Arithmetic of Ova

Thesis

by

A. H. Clifford

In Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

California Institute of Technology

Pasadena, California

1933.

INDEX

Introduction.

The property of unique decomposition into primes is fundamental in multiplicative arithmetic. The purpose of the present undertaking is to give criteria for this property, and to restore it by means of ideals when it is lacking, using only the single operation of multiplication.

We start, therefore, with a system closed under a single binary operation, assumed to be associative and commutative. Following Bell[1.], we shall call such a system an ovum. An ovum is said to be regular if cancellation is permissable. A regular ovum is a commutative semi-group, as Dickson has defined this term. Criteria for unique decomposition in regular ova have been given by Koenig[2.] in very beautiful form indeed (Theorem 4.1). Conditions have likewise been given by Klein-Barmen[3.] and by Ward[4.], the latter for the non-commutative case. We give criteria in § 1 for ova which are not necessarily regular (Theorem 1.1), and another set in § 5 generalizing Koenig's result (Theorem 5.3). The former is applied to general commutative rings, the result (Theorem 1.5) depending on a clever manipulation devised by Fraenkel[5.] in order to obtain unique decomposition in essentially finite rings.

The concept of an ideal, as introduced in § 2, is essentially that due to Prufer[6.]. The definition is framed differently, however, in order to preserve the analogy with Dedekind ideals.

In § 3 we postulate the Teilerkettensatz and the condition that every prime ideal by irreducible, and obtain the unique decomposition of any ideal into the product of mutually coprime, "einartig", primary ideals. In § 4 we obtain criteria that the ideals in a regular ovum admit unique decomposition into prime ideals, these being entirely analogous to those obtained by Noether[7]. The development in both § 3 and § 4 follows van der Waerden[8], who follows Krull[9].

In § 5 we note that, when we pass to rings, every ovoid ideal is also a ring ideal, but not always conversely. The two systems are multiply isomorphic, yet have in general very different arithmetic properties. It is noteworthy that if unique decomposition holds in the ring, then every ovoid ideal is a principal ideal, which is not necessarily the case for ring ideals. Thus ovoid ideals appear to have a more intimate connection with the multiplicative properties of the ring than do ring ideals, although they are not presumed to have such interesting additive properties, nor to be so useful in the study of algebraic manifolds.

Before passing on to the detailed development of the theory, I wish here to express my thanks to Professors E. T. Bell and M. Ward for many helpful suggestions in this endeavor.

1. E. T. Bell. "Unique decomposition".

Amer. Math. Monthly 37, 1930, 400-418.

2. J. Koenig. "Algebraischen Grössen", Ch I. Leipzig, 1903.

3. F. Klein-Barmen. "Über gekoppelte Axiomensysteme in der Theorie der abstrakten Verknüpfungen".

Math. Zeit. 37, 1933, 39-60.

4. M. Ward. "Postulates for an abstract arithmetic".

Proc. Natl. Acad. Sci. 14, 1928, 907-911.

5. A. Fraenkel. "Über die Teiler der Null und die Zerlegung von Ringen".

Jour. für Math. 145, 1915, 139-176.

6. H. Prufer. "Untersuchungen über Teilbarkeitseigenshaften in Körpern".

Jour. für Math. 168, 1932, 1-36.

7. E. Noether. "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern".

Math. Ann. 96, 1926, 26-61.

8. B. L. van der Waerden. "Moderne Algebra" v 2, p 50 and p 97.

Berlin, 1931.

9. W. Krull. "Zur Theorie der allgemeinen Zahlringe."

Math. Ann. 99, 1928, 51-70.

1. Criteria for unique factorization in ova.

A system consisting of a class $\mathcal{S}$, an equality relation $=$, and a binary operation $\circ$, will be called an ovum if the following postulates are satisfied:

P_1: To every pair a , b of elements of $\mathcal{S}$ there corresponds an element c unique to within equal elements. We write $a \circ b = c$

P_2: If $a = a'$ and $b = b'$, then $a \circ b = a' \circ b'$.

P_3: For every triplet a , b , c of elements of $\mathcal{S}$

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

P_4: $$a \circ b = b \circ a.$$

P_5: There exists an element i in $\mathcal{S}$ such that

$$a \circ i = i \circ a = a$$

for all a in $\mathcal{S}$.

The element i of P_5 is evidently unique. It will be called the identity element of $\mathcal{S}$.

The element $a \circ b$ is called the product of a and b , and a and b are factors thereof. We shall write simply ab in place of $a \circ b$.

The immediate consequences of P_3 and P_4 are well-known*. Briefly, we may form the product of any finite number of elements of $\mathcal{S}$. This product is independent of the order in which the

---

* See van der Waerden, "Moderne Algebra", v 1, pp 20-22.

successive products are formed, and of the order in which the factors occur. It depends only on the factors occurring therein, and the frequency with which they occur. Powers of any element a of $\mathcal{S}$ are defined in the usual way:

$$a^0 = i$$

$$a^n = a a^{n-1} \quad , \ (n = 1, 2, \dots).$$

Then the index laws

$$a^m a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$

hold for all non-negative integers m , n .

An element a of $\mathcal{S}$ is said to <u>divide</u>, or to be a <u>divisor</u> of, an element b of $\mathcal{S}$, if the equation

$$a x = b$$

has a solution x in $\mathcal{S}$. b is then called a <u>multiple</u> of a . We indicate this by $a \mid b$. The relation thus defined is transitive and reflexive, but not in general symmetric.

Divisors of the identity element i of $\mathcal{S}$ are called <u>unities</u>. They form a group.

If $a \mid b$ and $b \mid a$ always implies $a = b$, we shall say that the ~~ovum~~ $\mathcal{S}$ is <u>reduced</u>.

If $a \mid b$ and $b \mid a$ then we write $a \backsim b$, and say that a and b are <u>associate</u>. This is an equivalence relation with the property that if $a \backsim a'$ and $b \backsim b'$ then $a \circ b \backsim a' \circ b'$. Hence $\mathcal{S}$ forms a reduced ovum with respect to the binary operation $\circ$ and

$\sim$ as the equality relation. This ovum we called the <u>reduced ovum</u> of $\mathcal{S}$.

In the remainder of this section we consider only reduced ova. The results hold for any ova provided we interpret "$a = b$" as meaning " a is associate to b ," and "unique" as meaning "unique to within associates."

Let, then, $\mathcal{S}$ be a reduced ovum.

If a / b , but $a \neq b$, we write $a \,//\, b$, and say that a is a <u>proper divisor</u> of b . This relation is readily seen to be transitive.

An element of $\mathcal{S}$ which has no proper divisors othen than i is called <u>irreducible</u>; otherwise, <u>reducible</u>.

An element a of $\mathcal{S}$ is called <u>decomposable</u> if proper divisors b and c of a exist such that $a = bc$. Otherwise, a is called <u>indecomposable</u>. If a is indecomposable, and $a = bc$, then either $a = b$ or $a = c$; that is, if $x \,//\, a$ then $a = ax$. Hence the proper divisors of a form a subovum of $\mathcal{S}$.

An element p of $\mathcal{S}$ is called <u>prime</u> if the relation p / ab implies that either p / a or p / b , and <u>completely prime</u> if p^r / ab implies that either p^r / a or p^r / b , r being any positive integer. Every prime element is plainly indecomposable.

Consider the sequence of elements a , a^2 , a^3 , ..., where a is any element of $\mathcal{S}$. If they are not all distinct, let a^k be the first element of the sequence which is equal to an element a^{r+s} $(s > 0)$ further out in the sequence:

$$a^r = a^{r+s}.$$

Now $a^{r+1} \mid a^{r+s}$, so that a^{r+1} / a^r. Likewise a^r / a^{r+1}. Since we are assuming that $\mathcal{S}$ is reduced, this implies that

$$a^r = a^{r+1}.$$

Multiplying this repeatedly by a we find

$$a^r = a^{r+1} = a^{r+2} = \cdots$$

We arrive in this way at the following result:

If a is any element of a reduced ovum $\mathcal{S}$, then either every element of the sequence a, a^2, a^3, ... is distinct, or else they are all distinct up to a certain point, and all equal from that point on. The number of distinct elements in the sequence will be called the <u>index</u> of a; if all the powers of a are distinct, we shall say that a is of <u>infinite index</u>.

An element a of $\mathcal{S}$ is said to be <u>decomposable into irreducible elements</u> if distinct irreducibles $p_1, \cdots, p_r$ exist such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

where the α_i are positive integers. The decomposition of a is said to be <u>unique</u> if the existence of another,

$$a = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

implies that

(i) the sets $\{p_1, \dots, p_r\}$, $\{q_1, \dots, q_s\}$ are identical, so that, by suitable numeration, $s = r$ and

$$p_i = q_i \quad , \quad (i = 1, 2, \dots, r);$$

(ii) $$p_i^{\alpha_i} = q_i^{\beta_i} \quad , \quad (i = 1, 2, \dots, r).$$

The second of these is equivalent to the statement that either $\alpha_i = \beta_i$ or else neither α_i nor β_i is less then the index of p_i .

Theorem 1.1

The following conditions are necessary and sufficient that every element of a reduced ovum S admit unique decomposition into irreducible elements of S :

I. Teilerkettensatz: If a sequence a_1 , a_2 , ... of elements of S is such that $a_{i+1} \,/\!/\, a_i$, then the sequence terminates.

II. Every reducible element is decomposable.

III. Every irreducible element is completely prime.

Proof of Sufficiency:

We show first that every element of S is decomposable into a product of irreducible elements of S .

For if an element a of S had not this property, then it could not be itself irreducible. Hence by II we could write $a = bc$, where $b \,/\!/\, a$, $c \,/\!/\, a$. If both b and c were decomposable into irreducibles, then clearly a would also be. Selecting the one which is not decomposable, we proceed as with

a , obtaining a further proper divisor thereof not decomposable into irreducibles. But this process gives rise to an unending sequence of proper divisors, in contradiction to I.

