3$. The trace of x is $T(x) = x + \bar{x}$ and the norm of x is $N(x) = x\bar{x}$. Thus $T(x) = 2x_0$ and $N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ are elements of K. Furthermore, $N(x) = \bar{x}x$.

THEOREM 2.2. The mapping on Q defined by mapping each element of Q to its conjugate is an anti-automorphic involution of Q over K. Moreover, if x and y are in Q and c is in K, then $x^2-T(x)x + N(x) = 0$, and the norm and trace have the following properties:

(a) $T(x) = T(\bar{x})$ and $N(x) = N(\bar{x})$

(b) $T(cx) = cT(x)$ and $N(cx) = c^2N(x)$

(c) $T(x+y) = T(x) + T(y)$

(d) $N(xy) = N(x)N(y)$

(e) $T(x\bar{y}) = T(\bar{x}y)$

(f) $N(x + y) = N(x) + N(y) + T(x\bar{y})$

(g) $T(xy) = T(x)T(y) - T(x\bar{y})$

(h) $T(x_1x_2\ldots x_n) = T(x_nx_1x_2\ldots x_{n-1}), \quad x_i \in Q.$

PROOF. It is clear from the definition that $\overline{x+y} = \bar{x}+\bar{y}$ and $\bar{\bar{x}} = x$. Hence the conjugation mapping is involutory and is one-one onto Q. Since $\bar{u}_i = -u_i$ for $i = 1,2,3$, it is clear from the multiplication table of theorem 2.1 that $\overline{u_iu_j} = \bar{u}_j\bar{u}_i$ for $i = 0,1,2,3$. Furthermore, $\overline{cx} = c\bar{x}$. Thus if $x = \sum x_iu_i$ and $y = \sum y_ju_j$, then $\overline{xy} = \sum x_iy_j\overline{u_iu_j} = \sum x_iy_j\bar{u}_j\bar{u}_i = \sum y_j\bar{u}_j \sum x_i\bar{u}_i = \bar{y}\bar{x}$. Hence conjugation is an anti-automorphic involution of Q over K, and properties (a) through (d) follow. Moreover, $T(u_i\bar{u}_j) = T(\bar{u}_iu_j)$, hence $T(x\bar{y}) = \sum x_iy_jT(\bar{u}_iu_j) = T(\sum x_iy_j\bar{u}_iu_j) = T(\bar{x}y)$, proving (e). Property (f) is obvious, and (g) follows from the corresponding property of the basis elements. Finally, by applying (e), we have

$T(x_1x_2\ldots x_n) = T(x_1x_2\ldots\bar{\bar{x}}_n) = T(\bar{x}_{n-1}\bar{x}_{n-2}\ldots\bar{x}_1\bar{x}_n) = T(x_nx_1x_2\ldots x_{n-1})$. The identity $(x + \bar{x})x = x^2 + \bar{x}x$ implies that $x^2 - T(x)x + N(x) = 0$.

Certain of the properties of the above theorem will be useful in the ensuing discussion of the norm-forms of a lattice.

3

INTEGRALITY AND ORDERS

In this section we collect some of the basic properties of orders and the integral elements of Q. These properties are essentially known, but their presentation in the literature is rather scattered, and some do not seem to have been stated explicitly. With minor modifications, these properties hold in central simple algebras of arbitrary degree.

An element of Q is called integral over S (or simply integral if the ring S is understood), if it is a root of a monic polynomial whose coefficients are in S. A subset of Q is called integral over S if all its elements are integral over S.

We will denote by S[X] and K[X] the polynomial rings in one variable over S and K, respectively.

LEMMA 3.1 (Gauss). Let f be a monic polynomial in S[X], and suppose that $f = f_1 f_2$, where f_1 and f_2 are in K[X] and f_1 is monic. Then f_1 is in S[X].

PROOF. The roots of f in any extension field of K are integral over S, hence so are the roots of f_1. But f_1

is monic, so its coefficients, being polynomial functions of its roots, are also integral over S. Now S is a Dedekind ring and thus is integrally closed in K [16, pp. 270, 275] . It follows that f_1 is in S[X].

THEOREM 3.2. An element x of Q is integral over S if and only if T(x) and N(x) are in S.

PROOF. Suppose x is integral over S. If x is in K, then x is in S, since S is integrally closed. Then $T(x) = 2x$ and $N(x) = x^2$ are in S. Suppose x is not in K. Let f be a monic polynomial with coefficients in S such that $f(x) = 0$, and let f_1 be the polynomial $X^2 - T(x)X + N(x)$ in K[X]. Then by theorem 2.2, $f_1(x) = 0$. Since K[X] is a principal ideal ring, f and f_1 have a greatest common divisor g in K[X], and $g(x) = 0$. Since x is not in K, g must have degree two, so that $f_1 = ag$ for some non-zero element a of K. Therefore, f_1 divides f in K[X], and by lemma 3.1, f_1 is in S[X], i.e., T(x) and N(x) are in S. The converse follows from $f_1(x) = 0$.

LEMMA 3.3. Let M be an integral S-module contained in Q such that M contains a basis of Q over K. Let A be the set of all x in Q such that T(xy) is in S for all y in M. Let u be an arbitrary basis of Q over K, and B the set of all elements of K which appear as coefficients in the representation of the elements of A in terms of the basis u. Then there exists d in S such that B is contained in $d^{-1}S$.

