W. E. JENNER

Block ideals and arithmetics of algebras

Compositio Mathematica, tome 11 (1953), p. 187-203

<http://www.numdam.org/item?id=CM_1953__11__187_0>

Block ideals and arithmetics of algebras

by

W. E. Jenner [1]

Most investigations on arithmetics of algebras up to the present time have been concerned only with maximal orders (cf. [1], [5], [6], [8]). In this case, the most agreeable sort of ideal theory obtains and the results have had fruitful applications to the theory of simple algebras and to class field theory (cf. [9]). One of the first writers to discuss non-maximal orders seems to have been H. Fitting [7]. Aside from its intrinsic interest, a study of the non-maximal case would be profitable in view of the connection between the arithmetic in a group ring and the theory of modular representations which has been elucidated by R. Brauer [4].

This paper lays no claim to originality and is intended only to give a systematic account of results that are more or less already known, although some are not in the literature. The paper is divided into two parts since a considerable portion of the ideal theory, that of part I, is applicable to rings of a broader category than orders.

The writer is indebted to Professor Richard Brauer, under whose direction this investigation was undertaken, for stimulating advice and for access to certain of his unpublished results.

Part I. Block Ideals

1. Direct intersections.

Throughout Part I it will be assumed that $\mathfrak{O}$ is a ring with unit element 1. The discussion is restricted to two-sided ideals of $\mathfrak{O}$ except where explicit mention is made to the contrary.

Ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *relatively prime* if $(\mathfrak{a}, \mathfrak{b}) = (1) = \mathfrak{O}$.

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

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

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

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

[1] This paper is based on the author's doctoral dissertation, University of Michigan, 1952.

These conditions will be indicated by writing $\mathfrak{a} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$.

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

The following results of this section are elementary but, for the sake of completeness, proofs are given, except for Theorem 1.1.1 the proof of which is trivial but rather tedious.

LEMMA 1.1.1: *If* $\mathfrak{a} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$ *and* $\mathfrak{b}_i = \dot{\bigcap}_{\sigma=1}^{s} \mathfrak{c}_{i\sigma}$, *then* $\mathfrak{a} = \dot{\bigcap}_{i,\sigma} \mathfrak{c}_{i\sigma}$.

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

LEMMA 1.1.2: *If* $(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{b}, \mathfrak{c}) = (1)$, *then* $(\mathfrak{a}\mathfrak{b}, \mathfrak{c}) = (\mathfrak{b}\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}, \mathfrak{c}) = (1)$.

PROOF: This follows on observing that $(\mathfrak{a}, \mathfrak{c}) \,.\, (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{b}, \mathfrak{c}) \,.\, (\mathfrak{a}, \mathfrak{c}) = (1)$ and $(\mathfrak{a}\mathfrak{b}, \mathfrak{b}\mathfrak{a}) \subseteqq \mathfrak{a} \cap \mathfrak{b}$.

LEMMA 1.1.3: *If* $\mathfrak{a} = \dot{\bigcap}_{i=1}^{s} \mathfrak{b}_i$ *and* $\mathfrak{b} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$, $\mathfrak{c} = \dot{\bigcap}_{i=r+1}^{s} \mathfrak{b}_i$ *where* $1 \leqq r < s$, *then* $\mathfrak{a} = \mathfrak{b} \,\dot{\cap}\, \mathfrak{c}$.

PROOF: This follows by induction from the previous lemma.

LEMMA 1.1.4: *If* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *are relatively prime in pairs, then* $\dot{\bigcap}_{i=1}^{r} \mathfrak{a}_i = \Sigma \mathfrak{a}_{\pi(1)}, \ldots \mathfrak{a}_{\pi(r)}$ *where* π *ranges over all permutations of* $1, 2, \ldots, r$.

PROOF: For $r = 2$, $\mathfrak{a}_1 \cap \mathfrak{a}_2 = (\mathfrak{a}_1 \cap \mathfrak{a}_2) \,.\, (\mathfrak{a}_1, \mathfrak{a}_2) \subseteqq (\mathfrak{a}_1\mathfrak{a}_2, \mathfrak{a}_2\mathfrak{a}_1) \subseteqq \mathfrak{a}_1 \cap \mathfrak{a}_2$ and so $\mathfrak{a}_1 \cap \mathfrak{a}_2 = (\mathfrak{a}_1\mathfrak{a}_2, \mathfrak{a}_2\mathfrak{a}_1)$. The lemma follows by induction.

THEOREM 1.1.1: *If* $\mathfrak{a} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$, *then* $\mathfrak{O}/\mathfrak{a} = \mathfrak{C}_1/\mathfrak{a} \dot{+} \ldots \dot{+} \mathfrak{C}_r/\mathfrak{a}$ *where* $\mathfrak{C}_i = \bigcap_{j \neq i} \mathfrak{b}_j$. *Conversely, if* $\mathfrak{O}/\mathfrak{a} = \mathfrak{C}_1/\mathfrak{a} \dot{+} \ldots \dot{+} \mathfrak{C}_r/\mathfrak{a}$, *then* $\mathfrak{a} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$ *where* $\mathfrak{b}_i = \sum_{j \neq i} \mathfrak{C}_j$. *Furthermore, these constructions are reciprocal.*

COROLLARY 1.1.1: *If* $\mathfrak{a} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$ *and* $\varrho_1, \ldots, \varrho_r$ *are arbitrary elements of* $\mathfrak{O}$, *then the system of congruences* $\xi \equiv \varrho_i \pmod{\mathfrak{b}_i}$ *where* $i = 1, 2, \ldots, r$, *has a solution in* $\mathfrak{O}$ *and the solution is unique* mod $\mathfrak{a}$.

COROLLARY 1.1.2: *If* $\mathfrak{a} = \dot{\bigcap}_{i=1}^{r} \mathfrak{b}_i$, *then the* $\mathfrak{b}_i$ *commute* mod $\mathfrak{a}$.

As remarked above, the proof of Theorem 1.1.1 will be omitted.

Lemma 1.1.5: *If* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ *and* $\mathfrak{m}$ *is any ideal, then either* $(\mathfrak{a}, \mathfrak{m}) = (1)$ *or* $(\mathfrak{a}, \mathfrak{m}) = \bigcap_{\sigma} (\mathfrak{b}_\sigma, \mathfrak{m})$ *where* σ *ranges over the set* S *of indices for which* $(\mathfrak{b}_\sigma, \mathfrak{m}) \neq (1)$.

Proof: Suppose $(\mathfrak{a}, \mathfrak{m}) \neq (1)$. Then by lemma 1.1.2, S is not empty. Clearly $(\mathfrak{a}, \mathfrak{m}) \subseteqq \bigcap_{\sigma} (\mathfrak{b}_\sigma, \mathfrak{m})$ where σ ranges over S. On the other hand, $\Sigma(\mathfrak{b}_{\pi(1)}, \mathfrak{m}) \ldots (\mathfrak{b}_{\pi(r)}, \mathfrak{m}) \subseteqq (\mathfrak{a}, \mathfrak{m})$ where π ranges over all permutations of $1, \ldots, r$ and the lemma follows from lemma 1.1.4.

Lemma 1.1.6: *If* $\mathfrak{b}_i \subseteqq \mathfrak{b}'_i$ *for* $i = 1, 2, \ldots, r$ *and* $\bigcap_{i=1}^{r} \mathfrak{b}_i$ *is direct, then* $\bigcap_{i=1}^{r} \mathfrak{b}_i \subset \bigcap_{i=1}^{r} \mathfrak{b}'_i$ *except when* $\mathfrak{b}_i = \mathfrak{b}'_i$ *for* $i = 1, 2, \ldots, r$.

Proof: If $\bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{i=1}^{r} \mathfrak{b}'_i$, then by lemma 1.1.5, $\mathfrak{b}_i = \bigcap_{\sigma} (\mathfrak{b}'_\sigma, \mathfrak{b}_i)$ where σ ranges over the set of indices for which $(\mathfrak{b}'_\sigma, \mathfrak{b}_i) \neq (1)$. Clearly $\sigma = i$ is the only possibility and so $\mathfrak{b}_i = \mathfrak{b}'_i$ for $i = 1, 2, \ldots, r$.

Lemma 1.1.7: *If* $(\mathfrak{b}, \mathfrak{c}) = (1)$, $(\mathfrak{ac}, \mathfrak{m}) = (\mathfrak{ca}, \mathfrak{m})$ *and* $(\mathfrak{ab}, \mathfrak{m}) = (\mathfrak{ba}, \mathfrak{m})$, *then* $(\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}), \mathfrak{m}) = ((\mathfrak{b} \cap \mathfrak{c})\mathfrak{a}, \mathfrak{m})$.

Proof: It suffices to consider the case $\mathfrak{m} = (0)$. Then $\mathfrak{b} \cap \mathfrak{c} = (\mathfrak{bc}, \mathfrak{cb})$ by lemma 1.1.4 and $\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{a}(\mathfrak{bc}, \mathfrak{cb}) = (\mathfrak{abc}, \mathfrak{acb}) = (\mathfrak{bca}, \mathfrak{cba}) = (\mathfrak{b} \cap \mathfrak{c})\mathfrak{a}$.

Lemma 1.1.8: *If* $(\mathfrak{a}, \mathfrak{b}) = (1)$ *and* $(\mathfrak{ab}, \mathfrak{m}) = (\mathfrak{ba}, \mathfrak{m})$, *then for any ideals* $\mathfrak{A} \supseteqq \mathfrak{a}$ *and* $\mathfrak{B} \supseteqq \mathfrak{b}$, $(\mathfrak{AB}, \mathfrak{m}) = (\mathfrak{BA}, \mathfrak{m})$.

