DOCTORAL DISSERTATION SERIES

TITLE BLOCK IDEALS AND ARITHMETICS OF ALGEBRAS

AUTHOR WILLIAM ELLIOTT JENNER

UNIVERSITY OF MICHIGAN DATE 1951

DEGREE Ph. D. PUBLICATION NO. 3772



UNIVERSITY MICROFILMS
ANN ARBOR · MICHIGAN

BLOCK IDEALS

AND

ARITHMETICS OF ALGEBRAS

by
William Elliott Jenner

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in the
University of Michigan
1951

Committee in Charge:

Professor Richard D. Brauer, Chairman
Associate Professor Clyde H. Coombs
Professor Theophil H. Hildebrandt
Associate Professor Edwin E. Moise
Associate Professor Cecil J. Nesbitt

The author wishes to thank Professor Richard Brauer for access to certain of his unpublished results, as well as for helpful advice. Thanks also are due to Dr. Leonard Tornheim who read the manuscript and made several helpful suggestions.

TABLE OF CONTENTS

Page

Introduction. 1

Part I--Block Ideals. 3

1. Basic Concepts. 3

2. Properties of Direct Intersections. 4

3. Representation of Ideals as a Direct Intersection of Block Ideals. 9

4. Ideals $\mathfrak{m}$ Such That the Minimum Condition Holds for Left-Ideals of $\mathfrak{O}/\mathfrak{m}$. 14

Part II--Arithmetics of Algebras. 25

1. Basic Concepts and Definitions. 25

2. Elementary Properties of Orders 26

3. Ideals Generated by Ideals of $\mathfrak{o}$ 27

4. Transition to the Ring of $\mathfrak{M}$-Integers. . . 31

5. Ideals Generated by Ideals of $\mathfrak{O}$. 34

6. Prime Ideals and Arithmetics in Maximal Orders. 41

7. Arithmetics in Simple Algebras. 44

8. Extensions of $\mathfrak{G}$ 46

9. The Discriminant. 49

Conclusion. 54

References. 56

INTRODUCTION

This study is concerned in general with ideal theory in non-commutative rings and, in particular, with arithmetics of algebras. Part I is concerned with arbitrary rings having a unit element and satisfying appropriate chain conditions. It may be construed as a generalization to the non-commutative case of part of the theory in the fundamental paper of E. Noether (16). Previous work in this direction has been done by Fitting (9) and Krull (13). The paper of Fitting has proved especially suggestive and many of our remarks are contained at least implicitly therein.

In Part II these results are applied to the arithmetics of algebras. The classical theory is concerned exclusively with maximal orders (cf. Artin (2), Deuring (8), Hasse (10)). The essential feature of this study is the treatment of non-maximal orders. Fitting seems to have been one of the first to discuss such orders and has given preliminary results in (9). One of the main uses for such a theory would be to study the natural orders in group algebras which, as R. Brauer has shown in (5), are intimately related to the modular representations.

One of the more interesting questions in the theory is concerned with the relation between the arithmetic of the

algebra and that of the group field. This relation is especially evident in the discussion of simple algebras by Brandt (4), Chevalley (7) and Hasse (10). We have given a new proof of the prime ideal decomposition theorem for maximal orders which seems to throw some further light on this problem.

In view of the comparatively greater extent of the results on maximal orders, it is natural to study the relation of an arbitrary order to an imbedding maximal order. The conductor and discriminant play an important part in this connection and preliminary results relating them have been obtained.

All rings and algebras considered are assumed to be associative, although many of the more elementary results are valid in the non-associative case. In most instances, these generalizations have not been stated explicitly.

PART I--BLOCK IDEALS

1. Basic Concepts

Throughout Part I it will be assumed that Θ is a ring, associative but not necessarily commutative, which contains a unit element 1. The discussion is restricted to two-sided ideals of Θ unless explicit mention is made to the contrary.

Two-sided ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be relatively prime if $(\mathfrak{a}, \mathfrak{b}) = (1) = \Theta$.

An ideal $\mathfrak{a}$ is a direct intersection of ideals $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_r$ if

(i) $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$,

(ii) $(\mathfrak{b}_i, \mathfrak{b}_j) = (1)$ for $i \neq j$,

(iii) $\mathfrak{b}_i \neq (1)$ for $i = 1, 2, \ldots, r$.

We write $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ to indicate that $\mathfrak{a}$ is the direct intersection of the $\mathfrak{b}_i$.

An ideal is called a block ideal if it cannot be written as a direct intersection of two or more ideals.

Part I will be concerned with a systematic study of block ideal decompositions.

2. Properties of Direct Intersections

In this section we prove most of the elementary results that will be needed for the proofs of the subsequent theorems. Most of the results of this section are known.

[2.1] If $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ and if $\mathfrak{b}_i = \bigcap_{\sigma=1}^{s} \mathfrak{c}_{i\sigma}$ then $\mathfrak{a} = \bigcap_{i,\sigma} \mathfrak{c}_{i,\sigma}$.

Proof: Clearly $\mathfrak{a} = \bigcap_{i,\sigma} \mathfrak{c}_{i\sigma}$. If $i \neq j$, then $(\mathfrak{c}_{i\sigma}, \mathfrak{c}_{j\lambda}) \supseteq (\mathfrak{b}_i, \mathfrak{b}_j) = (1)$. If $\sigma \neq \lambda$, then $(\mathfrak{c}_{i\sigma}, \mathfrak{c}_{i\lambda}) = (1)$. Therefore $\mathfrak{a} = \bigcap_{i,\sigma} \mathfrak{c}_{i\sigma}$.

[2.2] If $(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{b}, \mathfrak{c}) = (1)$, then $(\mathfrak{a} \cap \mathfrak{b}, \mathfrak{c}) = (1)$.

Proof: There exist elements $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, c_1 and $c_2 \in \mathfrak{c}$ such that $a + c_1 = b + c_2 = 1$. Then $ab \equiv 1 \pmod{\mathfrak{c}}$, $ab \in \mathfrak{a} \cap \mathfrak{b}$ and so $(\mathfrak{a} \cap \mathfrak{b}, \mathfrak{c}) = (1)$.

[2.3] If $\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{b}_i$ and $\mathfrak{b} = \mathfrak{b}_1 \cap \cdots \cap \mathfrak{b}_r$, $\mathfrak{c} = \mathfrak{b}_{r+1} \cap \cdots \cap \mathfrak{b}_s$, where $1 \leq r < s$, then $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$.

Proof: This follows by induction from [2.2].

[2.4] If $(\mathfrak{a}, \mathfrak{b}) = (1)$ then $\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a}\mathfrak{b}, \mathfrak{b}\mathfrak{a})$.

Proof: $\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) \subseteq (\mathfrak{a}\mathfrak{b}, \mathfrak{b}\mathfrak{a}) \subseteq \mathfrak{a} \cap \mathfrak{b}$.

[2.5] If $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ are relatively prime in pairs, then $\bigcap_{i=1}^{n} \mathfrak{a}_i = \sum \mathfrak{a}_{\pi(1)} \cdots \mathfrak{a}_{\pi(n)}$ where π ranges over all permutations of $1, 2, \ldots, n$.

Proof: This follows by induction from [2.4]. (It will be noted that many terms in the sum may be redundant.)

The following theorem establishes a one-to-one correspondence between a decomposition of an ideal $\mathfrak{a}$ into a direct intersection of ideals and a decomposition of $\Theta/\mathfrak{a}$ into a direct sum of ideals. The result is well known but is included here for the sake of completeness. If $\mathfrak{m}$ is an ideal of Θ, let $[\alpha]_{\mathfrak{m}}$ denote the residue class of α mod $\mathfrak{m}$.

Theorem 2.1: If $\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{b}_i$, then $\Theta/\mathfrak{a} = \mathfrak{L}_1/\mathfrak{a} \dotplus \cdots \dotplus \mathfrak{L}_s/\mathfrak{a}$ where $\mathfrak{L}_i = \bigcap_{i \neq j} \mathfrak{b}_j$ and $\mathfrak{L}_i/\mathfrak{a} \cong \Theta/\mathfrak{b}_i$. Conversely, if $\Theta/\mathfrak{a} = \mathfrak{L}_1/\mathfrak{a} \dotplus \cdots \dotplus \mathfrak{L}_s/\mathfrak{a}$, then $\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{b}_i$ where $\mathfrak{b}_i = \sum_{i \neq j} \mathfrak{L}_j$. Furthermore these constructions are reciprocal.

Proof: 1. The mapping φ: $[\alpha]_{\mathfrak{a}} \longrightarrow ([\alpha]_{\mathfrak{b}_1}, \ldots, [\alpha]_{\mathfrak{b}_s})$ of $\Theta/\mathfrak{a}$ into $\Theta/\mathfrak{b}_1 \oplus \cdots \cdots \oplus \Theta/\mathfrak{b}_s$ is easily seen to be a ring-homomorphism. We wish to show it is a ring-isomorphism. Let $([\alpha_1]_{\mathfrak{b}_1}, \ldots, [\alpha_s]_{\mathfrak{b}_s})$ be any element of $\Theta/\mathfrak{b}_1 \oplus \cdots \cdots \oplus \Theta/\mathfrak{b}_s$. By [2.3], $(\mathfrak{b}_i, \mathfrak{L}_i) = (1)$ where $\mathfrak{L}_i = \bigcap_{i \neq j} \mathfrak{b}_j$, and so there exist elements $\beta_i \in \mathfrak{b}_i$ and $\gamma_i \in \mathfrak{L}_i$ such that $\alpha_i = \beta_i + \gamma_i$. Now $[\alpha_i]_{\mathfrak{b}_i} = [\gamma_i]_{\mathfrak{b}_i}$ and $[\gamma_i]_{\mathfrak{b}_j} = [0]_{\mathfrak{b}_j}$ for $i \neq j$. Let $\gamma = \gamma_1 + \cdots + \gamma_s$. Then φ maps $[\gamma]_{\mathfrak{a}}$ into $([\alpha_1]_{\mathfrak{b}_1}, \ldots, [\alpha_s]_{\mathfrak{b}_s})$ and, since φ has zero kernel, it follows that φ is an

isomorphism of $\Theta/\mathfrak{n}$ onto $\Theta/\mathfrak{b}_1 \oplus \cdots \oplus \Theta/\mathfrak{b}_s$. Now $\mathfrak{L}_i = \bigcap_{i \neq j} \mathfrak{b}_j$ is exactly the set of elements α in Θ such that the image of $[\alpha]_{\mathfrak{n}}$ under φ has all components, except possibly the i-th, equal to zero. The mapping $[\alpha]_{\mathfrak{n}} \longrightarrow [\alpha]_{\mathfrak{b}_i}$ is a ring-homomorphism of $\mathfrak{L}_i/\mathfrak{n}$ into $\Theta/\mathfrak{b}_i$. That the mapping is "onto" follows from the same property for φ, and the definition of $\mathfrak{L}_i$. The kernel is zero and so $\mathfrak{L}_i/\mathfrak{n} \cong \Theta/\mathfrak{b}_i$.

Now $\mathfrak{b}_i, \prod_{j=1}^{n} \mathfrak{j} = (1)$ for all i. Therefore $, \prod_{j=1}^{n} \mathfrak{j}$ $= \prod_{j=1}^{n} \mathfrak{j} = (1)$. If $\gamma = \gamma_1 + \cdots + \gamma_s = \gamma_1' + \cdots + \gamma_s'$ with γ_i, γ_i' $\mathfrak{i}$, then $\gamma_i - \gamma_i'$ is contained in $\mathfrak{i}$ $\prod_{i \neq j} \mathfrak{j}$ and so $\gamma_i - \gamma_i'$. It follows that / =

$\mathfrak{1}$ + ⋯ + $\mathfrak{s}$.

Now set $\mathfrak{b}_i^* = \sum_{i \neq j} \mathfrak{L}_j$. Clearly $\mathfrak{b}_i^*$ is the set of elements $x \in \Theta$ such that $[x]_{\mathfrak{n}}$ has zero projection in $\Theta/\mathfrak{b}_i$ and so $\mathfrak{b}_i = \mathfrak{b}_i^*$ for i = 1, 2,..., s.

2. Now let $\Theta/\mathfrak{n} = \mathfrak{L}_1/\mathfrak{n} \dotplus \cdots \dotplus \mathfrak{L}_s/\mathfrak{n}$ and let $\mathfrak{b}_i = \sum_{i \neq j} \mathfrak{L}_j$. Clearly $\mathfrak{n} \subseteq \bigcap_{i=1}^{s} \mathfrak{b}_i$ and $(\mathfrak{b}_i, \mathfrak{b}_j) = (1)$ for $i \neq j$. If x is any element of $\bigcap_{i=1}^{s} \mathfrak{b}_i$, then $[x]_{\mathfrak{n}}$ has

zero projection in each $\mathfrak{L}_j/\mathfrak{a}$ and so $x \in \mathfrak{a}$. Therefore $\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{b}_i$.

Now set $\mathfrak{L}_i^* = \bigcap_{i \neq j} \mathfrak{b}_j$. Then $\mathfrak{L}_i^* = \bigcap_{i \neq j} \sum_{j \neq k} \mathfrak{L}_k$ and so $\mathfrak{L}_i \subseteq \mathfrak{L}_i^*$. By the first part of the theorem, $\Theta/\mathfrak{a} = \mathfrak{L}_1^*/\mathfrak{a} \dotplus \cdots \dotplus \mathfrak{L}_s^*/\mathfrak{a} = \mathfrak{L}_1/\mathfrak{a} \dotplus \cdots \dotplus \mathfrak{L}_s/\mathfrak{a}$ and so $\mathfrak{L}_i = \mathfrak{L}_i^*$ for $i = 1, 2, \ldots, s$. This completes the proof of the theorem.

Corollary 2.1: If $\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{b}_i$ and ρ_i $(i = 1, 2, \ldots, s)$ are arbitrary elements of Θ, then the system $\xi \equiv \rho_i \pmod{\mathfrak{b}_i}$ for $i = 1, 2, \ldots, s$ has a solution in Θ and the solution is unique mod $\mathfrak{a}$.

[2.6] If $\mathfrak{a} = \bigcap_{\sigma=1}^{s} \mathfrak{b}_\sigma$, then for any ideal $\mathfrak{m}$, $(\mathfrak{a}, \mathfrak{m}) = \bigcap_{\sigma \in S} (\mathfrak{b}_\sigma, \mathfrak{m})$ where S is the set of all σ for which $(\mathfrak{b}_\sigma, \mathfrak{m}) \neq (1)$. If all $(\mathfrak{b}_\sigma, \mathfrak{m}) = (1)$ then the right-hand side is to be taken as (1).

Proof: Clearly $(\mathfrak{a}, \mathfrak{m}) \subseteq \bigcap_{\sigma \in S} (\mathfrak{b}_\sigma, \mathfrak{m})$ and the intersection on the right is direct. By [2.5], $\bigcap_{\sigma \in S} (\mathfrak{b}_\sigma, \mathfrak{m}) = \sum (\mathfrak{b}_{\sigma_1}, \mathfrak{m}) \cdots (\mathfrak{b}_{\sigma_s}, \mathfrak{m})$ where $\sigma_1, \ldots, \sigma_s$ ranges over

all permutations of $1,2,\ldots\ldots,s$. This sum is contained in $(\mathfrak{a}, \mathfrak{w})$ and so $(\mathfrak{a}, \mathfrak{w}) = \bigcap_{\sigma \in S} (\mathfrak{b}_\sigma, \mathfrak{w})$.

[2.7] <u>If</u> $\mathfrak{b}_i \subseteq \mathfrak{b}_i^*$ <u>and</u> $\bigcap_{i=1}^{r} \mathfrak{b}_i$ <u>is direct, then</u> $\bigcap_{i=1}^{r} \mathfrak{b}_i \subset \bigcap_{i=1}^{r} \mathfrak{b}_i^*$ <u>except when all</u> $\mathfrak{b}_i = \mathfrak{b}_i^*$.

Proof: If $\bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{i=1}^{r} \mathfrak{b}_i^*$, then by [2.6], $\mathfrak{b}_i = \bigcap_{\sigma \in S_i} (\mathfrak{b}_\sigma^*, \mathfrak{b}_i)$ for each $i = 1, 2, \ldots, r$ where S_i consists of the set of indices σ such that $(\mathfrak{b}_\sigma^*, \mathfrak{b}_i) \neq (1)$. Clearly $S_i = \{i\}$ and so $\mathfrak{b}_i = \mathfrak{b}_i^*$. The rest of the proof is trivial.

The next four results are known (cf. Fitting (9)). In what follows let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... denote ideals of Θ.

[2.8] $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = (1)$ <u>if and only if</u> $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{c}) = (1)$.