PROOF. By the hypothesis, there is a basis u' of Q over K such that $u'_i \in M$ $(i = 0,1,2,3)$. Since M is an S-module, it can be assumed, after multiplying by a suitable element of S, that u' has the additional property that $u'_{ijk} \in S$ $(i,j,k = 0,1,2,3)$. Thus by the integrality of M, we have $T(u'_i u'_j) = \sum u'_{ijk} T(u'_k) \in S$, and since Q is simple over K, the determinant $\det(T(u'_i u'_j))$ is non-zero [7, p. 34]. If $u_i = \sum c_{ik} u'_k$ $(i = 0,1,2,3)$ and if $\sum a_i u_i \in A$, where $a_i \in K$, then

$$(1) \qquad T((\sum a_i u_i)u'_j) = \sum a_i c_{ik} T(u'_k u'_j) \in S \qquad (j = 0,1,2,3).$$

Considering (1) as a system of linear equations in the variables $\sum a_i c_{ik}$ $(k = 0,1,2,3)$ with coefficients in S, we have

$$(2) \qquad \sum a_i c_{ik} = b/\det(T(u'_i u'_j)) \qquad (b \in S,\ k = 0,1,2,3).$$

By multiplying equations (2) by a suitable element of S, which is independent of the coefficients a_i, we can obtain a matrix (c'_{ik}) with elements in S and non-zero determinant, such that $\sum a_i c'_{ik} \in S$ $(k = 0,1,2,3)$. Setting $d = \det(c'_{ik})$, we have $a_i \in d^{-1}S$. Since d does not depend on the coefficients a_i, it follows that B is contained in $d^{-1}S$.

A subring J of Q is called an <u>order</u> <u>over</u> S (or simply an <u>order</u> if S is understood) if J is a finitely generated S-module which contains the identity of Q and which contains a basis of Q over K. An order over S is

called maximal if it is not properly contained in an order over S. Note that the ring S is contained in all orders over S.

THEOREM 3.4. Let J be a subring of Q which contains S and contains a basis of Q over K. Then J is an order if and only if it is integral.

PROOF. Suppose J is an order, and let x be a non-zero element of J. Denote by J_i the submodule of J generated over S by the elements $x, x^2, \ldots x^i$. Then the J_i form an ascending chain of submodules of J. Since S satisfies the ascending chain condition for ideals and J is finitely generated over S, it follows that J satisfies the ascending chain condition for submodules [16, p. 158]. Thus there is an integer n such that $x^n \in J_{n-1}$. Therefore, there is a monic polynomial f, with coefficients in S, such that $f(x) = 0$, so that x is integral.

Conversely, suppose J is integral. If A is the set of all x in Q such that $T(xy) \in S$ for all $y \in J$, then J is contained in A, since J is an integral ring. Let u be a basis for Q over K contained in J. Then by lemma 3.3, the coefficients which occur in the representation of the elements of J in terms of the basis u are all contained in $d^{-1}S$ for some d in S. Thus J is a submodule of the free S-module generated by the basis $d^{-1}u$. Since this free module satisfies the ascending chain condition for submodules, it follows that J is finitely generated over S,

and is therefore an order.

THEOREM 3.5. <u>There exists an order over</u> S, <u>and every order is contained in a maximal order over</u> S.

PROOF. Let u be a basis for Q over K such that $u_0 = 1$. Let M be the free S-module generated by u, and let J be the set of all x in Q such that xM is a subset of M. Then J is evidently a subring of Q which contains S. Furthermore, since M contains 1, J is a submodule of M over S. Hence J is finitely generated over S. To prove that J is an order, it remains only to show that J contains a basis for Q over K. Let $x = \sum x_i u_i$ be an arbitrary element of Q, where $x_i \in K$, and let $y = \sum y_i u_i$ be an arbitrary element of M, where $y_i \in S$. There exists a non-zero element a of S such that $au_{ijk} \in S$ for all i,j,k. Then $au_j y = \sum y_i au_{jik} u_k \in M$ for all j, whence $au_j \in J$ for all j. Thus $x = \sum (a^{-1}x_j)au_j$ belongs to the sub-K-module of Q generated over K by J. It follows that J generates Q over K, i.e., J contains a K-basis of Q.

Suppose $J_1, J_2, \ldots$ is an ascending chain of orders, i.e., J_i is contained in J_{i+1} $(i = 1,2,\ldots)$. Then the union of all the J_i is an integral subring J of Q, hence by theorem 3.4, J is an order. By the ascending chain condition, there is an integer n such that $J_n = J_{n+1} = \ldots$, and consequently every order is contained in a maximal order.

In general, there may be many maximal orders in Q.

Suppose we call two maximal orders over S equivalent if they are isomorphic (as rings) under an inner automorphism of Q. Then if $S = R_p$, any two maximal orders are equivalent [3, p. 11] . If S = R, then, at least in the case where Q is not a division algebra, the number of equivalence classes is always finite [13, p. 383] .

Concerning the structure of an order as an S-module, we have the following theorem:

THEOREM 3.6. Let J be an order over S. Then J is a projective S-module, and is isomorphic, as an S-module, to a direct sum $S \oplus S \oplus S \oplus A$, where A is an ideal of S. If S is a principal ideal ring, then we may take A = S, and J is then a free S-module.

PROOF. It has been observed in the proof of theorem 3.4 than an order is a submodule of a free S-module. If S is a principal ideal ring, then such a module is necessarily free over S [5,p. 13] , and J is then isomorphic to a direct sum of four copies of S. In general, since the non-zero ideals of S are invertible [16, p. 274] , they are projective S-modules [5, p. 132] . Thus J is isomorphic to a direct sum of four ideals of S [5, p. 13] , hence is projective [5, p. 6] . Finally, it follows from [6, p. 150] that J is isomorphic to $S \oplus S \oplus S \oplus A$, where A is an ideal of S.

4

LATTICES AND NORM-FORMS

A subset L of Q is called a *lattice over* S (or simply a *lattice* if S is understood) if L is a free S-module which contains the identity of Q and which contains a basis of Q over K. Thus a lattice L is just a direct sum $\sum Su_i$, where u is a basis of Q over K. We call u an S-basis of L. Note that S is contained in all lattices over S.

If u is a basis of Q over K, we denote by F_u the quaternary quadratic form whose (symmetric) matrix is $\frac{1}{2}(T(u_i\bar{u}_j))$. Because of lemma 4.1, F_u is called the *norm-form* of u. It will turn out that the determinant of a norm-form is a non-zero square in K.

LEMMA 4.1. *If* u *is any basis for* Q *over* K, *and if* $x = \sum x_i u_i$, *where* $x_i \in K$, *then* $N(x) = F_u(x_0,x_1,x_2,x_3)$.