Proof: It is sufficient to consider the case $\mathfrak{m} = (0)$ and to show that if $(\mathfrak{a}, \mathfrak{b}) = (1)$, $\mathfrak{ab} = \mathfrak{ba}$ and $\mathfrak{a} \subseteqq \mathfrak{A}$, then $\mathfrak{Ab} = \mathfrak{bA}$. If $\gamma \in \mathfrak{A}$, then there exist elements $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\gamma = \alpha + \beta$. Now $\beta = \gamma - \alpha \in \mathfrak{b} \cap \mathfrak{A}$ and so $\gamma \in \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{A})$. Therefore $\mathfrak{A} = \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{A})$. Now $(\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} = (\mathfrak{a}, \mathfrak{b}) \,.\, (\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} = \mathfrak{a}(\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} + \mathfrak{b}(\mathfrak{b} \cap \mathfrak{A})\mathfrak{b} \subseteqq \mathfrak{ab} + \mathfrak{bA} \subseteqq \mathfrak{bA}$ and so $\mathfrak{Ab} \subseteqq \mathfrak{bA}$. Similarly $\mathfrak{bA} \subseteqq \mathfrak{Ab}$ and the lemma follows.

2. Block Ideal Decompositions.

From theorem 1.1.1, it follows that an ideal $\mathfrak{a}$ is a block ideal if and only if $\mathfrak{O}/\mathfrak{a}$ is indecomposable (in the sense of direct sum). 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. Furthermore, if the minimum condition holds for left (right) ideals which contain a given two-sided ideal $\mathfrak{a}$ of $\mathfrak{O}$, then the maximum condition holds for two-sided ideals containing $\mathfrak{a}$, provided $\mathfrak{O}$ contains a unit element. These statements, together with theorem 1.1.1, imply

THEOREM 1.2.1: *Let* $\mathfrak{a}$ *be an ideal of* $\mathfrak{O}$ *such that either* (i) *the maximum condition holds for ideals containing* $\mathfrak{a}$ *or* (ii) *the minimum condition holds for left (right) ideals containing* $\mathfrak{a}$. *Then* $\mathfrak{a}$ *has a unique expression as a direct intersection of block ideals.*

LEMMA 1.2.1: *If* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ *and* $\mathfrak{m}$ *is a block ideal containing* $\mathfrak{a}$, *then* $\mathfrak{m}$ *contains exactly one of the* $\mathfrak{b}_i$.

PROOF: By lemma 1.1.5, $\mathfrak{m} = (\mathfrak{a}, \mathfrak{m}) = \bigcap_{\sigma} (\mathfrak{b}_\sigma, \mathfrak{m})$ where σ ranges over the 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 $(\mathfrak{b}_\sigma, \mathfrak{m}) \neq (1)$. Then $\mathfrak{m} = (\mathfrak{b}_\sigma, \mathfrak{m})$ and hence $\mathfrak{b}_\sigma \subseteqq \mathfrak{m}$. On the other hand, no $\mathfrak{b}_j$ for $j \neq \sigma$ is contained in $\mathfrak{m}$ since $\mathfrak{m} \neq (1)$.

LEMMA 1.2.2: *If* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{\sigma=1}^{s} \mathfrak{c}_\sigma$ *where the* $\mathfrak{c}_\sigma$ *are block ideals, then each* $\mathfrak{b}_i$ *is contained in at least one* $\mathfrak{c}_\sigma$ *and each* $\mathfrak{b}_i$ *is the intersection of the* $\mathfrak{c}_\sigma$ *containing it.*

PROOF: By lemma 1.2.1, each $\mathfrak{c}_\sigma$ contains exactly one $\mathfrak{b}_i$. If some particular $\mathfrak{b}_i$ is relatively prime to all $\mathfrak{c}_\sigma$ then $(\mathfrak{b}_i, \mathfrak{a}) = (1)$ by lemma 1.1.2, a contradiction. Therefore there exists some σ for which $(\mathfrak{b}_i, \mathfrak{c}_\sigma) \neq (1)$. Now each $\mathfrak{c}_\sigma$ 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 $\mathfrak{c}_\sigma$. Now let $\mathfrak{b}_i \subseteqq \bigcap_{\varrho(i)} \mathfrak{c}_{\varrho(i)}$ where $\varrho(i)$ ranges over the set of indices ϱ for which $\mathfrak{b}_i \subseteqq \mathfrak{c}_\varrho$. Now $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i \subseteqq \bigcap_{i=1}^{r} \left[\bigcap_{\varrho(i)} \mathfrak{c}_{\varrho(i)} \right] = \mathfrak{a}$ and so by lemma 1.1.6, $\mathfrak{b}_i = \bigcap_{\varrho(i)} \mathfrak{c}_{\varrho(i)}$.

REMARK: Lemma 1.2.2 can be used to give another proof of the uniqueness of block ideal decompositions.

LEMMA 1.2.3: *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are block ideals and the maximum condition holds for ideals containing* $\mathfrak{a} \cap \mathfrak{b}$, *then either* $\mathfrak{a} \cap \mathfrak{b}$ *is direct or* $\mathfrak{a} \cap \mathfrak{b}$ *is a block ideal,*

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 lemma 1.1.3 one may assume $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{c}_1 \cap \mathfrak{c}_2$. By lemma 1.2.2, $\mathfrak{c}_1 \subseteqq \mathfrak{a}$, say, and $\mathfrak{c}_2 \subseteqq \mathfrak{b}$. By lemma 1.1.6, $\mathfrak{a} = \mathfrak{c}_1$ and $\mathfrak{b} = \mathfrak{c}_2$ and so the intersection $\mathfrak{a} \cap \mathfrak{b}$ is direct.

Theorem 1.2.2: *If* $\mathfrak{a} = \bigcap_{\sigma=1}^{s} \mathfrak{c}_\sigma$ *where the maximum condition holds for ideals containing* $\mathfrak{a}$, *and where the* $\mathfrak{c}_\sigma$ *are block ideals, then the representation of* $\mathfrak{a}$ *as a direct intersection of block ideals can be obtained by distributing the* $\mathfrak{c}_\sigma$ *into minimal systems* $S_1, S_2, \ldots, S_r$ *such that every* $\mathfrak{c}_\sigma \in S_i$ *is relatively prime to every* $\mathfrak{c}_\tau \in S_j$ *for* $i \neq j$. *If* $\mathfrak{b}_i$ *is the intersection of the* $\mathfrak{c}_\sigma$ *in* S_i, *then* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$.

Proof: Suppose S_1 consists of the elements $\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_m$. Now $\mathfrak{c}_1$ cannot be relatively prime to all of $\mathfrak{c}_2, \ldots, \mathfrak{c}_m$ in view of the minimal property of S_1. If $(\mathfrak{c}_1, \mathfrak{c}_2) \neq (1)$, say, then by lemma 1.2.3, $\mathfrak{c}'_2 = \mathfrak{c}_1 \cap \mathfrak{c}_2$ is a block ideal and by virtue of lemma 1.1.2, S_1 may be replaced by $S'_1 = \{\mathfrak{c}'_2, \mathfrak{c}_3, \ldots, \mathfrak{c}_m\}$. It is easily seen that S'_1 has the required minimal property and that repetition of this process will lead to the desired result.

Theorem 1.2.3: *If* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ *where the* $\mathfrak{b}_i$ *are block ideals, then any representation of* $\mathfrak{a}$ *as a direct intersection of ideals* $\mathfrak{c}_1, \ldots, \mathfrak{c}_s$ *is obtained by distributing the* $\mathfrak{b}_i$ *into disjoint subsystems* $T_1, T_2, \ldots, T_s$ *and taking for* $\mathfrak{c}_\sigma$ *the intersection of the* $\mathfrak{b}_i$ *in* T_σ.

The proof follows by an elementary argument from lemmas 1.1.3 and 1.2.2.

3. Prime Ideals.

Throughout this section it will be assumed that $\mathfrak{a}$ is an arbitrary but fixed ideal of $\mathfrak{O}$ and that the minimum condition holds for left (right) ideals of $\mathfrak{O}/\mathfrak{a}$. In non-commutative ideal theory an ideal $\mathfrak{p}$ is said to be *prime* if whenever $\mathfrak{b}\mathfrak{c} \subseteqq \mathfrak{p}$ for any two ideals $\mathfrak{b}$ and $\mathfrak{c}$, then either $\mathfrak{b} \subseteqq \mathfrak{p}$ or $\mathfrak{c} \subseteqq \mathfrak{p}$. It is easily shown, using the Wedderburn-Artin structure theorems, that an ideal $\mathfrak{p} \supseteqq \mathfrak{a}$ is prime if and only if it is maximal (cf. [6]). The *radical* $\mathfrak{n}$ of $\mathfrak{a}$ is the ideal $\mathfrak{n}$ of $\mathfrak{O}$ such that $\mathfrak{n}/\mathfrak{a}$ is the radical, in the Wedderburn-Artin sense, of $\mathfrak{O}/\mathfrak{a}$.

