FINITE OVA

THESIS

by

A.R. Poole

In Partial Fulfillment of the Requirements for

the Degree of Doctor of Philosophy,

California Institute of Technology,

Pasadena, California,

1935.

FINITE OVA

Introduction.

In this thesis systems consisting of a finite number of elements and one binary commutative associative rule of combination are considered. Such systems are called ova. The distinctness of ova is first discussed. The elements of ova are then classified acoording to their behavior when raised to powers. A necessary and sufficient condition that an ovum have no associate elements is found, and ova having no associate elements are discussed in detail. A necessary and sufficient condition that an ovum be a finite Abelian group is also found. All the distinct ova of orders 2,3,4, have been computed and are listed in the course of the paper. There are 3 distinct ova of order 2, 12 of order3, and 56 of order 4. All concepts introduced in the discussion are illustrated in these ova.

Before passing to the detailed develop~~e~~ment of the theory I wish here to express my thanks to Professor E. T. Bell for his helpful suggestions in the course of the preparation of this thesis.

FINITE COMMUTATIVE ASSOCIATIVE MARK OVA

The concepts assumed for a finite mark ovum are:

1. A finite set U of distinct marks $(u_1, u_2, \ldots, u_n)$.

2. A binary rule of combination which to each double mark $u_i u_j$ formed from any ordered pair of marks of U, and to each mark u_i^2 formed from any mark of U, associates or makes correspond a unique mark of U.

We call the rule of combination multiplication. If to $u_i u_j$ is associated u_k, we write $u_i u_j = u_k$, or $u_k = u_i u_j$. We say that u_k is equal to the product of u_i and u_j in that order. If to u_i^2 is associated u_k, we write $u_i^2 = u_k$ or $u_k = u_i^2$, and say that u_k is equal to the product of u_i by itself, or to u_i squared.
Having thus by postulation established the possibility of forming the product of ordered pairs of elements of U, and the product of an element of U by itself, we define the mark $u_i(u_j u_k)$ to be the product of u_i by the product of u_j and u_k. We define the mark $u_i^2 u_j$ to be the product of the product of u_i by itself by u_j. In a similar manner we define the marks $u_i(u_i u_j)$ and $(u_i u_j)u_k$.

Thus we establish a correspondence between the compound marks of the above forms and the marks of U. If two of these compound marks correspond to the same mark of U, we say that they are equal to one another, and conversely equality of such marks only has this significance.

For a finite commutative associative mark ovum we further postulate:

3. For each pair of marks u_i and u_j of U, $u_i u_j = u_j u_i$.

4. For each pair of marks u_i and u_j of U, $u_i^2 u_j = u_i(u_i u_j)$.

5. For each triad of marks u_i, u_j, and u_k of U,

$$u_i(u_j u_k) = (u_i u_j)u_k.$$

From 3, 4, and 5 it follows * that in a finite commutative associative ovum we can form the product of any number $r \leq n$ of marks $(u_{i_1}, \ldots, u_{i_r})$ of U, any integral power p of a mark u_i of U, and the product of integral powers $a_1, \ldots, a_q$, of marks $u_{i_1}, \ldots, u_{i_q}$, $q \leq n$, of U, and that these products will be unique and will depend only on the elements which occur and the powers to which they occur, and not on the order in which the products are formed. We use the marks $u_{i_1} u_{i_2} \ldots u_{i_r}$, u_i^p, and $u_{i_1}^{a_1} u_{i_2}^{a_2} \ldots u_{i_q}^{a_q}$ to indicate these respective products.

We thus have a correspondence between any compound mark of the form $u_{i_1}^{a_1} u_{i_2}^{a_2} \ldots u_{i_q}^{a_q}$, $(q \leq n)$, where $a_1, \ldots, a_q$ are integers, and the marks of U. If such a compound mark corresponds to u_k, we write $u_{i_1}^{a_1} u_{i_2}^{a_2} \ldots u_{i_q}^{a_q} = u_k$. Two such compound marks are said to be equal when and only when they correspond to the same mark of U.

The set of marks $(u_1, u_2, \ldots, u_n)$ of a finite mark ovum will be called the mark set of the ovum. The number of marks in the set will be called the order of the ovum, and the marks will be called the elements of the ovum.

Concept 2 implies that for every finite mark ovum there are n relations giving products u_i^2, and n(n-1) relations giving products $u_i u_j$. These n^2 relations will be called the multiplication table of the ovum.

* Van der Waerden, Moderne Algebra p. 20-22.

A finite mark ovum is ,then, completely determined by its mark set and its multiplication table. It can be conveniently pictured as a square matrix of order n, where the element in the i^{th} row and j^{th} column is equal to the product $u_i u_j$,and the diagonal elements are equal to the squares of the elements of the ovum. It must be remembered, however, that by the multiplication table of the ovum we mean the n^2 relations mentioned above,and not the square matrix itself.

SIMPLE ISOMORPHISMS OF MARK OVA.

Two mark ova which have the same mark set will be said to be simply isomorphic to each other if and only if the multiplication table of one can be obtained from that of the other by a permutation of the elements of the mark set.

Example: The ova A
$$\begin{matrix} u_1 u_1 u_3 u_2 \\ u_4 u_2 u_1 u_3 \\ u_2 u_3 u_1 u_1 \\ u_4 u_1 u_3 u_2 \end{matrix}$$
and B
$$\begin{matrix} u_1 u_3 u_1 u_4 \\ u_2 u_3 u_1 u_4 \\ u_2 u_4 u_3 u_1 \\ u_3 u_1 u_4 u_1 \end{matrix}$$
are simply isomorphic to one another. The substitution taking the multiplication table of A into that of B is $\begin{pmatrix} u_1 u_2 u_3 u_4 \\ u_1 u_3 u_4 u_2 \end{pmatrix}$ or, written as a permutation on the subscripts, is (234).

Two mark ova of order n with different mark sets $(u_1, u_2, \ldots, u_n)$ and $(v_1, v_2, \ldots, v_n)$ will be said to be simply isomorphic if when every v_i is replaced by u_i

$(i=1,\ldots,n)$ the two mark ova with the set $u_1,\ldots,u_n$, are simply isomorphic. Mark ova which are not simply isomorphic will be said to be distinct.

In this discussion we will henceforth be treating only finite commutative associative mark ova, and will for brevity designate such systems merely as ova. It is evident that due to the commutative property of the ova the matrices representing them will be symmetric.

POWERS OF ELEMENTS IN OVA.