Suppose now that we have two decompositions of a :

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s} .$$

Since the result is evident for $a = i$ we can assume $a \neq i$, and that the irreducibles $p_1, \ldots, p_r$ are all different from i and from each other, and similarly for $q_1, \ldots, q_s$.

Since $p_1 \mid q_1^{\beta_1} \cdots q_s^{\beta_s}$ we infer from an obvious extension of III that p_1 divides one of the q_j , say q_1 . This implies that $p_1 = q_1$. Continuing with $p_2, \ldots, p_r$ we get the result that $s = r$, and, by suitable numeration, $p_i = q_i, (i = 1, \ldots, r)$.

Since now p_1 divides none of the elements $q_2, \ldots, q_r$, it follows from III that it cannot divide $q_2^{\beta_2} \cdots q_r^{\beta_r}$. But

$$p_1^{\alpha_1} \mid q_1^{\beta_1}(q_2^{\beta_2} \cdots q_r^{\beta_r}),$$

and hence from III again, $p_1^{\alpha_1} \mid q_1^{\beta_1}$. Similarly, $q_1^{\beta_1} \mid p_1^{\alpha_1}$, and since S is reduced,

$$p_1^{\alpha_1} = q_1^{\beta_1}$$

Similarly, $$p_i^{\alpha_i} = q_i^{\beta_i} , \quad (i = 2, \ldots, r).$$

q.e.d.

Proof of Necessity:

Assuming now that every element of $\mathcal{S}$ is uniquely decomposable into irreducible elements, we note first that if

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad , \ (\alpha_i > 0)$$

then the divisors of a are the elements

$$p_1^{\sigma_1} \cdots p_r^{\sigma_r}$$

where σ_i ranges from 0 to α_i . But these are finite in number. Hence I is certainly true.

Let now a be any reducible element of $\mathcal{S}$. Let

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad , \quad (\alpha_i > 0).$$

Then $b = p_1$ and $c = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ are both proper divisors of a , and $a = bc$. Hence II is established.

If now p^2 / ab , where p is irreducible, and if p does not occur in the decomposition of a , then it must occur in that of b with multiplicity ≥ 2 . Hence either p / a or p^2 / b . This proves III.

q.e.d.

Theorem 1.2

The conditions I, II, III of Theorem 1.1 are independent.

Proof:

Independence of I:

Take for example the set of all numbers of the form $2^{\alpha} \pi^{n}$, where α ranges over all non-negative real numbers, and n over all non-negative rational integers. Multiplication is the usual variety:

$$(2^{\alpha}\pi^{m})(2^{\beta}\pi^{n}) = 2^{\alpha+\beta}\pi^{m+n}.$$

The only irreducibles are 1 and π. Since they are evidently completely prime, III holds. Evidently II also holds. Yet I does not, e.g. the sequence $2, 2^{\frac{1}{2}}, 2^{\frac{1}{4}}, 2^{\frac{1}{8}}, \ldots$ violates it.

q.e.d.

Independence of II.

Take for example the set of divisors of 12, the product of a and b being the L.C.M of a and b. Since the set is finite, I holds. The irreducibles are 2 and 3, which are plainly prime (and hence completely prime, since the system is idempotent). Thus III holds.

Yet II does not. For example, the only decompositions of 4 are $4 = 2 \circ 4$ and $4 = 4 \circ 4$, so that 4 is indecomposable.

q.e.d.

Independence of III.

Take for example the ovum $\{0, i, p, q, r\}$ with multiplication table:

	p	q	r
p	0	0	0
q	0	q	0
r	0	0	r

Since the set is finite, I holds. Since 0 is the only reducible element, and since $0 = pq$, $p \neq 0$, $q \neq 0$, it is decomposable. Hence II holds. III does not, however, for $p^2 = qr$, so that $p \mid qr$, and yet $p \mid q$ and $p \mid r$ are both false.

q.e.d.

If an element a of an ovum $\mathcal{S}$ has the property that $ax = ay$ always implies $x = y$, it is called <u>regular</u>; otherwise, <u>irregular</u>. Every regular element is clearly of infinite index. The product of two regular elements is regular, and every divisor of a regular element is regular. An ovum is said to be regular if all its elements are regular.

If an element z of an ovum $\mathcal{S}$ has the property that $az = z$ for all a in $\mathcal{S}$, we call it a <u>zero element</u>. It is plainly unique, provided it exists. If z is decomposable: $z = ab$, $z \neq a$, $z \neq b$, then a and b are called <u>nilfactors</u>. Any nilfactor is clearly irregular, though, unlike the case in rings, an irregular element is not necessarily a nilfactor. We have excluded the existence of a zero element in regular ova since it contributes nothing to the arithmetic theory thereof.

Parenthetically, if a reduced ovum $\mathcal{S}$ has a zero z, and every element of $\mathcal{S}$, including z, admits unique decomposition into irreducibles, then $\mathcal{S}$ is finite. In fact, if

$$z = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

then $\mathcal{S}$ is identical with the set of all elements of the form $p_1^{\sigma_1} \cdots p_r^{\sigma_r}$ as each σ_i ranges independently from 0 to α_i. $\mathcal{S}$ is therefore simply isomorphic with the reduced ovum of the residue class ring of any positive integer of the form $\pi_1^{\alpha_1} \cdots \pi_r^{\alpha_r}$ where $\pi_1, \ldots, \pi_r$ are any distinct prime numbers.

In a regular ovum, every reducible element is decomposable. Likewise every prime element is completely prime. Hence from Theorem 1.1 we have immediately:

Theorem 1.3

Necessary and sufficient conditions that every element of a regular ovum be uniquely decomposable into irreducibles are

I. Teilerkettensatz.

II. Every irreducible element is prime.

If a and b are elements of $\mathcal{S}$, and if c is a common divisor thereof such that every other common divisor of a and b divides c, then c is said to be a greatest common divisor (G.C.D.) of a and b. If it exists, it is unique to within associates.

Koenig showed that if every pair of elements of a regular ovum possess a G.C.D., then every irreducible element is prime, and thence to the property of unique factorization, by Theorem 1.3. Since this condition is evidently also necessary, we have Koenig's elegant result:

Theorem 1.4

Necessary and sufficient conditions that every element of a regular ovum be uniquely decomposable into irreducibles are

I. Teilerkettensatz.

II. Existence of G.C.D. of every pair of elements.

Off hand we should suppose that similar criteria would hold for an irregular ovum, adjoining to these, say, the condition that every reducible element be decomposable. Such is not the case, as the third example in the proof of Theorem 1.2 shows. There every pair of elements has a G.C.D., and yet the prime property breaks down. The reason for this, and the proper generalization of Theorem 1.4 for irregular ova, will be given in § 5 (Theorem 5.3).

We shall close this section with applications of Theorem 1.1 to general commutative rings having a principal indentity. The next theorem, giving criteria for general rings, is very similar to a result of Fraenkel's mentioned in the Introduction. That the result is not true for ova can be seen by referring to the second example in the proof of Theorem 1.2. We remark that since we have to use addition and subtraction we are not at liberty to pass to the reduced ovum.

Theorem 1.5

Necessary and sufficient conditions that every element of a commutative ring $\mathcal{R}$ be uniquely decomposable into irreducibles are:

I. Teilerkettensatz: If $a_{i+1} /\!/ a_i$, then the sequence $a_1, a_2, \ldots$ terminates.

~~"Uber die Teiler der Null und die Zerleging von Ringen".~~

II. Vielfachenkettensatz: If $a_i \not| a_{i+1}$, then either the sequence $a_1, a_2, \ldots$ terminates, or no element $\neq 0$ is divisible by all the a_i .

III. Every irreducible element is completely prime.

Proof:

The condition II is plainly necessary. Hence by Theorem 1.1 we have only to show that if these three conditions are satisfied, then every reducible element is decomposable.

Let a be any reducible element of R .

If a is regular then it is decomposable. For if $a = bc$, $b \not| a$, $i \not| b$, a / c , then

$$ab / cb,$$
$$ab / a,$$
$$b / i,$$

in contradiction to $i \not| b$. Hence a / c is false, and $c \not| a$.

Now let a be irregular. By I every element has an irreducible divisor. Let p be an irreducible divisor of a . If a were indecomposable then

$$a = a'p$$

where $$a \backsim a'.$$

Hence $$ap \backsim a'p,$$

so that $$a \backsim ap \backsim ap^2 \backsim \ldots$$

If now p were regular, then a would be divisible by every member of the sequence $p, p^2, p^3, \ldots$ in contradiction to II.

Hence p is irregular.

Since we are in a ring, p is a divisor of zero, so that $c \neq 0$ exists in R such that

$$pc = 0.$$

Let

$$a' = ab.$$

We proceed to show that

$$a = (a'+c)p$$

affords a decomposition of a, i.e. that $(a'+c)//a$.

For if $a/(a'+c)$, then, since a/a', a/c. Let

$$c = ae.$$

Then

$$\begin{aligned} c &= a'pe \\ &= abpe \\ &= bpc \\ &= 0. \end{aligned}$$

But $c \neq 0$. Hence a cannot divide $a'+c$, so that $(a'+c)//a$.

q.e.d.

It is well known that if every ideal in a ring be a principal ideal, then I holds. We can also show that III holds. If $\bar{R}$ be a residue class ring of an algebraic ring R then

(i) since every ideal in R has a two-term basis, one of which can be chosen arbitrarily, it follows that every ideal in $\bar{R}$ is a principal ideal;

(ii) since II holds in R it holds in $\bar{R}$ also.