Theorem 1.3.1: *If* $\mathfrak{n}$ *is the radical of* $\mathfrak{a}$, *then* $\mathfrak{O}/\mathfrak{n} = \mathfrak{O}_1/\mathfrak{n} \dotplus \ldots \dotplus \mathfrak{O}_s/\mathfrak{n}$ *where the* $\mathfrak{O}_i/\mathfrak{n}$ *are simple two-sided ideals. There are exactly* s *prime ideal divisors of* $\mathfrak{a}$. *If* $s > 1$, *they are* $\mathfrak{p}_i = \sum_{j \neq i} \mathfrak{O}_j$ *and* $\mathfrak{n} = \bigcap_{i=1}^{s} \mathfrak{p}_i$. *If* $s = 1$, *then* $\mathfrak{n}$ *is the only prime ideal divisor of* $\mathfrak{a}$.

This is well known; it follows easily from the Wedderburn-Artin structure theorems.

Let $\mathfrak{a} = \bigcap_{j=1}^{r} \mathfrak{b}_j$ be the representation of $\mathfrak{a}$ as a direct intersection of block ideals. The s prime ideal divisors $\mathfrak{p}_i$ of $\mathfrak{a}$ are distributed into *r blocks* B_j, the block B_j consisting of the set of all $\mathfrak{p}_i$ which divide a given $\mathfrak{b}_j$. One now proceeds to investigate the relations between the block ideal components and the prime ideal divisors of a given ideal.

If the unit element $\underline{1}$ of $\mathfrak{O}/\mathfrak{a}$ is expressed as a sum of primitive idempotents, $\underline{1} = \underline{\varepsilon}_1 + \dots + \underline{\varepsilon}_k$, then there exist elements $\varepsilon_1, \dots, \varepsilon_k$ in $\mathfrak{O}$ with ε_i in the residue class $\underline{\varepsilon}_i$ such that $1 = \varepsilon_1 + \dots + \varepsilon_k$ 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 expressed as a sum of two other elements with these properties. The left ideal $\mathfrak{O}\varepsilon_i$ is primitive mod $\mathfrak{a}$ in the sense that if $\mathfrak{b}$ is a left ideal such that $\mathfrak{a} \subseteqq \mathfrak{b} \subset \mathfrak{O}\varepsilon_i + \mathfrak{a}$, then $\mathfrak{b} \subseteqq \mathfrak{n}$ and so $\mathfrak{b}$ is nilpotent mod $\mathfrak{a}$ (cf. [2]).

Lemma 1.3.1: *Let $\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_n$ be a system of ideals such that*

(i) $$\mathfrak{c}_i \neq (1) \text{ for } i = 1, 2, \dots, n,$$

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

(iii) $$\mathfrak{a} \subseteqq \bigcap_{i=1}^{n} \mathfrak{c}_i \subseteqq \mathfrak{n}.$$

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

Proof: No $\mathfrak{c}_i$ contains all ε_ϱ since $\mathfrak{c}_i \neq (1)$. Suppose some ε_ϱ is in neither $\mathfrak{c}_i$ nor $\mathfrak{c}_j$ for some $i \neq j$. Then $\mathfrak{O}\varepsilon_\varrho = (\mathfrak{c}_i, \mathfrak{c}_j)\varepsilon_\varrho = (\mathfrak{c}_i\varepsilon_\varrho, \mathfrak{c}_j\varepsilon_\varrho) \subseteqq (\mathfrak{c}_i \cap \mathfrak{O}\varepsilon_\varrho, \mathfrak{c}_j \cap \mathfrak{O}\varepsilon_\varrho) \subseteqq \mathfrak{n}$, a contradiction. It follows that for $i \neq j$, ζ_i and ζ_j can have no summand ε_ϱ in common. It follows from condition (iii) that every ε_ϱ appears in some ζ_i. The last statement of the lemma is clear.

If $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ where the $\mathfrak{b}_i$ are block ideals, then there exist elements $\eta_1, \dots, \eta_r$ (the ζ_i for the case $\mathfrak{c}_i = \mathfrak{b}_i$) such that $1 = \eta_1 + \dots + \eta_r$, $\eta_i \equiv 1 \pmod{\mathfrak{b}_i}$, $\eta_i \equiv 0 \pmod{\mathfrak{b}_j}$ for $i \neq j$. Furthermore the η_i are orthogonal idempotents mod $\mathfrak{a}$ and they lie in the center of $\mathfrak{O}$ mod $\mathfrak{a}$. If $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are the prime ideal divisors of $\mathfrak{a}$, then there exist elements $\delta_1, \dots, \delta_k$ (the ζ_i for $\mathfrak{c}_i = \mathfrak{p}_i$) such that $1 = \delta_1 + \dots + \delta_k$, $\delta_i \equiv 1 \pmod{\mathfrak{p}_i}$, $\delta_i \equiv 0 \pmod{\mathfrak{p}_j}$ for $i \neq j$ and the δ_i are orthogonal idempotents mod $\mathfrak{a}$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals in the block B_i. If $\varepsilon_\varrho \in \bigcap_{j=1}^{s} \mathfrak{p}_j$, then ε_ϱ is in the radical of $\mathfrak{b}_i$ so that $\varepsilon_\varrho^\lambda \in \mathfrak{b}_i$ for some $\lambda > 0$. But $\varepsilon_\varrho^\lambda - \varepsilon_\varrho \in \mathfrak{a} \subseteqq \mathfrak{b}_i$ and so $\varepsilon_\varrho \in \mathfrak{b}_i$. Therefore, if ε_ϱ occurs as a summand in η_i, it does likewise in some δ_j corresponding to one of $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. The converse is trivial and so

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

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 of $\mathfrak{O}$ mod $\mathfrak{a}$, it follows that

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

Two prime ideals $\mathfrak{p}_\varrho \supseteqq \mathfrak{a}$ and $\mathfrak{p}_\sigma \supseteqq \mathfrak{a}$ are said to be *connected directly* if either $\delta_\varrho\mathfrak{O}\delta_\sigma$ or $\delta_\sigma\mathfrak{O}\delta_\varrho$ is not contained in $\mathfrak{a}$. They are said to be *connected* if either $\mathfrak{p}_\varrho = \mathfrak{p}_\sigma$ or a chain $\mathfrak{p}_\varrho, \ldots, \mathfrak{p}_\nu, \ldots, \mathfrak{p}_\sigma$ of prime ideals $\mathfrak{p}_\nu \supseteqq \mathfrak{a}$ can be found such that any two adjacent elements in the chain are connected directly.

THEOREM 1.3.2: *Two prime ideal divisors of $\mathfrak{a}$ belong to the same block if and only if they are connected.*

PROOF: Suppose the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ divide $\mathfrak{a}$ and are connected. By lemma 1.2.1, each $\mathfrak{p}_j$ divides some $\mathfrak{b}_i$, so suppose $\mathfrak{b}_1 \subseteqq \mathfrak{p}_1$, $\mathfrak{b}_2 \subseteqq \mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are connected directly, say $\delta_1\mathfrak{O}\delta_2$ is not in $\mathfrak{a}$. By relation (2) above, $\eta_1\mathfrak{O}\eta_2$ is not in $\mathfrak{a}$. But $\eta_i \in \mathfrak{b}_j$ for $i \neq j$ and so $\eta_1\mathfrak{O}\eta_2 \subseteqq \mathfrak{a}$, a contradiction. This shows that $\mathfrak{p}_1. \ldots, \mathfrak{p}_s$ all belong to the same block.

Now let $\mathfrak{p}_1. \ldots, \mathfrak{p}_s$ be the prime ideals in B_1. Suppose these $\mathfrak{p}_i$ are not connected, say $\delta_i\mathfrak{O}\delta_j + \delta_j\mathfrak{O}\delta_i \subseteqq \mathfrak{a}$ for $i = 1, 2, \ldots, t$; $j = t + 1, \ldots, s$; $t < s$. Then $\gamma_1\mathfrak{O}\gamma_2 + \gamma_2\mathfrak{O}\gamma_1 \subseteqq \mathfrak{a}$ where $\gamma_1 = \delta_1 + \ldots + \delta_t$, $\gamma_2 = \delta_{t+1} + \ldots + \delta_s$. Set $\mathfrak{q}_i = \mathfrak{b}_1 + \gamma_i\mathfrak{O}\gamma_i$ for $i = 1, 2$. If $\delta_s \in \mathfrak{q}_1$, then $\delta_s \in \mathfrak{b}_1\delta_s + \gamma_1\mathfrak{O}\gamma_1\delta_s + \mathfrak{a} \subseteqq \mathfrak{b}_1$ since $\gamma_1\delta_s \in \mathfrak{a} \subseteqq \mathfrak{b}_1$. Therefore $\mathfrak{q}_1 \neq \mathfrak{O}$. Similarly $\mathfrak{q}_2 \neq \mathfrak{O}$. The sum of those ε_ϱ which are in $\mathfrak{b}_1$ is $\gamma_3 = 1 - \eta_1$. Now $\mathfrak{q}_1\mathfrak{O} = (\mathfrak{b}_1 + \gamma_1\mathfrak{O}\gamma_1)\mathfrak{O}(\gamma_1 + \gamma_2 + \gamma_3) \subseteqq \mathfrak{b}_1 + \gamma_1\mathfrak{O}\gamma_1 = \mathfrak{q}_1$ since $\gamma_1\mathfrak{O}\gamma_2 \subseteqq \mathfrak{a} \subseteqq \mathfrak{b}_1$ and $\gamma_3 \in \mathfrak{b}_1$. Similarly $\mathfrak{O}\mathfrak{q}_1 \subseteqq \mathfrak{q}_1$ and $\mathfrak{O}\mathfrak{q}_2\mathfrak{O} \subseteqq \mathfrak{q}_2$. Now $1 = \gamma_1 + \gamma_2 + \gamma_3$ with $\gamma_3 \in \mathfrak{b}_1$ and so $(\mathfrak{q}_1, \mathfrak{q}_2) = (1)$. By lemma 1.1.4, $\mathfrak{q}_1 \cap \mathfrak{q}_2 = (\mathfrak{q}_1\mathfrak{q}_2, \mathfrak{q}_2\mathfrak{q}_1) \subseteqq \mathfrak{b}_1 \subseteqq \mathfrak{q}_1 \cap \mathfrak{q}_2$ and so $\mathfrak{b}_1 = \mathfrak{q}_1 \cap \mathfrak{q}_2$, a contradiction. It follows that the prime ideals in B_1 are connected. The same argument works, of course, for any B_i and so the theorem follows.