Consider the chain of elements obtained by taking successive powers $u_i, u_i^2, u_i^3, \ldots, u_i^v, \ldots$ of an element of an ovum. Due to the finite order of the ovum the successive powers can not be all distinct. Let the p^{th} power be the first one which gives an element previously occurring in the chain, and suppose $u_i^p = u_i^r$. Let $p-r=s$, so that we have $u_i^{r+s} = u_i^r$. There are four possibilities:

1.	$r=1$	$s=1$
2.	$r>1$	$s=1$
3.	$r=1$	$s>1$
4.	$r>1$	$s>1$

Idempotent Elements.

If u_i is an element which comes under case 1 above,

$$u_i^2 = u_i$$

then u_i will be called an idempotent element. Evidently then all powers of u_i are equal to u_i.

Elements of Type a.

If u_i is an element which comes under case 2 above, we shall call u_i an element of type a.

We have $u_i, u_i^2, u_i^3, \ldots, u_i^r$, distinct and $u_i^{r+1} = u_i^r$. Hence all powers greater than r of u_i are equal to u_i^r. The integer r will be called the index of the element u_i and if $u_i^r = u_k$, we shall call u_k the index element of u_i. Since $u_k^2 = u_i^{2r} = u_i^r = u_k$, u_k is an idempotent element. Moreover it is the only idempotent element occurring in the chain of powers of u_i.

For, let t be any integer less than r and let

$$u_i^t = u_j .$$

Then

$$u_j^s = u_k$$

for all integers s for which $s\,t \geq r$. Let s_1 be the least s for which $s\,t \geq r$. Then $s_1 > 1$ and

$$u_j, u_j^2, \ldots, u_j^{s_1 - 1}$$

are distinct and all higher powers of u_j are equal to u_k. So u_j is an element of type a with index element u_k. Hence we see that if u_i is an element of type a of index r and index element u_k, then u_i^t $(t = 1, \ldots, r-1)$ are elements of type a with index element u_k and indices less than r.

Elements of type b.

If u_i is an element which comes under case 3 above,

u_i will be called an element of type b.

We then have

$$u_i, u_i^2, \dots, u_i^s$$

distinct, and

$$u_i^{s+1} = u_i$$

We shall call s the period of the element u_i.

Evidently $$u_i^{s+t} = u_i^t \qquad (t \geq 1),$$

and in particular

$$u_i^{2s} = u_i^s$$

so we see that u_i^s is an idempotent element.

If $u_i^s = u_k$, we shall call u_k the period element of u_i.

We show that u_k is the only idempotent element occurring in the chain of powers of u_i.

For if $h \leq s/2$, u_i^h can not be an idempotent element, since $u_i, u_i^2, \dots, u_i^s$ are distinct. If $s > h > s/2$, and u_i^h is an idempotent element, then

$$u_i^{2h} = u_i^h$$

But since $2h > s$,

$$u_i^{2h} = u_i^{2h-s}$$

so

$$u_i^{2h-s} = u_i^h$$

However, $2h-s < h$ and so u_i^{2h-s} precedes u_i^h in the chain of powers and so can not equal u_i^h. Hence we have a contradiction, so that u_i^h, $h < s$ can not be an idempotent element.

For $p > s$, if p is not a multiple of s we have $p = st + q$, $q < s$ and

$$u_i^p = u_i^{st+q} = u_i^q$$

Hence u_i^p is not an idempotent element.

If $p > s$ and p is a multiple of s, say $p = ts$

we have $$u_i^p = u_i^{ts} = u_k$$

Hence u_k is the only idempotent element in the chain of powers of u_i.

Now let $t < s$ and let $$u_i^t = u_j$$

Let h be an integer such that sh is a multiple of t.

Then if $k = 1 + sh/t$ we have

$$u_j^k = u_i^{t+sh} = u_i^t = u_j$$

and since u_j is not an idempotent element it must be an element of type b.

Also $$u_j^{k-1} = u_i^{sh} = u_k$$

Hence every element u_i^t, $t < s$, is an element of type b and has the same period element u as u_i.

Elements of Type c.

If u_i is an element which comes under case 4 of the above, we call u_i an element of type c.

We then have $$u_i, u_i^2, \ldots, u_i^r, \ldots, u_i^{r+s-1}$$

distinct, and $$u_i^{r+s} = u_i^r$$

whence for an integer $p \geq r$ and h any integer

$$u_i^{p+hs} = u_i^p$$

We will call r the index and s the period of the element u_i.

The elements $u_i, u_i^2, \ldots, u_i^{r-1}$ form the unrepeated part of the chain of powers of u_i, the elements $u_i^{r}, \dots, u_i^{r+s-1}$ form the repeated part of the chain.

Let m be the least integer such that $ms \geq r$.

Then $$(u_i^{ms})^2 = u_i^{ms+ms} = u_i^{ms}$$

so that u_i^{ms} is an idempotent element.

If $$u_i^{ms} = u_k$$

then u_k will be called the period element of u_i.

We show that u_k is the only idempotent element occurring in the chain of powers of u_i.

Let t be any integer less than r and let $u_i^{t} = u_j$

Then since u_j occurs in the unrepeated part of the chain of u_i, u_j cannot be an idempotent element or an element of type b. Hence it must be a type a or a type c element and it is easy to see that it is a type a element if and only if s is a divisor of t.

Now let t be an integer such that $r \leq t < r+s$ and let t not be a multiple of s. If $u_j = u_i^{t}$

then $$u_j^{s+1} = u_i^{ts+t} = u_i^{t} = u_j$$

So u_j is either an idempotent element of a type b element.

If now u_j were an idempotent element we would have
$$u_i^{2t} = u_i^{t}$$

whence $2t = t + ks$ where k is some integer, or $t = ks$. But this is in contradiction to the fact that t was not a multiple of s. So u_j is a type b element.

We thus see that the chain of powers of an element of type c, index r and period s consists of an unrepeated part of r-1 elements of type a or of type c, and a repeated part of s elements, s-1 of which are type b elements and one of which is an idempotent element.

From considerations of powers of non-idempotent elements in an ovum we can immediately state

THEOREM I. Any ovum contains at least one idempotent element.

DEFINITIONS.

At this stage we find it convenient to introduce the following terms and concepts.

The idempotent element of a non-idempotent element.

If u_i is a non-idempotent element it has been shown that in the chain of powers of u_i there occurs one and only one idempotent element, say u_k. The idempotent element u_k will be called the idempotent element of u_i.

Sub ovum.

