FALK, Daniel Allen, 1940-
ORDERS IN SEPARABLE ALGEBRAS.
The Ohio State University, Ph.D., 1971
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan
ORDERS IN SEPARABLE ALGEBRAS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in the Graduate School of The Ohio State University

By

Daniel A. Falk, B.A., M.S.

* * * * * * *

The Ohio State University
1971

Approved by

Hans Lassenhaus
Advisor
Department of Mathematics
ACKNOWLEDGMENTS

I wish to express my gratitude to the following people without whom this dissertation would have been either impossible or quite unenjoyable: Dr. Martin Burrow, Dr. Bernard Fine, William T. Ramage, Tom Leyland and Arthur Mandelbaum.

I want to give special thanks to my adviser, Professor Hans Zassenhaus, who taught me to find my own way in Mathematics, and to my wife Betsy, whose patience and encouragement have been unbounded.
VITA

March 24, 1940 . . Born - Cincinnati, Ohio


1965-1966 . . . . I. B. M. Fellow, Ohio State University, Columbus, Ohio

1966. . . . . . . . M. S., Ohio State University, Columbus, Ohio

1966-1969 . . . . N. D. E. A. Fellow, Ohio State University, Columbus, Ohio

1969-1971 . . . . Teaching Assistant, Department of Mathematics, Ohio State University, Columbus, Ohio

FIELDS OF STUDY

Major Field: Algebra

Studies in Representation Theory. Professors H. Zassenhaus and H. Ledermann

Studies in Group Theory. Professor W. Kappe

Studies in Geometry. Professors J. Yaqub and R. Bumcrot
TABLE OF CONTENTS

ACKNOWLEDGMENTS ................................................................. ii
VITA ......................................................................................... iii
INTRODUCTION ......................................................................... 1

Chapter

I. THE EMBEDDING PROBLEM ........................................... 9
II. THE INTERSECTION PROBLEM ..................................... 17
III. INVERTIBILITY OF IDEALS .......................................... 24
IV. REMARKS AND QUESTIONS ......................................... 38

BIBLIOGRAPHY ........................................................................ 41
Introduction

The study of integral quantities in algebras can be thought of as an attempt to extend number-theoretic questions to a non-commutative setting. We wish to study certain problems arising in algebraic systems called orders, which are a generalization of subrings of the ring of algebraic integers in a number field. To this end, we make the following definition:

Definition 0.1. - Let $R$ be a Dedekind domain with quotient field $k$, and let $A$ be a semi-simple $k$ algebra of finite dimension over $k$. An $R$-order in $A$ is a ring $O$ contained in $A$ such that:

1. $O$ is a finitely generated, $R$-torsion free $R$-module.
2. $O$ spans $A$ over $k$, i.e. $k\otimes_R O = A$.
3. $O$ contains the identity of $A$, and, hence, under the identification of $k$ with $k \cdot 1$, $O$ contains $R \cdot 1 = R$ in its center.

Some samples of $R$-orders are:

1. If $R$ is the rational integers, then $O$, the algebraic integers of a finite algebraic extension of the rational numbers, is an Order.

2. If $R$ is a Dedekind domain, with quotient field $k$, $A$ is the
algebra of nxn matrices over \( k \), then \( O \), the ring of matrices with entries in \( R \), is an \( R \)-order in \( A \).

3. If \( R \) is \( \mathbb{Z} \), \( G \) a finite group, and \( A \) is \( \mathbb{Q}G \), the group algebra over the rationals, then \( O=\mathbb{Z}G \), the group ring, is an \( R \) order \( A \).

We will also need the following standard definitions:

**Definition 0.2.** - Let \( R \) be a Dedekind domain. An \( R \)-lattice is a finitely generated \( R \)-torsion free \( R \)-module.

**Definition 0.3.** - The \( R \)-rank of an \( R \)-lattice \( M \) is the \( k \)-dimension of the vector space \( k\mathbb{R}M \).

**Definition 0.4.** - An **Ideal** is an \( R \)-lattice in \( A \) with the same \( R \)-rank as the \( k \)-dimension of \( A \). This is sometimes called a **full** \( R \)-lattice in \( A \).

**Definition 0.5.** - If \( B \) is an Ideal in \( A \), we define \( B=\{x|x\in A, Bx=B\} \).

Since Orders, Ideals, and Lattices are torsion free, finitely generated \( R \) modules for a Dedekind domain \( R \), we will need the basic properties of these objects.

**Theorem 0.6.** - Let \( M \) and \( N \) be \( R \)-lattices in the same vector space \( V \). Then:

1. If the \( R \)-rank of \( M=\text{R-rank of } N=\text{Dim}_k V \), then there exists an ideal \( S \) of \( R \) such that \( SN\leq M \) and an ideal \( T \) of \( R \) such that \( TM\leq N \).

2. If \( M\geq N \), then there exists \( x_1, x_2, \ldots, x_n \in M \), non-zero
3.

R-ideals $I_1$, $I_2$, ..., $I_n$ and integral ideals $J_1$, ..., $J_n$ such that:

$$M = I_1x_1 \oplus I_2x_2 \oplus \cdots \oplus I_nx_n$$
$$N = J_1I_1x_1 \oplus J_2I_2x_2 \oplus \cdots \oplus J_nI_nx_n.$$

If, in addition, the R-rank of $M$ is the R-rank of $N$, then the $J_i$'s are non-zero.

3. If $M$ and $N$ have the same R-rank and if $W$ is an $R$-module such that $M \leq W \leq N$, then $W$ is finitely generated and torsion free with the same R-rank as $M$ and $N$. (See [3])

From 2, we see that there is an integral $R$ ideal $J = J_1 \cdot J_2 \cdot \ldots \cdot J_n$ such that $JM \cong 0(N)$. From this, we give the following:

**Definition 0.7.** - If $M$ and $N$ are $R$-lattices with the hypothesis of Theorem 0.6 (2), then $(M:N) = J_1J_2\cdot \ldots \cdot J_n$.

We will often use some simple results on Orders. These can be found in [5].

**Theorem 0.8.** - If $B$ is an Ideal in $A$, then $L(B) = \{x \mid x \in A$ and $xB \subseteq B\}$ and $R(B) = \{x \mid Bx \subseteq B, \ x \in A\}$ are $R$-orders in $A$, called the left order of $B$ and the right order of $B$ respectively.

**Theorem 0.9.** - If $B$ is an ideal in $A$, then $B$ is an Ideal in $A$.

The following is also useful and well-known, but no proof appears.

**Theorem 0.10.** - If $B_1$, $B_2$ are ideals in $A$, then $B_1 \cap B_2$ is an Ideal.
Proof. - By Theorem 0.6, there exists $R$-ideal such that $SB_1 \subset B_2$. However, $SB_1 \subset B_2 \Rightarrow B_1 \cap B_2 \supset B_1 \cap SB_1$. By Theorem 0.6 again, $B_1$ has the form: $I_1 x_1 \oplus I_2 x_2 \oplus \ldots \oplus I_n x_n$. Hence, $SB_1$ has the form $SI_1 x_1 \oplus SI_2 x_2 \oplus \ldots \oplus SI_n x_n$. Therefore, $B_1 \cap SB_1$ is $(I_1 \cap SI_1) x_1 \oplus (I_2 \cap SI_2) x_2 \oplus \ldots \oplus (I_n \cap SI_n) x_n$. This is an $R$-module of the same $R$-rank as $B_1$, since the intersection of non-zero $R$-ideals is non-zero, and is finitely generated since $R$-ideals are finitely generated as $R$-modules. Therefore, $B_1 \cap B_2$ is an $R$-lattice of the same $R$-rank as $B_1$ and $B_2$, i.e. an Ideal in $A$. q.e.d.

As a simple consequence we have:

Theorem 0.11. - If $O_1$, $O_2$ are $R$-orders in $A$, then $O_1 \cap O_2$ is an $R$-order in $A$.