Proof: This follows from the proof of [2.2] and the remark that $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = (1)$ implies $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{c}) = (1)$ since $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{b} \cap \mathfrak{c}$.

[2.9] <u>If</u> $(\mathfrak{b}, \mathfrak{c}) = (1)$, $\mathfrak{a}\mathfrak{c} = \mathfrak{c}\mathfrak{a}$ <u>and</u> $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, <u>then</u> $\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{b} \cap \mathfrak{c})\mathfrak{a}$.

Proof: $(\mathfrak{b}, \mathfrak{c}) = (1)$ implies $(\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{b}\mathfrak{c}, \mathfrak{c}\mathfrak{b})$ by [2.4]. Then $\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{a}(\mathfrak{b}\mathfrak{c}, \mathfrak{c}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b}\mathfrak{c}, \mathfrak{a}\mathfrak{c}\mathfrak{b}) = (\mathfrak{b}\mathfrak{c}\mathfrak{a}, \mathfrak{c}\mathfrak{b}\mathfrak{a}) = (\mathfrak{b} \cap \mathfrak{c})\mathfrak{a}$.

[2.10] If $(\mathfrak{b}, \mathfrak{c}) = (1)$, $(\mathfrak{a}\mathfrak{c}, \mathfrak{m}) = (\mathfrak{c}\mathfrak{a}, \mathfrak{m})$ and $(\mathfrak{a}\mathfrak{b}, \mathfrak{m}) = (\mathfrak{b}\mathfrak{a}, \mathfrak{m})$, then $\{\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}), \mathfrak{m}\} = \{(\mathfrak{b} \cap \mathfrak{c})\mathfrak{a}, \mathfrak{m}\}$.

Proof: If $\mathfrak{a}'$ denotes the image of $\mathfrak{a}$ under the natural homomorphism of Θ on $\Theta/\mathfrak{m}$, then it follows from [2.9] that $\mathfrak{a}'(\mathfrak{b}' \cap \mathfrak{c}') = (\mathfrak{b}' \cap \mathfrak{c}')\mathfrak{a}'$ and this implies the statement.

[2.11] If $(\mathfrak{a}, \mathfrak{b}) = (1)$ and $(\mathfrak{a}\mathfrak{b}, \mathfrak{m}) = (\mathfrak{b}\mathfrak{a}, \mathfrak{m})$, then for any ideals $\mathfrak{A} \supseteq \mathfrak{a}$ and $\mathfrak{B} \supseteq \mathfrak{b}$, $(\mathfrak{A}\mathfrak{B}, \mathfrak{m}) = (\mathfrak{B}\mathfrak{A}, \mathfrak{m})$.

Proof: If the statement is known for $\mathfrak{m} = (0)$, then one can use an argument similar to that in the proof of [2.10] to treat the general case. Then it clearly suffices to show that if $(\mathfrak{a}, \mathfrak{b}) = (1)$, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ and $\mathfrak{a} \subseteq \mathfrak{A}$, then $\mathfrak{A}\mathfrak{b} = \mathfrak{b}\mathfrak{A}$. If $x \in \mathfrak{A}$ then there exist elements $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ such that $x = a + b$. Now $b = x - a \in \mathfrak{b} \cap \mathfrak{A}$ and so $x \in \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{A})$. Therefore $\mathfrak{A} = \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{A})$. Now $(\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} = (\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} = \mathfrak{a}(\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} + \mathfrak{b}(\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} + \mathfrak{b}\mathfrak{A} \subseteq \mathfrak{b}\mathfrak{A}$. Therefore $\mathfrak{A}\mathfrak{b} \subseteq \mathfrak{b}\mathfrak{A}$. Similarly $\mathfrak{A}\mathfrak{b} \supseteq \mathfrak{b}\mathfrak{A}$ and the statement follows.

3. Representation of Ideals as a Direct Intersection of Block Ideals

[3.1] An ideal $\mathfrak{a}$ is a block ideal if and only if $\Theta/\mathfrak{a}$ is indecomposable (in the sense of direct sum).

Proof: This follows immediately from Theorem 2.1.

It is well known that any ring with unit element which satisfies the maximum condition for two-sided ideals has a unique decomposition into a direct sum of indecomposable ideals (cf. Jacobson (11), p. 63). Furthermore, if the minimum condition holds for left (right) ideals which contain a given two-sided ideal $\mathfrak{n}$ of $\mathfrak{O}$, then the maximum condition holds for two-sided ideals containing $\mathfrak{n}$, provided $\mathfrak{O}$ contains a unit element. Then by virtue of Theorem 2.1, one can state

Theorem 3.1: Let $\mathfrak{n}$ be an ideal of $\mathfrak{O}$ such that either

(i) the maximum condition holds for ideals containing $\mathfrak{n}$ or

(ii) the minimum condition holds for left (right) ideals containing $\mathfrak{n}$. Then $\mathfrak{n}$ has a unique expression as a direct intersection of block ideals.

[3.2] If $\mathfrak{n} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ and $\mathfrak{M}$ is a block ideal containing $\mathfrak{n}$, then $\mathfrak{M}$ contains exactly one of the $\mathfrak{b}_i$.

Proof: By [2.6], $\mathfrak{M} = (\mathfrak{n}, \mathfrak{M}) = \bigcap_{i'} (\mathfrak{b}_{i'}, \mathfrak{M})$ where i' ranges over those values of i for which $(\mathfrak{b}_i, \mathfrak{M}) \neq (1)$. Since $\mathfrak{M}$ is a block ideal, there can be only one term, say $(\mathfrak{b}_\sigma, \mathfrak{M}) \neq (1)$. Then $\mathfrak{M} = (\mathfrak{b}_\sigma, \mathfrak{M})$ and hence $\mathfrak{b}_\sigma \subseteq \mathfrak{M}$ while no $\mathfrak{b}_\tau$ for $\tau \neq \sigma$ is contained in $\mathfrak{M}$.

[3.3] <u>If</u> $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{\sigma=1}^{s} \mathfrak{k}_\sigma$ <u>where the</u> $\mathfrak{k}_\sigma$ <u>are block ideals, then each</u> $\mathfrak{b}_i$ <u>is contained in at least one</u> $\mathfrak{k}_\sigma$ <u>and</u> $\mathfrak{b}_i$ <u>is the intersection of the</u> $\mathfrak{k}_\sigma$ <u>containing it</u>; $r \leq s$.

Proof: By [3.2], each $\mathfrak{k}_\sigma$ contains exactly one $\mathfrak{b}_i$. If, for some i, $(\mathfrak{b}_i, \mathfrak{k}_\sigma) = (1)$ for $\sigma = 1, 2, \ldots, s$, then by [2.2], $(\mathfrak{b}_i, \mathfrak{a}) = (1)$, a contradiction. Therefore there exists σ such that $(\mathfrak{b}_i, \mathfrak{k}_\sigma) \neq (1)$. Now each $\mathfrak{k}_\sigma$ contains some $\mathfrak{b}_j$ which clearly must be this particular $\mathfrak{b}_i$. This shows that each $\mathfrak{b}_i$ is contained in some $\mathfrak{k}_\sigma$. Suppose $\mathfrak{b}_i \subseteq \mathfrak{k}_\rho$ for $\rho = 1_i, 2_i, \ldots, \sigma_i$. Then $\mathfrak{b}_i \subseteq \bigcap_{\rho=1_i}^{\sigma_i} \mathfrak{k}_\rho$,

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i \subseteq \bigcap_i \left\{ \bigcap_{\rho=1_i}^{\sigma_i} \mathfrak{k}_\rho \right\} = \mathfrak{a}.$$

By [2.7] $\mathfrak{b}_i = \bigcap_{\rho=1_i}^{\sigma_i} \mathfrak{k}_\rho$.

3.4 <u>If</u> $\mathfrak{a}$ <u>and</u> $\mathfrak{b}$ <u>are block ideals and the maximum condition holds for ideals containing</u> $\mathfrak{a} \cap \mathfrak{b}$, <u>then either</u> $\mathfrak{a} \cap \mathfrak{b}$ <u>is direct or</u> $\mathfrak{a} \cap \mathfrak{b}$ <u>is a block ideal</u>.

Proof: If $\mathfrak{a} \cap \mathfrak{b}$ is not a block ideal, then it has a representation as a direct intersection of block ideals and by [2.3] we may assume $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{k}_1 \cap \mathfrak{k}_2$. By [3.3] $\mathfrak{k}_1 \subseteq \mathfrak{a}$ say, and $\mathfrak{k}_2 \subseteq \mathfrak{b}$. By [2.7] $\mathfrak{a} = \mathfrak{k}_1$ and $\mathfrak{b} = \mathfrak{k}_2$ and so $\mathfrak{a} \cap \mathfrak{b}$ is direct.

Theorem 3.2: If $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ where the maximum condition holds for ideals containing $\mathfrak{a}$, and where the $\mathfrak{b}_i$ are block ideals, then the representation of $\mathfrak{a}$ as a direct intersection of block ideals is obtained by replacing any two ideals $\mathfrak{b}_i$ which are not relatively prime, by their intersection and continuing in this way as long as possible.

Proof: This follows by an elementary argument from [3.4].

Theorem 3.3: If $\mathfrak{a} = \bigcap_{\sigma=1}^{s} \mathfrak{k}_\sigma$ where the maximum condition holds for ideals containing $\mathfrak{a}$, and where the $\mathfrak{k}_\sigma$ are block ideals, then the representation of $\mathfrak{a}$ as a direct intersection of block ideals can be obtained by distributing the $\mathfrak{k}_\sigma$ into minimal systems $S_1, \ldots, S_r$ such that every $\mathfrak{k}_\sigma \in S_i$ is relatively prime to every $\mathfrak{k}_\tau \in S_j$ for $i \neq j$. Then

$$\mathfrak{b}_i = \bigcap_{\mathfrak{k}_\sigma \in S_i} \mathfrak{k}_\sigma$$ is a block ideal and $$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i.$$

Proof: Suppose S_i consists of the elements $\mathfrak{k}_1, \ldots, \mathfrak{k}_m$. Then $\mathfrak{k}_1$ cannot be prime to all of $\mathfrak{k}_2, \ldots, \mathfrak{k}_m$ in view of the minimal property of S_1. Suppose $(\mathfrak{k}_1, \mathfrak{k}_2) \neq (1)$. Then by [3.4], $\mathfrak{k}_2^* = \mathfrak{k}_1 \cap \mathfrak{k}_2$ is a block ideal and, by virtue of [2.2], S_1 may be replaced by $S_1^* = \{\mathfrak{k}_2^*, \mathfrak{k}_3, \ldots, \mathfrak{k}_m\}$. It is easily seen that if S_1^* is not minimal, then neither is S_1.

Then it is clear that this process may be continued and will lead to the desired result.

Remark: It is possibly helpful to represent the situation by a graph where one represents each $\mathfrak{L}_\sigma$ by a dot and joins two dots by a line if the corresponding ideals are not relatively prime. The systems S_i are the connected components. In the proof, the replacing of $\mathfrak{r}_1$ and $\mathfrak{r}_2$ by $\mathfrak{r}_2^*$ can be interpreted as identifying the points corresponding to $\mathfrak{r}_1$ and $\mathfrak{r}_2$. It is clear that the graph of S_1 does not become disconnected by this process.

Theorem 3.4: If $\mathfrak{o} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ where the $\mathfrak{b}_i$ are block ideals, then any representation of $\mathfrak{o} = \bigcap_{\sigma=1}^{s} \mathfrak{r}_\sigma$ as a direct intersection of ideals $\mathfrak{r}_\sigma$ is obtained by distributing the $\mathfrak{b}_i$ into disjoint subsystems $T_1, \ldots, T_s$ and taking for $\mathfrak{r}_\sigma$ the intersection of the $\mathfrak{b}_i$ in T_σ.

Proof: By [2.3] such a procedure always gives an intersection of the required type. Conversely, if $\mathfrak{o} = \bigcap \mathfrak{r}_\sigma$, then by [3.3] each $\mathfrak{r}_\sigma$ is the intersection of all the $\mathfrak{b}_i$ which contain it. It is easily seen that this is a disjoint partitioning of all $\mathfrak{b}_i$.

[3.5] If $\mathfrak{a}$ is a block ideal of Θ and $\mathfrak{b} \subset \mathfrak{a}$, then $\mathfrak{a}/\mathfrak{b}$ is a block ideal of $\Theta/\mathfrak{b}$.

Proof: This follows from [3.1] and the fact that $\Theta/\mathfrak{a} \cong \Theta/\mathfrak{b} / \mathfrak{a}/\mathfrak{b}$.

3.6 If $\mathfrak{a}$ is a block ideal, then so is $\mathfrak{a}^\lambda$ where λ is a positive integer.

Proof: Suppose $\mathfrak{a}^\lambda = \mathfrak{b}_1 \cap \mathfrak{b}_2$. By [3.2] $\mathfrak{a} \supseteq \mathfrak{b}_1$, say, and so $(\mathfrak{a}, \mathfrak{b}_2) = (1)$. Then by [2.8], $(\mathfrak{a}^\lambda, \mathfrak{b}_2) = (1)$, a contradiction.

4. Ideals $\mathfrak{a}$ Such That the Minimum Condition Holds for Left-Ideals of $\Theta/\mathfrak{a}$

An ideal $\mathfrak{p}$ is called a prime ideal if $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ implies that either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$. It is to the prime ideal divisors of a given ideal $\mathfrak{a}$ and their relation to the block ideal components of $\mathfrak{a}$ that this section is mainly devoted. The significance of the assumption of the minimum condition for $\Theta/\mathfrak{a}$ lies in the fact that the Wedderburn-Artin structure theory can be applied. The results from the latter theory which will be used here can be found in (3).

[4.1] If the minimum condition holds for $\Theta/\mathfrak{a}$, then an ideal $\mathfrak{p} \supseteq \mathfrak{a}$ is a prime ideal if and only if $\mathfrak{p}$ has no proper divisors, that is, $\Theta/\mathfrak{p}$ is simple.

Proof: Suppose $\mathfrak{p}$ has no proper divisors. Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be two ideals not contained in $\mathfrak{p}$. Then

$(\mathfrak{a}_1, \mathfrak{p}) = (\mathfrak{a}_2, \mathfrak{p}) = (1)$ and so $(\mathfrak{a}_1\mathfrak{a}_2, \mathfrak{p}) = (1)$. Therefore $\mathfrak{p}$ is a prime ideal. Next, suppose $\mathfrak{p}$ is a prime ideal. Let $\mathfrak{N}/\mathfrak{p}$ be the radical of $\Theta/\mathfrak{p}$. Then there exists an integer $\lambda > 0$ such that $\mathfrak{N}^\lambda \subseteq \mathfrak{p}$ and so $\mathfrak{N} = \mathfrak{p}$. Then $\Theta/\mathfrak{p} = \Theta_1/\mathfrak{p} \dotplus \cdots \dotplus \Theta_r/\mathfrak{p}$, where $\Theta_i \supset \mathfrak{p}$ and the $\Theta_i/\mathfrak{p}$ are simple. If $r > 1$, then $\Theta_i \cdot \Theta_j \subseteq \mathfrak{p}$ for $i \neq j$. Therefore $r = 1$ and $\mathfrak{p}$ has no proper divisors.

The <u>radical</u> $\mathfrak{N}$ of $\mathfrak{a}$ is the ideal $\mathfrak{N}$ of Θ such that $\mathfrak{N}/\mathfrak{a}$ is the radical, in the Wedderburn-Artin sense, of $\Theta/\mathfrak{a}$.

<u>Theorem 4.1</u>: <u>If</u> $\mathfrak{N}$ <u>is the radical of</u> $\mathfrak{a}$, <u>and so</u> $\Theta/\mathfrak{N} = \Theta_1/\mathfrak{N} \dotplus \cdots \dotplus \Theta_k/\mathfrak{N}$ <u>with the</u> $\Theta_i/\mathfrak{N}$ <u>simple, then there are exactly</u> k <u>prime ideal divisors of</u> $\mathfrak{a}$, <u>namely</u> $\mathfrak{p}_i = \sum_{i \neq j} \Theta_j$, <u>and</u> $\mathfrak{N} = \bigcap_{i=1}^{k} \mathfrak{p}_i$.

Proof: Since the case $k = 1$ is trivial, we may assume $k > 1$. There exists an integer λ such that $\mathfrak{N}^\lambda \subseteq \mathfrak{a}$. If $\mathfrak{p}$ is a prime ideal divisor of $\mathfrak{a}$, then $\mathfrak{N}^\lambda \subseteq \mathfrak{p}$ and so $\mathfrak{N} \subseteq \mathfrak{p}$. Then, in view of [4.1], the ideals $\mathfrak{p}_i = \sum_{i \neq j} \Theta_j$ are precisely the prime ideal divisors of $\mathfrak{a}$. If $\alpha \in \bigcap_{i=1}^{k} \mathfrak{p}_i$ then $[\alpha]_{\mathfrak{N}}$ has zero projection under the projections $\Theta/\mathfrak{N} \longrightarrow \Theta_i/\mathfrak{N}$ for $i = 1, 2, \ldots, k$ and so $\alpha \in \mathfrak{N}$. It was seen above that $\mathfrak{N} \subseteq \bigcap_{i=1}^{k} \mathfrak{p}_i$ and so it follows that $\mathfrak{N} = \bigcap_{i=1}^{k} \mathfrak{p}_i$.