Suppose S is a sub-set of r elements of the mark-set U of an ovum O of degree n, $r \leq n$, and suppose the product of every pair of elements of S and the square of every element of S as determined by O is an element of S. Then multiplication is defined for S, and this multiplication is evidently commutative and associative. The set S together with the multiplication relations for the elements of S form an ovum P of order r. The ovum P is said to be a sub-ovum of O of order r.

Zero Element.

If an ovum contains an idempotent element u_i such that
$$u_i u_j = u_i$$
for every other element u_j in the ovum, the element u_i is called a zero element of the ovum. There is evidently not more than one zero element in an ovum.

Identity Element.

If an ovum contains an idempotent element u_i such that
$$u_i u_j = u_j$$
for every other element u_j in the ovum, u_i is called an identity element of the ovum. There is evidently not more than one identity element in an ovum.

Divisor of an Element.

Let u_i and u_j be any two elements of an ovum.

If
$$u_i = u_i u_j \qquad (1)$$
or if
$$u_i = u_j^2 \qquad (2)$$
or if there exists in the ovum a third element u_k such that
$$u_i = u_j u_k \qquad (3)$$
then u_j is said to divide or to be a divisor of u_i and we write
$$u_j / u_i$$
If no such relations as (1),(2),or (3) exist between

u_i and u_j we say that u_j does not divide u_i and write

$$u_j \nmid u_i$$

If
$$u_i = u_i^2 \qquad (4)$$

or if there exists in the ovum an element u_r such that

$$u_i = u_i \; u_r \qquad (5)$$

the element u_i is said to divide itself and we write

$$u_i \mid u_i$$

If u_i is non-idempotent and no relation such as (5) holds for u_i, u_i is said to not divide itself and we write
$$u_i \nmid u_i$$

Proper Divisor.

If u_i and u_j are any two elements of an ovum such that $u_j \mid u_i$ but $u_j \nmid u_i$, then u_j is said to be a proper divisor of u_i.

Irreducible Elements.

If an element u_i of an ovum has no proper divisors other than the identity element of the ovum (if one exists) u_i is said to be an irreducible element, otherwise a reducible element.

Associate Elements.

If u_i and u_j are any two elements of an ovum and if $u_j \mid u_i$ and $u_i \mid u_j$, the elements u_i and u_j are said to be associated to one another and we write $u_i \sim u_j$

Evidently if $u_i \sim u_k$

and $u_k \sim u_j$

then $u_i \sim u_j$

We extend the use of the symbol $\sim$ so that $u_i \sim u_i$ will mean $u_i | u_i$. We reserve the word "associated" for pairs of elements only.

Reduced Ovum.

An ovum in which no pair of elements are associated to one another is called a reduced ovum. Evidently in a reduced ovum every divisor of an element, which is not that element itself, is a proper divisor of that element.

HOMOMORPHISMS* IN OVA CONTAINING NON IDEMPOTENT ELEMENTS

In an ovum which contains at least one non-idempotent element, consider the correspondence formed by letting each idempotent element correspond to itself and each non-idempotent element correspond to its idempotent element. We see that such a correspondence is preserved under multiplication. For if u_i and u_j are two non-idempotent elements having the idempotent elements u_k and u_m respectively, then $u_i u_j$ is either equal to the idempotent element $u_k u_m$ or is a non-idempotent element whose idempotent element is $u_k u_m$. For, for some integers r and s

$$u_i^r = u_k$$

$$u_j^s = u_m$$

so $$(u_i u_j)^{rs} = u_i^{rs} u_j^{rs} = u_k u_m .$$

If u_i and u_j both have u_k as their idempotent element, evidently $u_i u_j$ has u_k as its idempotent element or else is equal to the idempotent element u_k. Similarly, if u_n is an

* Van der Waerden, Moderne Algebra, page 32.

idempotent element, $u_i u_n$ either equals $u_k u_n$ or is a non-idempotent element having $u_k u_n$ as its idempotent element, and $u_i u_k$ either equals u_k or has u_k as its idempotent element.

We have therefore

THEOREM 2. Any ovum which contains at least one non-idempotent element is homomorphic to the sub-ovum formed by its idempotent elements.

ASSOCIATE ELEMENTS IN OVA.

THEOREM 3. In any ovum no two idempotent elements can be associated.

Let u_i and u_j be two idempotent elements. Suppose u_i and u_j are associated. Then

$$u_i \mid u_j \qquad (1)$$

and

$$u_j \mid u_i \qquad (2)$$

From (1) there must exist in the ovum an element whose product with u_i is equal to u_j. This element is evidently not u_i itself, so we either have

$$u_i u_j = u_j \qquad (3)$$

or there exists a third element u_k in the ovum such that

$$u_i u_k = u_j \qquad (4)$$

However, if we multiply both sides of (4) by u_i we immediately get (3), so we see that (1) implies(3).

Similarly (2) implies

$$u_i u_j = u_i \qquad (5)$$

But (3) and (5) are contradictory, so the theorem follows.

THEOREM 4. In any ovum no two non-idempotent elements which have not the same idempotent element can be associated.

For, if u_i and u_j are two non-idempotent elements whose idempotent elements are u_k and u_m respectively and if r and s are integers such that

$$u_i^r = u_k$$
$$u_j^s = u_m$$

then $u_i | u_j$ and $u_j | u_i$ imply that $u_i^{rs} | u_j^{rs}$ and $u_j^{rs} | u_i^{rs}$. Hence if u_i and u_j are associated, it follows that the idempotent elements u_k and u_m are associated, which is impossible by theorem 3.

THEOREM 5. In any ovum a non-idempotemt element can not be associated to an idempotent element which is not its idempotent element.

The proof of this theorem is similar to that of theorem 4.

THEOREM 6. In any ovum, no type a or type c element can ba associated to its idempotent element, but every type b element is associated to its idempotent element.

Let u_i be a non-idempotent element and let u_k be its idempotent element. Then if

$$u_k | u_i \qquad (1)$$

we have either

$$u_k u_i = u_i \qquad (2)$$

or there exists a third element u_m in the ovum such that

$$u_k u_m = u_i \qquad (3)$$

Multiplying (3) by u_k however immediately gives (2),
so (1) implies (2).
Now if u_i is a type a element of index r, u_k is its index element and we have

$$u_i^r = u_k$$
$$u_i u_k = u_i^{r+1} = u_k \qquad (4)$$

If u_i is a type c element, u_k is its period element and we know that $u_i u_k$ is equal to a type b element, as it equals a non-idempotent element in the repeated part of the chain of u_i.
So, (1) is impossible if u_i is either a type a or a type c element.