Two prime ideals $\mathfrak{p}_\varrho \supseteqq \mathfrak{a}$ and $\mathfrak{p}_\sigma \supseteqq \mathfrak{a}$ are said to be *related* if either they are equal or a chain $\mathfrak{p}_\varrho, \ldots, \mathfrak{p}_\nu, \ldots, \mathfrak{p}_\sigma$ of prime ideals $\mathfrak{p}_\nu \supseteqq \mathfrak{a}$ can be found such that no two adjacent elements of the chain commute mod $\mathfrak{a}$.

Theorem 1.3.3: *Two prime ideal divisors of* $\mathfrak{a}$ *belong to the same block if and only if they are related.*

Proof: It follows from lemma 1.1.8 and corollary 1.1.2 that two related prime ideals belong to the same block. Now let $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ where the $\mathfrak{b}_i$ are block ideals and let $\mathfrak{n} = \bigcap_{j=1}^{s} \mathfrak{p}_j$ be the radical of $\mathfrak{a}$. Let S be the set consisting of the $\mathfrak{p}_j$ 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. [7]). The set of all $\mathfrak{p}_j$ in a given S_i all divide the same block ideal and so $k \geqq r$. Let $\mathfrak{b}$ denote any fixed one of the $\mathfrak{b}_\varrho$. Let $\mathfrak{M}_i$ be the intersection of all $\mathfrak{p}_j \in S_i$ such that $\mathfrak{b} \subseteqq \mathfrak{p}_j$. It is possible that $\mathfrak{M}_i$ is 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; $t \leqq k$. Then $\mathfrak{N} = \bigcap_{i=1}^{t} \mathfrak{M}_i$ is the radical of $\mathfrak{b}$. It follows from lemma 1.1.7 that the $\mathfrak{M}_i$ commute mod $\mathfrak{a}$. Then by lemma 1.1.4, $\mathfrak{N} = \mathfrak{b} + \mathfrak{M}_1 \ldots \mathfrak{M}_t$. There exists an integer $\sigma > 0$ such that $\mathfrak{N}^\sigma \subseteqq \mathfrak{b}$. The $\mathfrak{M}_i$ commute mod $\mathfrak{b}$ and so $\mathfrak{M}_1^\sigma \ldots \mathfrak{M}_t^\sigma \subseteqq \mathfrak{b}$. Set $\mathfrak{B}_i = \mathfrak{M}_i^\sigma + \mathfrak{b}$. By lemma 1.1.2, $(\mathfrak{M}_i^\sigma, \mathfrak{M}_j^\sigma) = (1)$ for $i \neq j$ and so $(\mathfrak{B}_i, \mathfrak{B}_j) = (1)$ for $i \neq j$. Now $\mathfrak{b} \subseteqq \bigcap_{i=1}^{t} \mathfrak{B}_i \subseteqq \mathfrak{M}_1^\varrho \ldots \mathfrak{M}_t^\varrho + \mathfrak{b} \subseteqq \mathfrak{b}$ by lemma 1.1.4 and so $\mathfrak{b} = \bigcap_{i=1}^{t} \mathfrak{B}_i$. This is impossible for $t > 1$ and so all prime ideal divisors of $\mathfrak{b}$ are related.

Theorem 1.3.4: *Let* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ *be the block ideal decomposition of* $\mathfrak{a}$; *let* $\mathfrak{n} = \bigcap_{j=1}^{s} \mathfrak{p}_j$ *be the radical of* $\mathfrak{a}$ *with exponent* σ; $\mathfrak{n}^\sigma \subseteqq \mathfrak{a}$. *Let* $\mathfrak{M}_i$ *be the intersection of the prime ideals in* B_i. *Then the* $\mathfrak{M}_i$ *commute* mod $\mathfrak{a}$ *and* $\mathfrak{b}_i = \mathfrak{M}_i^\sigma + \mathfrak{a}$. *Furthermore* $\mathfrak{b}_i = \mathfrak{M}_i^\sigma + \mathfrak{a} = \mathfrak{M}_i^{\sigma+\lambda} + \mathfrak{a}$ *for any positive integer* λ.

Proof: It follows from lemma 1.1.8 and corollary 1.1.2 that the $\mathfrak{M}_i$ commute mod $\mathfrak{a}$. Consequently $\mathfrak{M}_i^\sigma \ldots \mathfrak{M}_r^\sigma \subseteqq \mathfrak{a}$ and $\mathfrak{a} = \bigcap_{i=1}^{r} (\mathfrak{M}_i^\sigma + \mathfrak{a}) = \bigcap_{i=1}^{r} (\mathfrak{M}_i^{\sigma+\lambda} + \mathfrak{a}) = \bigcap_{i=1}^{r} \mathfrak{b}_i$. The theorem then follows from lemma 1.1.6.

Corollary 1.3.1: *Let* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ *be the block ideal decomposition of* $\mathfrak{a}$. *Assume that all prime ideal divisors* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ *of* $\mathfrak{a}$ *commute* mod $\mathfrak{a}$. *Then each block contains only one prime ideal,* $r = s$, *and for suitable indexing,* $\mathfrak{b}_i = \mathfrak{p}_i^\sigma + \mathfrak{a}$ *for* $i = 1, 2, \ldots, r$ *where* σ *is the exponent of the radical of* $\mathfrak{a}$. *For each* $\mathfrak{b}_i$, σ *may be replaced by any larger integer.*

COROLLARY 1.3.2: *Let* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i$ *be the block ideal decomposition of* $\mathfrak{a}$. *Assume that all prime ideal divisors of* $\mathfrak{a}$ *commute in the ordinary sense, that is,* mod (0). *Then the* $\mathfrak{b}_i$ *commute,* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i = \prod_{i=1}^{r} \mathfrak{b}_i$ *and* $\mathfrak{b}_i = \mathfrak{p}_i^{\sigma} + \mathfrak{a}$ *as in corollary* 1.3.1.

The proof follows by a trivial argument from lemma 1.1.8 and corollary 1.3.1.

Part II. Arithmetics of Algebras

1. Orders and Ideals.

Let $\mathfrak{o}$ be a Dedekind ring with quotient field k and A an algebra of finite dimension n over k. It will be assumed that A has a unit element 1 coinciding with that of k.

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

Since an order is a finitely-generated module over a Noetherian ring, it follows that the ascending chain condition holds for submodules. Consequently there exist elements $\sigma_1, \ldots, \sigma_s \in \mathfrak{O}$, $s \geqq n$, such that $\mathfrak{O} = \mathfrak{o}\{\sigma_1, \ldots, \sigma_s\}$. There also exist elements $\eta_1, \ldots, \eta_n \in \mathfrak{O}$ and $c \neq 0$ in $\mathfrak{o}$ such that every element $\alpha \in \mathfrak{O}$ has a unique representation of the form $\alpha = c^{-1} \sum_{i=1}^{n} a_i \eta_i$ with $a_i \in \mathfrak{o}$. If $\mathfrak{o}$ is a principal ideal ring the η_i can be chosen with $c = 1$. Such a basis is called a minimal basis.

If $\nu \neq 0$ is an element in the radical N of A with $\nu^r = 0$ for some $r > 0$, then the $\mathfrak{o}$-module generated by the products $\sigma_{i(1)}\nu^{t(1)} \cdot \ldots \cdot \sigma_{i(s)}\nu^{t)s)}$ with $\Sigma_{i=1}^{s} t(i) < r$ is easily seen to be an order containing $\mathfrak{O}$. If $N \neq (0)$, then there exists an element $\nu \in N$ with $\nu \notin \mathfrak{O}$. It follows that if an algebra possesses maximal orders then it is semisimple. If A is semisimple and separable, then every order can be imbedded in a maximal order (cf. [6]).

DEFINITION, *An additive subgroup* $\mathfrak{A}$ *of* A *is called an ideal if* $(\mathfrak{O}\mathfrak{A}, \mathfrak{A}\mathfrak{O}) \subseteq \mathfrak{A}$, $\mathfrak{A} \cap k \neq (0)$ *and there exists an element* $a \neq 0$ *in* k *such that* $a\mathfrak{A} \subseteqq \mathfrak{O}$. *If* $\mathfrak{A} \subseteqq \mathfrak{O}$ *it is said to be integral*; *otherwise, fractional.*

By virtue of the ascending chain condition, every integral ideal of $\mathfrak{O}$ has a unique expression as a direct intersection of block ideals. If $\mathfrak{A}$ is integral and $a \in \mathfrak{a} = \mathfrak{A} \cap \mathfrak{o}$, than $a\mathfrak{O} \subseteqq \mathfrak{A}$ and so $\mathfrak{O}/\mathfrak{A}$ may be regarded as an $\mathfrak{o}/\mathfrak{a}$-module where the operators act in the canonical manner. The minimum condition for $\mathfrak{o}/\mathfrak{a}$ implies the minimum condition for $\mathfrak{o}$-modules $\mathfrak{U}$ such that $\mathfrak{A} \subseteqq \mathfrak{U} \subseteqq \mathfrak{O}$ (cf. [10], p. 32). It follows that all results in part I apply to integral ideals in orders.