This yields a direct proof of the unique decomposition property in any residue class ring of a ring of algebraic integers.

2. Ideals and their fundamental properties.

If A and B are subclasses of an ovum S, we shall denote the class sum and common part of A and B by $A \cup B$ and $A \cap B$, respectively. If A is a subclass of B we write $A \subseteq B$ or $B \supseteq A$. We shall denote by AB the class of all products ab, as a ranges over A and b over B. If A consists of the single element a of S, we may write aB in place of AB. The class of all common divisors of A will be denoted by $\Delta(A)$.

A subclass A of S will be called an ideal class, or simply an ideal, if it includes every element s of S which has the property that sx is divisible by all common divisors of the set Ax, for every (fixed) element x of S. Expressed otherwise, if the class B has the property that, for each x in S,

$$\Delta(Bx) \supseteq \Delta(Ax),$$

then

$$A \supseteq B.$$

Whenever the letter x occurs in the following, the statement is assumed to hold for every x in S. Ideals will be denoted by small German letters.

Let $\mathfrak{a}$ be an ideal. Then if a class A has the property

$$\Delta(xA) = \Delta(x\mathfrak{a})$$

we say that A generates, or is a generator of, the ideal $\mathfrak{a}$. Evidently every possible generator of $\mathfrak{a}$ is a subclass of $\mathfrak{a}$.

A finite generator is called a basis.

Conversely, if A is any class, then the class $\mathfrak{a}$ of all elements a with the property that ax is divisible by every common divisor of Ax, is an ideal, and A is a generator thereof. For then

$$\Delta(\mathfrak{a}x) = \Delta(Ax)$$

and, from the way in which $\mathfrak{a}$ is defined, if

$$\Delta(\mathcal{B}x) \supseteq \Delta(Ax)$$

then
$$A \supseteq \mathcal{B}.$$

If A generates the ideal $\mathfrak{a}$, we write

$$\mathfrak{a} = (A).$$

If A consists of the elements a, b, ... of $\mathcal{S}$, we write

$$\mathfrak{a} = (a, b, \ldots).$$

<u>Theorem 2.1</u>

A necessary and sufficient condition that

$$(A) \subseteq (\mathcal{B})$$

is that
$$\Delta(Ax) \supseteq \Delta(\mathcal{B}x) \quad \text{for all } x \text{ in } \mathcal{S}.$$

A necessary and sufficient condition that

$$(A) = (\mathcal{B})$$

is that
$$\Delta(Ax) = \Delta(\mathcal{B}x) \quad \text{for all } x \text{ in } \mathcal{S}.$$

<u>Proof</u>:

Let $\mathfrak{a} = (A)$, $\mathfrak{b} = (\mathcal{B})$, so that

$$\Delta(Ax) = \Delta(\mathfrak{a}x)$$

$$\Delta(Bx) = \Delta(\mathfrak{b}x).$$

Then we have to show that a necessary and sufficient condition that

$$\mathfrak{a} \subseteq \mathfrak{b}$$

is that $$\Delta(\mathfrak{a}x) \supseteq \Delta(\mathfrak{b}x).$$

If $\mathfrak{a} \subseteq \mathfrak{b}$ then plainly

$$\mathfrak{a}x \subseteq \mathfrak{b}x$$

so that $$\Delta(\mathfrak{a}x) \supseteq \Delta(\mathfrak{b}x).$$

The converse is an immediate consequence of the definition that $\mathfrak{b}$ be an ideal.

The second part of the theorem is an obvious consequence of the first. q.e.d.

Theorem 2.2

If $(A) \subseteq (A')$ and $(B) \subseteq (B')$, then $(AB) \subseteq (A'B')$.
If $(A) = (A')$ and $(B) = (B')$, then $(AB) = (A'B')$.

Proof:

By Theorem 2.1,

$$\Delta(Ax) \supseteq \Delta(A'x)$$

$$\Delta(Bx) \supseteq \Delta(B'x).$$

Replacing x by $\mathfrak{b}x$ in the first of these, we have

$$\Delta(A\mathfrak{b}x) \supseteq \Delta(A'\mathfrak{b}x).$$

Since this is true (for each fixed x in $\mathcal{S}$) for all b in $\mathcal{S}$, and hence all b in $\mathcal{B}$, we infer that

$$\Delta(\cancel{A}\mathcal{B}x) \supseteq \Delta(A'\mathcal{B}x).$$

Again using Theorem 2.1, this gives us

$$(A\mathcal{B}) \subseteq (A'\mathcal{B}).$$

In similar fashion we prove that

$$(A'\mathcal{B}) \subseteq (A'\mathcal{B}'),$$

and hence that

$$(A\mathcal{B}) \subseteq (A'\mathcal{B}').$$

The second part of the theorem is an obvious consequence of the first. q.e.d.

If $\mathfrak{a} = A$ and $\mathfrak{b} = \mathcal{B}$ are ideals, then the <u>product</u> of $\mathfrak{a}$ and $\mathfrak{b}$ is defined to be the ideal generated by $A\mathcal{B}$. We shall write this $\mathfrak{a} \cdot \mathfrak{b}$ or $\mathfrak{a}\,\mathfrak{b}$, and in order to avoid confusion with the product of two classes, as already defined, we shall employ the convention that the juxtaposition of capital Latin letters will always denote simple class product, while the juxtaposition of small German letters will always denote ideal product.

Thus $$\mathfrak{a}\mathfrak{b} = (A\mathcal{B}).$$

<u>Theorem 2.3</u>

If A and $\mathcal{B}$ are any two subclasses of $\mathcal{S}$, then

$$(A) \cdot (\mathcal{B}) = (A\mathcal{B}).$$

Proof:

Let
$$\mathfrak{a} = A' = (A)$$
$$\mathfrak{b} = B' = (B).$$

Then by definition
$$(A)\cdot(B) = \mathfrak{a}\mathfrak{b} = (A'B').$$

But
$$(A) = (A')$$
$$(B) = (B'),$$

so that by Theorem 2.2,
$$(AB) = (A'B'),$$
$$(A)\cdot(B) = (AB).$$

q.e.d.

Theorem 2.4

If $\mathfrak{a}$ and $\mathfrak{b}$ are any ideals in $\mathcal{S}$, then $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$.

Proof:

Let $\mathfrak{a} = A$, $\mathfrak{b} = B$. Then since $AB = BA$ we have
$$(AB) = (BA).$$

Hence by Theorem 2.3,
$$(A)(B) = (B)(A).$$

q.e.d.

Theorem 2.5

If $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are any ideals in $\mathcal{S}$, then
$$\mathfrak{a}\cdot\mathfrak{b}\mathfrak{c} = \mathfrak{a}\mathfrak{b}\cdot\mathfrak{c}.$$

Proof:

Let $\mathfrak{a} = A$, $\mathfrak{b} = B$, $\mathfrak{c} = C$. Then, since $A\cdot BC = AB\cdot C$, we have $$(A \cdot BC) = (AB \cdot C).$$

Hence by Theorem 2.3,

$$(A)(BC) = (AB)(C)$$

and again $$(A)\cdot(B)(C) = (A)(B)\cdot(C).$$ q.e.d.

The proof of Theorem 2.5 shows incidentally that

$$\mathfrak{a}\mathfrak{b}\mathfrak{c} = (ABC).$$

The extension to any number of factors is obvious.

Theorem 2.6

If $\mathfrak{a} \subseteq \mathfrak{a}'$, $\mathfrak{b} \subseteq \mathfrak{b}'$, then $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}'\mathfrak{b}'$.

Proof:

Let $\mathfrak{a} = A$, $\mathfrak{a}' = A'$, $\mathfrak{b} = B$, $\mathfrak{b}' = B'$. Then by hypothesis

$$(A) \subseteq (A')$$

$$(B) \subseteq (B').$$

Hence by Theorem 2.2,

$$(AB) \subseteq (A'B')$$

and by Theorem 2.3, $$(A)(B) \subseteq (A')(B').$$

q.e.d.

If $\mathfrak{a} \supseteq \mathfrak{b}$ we say that the ideal $\mathfrak{a}$ divides, or is a divisor of, the ideal $\mathfrak{b}$. If $\mathfrak{a} \supset \mathfrak{b}$, we say that $\mathfrak{a}$ is a proper divisor of $\mathfrak{b}$. If $\mathfrak{a}$ divides $\mathfrak{b}$, we say also that $\mathfrak{b}$ is a multiple of $\mathfrak{a}$.

An ideal $\mathfrak{c}$ is called a <u>greatest common divisor</u> (G.C.D.) of the ideals $\mathfrak{a}$ and $\mathfrak{b}$ if

(i) it is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, and

(ii) every common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ divides $\mathfrak{c}$.

An ideal $\mathfrak{c}$ is called a least common multiple (L.C.M.) of the ideals $\mathfrak{a}$ and $\mathfrak{b}$ if

(i) it is a common multiple of $\mathfrak{a}$ and $\mathfrak{b}$,

(ii) every common multiple of $\mathfrak{a}$ and $\mathfrak{b}$ is a multiple of $\mathfrak{c}$.

If $\mathfrak{a}$ and $\mathfrak{b}$ have a G.C.D. it is plainly uniquely determined; we denote it by $(\mathfrak{a}, \mathfrak{b})$. Similarly for the L.C.M., which, if it exists, is denoted by $[\mathfrak{a}, \mathfrak{b}]$.

<u>Theorem 2.7</u>

Every pair of ideals $\mathfrak{a}$, $\mathfrak{b}$ possesses a G.C.D. In fact, if $\mathfrak{a} = (A)$, $\mathfrak{b} = (B)$, then

$$(\mathfrak{a}, \mathfrak{b}) = (A \cup B).$$

Proof: Let

$$C = A \cup B,$$

$$\mathfrak{c} = (C) = (A \cup B).$$

We need only show that $\mathfrak{c}$ has the desired properties.