PROOF. $N(x) = \frac{1}{2}T(x\bar{x}) = \frac{1}{2}T(\sum x_i x_j u_i \bar{u}_j) =$

$$\frac{1}{2}\sum T(u_i\bar{u}_j)x_i x_j.$$

THEOREM 4.2. *If* L *is a lattice over* S, *then* L *is integral over* S *if and only if the coefficients of* F_u *are in* S *for every* S-*basis* u *of* L.

PROOF. Suppose L is integral over S, and let u be an S-basis of L. For a fixed pair of indices r and s, $(0 \leq r \leq 3,\ 0 \leq s \leq 3)$, put $x_r = x_s = 1$ and $x_k = 0$ for $k \neq r$, $k \neq s$. Then $x = \sum x_i u_i$ is in L, and $N(x) = F_u(x_0,x_1,x_2,x_3) = N(u_r)$ or $T(u_r\bar{u}_s)$ according as $r = s$ or $r \neq s$. Since N(x) is in S, it follows that the coefficients of F_u are in S. Conversely, suppose the coefficients of F_u are in S. Let $x = \sum x_i u_i \in L$ and write $1 = \sum e_i u_i$. Then $x_i \in S$ and $e_i \in S$ $(i = 0,1,2,3)$. Thus $N(x) = F_u(x_0,x_1,x_2,x_3) \in S$ and $T(x) = T(\bar{x}) = T(\sum e_i x_j u_i \bar{u}_j) = \sum T(u_i \bar{u}_j) e_i x_j \in S$. By theorem 3.2, x is integral over S.

If F_u is the norm-form of u and if V is a linear transformation on the variables of F_u, then F_uV will denote the form which results by applying V to F_u, and uV will denote the matrix product in which u is considered as a row vector and V is identified with its own matrix.

LEMMA 4.3. Let L and L' be lattices over S with S-bases u and u', respectively. Let V be the linear transformation defined by $u' = uV$. Then

(a) $F_{u'} = F_uV$

(b) L' is contained in L if and only if the coefficients of V are in S.

(c) $L = L'$ if and only if the coefficients of V are in S and the determinant of V is a unit of S.

PROOF. Let (v_{ij}) denote the matrix of V. Then

$T(u_i'\bar{u}_j') = T(\sum v_{ri}v_{sj}u_r\bar{u}_s) = \sum v_{ri}v_{sj}T(u_r\bar{u}_s)$, so that V transforms F_u to $F_{u'}$. If L' is contained in L, then $u_j' = \sum v_{ij}u_i \in L$, whence $v_{ij} \in S$ $(i,j = 0,1,2,3)$. Conversely, if the coefficients of V are in S, then u' is contained in L, hence so is L'. If L = L', then by (b), the coefficients of V and V^{-1} are in S, so that det(V) is a unit of S. If V has its coefficients in S and det(V) is a unit of S, then the coefficients of V^{-1} are in S, so that by (b), L = L'.

If u is a basis for Q over K, then the linear form h_u and the quadratic form g_u will be defined by

$$h_u = \tfrac{1}{2}\sum T(u_i)x_i$$

$$g_u = \tfrac{1}{4}\sum (T(u_i\bar{u}_j) - T(u_iu_j))x_ix_j,$$

where the x_i are variables. Then by theorem 2.2 (g), we have

$$F_u = h_u^2 + g_u. \tag{1}$$

In case $u_0 = 1$, g_u is a ternary form in the variables x_1,x_2,x_3, and (1) expresses the result of completing squares. In this case, the form g_u will be used in the following theorem to obtain necessary and sufficient conditions for a lattice to be an order.

THEOREM 4.4. *Let* L *be a lattice over* S, *and suppose* u *is an* S-*basis of* L *such that* $u_0 = 1$. *Then there exists a ternary quadratic form* f_u *with coefficients in* K, *unique except for sign, such that* g_u *is the adjoint of* f_u. *If* L *is integral over* S, *then* L *is an order over* S *if and only if*

the coefficients of f_u are in S.

PROOF. Define $u'_0 = 1$ and $u'_i = u_i - \frac{1}{2}T(u_i)$, $(i = 1,2,3)$. Then u' is a K-basis of Q and $T(u'_i) = 0$ $(i = 1,2,3)$. Thus by expressing the coordinates of u' in terms of the canonical basis of theorem 2.1, it is seen that

$$(2) \qquad u'_{ij0} = u'_{ji0} \quad \text{and} \quad u'_{ijk} = -u'_{jik} \qquad (i,j,k = 1,2,3).$$

Let $A = (A_{ij})$ denote the (symmetric) matrix of g_u. Then by theorem 2.2 (g),

$$2A_{ij} + \tfrac{1}{2}T(u_i)T(u_j) = T(u_i\bar{u}_j) =$$
$$T((u'_i + \tfrac{1}{2}T(u_i))(-u'_j + \tfrac{1}{2}T(u_j))) = -2u'_{ij0} + \tfrac{1}{2}T(u_i)T(u_j).$$

It follows that

$$(3) \qquad A_{ij} = -u'_{ij0} \quad \text{and} \quad A_{ii} = -(u'_i)^2 \qquad (i,j = 1,2,3).$$

Now define the matrix $a = (a_{ij})$ by

$$(4) \qquad a_{1j} = u'_{23j}\ ,\ a_{2j} = -u'_{13j}\ ,\ a_{3j} = u'_{12j} \quad (j = 1,2,3).$$

The associativity conditions $u'_i(u'_ju'_k) = (u'_iu'_j)u'_k$ result in the equations

$$(5) \qquad \sum u'_{jkr}u'_{irs} = \sum u'_{ijr}u'_{rks} \qquad (i,j,k = 1,2,3;\ s = 0,1,2,3),$$

where the summations are for $0 \le r \le 3$. Certain of these equations will be used to show that $A = \text{adj } a$, where adj denotes the adjoint, and then to express the multiplication table of the basis u in terms of the matrices a and A. For this purpose, we will use the notation (i,j,k,s) to denote

the equation which results from (5) when the subscripts i,j,k, and s have the indicated values. Displayed below on the right are the results of substituting into the equations on the left the values obtained from equations (2), (3), and (4).