Proof. - By the previous theorem, $O_1 \cap O_2$ is an Ideal. But $O_1 \cap O_2$ contains the identity of $A$. Hence, $O_1 \cap O_2$ is also an Order. q.e.d.

We see that an Ideal is slightly more than an ideal in usual ring theoretic sense. It corresponds to the concept of fractional ideal in number theory. In one special situation, though, they are the same.

Theorem 0.12. - Let $O$ be an $R$-order in $A$. Let $L$ be a maximal left $O$ module contained in $O$ (i.e. a maximal left ideal in the ring theoretic sense). Then $L$ is an Ideal as in Definition 0.4.
Proof. - Since $L$ is an $O$-module, $L$ is an $R$-module, and since $L \subseteq O$, the $R$-rank of $L$ is less than or equal to the $R$-rank of $O$. Hence, by the elementary divisor theorem, we can write:

$$O = I_1 x_1 \oplus I_2 x_2 \oplus \ldots \oplus I_n x_n$$

$$L = E_1 I_1 x_1 \oplus E_2 I_2 x_2 \oplus \ldots \oplus E_n I_n x_n$$ where $E_1 \supseteq E_2 \supseteq \ldots \supseteq E_n$.

If all the $E_i$'s are non-zero, then $L$ is an Ideal. This follows from Theorem 0.6 since we have that $O \supset L \supset E_n O$. Therefore, we suppose not all $E_i$'s are non-zero, and obtain a contradiction. Let $E_j$ be the last non-zero Ideal and let $S$ be an Ideal properly contained in $E_j$. Then $L+S O$ can be written:

$$(E_1 I_1 x_1 \oplus E_2 I_2 x_2 \oplus \ldots \oplus E_n I_n x_n) + (S I_1 x_1 \oplus S I_2 x_2 \oplus \ldots \oplus S I_n x_n)$$

$$= E_1 I_1 x_1 \oplus E_2 I_2 x_2 \oplus \ldots \oplus E_j I_j x_j \oplus S I_{j+1} x_n \oplus \ldots \oplus S I_n x_n$$

This is a ring theoretic left $O$ ideal, and since $L$ is maximal this must be equal to $O$.

But then: $SI_j = I_j$. Hence, $S=R$. But $S$ is properly contained in $E_j$ which is integral. This is a contradiction. q.e.d.

The same proof gives the theorem:

**Theorem 0.13.** - If $M$ is a maximal two-sided $O$-module in $O$, then $M$ is an Ideal.

From the above demonstration, it is easy to see that each maximal left Ideal and each maximal two-sided Ideal contains $PO$ for some prime $P$ of $R$.

**Definition 0.14.** - An Ideal $M$ is called a left (right, two-sided)
O-ideal if O is contained in L(M) (R(M), L(M) ∩ R(M)). It is an integral O Ideal if M ⊂ O.

It is often useful to use the ring $R_P$ of P-integral elements instead of the ring $R$. It enables us to consider one prime at a time and to have a $R_P$-basis for lattices. The following definitions and results are standard.

**Definition 0.15.** - Let $R$-Dedekind domain with prime Ideal $P$.

$R_P = \{a/b | a \in R, b \in R-P\}$.

**Theorem 0.16.** - Let $R$-Dedekind domain with prime Ideal $P$.

Then:
1. $R_P$ is a P.I.D. with unique maximal ideal.
2. $R_P$ is a Dedekind domain.

**Definition 0.16.** - Let $M$-$R$-lattice. $M_P = R_P \cap M$. This is clearly an $R_P$ lattice with $R_P$-rank = $R$-rank of $M$.

**Definition 0.17.** - An $R$-order in $A$ is a maximal Order if it is properly contained in no larger $R$-order.

**Theorem 0.18.** - If $A$ is a separable $k$-algebra, then every $R$-order is contained in a maximal $R$-order. (See [7])

**Theorem 0.19.** - $O$ is a maximal $R$-order in $A$ if $O_P$ is a maximal $R_P$-order for all primes $P$. [1]

**Theorem 0.20.** - Let $O$ be an $R$-order in the separable $k$-algebra $A$. Then $O_P$ is a maximal $R_P$-order for all but a finite number of primes $P$.

**Proof.** - Let $O'$ be a maximal $R$-order containing $O$. Since $O'$
is an R-module of the same R-rank as O, (O':O) is a non-zero R ideal. Hence (O':O)O'\subset O\subset O' and is not equal to zero. Hence \( R_P(O':O)\subset R_PO. \)

But: \( R_P(O ':O)\subset R_P(0:0)R_PO' = R_P(O ':O)O'P. \) But: \( R_P(O ':O) = R_P \)

for all primes \( P \) which do not divided \( (O':O) \). Hence, for all but this finite number of primes, \( O_P \supset O_P' \) which is maximal. Hence \( O_P \) is maximal.

We will also use the following results in maximal orders:

**Theorem 0.21.** - Let \( O_1 \) be a maximal \( R_P \)-order in the central-simple \( k \)-algebra \( A \). Then \( O_P \) has a unique maximal two-sided Ideal which is the radical of \( O_P \), and all two-sided \( O_P \)-ideals are powers of the radical. [7]

**Theorem 0.22.** - Let \( O \) be a maximal \( R \)-order in the separable \( k \)-algebra \( A \). Then for any \( O \)-ideal \( B \), \( \overline{B} = L(B) \) and \( \overline{BB} = R(B). \) [5]

The first question we consider in this paper is that of the embedding of an Order in a maximal Order. In Chapter one, we show that if \( O_1 \) and \( O_2 \) are Orders such that \( O_1 \supset O_2 \) and \( O_1 \) is minimal with this property, then \( O_1 \subset L(B), \) where \( B \) is a maximal two-sided \( O_2 \)-ideal. This generalizes a result of Zassenhaus [10].

In Chapter two, we discuss the intersection of the maximal Orders which contain a given Order. It can be shown that if \( A \) is a central simple \( k \)-algebra, \( O', \ldots, O^n \) the maximal \( R_P \)-orders containing \( O_P \), the \( \bigcap_{i=1}^n O_i \) is an Order with the same irreducible
representations as \( O \). For this reason, this intersection of Orders is of interest.

In Chapter three, we discuss the invertability of Ideals and a generalization of this concept, weak invertability. We prove a generalization of the Zassenhaus-Taussky-Dade theorem \([4]\), that is, that some power of every Ideal is weakly invertable.

We now fix our basic notation.

\( R = \) Dedekind domain

\( k = \) quotient field of \( R \)

\( A = \) separable \( k \)-algebra of finite dimension over \( k \)

\( O = \) \( R \)-order in \( A \)

\( R_P = \{ a/b \mid a \in R, \ b \in R-P \ \text{for} \ P= \text{prime Ideal of} \ R \} \)

\( O_P = R_P \cap R^O \)

\( D = \) division ring containing \( k \) in its center such that \( \text{Dim}_k D < \infty \)

\( \Omega = \) maximal \( R \)-order in \( D \)

\( D^{n \times n} = \) ring of \( n \times n \) matrices with entries in \( D \)

\[
\begin{pmatrix}
A_{11} & A_{12} & \cdots & A_{1n} \\
A_{n1} & A_{n2} & \cdots & A_{nn}
\end{pmatrix}
\]

is lattice in \( k^{n \times n} \) generated by the elements \( A_{ij} \cdot e_{ij} \) for \( A_{ij} \) an Ideal of \( R \).
CHAPTER I

The Embedding Problem

Given an R-order O in a simple, separable k algebra A, the problem arises of defining a maximal Order O_{\text{max}} containing O intrinsically, i.e. in terms of the arithmetic of O. In [10] and [11], Zassenhaus gives methods for this determination of O_{\text{max}}. In [10], he shows that if R=Z, the rational integers, then there is a prime P in Z such that P \mid (O_{\text{max}};O) and a maximal two-sided Ideal B of O for which B \supseteq PO and \text{L}(B) \supseteq O. In [11], he shows that if R is a rank one valuation ring, and J the Jacobson radical of O, then \text{L}(J)=O if and only if O is hereditary. This second method of computing a larger Order containing a given Order O is computationally easier, since it is defined in terms of only one Ideal of O. But it has two drawbacks. The first is that it is not applicable to hereditary Orders. The second is that it does not give all Orders lying above O. The first method, although it requires a survey of all maximal two-sided Ideals of O containing a fixed prime P, has neither of these drawbacks, which is shown in Theorem 1.