Since $C \supseteq A$

if follows that $(C) \supseteq (A)$,

that is, $\mathfrak{c} \supseteq \mathfrak{a}$.

Similarly, $\mathfrak{c} \supseteq \mathfrak{b}$.

If now $\mathfrak{d} \supseteq \mathfrak{a}$, $\mathfrak{d} \supseteq \mathfrak{b}$

and $$\mathfrak{d} = \mathcal{D},$$

then $$\mathcal{D} \geq \mathcal{A}, \ \mathcal{D} \geq \mathcal{B},$$

so that $$\mathcal{D} \geq \mathcal{C}.$$

Hence $$(\mathcal{D}) \geq (\mathcal{C}),$$

that is, $$\mathfrak{d} \geq \mathfrak{c}.$$ q.e.d.

<u>Theorem 2.8</u>

Every pair of ideals $\mathfrak{a}$, $\mathfrak{b}$ possesses an L.C.M. In fact if $\mathfrak{a} = \mathcal{A}$, $\mathfrak{b} = \mathcal{B}$, then

$$[\mathfrak{a}, \mathfrak{b}] = \mathcal{A} \cap \mathcal{B}.$$

<u>Proof</u>:

Let $$\mathcal{C} = \mathcal{A} \cap \mathcal{B}.$$

We proceed to show that $\mathcal{C}$ is an ideal with the desired properties. To show the first, let the class $\mathcal{D}$ be such that

$$\Delta(\mathcal{D}x) \supseteq \Delta(\mathcal{C}x).$$

Now $$\mathcal{C} \subseteq \mathcal{A}$$

so that $$\mathcal{C}x \subseteq \mathcal{A}x$$

and $$\Delta(\mathcal{C}x) \supseteq \Delta(\mathcal{A}x).$$

Similarly, $$\Delta(\mathcal{C}x) \supseteq \Delta(\mathcal{B}x).$$

Hence $$\Delta(\mathcal{D}x) \supseteq \Delta(\mathcal{A}x)$$

and $$\Delta(\mathcal{D}x) \supseteq \Delta(\mathcal{B}x).$$

But $\mathcal{A}$ and $\mathcal{B}$ are ideals, so that

$$\mathcal{D} \subseteq \mathcal{A}$$

$$\mathcal{D} \subseteq \mathcal{B},$$

and hence $$\mathcal{D} \subseteq \mathcal{C}.$$

$\mathcal{C}$ is therefore an ideal. Let $\mathfrak{c} = \mathcal{C}$.

Now $$\mathcal{C} \subseteq \mathcal{A}\,, \quad \mathcal{C} \subseteq \mathcal{B},$$

i.e. $$\mathfrak{c} \subseteq \mathfrak{a}\,, \quad \mathfrak{c} \subseteq \mathfrak{b}.$$

Conversely, if $$\mathfrak{d} \subseteq \mathfrak{a}\,, \quad \mathfrak{d} \subseteq \mathfrak{b}$$

and $$\mathfrak{d} = \mathcal{D},$$

then $$\mathcal{D} \subseteq \mathcal{A}\,, \quad \mathcal{D} \subseteq \mathcal{B}$$

so that $$\mathcal{D} \subseteq \mathcal{C}.$$

That is, $$\mathfrak{d} \subseteq \mathfrak{c}.$$ q.e.d.

Theorem 2.8 shows that the common part of two ideals is also an ideal, and indeed the L.C.M. We thus sometimes write $\mathfrak{a} \cap \mathfrak{b}$ for $[\mathfrak{a}, \mathfrak{b}]$. The class sum of two ideals is not, however, in general an ideal.

Theorem 2.7 shows that if $\mathcal{A}$ generates $\mathfrak{a}$ and $\mathcal{B}$ generates $\mathfrak{b}$, then $\mathcal{A} \cup \mathcal{B}$ generates $(\mathfrak{a}, \mathfrak{b})$. We shall write $(\mathcal{A}, \mathcal{B})$ for $(\mathcal{A} \cup \mathcal{B})$, so that

$$(\mathcal{A}, \mathcal{B}) = (\mathfrak{a}, \mathfrak{b}).$$

We remark that $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a})$, $[\mathfrak{a}, \mathfrak{b}] = [\mathfrak{b}, \mathfrak{a}]$, and also that if $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{b}$ or $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a}$ then $\mathfrak{b} \supseteq \mathfrak{a}$, and conversely.

<u>Theorem 2.9</u>

If $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are any ideals in $\mathcal{S}$, then

$$(\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})) = ((\mathfrak{a}, \mathfrak{b}), \mathfrak{c})$$
$$[\mathfrak{a}, [\mathfrak{b}, \mathfrak{c}]] = [[\mathfrak{a}, \mathfrak{b}], \mathfrak{c}].$$

Proof:

By Theorem 2.7, both members of the first equation have the common value $(A \cup B \cup C)$, and both members of the second have the common value $A \cap B \cap C$. q.e.d.

We write $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ or (A, B, C) for the first, and $[\mathfrak{a}, \mathfrak{b}, \mathfrak{c}]$ or $\mathfrak{a} \cap \mathfrak{b} \cap \mathfrak{c}$ for the second, and similarly for any number of ideals.

Theorem 2.10

$$\mathfrak{a}(\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n) = (\mathfrak{a}\mathfrak{b}_1, \mathfrak{a}\mathfrak{b}_2, \ldots, \mathfrak{a}\mathfrak{b}_n).$$

Proof:

We shall prove this for $n = 2$, the induction to any n being quite obvious. Let $\mathfrak{a} = A$, $\mathfrak{b} = B$, $\mathfrak{c} = C$.

Evidently,

$$A\{B \cup C\} = AB \cup AC.$$

The ideal generated by the class on the left is, by Theorem 2.3, $(A)(B \cup C)$, that is, by Theorem 2.7,

$$\mathfrak{a}(\mathfrak{b}, \mathfrak{c}).$$

The ideal generated by the class on the right is, by Theorem 2.7, $((AB), (AC))$, that is, by Theorem 2.8,

$$(\mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}).$$

Since these must be identical,

$$\mathfrak{a}(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}).$$

q.e.d.

The class S is evidently an ideal, which we denote by $\mathfrak{o}$, and call the unit ideal.

Theorem 2.11

If $\mathfrak{a}$ is any ideal, then $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$.

Proof:

If a is in A and s is in S, then sax is divisible by every member of $\Delta(Ax)$, so that sa is in A. Hence $SA \subseteq A$.

Since S contains an identity element, $SA \supseteq A$.

Hence $SA = A$, and by Theorem 2.3, $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$.

q.e.d.

We remark that $\mathfrak{o} \geq \mathfrak{a}$ for all $\mathfrak{a}$. For $S \supseteq A$, so that $(S) \geq (A)$, for all A.

Theorem 2.12

$$\mathfrak{a} \geq \mathfrak{a}\mathfrak{b}.$$

$$[\mathfrak{a}, \mathfrak{b}] \geq \mathfrak{a}\mathfrak{b}.$$

Proof:

$$\mathfrak{a} \geq \mathfrak{a}$$

$$\mathfrak{o} \geq \mathfrak{b}.$$

Hence by Theorems 2.6 and 2.11,

$$\mathfrak{a} \geq \mathfrak{a}\mathfrak{b}.$$

Similarly $$\mathfrak{b} \geq \mathfrak{a}\mathfrak{b}.$$

Hence $$\mathfrak{a} \cap \mathfrak{b} \geq \mathfrak{a}\mathfrak{b}.$$ q.e.d.

If an ideal $\mathfrak{a}$ admits a basis A which consists of a single element a of S, then $\mathfrak{a}$ is called a <u>principal ideal</u>.

We write $\mathfrak{a} = (a)$.

Theorem 2.13

The set of principal ideals in S is an ovum simply isomorphic with the reduced ovum of S.

<u>Proof</u>:

To every a in $\mathcal{S}$ we let correspond the principal ideal (a). To every principal ideal $\mathfrak{a}$ we let correspond any element of $\mathcal{S}$ generating it.

If
$$(a) = (b)$$
then $a \mid b$ and $b \mid a$, so that $a \sim b$. Conversely if $a \sim b$, then every divisor of ax is also a divisor of bx, and vice versa, so that
$$(a) = (b).$$

Hence the correspondence is $(1,1)$ between the set of principal ideals in $\mathcal{S}$ and the reduced ovum of $\mathcal{S}$. Moreover it is an isomorphism, since, by Theorem 2.3,
$$(a)(b) = (ab).$$

q.e.d.

<u>Theorem 2.14</u>

If $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ and $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{d}$, then $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{d}$.

<u>Proof</u>:

On multiplying and using Theorem 2.10, we obtain
$$(\mathfrak{a}^2, \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}) = \mathfrak{o}\mathfrak{d} = \mathfrak{d}.$$

Now
$$(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) = (\mathfrak{o}, \mathfrak{c}) = \mathfrak{o}.$$

On multiplying by $\mathfrak{a}$, we obtain
$$(\mathfrak{a}^2, \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}) = \mathfrak{a}\mathfrak{o} = \mathfrak{a}.$$

By Theorem 2.9, then,
$$(\mathfrak{a}^2, \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}) = (\mathfrak{a}, \mathfrak{b}\mathfrak{c}),$$

whence
$$(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{d}.$$

q.e.d.