$$(6)\qquad \begin{matrix}(k,k,j,i) : a_{ii}(a_{ij} - a_{ji}) = 0\\ (j,i,k,i) : a_{ii}(a_{jk} - a_{kj}) = 0\end{matrix} \qquad (i,j,k \text{ distinct}).$$

$$(7)\qquad \begin{matrix}(i,i,j,j) : A_{ii} = a_{jj}a_{kk} - a_{kj}^2\\ (i,i,k,k) : A_{ii} = a_{jj}a_{kk} - a_{jk}^2\end{matrix} \qquad (i,j,k \text{ distinct}).$$

$$(8)\qquad (i,i,j,i) : A_{ij} = a_{ki}a_{kj} - a_{kk}a_{ji} \quad (i<j, k\neq i, k\neq j).$$

$$(9)\qquad (1,2,3,0) : a_{11}A_{11} + a_{12}A_{12} + a_{13}A_{13} = a_{31}A_{13} + a_{32}A_{23} + a_{33}A_{33}.$$

Suppose $a_{ii} \neq 0$ for some i. Then equations (6) show that a is symmetric, and then equations (7) and (8) show that A = adj a. In any case, equations (7) show that $a_{ij} = \pm a_{ji}$ $(i \neq j)$.

Suppose that a is not symmetric. Then $a_{ii} = 0$ for i = 1,2,3, and we can assume, for instance, that $a_{12} = -a_{21} \neq 0$. Then $\det a = a_{12}(a_{23}a_{31} - a_{32}a_{13})$. If $a_{23} = \pm a_{32}$ and $a_{13} = \pm a_{31}$, with the same choice of sign, then det a = 0. Substituting equations (7) and (8) into equation (9) gives

$$a_{12}(a_{32}a_{31} - a_{13}a_{23}) = a_{12}(a_{13}a_{32} - a_{23}a_{31}), \text{ hence}$$

$$a_{32}a_{31} + a_{23}a_{31} = a_{13}a_{32} + a_{13}a_{23}.$$

If $a_{23} = \pm a_{32}$ and $a_{13} = \mp a_{31}$, with the opposite choice of sign, then $a_{23}a_{13} = 0$, and again det a = 0. Thus if a is not symmetric then it has zero determinant. But then det A = $(\det a)^2 = 0$, and hence det F_u = det g_u = det A = 0. It follows by lemma 4.3(a) that det $F_{u'} = 0$, and thus det $(T(u_i'u_j')) = \det (T(u_i'\bar{u}_j')) = 0$. But this contradicts the fact that Q is semi-simple [7, p. 34] . Therefore, a is symmetric and A = adj a. Letting f_u denote the form whose matrix is a, the first assertion of the theorem is proved, since it is clear that f_u is determined up to sign.

It is worth remarking at this point that in determining all associative algebras over the rational field of dimension 4 and rank 2, Dickson [9, p. 161] exhibited algebras which correspond to cases where our matrix a may be non-symmetric and may have rank zero, one, or two.

Using the multiplication table of u' given by (2), (3), and (4), the definition of u' in terms of u, and the fact that A = adj a, we arrive at the following multiplication table for u:

$$(10) \qquad u_i^2 = (-A_{ii} - \tfrac{1}{4}T(u_i)T(u_i)) + T(u_i)u_i,$$

$$u_iu_j = \left[-(a_{ik} + \tfrac{1}{2}T(u_j))(a_{jk} + \tfrac{1}{2}T(u_i)) + a_{kk}(a_{ij} + \tfrac{1}{2}T(u_k)) - a_{kk}T(u_k)\right] + (a_{ik} + \tfrac{1}{2}T(u_j))u_i + (a_{jk} + \tfrac{1}{2}T(u_i))u_j + a_{kk}u_k \qquad (i,j,k \text{ distinct}).$$

Suppose L is integral over S. Then $T(u_i) \in S$ and by

(1), $N(u_i) = A_{ii} + \frac{1}{4}T(u_i)T(u_i) \in S$. If L is an order, then the coefficients of the u_i in (10) belong to S, hence $a_{ii} \in S$ and $2a_{ij} \in S$ $(i,j = 1,2,3)$. Thus the coefficients of f_u are in S. Conversely, if the coefficients of f_u are in S, then

$$(a_{ij} + \tfrac{1}{2}T(u_k))(a_{ij} - \tfrac{1}{2}T(u_k)) = a_{ii}a_{jj} - A_{kk} - \tfrac{1}{4}T(u_k)T(u_k) \in S;$$
$$(a_{ij} + \tfrac{1}{2}T(u_k)) + (a_{ij} - \tfrac{1}{2}T(u_k)) = 2a_{ij} \in S \quad (i,j,k \text{ distinct}).$$

If the sum and product of two elements of K belong to S, then so does each of the elements, since S is integrally closed in K. Thus $(a_{ij} + \frac{1}{2}T(u_k)) \in S$ $(i,j,k$ distinct). It follows that the coefficients of the u_i in (10) are in S, so that L is an order. Q.E.D.

Instead of starting with a lattice and constructing a ternary form, it is possible to start with a ternary form f and construct a quaternion algebra Q and a lattice L in Q in such a way that if the coefficients of f are in R, then L is an order over R. Pall [12] has done this for the case where K is the rational field, and has used the arithmetical properties of the order L to study certain properties of f and the associated norm-form. In fact, it was Pall's method which suggested the possibility of going the other way, as we have done in theorem 4.4. The construction in [12] can be generalized to the case of an arbitrary algebraic number field K, as follows.

Let f be a ternary quadratic form of non-zero determinant and with coefficients in K. Let $a = (a_{ij})$ and $A = (A_{ij})$ be the matrices of f and adj f, respectively. Let Q be the algebra over K with a basis $(u_0=1, u_1, u_2, u_3)$ which has the following multiplication table:

$$(11)\quad \begin{aligned} &u_{ij0} = u_{ji0} = -A_{ij}, \quad u_{12j} = a_{3j}, \quad u_{13j} = -a_{2j}, \\ &u_{23j} = a_{1j}, \quad u_{ijk} = -u_{jik} \qquad (i,j,k = 1,2,3). \end{aligned}$$

By a non-singular linear transformation over K, f can be transformed to a diagonal form f'. Denote by Q' the algebra defined by (11) when f is replaced by f'. Theorem 1 of [12] is also valid for the present case, and shows that Q and Q' are isomorphic. Since f' is a diagonal form with non-zero determinant, it follows that the basis used to define Q' has the property of theorem 2.1. Thus Q', and hence also Q, is a quaternion algebra over K.