2. Ideals generated by Ideals of $\mathfrak{o}$.

The main purpose of this section is to show that the block ideal components of ideals of the form $\mathfrak{a}\mathfrak{O}$, where $\mathfrak{a}$ is a non-zero integral $\mathfrak{o}$-ideal, generate a multiplicative abelian group.

For a fixed prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ let $\tilde{\mathfrak{o}}$ denote the ring of $\mathfrak{p}$-integers, that is, the set of elements of the form ab^{-1} where $a, b \in \mathfrak{o}$ and $(b, \mathfrak{p}) = (1)$. If $\mathfrak{M}$ is an $\mathfrak{O}$-ideal, set $\tilde{\mathfrak{M}} = \tilde{\mathfrak{o}}\mathfrak{M}$.

Lemma 2.2.1: *If $\mathfrak{M}$ is an integral $\mathfrak{O}$-ideal such that $\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o}$ is a power of $\mathfrak{p}$, then $\mathfrak{O}/\mathfrak{M} \simeq \tilde{\mathfrak{O}}/\tilde{\mathfrak{M}}$ where the isomorphism is canonical, being induced by the injection map of $\mathfrak{O}$ into $\tilde{\mathfrak{O}}$.*

Proof: If $\alpha \in \tilde{\mathfrak{O}}$, let d be an element of $\mathfrak{o}$ with $(1) = (d, \mathfrak{p}) = (d, \mathfrak{m})$ such that $d\alpha \in \mathfrak{O}$. Then $\alpha \in (d\alpha, \mathfrak{m}\alpha) \subseteqq \mathfrak{O} + \tilde{\mathfrak{M}}$. It follows that $\tilde{\mathfrak{O}} = \mathfrak{O} + \tilde{\mathfrak{M}}$. If $\beta \in \tilde{\mathfrak{M}} \cap \mathfrak{O}$, let h be an element of $\mathfrak{o}$ with $(1) = (h, \mathfrak{p}) = (h, \mathfrak{m})$ such that $h\beta \in \mathfrak{M}$. Now $\beta \in (h\beta, \mathfrak{m}\beta) \subseteqq \mathfrak{M}$ and so $\tilde{\mathfrak{M}} \cap \mathfrak{O} = \mathfrak{M}$. Then $\tilde{\mathfrak{O}}/\tilde{\mathfrak{M}} = (\mathfrak{O} + \tilde{\mathfrak{M}})/\tilde{\mathfrak{M}} \simeq \mathfrak{O}/\tilde{\mathfrak{M}} \cap \mathfrak{O} = \mathfrak{O}/\mathfrak{M}$ where the isomorphism is canonical.

Lemma 2.2.2: *Let $\mathfrak{N}$ range over the set of integral $\mathfrak{O}$-ideals for which $\mathfrak{N} \cap \mathfrak{o}$ either equals $\mathfrak{o}$ or is a power of $\mathfrak{p}$. Then ψ: $\mathfrak{N} \to \tilde{\mathfrak{N}}$ is a one-to-one mapping onto the set of all integral $\tilde{\mathfrak{O}}$-ideals. Furthermore, ψ is an isomorphism with respect to sum, product and intersection.*

Proof: It is trivial that ψ is a homomorphism with respect to sum and product. If $\alpha \in \tilde{\mathfrak{N}}_1 \cap \tilde{\mathfrak{N}}_2$, then there exists an element $d \in \mathfrak{o}$ with $(d, \mathfrak{p}) = (1)$ such that $d\alpha \in \mathfrak{N}_1 \cap \mathfrak{N}_2$. It follows that ψ is a homomorphism with respect to intersection. If $\mathfrak{N}_1 \to \tilde{\mathfrak{N}}$ and $\mathfrak{N}_2 \to \tilde{\mathfrak{N}}$, then $\mathfrak{N}_1 + \mathfrak{N}_2 \to \tilde{\mathfrak{N}}$ and so one may assume $\mathfrak{N}_1 \subseteqq \mathfrak{N}_2$. By lemma 2.2.1, $\mathfrak{O}/\mathfrak{N}_1 \simeq \tilde{\mathfrak{O}}/\tilde{\mathfrak{N}} \simeq \mathfrak{O}/\mathfrak{N}_2$ where the isomorphisms are canonical and so $\mathfrak{N}_1 = \mathfrak{N}_2$. Consequently ψ is an isomorphism. Now let $\mathfrak{T}$ be any integral $\tilde{\mathfrak{O}}$-ideal. It is easily seen that $\mathfrak{T} = \tilde{\mathfrak{M}}$ where $\mathfrak{M} = \mathfrak{T} \cap \mathfrak{O}$. If $\mathfrak{M} \cap \mathfrak{o}$ is a power of $\mathfrak{p}$, then $\mathfrak{M}$ is in the domain of definition of ψ. If $\mathfrak{M} \cap \mathfrak{o}$ is prime to $\mathfrak{p}$, then it is easily seen that $\tilde{\mathfrak{M}} = \tilde{\mathfrak{D}}$ and $\mathfrak{M}$, insofar as its behavior under ψ is concerned, can be replaced by $\mathfrak{D}$ which is in the domain of definition of ψ. Now assume that neither of these extreme cases holds and that $\mathfrak{M} = \bigcap_{i=1}^{r} \mathfrak{B}_i$ where the $\mathfrak{B}_i$ are block ideals. It is easily seen, using lemma 1.2.1, that the $\mathfrak{B}_i \cap \mathfrak{o}$ are block ideals of $\mathfrak{o}$. Let $\mathfrak{N}$ be the intersection of those $\mathfrak{B}_i$ such that $\mathfrak{B}_i \cap \mathfrak{o}$ is a power of $\mathfrak{p}$. Let $\mathfrak{Q}$ be the intersection of the remaining $\mathfrak{B}_i$. By lemma 1.1.3, $\mathfrak{M} = \mathfrak{N} \cap \mathfrak{Q}$. Now $\tilde{\mathfrak{Q}} = \tilde{\mathfrak{D}}$ and since ψ is a homomorphism with respect to intersection, it follows that $\tilde{\mathfrak{M}} = \tilde{\mathfrak{N}}$. This shows that the set of images under ψ coincides with the set of all integral $\tilde{\mathfrak{D}}$-ideals.

LEMMA 2.2.3: *Let* $\mathfrak{a}\mathfrak{D} = \bigcap_{i=1}^{r} \mathfrak{B}_i$ *where* $\mathfrak{a}$ *is an integral* $\mathfrak{o}$*-ideal. Then* $\mathfrak{a}^{\lambda}\mathfrak{D} = \bigcap_{i=1}^{r} \mathfrak{B}_i^{\lambda}$ *where* λ *is any positive integer.*

PROOF: The lemma is trivial for $\lambda = 1$. Now assume $\mathfrak{a}^{\sigma-1}\mathfrak{D} = \bigcap_{i=1}^{r} \mathfrak{B}^{\sigma-1}$. By lemma 1.1.4, $\bigcap_{i=1}^{r} \mathfrak{B}_i^{\sigma} = \Sigma \mathfrak{B}_{\pi(1)}^{\sigma} \ldots \mathfrak{B}_{\pi(r)}^{\sigma}$ where π ranges over all permutations of the indices $1, 2, \ldots, r$. Since, by corollary 1.1.2, the $\mathfrak{B}_i$ commute mod $\mathfrak{a}\mathfrak{D}$, it can easily be verified that $\Sigma \mathfrak{B}_{\pi(1)}^{\sigma} \ldots \mathfrak{B}_{\pi(r)}^{\sigma} \subseteqq \Sigma \mathfrak{B}_{\pi(1)}^{\sigma-1} \ldots \mathfrak{B}_{\pi(r)}^{\sigma-1} (\mathfrak{B}_1 \ldots \mathfrak{B}_r) + \mathfrak{a}^{\sigma}\mathfrak{D}$. This implies that $\bigcap_{i=1}^{r} \mathfrak{B}_i^{\sigma} \subseteqq \mathfrak{a}^{\sigma}\mathfrak{D}$ and the lemma follows immediately.

LEMMA 2.2.4: *Let* $\eta_1, \ldots, \eta_n$ *be a minimal basis for* $\tilde{\mathfrak{D}}$ *and suppose the congruences* $\xi_\sigma \eta_i - \eta_i \xi_\sigma \equiv 0 \pmod{\mathfrak{p}^{\sigma}\tilde{\mathfrak{D}}}$ *have a solution* ξ_σ *for* $i = 1, 2, \ldots, n$ *and for each positive integer* σ. *Then there exists an element* $\zeta \in Z \cap \tilde{\mathfrak{D}}$, *where* Z *is the center of* A, *such that for* σ *sufficiently large,* $\zeta \equiv \xi_\sigma \pmod{\mathfrak{p}\tilde{\mathfrak{D}}}$.