Remarks: It is of interest to compare this theorem with Krull's result to the effect that the radical of an ideal in a commutative ring (without chain conditions) is the intersection of all its minimal prime ideal divisors (cf. McCoy (15)). In a recent paper (14), McCoy has generalized Krull's result to non-commutative rings in such a way that our theorem 4.1 is essentially a special case.

Let $\mathfrak{a} = \bigcap_{j=1}^{r} \mathfrak{b}_j$ be the representation of $\mathfrak{a}$ as a direct intersection of block ideals. We distribute the k prime ideal divisors $\mathfrak{p}_i$ of $\mathfrak{a}$ into r blocks B_j, the block B_j consisting of the set of all $\mathfrak{p}_i$ which divide $\mathfrak{b}_j$. We now proceed to investigate the relations between the block ideal components and the prime ideal divisors of a given ideal. In particular, two criteria are established for two prime ideals to belong to the same block. Furthermore, we prove a theorem which determines the block ideals in terms of the prime ideal divisors.

If the unit element $\underline{1}$ of $\mathfrak{O}/\mathfrak{a}$ is written as a sum of primitive idempotents, $\underline{1} = \underline{\varepsilon_1} + \cdots + \underline{\varepsilon_k}$, then there exist elements $\varepsilon_1, \ldots, \varepsilon_k \in \mathfrak{O}$ with ε_i in the residue class of $\underline{\varepsilon_i}$, such that $1 = \varepsilon_1 + \cdots + \varepsilon_k$ where $\varepsilon_i^2 \equiv \varepsilon_i \pmod{\mathfrak{a}}$, $\varepsilon_i \not\equiv 0 \pmod{\mathfrak{a}}$, $\varepsilon_i \varepsilon_j \equiv 0 \pmod{\mathfrak{a}}$ for $i \neq j$, and no ε_i can be written as a sum of two other elements with these properties (cf. (3), pp. 100-101). Such elements ε_i will be called primitive idempotents mod $\mathfrak{a}$. The left-ideal $\mathfrak{O}\varepsilon_i$ is

primitive mod $\mathfrak{n}$ in the sense that if $\mathfrak{b}$ is a left-ideal such that $\mathfrak{n} \subseteq \mathfrak{b} \subset \Theta\varepsilon_i + \mathfrak{n}$, then $\mathfrak{b} \subseteq \mathfrak{N}$ and so $\mathfrak{b}$ is nilpotent mod $\mathfrak{n}$. (For a proof see (3), pp. 98-99.)

[4.2] Let $\mathfrak{r}_1, \mathfrak{r}_2, \ldots, \mathfrak{r}_n$ be a system of ideals such that

(i) $\mathfrak{r}_i \neq (1)$ for all i,

(ii) $(\mathfrak{r}_i, \mathfrak{r}_j) = (1)$ for $i \neq j$,

(iii) $\mathfrak{n} \subseteq \bigcap_{i=1}^{n} \mathfrak{r}_i \subseteq \mathfrak{N}$.

Then each ε_ρ belongs to all the $\mathfrak{r}_i$ except one; for each $\mathfrak{r}_i$ there exist ε_ρ which do not belong to it. If ζ_i is the sum of those ε_ρ not in $\mathfrak{r}_i$, then $1 = \zeta_1 + \cdots + \zeta_n$, $\zeta_i \equiv 1 \pmod{\mathfrak{r}_i}$ and $\zeta_i \equiv 0 \pmod{\mathfrak{r}_j}$ for $i \neq j$.

Proof: No $\mathfrak{r}_i$ contains all ε_ρ since $\mathfrak{r}_i \neq (1)$. Suppose some ε_ρ is in neither $\mathfrak{r}_i$ nor $\mathfrak{r}_j$ for $i \neq j$. Then, from the preceding discussion, $\mathfrak{r}_i \cap \Theta\varepsilon_\rho \subseteq \mathfrak{N}$ and $\mathfrak{r}_j \cap \Theta\varepsilon_\rho \subseteq \mathfrak{N}$. Then $\Theta\varepsilon_\rho = (\mathfrak{r}_i, \mathfrak{r}_j)\varepsilon_\rho = (\mathfrak{r}_i\varepsilon_\rho, \mathfrak{r}_j\varepsilon_\rho) \subseteq (\mathfrak{r}_i \cap \Theta\varepsilon_\rho, \mathfrak{r}_j \cap \Theta\varepsilon_\rho) \subseteq \mathfrak{N}$, a contradiction. Hence either $\varepsilon_\rho \in \mathfrak{r}_i$ or $\varepsilon_\rho \in \mathfrak{r}_j$. It follows that for $i \neq j$, ζ_i and ζ_j can have no summand ε_ρ in common. Every ε_ρ appears in some ζ_i since otherwise $\varepsilon_\rho \in \bigcap \mathfrak{r}_i \subseteq \mathfrak{N}$. The final statement of the theorem is now clear.

From this result, the following useful consequences may be drawn:

1. If $\mathfrak{n} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ where the $\mathfrak{b}_i$ are block ideals, then there exist elements $\eta_1, \eta_2, \ldots, \eta_r$ (the ζ_i for the case $\tau_i = \mathfrak{b}_i$) such that $1 = \eta_1 + \cdots + \eta_r$, $\eta_i \equiv 1 \pmod{\mathfrak{b}_i}$, $\eta_i \equiv 0 \pmod{\mathfrak{b}_j}$ for $i \neq j$. Furthermore, the η_i are orthogonal idempotents mod $\mathfrak{n}$ and they lie in the center of $\mathfrak{O}$ mod $\mathfrak{n}$ since if $x \in \mathfrak{O}$, then $x\eta_i - \eta_i x \equiv 0 \pmod{\mathfrak{b}_j}$ for all j and so $x\eta_i - \eta_i x \equiv 0 \pmod{\mathfrak{n}}$.

2. If $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ are the prime ideal divisors of $\mathfrak{n}$, then there exist elements $\delta_1, \delta_2, \ldots, \delta_k$ (the ζ_i for $\tau_i = \mathfrak{p}_i$) such that $1 = \delta_1 + \cdots + \delta_k$, $\delta_i \equiv 1 \pmod{\mathfrak{p}_i}$, $\delta_i \equiv 0 \pmod{\mathfrak{p}_j}$ for $i \neq j$ and the δ_i are orthogonal idempotents mod $\mathfrak{n}$.

We now derive some relations between the η_i and δ_i which will be used later. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be all the prime ideals in the block B_i. If $\varepsilon_\rho \in \bigcap_{j=1}^{s} \mathfrak{p}_j$, then ε_ρ is in the radical of $\mathfrak{b}_i$, so that $\varepsilon_\rho^\lambda \in \mathfrak{b}_i$ for some $\lambda > 0$. But $\varepsilon_\rho^\lambda - \varepsilon_\rho \in \mathfrak{n} \subseteq \mathfrak{b}_i$ and so $\varepsilon_\rho \in \mathfrak{b}_i$. Therefore, if ε_ρ occurs as a summand in η_i, it does likewise in the δ_j corresponding to one of $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. The converse is trivial, and we obtain

$$\eta_i = \delta_1 + \cdots + \delta_s. \qquad (1)$$

From the fact that if ϵ_ρ occurs as a summand in some δ_j, it also occurs in η_i, and since the η_i are in the center mod $\mathfrak{o}$, we obtain

$$\eta_i \delta_j \equiv \delta_j \eta_i \equiv \delta_j \pmod{\mathfrak{o}}. \qquad (2)$$

Two prime ideals $\mathfrak{P}_\rho \supseteq \mathfrak{o}$ and $\mathfrak{P}_\sigma \supseteq \mathfrak{o}$ are said to be <u>connected directly</u> if either $\delta_\rho \ominus \delta_\sigma$ or $\delta_\sigma \ominus \delta_\rho$ is not contained in $\mathfrak{o}$. They are said to be <u>connected</u> if either $\mathfrak{P}_\rho = \mathfrak{P}_\sigma$ or one can find a chain $\mathfrak{P}_\rho, \mathfrak{P}_1, \cdots, \mathfrak{P}_\tau, \mathfrak{P}_\sigma$ of prime ideals $\mathfrak{P}_i \supseteq \mathfrak{o}$ such that any two adjacent prime ideals are connected directly.

<u>Theorem 4.2: Two prime ideal divisors of $\mathfrak{o}$ belong to the same block if and only if they are connected.</u>

Proof: Suppose the prime ideals $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_s$ divide $\mathfrak{o}$ and are connected. By [3.2], each $\mathfrak{P}_j$ divides some $\mathfrak{b}_i$, so suppose $\mathfrak{b}_1 \subseteq \mathfrak{P}_1$, $\mathfrak{b}_2 \subseteq \mathfrak{P}_2$ where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are connected directly, say $\delta_1 \ominus \delta_2$ is not in $\mathfrak{o}$. By relation (2) above, $\eta_1 \delta_1 \equiv \delta_1 \eta_1 \equiv \delta_1 \pmod{\mathfrak{o}}$ and so $\eta_1 \ominus \eta_2$ is not in $\mathfrak{o}$. But $\eta_i \in \mathfrak{b}_j$ for $i \neq j$ and so $\eta_1 \ominus \eta_2$ is contained in all the block ideal components of $\mathfrak{o}$, hence in $\mathfrak{o}$ itself, a contradiction. This shows that $\mathfrak{P}_1, \cdots, \mathfrak{P}_s$ all belong to the same block.

Now suppose $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ are all the prime ideals in B_1. Let $\delta_1, \ldots, \delta_s$ be the corresponding δ_i and note that $\eta_1 = \delta_1 + \cdots + \delta_s$ by relation (1) above. Suppose these $\mathfrak{P}_i$ are not connected, say $\delta_i \Theta \delta_j + \delta_j \Theta \delta_i \subseteq \mathfrak{m}$ for $i = 1, 2, \ldots, t$; $j = t+1, \ldots, s$; $t < s$. Then $\gamma_1 \Theta \gamma_2 + \gamma_2 \Theta \gamma_1 \subseteq \mathfrak{m}$ where $\gamma_1 = \delta_1 + \cdots + \delta_t$, $\gamma_2 = \delta_{t+1} + \cdots + \delta_s$. We are going to show that $\mathfrak{q}_i = \mathfrak{b}_1 + \gamma_i \Theta \gamma_i$ for $i = 1, 2$ are ideals and that $\mathfrak{b}_1 = \mathfrak{q}_1 \cap \mathfrak{q}_2$.

If $\delta_s \in \mathfrak{q}_1$, then $\delta_s \in \mathfrak{q}_1 \delta_s = \mathfrak{b}_1 \delta_s + \gamma_1 \Theta \gamma_1 \delta_s \subseteq \mathfrak{b}_1$ since $\gamma_1 \delta_s \in \mathfrak{m} \subseteq \mathfrak{b}_1$. Therefore $\mathfrak{q}_1 \neq \Theta$. Similarly $\mathfrak{q}_2 \neq \Theta$. Set $\gamma_3 = 1 - \eta_1$ and note that γ_3 is the sum of those ε_ρ which are in $\mathfrak{b}_1$, so that $\gamma_3 \in \mathfrak{b}_1$. Now $\mathfrak{q}_1 \Theta = (\mathfrak{b}_1 + \gamma_1 \Theta \gamma_1) \Theta \cdot 1 = (\mathfrak{b}_1 + \gamma_1 \Theta \gamma_1) \Theta (\gamma_1 + \gamma_2 + \gamma_3) \subseteq \mathfrak{b}_1 + \gamma_1 \Theta \gamma_1 = \mathfrak{q}_1$ since $\gamma_1 \Theta \gamma_2 \subseteq \mathfrak{m} \subseteq \mathfrak{b}_1$ and $\gamma_3 \in \mathfrak{b}_1$. Similarly, $\Theta \mathfrak{q}_1 \subseteq \mathfrak{q}_1$ and $\Theta \mathfrak{q}_2 \Theta \subseteq \mathfrak{q}_2$. Now $1 = \gamma_1 + \gamma_2 + \gamma_3$ where $\gamma_3 \in \mathfrak{b}_1$ and so $(\mathfrak{q}_1, \mathfrak{q}_2) = (1)$. By [2.4], $\mathfrak{q}_1 \cap \mathfrak{q}_2 = (\mathfrak{q}_1 \mathfrak{q}_2, \mathfrak{q}_2 \mathfrak{q}_1) \subseteq \mathfrak{b}_1 \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2$ and so $\mathfrak{b}_1 = \mathfrak{q}_1 \cap \mathfrak{q}_2$, a contradiction. Therefore the prime ideals in B_1 are connected.

Two prime ideals $\mathfrak{P}_\rho \supseteq \mathfrak{m}$ and $\mathfrak{P}_\sigma \supseteq \mathfrak{m}$ are said to be <u>related</u> if either they are equal or can be joined

by a chain of prime ideals $\mathfrak{P}_i \supseteq \mathfrak{a}$ such that in $\mathfrak{P}_\rho$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_\tau, \mathfrak{P}_\sigma$ no two adjacent prime ideals commute mod $\mathfrak{a}$.

Theorem 4.3: Two prime ideal divisors of $\mathfrak{a}$ belong to the same block if and only if they are related.

Proof: The block ideal components of $\mathfrak{a}$ commute mod $\mathfrak{a}$ and so if $\mathfrak{P}_i$ and $\mathfrak{P}_j$ belong to two different blocks, it follows from [2.11] that they also commute mod $\mathfrak{a}$ and so prime ideals in different blocks cannot be related.

Now let $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ be the block ideal decomposition of $\mathfrak{a}$ and let its radical be $\mathfrak{N} = \bigcap_{j=1}^{s} \mathfrak{P}_j$. Let S be the set consisting of the ideals $\mathfrak{P}_i$ and decompose S into minimal disjoint subsets $S_1, \ldots, S_k$ such that the ideals in S_i commute mod $\mathfrak{a}$ with those in S_j for $i \neq j$ (cf. Fitting (9)). The $\mathfrak{P}_j$ in a given S_i all divide the same block ideal by virtue of the remark at the beginning of the proof. It follows that $k \geq r$. Let $\mathfrak{b}$ denote any fixed one of the $\mathfrak{b}_\rho$. Let $\mathfrak{M}_i$ be the intersection of all $\mathfrak{P}_j \in S_i$ such that $\mathfrak{b} \subseteq \mathfrak{P}_j$. It is possible that the $\mathfrak{M}_i$ are not defined for all $i = 1, 2, \ldots, k$. Suppose, however, that $\mathfrak{M}_1, \ldots, \mathfrak{M}_t$ are the $\mathfrak{M}_i$ which are defined; $t \leq k$. Then $\mathfrak{N} = \bigcap_{i=1}^{t} \mathfrak{M}_i$ is the radical of $\mathfrak{b}$, that is, the intersection of all its prime ideal divisors. It follows from [2.10] that the $\mathfrak{M}_i$ commute

mod $\mathfrak{o}$ and so also mod $\mathfrak{b}$. Then by [2.5], $\mathfrak{N} = \mathfrak{b} + \mathfrak{M}_1 \cdots \mathfrak{M}_t$. There exists an integer $\sigma \geq 1$ such that $\mathfrak{N}^\sigma \subseteq \mathfrak{b}$ and so $(\mathfrak{M}_1 \cdots \mathfrak{M}_t)^\sigma \subseteq \mathfrak{b}$. But the $\mathfrak{M}_i$ commute mod $\mathfrak{b}$ and so $\mathfrak{M}_1^\sigma \cdots \mathfrak{M}_t^\sigma \subseteq \mathfrak{b}$. Set $\mathfrak{L}_i = \mathfrak{M}_i^\sigma + \mathfrak{b}$. By [2.8], $(\mathfrak{M}_i^\sigma, \mathfrak{M}_j^\sigma) = (1)$ for $i \neq j$ and so $(\mathfrak{L}_i, \mathfrak{L}_j) = (1)$ for $i \neq j$. Now $\mathfrak{b} \subseteq \bigcap_{i=1}^{t} \mathfrak{L}_i$ and by [2.5] $\bigcap_{i=1}^{t} \mathfrak{L}_i \subseteq \mathfrak{M}_1^\sigma \cdots \mathfrak{M}_t^\sigma + \mathfrak{b} \subseteq \mathfrak{b}$. Therefore $\mathfrak{b} = \bigcap_{i=1}^{t} \mathfrak{L}_i$. This is impossible for $t > 1$ and so all the prime ideal divisors of $\mathfrak{b}$ belong to the same S_i and so they are related.