<u>Theorem 2.15</u> $$[\mathfrak{a},\mathfrak{b}]\cdot(\mathfrak{a},\mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}.$$

<u>Proof</u>: By Theorem 2.10,

$$[\mathfrak{a},\mathfrak{b}]\cdot(\mathfrak{a},\mathfrak{b}) = ([\mathfrak{a},\mathfrak{b}]\mathfrak{a},\ [\mathfrak{a},\mathfrak{b}]\mathfrak{b}).$$

Now $\qquad [\mathfrak{a},\mathfrak{b}] \subseteq \mathfrak{b}$

so that $\qquad [\mathfrak{a},\mathfrak{b}]\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b}.$

Similarly, $\qquad [\mathfrak{a},\mathfrak{b}]\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}.$

Hence $\qquad [\mathfrak{a},\mathfrak{b}]\cdot(\mathfrak{a},\mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}.$ q.e.d.

<u>Theorem 2.16</u>

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

<u>Proof</u>:

From Theorem 2.12 we have

$$[\mathfrak{a},\mathfrak{b}] \supseteq \mathfrak{a}\mathfrak{b}.$$

From Theorem 2.15 we have

$$[\mathfrak{a},\mathfrak{b}] \subseteq \mathfrak{a}\mathfrak{b}.$$

Hence $\qquad [\mathfrak{a},\mathfrak{b}] = \mathfrak{a}\mathfrak{b}.$ q.e.d.

If $(\mathfrak{a},\mathfrak{b}) = \mathfrak{o}$, then $\mathfrak{a}$ and $\mathfrak{b}$ have no common divisor other than $\mathfrak{o}$, and we say that they are <u>coprime</u>.

<u>Theorem 2.17</u>

If $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ are coprime~~s~~ in pairs, then

$$[\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n] = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n.$$

<u>Proof</u>:

By Theorem 2.16 the result is true for $n = 2$. Assuming it to be true for $n-1$,

$$[\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{n-1}] = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1} .$$

By hypothesis,

$$(\mathfrak{a}_i , \mathfrak{a}_n) = \mathfrak{o} , \qquad (i = 1, 2, \ldots, n-1).$$

Hence by an obvious extension of Theorem 2.14 for the case $\mathfrak{d} = \mathfrak{o}$,

$$(\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1} , \mathfrak{a}_n) = \mathfrak{o} .$$

By Theorem 2.16, then

$$\begin{aligned}[\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n] &= [[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}], \mathfrak{a}_n] \\ &= [\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1} , \mathfrak{a}_n] \\ &= \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n .\end{aligned}$$

Hence the result follows by induction. q.e.d.

<u>Theorem 2.18</u>

If $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ and $\mathfrak{a} \supseteq \mathfrak{b}\mathfrak{c}$, then $\mathfrak{a} \supseteq \mathfrak{c}$.

<u>Proof</u>:

Let $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{d}$.

Then, by Theorem 2.14,

$$(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{d}.$$

By hypothesis, $\mathfrak{a} \supseteq \mathfrak{b}\mathfrak{c}$, so that $\mathfrak{a} = \mathfrak{d}$. Hence

$$\mathfrak{a} \supseteq \mathfrak{c} .$$

q.e.d.

An ideal having no proper divisor other than $\mathfrak{o}$ is called <u>irreducible</u>. An ideal $\mathfrak{p}$ with the property that $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ implies that $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$ is called <u>prime</u>.

Theorem 2.19

Every irreducible ideal is prime.

Proof:

Let $\mathfrak{p}$ be irreducible, and let $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$.

Let $$(\mathfrak{p}, \mathfrak{a}) = \mathfrak{c}.$$

Then $\mathfrak{c} \supseteq \mathfrak{p}$, so that either $\mathfrak{c} = \mathfrak{p}$ or $\mathfrak{c} = \mathfrak{o}$. If $\mathfrak{c} = \mathfrak{p}$, then $\mathfrak{p} \supseteq \mathfrak{a}$. If $\mathfrak{c} = \mathfrak{o}$, then $\mathfrak{p} \supseteq \mathfrak{b}$ by Theorem 2.18.

q.e.d.

Theorem 2.20

A sufficient condition that every ideal in $\mathfrak{S}$ have a finite basis, is that the Teilerkettensatz hold for ideals in $\mathfrak{S}$, that is, if $\mathfrak{a}_{i+1} \supset \mathfrak{a}_i$, then the sequence $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ must terminate.

Proof:

Let a_1 be any element of the ideal $\mathfrak{a}$. If $\mathfrak{a} = (a_1)$, then the result is true. If $\mathfrak{a} \neq (a_1)$, then there exists a_2 in $\mathfrak{a}$ but not in (a_1), so that

$$(a_1, a_2) \supset (a_1).$$

If $\mathfrak{a} \neq (a_1, a_2)$, then we can find a_3 in $\mathfrak{a}$ but not in (a_1, a_2), so that

$$(a_1, a_2, a_3) \supset (a_1, a_2).$$

Since this process gives rise to a sequence of proper divisors, it must terminate after a finite number of steps.

Hence we obtain a set of elements $a_1, a_2, \ldots, a_n$ of $\mathcal{S}$ such that

$$\mathfrak{a} = (a_1, a_2, \ldots, a_n).$$

q.e.d.

Unlike the case in rings, the Teilerkettensatz is not a necessary condition that every ideal have a finite basis. This is shown by the first example in the proof of Theorem 1.2. In fact here every ideal is a principal ideal.

3. Decomposition of ideals

In this section we make the following assumptions concerning the ideals of an ovum $\mathcal{S}$:

I. Teilerkettensatz: If $\mathfrak{a}_{i+1} \supset \mathfrak{a}_i$, then the sequence $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ terminates.

II. Every prime ideal is irreducible.

The final result to be obtained is the unique decomposition of every ideal into the product of mutually coprime, primary ideals (Theorem 3.4).

Postulate II is the converse of Theorem 2.19, so that we speak indiscriminately of prime ideals and irreducible ideals.

The following theorem depends only on the postulate I.

Theorem 3.1

If $\mathfrak{a}$ is any ideal, then there exists a finite number of distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

(i) $\mathfrak{p}_i \supseteq \mathfrak{a}$, $(i = 1, 2, \ldots, r)$

(ii) $\mathfrak{a} \supseteq \mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_r^{\alpha_r}$, $(\alpha_i > 0)$.

<u>Proof</u>:

If $\mathfrak{a}$ is itself prime, the result is evident. If $\mathfrak{a}$ is not prime, then there must exist ideals $\mathfrak{b}$ and $\mathfrak{c}$ such that

$$\mathfrak{a} \supseteq \mathfrak{b}\mathfrak{c}\ , \quad \mathfrak{a} \not\supseteq \mathfrak{b}\, , \quad \mathfrak{a} \not\supseteq \mathfrak{c}\, .$$

Here $\mathfrak{a} \not\supseteq \mathfrak{b}$ means that $\mathfrak{a}$ is not a divisor of $\mathfrak{b}$.

Setting
$$\mathfrak{b}' = (\mathfrak{a}, \mathfrak{b})$$
$$\mathfrak{c}' = (\mathfrak{a}, \mathfrak{c})$$

we note that $\mathfrak{b}' \supset \mathfrak{a}$, $\mathfrak{c}' \supset \mathfrak{a}$. By Theorem 2.10,

$$\mathfrak{b}'\mathfrak{c}' = (\mathfrak{a}^2, \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}),$$

and, since $\mathfrak{a}$ is a common divisor of $\mathfrak{a}^2, \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}$,

$$\mathfrak{a} \supseteq \mathfrak{b}'\mathfrak{c}'.$$

If both $\mathfrak{b}'$ and $\mathfrak{c}'$ have the desired property, then $\mathfrak{a}$ must have it. Hence if $\mathfrak{a}$ has it not, we can find a proper divisor of $\mathfrak{a}$ also not having it. Continuing thus we get an infinite sequence of proper divisors, in contradiction to I.

q.e.d.

An ideal $\mathfrak{q}$ with the property that $\mathfrak{q} \supseteq \mathfrak{a}\mathfrak{b}$ always implies that $\mathfrak{q} \supseteq \mathfrak{a}$ or else that $\mathfrak{q} \supseteq \mathfrak{b}^{\sigma}$, for some positive integer σ , will be called <u>primary</u>.

<u>Theorem 3.2</u>

A primary ideal is characterized by the property that it has only one prime ideal divisor other than $\mathfrak{o}$.

Proof:

Let $\mathfrak{q}$ be a primary ideal, and let distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be chosen as in Theorem 3.1 so that

$$\mathfrak{p}_i \supseteq \mathfrak{q} \quad , (i = 1, 2, \ldots, r);$$

$$\mathfrak{q} \supseteq \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} \quad , \quad (\alpha_i > 0).$$

Now $\qquad \mathfrak{q} \not\supseteq \mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_r^{\alpha_r},$

for otherwise

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_r^{\alpha_r},$$

contrary to the prime property of $\mathfrak{p}_1$, the condition II, and the fact that

$$\mathfrak{p}_1 \neq \mathfrak{p}_j \quad , \quad (j = 2, \ldots, r).$$

Hence $\mathfrak{q}$ must divide some power of $\mathfrak{p}_1^{\alpha_1}$, say

$$\mathfrak{q} \supseteq \mathfrak{p}_1^{\sigma\alpha_1}.$$

But then $\qquad \mathfrak{p}_j \supseteq \mathfrak{q} \supseteq \mathfrak{p}_1^{\sigma\alpha_1} \quad , \quad (j = 2, \ldots, r)$

and hence $\qquad \mathfrak{p}_j = \mathfrak{p}_1 .$

We thus conclude that $r = 1$, and $\mathfrak{p}_1$ the only prime divisor of $\mathfrak{q}$.