PROOF: Suppose $\eta_i \eta_j = \sum_{k=1}^{n} c_{ijk} \eta_k$ and let $\xi_\sigma = \sum_{j=1}^{n} a_j \eta_j$. Then $\sum_{j=1}^{n} a_j (c_{ijk} - c_{jik}) \equiv 0 \pmod{\mathfrak{p}^{\sigma} \tilde{\mathfrak{o}}}$ for all i, k. Set $c_{ijk} - c_{jik} = b_{i+(k-1)n,\, j}$ and let π be the local prime of $\tilde{\mathfrak{o}}$. Then

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

where $i = 1, 2, \ldots, n^2$ and $y_i \in \tilde{\mathfrak{o}}$. By the theory of elementary divisors there exists a unimodular transformation which maps a_j into a'_j, say, for $j = 1, 2, \ldots, n$ and transforms the system (1) into the form:

$$\begin{array}{rcl} e_1 a'_1 & = & \pi^\sigma y'_1 \\ \vdots & & \vdots \\ e_r a'_r & = & \pi^\sigma y'_r \\ 0 \,.\, a'_{r+1} & = & \pi^\sigma y'_{r+1} \\ \vdots & & \vdots \\ 0 \,.\, a'_n & = & \pi^\sigma y'_n \\ 0 & = & \pi^\sigma y'_{n+1} \\ \vdots & & \vdots \\ 0 & = & \pi^\sigma y'_{n^2} \end{array} \tag{2}$$

where $e_i \neq 0$ for $i = 1, 2, \ldots, r$ and $y'_i \in \tilde{\mathfrak{o}}$. 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 $a_i = \sum_{j=1}^{r} d_{ij}a'_j + \sum_{j=r+1}^{n} d_{ij}a'_j$ for $i = 1, 2, \ldots, n$ with $d_{ij} \in \tilde{\mathfrak{o}}$. The element $\zeta = \sum_{i=1}^{n} \bar{a}_i \eta_i$ where $\bar{a}_i = \sum_{j=r+1}^{n} d_{ij}\, a'_j$ has the required property.

Now let $\mathfrak{p}\mathfrak{O} = \bigcap_{i=1}^{r} \mathfrak{B}_i$ where the $\mathfrak{B}_i$ are block ideals. By lemma 2.2.2, $\tilde{\mathfrak{p}}\tilde{\mathfrak{O}} = \bigcap_{i=1}^{r} \tilde{\mathfrak{B}}_i$ where the $\tilde{\mathfrak{B}}_i$ are block ideals. By lemma 2.2.3, $\tilde{\mathfrak{p}}^\sigma\tilde{\mathfrak{O}} = \bigcap_{i=1}^{r} \tilde{\mathfrak{B}}_i^\sigma$. By theorem 1.1.1, there exist elements $e'_1, \ldots, e'_r$ in $\tilde{\mathfrak{O}}$ such that $1 = e'_1 + \ldots + e'_r$ with $e'_i \equiv 0 \pmod{\tilde{\mathfrak{B}}_j^\sigma}$ for $i \neq j$ and $e'_i \equiv 1 \pmod{\tilde{\mathfrak{B}}_i^\sigma}$. It is easily verified that the e'_i are in the center Z mod $\mathfrak{p}^\sigma\tilde{\mathfrak{O}}$ and so, by taking σ sufficiently large and applying lemma 2.2.4, one can obtain elements $e_i \equiv e'_i \pmod{\mathfrak{p}\tilde{\mathfrak{O}}}$ with $e_i \in Z \cap \tilde{\mathfrak{O}}$. It follows from this result, together with lemmas 2.2.2 and 1.1.8, that the $\mathfrak{B}_i$ commute. The inverse of an ideal of $\mathfrak{B}_i$ is $\mathfrak{B}_i^{-1} = \mathfrak{p}^{-1} \prod_{j \neq i} \mathfrak{B}_j$. If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct prime ideals of $\mathfrak{o}$, then, by lemma 1.1.8, every block ideal component of $\mathfrak{p}_1\mathfrak{O}$ commutes with every block ideal component of $\mathfrak{p}_2\mathfrak{O}$. From these remarks one readily deduces

THEOREM 2.2.1: *The block ideal components of ideals $\mathfrak{a}\mathfrak{O}$, where $\mathfrak{a}$ is an integral ideal of $\mathfrak{o}$, generate an abelian group. The representation of an element of this group as a product of powers of distinct generators is unique.*

THEOREM 2.2.2: *If Z is the center of A, then $\mathfrak{Q} = Z \cap \mathfrak{O}$ is an order of Z. If $\mathfrak{p}\mathfrak{O} = \bigcap_{i=1}^{r} \mathfrak{B}_i$ where $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$ and the $\mathfrak{B}_i$*

are block ideals, then $\mathfrak{p}\mathfrak{O} = \bigcap_{i=1}^{r} \mathfrak{T}_i$ *where* $\mathfrak{T}_i = \mathfrak{B}_i \cap \mathfrak{O}$ *are block ideals of* $\mathfrak{O}$. *Furthermore,* $\mathfrak{B}_i = \mathfrak{T}_i\mathfrak{D}$.

Proof: It is trivial to verify that $\mathfrak{O}$ is an order of Z. From the remarks preceding theorem 2.2.1, it follows that the $\mathfrak{T}_i$ are relatively prime. It is easily seen using lemma 1.2.1, that the $\mathfrak{T}_i \cap \mathfrak{o}$ are block ideals of $\mathfrak{o}$ and that $\mathfrak{T}_i \cap \mathfrak{o} = \mathfrak{p}$. Now $\mathfrak{p}^{-1}(\mathfrak{p}\mathfrak{D} \cap \mathfrak{O}) \subseteqq \mathfrak{O}$ and so $\mathfrak{p}\mathfrak{D} \cap \mathfrak{O} = \mathfrak{p}\mathfrak{O}$. It follows that $\mathfrak{p}\mathfrak{O} = \bigcap_{i=1}^{r} \mathfrak{T}_i$. Now $\mathfrak{p}\mathfrak{D} = \bigcap_{i=1}^{r} \mathfrak{T}_i\mathfrak{D}$ and so $\mathfrak{B}_i = \mathfrak{T}_i\mathfrak{D}$ by lemma 1.1.6. If $\mathfrak{T}_i = \mathfrak{T}_i' \cap \mathfrak{T}_i''$ for some i, then $\mathfrak{B}_i = \mathfrak{T}_i'\mathfrak{T}_i''\mathfrak{D} = \mathfrak{T}_i'\mathfrak{D} \cap \mathfrak{T}_i''\mathfrak{D}$, a contradiction. The theorem follows immediately.

Theorem 2.2.3: *Let* $\mathfrak{A}$ *be an integral* $\mathfrak{D}$*-ideal and let* $(\mathfrak{A} \cap \mathfrak{o})\mathfrak{D} = \bigcap_{i=1}^{r} \mathfrak{B}_i$ *where the* $\mathfrak{B}_i$ *are block ideals. Then* $\mathfrak{A}$ *can be expressed uniquely as a product* $\mathfrak{A} = \mathfrak{A}_1 \ldots \mathfrak{A}_r$ *where* $\mathfrak{A}_i$ *divides* $\mathfrak{B}_i$, $\mathfrak{A}_i = (\mathfrak{A}, \mathfrak{B}_i)$ *and the* $\mathfrak{A}_i$ *commute.*

The proof follows easily from Theorem 2.2.1 and lemma 1.1.8.

3. Maximal Orders.

The results of the last section permit a development, different from those usually given, of the prime ideal decomposition theorem for maximal orders.

Lemma 2.3.1: *If a block of* $\mathfrak{p}\mathfrak{D}$, *where* $\mathfrak{p}$ *is a prime ideal of* $\mathfrak{o}$, *contains a completely regular prime ideal* $\mathfrak{P}$, *then the corresponding block ideal* $\mathfrak{B}$ *is a power of* $\mathfrak{P}$. *Furthermore, every ideal which divides a power of* $\mathfrak{P}$ *is itself a power of* $\mathfrak{P}$.

Proof: The ideal $\mathfrak{B}' = \mathfrak{P}^{-1}\mathfrak{B}$ is integral since $\mathfrak{P}$ divides $\mathfrak{B}$. If $\mathfrak{B} = \mathfrak{B}'$, then $\mathfrak{P}^{\lambda}\mathfrak{B} = \mathfrak{B}$ for every integer $\lambda > 0$, which is impossible by virtue of the ascending chain condition. A completely regular prime ideal commutes with all other prime ideals (cf. [6]) and so by corollary 1.3.1, $\mathfrak{B} = \mathfrak{P}^{\sigma} + \mathfrak{p}\mathfrak{D}$ for some $\sigma > 0$. If $\mathfrak{B} \subset \mathfrak{B}' \subseteqq \mathfrak{P}'$ for some prime ideal $\mathfrak{P}'$, then $\mathfrak{P} = \mathfrak{P}'$ and, proceeding by induction, it is easily shown that $\mathfrak{B} = \mathfrak{P}^{\mu}$ for some $\mu > 0$. Similarly, if $\mathfrak{P}^{\nu} \subseteqq \mathfrak{A}$ for some ideal $\mathfrak{A}$ with $\nu > 0$, then $\mathfrak{A} = \mathfrak{P}^{\lambda}$ for some $\lambda > 0$.

Theorem 2.3.1: *If* $\mathfrak{D}$ *is a maximal order, then every ideal can be expressed uniquely as a product of powers of distinct prime ideals. The ideals of* $\mathfrak{D}$ *form a multiplicative abelian group generated by the prime ideals.*

PROOF: In a maximal order, all prime ideals are completely regular (cf. [6]). Let $\mathfrak{A}$ be an integral $\mathfrak{O}$-ideal. Then $(\mathfrak{A} \cap \mathfrak{o})\mathfrak{O} = = \mathfrak{P}_1^{\mu_1} \ldots \mathfrak{P}_s^{\mu_s}$ where the prime ideals $\mathfrak{P}_i$ commute by virtue of either theorem 2.2.1 or the fact that completely regular prime ideals commute. Then by theorem 2.2.3 and lemma 2.3.1, $\mathfrak{A} = \mathfrak{P}_1^{\nu_1} \ldots \mathfrak{P}_s^{\nu_s}$ with $\nu_i \leqq \mu_i$. The extension to fractional ideals and the uniqueness proof proceed as usual.