However, if u_i is a type b element, with period r, u_k is its period element so that

$$u_i^r = u_k \qquad (5)$$

whence $u_i u_k = u_i^{r+1} = u_i$

and we see that (1) holds. Moreover from (5)

$$u_i | u_k \qquad (6)$$

and from (1) and (6) $\quad u_i \sim u_k$.

THEOREM 7. In any ovum no type a or type c element can be associated to an idempotent element or to an element of type b.

This follows immediately on combining theorems 5,6.

THEOREM 8. In any ovum, two type b elements are associated if and only if they have the same period element.

This follows on combining theorems 4,6.

THEOREM 9. In any ovum, two type a elements, two type c elements, or an element of type a and an element of type c, can not be associated if they do not have the same index.

Let u_i and u_j be two elements, either of which is either an element of type a or an element of type c, with different indices r_i and r_j respectively.

Assume $\quad u_i \sim u_j \quad (1)$

Then $\quad u_i^{r_i} \sim u_j^{r_i} \quad (2)$

and $\quad u_i^{r_j} \sim u_j^{r_j} \quad (3)$

First we consider the case in which u_i and u_j are both type a elements. If $r_i < r_j$, $u_i^{r_i}$ is an idempotent element, while $u_j^{r_i}$ is a type a element, so that (2) is in contradiction to theorem 7. If $r_j < r_i$ we find similarly that (3) is in contradiction to theorem 7.

Secondly, let u_i and u_j both be elements of type c. Then if $r_i < r_j$, $u_i^{r_i}$ is a type b element or an idempotent element while $u_j^{r_i}$ is a type a or a type c element. Again, then, (2) contradicts theorem 7. Similarly if $r_j < r_i$ we arrive at a contradiction.

Thirdly, If u_i is a type a element and u_j is a type c element and if $r_i < r_j$, $u_i^{r_i}$ is an idempotent element while $u_j^{r_i}$ is a type a or a type c element. If $r_j < r_i$, $u_i^{r_j}$ is a type a element, while $u_j^{r_j}$ is a type b element or an idempotent element. Again theorem 7 is contradicted in either case by (2) and (3) respectively.

Thus in all cases (1) leads to contradictions, so we conclude that u_i can not be associated to u_j.

OVA OF TYPE I.

We now discuss properties of those ova which contain only elements of certain of the four possible types, and first consider those elements which contain no elements of type b and no elements of type c. Such ova will be called ova of type I. An ovum of type I, then, may consist only of idempotent elements, or it may have idempotent elements and elements of type a. A reduced ovum is easily seen to be an ovum of type I *. Conversely we now prove

THEOREM 10. Every type I ovum is a reduced ovum.

From theorems 3,4,7,9, it is seen that the theorem will follow if we show that in an ovum of type I, no two type a elements which have the same index element, and the same index, can be associated.

To do this we make use of the following lemmas:

LEMMA 1. In any ovum, if u_i is a type a element with index element u_k, and u_m is another idempotent element such that $u_k u_m = u_m$ (a)

then $u_i u_m = u_m$ (b)

For, from properties of a type a element

$$u_i\, u_k = u_k \qquad \text{(c)}$$

Multiplying both sides of (c) by u_m and using (a) immediately gives (b).

LEMMA 2. In any ovum, if u_i and u_j are two type a elements with the same index element u_k and the same index, then none of the relations

* A. Clifford, Thesis for Ph.D. Degree, C.I.T., 1933.

$$u_i u_k = u_i \qquad \text{(a)}$$

$$u_i u_k = u_j \qquad \text{(b)}$$

$$u_i u_j = u_j \qquad \text{(c)}$$

$$u_i^2 = u_j \qquad \text{(d)}$$

is possible.

From properties of a type a element

$$\forall \quad u_i u_k = u_k$$

so that (a) and (b) are false.

Let r be the index of u_i and of u_j . If $r = 2$, then

$$u_i^2 = u_j^2 = u_k$$

Assuming that (c) holds and multiplying both sides of (c) by u_i gives

$$u_i u_j = u_k u_j = u_k \qquad \text{(e)}$$

which contradicts (c), so that (c) can not hold if r equals 2.

If $r > 2$ and we assume that (c) holds , we get

$$u_i^{r-1} u_j^{r-1} = u_j^{r-1} \qquad \text{(f)}$$

But u_i^{r-1} and u_j^{r-1} for $r > 2$ are type a elements of index 2, and so (f) is not possible, by what we have just shown above. Hence (c) does not hold for any value of r.

Relation (d) implies that the index of u_i is less than that of u_j which is contrary to hypothesis.

To return to the main theorem, let u_i and u_j be two type a elements with index element u_k and index r, in an ovum O of type I.

Then

$$u_i u_k = u_k \qquad (1)$$

$$u_j u_k = u_k \qquad (2)$$

Assume $$u_i \sim u_j \qquad (3)$$
Then there exists in O an element whose product with u_i is equal to u_j, and by lemma 2 this element is neither u_i, u_j, nor u_k. There must therefore exist in O another element, say u_l, which is such that $$u_i\, u_l = u_j \qquad (4)$$
From (3) there must also exist in O an element whose product with u_j is equal to u_i. From lemma 2 this element is neither u_i, u_j, nor u_k. We show that it cannot be u_l.

Assume $$u_j\, u_l = u_i \qquad (5)$$
and combine this with (4) and we have
$$u_j\, u_l^2 = u_j \qquad (6)$$
$$u_i\, u_l^2 = u_i \qquad (7)$$
Now, $$u_l^2 = u_l$$
implies from (6) $$u_j\, u_l = u_j$$
in contradiction to (5), so that u_l^2 can not equal u_l. From lemma 2 and (6) and (7) it follows that u_l^2 can not equal any of u_i, u_j, or u_k. Hence if (5) holds O must contain another element u_m such that
$$u_l^2 = u_m \qquad (8)$$
$$u_j\, u_m = u_j \qquad (9)$$
$$u_i\, u_m = u_i \qquad (10)$$
From (8) u_m is either the index element of u_l or is a type a element having the same index element as u_l. Hence, for s sufficiently large ($s \geq 1$ if u_m is idempotent, $s \geq t$ where t is the index of u_m if u_m

is a type a element)

$$u_l\, u_m^s = u_m^s \qquad (11)$$

From (9) and (10) we have

$$u_j\, u_m^s = u_j\, u_m^{s-1} \quad \ldots \quad u_j\, u_m = u_j \qquad (12)$$

and

$$u_i\, u_m^s = u_i\, u_m^{s-1} \quad \ldots \quad u_i\, u_m = u_i \qquad (13)$$

Multiplying both sides of (4) by u_m^s gives

$$u_i\, u_l\, u_m^s = u_j\, u_m^s$$

which on employing (11) and (12) gives

$$u_i\, u_m^s = u_j$$

in contradiction to (13).