<u>Theorem 4.4</u>: <u>Let</u> $\mathfrak{o} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ <u>be the block ideal decomposition of</u> $\mathfrak{o}$; <u>let</u> $\mathfrak{N} = \bigcap_{j=1}^{k} \mathfrak{P}_j$ <u>be the radical of</u> $\mathfrak{o}$ <u>with exponent</u> σ, $\mathfrak{N}^\sigma \subseteq \mathfrak{o}$. <u>Let</u> $\mathfrak{M}_i$ <u>be the intersection of the prime ideals in</u> B_i. <u>Then the</u> $\mathfrak{M}_i$ <u>commute</u> mod $\mathfrak{o}$ <u>and</u> $\mathfrak{b}_i = \mathfrak{M}_i^\sigma + \mathfrak{o}$. <u>Furthermore if</u> λ <u>is any positive integer, then</u> $\mathfrak{b}_i = \mathfrak{M}_i^\sigma + \mathfrak{o} = \mathfrak{M}_i^{\sigma+\lambda} + \mathfrak{o}$.

Proof: The $\mathfrak{b}_i$ commute mod $\mathfrak{o}$ and $\mathfrak{b}_i \subseteq \mathfrak{M}_i$ for $i = 1, 2, \ldots, r$. Then by [2.11], the $\mathfrak{M}_i$ also commute mod $\mathfrak{o}$. Consequently $\mathfrak{N} = \bigcap_{i=1}^{r} \mathfrak{M}_i = \mathfrak{o} + \mathfrak{M}_1 \cdots \mathfrak{M}_r$. Now $\mathfrak{N}^\sigma = (\mathfrak{M}_1 \cdots \mathfrak{M}_r)^\sigma + \mathfrak{o}'$ where $\mathfrak{o}' \subseteq \mathfrak{o}$ and so $\mathfrak{M}_1^\sigma \cdots \mathfrak{M}_r^\sigma \subseteq \mathfrak{o}$

since the $\mathfrak{M}_i$ commute mod $\mathfrak{n}$. By [2.8], $(\mathfrak{M}_i^{\sigma}, \mathfrak{M}_j^{\sigma}) = (1)$ for $i \neq j$ and so $\mathfrak{n} = \bigcap_{i=1}^{r} (\mathfrak{M}_i^{\sigma} + \mathfrak{n}) = \bigcap_{i=1}^{r} \mathfrak{b}_i$. By [2.7] and [3.2] it follows that $\mathfrak{b}_i = \mathfrak{M}_i^{\sigma} + \mathfrak{n}$. It is clear that σ can be replaced by $\sigma + \lambda$ where λ is a positive integer.

Corollary 4.1: Let $\mathfrak{n} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ be the block ideal decomposition of $\mathfrak{n}$. Assume that all the prime ideal divisors $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ of $\mathfrak{n}$ commute mod $\mathfrak{n}$. Then each block contains only one prime ideal, $r = k$, and for suitable indexing, $\mathfrak{b}_i = \mathfrak{p}_i^{\sigma} + \mathfrak{n}$ where σ is the exponent of the radical $\mathfrak{w}$ of $\mathfrak{n}$. For each $\mathfrak{b}_i$, σ may be replaced by any larger integer.

Theorem 4.5: Let $\mathfrak{n} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ be the block ideal decomposition of $\mathfrak{n}$. Assume that all the prime ideal divisors of $\mathfrak{n}$ commute in the ordinary sense, that is, mod (0). Then the $\mathfrak{b}_i$ commute, $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{b}_i$ and $\mathfrak{b}_i = \mathfrak{p}_i^{\sigma} + \mathfrak{n}$ as in corollary 4.1.

Proof: This follows by a trivial argument from [2.11] and corollary [4.1].

We conclude Part I with some elementary applications of the preceding theory to rings $\mathfrak{O}$ with unit element and satisfying the minimum condition for all left ideals; for example, finite-dimensional algebras with unit element.

If $\mathfrak{G}$ is semisimple, then all its ideals commute. The block ideal components $\mathfrak{b}_i$ of any ideal $\mathfrak{a}$ consist of the sums of $\mathfrak{a}$ with all except one of the r emaining simple components. Block ideals are evidently prime ideals and an ideal coincides with its radical. If $\mathfrak{G}$ has a radical $\mathfrak{N}$ then any ideals, and in particular the block ideals, commute mod $\mathfrak{N}$.

PART II--ARITHMETICS OF ALGEBRAS

1. Basic Concepts and Definitions

Let A be an algebra of rank n over a field K. It is assumed that A has a unit element 1 which coincides with that of K; also that K is the quotient field of a proper Noetherian subring $\mathfrak{o}$ with $1 \in \mathfrak{o}$.

A subring $\mathfrak{O}$ of A is called an order if it is a finitely generated $\mathfrak{o}$-module, not contained in a proper subalgebra, and contains the unit element 1.

For every algebra A of the type considered, orders exist. Indeed, let $\varepsilon_1 = 1, \varepsilon_2, \ldots, \varepsilon_n$ be a K-basis for A with $\varepsilon_i \varepsilon_j = \sum_{k=1}^{n} c_{ijk} \varepsilon_k$; $c_{ijk} \in K$; $i, j \geq 2$. Determine $a \neq 0$ in $\mathfrak{o}$ such that $a \cdot c_{ijk} \in \mathfrak{o}$ for $i, j \geq 2$; $k \geq 1$. Then the $\mathfrak{o}$-module $\mathfrak{o}\{\varepsilon_1, a\varepsilon_2, \ldots, a\varepsilon_n\}$ is an order of A. In particular, A may be the group algebra of a finite group where the ε_i correspond to the group elements in the usual manner. Then one may set $a = 1$. In general, such an order is not maximal; in the case $n = 2$ with $\varepsilon_2^2 = \varepsilon_1 = 1$, it is easy to verify that the element $(\varepsilon_1 + \varepsilon_2)/2$ can be adjoined to give an order which properly contains the first.

It is well known that a finitely-generated module over a Noetherian ring satisfies the ascending chain condition for sub-modules. It follows that every integral ideal $\mathfrak{A}$ of Θ has a unique expression as a direct intersection of block ideals. Indeed, it will be shown later that the descending chain condition holds for sub-modules of Θ which contain $\mathfrak{A} \neq (0)$, provided the classical ideal theory holds for K. In this case, all the results of Part I are applicable.

2. Elementary Properties of Orders

[2.1] *There exist n elements* $\sigma_1, \ldots, \sigma_n \in \Theta$ *and a non-zero element* $c \in \mathfrak{o}$ *such that every element* $\alpha \in \Theta$ *has a unique representation* $\alpha = \frac{1}{c} \sum_{i=1}^{n} c_i \sigma_i$ *with* $c_i \in \mathfrak{o}$.

Proof: Let $\sigma_1, \ldots, \sigma_r$ be a set of $\mathfrak{o}$-generators for Θ and let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be a maximal subset linearly independent over K. Of necessity, $m = n$ and $\sigma_i = \sum_{j=1}^{n} a_{ij} \sigma_j$ for $i = 1, 2, \ldots, r$; $a_{ij} \in K$. Choose $c \neq 0$ in $\mathfrak{o}$ such that $ca_{ij} \in \mathfrak{o}$ for all i, j. The result follows immediately.

The converse is trivial:

[2.2] *If a subring* $\Theta \subseteq A$ *contains* $\mathfrak{o}$ *and a set of elements* $\sigma_1, \ldots, \sigma_n$ *such that every element* $\alpha \in \Theta$ *has a unique representation* $\alpha = \frac{1}{c} \sum_{i=1}^{n} c_i \sigma_i$ *where* $c_i \in \mathfrak{o}$ *and* c *is a fixed non-zero element of* $\mathfrak{o}$, *then* Θ *is an order*.

[2.3] If Θ is an order and ν is an element of the radical N of A, then there exists an order Θ^* containing Θ and ν.

Proof: Let $\{\sigma_1, \ldots, \sigma_r\}$ be a set of $\mathfrak{o}$-generators for Θ and suppose $N^\lambda = (0)$, $\lambda > 0$. The $\mathfrak{o}$-module Θ^* generated by the products $\sigma_{i_1}\nu^{a_1}\cdots\sigma_{i_\tau}\nu^{a_\tau}$ with $\sum_{i=1}^{\tau} a_i < \lambda$ is a ring since $N^\lambda = (0)$. It is evident that Θ^* is an order and has the required properties.

Theorem 2.1: If A possesses maximal orders, then A is semisimple.

Proof: Let Θ be a maximal order in A. By [2.3] $N \subseteq \Theta$. Let $\alpha \neq 0$ be an element of N, $\alpha = \frac{1}{c}\sum_{i=1}^{n} c_i\sigma_i$ as in [2.1]. Suppose $c_1 \neq 0$. Let b be an element of K such that bc_1 is not in $\mathfrak{o}$. Then $b\alpha$ is not in Θ, although in N, a contradiction. It follows that $N = (0)$.

For the proof of the following result see (8).

Theorem 2.2: If A is semisimple and separable, then any order can be imbedded in a maximal order.

3. Ideals Generated by Ideals of $\mathfrak{o}$

As in algebraic number theory, in order to obtain a satisfactory theory, it is necessary to generalize the notion of ideal to include the fractional ideals. Henceforth, our use of the term is to be understood in the following sense:

A subset $\mathfrak{A}$ of A is called an Θ-ideal if

(1) $\mathfrak{A}$ is an additive group such that $\mathfrak{O}\mathfrak{A}\mathfrak{O} = \mathfrak{A}$,

(2) There exists an element $\mu \neq 0$ in K such that $\mu\mathfrak{A} \subseteq \mathfrak{O}$ or, equivalently, $\mathfrak{A}$ is finitely generated.

(3) If $\mathfrak{A} \neq (0)$ then $\mathfrak{A} \cap K \neq (0)$.

If $\mathfrak{A} \subseteq \mathfrak{O}$, then $\mathfrak{A}$ is said to be <u>integral</u>; otherwise, <u>fractional</u>.

In what is to follow, a crucial role is played by the ideals generated by ideals of $\mathfrak{o}$. If $\mathfrak{a}$ is an $\mathfrak{o}$-ideal, then $\mathfrak{a}^* = \mathfrak{a}\mathfrak{O}$ is an $\mathfrak{O}$-ideal. If $\mathfrak{A}$ is an integral $\mathfrak{O}$-ideal, then $\mathfrak{A}^\# = \mathfrak{A} \cap \mathfrak{o}$ is an integral $\mathfrak{o}$-ideal. The purpose of this section is to determine to what extent the mappings $\mathfrak{a} \longrightarrow \mathfrak{a}^*$ and $\mathfrak{A} \longrightarrow \mathfrak{A}^\#$ are reciprocal.

We shall now show that $\mathfrak{a}^{*\#} = \mathfrak{a}$ for integral $\mathfrak{o}$-ideals $\mathfrak{a}$ in the case that the <u>classical</u> ideal theory holds for K; that is, every non-zero $\mathfrak{o}$-ideal may be expressed uniquely as a product of powers of prime ideals. This condition holds, for instance, if K is an algebraic number field considered either globally or locally with respect to one of its $\mathfrak{p}$-adic valuations.

<u>Theorem 3.1</u>: <u>If the classical ideal theory holds for</u> K, <u>then</u> $\mathfrak{a}^{*\#} = \mathfrak{a}$ <u>for integral</u> $\mathfrak{o}$-<u>ideals</u> $\mathfrak{a}$. <u>The mapping</u> $\mathfrak{a} \rightarrow \mathfrak{a}^*$ <u>sends the set of all</u> $\mathfrak{o}$-<u>ideals onto a set of</u> $\mathfrak{O}$-<u>ideals in a one-to-one manner. The mapping is an isomorphism with respect to product, sum and intersection. Furthermore,</u> $\mathfrak{O} \cap K = \mathfrak{o}$ <u>and</u> $\mathfrak{A} \cap K = \mathfrak{A}^\#$ <u>for every integral</u> $\mathfrak{O}$-<u>ideal</u> $\mathfrak{A}$.

Proof: Let $\mathfrak{a}$ be an integral σ-ideal. $\sigma = \mathfrak{a}\cdot\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}(\mathfrak{a}\Theta \cap \sigma) = \mathfrak{a}^{-1}\mathfrak{a}^{*\#} \subseteq \Theta \cap \mathfrak{a}^{-1}$. Now elements of $\Theta \cap \mathfrak{a}^{-1}$ are σ-integral elements of K (cf. (8)) and so $\Theta \cap \mathfrak{a}^{-1} \subseteq \sigma$ since σ is integrally closed. Therefore $\mathfrak{a}^{-1}\mathfrak{a}^{*\#} = \sigma$ and so $\mathfrak{a}^{*\#} = \mathfrak{a}$. Now consider the mapping $\mathfrak{a} \to \mathfrak{a}^*$ for $\mathfrak{a}$ integral or fractional. If $\mathfrak{a}^* = \mathfrak{b}^*$, then there exists an element $\mu \neq 0$ in K such that $\mu\mathfrak{a}$, $\mu\mathfrak{b} \subseteq \sigma$ and $(\mu\mathfrak{a})^* = (\mu\mathfrak{b})^*$, $(\mu\mathfrak{a})^{*\#} = (\mu\mathfrak{b})^{*\#}$, $\mathfrak{a} = \mathfrak{b}$. Consequently the mapping is one-to-one. It is trivial to verify that $(\mathfrak{a}\mathfrak{b})^* = \mathfrak{a}^*\mathfrak{b}^*$ and $(\mathfrak{a},\mathfrak{b})^* = (\mathfrak{a}^*, \mathfrak{b}^*)$. The proof that $(\mathfrak{a}\cap\mathfrak{b})^* = \mathfrak{a}^*\cap\mathfrak{b}^*$ is less trivial. Certainly $(\mathfrak{a}\cap\mathfrak{b})^* \subseteq \mathfrak{a}^*\cap\mathfrak{b}^*$. Now $(\mathfrak{a}\cap\mathfrak{b})^{-1} = (\mathfrak{a}^{-1}, \mathfrak{b}^{-1})$, $\mathfrak{a}^{-1}(\mathfrak{a}\Theta \cap \mathfrak{b}\Theta) \subseteq \Theta$, $\mathfrak{b}^{-1}(\mathfrak{a}\Theta\cap\mathfrak{b}\Theta) \subseteq \Theta$, $(\mathfrak{a}^{-1}, \mathfrak{b}^{-1})(\mathfrak{a}\Theta\cap\mathfrak{b}\Theta) \subseteq \Theta$ and so $\mathfrak{a}^*\cap\mathfrak{b}^* \subseteq (\mathfrak{a}\cap\mathfrak{b})^*$. Therefore $(\mathfrak{a}\cap\mathfrak{b})^* = \mathfrak{a}^*\cap\mathfrak{b}^*$. Now $\Theta \cap K$ consists of σ-integers of K and so $\Theta \cap K = \sigma$. Then if $\mathfrak{A}$ is an integral ideal of Θ, $\mathfrak{A}\cap K = \mathfrak{A}\cap\Theta\cap K = \mathfrak{A}^*$.

<u>From now on, it will be assumed that the classical ideal theory holds for K</u>.

[3.1] <u>If $\mathfrak{M}$ is a non-zero integral proper Θ-ideal, then $\mathfrak{m} = \mathfrak{M}^{\#}$ is an integral σ-ideal with $(0) \subset \mathfrak{m} \subset \sigma$.</u>

Proof: It is clear that $\mathfrak{m}$ is an integral σ-ideal with $\mathfrak{m} \subset \sigma$. There exists an element $a \neq 0$ in $\mathfrak{M}\cap K$ and by theorem 3.1, $a \in \sigma$. Therefore $(0) \subset \mathfrak{m}$.

[3.2] If $\mathfrak{M}$ is a block ideal of Θ, then $\mathfrak{w} = \mathfrak{M}^{\#}$ is a block ideal of $\mathfrak{o}$.

Proof: By [3.1], $(0) \subset \mathfrak{w} \subset \mathfrak{o}$. Suppose $\mathfrak{w} = \mathfrak{b}_1 \cap \mathfrak{b}_2$ (cf. I[2.3]). Then by theorem 3.1, $\mathfrak{w}^* = \mathfrak{b}_1^* \cap \mathfrak{b}_2^*$. But $\mathfrak{M}$ is a block ideal and so by I[3.2], $\mathfrak{b}_2^* \subseteq \mathfrak{M}$ say. Then by theorem 3.1, $\mathfrak{b}_2 \subseteq \mathfrak{w}$, a contradiction. It follows that $\mathfrak{w}$ is a block ideal.