At this point it is easily shown using theorem 2.2.2 that if A is central simple over k and $\mathfrak{O}$ is a maximal order of A, then $\mathfrak{p}\mathfrak{O}$ is a power of a prime ideal where $\mathfrak{p}$ is any prime ideal of $\mathfrak{o}$. This result is due to Brandt [3]. As another application, consider the case of a simple algebra A, not necessarily central, where k is a field with a discrete non-trivial rank one valuation. Let $\mathfrak{O}$ be a maximal order with respect to the local integers of k. Then, since k has only one prime, it is easily shown that every ideal of $\mathfrak{O}$ has the form $\mathfrak{P}^e$ where $\mathfrak{P}$ is the unique prime ideal in $\mathfrak{O}$. A development of this result for the case where k is a $\mathfrak{p}$-adic field has been given by Hasse [8].

4. The Discriminant.

In this section it will be assumed that A is semisimple and separable over k Let $\mathfrak{o}_\mathfrak{p}$ denote the ring of $\mathfrak{p}$-integers of k and set $\mathfrak{O}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{O}$. Let $\sigma_1, \ldots, \sigma_n$ be a minimal basis for $\mathfrak{O}_\mathfrak{p}$ with $\sigma_i \in \mathfrak{O}$ for $i = 1, 2, \ldots, n$. If $\alpha_1, \ldots, \alpha_n \in A$ then the discriminant $\Delta(\alpha_1, \ldots, \alpha_n) = \det [S(\alpha_i\alpha_j)]$ where $[S(\alpha_i\alpha_j)]$ is the matrix with i as row index, j as column index, and where $S(\alpha)$ denotes the trace of α in the right (or left) regular representation of A. It is known that if $\beta_i = \sum_{j=1}^{n} c_{ij}\alpha_j$ with $c_{ij} \in k$ for $i = 1, 2, \ldots, n$, then $\Delta(\beta_1, \ldots, \beta_n)$ $= (\det [c_{ij}])^2 \Delta(\alpha_1, \ldots, \alpha_n)$. It is easily seen that if $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}$, then $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathfrak{o}$. The *$\mathfrak{p}$-component $\mathfrak{D}_\mathfrak{p}$ of the discriminant of* $\mathfrak{O}$ is defined to be the greatest power of $\mathfrak{p}$ which divides $\Delta(\sigma_1, \ldots, \sigma_n)$.

LEMMA 2.4.1: *$\mathfrak{D}_\mathfrak{p}$ is the greatest power of $\mathfrak{p}$ which contains all elements $\Delta(\alpha_1, \ldots, \alpha_n)$ for $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}$.*

PROOF: Set $\mathfrak{o} \, . \, \Delta(\sigma_1, \ldots, \sigma_n) = \mathfrak{p}^\lambda \mathfrak{q}$ where $\mathfrak{p}$ does not divide $\mathfrak{q}$. If $\alpha_i \in \mathfrak{O}$, then $\alpha_i = \sum_{j=1}^{n} c_{ij}\sigma_j$ with $c_{ij} \in \mathfrak{o}_\mathfrak{p}$. Since the denominator of $\det [c_{ij}]$ is prime to $\mathfrak{p}$, it follows that $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathfrak{p}^\lambda$.

The integral $\mathfrak{o}$-ideal $\mathfrak{D}$ generated by the set of all elements $\Delta(\alpha_1, \ldots, \alpha_n)$ for $\alpha_i \in \mathfrak{O}$ is called the *discriminant* of $\mathfrak{O}$. From lemma

2.4.1 it follows that $\mathfrak{D} = \prod_{\mathfrak{p}} \mathfrak{D}_{\mathfrak{p}}$ and that there are only a finite number of terms $\mathfrak{D}_{\mathfrak{p}} \neq \mathfrak{o}$.

THEOREM 2.4.1: *Let $\mathfrak{D}$ be the discriminant of $\mathfrak{O}$ and $\mathfrak{D}^*$ the discriminant of an order $\mathfrak{O}^*$ with $\mathfrak{O}^* \supseteqq \mathfrak{O}$. Then $\mathfrak{D}^* \supset \mathfrak{D}$ if and only if $\mathfrak{O}^* \supset \mathfrak{O}$.*

PROOF: It suffices to show that $\mathfrak{D} = \mathfrak{D}^*$ implies $\mathfrak{O} = \mathfrak{O}^*$. Suppose $\mathfrak{D} = \mathfrak{D}^*$. Let $\sigma_1, \ldots, \sigma_n$ be a minimal basis for $\mathfrak{O}_{\mathfrak{p}}$ with $\sigma_i \in \mathfrak{O}$ and let $\sigma_1^*, \ldots, \sigma_n^*$ be a minimal basis for $\mathfrak{O}_{\mathfrak{p}}^*$ with $\sigma_i^* \in \mathfrak{O}^*$. Then $\sigma_i = \sum_{j=1}^{n} c_{ij}\sigma_j^*$ for $i = 1, 2, \ldots, n$ and where $c_{ij} \in \mathfrak{o}_{\mathfrak{p}}$. Since $\mathfrak{D}_{\mathfrak{p}} = \overset{*}{\mathfrak{D}}_{\mathfrak{p}}$, it follows that $(\det [c_{ij}])^{-1} \in \mathfrak{o}_{\mathfrak{p}}$ and so $\mathfrak{O}_{\mathfrak{p}} = \overset{*}{\mathfrak{O}}_{\mathfrak{p}}$ for all primes $\mathfrak{p}$. For $\alpha \in \mathfrak{O}^*$, let $\mathfrak{q}(\alpha)$ be the set of elements $d \in \mathfrak{o}$ such that $d\alpha \in \mathfrak{O}$. If $\alpha \in \mathfrak{O}^*$, then for each prime $\mathfrak{p}$ there exists an element $h \in \mathfrak{o}$ with $(h, \mathfrak{p}) = (1)$ such that $h\alpha \in \mathfrak{O}$. It follows that $\mathfrak{q}(\alpha) = \mathfrak{o}$ for all $\alpha \in \mathfrak{O}^*$ and so $\mathfrak{O} = \mathfrak{O}^*$.

The ring $\mathfrak{O}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{O}_{\mathfrak{p}}$ can be construed as an algebra over $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$. Assume now that k has finite residue rings, that is, $\mathfrak{o}/\mathfrak{a}$ is finite for every integral ideal $\mathfrak{a}$ of k. Then if $\mathfrak{O}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{O}_{\mathfrak{p}}$ is semisimple, the centers of the simple components are separable extensions of the ground field and so the algebra $\mathfrak{O}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{O}_{\mathfrak{p}}$ is separable and has a non-zero discriminant (cf. [10]). Therefore $\mathfrak{O}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{O}_{\mathfrak{p}}$ is semisimple if and only if $\mathfrak{D}_{\mathfrak{p}} = \mathfrak{o}$ where $\mathfrak{D} = \prod_{\mathfrak{p}} \mathfrak{D}_{\mathfrak{p}}$ is the discriminant of $\mathfrak{O}$.

If $\mathfrak{O}$ is maximal, a prime ideal $\mathfrak{p}$ of k is said to be *ramified* in $\mathfrak{O}$ at $\mathfrak{P}_i$ if in its prime ideal decomposition, $\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_s^{e_s}$, e_i is greater than 1.

From the preceding remarks, together with lemma 2.2.1 and theorem 1.1.1, the following result is readily deduced.

THEOREM 2.4.2: *Let A be a separable algebra over k and assume that k has finite residue rings. Let $\mathfrak{O}$ be an arbitrary order of A and let $\mathfrak{p}$ be a prime ideal of k. Then the algebra $\mathfrak{O}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{O}_{\mathfrak{p}}$ over $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ is semisimple if and only if $\mathfrak{D}_{\mathfrak{p}} = \mathfrak{o}$ where $\mathfrak{D} = \prod_{\mathfrak{p}} \mathfrak{D}_{\mathfrak{p}}$ is the discriminant of $\mathfrak{O}$. In particular, if $\mathfrak{O}$ is maximal then a prime ideal $\mathfrak{p}$ of k is ramified in $\mathfrak{O}$ if and only if $\mathfrak{p}$ divides $\mathfrak{D}$.*

5. The Conductor.

If an order $\mathfrak{O}$ is properly contained in another order $\mathfrak{O}^*$, it is natural to study the relation between the arithmetic of $\mathfrak{O}$ and that of $\mathfrak{O}^*$. Of particular interest is the case where $\mathfrak{O}^*$ is maximal.