Thus (5) is impossible, so O must contain besides u_i ,u_j ,u_k ,u_l , an element u_n which is such that

$$u_j\, u_n = u_i \qquad (14)$$

From (4) and (14)

$$u_i\, u_n\, u_l = u_i$$

$$u_j\, u_n\, u_l = u_j$$

From lemma 2, $u_n\, u_l$ can equal neither u_k ,u_i, or u_j. From (4) it cannot equal u_l , and from (14) it can not equal u_n . Hence O contains another element u_p w which is such that

$$u_n\, u_l = u_p \qquad (15)$$

$$u_i\, u_p = u_i \qquad (16)$$

$$u_j\, u_p = u_j \qquad (17)$$

We show now that of the three elements u_l ,u_n, and u_p , no one can be the index element of any other, no pair of them can have the same index element, and no one of them has index element u_k .

For if u_p is the index element of u_n, or if u_n is the index element of u_p, or if u_n and u_p both have the same index element, for t sufficiently large, ($t \geq 1$ if u_p is an idempotent element, t greater than or equal to the index of u_p if u_p is a type a element)

$$u_n u_p^t = u_p^t \tag{18}$$

Moreover from (16) and (17) we have

$$u_i u_p^t = u_i \tag{19}$$

$$u_j u_p^t = u_j \tag{20}$$

and from (14)

$$u_j u_n u_p^t = u_i u_p^t$$

which using (18) and (19) gives

$$u_j u_p^t = u_i$$

in contradiction to (20).

Similarly u_p can not be the index element of u_l, u_l can not be the index element of u_p, and u_p and u_l can not have the same index element.

Also, if u_n and u_l had the same index element, u_p would be that index element or would have the same index element by (15), in contradiction to what we have just shown. If u_n were the index element of u_l or if u_l were the index element of u_n, we would have

$$u_n u_l = u_n$$

or

$$u_n u_l = u_l$$

in contradiction to (15).

To show that no one of u_l, u_n, or u_p has index element u_k, we first assume that u_p has index element u_k, so that for t greater than or equal to the index of u_p ,

$$u_p^t = u_k$$

whence from (1)

$$u_i\, u_p^t = u_k$$

in contradiction to (19); hence u_p can not have u_k as its index element.

Assume that u_l has index element u_k . Then, by the above u_n does not have index element u_p , and does not have index element u_k . So u_n is either an idempotent element or there exists in O another element u_q which is the index element of u_n . If u_n is an idempotent element, from (14) and theorem 2 follows

$$u_k\, u_n = u_k \tag{21}$$

otherwise for u_n a type a element , from (14) and theorem 2 ,

$$u_k\, u_q = u_k \tag{22}$$

From (15), for any integer s

$$u_n^s\, u_l^s = u_p^s$$

and for s sufficiently large

$$u_n\, u_k = u_p^s \tag{23}$$

if u_n is an idempotent element, otherwise

$$u_q\, u_k = u_p^s \tag{24}$$

For u_n an idempotent element, combining (21) and (23) gives

$$u_p^s = u_k \tag{25}$$

and for u_n a type a element, combining (22) and (24) also gives (25).

But (25) indicates that u_k is the index element of u_p , which we have proved impossible. Hence u_l and similarly

u_n can not have u_k as its index element.

We have now shown that assumption (3) implies that O contains besides the three elements u_i, u_j, u_k, at least three more elements u_l, u_n, u_p, and that these six elements satisfy the seven relations

$$u_i\, u_k = u_k \qquad (1)$$

$$u_j\, u_k = u_k \qquad (2)$$

$$u_i\, u_l = u_j \qquad (4)$$

$$u_j\, u_n = u_i \qquad (14)$$

$$u_l\, u_n = u_p \qquad (15)$$

$$u_i\, u_p = u_i \qquad (16)$$

$$u_j\, u_p = u_j \qquad (17)$$

Moreover, of the three elements u_l, u_n, u_p, no one can be the index element of any other, no pair of them can have the same index element, and no one of them can have index element u_k.

Now let u_L denote the index element of u_l if u_l is a type a element, and let u_L denote u_l itself if u_l is idempotent. Let u_N and u_P have similar significance with respect to u_n and u_p.

Then from (15) and theorem 2 follows

$$u_L\, u_N = u_P \qquad (26)$$

Multiplying both sides of (26) by u_L gives

$$u_P\, u_L = u_P \qquad (27)$$

which by lemma 1 gives

$$u_P\, u_l = u_P \qquad (28)$$

From (16) for any integer t,

$$u_\rho^t \; u_i = u_i$$

which for t sufficicently large gives

$$u_\rho \, u_i = u_i \qquad (29)$$

Similarly from (17)

$$u_\rho \, u_\gamma = u_\gamma \qquad (30)$$

From (4) multiplying both sides by u_ρ

$$u_i \, u_\ell \, u_\rho = u_\gamma \, u_\rho$$

which on employing (28) and (30) yields

$$u_i \, u_\rho = u_\gamma$$

in contradiction to (29).

Thus assumption (3) leads to a contradiction so that we conclude that in a type I ovum no type a elements having the same index and the same index element can be associated. The proof of the theorem is now complete.

THEOREM 11. A reduced ovum must contain a zero element.

Let O be a reduced ovum having the idempotent elements u_{γ_1}, u_{γ_2}, ..., u_{γ_m}. The product of these idempotent elements is one of them, say u_{γ_i}. That is

$$u_{\gamma_1} \, u_{\gamma_2} \dots u_{\gamma_m} = u_{\gamma_i}$$

and for any other one of them, say u_{γ_k}, evidently

$$u_{\gamma_k} \, u_{\gamma_i} = u_{\gamma_i} \qquad (1)$$

For a type a element u_i with index element u_{γ_i}, from properties of type a elements

$$u_i \, u_{\gamma_i} = u_{\gamma_i} \qquad (2)$$

and for a type a element u_k with index element some other idempotent say u_{γ_k}, by lemma 1 of the previous theorem $u_k \, u_{\gamma_i} = u_{\gamma_i}$ (3)

(1),(2),(3), show that u_{γ_i} is the zero element of O.

THEOREM 12. If a reduced ovum has an identity element, that element is an irreducible element.

Let u_i be the identity element in a reduced ovum O. If u_j is another element of O with index element u_i, we have

$$u_i u_j = u_i$$

in contradiction to the fact that u_i is the identity element. Thus, u_i can not equal the power of any element in O.