Suppose now that the coefficients of f are in R. Let $(w_0=1, w_1, w_2, \ldots, w_{n-1})$ be an integral basis for K over the rational field, where n is the degree of K over the rationals. Since $2a_{ij} \in R$ $(i,j = 1,2,3)$, the equations $2a_{ij} = \sum a_{ijr} w_r$ define rational integers a_{ijr} $(i,j = 1,2,3$; $r = 0,1,\ldots,n-1)$. Let (i,j,k) be any permutation of (1,2,3). Define $e_{kr} = 0$ or 1 according as a_{ijr} is even or odd, and define $e_k = \sum e_{kr} w_r$. Then $(a_{ij} \pm \tfrac{1}{2} e_k) \in R$.

Define the basis u' for Q over K by

$$u_0' = 1, \quad u_i' = u_i + \tfrac{1}{2}e_i.$$

Then $T(u_i') = e_i \in R$ and

$$T(u_i'\bar{u}_j') = 2A_{ij} + \tfrac{1}{2}e_ie_j = (a_{ik} + \tfrac{1}{2}e_j)(a_{jk} - \tfrac{1}{2}e_i) + (a_{ik} - \tfrac{1}{2}e_j)(a_{jk} + \tfrac{1}{2}e_i) + e_ie_j - 2a_{ij}a_{kk}.$$

Thus $T(u_i'\bar{u}_j') \in R$. Furthermore,

$$\tfrac{1}{2}T(u_i'\bar{u}_i') + A_{ii} + \tfrac{1}{4}e_i^2 = a_{jj}a_{kk} - (a_{jk} + \tfrac{1}{2}e_i)(a_{jk} - \tfrac{1}{2}e_i),$$

Hence $\tfrac{1}{2}T(u_i'\bar{u}_i') \in R$. It follows that the coefficients of $F_{u'}$ are in R, hence by theorem 4.2 the lattice $L = \sum Ru_i'$ is integral over R. Moreover,

$$F_{u'} = x_0^2 + \sum{}'e_ix_0x_i + \sum{}'(A_{ij} + \tfrac{1}{4}e_ie_j)x_ix_j = (x_0 + \tfrac{1}{2}\sum{}'e_ix_i)^2 + \sum{}'A_{ij}x_ix_j = h_{u'}^2 + \text{adj } f,$$

where $\sum'$ indicates summation over the indices 1,2,3. By theorem 4.4, $f = \pm f_{u'}$ and L is an order.

Theorem 4.4 implies that the determinant of a norm-form is the square of an element of K, since $\det F_u = \det g_u = \det(\text{adj } f_u) = (\det f_u)^2$. On the other hand we have

THEOREM 4.5. *If F is any quaternary quadratic form over K whose determinant is a non-zero square in K and whose first coefficient is 1, then there exists a*

quaternion algebra Q over K and a basis u of Q, such that $F = F_u$.

PROOF. Since F has first coefficient 1, we may complete squares and write $F = h^2 + g$, where h is a linear form in four variables and g is a ternary quadratic form. Since det F = det g is a square, g = adj f for some ternary form f over K. In the quaternion algebra Q associated with f, the above construction shows that we may select a basis u such that $F = F_u$.

5

FUNDAMENTAL LATTICES

A quaternary quadratic form F over K with non-zero determinant is called fundamental over S if the coefficients of F are in S, and for every quaternary form G with coefficients in S, and every linear transformation V with coefficients in S, the relation F = GV implies that the determinant of V is a unit of S.

An integral lattice L over S is called fundamental over S if it is maximal, i.e., if L is not properly contained in an integral lattice over S.

LEMMA 5.1. A lattice L is fundamental over S if and only if F_u is fundamental over S for every S-basis u of L.

PROOF. Suppose L is fundamental over S, and let u be an S-basis of L. If F_u is not fundamental over S, then there is quaternary form G and a linear transformation V, both with coefficients in S, such that $F_u = GV$ and det(V) is a non-unit of S. By lemma 4.3, $G = F_{u'}$, where $u' = uV^{-1}$, and L is contained in the integral lattice L' generated over S by u'. Since det(V) is a non-unit, it follows that

L is properly contained in L', contradicting its maximality. Conversely, if F_u is fundamental and L is not, then there is an integral lattice L' such that L is properly contained in L'. If u' is an S-basis for L', and V is the linear transformation defined by $u = u'V$, then by lemma 4.3, the coefficients of V are in S, det(V) is a non-unit of S, and $F_u = F_{u'}V$, contradicting the fundamentalness of F_u.

In the case S = R, it will be convenient to define the <u>discriminant</u> of a lattice L over R. We denote the discriminant by d(L) and define it to be the absolute value of $N'\left[\det(T(u_i\bar{u}_j))\right]$, where u is any R-basis of L and N' denotes the usual norm on K into the rational field. Thus d(L) is a positive rational number. To show that the definition is valid, suppose u and u' are any two R-bases of L. Then by lemma 4.3, $\det(T(u_i\bar{u}_j))$ and $\det(T(u'_i\bar{u}'_j))$ differ by a factor a^2, where a is a unit of R. Since $N'(a^2) = \pm 1$, it follows that d(L) is well defined.

THEOREM 5.2. <u>There exists an integral lattice over</u> S, <u>and every integral lattice over</u> R <u>is contained in a fundamental lattice over</u> R.

PROOF. To show the existence of an integral lattice over S, we can use the canonical basis u of theorem 2.1, and take a = b = -1, so that the coefficients of F_u are in S and the lattice generated by u over S is integral. Suppose $L_1, L_2, \ldots$ is a sequence of integral lattices over

R such that L_i is contained in L_{i+1} $(i = 1,2,\ldots)$. Now $d(L_i)$ is a positive rational integer, and by lemma 4.3, $d(L_1) \geq d(L_2) \geq \ldots$, so that there is an n such that $L_n = L_{n+1} = \ldots$, and the theorem follows.