We need first the following definition:
Definition. - Let $O', O$ be two $R$-orders in the $k$-algebra $A$. The left conductor from $O$ to $O'$, written $C(O, O')$, is $\{x \mid x \in A$ and $O'x \subseteq O \}$. Clearly $C(O, O')$ is a left $O'$ and right $O$ ideal, and if $O' \supseteq O$, then $C(O, O')$ is the largest integral two-sided $O$ ideal such that $O' \subseteq L(C(O, O'))$. (See [8]).

Lemma. - Let $O', O$ be $R$-orders such that $O' \supseteq O$, and suppose that $O'$ is minimal with this property. Then there is a prime ideal $P$ in $R$ such that $PO' \subseteq O$.

Proof. - $O'/O$ can be considered as an $R$ module in the obvious way. Since $O'$ and $O$ have the same $R$ rank, the quotient module has a non-zero annihilating $R$ ideal $N$. Let $P$ be a prime ideal of $R$ containing $N$. Let $O^* = \{x \mid x \in O'$ and $P^n x \subseteq O$ for some $n\}$. Clearly $O^*$ is an Order containing $O$ and, since the quotient module $O'/O$ is nontrivial, $O^* \supseteq O$. By the minimality of $O'$, $O' = O^*$, for some $P$ dividing $N$. Now, let $O'' = O + PO'$. $O''$ is an Order containing $O$ and contained in $O'$, hence equal to one or the other.

If $O'' = O$, we are done. If not, then $O'' = O'$, that is, $O' = O + PO'$. Hence, $O' = O + P(O + PO')$, or $O' = O + PO + P^2 O' = O + P^2 O'$. Continuing, we get $O' = O + P^n O'$ for all $n$. But, since $O'/O \cong \bigoplus_{i=1}^m R/P^{n_i}$ and since each element is annihilated by some power of $P$, this is a contradiction. q.e.d.

Theorem 1. - Let $O', O$ by $R$-orders in $A$ such that $O'$ contains $O$ and is minimal with this property. Let $C = C(O, O')$ be the
left conductor from $O$ to $O'$. Then $C$ is a maximal two-sided $O$ Ideal.

**Proof.** - From the preceding lemma, we see that $PO' \subset O$ for some prime ideal $P$ of $R$. Hence, by the definition of the left conductor, $C \supset PO'$. Further, since $O' \supset O$, $PO' \supset PO$, let $\{B_i\}$ be the set of maximal two-sided $O$ Ideals which contain $C$. We first show there are finitely many of these. $O/C$ can be considered as an $R/P$ algebra, and it is of finite dimension since $R$ is finitely generated and $C$ is an Ideal. Let $\mathcal{J}$ be the radical of this algebra. We claim that $\mathcal{J}$ is contained in every maximal two-sided Ideal. For, if not, $\mathcal{J} + \mathcal{M} = O/C = 0$ for $\mathcal{M}$ maximal two-sided. But, since $O$ has an identity, so does $\overline{O}$. However, $\mathcal{I} = \mathcal{a} + \mathcal{m}$, $\mathcal{a} \in \mathcal{J}$, $\mathcal{m} \in \mathcal{M}$. $\mathcal{J}$ is nilpotent of finite index $n$, hence $\mathcal{I} = (\mathcal{I})^n = (\mathcal{a} + \mathcal{m})^n = \mathcal{a}^n + \mathcal{m}^n = \mathcal{m}'$ for $\mathcal{m}' \in \mathcal{M}$. Therefore, $\mathcal{I} \subseteq \mathcal{M}$, hence, $\mathcal{M} = \mathcal{O}$. Contradiction. Since every maximal two-sided ideal of $O/C$ contains $\mathcal{J}$, and since $O/J$ is semi-simple and finite dimensional, there are only finitely many maximal two-sided $O$ Ideals. But these correspond in a 1-1 fashion with their pre-images, the maximal two-sided $O$ Ideals which contain $C$. Hence, there are only finitely many $B_i$'s as claimed.

Writing $B_i$ for $B_i/C$, we know that $\overline{B_1} \cdot \overline{B_2} \cdots \cdot \overline{B_m} \in 0(\mathcal{J})$ for some $m$, or that $B_1 \cdot B_2 \cdots \cdot B_m \subset \mathcal{J}$. Since $\mathcal{J}$ is nilpotent, $(\mathcal{J})^n \in 0(C)$; then we also have that $(B_1 \cdot B_2 \cdots \cdot B_m)^n \subset C$. We will now show that $C = B_i$ for some $i$.

Let $B_{a_1} B_{a_2} \cdots \cdot B_{a_t}$ be the shortest product of the $B_i$'s such
that $B_{a_1} B_{a_2} \ldots B_{a_t} \subseteq C$. If $t=1$, we are done; so suppose that $t \neq 1$.

Let $B=B_{a_1} B_{a_2} \ldots B_{a_{t-1}}$. By definition $B \subseteq C$. Now consider the Ideal $O'B$. If $O'B$ is in $O$, then $O'B \subseteq C$, since $O'B$ is a two-sided $O$ Ideal containing $O'$ in its left order. But, $B \subseteq O'B \subseteq C$ is a contradiction, hence $O'B \not\subseteq O$. (We note here that $O'B \subseteq O'$.) Now $O'B \cdot B_{a_t} = O'B \cdot B_{a_1} \cdot B_{a_2} \ldots \cdot B_{a_t} \subseteq O' \cdot C = C \subseteq B_{a_t}$. Hence $O'B$ is contained in $L(B_{a_t})$. Now $L(B_{a_t}) \cap O'$ is an Order which contains $O$ and is contained in a minimal super Order $O'$. But this intersection contains $O'B$ which is not in $O$. Hence, $L(B_{a_t}) \cap O' = O'$. But since $C$ is maximal with the property that $L(C) \supset O'$ we have that $C = B_{a_t}$. q.e.d.

The obvious extensions of this theorem are not true in general. The maximal Ideals of an Order give no reliable way of counting the minimal super Orders containing $O$. This is shown in the following examples.

Example 1.1. - It is not the case that $L(B) \supset O$ for every maximal two-sided $O$ Ideal. Let $R=Z$, $k=Q$, $A=E^2$ where $E$ is an extension of $Q$ with the property that the dimension of $E$ over $Q=4$, and a prime $P$ of $Z$ remains prime in $L$, the integers of $E$. $L/PL$ is an extension of degree 4 of $Z/PZ$, hence, it has a quadratic subfield. Let $L_1$ be the complete pre-image of this subfield in $L$.

Let $L_2 = PL + Z$. Clearly, we have $L_2 \supset L_1 \supset L_2$. Now let
Now \( O_1 / B^2 = L / PL \) and since \( P \) is prime in \( L \), \( B \) is a maximal ideal.

Computation gives us that \( B \) is a two-sided \( O_1 \) ideal and that \( L(B) = R(B) = O_1 \). This example is due to Faddeev [8].

**Example 1.2.** - It is not the case that if \( L(B) \) properly contains \( O \), then \( R(B) \) properly contains \( O \). Let \( O_1 \) be as in the previous example. Let

\[
O_2 = \begin{pmatrix} L_1 & PL \\ L_1 & L_2 \end{pmatrix}
\]

\[
B = \begin{pmatrix} PL & PL \\ L_1 & L_2 \end{pmatrix}
\]

\( B \) is a maximal two-sided \( O_2 \) ideal and \( L(B) = O_1 \), \( O_2 = R(B) \).