Moreover, there exist in O no elements u_j and u_k such that

$$u_j u_k = u_i$$

For, this implies

$$u_j / u_i$$

whence

$$u_j \mid u_i u_k$$

or

$$u_j \mid u_k$$

Also, in a similar manner,

$$u_k \mid u_j$$

But O is a reduced ovum. Thus, u_i has no proper divisors and hence is an irreducible element.

From theorem 12 follows:

COROLLARY 1. A reduced ovum O containing an identity element has a reduced sub-ovum of order n-1, consisting of all the elements of O except the identity.

COROLLARY 2. From a reduced ovum O of order n, mark set $(u_1, u_2, \ldots, u_n)$, we can form a reduced ovum of order n+1, containing an identity element, by adjoining to the mark set of O an element u_{n+1}, and to the multiplication table of O the relations

$$u_{n+1}^2 = u_{n+1}$$

$$u_{n+1}\, u_i = u_i\, u_{n+1} = u_i \qquad (i = 1,2,3,\ldots,n)$$

THEOREM 13. A reduced ovum has at least one irreducible element which is not an identity element.

First let O be a reduced ovum which contains no identity element, and assume that O possesses no irreducible element. Then any element u_{i_1} has a proper divisor u_{i_2}, which in turn has a proper divisor u_{i_3}, and so on, so that we get a chain of elements each of which is a proper divisor of all those elements which precede it. However, due to the finite number of elements in O we must eventually come to an element u_{i_j} which has occurred earlier in the chain. Suppose the chain is $u_{i_1}, u_{i_2}, \ldots, u_{i_j}, u_{i_{j+1}}, \ldots, u_{i_j}, \ldots$

Then, this implies

$$u_{i_{j+1}} \mid u_{i_j}$$

and

$$u_{i_j} \mid u_{i_{j+1}}$$

in contradiction to the fact that $u_{i_{j+1}}$ was a proper divisor of u_{i_j}.

Thus, O contains an irreducible element which is not an identity element.

If O has an identity element, consider the sub-ovum O' formed of all the elements of O except the identity. Then, as above O' possesses an irreducible element which is also irreducible in O and which is not the identity element of O. Thus, O contains an irreducible element which is not the identity element.

Since in a reduced ovum an irreducible element possesses no divisors except itself and the identity element if one exists in the ovum , we can conclude from theorem 13

COROLLARY 1. Every reduced ovum of order n has at least one reduced sub-ovum of order n-1.

Cyclic Reduced Ova.

Consider an ovum of order n in which every element is a power of a certain element . Such an ovum will be said to be cyclic. We prove

THEOREM 14. For a given n there exists one and only one cyclic reduced ovum of order n.

Let the n elements be powers of one u_1 . That is

$$u_i = u_1^i \qquad (\quad i = 1, 2, \ldots, n)$$

The zero of the ovum is evidently u_n , since if u_i $i < n$, were a zero element we should have

$$u^{i+1} = u_i \, u_1 = u_i$$

and the ovum would not contain n elements.

Then, the multiplication table is given by the relations

$$\begin{array}{ll} u_i^2 = u_{2i} & 2i < n \\ u_i^2 = u_n & 2i \geq n \\ u_i \, u_j = u_{i+j} & i + j < n \\ u_i \, u_j = u_n & i + j \geq n \end{array}$$

It is evident that such a multiplication table is both commutative and associative so that the theorem follows.

Construction of Reduced or Type I Ova.

Corollary 1, theorem 13 shows that from all possible distinct reduced ova of order n-1 we can obtain all possible distinct ova of order n by adjoining to the ova of order n-1 another idempotent or type a element , making multiplication of this element with itself and with the original elements commutative and associative, and examining the ova thus formed to see which are simply isomorphic to one another.

In forming thus reduced ova of order n from reduced ova of order n-1 theorems 2 and 11 are found to be useful.

The distinct reduced ova of order 2 are two in number.

$$R2_1 \quad \begin{array}{cc} u_1 & u_1 \\ u_1 & u_2 \end{array} \qquad \text{and} \qquad R2_2 \quad \begin{array}{cc} u_1 & u_1 \\ u_1 & u_1 \end{array}$$

From $R2_1$ adjoining the element u_3 we obtain the following reduced ova of order 3.

$$R3_1 \quad \begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 \\ u_1 & u_1 & u_3 \end{array} \qquad R3_2 \quad \begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 \\ u_1 & u_2 & u_3 \end{array} \qquad R3_3 \quad \begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 \\ u_1 & u_1 & u_1 \end{array}$$

$$R3_4 \quad \begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_2 & u_3 \\ u_1 & u_3 & u_1 \end{array} \qquad R3_5 \quad \begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 \\ u_1 & u_2 & u_2 \end{array}$$

From $R2_2$ we obtain only two more reduced ova of order 3, which are distinct from one another and from the ova already obtained from $R2_1$. They are

$R3_6$
$$\begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 \end{array}$$

$R3_7$
$$\begin{array}{ccc} u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 \\ u_1 & u_1 & u_2 \end{array}$$

Proceeding in this way from $R3_1$ adjoinig the element u_4, we get the distinct reduced ova of order 4.

$R4_1$
$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_3 & u_1 \\ u_1 & u_1 & u_1 & u_4 \end{array}$$

$R4_2$
$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_3 & u_3 \\ u_1 & u_1 & u_3 & u_4 \end{array}$$

$R4_3$
$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_2 \\ u_1 & u_1 & u_3 & u_3 \\ u_1 & u_2 & u_3 & u_4 \end{array}$$

$R4_4$
$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_3 & u_1 \\ u_1 & u_1 & u_1 & u_1 \end{array}$$

$R4_5$
$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_3 & u_4 \\ u_1 & u_1 & u_4 & u_1 \end{array}$$

$R4_6$
$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_2 \\ u_1 & u_1 & u_3 & u_1 \\ u_1 & u_2 & u_1 & u_2 \end{array}$$

From $R3_2$ and $R3_3$ we get the further distinct ova

$$R_{4_7}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_3 & u_3 \\ u_1 & u_2 & u_3 & u_4 \end{matrix}$$

$$R_{4_8}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_1 \\ u_1 & u_2 & u_3 & u_1 \\ u_1 & u_1 & u_1 & u_4 \end{matrix}$$

$$R_{4_9}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_1 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_1 & u_4 & u_1 \end{matrix}$$

$$R_{4_{10}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_4 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_4 & u_4 & u_1 \end{matrix}$$

$$R_{4_{11}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_3 & u_2 \\ u_1 & u_2 & u_2 & u_2 \end{matrix}$$

$$R_{4_{12}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_2 & u_4 & u_2 \end{matrix}$$

$$R_{4_{13}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_3 & u_3 \\ u_1 & u_2 & u_3 & u_3 \end{matrix}$$

$$R_{4_{14}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \end{matrix}$$

$$R_{4_{15}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_2 \\ u_1 & u_1 & u_2 & u_1 \end{matrix}$$

$$R_{4_{16}}$$
$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_4 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_4 & u_1 & u_1 \end{matrix}$$