Using the fact that orders are finitely-generated $\mathfrak{o}$-modules, it is easily shown that if $\mathfrak{O} \subset \mathfrak{O}^*$ then there exist elements $c \neq 0$ in $\mathfrak{o}$ such that $c\mathfrak{O}^* \subseteqq \mathfrak{O}$. It follows that there exist non-zero $\mathfrak{O}^*$-ideals which lie in $\mathfrak{O}$. The ideal generated by the set of all such ideals is called the *conductor* $\mathfrak{F}$ of $\mathfrak{O}$ with respect to $\mathfrak{O}^*$. An $\mathfrak{O}$-ideal $\mathfrak{A}$ is said to be *regular with respect to* $\mathfrak{O}^*$ if $(\mathfrak{A}, \mathfrak{F}) = \mathfrak{O}$. An $\mathfrak{O}^*$-ideal $\mathfrak{C}$ is said to be *regular with respect to* $\mathfrak{O}$ if $(\mathfrak{C}, \mathfrak{F}) = \mathfrak{O}^*$. With each integral $\mathfrak{O}$-ideal $\mathfrak{A}$ can be associated the integral $\mathfrak{O}^*$-ideal $\{\mathfrak{A}\} = = \mathfrak{O}^*\mathfrak{A}\mathfrak{O}^*$; with each integral $\mathfrak{O}^*$-ideal $\mathfrak{C}$ can be associated the integral $\mathfrak{O}$-ideal $\mathfrak{C}^\circ = \mathfrak{C} \cap \mathfrak{O}$.

Lemma 2.5.1: *If the $\mathfrak{O}$-ideal $\mathfrak{A}$ is regular, then so is $\{\mathfrak{A}\}$. If the $\mathfrak{O}^*$-ideal $\mathfrak{C}$ is regular, then so is $\mathfrak{C}^\circ$. In this case $\{\mathfrak{A}\}^\circ = \mathfrak{A}$ and $\{\mathfrak{C}\} = \mathfrak{C}$.*

Proof: If $\mathfrak{A}$ is a regular $\mathfrak{O}$-ideal it is clear that $\{\mathfrak{A}\}$ is also regular. If $\mathfrak{C}$ is a regular $\mathfrak{O}^*$-ideal then there exist elements $\gamma \in \mathfrak{C}$, $\delta \in \mathfrak{F}$ such that $\gamma + \delta = 1$. But then γ is clearly in $\mathfrak{O}$ and so $\mathfrak{C}^\circ$ is regular. The last statement follows from the relations $\{\mathfrak{A}\}^\circ = (\mathfrak{A}, \mathfrak{F})\{\mathfrak{A}\}^\circ (\mathfrak{A}, \mathfrak{F}) \subseteqq \mathfrak{A}$ and $\mathfrak{C} = (\{\mathfrak{C}^\circ\}, \mathfrak{F})\mathfrak{C}(\{\mathfrak{C}^\circ\}, \mathfrak{F}) \subseteqq \{\mathfrak{C}^\circ\}$.

Theorem 2.5.1: *The mapping $\mathfrak{A} \rightarrow \{\mathfrak{A}\}$ is a one-to-one mapping of the set of regular $\mathfrak{O}$-ideals onto the set of all regular $\mathfrak{O}^*$-ideals. It is an isomorphism with respect to sum, product and intersection.*

Proof: The first statement follows from lemma 2.5.1. If $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are regular $\mathfrak{O}$-ideals, then so are $(\mathfrak{A}_1, \mathfrak{A}_2)$ and, by lemma 1.1.2, $\mathfrak{A}_1 \cap \mathfrak{A}_2$ and $\mathfrak{A}_1\mathfrak{A}_2$. It is easy to verify that the mapping preserves sums and intersections. If $\omega \in \mathfrak{O}^*$, $\alpha_1 \in \mathfrak{A}_1$ and $\alpha_2 \in \mathfrak{A}_2$, then $\alpha_1\omega\alpha_2 \in \alpha_1(\mathfrak{A}_2, \mathfrak{F})\omega\alpha_2(\mathfrak{A}_1, \mathfrak{F}) \subseteqq \{\mathfrak{A}_1\mathfrak{A}_2\}$ and so $\{\mathfrak{A}_1\mathfrak{A}_2\} = \{\mathfrak{A}_1\}.\{\mathfrak{A}_2\}$. This completes the proof.

Theorem 2.5.2: *Let $\mathfrak{O}$ be an order contained in a maximal order $\mathfrak{O}^*$ and assume that A is separable. Let $\mathfrak{D}$ and $\mathfrak{D}^*$ be the discriminants of $\mathfrak{O}$ and $\mathfrak{O}^*$ respectively. Let $\mathfrak{F}$ be the conductor of $\mathfrak{O}$ with respect to $\mathfrak{O}^*$. Then $\mathfrak{D}_{\mathfrak{p}}{}^* \supset \mathfrak{D}_{\mathfrak{p}}$ if and only if $\mathfrak{p}$ is divisible by a prime ideal divisor in $\mathfrak{O}^*$ of $\mathfrak{F}$.*

Proof: Let $\mathfrak{F}'$ be the conductor of $\mathfrak{O}_{\mathfrak{p}}$ with respect to $\mathfrak{O}_{\mathfrak{p}}{}^*$. It will be shown that $\mathfrak{F}' = \mathfrak{F}_{\mathfrak{p}}$. If $\alpha \in \mathfrak{F}'$, then there exists an element $a \in \mathfrak{o}$ with $(a, \mathfrak{p}) = (1)$ such that $a\alpha \in \mathfrak{O}$. Then $\mathfrak{O}^*(a\alpha)\mathfrak{O}^* \subseteqq \mathfrak{O}_{\mathfrak{p}} \cap \mathfrak{O}^*$ Now $\mathfrak{O}_{\mathfrak{p}} \cap \mathfrak{O}^*$ is a finitely-generated $\mathfrak{o}$-module and so it contains elements $\sigma_1, \ldots, \sigma_s$ such that $\mathfrak{O}_{\mathfrak{p}} \cap \mathfrak{O}^* = \mathfrak{o}\{\sigma_1, \ldots, \sigma_s\}$. Let b be an element of $\mathfrak{o}$ with $(b, \mathfrak{p}) = (1)$ such that $b\sigma_i \in \mathfrak{O}$ for $i = 1, 2, \ldots, r$. Then $\mathfrak{O}^*(ab\alpha)\mathfrak{O}^* \subseteqq \mathfrak{O}$ and so $\alpha \in \mathfrak{F}_{\mathfrak{p}}$. Clearly $\mathfrak{F}_{\mathfrak{p}} \subseteqq \mathfrak{F}'$ and so $\mathfrak{F}' = \mathfrak{F}_{\mathfrak{p}}$. Let $\mathfrak{F} = \mathfrak{P}_1^{\lambda_1} \ldots \mathfrak{P}_s^{\lambda_s}$ be the prime ideal decomposition of $\mathfrak{F}$ in $\mathfrak{O}^*$. Set $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathfrak{o}$. This is clearly a prime ideal of k. If $1 \in \mathfrak{F}_{\mathfrak{p}_i}$ then $1 = \sum_{j=1}^{m} c_i^{(j)} \pi_i^{(j)}$ where $c_i^{(j)} \in \mathfrak{o}_{\mathfrak{p}_i}$ and $\pi_i^{(j)} \in \mathfrak{P}_i$ for $j = 1, 2, \ldots, m$. Now choose $d \in \mathfrak{o}$ such that $(d, \mathfrak{p}_i) = (1)$ and $dc_i^{(j)} \in \mathfrak{o}$ for $j = 1, 2, \ldots, m$. Then $d = \sum_{j=1}^{m} dc_i^{(j)} \pi_i^{(j)} \in \mathfrak{P}_i$, a contradiction. Therefore $\mathfrak{F}_{\mathfrak{p}_i} \neq \mathfrak{Q}_{\mathfrak{p}_i}$. It follows that $\mathfrak{O}_{\mathfrak{p}_i}^* \supset \mathfrak{O}_{\mathfrak{p}_i}$ and so, by theorem 2.4.1, $\mathfrak{D}_{\mathfrak{p}_i}^* \supset \mathfrak{D}_{\mathfrak{p}_i}$. On the other hand, if $\mathfrak{p}$ is a prime ideal of k not among $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, then $\mathfrak{F}_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}}^*$. Therefore $\mathfrak{O}_{\mathfrak{p}}^* = \mathfrak{O}_{\mathfrak{p}}$ and so $\mathfrak{D}_{\mathfrak{p}}^* = \mathfrak{D}_{\mathfrak{p}}$.

REFERENCES.

Artin, E.

[1] Zur Arithmetik hyperkomplexer Zahlen. Abh. Math. Sem. Univ. Hamburg 5 (1927), 261—289.

Artin, E., Nesbitt, C. J. and Thrall, R. M.

[2] Rings with Minimum Condition, Michigan, 1946.

Brandt, H.

[3] Zur Idealtheorie Dedekindscher Algebren, Comm. Math. Helv. 2 (1930), 13—17.

Brauer, R.

[4] On the Arithmetic in a Group Ring, Proc. Nat. Acad. Sci. 30 (1944), 109—114,

Chevalley, C.

[5] L'Arithmétique dans les Algèbres de Matrices, Act. Sci. Ind. no. 323, Paris, 1936.

Deuring, M.

[6] Algebren. Ergebnisse der Math. 4, Berlin, 1935, New York, 1948.

Fitting, H.

[7] Primärkomponentenzerlegung in nichtkommutativen Ringen, Math. Ann. 111 (1935), 19—41.

Hasse. H.

[8] Über $\mathfrak{p}$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Math. Ann. 104 (1931), 495—543.

[9] Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann. 107 (1933), 731—760.

Jacobson, N.

[10] The Theory of Rings, Amer. Math. Soc. Surveys II, 1943.

van der Waerden, B. L.

[11] Moderne Algebra, 2nd ed. Berlin 1937, 1940.

(Oblatum 9-7-53)

Northwestern University
Evanston Ill. U.S.A.