**Example 1.3.** - If \( O \) is an \( R \)-order and \( B \) a maximal two-sided \( O \) ideal with \( L(B) \) \( O \), then \( L(B) \) need not be a minimal super order containing \( O \). Let \( R = \mathbb{Z} \), \( k = \mathbb{Q} \), \( A = k^{2 \times 2} \). Let \( O \) be the order generated by the elements \( \{ p e_{i,j} \}_{i=1,2; j=1,2} \), and the identity of \( A \) where \( p \) is a rational prime and \( e_{i,j} \) are the matrix units of \( A \). Let
\[ B = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{pmatrix} \]

\[ O' = \begin{pmatrix} Z & Z \\ Z & Z \end{pmatrix} \]

\[ O^* = \begin{pmatrix} Z & \mathbb{Z} \\ \mathbb{Z} & Z \end{pmatrix} \]

B is clearly a maximal two-sided \(O\) ideal since \(B\) is a maximal two-sided \(O'\) ideal and \(O' \not\subseteq O\). We also have \(O \subseteq O^* \subseteq O'\) and \(O' = L(B) = R(B)\). Hence, \(L(B)\) is not minimal.

Example 1.4. - There exist pairs of \(R_p\)-orders \(O_1, O_2\) with the following property:

\(O_2 \supsetneq O_1, O_2\) intersected with the left Order of the radical of \(O_1 = O_1\) and \(O_1\) is not hereditary. This means that examining \(L(J(O))\) will not give the entire set of Orders containing \(O\), even if \(O\) is not hereditary.

Let \(R_p\) be a localization of \(R\) at a prime \(P\) and let \(qR_p\) be unique prime Ideal of \(R_p\). Let \(\{e_{i,j} \}_{i,j=1}^{4} \in \mathbb{K}^{4 \times 4}\) be the matrix units in \(\mathbb{K}^{4 \times 4}\) with the usual multiplication:

\[ e_{i,j} e_{r,s} = \delta_{j,r} e_{i,s}. \]

Let \(O_1\) be the \(R_p\)-order with \(R_p\)-basis:
Simple computation shows that $O_1$ is an $R_p$-order with identity $x_1 + x_2$.

We claim that $J(O_1)$ is the Ideal with $R_p$-basis:

$qx_1, qx_2, x_3, x_4, \ldots, x_{16}$. This Ideal contains $qO_1$ and modulo $qO_1$ is nilpotent. Also, the quotient of $O_1$ by this Ideal is isomorphic to $R / qR$, hence, this Ideal is $J(O_1)$. Now let $O_2$ be the Order with $R_p$-basis:

First of all, it is clear that $O_2$ is $O_1$ adjoined only the elements $a(e_{10} + e_{13})$ where $a$ is a unit of $R_p$. Hence, the quotient $O_2 / O_1$ is isomorphic to $R_p / qR_p$ as an $R_p$-module and $O_2$ is therefore minimal over $O_1$. Finally, we note that $y_{10} x_3 = (e_{31} + e_{42})(e_{13} + e_{24}) = (e_{33} + e_{44}) x_2$, which is not in $J(O_1)$. Hence, $L(J(O_1)) O_2 = O_1$.

Examples 1.1, 1.2, 1.3 show that there is no exact correspondence between maximal two-sided Ideals and minimal
super Orders, while Example 1.4 shows that examining $L(J(O))$
will not give all Orders containing a given Order.
CHAPTER II

The Intersection Problem

In [2], Armand Brummer showed that if \( R \) was a complete rank one valuation ring, and \( O \) an hereditary \( R \)-order, then \( O \) could be written as the set-theoretic intersection of the maximal \( O \) orders containing \( O \). This result was expanded by several authors to the following: Among the \( O \) orders which are the intersection of the maximal \( O \) orders containing them, the hereditary \( O \) orders are distinguished by the following property: Suppose \( O_1, O_2, \ldots, O_n \) are all the maximal \( O \) orders containing \( O \). Then \( O \) is hereditary if and only if \( O = \bigcap_{i=1}^{n} O_i \) and \( O = \bigcap_{i=1}^{n} O_i \) for any \( j \) (See [9]).

Several questions arise quite naturally. Can every \( O \) order be written as the intersection of maximal \( O \) orders? If not, are there necessary and/or sufficient conditions to guarantee this? If \( O \) is not the intersection of maximal \( O \) orders, is there some way to locate an integral \( O \) ideal whose left \( O \) order is the intersection of the maximal \( O \) orders containing \( O \)?

The first question is answered in the negative by the following example.
Example 2.1. - Let $R$ be a local ring with prime ideal $P$ and $A$ be $k^{2 \times 2}$, where $k$ is the quotient field of $R$.

$$O = \begin{pmatrix}
a + Pb & c \\
Pd & a
\end{pmatrix}, \quad a, b, c, d, \text{ in } R$$

The radical of $O$ is $J(O)$. Since the quotient $O/J(O)$ is isomorphic to $R/PR$, we conclude that $J(O)$ is the unique maximal two-sided ideal of $O$. A simple calculation shows that the left order of $J(O)$ is equal to the right order of $J(O)$ and they are:

$$O = \begin{pmatrix}
R & R \\
PR & R
\end{pmatrix}$$

That $O'$ is minimal over $O$ can be seen from the fact that the quotient $O'/O$ is isomorphic to $R/PR$. Hence, by Theorem 1, $O'$ is the unique minimal super order containing $O$. We claim therefore, that every maximal order that contains $O$ also contains $O'$. For, if not, then there is a maximal order containing $O$ which does not contain $O'$. But then, in the lattice of orders between $O$ and $O'_{\text{max}}$ there must be a minimal order. But $O'$ is the unique minimal super order containing $O$, contradiction. Hence $O$ is not the intersection of maximal orders.

As to necessary and/or sufficient conditions, we have the following theorem.
Theorem 2. - Let $R$ be the localization of a Dedekind domain and let $O$ be an $R$-order in $A$, a central simple $k$-algebra. We consider $A$ as $\text{Hom}_D(V, V)$ for a division ring $D$ over $k$. Let $\dim_k D = S$ and $\dim_k V = t$ and let $n = \frac{t}{s}$. We suppose that $O$ contains $n$ mutually orthogonal idempotents, $\{e_i\}_{i=1}^n$. We further suppose that after picking a basis for $V$ composed of eigenvectors for the $e_i$'s, that the matrices representing $O$ contain a maximal Order in $D$ on the diagonal. Then $O$ is the intersection of maximal Orders.

Proof. - This theorem is most easily proven by choosing a $D$-basis for $V$, representing $A$ as the algebra of $n$ by $n$ matrices with entries in $D$ and then calculating with matrices. We choose, therefore, a basis $v_1, v_2, \ldots, v_n$ such that the $v_i$'s are eigenvectors for the $e_i$'s. Writing our operators on the left and scalars on the right, we have then that $e_i v_j = v_j \delta_{ij}$ for all $i$ and $j$. Using this basis for $V$, our idempotents have the representation as matrices of the form:

$$e_i = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{pmatrix}$$

This gives $O$ the particularly nice form:

$$O = \begin{pmatrix} P^{m_{11}} & \bar{P}^{m_{1n}} \\ \bar{P}^{m_{11}} & \bar{P}^{m_{nn}} \end{pmatrix}$$

where $\bar{P}$ is the unique maximal ideal of $\mathcal{O}$, guaranteed by Theorem 0.21. This is clear, since $e_i O e_j$ is an $\mathcal{O}$-module of $R$-rank $s$, hence
Ideal of $\mathcal{O}$. Since $O$ is a ring closed under multiplication, we have that $P_{mij}^m \cdot P_{mjk}^m \leq P_{mik}^m$ from which follows that $mij + mjk \geq mik$. We note that $mii = 0$ for all $i$.