$R\,4_{17}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_2 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_2 \end{matrix}$$

$R\,4_{18}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_3 \end{matrix}$$

From $R\,3_4$ we get

$R\,4_{19}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_3 & u_3 \\ u_1 & u_3 & u_1 & u_1 \\ u_1 & u_3 & u_1 & u_1 \end{matrix}$$

$R\,4_{20}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_3 & u_1 & u_1 \\ u_1 & u_4 & u_1 & u_1 \end{matrix}$$

$R\,4_{21}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_3 & u_2 \\ u_1 & u_3 & u_1 & u_3 \\ u_1 & u_2 & u_1 & u_2 \end{matrix}$$

$R\,4_{22}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_3 & u_1 & u_1 \\ u_1 & u_4 & u_1 & u_3 \end{matrix}$$

From $R\,3_5$ we get

$R\,4_{23}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_2 & u_2 \end{matrix}$$

$R\,4_{24}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_2 & u_3 \end{matrix}$$

From $R\,3_6$ we get

$R4_{25}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \end{matrix}$$

$R4_{26}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_2 \\ u_1 & u_1 & u_2 & u_1 \end{matrix}$$

$R4_{27}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_2 \end{matrix}$$

$R4_{28}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_2 \\ u_1 & u_1 & u_2 & u_2 \end{matrix}$$

$R4_{29}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_1 & u_1 & u_3 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_3 & u_1 & u_2 \end{matrix}$$

From $R3_7$ we get only one further distinct ovum

$R4_{30}$

$$\begin{matrix} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_2 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_2 \end{matrix}$$

OVA OF TYPE II.

An ovum which contains no elements of type a or of type c, but at least one element of type b will be called an ovum of type II.

If G is a finite Abelian group [1] of order $n>1$ and if i is its identity element, every element a of G has the property [2]

$$a^{n} = i$$

whence

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

and so G is an ovum of type II with only one idempotent element, the identity.

Conversely, an ovum O of type II containing only one idempotent element is a group. For, let the idempotent element of O be u_k. Then u_k is the period element of any type b element u_i in O, and so for some integer s

$$u_i^{s} = u_k$$

$$u_i\, u_k = u_i^{s+1} = u_i$$

so that u_k is an identity element.

Moreover,

$$u_i\, u_i^{s-1} = u_k$$

so that u_i has an inverse in O. Thus O is a group.

The product of two type b elements having period element u_k, or of a type b element and its period element u_k is either u_k or a type b element having period element u_k. Thus all type b elements with period element u_k together with u_k form a sub-ovum of O. By what we have just shown, such a sub-ovum is a group. Remembering also that an idempotent element is itself a group of order 1, we can then state

THEOREM 15. Every ovum O of type II is either a group or consists of sub-ova which have no element in common and each of which is a group. Each of these groups consists of an idempotent element and of all the type b elements which have this idempotent element for period element.

1. Van Der Waerden, Moderne Algebra p. 15.
2. " " " " " p. 27.

THEOREM 16. From a finite Abelian group G of order n-1 we can obtain two and only two ova of order n, by the adjunction of an idempotent element.

For, let the identity element of G $(u_1, \ldots, u_{n-1})$ be u_i and suppose u_n is an idempotent element which we wish to attach to G to form an ovum of order n. The product $u_i u_n$ is then an idempotent element and hence must equal either u_i or u_n. From theorem 2 it then follows that u_n must either have properties of a zero element or of an identity element in any ovum formed from u_n and G. Letting u_n be either a zero or an identity gives us commutative and associative multiplication for the mark set $(u_1, \ldots, u_n)$ and thus we can form the two ova of order n each of which has G as a sub-ovum.

In a group every element divides every other element so that every element is associated to every other element. From theorems 3,6 it follows that an ovum in which every element is associated to every other element can have only one idempotent element and type b elements and is therefore a group. So we have

THEOREM 17. A sufficient condition that an ovum be a group is that every element be associated to every other element.

It must be noted that the condition given in this theorem is not the same as the condition given by Van der Waerden in his postulates for groups *. His postulate 5 not only demands that every element be associated to every other element but also that every element divide itself.

Construction of Ova of Type II.

From theorem 15 we know that all type II ova of order n can be obtained by compounding groups of order $\leq$ n, only those combinations being taken the sum of whose orders is n. The commutative and associative laws must be satisfied and ova simply isomorphic to one already listed must be thrown out. In particular, to groups of order n-1 we adjoin one idempotent element , and to groups of order n-2 we adjoin 2 idempotent elements, and so on. We use the letter S to designate type II ova.

Thee only type II ovam of order 2 is the Abelian group

$$S2_1$$
$$\begin{array}{cc} u_1 & u_2 \\ u_2 & u_1 \end{array}$$

Type II ova of order 3 are 3 in number:

The Abelian group $S3_1$

$$\begin{array}{ccc} u_1 & u_2 & u_3 \\ u_2 & u_3 & u_1 \\ u_3 & u_1 & u_2 \end{array}$$

and the two ova obtained from $S2_1$ on adjoining an idempotent element

$$S3_2 \qquad\qquad\qquad\qquad S3_3$$
$$\begin{array}{ccc} u_1 & u_2 & u_1 \\ u_2 & u_1 & u_2 \\ u_1 & u_2 & u_3 \end{array} \qquad\qquad \begin{array}{ccc} u_1 & u_2 & u_3 \\ u_2 & u_1 & u_3 \\ u_3 & u_3 & u_3 \end{array}$$

* Van der Waerden Moderne Algebra, page 19, 5.