Let now $\mathfrak{q}$ have only the single prime divisor $\mathfrak{p} \neq \mathfrak{o}$. Then by Theorem 3.1 an integer σ exists such that

$$\mathfrak{q} \supseteq \mathfrak{p}^{\sigma}.$$

Suppose now that $\quad \mathfrak{q} \supseteq \mathfrak{a}\mathfrak{b}.$

If $\mathfrak{p} \not\supseteq \mathfrak{b}$, then $(\mathfrak{p}, \mathfrak{b}) = \mathfrak{o}$ by II, and hence by

Theorem 2.14, for the case $\mathfrak{d} = \mathfrak{o}$,

$$(\mathfrak{p}^{\sigma}, \mathfrak{b}) = \mathfrak{o}.$$

Consequently $$(\mathfrak{q}, \mathfrak{b}) = \mathfrak{o}$$

and, by Theorem 2.18, $$\mathfrak{q} \supseteq \mathfrak{a}.$$

If $\mathfrak{p} \supseteq \mathfrak{b}$, then $\mathfrak{p}^{\sigma} \supseteq \mathfrak{b}^{\sigma}$, and hence $\mathfrak{q} \supseteq \mathfrak{b}^{\sigma}$.

Thus either $\mathfrak{q} \supseteq \mathfrak{a}$ or else $\mathfrak{q} \supseteq \mathfrak{b}^{\sigma}$, and $\mathfrak{q}$ is therefore primary. q.e.d.

Theorem 3.3

If $\mathfrak{a}$ and $\mathfrak{b}$ have no prime divisor $\neq \mathfrak{o}$ in common, then

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

Proof:

Let $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$. Then $\mathfrak{c}$ has no prime divisor other than $\mathfrak{o}$, and hence by Theorem 3.1, $\mathfrak{c} = \mathfrak{o}$. q.e.d.

Theorem 3.4

Every ideal is uniquely representable as the product of mutually coprime, primary ideals.

Proof:

Let $\mathfrak{a}$ be any ideal $\neq \mathfrak{o}$, and let distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be chosen as in Theorem 3.1 so that

$$\mathfrak{p}_i \supseteq \mathfrak{a}, \qquad (i = 1, \ldots, r)$$

$$\mathfrak{a} \supseteq \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}, \quad (\alpha_i > 0).$$

Set $$\mathfrak{q}_i = (\mathfrak{a}, \mathfrak{p}_i^{\alpha_i}).$$

Clearly, $\mathfrak{p}_i$ is the only prime ideal divisor of $\mathfrak{q}_i$ other than $\mathfrak{o}$, and hence by Theorem 3.3

$$(\mathfrak{q}_i , \mathfrak{q}_j) = \mathfrak{o} \quad , \quad (i \neq j).$$

Hence, by Theorem 2.17,

$$[\mathfrak{q}_1 , \ldots , \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r .$$

On multiplying out the product

$$\mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r = (\mathfrak{a} , \mathfrak{p}_1^{\alpha_1})(\mathfrak{a} , \mathfrak{p}_2^{\alpha_2}) \cdots (\mathfrak{a} , \mathfrak{p}_r^{\alpha_r})$$

by means of Theorem 2.10, we see that each term in the resulting expression on the right is divisible by $\mathfrak{a}$. Hence

$$\mathfrak{a} \supseteq \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r .$$

But $\qquad \mathfrak{q}_i \supseteq \mathfrak{a} \quad , \quad (i = 1, \ldots , r)$

so that $\qquad \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r \supseteq \mathfrak{a} .$

Hence $\qquad \mathfrak{a} = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r .$

Since by Theorem 3.2 each $\mathfrak{q}_i$ is primary, this gives the desired representation. Suppose now that we have another such :

$$\mathfrak{a} = \mathfrak{q}_1' \mathfrak{q}_2' \cdots \mathfrak{q}_s' .$$

Since $\qquad \mathfrak{p}_1 \supseteq \mathfrak{q}_1' \mathfrak{q}_2' \cdots \mathfrak{q}_s'$

it follows that $\mathfrak{p}_1$ must divide one of the $\mathfrak{q}_j'$, say $\mathfrak{q}_1'$. By Theorem 3.2, $\mathfrak{p}_1$ is the only prime ideal divisor of $\mathfrak{q}_1'$. Hence $\mathfrak{p}_2$ must divide one of the remaining $\mathfrak{q}_j'$, say $\mathfrak{q}_2'$. Continuing in this fashion, we get $s = r$, and, by proper numeration,

$$\mathfrak{p}_i \supseteq \mathfrak{q}_i' \quad , \quad (i = 1, \ldots , r).$$

By Theorem 3.3, $(\mathfrak{q}_1', \mathfrak{q}_i) = \mathfrak{o}$, $(i = 2, \ldots, r)$.

Hence by Theorem 2.14,

$$(\mathfrak{q}_1', \mathfrak{q}_2 \cdots \mathfrak{q}_r) = \mathfrak{o}.$$

But $\mathfrak{q}_1' \supseteq \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r$.

Hence, by Theorem 2.18,

$$\mathfrak{q}_1' \supseteq \mathfrak{q}_1 .$$

Similarly we can show that

$$\mathfrak{q}_1 \supseteq \mathfrak{q}_1' ,$$

whence $\mathfrak{q}_1 = \mathfrak{q}_1'$.

Likewise, $\mathfrak{q}_i = \mathfrak{q}_i'$, $(i = 2, \ldots, r)$

and hence the representation is unique. q.e.d.

4. Ideal theory for regular ova.

In the present section $\mathcal{S}$ will denote a regular ovum. If we construct formally quotients $\frac{a}{b}$ from $\mathcal{S}$, and operate with them as with ordinary fractions, we obtain an abelian group, which we shall call the quotient-group of $\mathcal{S}$, and which we shall denote by Σ . Since this is a well-known process we shall only very briefly give the steps involved.

We say that $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. The relation $=$ thus defined is found to be reflexive, symmetric, and transitive.

The product of two fractions is defined thus:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} .$$

We readily see that if $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$, then

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'} .$$

We then show that Σ is an abelian group with respect to = and $\cdot$ thus defined.

The subset $\frac{a}{i}$, where i is the identity element of $\mathcal{S}$, is simply isomorphic with $\mathcal{S}$, and so may be "identified" with $\mathcal{S}$ by passing to a whole new system isomorphic with $\mathcal{S}$.

The elements of Σ will be denoted by small Greek letters.

An element α of Σ is said to <u>divide</u> an element ζ of Σ , relative to $\mathcal{S}$, if the equation

$$\alpha x = \zeta$$

has a solution x in $\mathcal{S}$. We then write $\alpha \mid \zeta$. This relation is plainly transitive and reflexive.

The class of common divisors of a subclass A of Σ will be denoted by $\Delta(A)$. A will be called an $\mathcal{S}$ -module if it includes every subclass B of Σ having the property that

$$\Delta(B\xi) \supseteq \Delta(A\xi)$$

for every ξ in Σ . This is equivalent to saying that

$$\Delta(Bx) \supseteq \Delta(Ax)$$

for every x in $\mathcal{S}$.

For if we put $\xi = \frac{x}{y}$ and if α be in $\Delta(A\xi)$ then αy is in $\Delta(Ax)$. Hence αy is in $\Delta(Bx)$ and α is in $\Delta(B\xi)$.

We can carry over the whole of the theory of ideals as presented in §2 to $\mathcal{S}$-modules. Since the set of ideals of $\mathcal{S}$ is a subclass of the set of $\mathcal{S}$-modules, it is permissable to multiply an ideal by an $\mathcal{S}$-module. $\mathcal{S}$-modules will be denoted by small German letters with a tilde, as $\tilde{\mathfrak{a}}$, unless otherwise designated.

The purpose of the present section is to show that the following three conditions are necessary and sufficient that the system of ideals in $\mathcal{S}$ constitute a regular arithmetic:

I. Teilerkettensatz: If $\tilde{\mathfrak{a}}_{i+1} \supset \tilde{\mathfrak{a}}_i$, then the sequence $\tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_2, \ldots$ must terminate.

II. Every prime ideal is irreducible.

III. $\mathcal{S}$ is integrally closed in Σ .

The meaning of III is that if α in Σ is such that a exists in $\mathcal{S}$ such that $a\alpha^n$ is in $\mathcal{S}$ for every positive integer n , then α is in $\mathcal{S}$.

<u>Theorem 4.1</u>

If $\mathcal{S}$ contains every element ρ of Σ with the property that $\rho\tilde{\mathfrak{a}} \subseteq \mathfrak{a}$, then $\tilde{\mathfrak{a}} = \mathfrak{a}$, and conversely.

<u>Proof</u>:

Evidently $\Delta(x) = \Delta(\mathfrak{a} x)$, so that by Theorem 2.1 it suffices to show that

$$\Delta(\mathfrak{a}x) \subseteq \Delta(x).$$

For then $\mathfrak{a} \supseteq \mathfrak{o}$, whence $\mathfrak{a} = \mathfrak{o}$.

Let d be in $\Delta(\mathfrak{a}x)$, so that d/ax for every a in $\mathfrak{a}$. Set $\rho = \frac{x}{d}$. Then ρa is in $\mathcal{S}$ for all a in $\mathfrak{a}$, that is, $\rho\mathfrak{a} \subseteq \mathfrak{o}$. Hence by hypothesis ρ is in $\mathcal{S}$, so that d/x , and

$$\Delta(\mathfrak{a}x) \subseteq \Delta(x).$$

To prove the converse we note that if $\rho\mathfrak{o} \subseteq \mathfrak{o}$, then $\rho i = \rho$ is in $\mathfrak{o}$. q.e.d.

<u>Theorem 4.2</u>

If $\mathfrak{a}$ be any ideal, then the class P of elements ρ of Σ such that

$$\rho\mathfrak{a} \subseteq \mathfrak{o}$$

is an $\mathcal{S}$-module.