We now consider the $n$ modules $\bigoplus_{i=1}^{n} M_i$ in $V$ of the form:

$$M_i = P_{m_{il}}^i v_1 \oplus P_{m_{i2}}^i v_2 \oplus \ldots \oplus P_{m_{in}}^i v_n.$$ 

We know from [1], that $\text{Hom}_{\mathcal{O}}(M_i, M_j) = 0$ are maximal Orders in $A$.

Retaining our original basis for $A$, a simple calculation gives that:

$$\begin{pmatrix} P^r_i, 1, 1, \ldots, P^r_i, 1, n \\ P^{r_i, n, 1, \ldots, P^{r_i, n, n}} \end{pmatrix}$$

The fact that $O_i$ contains $O$ is just the inequality $r_i, s, t \leq m_{s, t}$ or $m_{s, i} - m_{t, i} \leq m_{s, t}$. But adding $m_{t, i}$ to both sides, we have $m_{s, i} \leq m_{s, t} + m_{t, i}$, the condition for closure of $O$. To show that the $O$ is the intersection of the $O_i$'s, we must show that for some $i$,

$$r_i, s, t = m_{s, t}.$$ 

But this holds when $i=t$, for we have $r_t, s, t = m_{s, t} - m_{t, t}$, but $m_{t, t} = 0$ for all $t$. q.e.d.

To show that these conditions are not necessary is somewhat more delicate problem for the following reasons. If $O$ is the intersection of two maximal Orders, then it is a consequence of the elementary divisor theorem that $O$ contains a full set of orthogonal idempotents. Also, if $O$ is contained in exactly three maximal Orders,
it can be shown that the same holds true. Therefore, an example of
the failure of the necessity of this condition is somewhat more
complex.

Example 2.2. - Let $R$ be the localization of a Dedekind domain
for some prime ideal $P = pR$ and such that $P \nmid (2)$. Let $k$ be its
quotient field and let $A = k^{2x2}$. From Theorem 2, we know that if $O$
has the form:

$$O = \begin{pmatrix} R & R \\ P^m & R \end{pmatrix}$$

$m = \text{fixed integer}$

then $O$ is the intersection of maximal Orders. Further, we know
that every maximal Order in $A$ can be written as $\text{Hom}_R(M, M)$ for
some $R$-module $M$ in a two-dimensional $k$ space [1]. Since $R$ is a
P.I.D., $M$ has an $R$-basis and, hence, all maximal Orders in $A$ are
conjugate by some regular element in $A$. Consider a conjugate $O'$
of the maximal Order $O^{\ast}$:

$O^{\ast} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},
O' = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix},
O^{\ast\ast} = \begin{pmatrix} x^{-1} & yx^{-1} & z^{-1} \\
0 & 0 & 0 \end{pmatrix}$

$a, b, c, d, x, y, z \in R$

The elements of $O'$ are of the form:

$$e = \begin{pmatrix} a-cyx^{-1} & z^{-1}(xb+yd-ay-y^2 cx^{-1}) \\
zcx^{-1} & d-cyx^{-1} \end{pmatrix}$$

If $e$ is an idempotent, then so is its pre-image $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

A primitive idempotent in $A$ can be characterized as a matrix with
trace 1 and determinant 0. Hence, if $e$ is an idempotent, then its
pre-image has the form
\[
\begin{pmatrix}
  a & \frac{a-a^2}{c} \\
  c & 1-a
\end{pmatrix}
\] if \( c \not= 0 \) or
\[
\begin{pmatrix}
  a & b \\
  0 & 1-a
\end{pmatrix}
\] if \( c = 0 \).

If \( c = 0 \), then \( a \) satisfies \( a^2 - a = 0 \), i.e., \( a = 0 \) or \( 1 \).

We note that since the pre-image of \( e \) is in \( O^* \), then \( c \mid a - a^2 \). Now, we let \( x = z = 1 \), \( m = 10 \), and \( y = p^{-3} \). Then, \( e \) has the form:
\[
\begin{pmatrix}
  a & b + (1-2a)p^{-3} \\
  0 & 1-a
\end{pmatrix}
\] or
\[
\begin{pmatrix}
  a + p^{-3}c & \frac{a-a^2}{c} + p^{-3}(1-2a+cp^{-3}) \\
  c & 1-a-p^{-3}c
\end{pmatrix}
\]

If \( e \) has the first form, with \( c = 0 \), then since \( a = 0 \) or \( 1 \), the upper right hand corner of the matrix of \( e \) is \( b + p^{-3} \), which is not an element of \( R \) for any value of \( b \) in \( R \). Hence the intersection of \( O \) and \( O' \) has no idempotent of this form. If \( e \) is of the second form with \( c = 0 \), then for \( e \) to be in \( O' \cap O \), the lower left hand entry must be in \( p^{10} \), hence \( c \) is in \( p^{10} \). Since \( c \mid (a-a^2) \) we can write \( a-a^2 = Uc \) with \( U \) in \( R \), and rewriting the element in the first row, second column we get:
\[
U + p^{-3}(1-za) + \frac{c}{p} 6 \in R
\]
Since \( U \) is in \( R \) and \( c \) is in \( p^{10} \), we must have that \( p^{-3}(1-2a) \) is in \( R \). This is impossible if \( 1-2a \) is a unit of \( R \). So we suppose that \( 1-2a \) is a non-unit. If \( 1-2a \) is zero, then \( a = 1/2 \), which is a unit in \( R \). But this contradicts the fact that \( c \mid a-a^2 = \frac{1}{4} \) which is also a unit of \( R \).

Now, \( 1-2a \) is a unit of \( R \) unless \( 2a \) is a unit and if \( 2a \) is a unit, then
so is $a$. But, if $a$ is a unit, then since $c \mid (1-a)a$, we must have that $1-a$ is in $p^k$ for $k \geq 10$. Writing $1-a = sp^{10}$ with $s \in R$, we get that $a = 1 - sp^{10}$, hence $1 - 2a = -(1 - 2sp^{10})$ which is a unit, contradicting our assumption. Therefore, the intersection of $O$ and $O'$ is an Order which contains no idempotents of rank 1, but is the intersection of maximal Orders.
CHAPTER III

Invertibility of Ideals

The question of invertibility of ideals is a standard question of number theory and ring theory in general. If we consider the theory of Orders as "non-commutative number theory," we should expect some results analogous to the Zassenhaus-Taussky-Dade theorems for non-maximal Orders and the invertibility of Ideals for the maximal Orders. The question of invertibility of Ideals for maximal Orders was settled by Brandt, see [5]. Here we will discuss the non-maximal cases and some related questions.

Throughout this section, A will be a central-simple, k-algebra of finite dimension over k and R is the maximal Order in k, a Dedekind ring with finite residue class fields for all primes P of R. Throughout this chapter, we discuss two-sided O Ideals B. This is not a restriction on the Ideals considered, since B is a two-sided O Ideal for O=L(B) R(B). First, we recall Definition 0.5.

**Definition.** - Let C be an Ideal in A. We define $\overline{C}$ to be the set of all elements x in A such that: $CxC^c\subset C$.

**Definition.** - An Ideal in A is said to be invertible if: $C\overline{C}=L(C)$ and $\overline{C}C=R(C)$. 

24.
Definition. - If \( L(C) = R(C) = 0 \) and \( C \) is invertible, then \( C \) is said to be two-sided \( O \) invertible.

In [10], many theorems deal with two-sided \( O \) Ideals which are both maximal in \( O \) and two-sided \( O \) invertible. (Lemma 2, Theorem 1, Theorem 2, Corrolary 1, Corrolary 3, Theorem 3).