[3.3] If $\mathfrak{M}$ and $\mathfrak{N}$ are integral Θ-ideals such that $\mathfrak{w} = \mathfrak{M}^{\#}$ and $\mathfrak{w} = \mathfrak{N}^{\#}$ are relatively prime, then $\mathfrak{M} \cap \mathfrak{N} = \mathfrak{M} \cdot \mathfrak{N} = \mathfrak{N} \cdot \mathfrak{M}$.

Proof: Since $(\mathfrak{w}, \mathfrak{w}) = \mathfrak{o}$, it follows that $(\mathfrak{M}, \mathfrak{N}) = (1)$. By I[2.4], $\mathfrak{M} \cap \mathfrak{N} = (\mathfrak{M}\mathfrak{N}, \mathfrak{N}\mathfrak{M})$. Now $\mathfrak{w}^* \mathfrak{w}^* = \mathfrak{w}^* \mathfrak{w}^*$ and so by I[2.11], $\mathfrak{M} \cap \mathfrak{N} = \mathfrak{M} \cdot \mathfrak{N} = \mathfrak{N} \cdot \mathfrak{M}$.

[3.4] If $\mathfrak{M}$ is a non-zero integral Θ-ideal, then the minimum condition holds for $\mathfrak{o}$-modules L such that $\mathfrak{M} \subseteq L \subseteq \Theta$.

Proof: Using the notation of [2.1], let $\alpha = \frac{1}{c} \sum_{i=1}^{n} c_i \sigma_i$ be an arbitrary element of Θ. Let $\mathfrak{w} = \mathfrak{M}^{\#}$. If $\alpha \in c\mathfrak{w}$, then $\alpha\Theta \subseteq \mathfrak{M}$. Therefore, for elements α of Θ taken mod $\mathfrak{M}$, the elements c_i may be changed mod $c\mathfrak{w}$. It follows that $\Theta/\mathfrak{M}$ can be regarded as an $\mathfrak{o}/c\mathfrak{w}$-module where the operators act in the natural manner. Under this definition, $\Theta/\mathfrak{M}$ is finitely-generated and so satisfies the minimum condition for sub-modules since the minimum condition holds in $\mathfrak{o}/c\mathfrak{w}$ (cf. (11), p. 32).

By virtue of [3.4], it follows that the results in section 4 of Part I are applicable to orders, provided attention is restricted to non-zero ideals.

4. Transition to the Ring of $\mathfrak{n}$ -Integers

For a fixed integral $\mathfrak{o}$ -ideal $\mathfrak{n}$ we define the ring of $\mathfrak{n}$ -integers of K to be the set of all elements of the form α/β where $\alpha, \beta \in \mathfrak{o}$ and $(\beta, \mathfrak{n}) = (1)$. It is trivial to verify that this set forms a ring under the operations of K. Of particular importance is the case where $\mathfrak{n}$ is a prime ideal $\mathfrak{p}$. The ring of $\mathfrak{p}$ -integers is precisely the ring of local integers of K in the sense of the $\mathfrak{p}$ -adic valuation. The ring of $\mathfrak{n}$ -integers will be denoted by $\tilde{\mathfrak{o}}$. We set $\tilde{\mathfrak{O}} = \tilde{\mathfrak{o}}\mathfrak{O}$ and $\tilde{\mathfrak{M}} = \tilde{\mathfrak{o}}\mathfrak{M}$ for $\mathfrak{O}$ -ideals $\mathfrak{M}$.

It may clarify matters to give some motivation for the considerations of this section. In general, orders do not possess a minimal basis. However, if $\mathfrak{o}$ is a principal ideal ring, for instance a ring of $\mathfrak{p}$ -integers, then an order does possess a minimal basis and the theory of elementary divisors is valid. In the next section we wish to use these two facts and so we now investigate the relation of an order $\mathfrak{O}$ to its extension $\tilde{\mathfrak{O}}$.

[4.1] *If $\mathfrak{M}$ is an integral $\mathfrak{O}$ -ideal such that $\mathfrak{w} = \mathfrak{M}^{\#}$ has only prime ideal factors which divide $\mathfrak{n}$, then $\tilde{\mathfrak{O}}/\tilde{\mathfrak{M}} \cong \mathfrak{O}/\mathfrak{M}$. The isomorphism is canonical, being induced by the injection map of $\mathfrak{O}$ into $\tilde{\mathfrak{O}}$.*

Proof: We contend that $\tilde{\mathfrak{O}} = \mathfrak{O} + \tilde{\mathfrak{m}}$. Certainly $\mathfrak{O} + \tilde{\mathfrak{m}} \subseteq \tilde{\mathfrak{O}}$. Let α be any element of $\tilde{\mathfrak{O}}$ and let d be an element of $\mathfrak{o}$ with $(1) = (d, \mathfrak{o}) = (d, \mathfrak{w})$ such that $d\alpha \in \mathfrak{O}$. Then $\alpha \in (d\alpha, \mathfrak{w}\alpha) \subseteq \mathfrak{O} + \tilde{\mathfrak{m}}$ and so $\tilde{\mathfrak{O}} = \mathfrak{O} + \tilde{\mathfrak{m}}$. Next we show that $\tilde{\mathfrak{m}} \cap \mathfrak{O} = \mathfrak{m}$. Certainly $\mathfrak{m} \subseteq \tilde{\mathfrak{m}} \cap \mathfrak{O}$. Now let β be an arbitrary element of $\tilde{\mathfrak{m}} \cap \mathfrak{O}$ and determine $h \in \mathfrak{o}$ such that $(1) = (h, \mathfrak{o}) = (h, \mathfrak{w})$ and $h\beta \in \mathfrak{m}$. Now $\beta \in (h\beta, \mathfrak{w}\beta) \subseteq \mathfrak{m}$ and so $\tilde{\mathfrak{m}} \cap \mathfrak{O} = \mathfrak{m}$. From these two facts one immediately deduces $\tilde{\mathfrak{O}}/\tilde{\mathfrak{m}} = (\mathfrak{O} + \tilde{\mathfrak{m}})/\tilde{\mathfrak{m}} \cong \mathfrak{O}/\tilde{\mathfrak{m}} \cap \mathfrak{O} = \mathfrak{O}/\mathfrak{m}$ where the isomorphism is canonical in the sense of being induced by the injection map of $\mathfrak{O}$ into $\tilde{\mathfrak{O}}$.

[4.2] <u>If $\mathfrak{m}$ is an integral ideal of $\mathfrak{O}$ and $\mathfrak{w} = \mathfrak{m}^{\#}$ is prime to $\mathfrak{o}$, then</u> $\tilde{\mathfrak{m}} = \tilde{\mathfrak{O}}$.

Proof: There exist elements $\mu \in \mathfrak{w}$ and $\alpha \in \mathfrak{o}$ such that $\mu + \alpha = 1$. Then $\mu(1 - \alpha)^{-1} = 1 \in \tilde{\mathfrak{w}}$ and so $\tilde{\mathfrak{m}} = \tilde{\mathfrak{O}}$.

[4.3] <u>Every integral $\tilde{\mathfrak{O}}$-ideal $\mathfrak{f}$ is of the form $\mathfrak{f} = \tilde{\mathfrak{m}}$ where $\mathfrak{m}$ is an integral $\mathfrak{O}$-ideal</u>.

Proof: Set $\mathfrak{m} = \mathfrak{f} \cap \mathfrak{O}$ and let α be an arbitrary element of $\mathfrak{f}$. Then $\alpha = \sum x_i \gamma_i$ where $x_i \in \tilde{\mathfrak{o}}$ and $\gamma_i \in \mathfrak{O}$. There exists an element $d \in \mathfrak{o}$ such that $(d, \mathfrak{o}) = (1)$ and $d\alpha = \sum dx_i \gamma_i$ with $dx_i \in \mathfrak{o}$. Then $d\alpha \in \mathfrak{m}$ and $\alpha \in d^{-1}\mathfrak{m} \subseteq \tilde{\mathfrak{m}}$. Hence $\mathfrak{f} \subseteq \tilde{\mathfrak{m}}$ and so $\mathfrak{f} = \tilde{\mathfrak{m}}$.

[4.4] The mapping $\varphi: \mathfrak{M} \to \tilde{\mathfrak{M}}$ is a homomorphism with respect to sum, product and intersection of the set of integral Θ-ideals onto the set of integral $\tilde{\Theta}$-ideals.

Proof: It is trivial to verify that φ is a homomorphism with respect to sum and product. If $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are integral Θ-ideals then $\varphi(\mathfrak{M}_1 \cap \mathfrak{M}_2) \subseteq \tilde{\mathfrak{M}}_1 \cap \tilde{\mathfrak{M}}_2$. If $\alpha \in \tilde{\mathfrak{M}}_1 \cap \tilde{\mathfrak{M}}_2$ then, as in the proof of [4.3], there exists an element $d \in \mathfrak{o}$ with $(d, \mathfrak{o}) = (1)$ such that $d\alpha \in \mathfrak{M}_1 \cap \mathfrak{M}_2$. Then $\alpha \in d^{-1}(\mathfrak{M}_1 \cap \mathfrak{M}_2) \subseteq \varphi(\mathfrak{M}_1 \cap \mathfrak{M}_2)$. Therefore $\varphi(\mathfrak{M}_1 \cap \mathfrak{M}_2) = \tilde{\mathfrak{M}}_1 \cap \tilde{\mathfrak{M}}_2$. That the mapping is "onto" follows from [4.3].

Theorem 4.1: Let $\mathfrak{N}$ range over the set of integral Θ-ideals such that $\mathfrak{N}^{\#}$ either equals $\mathfrak{o}$ or possesses only prime ideal factors which divide $\mathfrak{o}$. Then $\bar{\varphi}: \mathfrak{N} \longrightarrow \tilde{\mathfrak{N}}$ is a one-to-one mapping onto the set of all integral $\tilde{\Theta}$-ideals. Furthermore, $\bar{\varphi}$ is an isomorphism with regard to sum, product and intersection; also $\mathfrak{N} = \tilde{\mathfrak{N}} \cap \Theta$.

Proof: In view of [4.4] it suffices to show that $\bar{\varphi}$ is one-to-one and "onto." If $\mathfrak{N}_1 \to \tilde{\mathfrak{N}}$ and $\mathfrak{N}_2 \to \tilde{\mathfrak{N}}$, then $\mathfrak{N}_1 + \mathfrak{N}_2 \to \tilde{\mathfrak{N}}$. Consequently, one may assume $\mathfrak{N}_1 \subseteq \mathfrak{N}_2$. By [4.1], $\Theta/\mathfrak{N}_1 \cong \tilde{\Theta}/\tilde{\mathfrak{N}} \cong \Theta/\mathfrak{N}_2$ where the induced isomorphism of $\Theta/\mathfrak{N}_1$ and $\Theta/\mathfrak{N}_2$ is canonical. It follows that $\mathfrak{N}_1 = \mathfrak{N}_2$. This shows $\bar{\varphi}$ is one-to-one. Now let $\mathfrak{q}$ be any

integral $\tilde{\Theta}$ -ideal. By [4.3], $\mathfrak{J} = \tilde{\mathfrak{M}}$ where $\mathfrak{M}$ is an integral Θ -ideal. If $\mathfrak{M}^{\#}$ has only prime ideal factors which divide $\mathfrak{a}$, then it is in the domain of definition of $\bar{\varphi}$. If $\mathfrak{M}^{\#}$ has only prime ideal factors which are relatively prime to $\mathfrak{a}$, then $\tilde{\mathfrak{M}} = \tilde{\Theta}$ and $\mathfrak{M}$, insofar as its behavior under $\bar{\varphi}$ is concerned, can be replaced by Θ which is in the domain of definition of $\bar{\varphi}$. Now assume that neither of these extreme cases holds. Let $\mathfrak{M} = \bigcap_{i=1}^{r} \mathfrak{L}_i$ where the $\mathfrak{L}_i$ are block ideals. By [3.2], $\mathfrak{L}_i^{\#}$ is a block ideal of $\mathfrak{o}$ and so a power of a prime ideal. Let $\mathfrak{N}$ be the intersection of those $\mathfrak{L}_i$ such that the prime ideal divisor of $\mathfrak{L}_i^{\#}$ also divides $\mathfrak{a}$. Let $\mathfrak{O}$ be the intersection of the remaining $\mathfrak{L}_i$. By I[2.3], $\mathfrak{M} = \mathfrak{N} \cap \mathfrak{O}$ and by [4.2] and [4.4], $\tilde{\mathfrak{M}} = \tilde{\mathfrak{N}}$. Since $\mathfrak{N}$ is in the domain of definition of $\bar{\varphi}$, it follows that $\bar{\varphi}$ is "onto." Since $\tilde{\mathfrak{N}} = \tilde{\mathfrak{o}}\mathfrak{N} \subseteq \tilde{\mathfrak{o}}[\tilde{\mathfrak{N}} \cap \Theta] \subseteq \tilde{\mathfrak{N}}$ and since $\bar{\varphi}$ is one-to-one, it follows that $\mathfrak{N} = \tilde{\mathfrak{N}} \cap \Theta$.

5. Ideals Generated by Ideals of $\mathfrak{o}$

In this section we study block ideal decompositions of ideals of the form $\mathfrak{a}\Theta$ where $\mathfrak{a}$ is a non-zero integral $\mathfrak{o}$ -ideal. In particular, it is shown that the block ideal components of such ideals generate a multiplicative abelian group.

[5.1] Let $\mathfrak{n}\Theta = \bigcap_{i=1}^{s} \mathfrak{L}_i$ where $\mathfrak{n}$ is an integral σ-ideal and the $\mathfrak{L}_i$ are block ideals. Then $\mathfrak{n}^{\lambda}\Theta = \bigcap_{i=1}^{s} \mathfrak{L}_i^{\lambda}$ where λ is any positive integer.

Proof: It is trivial that $\mathfrak{n}^{\lambda}\Theta \subseteq \bigcap_{i=1}^{s} \mathfrak{L}_i^{\lambda}$. The result is true for $\lambda = 1$. Now assume $\mathfrak{n}^{\sigma-1}\Theta = \bigcap_{i=1}^{s} \mathfrak{L}_i^{\sigma-1}$.

By I[2.5], $\bigcap_{i=1}^{s} \mathfrak{L}_i^{\sigma} = \sum_{\pi} \mathfrak{L}_{\pi(1)}^{\sigma} \cdots \mathfrak{L}_{\pi(s)}^{\sigma}$ where π ranges over all permutations of 1, 2,..., s. We now consider a generic term in this sum. From I, theorem 2.1 it follows that the $\mathfrak{L}_i$ commute mod $\mathfrak{n}\Theta$. Therefore

$$\mathfrak{L}_{\pi(1)}^{\sigma} \cdots \mathfrak{L}_{\pi(i-1)}^{\sigma} \mathfrak{L}_{\pi(i)}^{\sigma-1} (\mathfrak{L}_{\pi(i)} \mathfrak{L}_{\pi(i+1)}) \mathfrak{L}_{\pi(i+1)}^{\sigma-1} \mathfrak{L}_{\pi(i+2)}^{\sigma} \cdots \mathfrak{L}_{\pi(s)}^{\sigma}$$

$$\subseteq \mathfrak{L}_{\pi(1)}^{\sigma} \cdots \mathfrak{L}_{\pi(i-1)}^{\sigma} \mathfrak{L}_{\pi(i)}^{\sigma-1} (\mathfrak{L}_{\pi(i+1)} \mathfrak{L}_{\pi(i)} + \mathfrak{n}\Theta) \mathfrak{L}_{\pi(i+1)}^{\sigma-1} \mathfrak{L}_{\pi(i+2)}^{\sigma} \cdots$$

$$\cdots \mathfrak{L}_{\pi(s)}^{\sigma}.$$

By the induction hypothesis, the right-hand side is contained in

$$\mathfrak{L}_{\pi(1)}^{\sigma} \cdots \mathfrak{L}_{\pi(i-1)}^{\sigma} \mathfrak{L}_{\pi(i)}^{\sigma-1} \mathfrak{L}_{\pi(i+1)} \mathfrak{L}_{\pi(i)} \mathfrak{L}_{\pi(i+1)}^{\sigma-1} \mathfrak{L}_{\pi(i+2)}^{\sigma} \cdots \mathfrak{L}_{\pi(s)}^{\sigma}$$

$$+ \mathfrak{n}^{\sigma}\Theta.$$

Repeating this process of interchanging the $\mathfrak{L}_i$ sufficiently often, one obtains

$$\sum_{\pi} \mathfrak{P}^{\sigma}_{\pi(1)} \cdots \mathfrak{P}^{\sigma}_{\pi(s)} \subseteq \sum_{\pi} \mathfrak{P}^{\sigma-1}_{\pi(1)} \cdots \mathfrak{P}^{\sigma-1}_{\pi(s)} (\mathfrak{P}_1 \cdots \mathfrak{P}_s) + \mathfrak{p}^{\sigma}\Theta .$$

By virtue of the induction hypothesis, this implies that

$\prod_{i=1}^{s} \mathfrak{P}^{\sigma}_i \subseteq \mathfrak{p}^{\sigma}\Theta$ and the result follows immediately.