<u>Proof</u>:

Let δ be any element of Σ such that δx is divisible by every member of $\Delta(Px)$. Then δa is divisible by every member of $\Delta(Pa)$, for each a in $\mathfrak{a}$. Since all the members of Pa are in $\mathcal{S}$, the element i occurs in $\Delta(Pa)$. Hence δa is divisible by i , that is, δa is in $\mathcal{S}$.

Hence, by definition of P , δ is in P . P is consequently an $\mathcal{S}$-module. q.e.d.

The $\mathcal{S}$-module defined by Theorem 4.2 for an ideal $\mathfrak{a}$, will be denoted by $\mathfrak{a}^{-1}$.

Theorem 4.3

If $\mathfrak{a} \neq \mathfrak{o}$, then $\mathfrak{a}^{-1}$ contains an element ρ of Σ not in $\mathcal{S}$.

Proof:

If every element of $\mathfrak{a}^{-1}$ were in $\mathcal{S}$, then, by definition of $\mathfrak{a}^{-1}$, $\mathcal{S}$ would contain every element ρ of Σ with the property that $\rho\,\mathfrak{a} \subseteq \mathfrak{o}$. Hence by Theorem 4.1, $\mathfrak{a} = \mathfrak{o}$, contrary to hypothesis. q.e.d.

Theorem 4.4

For every prime ideal $\mathfrak{p}$, $\mathfrak{p}\,\mathfrak{p}^{-1} = \mathfrak{o}$.

Proof:

Since
$$\mathfrak{p}^{-1} \supseteq \mathfrak{o}$$
we have
$$\mathfrak{o} \supseteq \mathfrak{p}\,\mathfrak{p}^{-1} \supseteq \mathfrak{p}.$$

Hence by II, $\mathfrak{p}\,\mathfrak{p}^{-1} = \mathfrak{p}$ or $\mathfrak{p}\,\mathfrak{p}^{-1} = \mathfrak{o}$.

If $\mathfrak{p}\,\mathfrak{p}^{-1} = \mathfrak{p}$, then
$$\mathfrak{p} = \mathfrak{p}\,\mathfrak{p}^{-1} = \mathfrak{p}(\mathfrak{p}^{-1})^2 = \cdots = \mathfrak{p}(\mathfrak{p}^{-1})^n = \cdots$$

Hence if a be any element of $\mathfrak{p}$, and α any element of $\mathfrak{p}^{-1}$, the elements $a\alpha^n$ of Σ lie in $\mathfrak{p}$. Consequently, by III, α is in $\mathcal{S}$.

Thus we conclude that every element of $\mathfrak{p}^{-1}$ is in $\mathcal{S}$, in contradiction to Theorem 4.3.

Hence $$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o} .$$ q.e.d.

Theorem 4.5

Every ideal is representable as the product of a finite number of prime ideals.

Proof:

Let $\mathfrak{a}$ be any ideal. Then by Theorem 3.1 there exists a set $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of prime ideal divisors of $\mathfrak{a}$, not all necessarily distinct, such that

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r .$$

Choose a set with this property, and such that r is as small as possible.

If $r = 1$, then $\mathfrak{p}_1 \supseteq \mathfrak{a} \supseteq \mathfrak{p}_1$, and $\mathfrak{a} = \mathfrak{p}_1$. Assume the result to be true for all ideals for which $r-1$ primes can be found with the above property. Then if $\mathfrak{a}$ require exactly r primes at least, we have

$$\mathfrak{p}_1 \supseteq \mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r .$$

Multiplying by $\mathfrak{p}_1^{-1}$ and using Theorem 4.4,

$$\mathfrak{o} \supseteq \mathfrak{a}\mathfrak{p}_1^{-1} \supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r .$$

Hence $\mathfrak{a}\mathfrak{p}_1^{-1}$ is an ideal (since it is an $\mathcal{S}$ -module included in $\mathfrak{o}$), admitting the result of Theorem 3.1 for $r-1$ primes. By hypothesis for induction

$$\mathfrak{a}\mathfrak{p}_1^{-1} = \mathfrak{p}_2' \cdots \mathfrak{p}_s'$$

Multiplying by $\mathfrak{p}_1$,

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2' \cdots \mathfrak{p}_s' .$$

q.e.d.

<u>Theorem 4.6</u>

If $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{p}_1' \cdots \mathfrak{p}_s'$, and $\mathfrak{b} \supseteq \mathfrak{a}$, then every prime ideal $\neq \mathfrak{o}$ occurring in the representation of $\mathfrak{b}$ occurs in that of $\mathfrak{a}$, and in fact at least as often.

<u>Proof</u>:

The theorem is trivial for $\mathfrak{b} = \mathfrak{o}$. Hence we can assume $s > 0$ and $\mathfrak{p}_1' \neq \mathfrak{o}$.

Since $\mathfrak{p}_1' \supseteq \mathfrak{b} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ we have from the prime property of $\mathfrak{p}_1'$ that $\mathfrak{p}_1'$ must divide one of the $\mathfrak{p}_i$, say $\mathfrak{p}_1$. Using II, we infer that

$$\mathfrak{p}_1' = \mathfrak{p}_1 .$$

Multiplying the relation

$$\mathfrak{p}_1' \cdots \mathfrak{p}_s' \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

by $\mathfrak{p}_1^{-1}$, we get

$$\mathfrak{p}_2' \cdots \mathfrak{p}_s' \supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r .$$

The theorem is evidently true for $s = 1$, as the result

$$\mathfrak{p}_1' = \mathfrak{p}_1$$

shows. Assuming it to be true for all products $\mathfrak{b}$ of less than s primes, then $\mathfrak{p}_2', \ldots, \mathfrak{p}_s'$ all occur among the primes $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, repeated ones occurring at least as frequently. Hence the same result holds when we adjoin $\mathfrak{p}_1'$ to the former set, and its equal $\mathfrak{p}_1$ to the latter. q.e.d.

Combining Theorems 4.5 and 4.6 we have immediately:

Theorem 4.7

Every ideal is uniquely representable as the product of a finite number of primes, the multiplicity of each prime being uniquely determined.

Theorem 4.8

If $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, then $\mathfrak{b} = \mathfrak{c}$.

[An immediate consequence of Theorem 4.7.]

Theorem 4.9

If $\mathfrak{a} \geq \mathfrak{b}$, then $\mathfrak{c}$ exists such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$.

Proof:

Define $\mathfrak{c}$ to be the product of those primes in the representation of $\mathfrak{b}$ which are left after those in the representation of $\mathfrak{a}$ have been removed. The result is then clear.

q.e.d.

Theorem 4.10

The conditions I, II, III for a regular ovum $\mathcal{S}$ are equivalent to the following conditions:

IV. Every ideal in $\mathcal{S}$ is uniquely representable as the product of a finite number of prime ideals.

V. If $\mathfrak{a} \supseteq \mathfrak{c}$ then $\mathfrak{b}$ exists such that $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$.

VI. If $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, then $\mathfrak{b} = \mathfrak{c}$. [This is a consequence of IV if we assume that multiplicities are uniquely determined.]

Proof:

I follows on converting the usual Teilerkettensatz for an arithmetic to the Teilerkettensatz for ideals by means of V.

II follows from the fact that $\mathfrak{p} = \mathfrak{p}$ is the unique representation of a prime $\mathfrak{p}$, so that it can have no proper divisor $\neq \mathfrak{p}$.

It remains now to show III. Let α be an element of Σ with the property that a exists in $\mathcal{S}$ such that $a\alpha^n$ is in $\mathcal{S}$ for every positive integer n. We are to show that α lies in $\mathcal{S}$.

Let $\mathfrak{a}$ be the ideal generated by the elements $a, a\alpha, a\alpha^2, \ldots$ of $\mathcal{S}$:

$$\mathfrak{a} = (a, a\alpha, a\alpha^2, \ldots).$$

Then

$$\mathfrak{a}^2 = (a^2, a^2\alpha, a^2\alpha^2, \ldots)$$

$$= (a)(a, a\alpha, a\alpha^2, \ldots)$$

$$= (a)\mathfrak{a}.$$

Using VI,

$$\mathfrak{a} = (a).$$

Consequently $a / a\alpha$, so that $1 / \alpha$, and α is in $\mathcal{S}$.

q.e.d.

Theorem 4.11

If $\mathfrak{a}$ be any ideal, then an ideal $\mathfrak{b}$ and a principal ideal (c) exist such that $\mathfrak{a}\mathfrak{b} = (c)$.

Proof:

We need only take c to be an element of $\mathfrak{a}$. Then $\mathfrak{a} \supseteq (c)$ and the result follows from V.

q.e.d.

We shall conclude this section with a brief account of fractional ideals. By a fractional ideal $\breve{\mathfrak{a}}$ we mean an $\mathcal{S}$-module for which b exists in $\mathcal{S}$ such that $b\breve{\mathfrak{a}}$ is an ideal.

Theorem 4.12

Necessary and sufficient for $\breve{\mathfrak{a}}$ to be a fractional ideal is that $\breve{\mathfrak{a}}$ have a finite basis.

Proof: If $\breve{\mathfrak{a}} = (\alpha_1, \ldots, \alpha_n)$

then by multiplying by the product b of the denominators of the α_i we see that $b\breve{\mathfrak{a}} \subseteq \mathfrak{o}$.

Conversely, if $b\breve{\mathfrak{a}}$ is an ideal, then by Th 2.20 and I it has a finite basis:

$$b\breve{\mathfrak{a}} = (a_1, \ldots, a_n).$$

Hence
$$\breve{\mathfrak{a}} = \left(\frac{a_1}{b}, \ldots, \frac{a_n}{b}\right).$$

q.e.d.

Theorem 4.13

If $\mathfrak{a}$ is any ideal, then $\mathfrak{a}^{-1}$ is a fractional ideal.

Proof:

If a is any element of $\mathfrak{a}$, then $a\mathfrak{a}^{-1} \subseteq \mathfrak{o}$.

q.e.d.