The next theorem shows that this is a very rare occurrence.

Lemma 3.1. - Let \( O \) be an \( R \)-order in \( A \). If \( M_1 \supseteq M_2 \supseteq \ldots \supseteq M_n \ldots \) is a properly decreasing sequence of two-sided \( O \) Ideals, then \( \bigcap_{i=1}^{\infty} M_i = 0 \).

Proof. - Let \( N \) be the intersection of the \( M_i \)'s, and suppose that \( N \) is not 0. We first note that without loss of generality, we can assume that the \( M_i \)'s are integral. For there exists an invertible \( R \) ideal \( S \) such that \( SM_1 \) is in \( O \), and since the \( M_i \)'s are decreasing, \( SM_i \) is in \( O \) for all \( i \). Further, if there is an element \( w \) in all \( M_i \)'s iff there is an element \( sm \) in all the \( SM \)'s since the \( M \)'s are \( R \) torsion free. Now, the \( M \)'s being integral Ideals means that \( N \) is an \( O \) Ideal if it has full \( R \)-rank. But, if \( N \) is an \( O \) Ideal, then by Theorem 0.6 there is an \( R \)-ideal \( T \) such that \( TO \) \( N \). Since \( TO \) \( N \), then \( TO \) \( M_i \) for all \( i \). But since \( O/TO \) is finite, this contradicts the fact that the \( M_i \)'s are an \( \infty \)nfinite decreasing sequence. Hence, the intersection of the \( M_i \)'s does not have the same \( R \)-rank as \( O \).

But now, consider the algebra \( k \otimes_R N \). This is a proper subalgebra of \( k \otimes_R O = A \), and is a two-sided \( k \otimes_R O = A \) ideal. But this contradicts
the simplicity of $A$. Hence, $N = 0$. q.e.d.

**Definition 3.2.** Let $O$ be an $R$-order in $A$. The $P$-radical of $O$ is the intersection of all maximal left $O$-ideals which contain $PO$.

**Theorem 3.3.** Let $O$ be an $R$-order in $A$. Let $P$ be prime ideal of $R$. Suppose $M$ is two-sided $O$ ideal such that $M \subseteq O$, and $M \supseteq P$-radical of $O$.

Then $M$ is not two-sided $O$ invertible.

**Proof.** Suppose the theorem is false. We claim first, that the powers of $M$ form a properly descending sequence of ideals. For since $M$ is integral, $M^n \supseteq M^{n+1}$. But if $M^n = M^{n+1}$, and $n$ is minimal with this property, then

$$M^n M = M^{n+1} M$$

$$M^{n-1} M = M^n M$$

$$M^{n-1} O = M^n O$$

$$M = M$$

and, hence, $n$ was not minimal. Therefore, $M^n \nsubseteq M^{n+1}$. Hence, by Lemma 3.1, $\bigcap_i M^i = 0$.

Now, let $J_P(O)$ be the $P$-radical of $O$. Since $O/PO$ is a $R/PR$ algebra with radical $J_P(O)/PO$, we see that $O/J_P(O)$ is semi-simple. Hence, $M/J_P(O)$ is two-sided ideal in a semi-simple algebra, and therefore, is idempotent. But this means that $M/J_P(O) = M + J_P(O)/J_P(O) = \ldots = M^n + J_P(O)/J_P(O)$. From the hypotheses we know that $M$ properly contains $J_P(O)$. Hence,
\[ \bigcap_i M + J_P(O)/J_P(O) \neq M/J_P(O) \text{ which is non-zero. But from the previous argument, } \bigcap M^i = 0. \text{ From this we can conclude that } \bigcap_i M^i + J_P(O)/J_P(O) = J_P(O)/J_P(O) \text{ which is zero. This is a contradiction. Therefore, } M \text{ is not two-sided } O \text{ invertible. } \text{q.e.d.} \]

Corollary 3.4. - If \( M \) is a two-sided \( O \) invertible integral \( O \) Ideal, then \( M \) is contained in the \( P \)-radical of \( O \) for some \( P \).

Proof. - Let \( L \) be a maximal left \( O \) Ideal containing \( M \). Then \( L \) contains \( P \) for some \( P \). Hence, \( L \) contains \( J_P(O) \), the \( P \)-radical of \( O \). Consider the two-sided \( O \) Ideal \( M + J_P(O) \). If \( M + J_P(O) = J_P(O) \), we are done; therefore, suppose not. Then \( M + J_P(O) \) is a proper two-sided \( O \) Ideal properly containing \( J_P(O) \).

Therefore, in the factor-space \( O/J_P(O) \), \( M + J_P(O)/J_P(O) \) is an idempotent Ideal; this means that \( M + J_P(O) = M^1 + J_P(O) = \ldots = M^n + J_P(O) \) for all \( n \). Hence again, we have that \( \bigcap \bigcap M^n + J_P(O) = M + J_P(O) \).

But since the \( M \)'s are invertible, \( \bigcap M^i = 0 \). Therefore, \( M^n + J_P(O) = J_P(O) \). A contradiction. Therefore, \( M + J_P(O) = J_P(O) \Rightarrow M \leq J_P(O) \). q.e.d.

Corollary 3.4 shows that if \( M \) is a maximal two-sided \( O \)-ideal which is two-sided \( O \) invertible, then it must be contained in the \( P \)-radical of \( O \). Hence, the Ideals mentioned in [10] must be both contained in and contain the \( P \)-radical for \( P \) dividing \( (O_{\text{max}}; O) \). Hence, they are the \( P \)-radical and the radical must be a maximal two-sided \( O \)-ideal. Since this holds locally, we can apply the
criterion in [1] to conclude that $O_P$ is an hereditary $R_P$-order for $P$ dividing the $R$-ideal above. Since $J_P(O)$ is maximal, we see that in fact $O_P$ is a maximal $R_P$-order. Hence, $P$ does not divide $(O_{\text{max}}:O)$.

We now turn to the question of invertibility in general. The following lemma will be very useful.

**Lemma 3.4.** Let $O_P$ be an $R_P$-order in $A$. Let $O'$ be a maximal order containing $O_P$ with unique maximal two-sided ideal $\Lambda$. Let $B$ be an integral two-sided $O_P$ ideal such that $B \subseteq P O_P$. Then there is an integer $n$, independent of $B$, such that $B \subseteq P^n O_P$.

**Proof.** We claim that there exists an integer $d$ such that $\Lambda^d \subseteq P O_P$. We see this from the following: $(O':P O_P)$ is an $R_P$-ideal such that $(O':P O_P)O' \subseteq P O_P$. But $(O':P O_P)O'$ is a two-sided $O'$-ideal, hence, a power of $\Lambda$, say $\Lambda^d$. Therefore, let $d$ be smallest such integer. Now let $B^* = O'B O'$, the $O'$-ideal generated by $B$. We know that $B^*$ is a power of $\Lambda$, say $B^* = \Lambda^r$, for some $r > 0$. Now $\Lambda^r \subseteq O'$.

We claim that $\Lambda^{dk}$ does not contain $\Lambda^r$ for any $k > 0$. For if it did, we would have:

$$B \subseteq O'B O' = \Lambda^r \subseteq \Lambda^{dk} \subseteq P O_P \quad \text{or}$$

$$B \subseteq P O_P \quad \text{contrary to hypothesis.}$$

We now claim that $\Lambda^{3d}$ is contained in $B$. By the above remarks, we have that $\Lambda^d \subseteq \Lambda^r$ and by construction $\Lambda^d \subseteq O_P$.

Hence:
Now, since $\Lambda$ and $\Lambda^3$ are $R_P$-modules of the same $R_P$-rank, then $(\Lambda^3, \Lambda)$ is an $R_P$-ideal, a power $(PR_P)$, such that $(PR_P)^n \subset \Lambda^3 \subset B$.

But $B$ is arbitrary. q.e.d.