Type II ova of order 4 are 11 in number. The two Abelian groups

$S4_1$

u_1	u_2	u_3	u_4
u_2	u_1	u_4	u_3
u_3	u_4	u_2	u_1
u_4	u_3	u_1	u_2

$S4_2$

u_1	u_2	u_3	u_4
u_2	u_1	u_4	u_3
u_3	u_4	u_1	u_2
u_4	u_3	u_2	u_1

The two ova obtained from the group $S3_1$ by adjoining an idemppotent element

$S4_3$

u_1	u_2	u_3	u_4
u_2	u_3	u_1	u_4
u_3	u_1	u_2	u_4
u_4	u_4	u_4	u_4

$S4_4$

u_1	u_2	u_3	u_1
u_2	u_3	u_1	u_2
u_3	u_1	u_2	u_3
u_1	u_2	u_3	u_4

Two ova obtained on compounding two groups simply isomorphic to $S2_1$

$S4_5$

u_1	u_2	u_1	u_1
u_2	u_1	u_2	u_2
u_1	u_2	u_3	u_4
u_1	u_2	u_4	u_3

$S4_6$

u_1	u_2	u_1	u_2
u_2	u_1	u_2	u_1
u_1	u_2	u_3	u_4
u_2	u_1	u_4	u_3

Adjoining two idempotent elements to $S2_1$ which is the same thing as adjoining one idempotent element to $S3_2$ and $S3_3$ gives, from $S3_2$

$S4_7$

u_1	u_2	u_1	u_1
u_2	u_1	u_2	u_2
u_1	u_2	u_3	u_1
u_1	u_2	u_1	u_4

$S4_8$

u_1	u_2	u_1	u_1
u_2	u_1	u_2	u_2
u_1	u_2	u_3	u_4
u_1	u_2	u_4	u_4

and from $S3_3$

$S4_9$

$$\begin{array}{cccc} u_1 & u_2 & u_3 & u_1 \\ u_2 & u_1 & u_3 & u_2 \\ u_3 & u_3 & u_3 & u_3 \\ u_1 & u_2 & u_3 & u_4 \end{array}$$

$S4_{10}$

$$\begin{array}{cccc} u_1 & u_2 & u_3 & u_3 \\ u_2 & u_1 & u_3 & u_3 \\ u_3 & u_3 & u_3 & u_3 \\ u_3 & u_3 & u_3 & u_4 \end{array}$$

$S4_{11}$

$$\begin{array}{cccc} u_1 & u_2 & u_3 & u_4 \\ u_2 & u_1 & u_3 & u_4 \\ u_3 & u_3 & u_3 & u_4 \\ u_4 & u_4 & u_4 & u_4 \end{array}$$

FURTHER OVA OF ORDER $N \leq 4$

We list here the remaining distinct ova of order 2,3,4.

There are no more of order 2.

There are only two more of order 3:

$T3_1$

$$\begin{array}{ccc} u_1 & u_2 & u_1 \\ u_2 & u_1 & u_2 \\ u_1 & u_2 & u_1 \end{array}$$

$T3_2$

$$\begin{array}{ccc} u_1 & u_2 & u_2 \\ u_2 & u_1 & u_1 \\ u_2 & u_1 & u_1 \end{array}$$

and 15 of order 4.

$T4_1$

$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_4 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_3 & u_1 & u_4 \\ u_4 & u_4 & u_4 & u_1 \end{array}$$

$T4_2$

$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_4 \\ u_1 & u_2 & u_1 & u_4 \\ u_1 & u_1 & u_1 & u_4 \\ u_4 & u_4 & u_4 & u_1 \end{array}$$

$T4_3$

$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_4 \\ u_1 & u_2 & u_1 & u_4 \\ u_1 & u_1 & u_1 & u_4 \\ u_4 & u_4 & u_4 & u_1 \end{array}$$

$T4_4$

$$\begin{array}{cccc} u_1 & u_1 & u_3 & u_3 \\ u_1 & u_2 & u_3 & u_4 \\ u_3 & u_3 & u_1 & u_1 \\ u_3 & u_4 & u_1 & u_1 \end{array}$$

$T4_5$

$$\begin{array}{cccc} u_1 & u_2 & u_1 & u_4 \\ u_2 & u_2 & u_2 & u_2 \\ u_1 & u_2 & u_1 & u_4 \\ u_4 & u_2 & u_4 & u_1 \end{array}$$

$T4_6$

$$\begin{array}{cccc} u_1 & u_2 & u_4 & u_4 \\ u_2 & u_2 & u_2 & u_2 \\ u_4 & u_2 & u_1 & u_1 \\ u_4 & u_2 & u_1 & u_1 \end{array}$$

$T4_7$

$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_4 \\ u_1 & u_1 & u_1 & u_1 \\ u_1 & u_4 & u_1 & u_2 \end{array}$$

$T4_8$

$$\begin{array}{cccc} u_1 & u_1 & u_1 & u_1 \\ u_1 & u_2 & u_3 & u_4 \\ u_1 & u_3 & u_1 & u_3 \\ u_1 & u_4 & u_3 & u_2 \end{array}$$

$T4_9$

$$\begin{array}{cccc} u_1 & u_1 & u_3 & u_1 \\ u_1 & u_2 & u_3 & u_2 \\ u_3 & u_3 & u_1 & u_3 \\ u_1 & u_2 & u_3 & u_2 \end{array}$$

$T4_{10}$

$$\begin{array}{cccc} u_1 & u_2 & u_1 & u_1 \\ u_2 & u_1 & u_2 & u_2 \\ u_1 & u_2 & u_1 & u_1 \\ u_1 & u_2 & u_1 & u_1 \end{array}$$

$T4_{11}$

$$\begin{array}{cccc} u_1 & u_2 & u_1 & u_2 \\ u_2 & u_1 & u_2 & u_1 \\ u_1 & u_2 & u_1 & u_2 \\ u_2 & u_1 & u_2 & u_1 \end{array}$$

$T4_{12}$

$$\begin{array}{cccc} u_1 & u_2 & u_2 & u_2 \\ u_2 & u_1 & u_1 & u_1 \\ u_2 & u_1 & u_1 & u_1 \\ u_2 & u_1 & u_1 & u_1 \end{array}$$

$$T_{4,13}$$

$$\begin{matrix} u_1 & u_1 & u_3 & u_1 \\ u_1 & u_1 & u_3 & u_1 \\ u_3 & u_3 & u_1 & u_3 \\ u_1 & u_1 & u_3 & u_2 \end{matrix}$$

$$T_{4,14}$$

$$\begin{matrix} u_1 & u_1 & u_3 & u_3 \\ u_1 & u_1 & u_3 & u_3 \\ u_3 & u_3 & u_1 & u_1 \\ u_3 & u_3 & u_1 & u_2 \end{matrix}$$

$$T_{4,15}$$

$$\begin{matrix} u_1 & u_2 & u_3 & u_3 \\ u_2 & u_3 & u_1 & u_1 \\ u_3 & u_1 & u_2 & u_2 \\ u_3 & u_1 & u_2 & u_2 \end{matrix}$$