[5.2] Let $\tilde{\mathfrak{o}}$ be the ring of $\mathfrak{P}$-integers of K where $\mathfrak{P}$ is a prime ideal; let $\tilde{\Theta} = \tilde{\mathfrak{o}}\Theta$ and let $\{\eta_1, \ldots, \eta_n\}$ be a minimal basis for $\tilde{\Theta}$. Suppose the congruences $x_\sigma \eta_i - \eta_i x_\sigma \equiv 0 \pmod{\mathfrak{P}^{\sigma}\tilde{\Theta}}$ have a solution x_σ for $i = 1, 2, \ldots, n$ and for each positive integer σ. Then there exists an element $z \in Z \cap \tilde{\Theta}$, where Z is the center of A, such that for some σ, $z \equiv x_\sigma \pmod{\mathfrak{P}\tilde{\Theta}}$.

Proof: Suppose $\eta_i \eta_j = \sum_{k=1}^{n} c_{ijk}\eta_k$ and let $x = \sum_{j=1}^{n} a_j \eta_j$ be some particular x_σ. Then $\sum_{j=1}^{n} a_j(\eta_i \eta_j - \eta_j \eta_i)$ $= \sum_{j=1}^{n}\sum_{k=1}^{n} a_j(c_{ijk} - c_{jik})\eta_k \equiv 0 \pmod{\mathfrak{P}^{\sigma}\tilde{\Theta}}$ and so $\sum_{j=1}^{n} a_j(c_{ijk} - c_{jik}) \equiv 0 \pmod{\mathfrak{P}^{\sigma}\tilde{\mathfrak{o}}}$ for all i, k. Set $c_{ijk} - c_{jik} = b_{i+(k-1)n,\,j}$ and let $\tilde{\mathfrak{P}} = (\pi)$. Then

$$\sum_{j=1}^{n} b_{ij} a_j = \pi^{\sigma} y_i \qquad (1)$$

where $i = 1, 2, \ldots, n^2$ and $y_i \in \tilde{\mathfrak{o}}$. We regard (1) as a system of equations for the a_j. By the theory of elementary

divisors there exists a unimodular transformation which maps $a_j \longrightarrow a'_j = Ta_j$, say, and transforms the system (1) into the form:

$$\begin{aligned} e_1 a'_1 &= \pi^{\sigma} y'_1 \\ &\vdots \quad\quad \vdots \\ e_r a'_r &= \pi^{\sigma} y'_r \\ 0 \cdot a'_{r+1} &= \pi^{\sigma} y'_{r+1} \\ &\vdots \quad\quad \vdots \\ 0 \cdot a'_n &= \pi^{\sigma} y'_n \\ 0 &= \pi^{\sigma} y'_{n+1} \\ &\vdots \quad\quad \vdots \\ 0 &= \pi^{\sigma} y'_{n^2} \end{aligned} \qquad (2)$$

where $e_i \neq 0$ for $i = 1, 2, \ldots, r$; $y'_i \in \tilde{\mathfrak{o}}$. For σ sufficiently large, $a'_1, \ldots, a'_r$ are in $\tilde{\mathfrak{p}}$ and $(0, \ldots, 0, a'_{r+1}, \ldots, a'_n)$ affords a solution to the homogeneous equations corresponding to (2). Now $a_i = \sum_{j=1}^{r} d_{ij} a'_j + \sum_{j=r+1}^{n} d_{ij} a'_j$ where (d_{ij}) is the matrix of T^{-1} and so has integer coefficients. Now the first term is in $\tilde{\mathfrak{p}}$ and so $a_i \equiv \tilde{a}_i \pmod{\tilde{\mathfrak{p}}}$ where $\tilde{a}_i = \sum_{j=r+1}^{n} d_{ij} a'_j$ affords a solution of the homogeneous equations corresponding to (1). The element $z = \sum_{i=1}^{n} \tilde{a}_i \eta_i$ has the required property.

[5.3] Let $\mathfrak{p}\,\Theta = \bigcap_{i=1}^{s} \mathfrak{L}_i$ where the $\mathfrak{L}_i$ are block ideals and $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$. Let $\tilde{\Theta}$ and Z have the same significance as in [5.2]. Then there exist elements $e_1, \ldots, e_s \in Z \cap \tilde{\Theta}$ such that $1 = e_1 + \cdots + e_s$, $e_i \equiv 0 \pmod{\tilde{\mathfrak{L}}_j}$ for $i \neq j$, $e_i \equiv 1 \pmod{\tilde{\mathfrak{L}}_i}$. Furthermore $\tilde{\mathfrak{L}}_i \tilde{\mathfrak{L}}_j = \tilde{\mathfrak{L}}_j \tilde{\mathfrak{L}}_i$ for $i, j = 1, 2, \ldots, s$.

Proof: By theorem 4.1, $\mathfrak{p}\tilde{\Theta} = \bigcap_{i=1}^{s} \tilde{\mathfrak{L}}_i$ where the $\tilde{\mathfrak{L}}_i$ are block ideals. By [5.1] and I [3.6], $\bigcap_{i=1}^{s} \tilde{\mathfrak{L}}_i^{\sigma}$ is the block ideal decomposition of $\mathfrak{p}^{\sigma}\tilde{\Theta}$. It follows from I, theorem 2.1 that there exist elements $e_i' \in \tilde{\Theta}$ such that $1 = e_1' + \cdots + e_s'$, $e_i' \equiv 0 \pmod{\tilde{\mathfrak{L}}_j^{\sigma}}$ for $i \neq j$, $e_i' \equiv 1 \pmod{\tilde{\mathfrak{L}}_i^{\sigma}}$. It is easy to verify that the e_i' are in the center Z modulo $\mathfrak{p}^{\sigma}\tilde{\Theta}$ and so, by taking σ large enough, one may obtain elements $e_i \equiv e_i' \pmod{\mathfrak{p}\tilde{\Theta}}$ with $e_i \in Z \cap \tilde{\Theta}$ by virtue of [5.2]. The fact that $\sum_{i \neq j} e_j \tilde{\Theta}$ is contained in $\tilde{\mathfrak{L}}_i$, together with I [2.11], implies that the $\tilde{\mathfrak{L}}_i$ commute.

[5.4] If $\mathfrak{p}\,\Theta = \bigcap_{i=1}^{r} \mathfrak{L}_i$ where the $\mathfrak{L}_i$ are block ideals and $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$, then the $\mathfrak{L}_i$ commute and

$$\mathfrak{p}\,\Theta = \prod_{i=1}^{r} \mathfrak{L}_i .$$

Proof: This follows immediately from I[2.5], [5.3] and theorem 4.1.

For $\mathfrak{L}_i$ as in [5.4] let $\mathfrak{L}_i^{-1}$ be the set of elements $x \in A$ such that $x\mathfrak{L}_i \subseteq \Theta$. Clearly $\mathfrak{L}_i^{-1}$ is an Θ -ideal containing Θ . It is easily verified that $\mathfrak{L}_i^{-1} = \mathfrak{p}^{-1} \prod_{j \neq i} \mathfrak{L}_j$ and that $\mathfrak{L}_i \mathfrak{L}_i^{-1} = \mathfrak{L}_i^{-1} \mathfrak{L}_i = \Theta$.

If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct prime ideals of $\mathfrak{o}$, then by I[2.11] every block ideal of $\mathfrak{p}_1\Theta$ must commute with every block ideal of $\mathfrak{p}_2\Theta$.

Theorem 5.1: The block ideal components of ideals $\mathfrak{p}\Theta$, where $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$, generate an abelian group $\mathfrak{J}$. The representation of an ideal $\mathfrak{A} = \mathfrak{L}_1^{\lambda_1} \cdots \mathfrak{L}_s^{\lambda_s}$ of $\mathfrak{J}$ as a product of powers of distinct block ideals $\mathfrak{L}_i$, where the λ_i are non-zero rational integers, is unique.

Proof: The first part of the theorem follows from the preceding discussion. The uniqueness is proved as in algebraic number theory.

Theorem 5.2: If Z is the center of A, then $Q = Z \cap \Theta$ is an order of Z. If $\mathfrak{p}\Theta = \bigcap_{i=1}^{s} \mathfrak{L}_i$ where $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$ and the $\mathfrak{L}_i$ are block ideals, then $\mathfrak{p}Q = \bigcap_{i=1}^{s} \mathfrak{q}_i$ where $\mathfrak{q}_i = \mathfrak{L}_i \cap Q$ are block ideals of Q. Furthermore, $\mathfrak{L}_i = \mathfrak{q}_i\Theta$.

Proof: It is trivial to verify that Q is an order of Z. By [5.3], the $\tilde{\mathfrak{P}}_i$ are relatively prime. By [3.2], the $\mathfrak{P}_i \cap \mathfrak{o}$ are block ideals. This, together with the fact that $\mathfrak{p} \subseteq \mathfrak{P}_i \cap \mathfrak{o}$, implies that $\mathfrak{p} = \mathfrak{P}_i \cap \mathfrak{o}$. Applying theorem 4.1 to Q in place of Θ, one obtains $\mathfrak{p}Q \subseteq \bigcap_{i=1}^{s} \mathfrak{P}_i$. Now $\mathfrak{p}Q \subseteq \mathfrak{p}\Theta \cap Q$ and $\mathfrak{p}^{-1}(\mathfrak{p}\Theta \cap Q) \subseteq Q$, $\mathfrak{p}\Theta \cap Q \subseteq \mathfrak{p}Q$ and so $\mathfrak{p}\Theta \cap Q = \mathfrak{p}Q$. It follows that $\mathfrak{p}Q = \bigcap_{i=1}^{s} \mathfrak{P}_i$. Now $\mathfrak{p}\Theta = \bigcap_{i=1}^{s} \mathfrak{P}_i\Theta$ and so $\mathfrak{L}_i = \mathfrak{P}_i\Theta$ by I, theorem 3.1. If $\mathfrak{P}_i = \mathfrak{P}_i' \cap \mathfrak{P}_i''$ for some i, then $\mathfrak{P}_i = \mathfrak{P}_i' \cdot \mathfrak{P}_i''$ by I[2.4] and $\mathfrak{L}_i = \mathfrak{P}_i' \cdot \mathfrak{P}_i''\Theta = \mathfrak{P}_i'\Theta \cap \mathfrak{P}_i''\Theta$, a contradiction. Consequently, the $\mathfrak{P}_i$ are block ideals and, being in the center, they commute.

Remark: This result is of crucial importance for the subsequent developments. It would be extremely desirable to find an elementary proof, thereby avoiding the "local" device of section 4 and the elementary divisor theory used in [5.2]. Unfortunately, we have been unable as yet to construct such a proof.

Theorem 5.3: Let $\mathfrak{A}$ be an integral Θ-ideal and set $\mathfrak{a} = \mathfrak{A}^{\#}$. Let $\mathfrak{a}\Theta = \mathfrak{L}_1 \cap \cdots \cap \mathfrak{L}_s$ where the $\mathfrak{L}_i$ are block ideals. Then $\mathfrak{A}$ can be expressed uniquely as a product $\mathfrak{A} = \mathfrak{A}_1 \cdots \mathfrak{A}_s$ where $\mathfrak{A}_i$ divides $\mathfrak{L}_i$; $\mathfrak{A}_i = (\mathfrak{A}, \mathfrak{L}_i)$ and the $\mathfrak{A}_i$ commute.

Proof: This follows by an elementary argument from theorem 5.1 and I[2.11].

6. Prime Ideals and Arithmetics in Maximal Orders

If $\mathfrak{P}$ is a prime ideal of $\mathfrak{O}$, then it is easily verified that $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$ is a prime ideal of $\mathfrak{o}$. From [3.4] and I, theorem 4.1 it is clear that a prime ideal $\mathfrak{p}$ in $\mathfrak{o}$ has only a finite number of prime ideal divisors $\mathfrak{P}$ in $\mathfrak{O}$.

For a fixed prime ideal $\mathfrak{P} \subset \mathfrak{O}$ let $\mathfrak{O}_\mathfrak{P}$ be the set of elements $\mu \in A$ such that $\mu \mathfrak{P} \subseteq \mathfrak{O}$. There exists an element $\omega \neq 0$ in $\mathfrak{p}$ such that $\mathfrak{O}_\mathfrak{P} \omega \subseteq \mathfrak{O}$ and so $\mathfrak{O}_\mathfrak{P}$ is an ideal of $\mathfrak{O}$ with $\mathfrak{O}_\mathfrak{P} \geq \mathfrak{O}$. Since $\mathfrak{P}$ is maximal and $\mathfrak{P} \subseteq \mathfrak{O}_\mathfrak{P} \mathfrak{P} \subseteq \mathfrak{O}$, it follows that either $\mathfrak{P} = \mathfrak{O}_\mathfrak{P} \mathfrak{P}$ or $\mathfrak{O}_\mathfrak{P} \mathfrak{P} = \mathfrak{O}$. In the first case $\mathfrak{O}_\mathfrak{P}^2 \subseteq \mathfrak{O}_\mathfrak{P}$ and so $\mathfrak{O}_\mathfrak{P}$ is an order. If $\mathfrak{O}_\mathfrak{P} \supset \mathfrak{O}$, then $\mathfrak{P}$ is said to be <u>regular</u>. These results are summarized in

[6.1] <u>If $\mathfrak{P}$ is a regular prime ideal, then either there exists a fractional ideal $\mathfrak{O}_\mathfrak{P} \supset \mathfrak{O}$ with $\mathfrak{O}_\mathfrak{P} \mathfrak{P} = \mathfrak{O}$, or there exists an order $\mathfrak{O}_\mathfrak{P} \supset \mathfrak{O}$ such that $\mathfrak{O}_\mathfrak{P} \mathfrak{P} = \mathfrak{P}$.</u>

[6.2] <u>In the first case of</u> [6.1], <u>i.e.</u> $\mathfrak{O}_\mathfrak{P} \supset \mathfrak{O}$ <u>with</u> $\mathfrak{O}_\mathfrak{P} \mathfrak{P} = \mathfrak{O}$, <u>either</u> $\mathfrak{P} \mathfrak{O}_\mathfrak{P} = \mathfrak{O}$ <u>or there exists an order</u> $\mathfrak{R} \supset \mathfrak{O}$ <u>such that</u> $\mathfrak{R} \mathfrak{P} = \mathfrak{P}$.

Proof: Since $(\mathfrak{P} \mathfrak{O}_\mathfrak{P})^2 = \mathfrak{P} \mathfrak{O}_\mathfrak{P}$ and $\mathfrak{P} \mathfrak{O}_\mathfrak{P}$, being an ideal, is finitely generated, it follows that $(\mathfrak{P} \mathfrak{O}_\mathfrak{P}, \mathfrak{O}) = \mathfrak{R}$ is an order containing $\mathfrak{O}$. If $(\mathfrak{P} \mathfrak{O}_\mathfrak{P}, \mathfrak{O}) = \mathfrak{O}$, then $\mathfrak{P} \mathfrak{O}_\mathfrak{P} \subseteq \mathfrak{O}$ and so $\mathfrak{P} \mathfrak{O}_\mathfrak{P} = \mathfrak{O}$ or $\mathfrak{P}$, since $\mathfrak{O}_\mathfrak{P} \supset \mathfrak{O}$. If $\mathfrak{P} \mathfrak{O}_\mathfrak{P} = \mathfrak{P}$,

then $\mathfrak{N} = \mathfrak{N}\mathfrak{P}\mathfrak{N} = \mathfrak{N}\mathfrak{P} = \mathfrak{O}$, a contradiction. Therefore either $\mathfrak{P}\mathfrak{N} = \mathfrak{O}$ or $\mathfrak{N}$ is an order with $\mathfrak{N} \supset \mathfrak{O}$ and $\mathfrak{N}\mathfrak{P} = \mathfrak{P}$.

If $\mathfrak{N}$ is an ideal of $\mathfrak{O}$, then the set of elements $x \in A$ such that $x\mathfrak{N} \subseteq \mathfrak{N}$ is an order $\mathfrak{O}^*$ called the <u>left-order of</u> $\mathfrak{N}$. (In the verification that $\mathfrak{O}^*$ is an order, observe that there exists an element $\omega \neq 0$ in $\mathfrak{N} \cap K$ such that $\omega\mathfrak{O}^* \subseteq \mathfrak{N}$ and that one may assume $\omega \in \mathfrak{o}$.)