As our first corollary, we have:

**Theorem 3.6.** - Let $O_P$ be an $R_P$-order in $A$. Then the group of two-sided $O_P$-invertible ideals is finitely generated.

**Proof.** - If \( \{B_i\}_{i=1}^{\infty} \) is a set of generators, then so is \( \{B_i\}_{i=0}^{\infty} \) where $B_0$ is $PO_P$. Now choose $n_i$ such that $P^{n_i}B_i$ is in $OP$ but $P^{n_i-1}$ is not. Clearly $P^{n_i}B_i$ is not in $PO$. Now, let $C_i = P^{n_i}B_i, C_0 = B_0$. The $C_i$'s clearly generate the same group that the $B_i$'s generate, since $PO_P$ is an invertible $O_P$-ideal. But by Lemma 3.5, $O_P \supset C_i \supset P^nO_P$ for some fixed integer $n$. Now since $O_P/P^nO_P$ is finite, there are only finitely many distinct $C_i$'s. q.e.d.

**Theorem 3.7.** - The semi-group of two-sided $O_P$-ideals is finitely generated.

**Proof.** - Same as above.

We now define a relation on the set of two-sided $O_P$-ideals by:

$C \# B$ iff $C = P^nB$ for some $n$

This clearly is an equivalence relation, for:

1. $B \# B$ by letting $n = 1$.

2. If $C \# B$ then $C = P^nB$ hence $B = P^{-n}C$, hence $B \# C$. 

3. If $C \# B$ and $B \# D$ then $C = P^m B$, $B = P^n D$ hence $C = P^{m+n} D$, hence $C \# D$.

Let $[C] = \left[ B \mid C \# B \right]$. We define a multiplication of classes by:

$$[C] \cdot [B] = [CB].$$

This multiplication is well-defined for if $C_1 \# C_2$, $B_1 \# B_2$, then

$$C_1 = P^{n_1} C, \quad C_2 = P^{n_2} C, \quad B_1 = P^{m_1} B, \quad B_2 = P^{m_2} B \quad \text{and}$$

$$C_1 B_1 = P^{n_1} C \cdot P^{m_1} B = P^{n_1+m_1} CB$$

$$C_2 B_2 = P^{n_2} C \cdot P^{m_2} B = P^{n_2+m_2} CB,$$

hence $[C_1 B_1] = [C_2 B_2]$. We remark here that $L(C) = L(B)$ and $R(C) = R(B)$ if $C \# B$. Now, by Lemma 3.4 we can find a representative of each class which contains $P^n O_P$ for $n$ fixed. Hence, there are only a finite number of classes. If we now consider the classes:

$[C]^k \quad k = 0, 1, \ldots$, we see that these classes form an abelian semi-group which is finite. Hence, by a well-known result [4], this set of classes contains an idempotent class. Let $[C]^k = [C]^{2k}$ be an idempotent class. Let $B = [C]^k$. Then $[B] = [B]^2$ which means that $B^2 = P^n B$. Let $B' = P^{-n} B$. Then $B'^2 = P^{-2n} B^2 = P^{-2n} P^n B = P^{-n} B = B'$.

Hence we have proven:

**Theorem 3.8.** - Every idempotent class contains an idempotent Ideal.

This can be stated somewhat differently as:

**Theorem 3.9.** - For every two-sided $O_P$-ideal $C$ there is an $m$ such that $C^m = B P^k$ where $B^2 = B$. 
The idempotent ideal in the idempotent class is clearly unique.

For if \( B^2 = B \), \( C^2 = C \) and \( B = P^n C \), then

\[
B^2 = (P^n C)^2 = P^{2n} C^2 = P^{2n} C = P^n P^n C = P^n B.
\]

hence \( n = 1 \), and \( B = C \).

For commutative orders we have the strong result of Zassenhaus-Taussky-Dade:

**Theorem 3.10.** - Let \( A \) be a number field and \( O = \mathbb{Z} \)-order in \( A \). Then some power of every \( O \)-ideal is invertible [4].

For the non-commutative case, no such result is possible as the following example shows.

**Example 3.11.** - Let \( \mathbb{R}_P \) be the localization of Dedekind domain at a prime \( P \). Let \( k \) be the quotient field of \( \mathbb{R}_P \), and let \( A = k^{3 \times 3} \).

Let \( B \) be the Ideal:

\[
B = \begin{pmatrix}
R & P^7 & P^8 \\
P^2 & R & P^6 \\
P^5 & P^4 & P^{10}
\end{pmatrix}
\]

\( L(B) \) and \( R(B) \) both have three mutually orthogonal idempotents. A lengthy calculation gives that:

\[
\tilde{B} = \begin{pmatrix}
R & P^7 & P^3 \\
P^2 & R & P^3 \\
P^{-4} & P^{-1} & P^5
\end{pmatrix}
\]
Hence, $BB \uparrow L(B)$ and $BB \uparrow R(B)$ so $B$ is neither left nor right invertible. Finally we note that $B^2 = B$. Hence no power of $B$ is invertible.

For the non-commutative orders, a much weaker statement holds. Following Faddeev [8], we make the following definition.

**Definition 3.12.** - An $O$-ideal $C$ in $A$ is **weakly** invertible if $CCC = C$.

We note that $CCC$ is always contained in $C$ and $\overline{C}$ is the largest ideal such that $CBC \subseteq C$.

**Theorem 3.13.** - Let $O_P$ be an $R_P$-order in $A$ and let $B$ be a two-sided $O_P$-ideal. Then some power of $B$ is weakly invertible.

**Proof.** - By Theorem 3.9 there is a power of $B$ such that $B^m = P^r C$ where $C$ is idempotent. Hence we need only show that $P^r C$ is weakly invertible. Clearly $C$ is weakly invertible since $CO_P C = CC = C$ and we know that $CCC \subseteq C$. But now consider:

$$P^r C \left( P^{-r} C \right) P^r C = P^r C^2 = P^r C.$$ Hence $P^r C = B$ is also weakly
invertible. q.e.d.

Theorem 3.13 has been proven only in the local case. But a simple argument gives the global proof.

**Theorem 3.14.** - Let $B$ be a two-sided $O$-ideal in $A$. Then some power of $B$ is weakly invertible.

**Proof.** - W.L.O.G. $B$ is an integral $O$-ideal, since $B$ is weakly invertible iff $SO$ is weakly invertible for all ideals $S$ of $R$.

We first claim that for all but a finite number of primes in $R$, $R_p \cap_R B = B_p$ is a maximal Order in $A$. That can be seen by considering the $R$-ideal $(O_{\text{max}}:B) = (S)$. Since $SO_{\text{max}}$ is contained in $B$ and since $S_p = R_p$ for all but a finite number of primes $P$, the assertion is true. Therefore, the power to which $B_p$ must be raised in order to be $P$ to some power times an idempotent ideal is one for all but a finite number of primes. Let $M$ be the product of all such powers. Then $(B^M_p)^P = (B^M_p)$ is $P$ to some power times an idempotent ideal, and hence, is weakly invertible. Writing $B^M_p = C$, we have $C_p \widetilde{C}_p C_p = C_p$ for all primes $P$ of $R$. But since ideals of Orders are completely determined by their localizations, see [7], we have that $C \widetilde{C}C = C$. q.e.d.

The result of Zassenhaus-Taussky-Dade is a good deal stronger than Theorem 3.14 in that it gives a bound for the power to which the Ideal must be raised in order to be invertible, and this bound is dependent only on $A$ instead of the Order $O$. If such a result
held in the non-commutative case, one would expect that it would be of the same type, namely \((A:k)\). The following example shows that this is not the case. Let \(A\) be \(k^{5 \times 5}\) and let \(B\) be the Ideal:

\[
B = \begin{pmatrix}
 p^{1032} & p^{5042} & p^{1042} & p^{873} & p^{5858} \\
 p^{7287} & p^{994} & p^{383} & p^{3347} & 6633 \\
 p^{9672} & p^{8334} & p^{2956} & p^{2730} & p^{9775} \\
 p^{4077} & p^{6490} & p^{2242} & p^{5045} & 89 \\
 p^{5127} & p^{9956} & p^{3593} & p^{1947} & p^{9348}
\end{pmatrix}
\]

Then the lowest power of \(B\) which is weakly invertible is 276.