It should be remarked that not every integral lattice is an order. For instance, if we take $a = b = -1$ for the canonical basis u of theorem 2.1 and define the basis u' by $u_1' = 2u_1$ and $u_i' = u_i$ for $i \neq 1$, then the lattice L' generated by u' is integral over R, but $u_2'u_3' = \frac{1}{2}u_1'$, so that L' is not an order over R.

If L is a lattice over R, then $L \otimes R_p$ is a lattice over R_p, whose R_p-bases are the same as the R-bases of L (see p. 7).

LEMMA 5.3. A lattice L over R is integral over R if and only if $L \otimes R_p$ is integral over R_p for all prime ideals p of R.

PROOF. Let u be an R-basis of L. If the coefficients of F_u are in R, then they are in R_p for all p. Conversely, if the coefficients of F_u are in R_p for all p, then, since R is the intersection of all the R_p, it follows that F_u has its coefficients in R. The lemma now follows from theorem 4.2.

LEMMA 5.4. Let L be a lattice over R. If $L \otimes R_p$ is fundamental over R_p for all prime ideals p of R, then

L is fundamental over R. If R is a principal ideal ring, then the converse also holds.

PROOF. Suppose $L \otimes R_p$ is fundamental over R_p for all p. Let u be an R-basis of L, and suppose $F_u = GV$, where G is a form with coefficients in R and V is a linear transformation with coefficients in R. The hypothesis implies that det(V) is a unit of R_p for all p. Thus $\det(V) \in R - p$ for all p. It follows that det(V) is a unit of R, and L is fundamental over R.

Suppose now that R is a principal ideal ring and that L is fundamental over R. Let u be an R-basis of L, p a prime ideal of R, and assume that $F_u = GV$, where G is a form with coefficients in R_p, V is a linear transformation with coefficients in R_p and det(V) is a non-unit of R_p. If t denotes a generator of p, then $\det(V) = et^k$, where e is a unit of R_p and $k \geq 1$. Let m be an element of R - p such that the coefficients of mV are in R. Identifying mV with its own matrix, we can write $mV = U_1 D U_2$, where U_1 and U_2 are matrices with elements in R whose determinants are units of R, and D is a diagonal matrix with elements in R [10, p. 575].

Now D can be factored as $D = D_1 D_2$, where D_1 and D_2 are diagonal and $\det(D_2) = t$. Thus $G = F_u V^{-1} = F_u(m(D_2U_2)^{-1}(U_1D_1)^{-1})$, which by hypothesis is a form with coefficients in R_p. The transformation $m^{-1}U_1D_1$ has coefficients in R_p, hence so does the form $F_u(D_2U_2)^{-1}$.

But since $\det(U_2)$ is a unit of R, p is the only prime ideal factor of $\det(D_2U_2)$, whence it follows that the coefficients of $F_u(D_2U_2)^{-1}$ are in R_q for all prime ideals q, i.e., $F_u(D_2U_2)^{-1}$ has coefficients in R. This contradicts the assumption that F_u is fundamental over R, and it follows that $L \otimes R_p$ is fundamental over R_p.

A prime ideal of R is called <u>even</u> if it is a factor of the principal ideal generated by 2, and is called <u>odd</u> otherwise.

LEMMA 5.5. <u>Let</u> p <u>be an even prime ideal of</u> R, <u>and let</u> H <u>be the set of non-zero squares in the residue class ring</u> R/p^2. <u>Then</u> H <u>is a group</u>.

PROOF. Evidently, H is closed under multiplication and contains the identity. If $a \in R$ and $b \in R$, then $a^2 \equiv b^2 \pmod{p^2}$ if and only if $a \equiv b \pmod{p}$, since p is even. Thus the number of squares in R/p^2 is the same as the number of elements of R/p. It follows that the natural homomorphism on R/p^2 to R/p induces an isomorphism of H onto the non-zero elements of a field, so that H is a group.

THEOREM 5.6. <u>If</u> R <u>is a principal ideal ring, then every fundamental lattice over</u> R <u>is an order over</u> R.

PROOF. Let L be a fundamental lattice over R, u' an R-basis of L, and write $1 = \sum e_i u_i'$. Then $e_i \in R$ $(i = 1,2,3)$ and 1 is a greatest common divisor of the e_i.

Thus there is a square matrix V with elements in R whose determinant is 1 and whose first column consists of the e_i [10, p. 568]. If we define the basis u by u = u'V, then $u_0 = 1$, and by lemma 4.3, u is an R-basis of L.

To show that L is an order, it suffices, by theorem 4.4, to show that the coefficients of f_u are in R. Recalling that det F_u is the square of an element of K, we define the quaternary form G_u by $G_u = \text{adj } F_u/(\det F_u)^{1/2}$, where the choice of sign is arbitrary.

Writing $F_u = h_u^2 + \text{adj } f_u$ in accordance with theorem 4.4, we have $F_u = HV$, where $H = x_0^2 + \text{adj } f_u$ and V is the transformation which replaces x_0 by h_u. Now adj H = $(\det f_u)^2 x_0^2 + (\det f_u) f_u$; adj F_u = (adj H)(adj V'), where V' is the transpose of V; and $(\det F_u)^{1/2} = \pm \det f_u$. Therefore, $G_u = \sum B_{0j} x_0 x_j \pm f_u$, where (B_{ij}) is the matrix of G_u. Thus, to prove the theorem, it suffices to show that the coefficients of G_u are in R.

Let p be a prime ideal of R, t a generator of p, and denote by e the exponent of the exact power of p which divides 2. Then it is known [15] that there exists a linear transformation V with coefficients in R such that det(V) is not divisible by p, and $F_u V$ is one of the following forms:

$$G_1 = a_0 x_0^2 + t^k a_1 x_1^2 + t^m a_2 x_2^2 + t^n a_3 x_3^2,$$

where the a_i are in R-p and $0 \le k \le m \le n$.

$$G_2 = t^k(t^r a_0 x_0^2 + 2a_1 x_0 x_1 + t^r b x_1^2) + t^m a_2 x_2^2 + t^n a_3 x_3^2,$$

where the a_i are in R-p, $b \in R$, $0 \leq m \neq k$, $0 \leq n \neq k$, and $1 \leq r \leq e$.

$$G_3 = t^k(t^r a_0 x_0^2 + 2a_1 x_0 x_1 + t^r b_1 x_1^2) + t^m(t^s a_2 x_2^2 + 2a_3 x_2 x_3 + t^s b_3 x_3^2),$$

where the a_i are in R-p, the b_i are in R, $1 \leq r \leq e$, and $1 \leq s \leq e$.