[6.3] <u>If $\mathfrak{P}$ is a regular prime ideal whose left-order is $\mathfrak{O}$, then</u> $\mathfrak{P}\mathfrak{N} = \mathfrak{N}\mathfrak{P} = \mathfrak{O}$.

Proof: This follows immediately from [6.1] and [6.2].

If a prime $\mathfrak{P}$ has the property of [6.3], then it is said to be <u>completely regular</u>. One defines $\mathfrak{N} = \mathfrak{P}^{-1}$.

[6.4] <u>If a block of $\mathfrak{g}\mathfrak{O}$ contains a completely regular prime $\mathfrak{P}$, then the corresponding block ideal $\mathfrak{L}$ is a power of $\mathfrak{P}$. Every ideal which divides a power of $\mathfrak{P}$ is itself a power of $\mathfrak{P}$.</u>

Proof: The ideal $\mathfrak{L}' = \mathfrak{P}^{-1}\mathfrak{L}$ is integral since $\mathfrak{P}$ divides $\mathfrak{L}$. If $\mathfrak{L} = \mathfrak{L}'$, then $\mathfrak{P}^{\lambda}\mathfrak{L}' = \mathfrak{L}$ for every integer $\lambda > 0$. Then each $\mathfrak{P}^{\lambda}$ divides $\mathfrak{L}$. But the $\mathfrak{P}^{\lambda}$ are distinct and [3.4] implies that only a finite number of them can divide $\mathfrak{L}$. It follows that $\mathfrak{L}' \neq \mathfrak{L}$. A completely regular prime commutes with all other primes (cf. (8), p. 74) and so by I, theorem 4.3, the block to which $\mathfrak{P}$ belongs consists only of $\mathfrak{P}$ itself. Then by I, theorem 4.4, $\mathfrak{L} = \mathfrak{P}^{\sigma} + \mathfrak{g}\mathfrak{O}$

for some $\sigma > 0$. Now if $\mathfrak{L} \subseteq \mathfrak{L}' \subseteq \mathfrak{P}'$ for a prime $\mathfrak{P}'$ then $\mathfrak{P}' = \mathfrak{P}$. Therefore $\mathfrak{P}$ divides $\mathfrak{L}'$. We proceed by induction to obtain $\mathfrak{L} = \mathfrak{P}^{\mu}$, $\mu > 0$. If $\mathfrak{P}^{\alpha} \subseteq \mathfrak{A}$, the only prime dividing $\mathfrak{A}$ is $\mathfrak{P}$ and, proceeding as before, we obtain $\mathfrak{A} = \mathfrak{P}^{\lambda}$, $\lambda \leq \alpha$.

Theorem 6.1: If Θ is a maximal order, then every non-zero ideal can be expressed uniquely as a product of powers of prime ideals. The non-zero ideals of Θ form a multiplicative abelian group generated by the prime ideals.

Proof: Every prime ideal is regular (cf. (8), p. 74) and so completely regular by [6.1] and [6.2]. Let $\mathfrak{A}$ be an integral Θ-ideal. Set $\mathfrak{a} = \mathfrak{A}^{\#}$. By [6.4], $\mathfrak{a}\Theta = \mathfrak{P}_1^{\mu_1} \cdots \mathfrak{P}_s^{\mu_s}$ where the $\mathfrak{P}_i$ commute by virtue of either theorem 5.1 or the fact that completely regular prime ideals commute. Then by [6.4] and theorem 5.3, $\mathfrak{A} = \mathfrak{P}_1^{\nu_1} \cdots \mathfrak{P}_s^{\nu_s}$ with $\nu_i \leq \mu_i$. If $\mathfrak{L}$ is a fractional ideal, determine $\mu \neq 0$ such that $\mu \mathfrak{L} \subseteq \Theta$. Constructing the prime ideal decomposition for $\mu\Theta$ and $\mu\mathfrak{L}$, it follows that $\mathfrak{L}$ has a prime ideal decomposition. The uniqueness is proved as in algebraic number theory.

Theorem 6.2: Let Θ be an order whose non-zero ideals form a multiplicative group. Then Θ is maximal.

Proof: See (2).

Theorem 6.3: If Θ is an arbitrary order, then every integral ideal has a unique decomposition $\mathfrak{A} = \mathfrak{P}_1^{\mu_1} \cdots \mathfrak{P}_s^{\mu_s} \mathfrak{M}$ where the $\mathfrak{P}_i$ are completely regular prime ideals and $\mathfrak{M}$ is an integral ideal not divisible by any completely regular prime ideal. The $\mathfrak{P}_i$ and $\mathfrak{M}$ commute.

Proof: Let $\mathfrak{A} = \bigcap_{i=1}^{n} \mathfrak{Q}_i$ where the $\mathfrak{Q}_i$ are block ideals. Suppose $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$ are the $\mathfrak{Q}_i$ which are divisible by completely regular prime ideals. As in the proof of theorem 6.1, one finds $\mathfrak{Q}_i = \mathfrak{P}_i^{\mu_i}$ $(i = 1, 2, \ldots, r)$ with $\mathfrak{P}_i$ completely regular. By I[3.2], $\mathfrak{M} = \bigcap_{i=r+1}^{n} \mathfrak{Q}_i$ is not divisible by any completely regular prime ideal. The $\mathfrak{P}_i$ commute with all prime ideal divisors $\mathfrak{P}_a$ of $\mathfrak{M}$ and so, by I[2.9], with any intersection of these $\mathfrak{P}_a$. By I, theorem 4.3, I[2.11] and I[2.9] it follows that $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ commute with $\mathfrak{M}$. By I[2.3] and I[2.4], $\mathfrak{A} = \mathfrak{P}_1^{\mu_1} \cdots \mathfrak{P}_r^{\mu_r} \mathfrak{M}$ as required. The uniqueness follows from I, theorem 3.1.

7. Arithmetics in Simple Algebras

In this section we apply the preceding results to certain classes of simple algebras.

First, suppose A is central simple over K. Let $\mathfrak{A} = \bigcap_{i=1}^{s} \mathfrak{Q}_i$ be an integral Θ-ideal where the $\mathfrak{Q}_i$ are

block ideals. Let $\mathfrak{A}^{\#} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where the $\mathfrak{p}_i$ are prime ideals of $\mathfrak{o}$. By theorem 5.2 it follows that r = s and the $\mathfrak{P}_i$ can be indexed so that $\mathfrak{p}_i^{e_i} = \mathfrak{P}_i^{\#}$. By the same theorem, $\mathfrak{p}_i^{e_i}\Theta = \mathfrak{P}_i$ and so the $\mathfrak{P}_i$ commute. This proves

Theorem 7.1: If A is central simple over K and Θ is any order of A, then the block ideal components of any integral Θ-ideal commute.

If Θ is maximal and $\mathfrak{A} = \mathfrak{p}\Theta$ where $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$, then s = 1, $\mathfrak{p}\Theta$ is a block ideal, and so a power of a prime ideal of Θ. This proves the following theorem due to Brandt (4).

Theorem 7.2: If Θ is a maximal order in a central simple algebra A and $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$, then $\mathfrak{p}\Theta = \mathfrak{P}^e$ where $\mathfrak{P}$ is a prime ideal of Θ.

Theorem 7.3: Let K be a field with a discrete non-trivial valuation. Let A be a simple algebra over K, not necessarily central, and let Θ be a maximal order with respect to the local integers of K. Then Θ has a unique prime ideal $\mathfrak{P}$ and every Θ-ideal has the form $\mathfrak{P}^e$ where e is a rational integer.

Proof: This follows immediately from [6.4] since K has only one local prime ideal.

Another development of this result for the case where K is a $\mathfrak{p}$-adic field has been given by Hasse (10).

8. Extensions of $\mathfrak{O}$

If $\mathfrak{O}$ and $\mathfrak{O}^* \supseteq \mathfrak{O}$ are two orders of A, it is natural to ask what is the relation between the arithmetic of $\mathfrak{O}$ and that of $\mathfrak{O}^*$. In this section we introduce some of the concepts used in the study of this problem.

[8.1] *There exist integral ideals of $\mathfrak{O}^*$ which lie in $\mathfrak{O}$; indeed, there exists an element $d \neq 0$ in $\mathfrak{o}$ such that $d\mathfrak{O}^* \subseteq \mathfrak{O}$.*

Proof: By [2.1] there exist elements $\sigma_1, \ldots, \sigma_n \in \mathfrak{O}$ and $c \neq 0$ in $\mathfrak{o}$ such that every element $\alpha \in \mathfrak{O}$ has a unique representation $\alpha = \frac{1}{c} \sum_{i=1}^{n} a_i \sigma_i$, $a_i \in \mathfrak{o}$. There exist analogous elements $\sigma_1^*, \ldots, \sigma_n^*$ and c^* for $\mathfrak{O}^*$. The σ_i constitute a K-basis for A and so there exist elements $c_{ij} \in K$ such that $\sigma_i^* = \sum_{j=1}^{n} c_{ij}\sigma_j$. Since K is the quotient field of $\mathfrak{o}$, there exist elements $d_i \in \mathfrak{o}$, $d_i \neq 0$, such that $d_i \sigma_i^* \in \mathfrak{O}$. Set $d = c^* \cdot d_1 \cdots d_n$. Then $d\mathfrak{O}^* \subseteq \mathfrak{O}$ and $d\mathfrak{O}^*$ is clearly an integral ideal of $\mathfrak{O}^*$.

Throughout this section, attention will be restricted to integral ideals. Every $\mathfrak{O}$-ideal $\mathfrak{L}$ determines an $\mathfrak{O}^*$-ideal $\{\mathfrak{L}\} = \mathfrak{O}^*\mathfrak{L}\mathfrak{O}^*$ and every $\mathfrak{O}^*$-ideal $\mathfrak{L}$ determines an $\mathfrak{O}$-ideal $\mathfrak{L}^\circ = \mathfrak{L} \cap \mathfrak{O}$.

It is trivial to verify

[8.2] Let $\mathfrak{A}$, $\mathfrak{B}$ be Θ-ideals and $\mathfrak{L}$, $\mathfrak{M}$ be Θ^*-ideals. Then $\{\mathfrak{B}\}^0 \supseteq \mathfrak{B}$, $\{\mathfrak{L}^0\} \subseteq \mathfrak{L}$; if $\mathfrak{A} \subseteq \mathfrak{B}$, then $\{\mathfrak{A}\} \subseteq \{\mathfrak{B}\}$; if $\mathfrak{L} \subseteq \mathfrak{M}$, then $\mathfrak{L}^0 \subseteq \mathfrak{M}^0$. Furthermore, $\{\{\mathfrak{A}\}^0\} = \{\mathfrak{A}\}$ and $\{\mathfrak{L}^0\}^0 = \mathfrak{L}^0$.

The ideal generated by the set of Θ^*-ideals which lie in Θ is called the conductor $\mathfrak{F}$ of Θ with respect to Θ^*. By [8.1], $\mathfrak{F} \neq (0)$. The conductor enjoys the property of being an integral ideal of both Θ and Θ^* simultaneously. This fact will be of crucial importance in what follows.

An Θ-ideal $\mathfrak{A}$ is said to be regular with respect to Θ^* if $(\mathfrak{A}, \mathfrak{F}) = \Theta$. An Θ^*-ideal $\mathfrak{L}$ is said to be regular with respect to Θ if $(\mathfrak{L}, \mathfrak{F}) = \Theta^*$. (This use of the term "regular" is not to be confused with that in section 6. Unfortunately, the word occurs with both senses in the literature. In the following discussion, we shall use the term in the sense just defined.)

[8.3] If the Θ-ideal $\mathfrak{A}$ is regular, then so is $\{\mathfrak{A}\}$. If the Θ^*-ideal $\mathfrak{L}$ is regular, then so is $\mathfrak{L}^0$. In this case $\{\mathfrak{A}\}^0 = \mathfrak{A}$, $\{\mathfrak{L}^0\} = \mathfrak{L}$.

Proof: Suppose $\mathfrak{A}$ is regular. Then $1 \in (\mathfrak{A}, \mathfrak{F}) \subseteq (\{\mathfrak{A}\}, \mathfrak{F})$ and so $\{\mathfrak{A}\}$ is regular. If $(\mathfrak{L}, \mathfrak{F}) = \Theta^*$, then there exist elements $c \in \mathfrak{L}$, $f \in \mathfrak{F}$ such that $1 = c + f$. Now $1 - f = c \in \Theta$ and so $(\mathfrak{L}^0, \mathfrak{F}) = \Theta$. By [8.2], $\{\mathfrak{A}\}^0 \supseteq \mathfrak{A}$. Since $(\mathfrak{A}, \mathfrak{F}) = \Theta$, it follows that there exist elements

$a \in \mathfrak{A}$, $f \in \mathfrak{F}$ such that $a + f = 1$. Now suppose $x \in \{\mathfrak{A}\}^0$. Then $x = (a + f)\, x\, (a + f) = (axa + axf + fxa) + fxf$. The bracketed term in the latter expression is in $\mathfrak{A}$ and $fxf \in \mathfrak{F}(\Theta^* \mathfrak{A} \Theta^*)\mathfrak{F} \subseteq \mathfrak{F}\mathfrak{A}\mathfrak{F} \subseteq \mathfrak{A}$ and so $x \in \mathfrak{A}$. Therefore $\{\mathfrak{A}\}^0 = \mathfrak{A}$. By [8.2], $\{\mathfrak{L}^0\} \subseteq \mathfrak{L}$. Since $\{\mathfrak{L}^0\}$ is regular, it follows that there exist elements $c \in \{\mathfrak{L}^0\}$, $f \in \mathfrak{F}$ such that $c + f = 1$. Now suppose $x \in \mathfrak{L}$. Then $x = (c + f)\, x\, (c + f) = (cxc + cxf + fxc) + fxf$. The final bracketed expression is in $\{\mathfrak{L}^0\}$ and $fxf \in \mathfrak{L}^0 \subseteq \{\mathfrak{L}^0\}$. Then $x \in \{\mathfrak{L}^0\}$ and so $\{\mathfrak{L}^0\} = \mathfrak{L}$.

<u>Theorem 8.1: The mapping $\psi : \mathfrak{A} \longrightarrow \{\mathfrak{A}\}$ is a one-to-one mapping of the set of regular Θ-ideals onto the set of all regular Θ^*-ideals. It is an isomorphism with respect to sum, product and intersection.</u>

Proof: The first statement follows from [8.3]. Now suppose $\mathfrak{A}_1 \longrightarrow \{\mathfrak{A}_1\}$ and $\mathfrak{A}_2 \longrightarrow \{\mathfrak{A}_2\}$. Then $\{\mathfrak{A}_1 + \mathfrak{A}_2\} = \{\mathfrak{A}_1\} + \{\mathfrak{A}_2\}$ is the image of $\mathfrak{A}_1 + \mathfrak{A}_2$ and is regular. Now $\mathfrak{A}_1 \cap \mathfrak{A}_2 \longrightarrow \{\mathfrak{A}_1 \cap \mathfrak{A}_2\}$. By I[2.2], $\mathfrak{A}_1 \cap \mathfrak{A}_2$ is regular. Now $(\{\mathfrak{A}_1\} \cap \{\mathfrak{A}_2\})^0 = \{\mathfrak{A}_1\}^0 \cap \{\mathfrak{A}_2\}^0 = \mathfrak{A}_1 \cap \mathfrak{A}_2$ and $(\{\mathfrak{A}_1\} \cap \{\mathfrak{A}_2\})^0$ maps onto $\{\mathfrak{A}_1\} \cap \{\mathfrak{A}_2\}$. Therefore $\{\mathfrak{A}_1\} \cap \{\mathfrak{A}_2\} = \{\mathfrak{A}_1 \cap \mathfrak{A}_2\}$. By I[2.8], the product of two regular ideals is regular. We now show $\{\mathfrak{A}_1 \mathfrak{A}_2\} = \{\mathfrak{A}_1\} \cdot \{\mathfrak{A}_2\}$. Certainly $\{\mathfrak{A}_1 \mathfrak{A}_2\} \subseteq \{\mathfrak{A}_1\} \cdot \{\mathfrak{A}_2\}$. Elements of

$\{\mathfrak{A}_1\} \cdot \{\mathfrak{A}_2\}$ have the form $\sum y a_1 x a_2 y'$ where $a_i \in \mathfrak{A}_i$; $x, y, y' \in \Theta^*$. It will suffice to show that $a_1 x a_2 \in \{\mathfrak{A}_1 \mathfrak{A}_2\}$. There exist elements $b \in \mathfrak{o}$, $f \in \mathfrak{F}$ such that $1 = b + f$. Now $a_1 x a_2 = a_1(b + f) x a_2$. A straightforward computation reveals that this latter expression is in $\{\mathfrak{A}_1 \mathfrak{A}_2\}$. This completes the proof.