Whether or not there is a bound independent of the order \(O\) is not known at present. We can state that there is a bound dependent on \(O\) in the following form:

**Theorem 3.15.** - Given an Order \(O\), there exists an integer \(M(O)\) such that for any two-sided \(O\)-Ideal \(B\), \(B^M\) is weakly invertible for all \(M > M(O)\).

**Proof.** - First, we show that this result holds locally. By Lemma 3.4 there are only finitely many classes of the type defined previously, for a fixed prime \(P\). For each of those there is an integer \(M_i\) such that \(B_{P_i}^{M_i}\) is an idempotent class. Let \(M_P(O)\) be the product of these \(M_i\)'s. Then \((B_P)^{MP(O)}\) is a power of \(P\) times an idempotent Ideal. We now claim that \((B_P)^M\) has this same form for \(M > M_P(O)\). For this we need the result of Faddeev [8]; if \(B\) is weakly invertible, then \(BB = T(B)\) is the smallest two-sided \(L(B)\)
Ideal such that $T(B) \cdot B = B$. This ideal is called the left inertial ideal of $B$.

It is also clear that $T(B) \cong T(B^2)$ if $L(B) = L(B^2)$ and $R(B) = R(B^2)$. But we now claim that $L(B^M_P) = L(B^M_P(\mathcal{O}))$ for $M > M_P(\mathcal{O})$. This follows from the simple fact that $L(B^M_P) = L(B^{M \cdot \mathcal{O}}_P)$ if $n \cdot M$ and the fact that $L(B^{M_P(\mathcal{O})}_P) = L(B^{2M_P(\mathcal{O})}_P) = \ldots = L(B^{kM_P(\mathcal{O})}_P)$ since $3_P$ is a central ideal times an idempotent $O$ ideal. Therefore, we have that:

$$T(B^{M_P(\mathcal{O})}_P) \cong T(B^{M_P(\mathcal{O})+1}_P) \cong \ldots \cong T(B^{2M_P(\mathcal{O})}_P) = T(B^{M_P(\mathcal{O})}_P)$$

The last equality is clear since $B^{M_P(\mathcal{O})}_P$ differs from $B^{2M_P(\mathcal{O})}_P$ by only central elements. We now write $B^{M_P(\mathcal{O})}_P$ as

$$B^{M_P(\mathcal{O})+j}_P$$

for $0 \leq j < M_P(\mathcal{O})$

And we have that:

$$B^{(t+1)M_P(\mathcal{O})}_P \cdot B^{M_P(\mathcal{O})+j}_P = B^{tM_P(\mathcal{O})+j}_P$$

Hence $B^{M_P(\mathcal{O})}_P$ is weakly invertible.

To see that this theorem is true globally, we recall that from
Theorem 0.20. Op is a maximal Order for all but a finite number of primes P. Since all Ideals of a maximal Order are invertible, we can take $M_P = 1$ for the primes where $O_P$ is maximal. Taking $M(O)$ to be the product of the $M_P(O)'s$, we see that $B_P^M$ is weakly invertible for all P when $M > M(O)$. Hence we can conclude that $B^M$ is weakly invertible. q.e.d.

In some special cases, we can make a stronger statement than Theorem 3.14.

We can prove a theorem analogous to Theorem 3.10 if our algebra $A$ is isomorphic to $k^{2 \times 2}$, the ring of 2x2 matrices over k.

This result is due to Drozd and Kirichenko [6].

**Theorem 3.16.** - Let $A = k^{2 \times 2}$, the algebra of 2 by 2 matrices over k. Let $B$=Ideal in $A$. Then some power of $B$ is invertible.

**Proof.** - We shall only sketch the proof.

We let $A_P^* = k_P^* \otimes k A$ where $k_P^*$ is the completion of k with respect to the $P$-adic valuation determined by the prime Ideal $P$.

We shall use the fact that $B$ is invertible iff $B_P^*$ is invertible [8], for all primes $P$, where $B_P^* = R_P^* \otimes_{R} B$, $R_P^*$ being the valuation ring. For $R_P$-orders we have the lifting of idempotents theorem, hence, we can show that some power of $B_P^*$ has an idempotent element. But if $(B_P^*)^t$ has an idempotent, then so does $O_P^*$. Hence, by proper choice of basis for $A_P^*$, $(B_P^*)^t$ has the form:
But a simple calculation shows that this Ideal is invertible. We also note that by an argument similar to that in Theorem 3.15, for all but a finite number of primes, $B_P^*$ is a maximal Order. Therefore, we can find an $M(B)$ such that $B_P^{M(B)}$ is invertible at all primes, hence $B$ is invertible.
CHAPTER IV

Remarks and Questions

We conclude this paper with some remarks and unsolved questions involving the problems discussed in this paper. From Example 1.1, our example seems to be slightly artificial, in that the Order does not contain a maximal Order of the center. But this hypothesis is difficult to use.

The question discussed in Chapter Two, that is, to characterize Orders which are the intersection of maximal Orders, is still open. As mentioned in the introduction, the solution to this would be quite useful in the representation theory of an Order. Zassenhaus and Benz [11] has shown that for a faithful irreducible rational representation of a metabelian group, the intersection of the maximal Orders containing the representation of the group ring over \( \mathbb{Z} \) contains a full set of orthogonal idempotents. Is this true for all finite groups?

Chapter Three generates a number of questions. Faddeev's use of the dual lattice \( \text{Hom}_R(B,R)=B^\ast \), and the relations therein generated makes a number of calculations quite simple. For if
if $A_{ij}$ = ideal of a maximal Order of the center $k$, and the algebra $A = k^{n \times n}$ then $A_{ij}^{-1} = A_{ij}$. Restricting ourselves to one prime ideal $P$, we can calculate with the exponents alone, for if $A_{ij} = P^{n_{ij}}$ and $B_{ij} = P^{m_{ij}}$, then $(A_{ij})(B_{ij}) = (C_{ij})$ where $C_{ij} = P^{\min(n_{ij} + m_{ij})}$.

This approach lends itself to integer programming and the example in Chapter Three was obtained in this fashion. Examples show that by allowing larger and larger values for the $n_{ij}$'s, the first power of an Ideal that is weakly invertible becomes larger. The same evidence exists if we restrict our examples to those Ideals for which some power is both left and right invertible, i.e. the first $n$ such that $B^n$ is left and right invertible.

But no example has been abstracted from those results to give a family of Ideals so that this first power increases without bound. Does such an example exist or is there a bound dependent on the algebra $A$ alone?

If we restrict even further and ask that we mimick the hypotheses of the Zassenhaus-Taussky-Dade Theorems, i.e. that this first power be two-sided $O$ invertible, then evidence seems to suggest that this power will be small, and that a bound exists.

We make one final remark with respect to Chapter Three. Let $A = D^{n \times n}$, for a division ring $D$ with maximal order $\mathcal{O}$ and let $O$
be an $R$-order in $A$ which contains $\mathcal{L}$. We define $C \triangleright B$ if $C = Ba$ for $a \in D$, where $B$ and $C$ are two-sided $O$-ideals. It is not hard to show, using standard localization techniques, that if $\mathcal{L}$ has a finite class number, then the number of newly defined classes is finite. This depends to a large extent on the results of Chapter Three. It may be possible that a new proof of the Jordan-Zassenhaus Theorem could be found using the characterizations of maximal $R_P$-orders and the techniques of Chapter Three.
BIBLIOGRAPHY