Theorem 4.14

The set of fractional ideals in Σ forms an abelian group with respect to multiplication.

Proof:

If $a\breve{\mathfrak{a}} \subseteq \mathfrak{o}$, $b\breve{\mathfrak{b}} \subseteq \mathfrak{o}$, then $(ab)(\breve{\mathfrak{a}}\breve{\mathfrak{b}}) \subseteq \mathfrak{o}$; hence the closure property. The associative and commutative laws and the existence of identity are clear.

Let $\breve{\mathfrak{c}}$ be any fractional ideal, so that b exists in S such that $b\breve{\mathfrak{c}} = \mathfrak{a} \subseteq \mathfrak{o}$. By IV,

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r .$$

By Theorem 4.13, $\mathfrak{p}_1^{-1}, \dots, \mathfrak{p}_r^{-1}$ are fractional ideals. Since

$$\mathfrak{a}\,\mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1} = \mathfrak{o}$$

we see that $\breve{\mathfrak{c}}$ has the inverse

$$\breve{\mathfrak{c}}^{-1} = b\,\mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1} .$$

Hence the set is an abelian group. q.e.d.

We shall denote $\mathfrak{a}\mathfrak{b}^{-1}$ by $\dfrac{\mathfrak{a}}{\mathfrak{b}}$.

Theorem 4.15

The group of fractional ideals is the quotient-group of the ovum of ideals in S. Every fractional ideal $\breve{\mathfrak{a}}$ is representable in the form

$$\breve{\mathfrak{a}} = \frac{\mathfrak{b}}{\mathfrak{c}} = \frac{\mathfrak{p}_1\cdots\mathfrak{p}_r}{\mathfrak{p}_1'\cdots\mathfrak{p}_s'} ,$$

where $\mathfrak{b}$ and $\mathfrak{c}$ are coprime, and the sets $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, $\{\mathfrak{p}_1', \ldots, \mathfrak{p}_s'\}$ have no element in common.

Proof:

Since c exists in S such that $c\,\mathfrak{a} = \mathfrak{b} \subseteq \mathfrak{o}$ we have that

$$\mathfrak{a} = \frac{\mathfrak{b}}{\mathfrak{c}}$$

where $\mathfrak{c} = (c) \subseteq \mathfrak{o}$.

If now we represent $\mathfrak{b}$ and $\mathfrak{c}$ as the product of primes, and cancel those occurring in both numerator and denominator, we get the desired representation.

q.e.d.

5. Criteria for unique decomposition in terms of ideals.

In this section we show that the condition that every irreducible element be completely prime, occurring in the criteria for unique decomposition (Theorem 1.1), can be replaced by the condition that every ideal be a principal ideal. The fact that, unlike the case of principal ideals in ring theory, this condition is necessary, points to the conclusion that ovoid ideals have a more intimate connection with the multiplicative properties of the ovum or ring than do ring ideals. For example, in the ring $C[x]$ of polynomials with integer coefficients every ovoid ideal is a principal ideal, whereas polynomial ideals are notoriously lacking in the usual properties of an arithmetic. Ovoid ideals, however, are not presumed to have the interesting additive properties of ring ideals, nor the utility of polynomial ideals in the study of algebraic manifolds.

As a matter of fact, every ovoid ideal defined for a ring R is also a ring ideal, though not conversely. Since $\mathfrak{a}R = \mathfrak{a}$, ax is in $\mathfrak{a}$ for every a in $\mathfrak{a}$ and every x in R. If a_1 and a_2 are in $\mathfrak{a}$, then $(a_1 \pm a_2)x$ is divisible by every common divisor of the set $\mathfrak{a}x$ (since $a_1 x$ and $a_2 x$ are). Hence $\mathfrak{a}$ is closed under addition and subtraction, and under multiplication by any element of R. As an example of a ring ideal which is not an ovoid ideal we have $(2, x)$ in the ring $C[x]$. Since $f(x)$ is divisible by every common divisor of $2f(x)$ and $xf(x)$, the element 1 should occur in $(2, x)$, which it does not.

To every ring ideal there corresponds a unique ovoid ideal, namely that generated by any generator of the ring ideal, including the ring ideal itself. As we have noted, the correspondence is many-one. It is, moreover, an isomorphism. Hence the arithmetic of ring ideals is multiply isomorphic to that of ovoid ideals.

Turning now to the matter of principal ideals in an ovum S, we ask, what is the significance of the equation

$$(a, b) = (c),$$

where a, b, c are elements of S? It must be remarked that it means decidedly more than that c be the G. C. D. of a and b. It says that for every x in S, cx is the G.C.D.

of ax and bx. The same is ~~ture~~ true for ring ideals, since then c is a linear combination of a and b. Thus the above relation is in a sense a generalization to an ovum of the notion of a linear function in a ring. This is borne out by the way ovoid ideals multiply:

$$(a, b)(c, d) = (ac, bc, ad, bd).$$

See also the remark after Theorem 5.2.

If we replace the ideals in Theorem 2.14 by principal ideals, we obtain the following:

<u>Theorem 5.1</u>

If $(a, b) = (i)$ and $(a, c) = (i)$, then

$$(a, bc) = (i).$$

<u>Theorem 5.2</u>

If $(a, b) = (i)$ then a / bc implies a / c.

<u>Proof</u>:

If $(a, b) = (i)$ then every common divisor of ax and bx is a divisor of x. If a / bc, then a is a common divisor of ac and bc, whence a / c.

q.e.d.

This simple but fundamental result shows that $(a, b) = (i)$ is the proper generalization of the notion of "linearly coprime" elements, i.e. elements a and b such that $ra + sb = 1$.

Theorem 5.3

Necessary and sufficient conditions for unique decomposition into irreducibles in a reduced ovum are:

I. Teilerkettensatz (as in Theorem 1.1).

II. Every reducible element is decomposable (as in Theorem 1.1).

III. Every ideal is a principal ideal.

Proof of Sufficiency

We have to show that III implies that every irreducible element be completely prime.

Let p be an irreducible element, and let

$$p^r / ab.$$

Let
$$(a, p) = (d).$$

Since d / p and p is irreducible, either $d = p$ or $d = i$.

.

If $d = p$, then p / a .

If $d = i$, then by a successive application of Theorem 5.1,

$$(a, p^r) = (i).$$

Hence by Theorem 5.2,

$$p^r / b.$$

Hence either p / a or p^r / b, so that p is completely prime. q.e.d.

__Proof__ __of__ __Necessity__.

Let a and b be any two elements of $\mathcal{S}$, and let $p_1, \ldots, p_r$ be the irreducibles occurring in the decompositions of a and b*. Let

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

where some of the α_i or β_i may be zero, but where none exceeds the index of the corresponding p_i. The element

$$c = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$$

where

$$\gamma_i = \min(\alpha_i, \beta_i), \quad (i = 1, \ldots, r),$$

is evidently the G.C.D. of a and b.

Let x be an arbitrary element of $\mathcal{S}$, and let

$$x = p_1^{\xi_1} \cdots p_r^{\xi_r}.$$

Then since

$$\gamma_i + \xi_i = \min(\alpha_i + \xi_i, \beta_i + \xi_i),$$

it follows that $cx = p_1^{\gamma_1 + \xi_1} \cdots p_r^{\gamma_r + \xi_r}$

is the G.C.D. of

$$ax = p_1^{\alpha_1 + \xi_1} \cdots p_r^{\alpha_r + \xi_r}$$

and

$$bx = p_1^{\beta_1 + \xi_1} \cdots p_r^{\beta_r + \xi_r}.$$

Hence $(a, b) = (c)$.

* and of the arbitrary element x below.

Let now $\mathfrak{A}$ be any ideal. Let a_1 be any element of $\mathfrak{A}$. If

$$\mathfrak{A} = (a_1)$$

then the desired result is true. If not, then b_1 exists in $\mathfrak{A}$ but not in (a_1). Let

$$(a_2) = (a_1, b_1).$$

Then $a_2 \,//\, a_1$, for if $a_2 = a_1$ then $a_1 \mid b_1$, and b_1 would be in (a_1). Evidently a_2 is in $\mathfrak{A}$.

If $$\mathfrak{A} = (a_2)$$

then the desired result is true. If not, then a_3 exists in $\mathfrak{A}$ such that $a_3 \,//\, a_2$.

But I is a consequence of unique decomposition, so that this process must terminate, and $\mathfrak{A} = (a_n)$ for some integer n.

q.e.d.

This theorem gives the correct generalization of Koenig's Theorem 1.4. It has already been noted that III is equivalent to the following two postulates:

III_1: Every pair a, b of elements of S has a G.C.D. (a, b).

III_2: $(a, b)c = (ac, bc)$ for all a, b, c in S.

The third example in the proof of Theorem 1.2 illustrates the necessity of III_2. It satisfies I, II, and III_1, but not III_2. For i is the G.C.D. of p and q, but x is not the G.C.D.

of px and qx for all x . For example, put $x = p$: the G.C.D. of $p^2 = 0$ and $qp = 0$ is 0 , not p .

It should be remarked that, unlike the case in rings, I is not a consequence of III. The first example in the proof of Theorem 1.2 illustrates this. See also the remark at the end of § 2.

Applying this result to that of Theorem 1.5 we get the following:

Theorem 5.4

Necessary and sufficient conditions that every element of a commutative ring $\mathcal{R}$ be uniquely decomposable into irreducibles are:

I. Teilerkettensatz (as in Theorem 1.5).

II. Vielfachenkettensatz (as in Theorem 1.5).

III. Every pair a, b of elements of $\mathcal{R}$ has a G.C.D., (a, b), in $\mathcal{R}$.

IV. $(a, b)c = (ac, bc)$ for all a, b, c in $\mathcal{R}$.