Note that the coefficients of the G_i are in R, and that the conditions on G_2 and G_3 imply that if p is odd, so that $e = 0$, then V can be chosen such that $F_u V = G_1$.

By lemma 5.4, F_u is fundamental over R_p. Since $\det(V)$ is a unit of R_p, and since fundamentalness is evidently preserved under unimodular transformations, it follows that $F_u V$ is fundamental over R_p.

Suppose first that $F_u V = G_1$. If $n \geq 2$, then the transformation W which replaces x_3 by $t^{-1}x_3$ has the property that the coefficients of W^{-1} are in R, $\det(W^{-1}) = t$ and the coefficients of $G_1 W$ are in R, contradicting the fact that G_1 is fundamental over R_p. Thus $n \leq 1$. Furthermore, $\det G_1 = (\det V)^2(\det F_u)$, which is a square, hence $k+m+n$ is even, which implies that either $k=m=n=0$ or $k=0$ and $m=n=1$. Therefore, we have either

$$G_u \sim a_0' x_0^2 + a_1' x_1^2 + a_2' x_2^2 + a_3' x_3^2, \text{ or}$$

$$G_u \sim t a_0' x_0^2 + t a_1' x_1^2 + a_2' x_2^2 + a_3' x_3^2,$$

where the a_i' are units of R_p and $\sim$ denotes equivalence over

R_p. Thus the coefficients of G_u are in R_p.

Suppose next that $F_uV = G_2$. Then it may be assumed that p is even. Using the fundamentalness of G_2 over R_p, we conclude as above that $0 \le m \le 1$ and $0 \le n \le 1$. Since G_2 has square determinant, $2k+m+n$ is even, hence $m=n=\sigma$, where $\sigma=0$ or 1. Now

$$\det G_2 = t^{(2\sigma+k)}a_2a_3(t^{2r}ba_0-a_1^2),$$

hence there exists $c \in R-p$ such that

$$a_2a_3(t^{2r}ba_0-a_1^2) = c^2.$$ Thus

$$-a_1^2a_2a_3 \equiv c^2 \pmod{t^2}. \tag{1}$$

By lemma 5.5, we can divide (1) by the p^2-residue of $a_1^2a_2^2$ in R/p^2 and conclude that the p^2-residue of $-a_3a_2^{-1}$ is a non-zero square. It follows that there exists $d \in R$ such that

$$d^2a_2 + a_3 \equiv 0 \pmod{t^2}. \tag{2}$$

Let W be the transformation which replaces x_2 by $x_2 + t^{-1}dx_3$ and x_3 by $t^{-1}x_3$. Then the coefficients of W^{-1} are in R, $\det(W^{-1}) = t$, and

$$G_2W = t^k(t^ra_0x_0^2 + 2a_1x_0x_1 + t^rbx_1^2) + t^\sigma a_2x_2^2 + 2t^{\sigma-1}da_2x_2x_3 + t^{\sigma-2}(d^2a_2 + a_3)x_3^2.$$

Since t divides 2, the coefficient of x_2x_3 is in R. By (2), the coefficient of x_3^2 is in R. Thus the coefficients

of G_2W are in R, contradicting the fundamentalness of G_2 over R_p. Therefore, the form G_2 cannot occur.

Finally, suppose $F_uV = G_3$. Then

$$G_u \sim t^m(t^r b_0' x_0^2 - 2a_0' x_0 x_1 + t^r a_1' x_1^2) + t^k(t^s b_2' x_2^2 - 2a_2' x_2 x_3 + t^s a_3' x_3^2),$$

where the a_i' are units of R_p, the b_i' are in R_p, and $\sim$ denotes equivalence over R_p. Suppose the coefficients of G_u are not all in R_p. Then either $m+r<0$ or $k+s<0$. But since $k+r\geq 0$ and $m+s\geq 0$, it follows that $m \neq k$, say $k<m$. Now $m+r\geq 0$ and $k+s<0$, so that $s<r$. Furthermore, since $r-s\leq e-1$, we have $1-e<0$. In particular, $e>1$, so it can be concluded at this point that if p divides 2 only to the first power, then the coefficients of G_u are in R_p, without using any fundamentalness condition. Now

$$\det G_3 = t^{2(k+m)}(t^{2r}a_0b_1 - a_1^2)(t^{2s}a_2b_3 - a_3^2),$$

hence there exists $c \in R-p$ such that

$$(t^{2r}a_0b_1 - a_1^2)(t^{2s}a_2b_3 - a_3^2) = c^2.$$

Dividing by t^{2s}, we obtain

$$t^2(t^r a_0 b_1 a_2 b_3) - t^2(t^{r-s} a_0 b_1 a_3^2) - a_2 b_3 a_1^2 = t^{-2s}((c - a_1a_3)(c + a_1a_3)) \in R.$$

Since $e\geq 2$, we have $c - a_1a_3 \equiv c + a_1a_3 \pmod{t^2}$, and thus

(3) $$-a_2b_3a_1^2 \equiv (t^{-s}(c + a_1a_3))^2 \pmod{t^2}.$$

By lemma 5.5, we can divide (3) by the p^2-residue of $a_1^2a_2^2$ in R/p^2 and conclude that the p^2-residue of $-b_3a_2^{-1}$ is a non-zero square. It follows that there exists $d \in R$ such that

(4) $$d^2a_2 + b_3 \equiv 0 \pmod{t^2}.$$

Let W be the transformation which replaces x_2 by $x_2+t^{-1}dx_3$ and x_3 by $t^{-1}x_3$. Then the coefficients of W^{-1} are in R, $\det(W^{-1}) = t$, and

$$G_3W = t^k(t^ra_0x_0^2 + 2a_1x_0x_1 + t^rb_1x_1^2) + t^m[t^sa_2x_2^2 + (2t^{s-1}da_2 + 2t^{-1}a_3)x_2x_3 + (d^2a_2t^{s-2} + 2da_3t^{-2} + b_3t^{s-2})x_3^2].$$