9. The Discriminant

In this section it will be assumed that A is semi-simple and separable over K. This latter condition will obtain, for instance, if K has characteristic zero. If $\tilde{\mathfrak{o}}$ is the ring of $\mathfrak{p}$-integers, we shall set $\tilde{\mathfrak{o}} = \mathfrak{o}_\mathfrak{p}$, $\tilde{\Theta} = \Theta_\mathfrak{p}$ since it will be necessary to consider extensions by different primes. (This notation is not to be confused with that of Hasse in (10) where the complete $\mathfrak{p}$-adic field is used.)

Since $\mathfrak{o}_\mathfrak{p}$ is a principal ideal ring, it follows that $\Theta_\mathfrak{p}$ has a minimal basis, say $\sigma_1, \ldots, \sigma_n$. It is evident that the σ_i may be assumed to be in Θ. Every element $\alpha \in \Theta_\mathfrak{p}$ has a unique expression $\alpha = \sum_{i=1}^{n} c_i \sigma_i$ with $c_i \in \mathfrak{o}_\mathfrak{p}$. Let $S(\alpha)$ denote the trace of α in the regular representation.

If $\alpha_1, \ldots, \alpha_n \in A$, then one defines the <u>discriminant</u> to be $\Delta(\alpha_1, \ldots, \alpha_n) = \det(S(\alpha_i \alpha_j))$ where $(S(\alpha_i \alpha_j))$ is the matrix with i as row-index and j as column index. If $\beta_i = \sum_{j=1}^{n} c_{ij} \alpha_j$ with $c_{ij} \in K$, it is easily verified that

$\Delta(\beta_1,\ldots,\beta_n) = (\det(c_{ij}))^2\Delta(\alpha_1,\ldots,\alpha_n)$. By [2.1], there exist elements $\eta_1,\ldots,\eta_n \in \mathcal{O}$ and an element $c \in \sigma$ such that $\mathcal{O} \subseteq \frac{1}{c}\cdot\sigma\{\eta_1,\ldots,\eta_n\}$. If one uses the $\eta_i c^{-1}$ as a K-basis for A in calculating Δ, it is evident that if $\alpha_1,\ldots,\alpha_n \in \mathcal{O}$, then $\Delta(\alpha_1,\ldots,\alpha_n) \in \sigma$.

We define $\mathfrak{d}_\mathfrak{p}$, <u>the $\mathfrak{p}$-component of the discriminant of</u> $\mathcal{O}$, to be the power of $\mathfrak{p}$ which divides $\Delta(\sigma_1,\ldots,\sigma_n)$.

[9.1] <u>$\mathfrak{d}_\mathfrak{p}$ is the largest power of $\mathfrak{p}$ which contains all elements $\Delta(\alpha_1,\ldots,\alpha_n)$ for $\alpha_i \in \mathcal{O}$</u>.

Proof: Set $\sigma\cdot\Delta(\sigma_1,\ldots,\sigma_n) = \mathfrak{p}^\lambda\mathfrak{n}$ where $\mathfrak{p} \nmid \mathfrak{n}$. For $\alpha_i \in \mathcal{O}$, $\alpha_i = \sum_{j=1}^{n} c_{ij}\sigma_j$ with $c_{ij} \in \sigma_\mathfrak{p}$. Now $\Delta(\alpha_1,\ldots,\alpha_n)$ $= (\det(c_{ij}))^2\Delta(\sigma_1,\ldots,\sigma_n)$ and $\det(c_{ij})$ has denominator prime to $\mathfrak{p}$. Therefore $\Delta(\alpha_1,\ldots,\alpha_n) \in \mathfrak{p}^\lambda$ and the result follows.

The integral σ-ideal $\mathfrak{d}$ generated by the set of all elements $\Delta(\alpha_1,\ldots,\alpha_n)$ for $\alpha_i \in \mathcal{O}$ is called the <u>discriminant</u> of $\mathcal{O}$.

Since $\mathfrak{d}$ is the product of the largest powers of the prime ideals which divide all $\Delta(\alpha_1,\ldots,\alpha_n)$ for $\alpha_i \in \mathcal{O}$, it follows from [9.1] that $\mathfrak{d} = \prod_\mathfrak{p} \mathfrak{d}_\mathfrak{p}$ and that there are only a finite number of terms $\mathfrak{d}_\mathfrak{p} \neq \sigma_\mathfrak{p}$.

<u>Theorem 9.1</u>: <u>Let $\mathfrak{d}$ be the discriminant of $\mathcal{O}$ and $\mathfrak{d}^*$ the discriminant of $\mathcal{O}^* \supseteq \mathcal{O}$. Then $\mathfrak{d}^*$ divides $\mathfrak{d}$; furthermore $\mathfrak{d} = \mathfrak{d}^*$ if and only if $\mathcal{O} = \mathcal{O}^*$</u>.

Proof: The first statement follows immediately from [9.1]. Now suppose $\mathfrak{d} = \mathfrak{d}^*$. Let $\{\sigma_i\}$ be a minimal basis for $\Theta_\mathfrak{p}$ with $\sigma_i \in \Theta$; let $\{\sigma_i^*\}$ be a minimal basis for $\Theta_\mathfrak{p}^*$ with $\sigma_i^* \in \Theta^*$. Then $\sigma_i = \sum_{j=1}^{n} c_{ij}\sigma_j^*$ where $c_{ij} \in o_\mathfrak{p}$. Then $\Delta(\sigma_1, \ldots, \sigma_n) = (\det(c_{ij}))^2 \Delta(\sigma_1^*, \ldots, \sigma_n^*)$. Since $\mathfrak{d}_\mathfrak{p} = \mathfrak{d}_\mathfrak{p}^*$, it follows that $\det(c_{ij})$ is not in $\mathfrak{p}$. Therefore $(\det(c_{ij}))^{-1} \in o_\mathfrak{p}$ and so $\sigma_j^* \in o_\mathfrak{p}\{\sigma_1, \ldots, \sigma_n\} = \Theta_\mathfrak{p}$ for $j = 1, 2, \ldots, n$ by Cramer's rule. Therefore $\Theta_\mathfrak{p} = \Theta_\mathfrak{p}^*$ for all primes $\mathfrak{p}$. From this we wish to show $\Theta = \Theta^*$. For $\alpha \in \mathcal{O}^*$, let o_α be the set of elements $\omega \in o$ such that $\omega\alpha \in \mathcal{O}$. Now $\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^*$ for all $\mathfrak{p}$ and so $\lambda\alpha \in \mathcal{O}$ for some element $\lambda \in o$ with $(\lambda, \mathfrak{p}) = (1)$. Therefore $o_\alpha = o$ for all $\alpha \in \mathcal{O}$ and so $\mathcal{O} = \mathcal{O}^*$. The converse is trivial.

[9.2] <u>If the prime ideal $\mathfrak{p}$ of o has an Θ-prime ideal divisor $\mathfrak{P}$ whose left order is $\Theta^* \supset \Theta$, then the discriminant of Θ^* contains $\mathfrak{p}$ to a smaller power than does the discriminant of Θ</u> .

Proof: If $\alpha \in \Theta^*$, then $\alpha\mathfrak{P} \subseteq \mathfrak{P} \subset \Theta$. For each prime ideal $\mathfrak{p}' \neq \mathfrak{p}$, there exists an element $\pi \in \mathfrak{p} = \mathfrak{P} \cap o$ such that $(\pi, \mathfrak{p}') = (1)$. Then $\alpha\pi \in \Theta$, $\alpha \in \pi^{-1}\Theta \subseteq \Theta_{\mathfrak{p}'}$. Therefore $\Theta^* \subseteq \Theta_{\mathfrak{p}'}$, $\Theta_{\mathfrak{p}'}^* \subseteq \Theta_{\mathfrak{p}'}$ and so $\Theta_{\mathfrak{p}'} = \Theta_{\mathfrak{p}'}^*$ for $\mathfrak{p} \neq \mathfrak{p}'$. By theorem 9.1 it follows that $\mathfrak{d}_\mathfrak{p}^* \supset \mathfrak{d}_\mathfrak{p}$.

Theorem 9.2: *Let Θ be an order contained in a maximal order Θ^*. Let $\mathfrak{o}$ and $\mathfrak{o}^*$ be the discriminants of Θ and Θ^* respectively. Let $\mathfrak{F}$ be the conductor of Θ with respect to Θ^*. Then $\mathfrak{o}_\mathfrak{g}^* \supset \mathfrak{o}_\mathfrak{g}$ if and only if $\mathfrak{g}$ is divisible by a prime ideal divisor in Θ^* of $\mathfrak{F}$.*

Proof: Suppose $\mathfrak{F} = \mathfrak{P}_1^{*\lambda_1} \cdots \mathfrak{P}_s^{*\lambda_s}$ is the prime ideal decomposition of $\mathfrak{F}$ in Θ^*. Set $\mathfrak{g}_i = \mathfrak{P}_i^* \cap \mathfrak{o}$ and let $\mathfrak{g}$ be one of these $\mathfrak{g}_i$, with $\mathfrak{P}^*$ the corresponding $\mathfrak{P}_i^*$. We wish to show $\mathfrak{o}_\mathfrak{g}^* \supset \mathfrak{o}_\mathfrak{g}$. By theorem 9.1, it will suffice to show $\Theta_\mathfrak{g}^* \supset \Theta_\mathfrak{g}$. Let $\tilde{\mathfrak{F}}$ be the conductor of $\Theta_\mathfrak{g}$ with regard to $\Theta_\mathfrak{g}^*$. We contend that $\mathfrak{F}_\mathfrak{g} = \tilde{\mathfrak{F}}$. Certainly $\mathfrak{F}_\mathfrak{g} \subseteq \tilde{\mathfrak{F}}$. Now let α be an arbitrary element of $\tilde{\mathfrak{F}}$. There exists an element $a \in \mathfrak{o}$ with $(a, \mathfrak{g}) = (1)$ such that $a\alpha \in \Theta$. Then $\Theta^*(a\alpha)\Theta^* \subseteq \Theta_\mathfrak{g} \cap \Theta^*$. Now $\Theta_\mathfrak{g} \cap \Theta^*$ is an $\mathfrak{o}$-order and so satisfies the ascending chain condition for sub-modules. Consequently one can find elements $\sigma_1, \ldots, \sigma_m$ such that $\Theta_\mathfrak{g} \cap \Theta^* = \mathfrak{o}\{\sigma_1, \ldots, \sigma_m\}$. Then one can find an element $b \in \mathfrak{o}$ with $(b, \mathfrak{g}) = (1)$ such that $b\sigma_i \in \Theta$ for all i. Then $\Theta^*(ab\alpha)\Theta^* \subseteq \Theta$ and so $ab\alpha \in \mathfrak{F}$, $\alpha \in (ab)^{-1}\mathfrak{F} \subseteq \mathfrak{F}_\mathfrak{g}$. It follows that $\tilde{\mathfrak{F}} = \mathfrak{F}_\mathfrak{g}$.

If $1 \in \mathfrak{F}_{\mathfrak{p}}$, then $1 = \sum_{i=1}^{m} c_i p_i$ where $c_i \in \mathfrak{o}_{\mathfrak{p}}$ and $p_i \in \mathfrak{P}^{*\lambda}$. There exists an element γ with $(\gamma, \mathfrak{p}) = (1)$ such that $\gamma = \sum_{i=1}^{m} (c_i\gamma)p_i$ where $c_i\gamma \in \mathfrak{o}$. Therefore $\gamma \in \mathfrak{P}^*$, a contradiction. Therefore $\mathfrak{F}_{\mathfrak{p}} \neq \mathfrak{O}^*_{\mathfrak{p}}$, $\mathfrak{O}^*_{\mathfrak{p}} \supset \mathfrak{O}_{\mathfrak{p}}$ and so $\mathfrak{d}^*_{\mathfrak{p}} \supset \mathfrak{d}_{\mathfrak{p}}$.

Now suppose $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$ different from all the $\mathfrak{p}_i (i = 1, 2, \ldots, s)$. Using the same technique as above, one easily shows that $\mathfrak{F}_{\mathfrak{p}} = \mathfrak{O}^*_{\mathfrak{p}}$. Now $\mathfrak{F}_{\mathfrak{p}} \subseteq \mathfrak{O}_{\mathfrak{p}}$ and so $\mathfrak{O}_{\mathfrak{p}} = \mathfrak{O}^*_{\mathfrak{p}}$ for all such $\mathfrak{p}$. Therefore, if $\mathfrak{d}^*_{\mathfrak{p}} \supset \mathfrak{d}_{\mathfrak{p}}$, and so $\mathfrak{O}^*_{\mathfrak{p}} \supset \mathfrak{O}_{\mathfrak{p}}$ by theorem 9.1, then $\mathfrak{p}$ must be one of the $\mathfrak{p}_i$. This completes the proof.

CONCLUSION

In this study a preliminary investigation has been made into the ideal theory of non-maximal orders in algebras. The principal aim has been to collect and expand the known results and to develop methods for further investigations.

The main results of Part I are the theorem on the existence and uniqueness of block ideal decompositions and the two criteria for prime ideals to belong to the same block. Of crucial importance in Part II is the theorem stating that the block ideal components of ideals generated by non-zero integral ideals in the ground field generate a multiplicative abelian group. In particular, this permits a new development of the classical theory for maximal orders. It is shown that if A is a simple algebra over a field K with a discrete non-trivial valuation, then a maximal order of A has a unique prime ideal of which every other non-zero ideal is a power. In studying the ideal theory of an order imbedded in a maximal order, it is natural to introduce the notion of conductor. A preliminary theorem has been obtained which relates the conductor to the discriminants of the two orders. It is likely that many further results can be obtained in this direction.

As remarked in the Introduction, one of the main applications of the theory is the study of the natural order

in the group algebra over an algebraic number field K. If $\mathfrak{p}$ is a prime ideal of K, then $\mathfrak{o}/\mathfrak{p}\mathfrak{o}$ can be regarded as an algebra over $\mathfrak{o}/\mathfrak{p}$ and as such is isomorphic to the group <u>algebra</u> over $GF(p^n) \cong \mathfrak{o}/\mathfrak{p}$. (Here, p is the rational prime in $\mathfrak{p}$.) The prime ideal divisors of $\mathfrak{p}\mathfrak{o}$ in $\mathfrak{o}$ determine the irreducible modular representations of the group and so it is natural to study such prime ideals. In particular, it would be desirable to establish a bound for the number of prime ideals in a given block. Preliminary results in this direction have been obtained by R. Brauer in (6) and it is conceivable that they are capable of refinement. In this same connection, it would appear desirable to develop a theory of one-sided ideals for arbitrary orders. Some work in this direction has already been done by Fitting (9). It is evident that these problems are of significance for arbitrary algebras, not necessarily group algebras.

REFERENCES

1. Albert, A. A. Structure of Algebras, Amer. Math. Soc. Colloquium Publications, 1939.

2. Artin, E. Zur Arithmetik hyperkomplexer Zahlen, Abh. Math. Sem. Univ. Hamburg 5(1927), 261-289.

3. Artin, E., Nesbitt, C. J., and Thrall, R.M. Rings with Minimum Condition, Michigan, 1946.

4. Brandt, H. Zur Idealtheorie Dedekindscher Algebren, Comm. Math. Helv. 2(1930), 13-17.

5. Brauer, R. On the Arithmetic in a Group Ring, Proc. Nat. Acad. Sci. 30(1944), 109-114.

6. -----. On Blocks of Characters of Groups of Finite Order II, Proc. Nat. Acad. Sci. 32(1946), 215-219.

7. Chevalley, C. L'Arithmétique dans les Algèbres de Matrices, Act. Sci. Ind. No. 323, Paris, 1936.

8. Deuring, M. Algebren, Ergebnisse der Math. 4, Berlin, 1935; New York, 1948.

9. Fitting, H. Primärkomponentenzerlegung in nichtkommutativen Ringen, Math. Ann. 111(1935), 19-41.

10. Hasse, H. Über $\mathfrak{p}$-adische Schiefkorper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Math. Ann. 104(1931), 495-543.

11. Jacobson, N. Theory of Rings, Amer. Math. Soc. Surveys II, 1943.

12. Krull, W. Idealtheorie, Ergebnisse der Math. 3, Berlin, 1935.

13. -----. Zur Theorie der zweiseitigen Ideale in nichtkommutativen Bereichen, Math. Zeit. 28(1928), 481-503.

14. McCoy, N. H. Prime Ideals in General Rings, Amer. J. Math. 71(1949), 823-833.

15. -----. Rings and Ideals, Carus Monographs No. 8, 1948.

16. Noether, E. Idealtheorie in Ringbereichen, Math. Ann. 83(1921), 24-66.

17. van der Waerden, B. L. Moderne Algebra, 2nd ed., Berlin, 1937, 1940.