If $m+e-1<0$, then $m+e=0$ and $s=e$, contradicting the assumption that $s<r\leq e$. Thus $m+e-1\geq 0$. Furthermore, $m+e+s-1>0$, so that the coefficient of x_2x_3 in G_3W is in R. The coefficient of x_3^2 is $t^{m+s-2}(d^2a_2 + 2da_3t^{-s} + b_3)$. Since t^2 divides 2, d also satisfies the congruence

$$d^2a_2 + 2da_3t^{-s} + b_3 \equiv 0 \pmod{t^2}.$$

Thus, since $m+s\geq 0$, it follows that the coefficient of x_3^2 is in R. Therefore, G_3W has coefficients in R, contradicting the fundamentalness of G_3 over R_p.

It has been shown that the coefficients of G_u are

in R_p for every prime ideal p of R. It follows that the coefficients of G_u are in R. Q.E.D.

As a consequence of theorem 5.6, we have the following characterization of maximal orders over principal ideal rings.

THEOREM 5.7. *If R is a principal ideal ring, then a subset of Q is a maximal order over R if and only if it is a fundamental lattice over R.*

PROOF. Suppose J is a maximal order over R. By theorem 3.6, J is an integral lattice over R, and by theorem 5.2 there exists a fundamental lattice L over R which contains J. By theorem 5.6, L is an order, hence J = L.

Conversely, suppose L is a fundamental lattice over R. By theorem 5.6, L is an order, and by theorem 3.5, there is a maximal order J which contains L. By theorem 3.6, J is an integral lattice, hence L = J.

An analogous local statement can be made:

THEOREM 5.8. *Suppose R is a principal ideal ring, and let J be an order over R. Then $J \otimes R_p$ is a maximal order over R_p for all prime ideals p if and only if $J \otimes R_p$ is a fundamental lattice over R_p for all prime ideals p.*

PROOF. It is known that an order J is maximal over R if and only if $J \otimes R_p$ is a maximal order over R_p for all

prime ideals p [3, p. 2] . Since J is an integral lattice in the present case (theorem 3.6), the theorem follows immediately from theorem 5.7 and lemma 5.4.

APPENDIX

The terms used in this paper for which definitions are not given can be found in books which are now usually considered standard in the field of algebra. For completeness, and to alleviate any possible confusion, we list below the definitions of certain of these terms which may not be as well known as the classical algebraic terminology. The definitions given are only general enough to cover their usage in the text.

Associative algebra over a field K: A finite-dimensional vector space A over K in which there is defined an associative multiplication such that A is a ring and $a(xy) = (ax)y = x(ay) = (xa)y$ for a in K, x and y in A. As used herein the term "algebra" always means an associative algebra.

Anti-automorphism of an algebra: A one-one mapping T of the algebra A onto itself such that T is a linear transformation over K and $T(xy) = T(y)T(x)$ for x and y in A.

Involution of an algebra: A one-one mapping T of an algebra A onto itself such that $T(T(x)) = x$ for x in A.

Dedekind ring: A commutative ring with an identity, and without zero-divisors, in which every ideal is a unique product of prime ideals.

Module over a Dedekind ring S (also called an S-module): An additive abelian group M for which there is defined a multiplication ax for each a in S and x in M, such that ax is in M, $a(x+y) = ax+ay$, $(a+b)x = ax+bx$, $(ab)x = a(bx)$, and $1x = x$ for a and b in S, x and y in M.

Finitely-generated S-module: An S-module M in which there exists a finite set $x_1, x_2, \ldots x_n$ of elements such that each element of M is a linear combination of the x_i with coefficients in S.

Rank of an S-module: In case the S-module M is contained in an algebra over the quotient field of S, the rank is the maximal number of elements of M which are linearly independent over S.

Free S-module: A finitely-generated S-module which has a set of generators which are linearly independent over S.

Projective S-module: A direct summand of a free S-module.

REFERENCES

1. A.A. Albert, Structure of algebras, American Mathematical Society colloquium publications, vol. 24, 1939.

2. E. Artin, Zur Arithmetik der hypercomplexer Zahlen, Abh. aus dem Mat. Sem. der Hamb. Univ. 5 (1927), 261-288.

3. M. Auslander and O. Goldman, Maximal orders, Trans. Amer. Math. Soc. 97 (1960), 1-24.

4. H. Brandt, Idealtheorie in Quaternionalgebren, Math. Ann. 99 (1928), 1-29.

5. H. Cartan and S. Eilenberg, Homological algebra, Princeton, 1956.

6. C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Pure and applied mathematics, vol. XI, Interscience, New York, 1962.

7. M. Deuring, Algebren, Springer, Berlin, 1935.

8. L.E. Dickson, Algebras and their arithmetics, Stechert, New York, 1923.

9. _____, The rational linear algebras of maximum and minimum ranks, Proc. London Math. Soc. (2) 22

(1923), 143-162.

10. C.C. MacDuffee, Matrices with elements in a principal ideal ring, Bull. Amer. Math. Soc. 39 (1933), 564-584.

11. G. Pall, On the arithmetic of quaternions, Trans. Amer. Math. Soc. 47 (1940), 487-500.

12. _____, On generalized quaternions, Trans. Amer. Math. Soc. 59 (1946), 280-332.

13. O.F.G. Schilling, Über gewisse Beseihungen zwischen der Arithmetik hypercomplexer Zahlsysteme und algebraische Zahlkörper, Math. Ann. 111 (1935), 372-398.

14. _____, The theory of valuations, Mathematical Surveys, number 4, American Mathematical Society, 1950.

15. E.F. Stueben, The ordinal invariants of quadratic forms over algebraic number fields, Dissertation, Illinois Institute of Technology, 1963.

16. O. Zariski and P. Samuel, Commutative algebra, vol. 1, Van Nostrand, 1958.

17. _____, Commutative algebra, vol. 2, Van Nostrand, 1960.