THE FOUNDATIONS OF GENERAL ARITHMETIC

Thesis

By Morgan Ward.

In Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy.

California Institute of Technology
Pasadena, California

1928

CONTENTS

THE FOUNDATIONS OF GENERAL ARITHMETIC

PART I. PRELIMINARY NOTIONS FROM FORMAL LOGIC.

SECTION 1. INTRODUCTION.

We assume as known the whole machinery of formal logic, such as the notion of class, relation, propositional function, correspondence, formal equivalence, counting, and the like. We shall use this machinery to investigate a kind of class called a "collection" whose elements consist of "entities" which in a given collection are either all "objects" or all "marks," and certain special types of propositional functions associated with the collection.

The reason for introducing these terms is to avoid confusing the general use of the words "class" "element" in our reasoning about collections and entities with the particular collections and entities themselves.

Loosely speaking, by "marks" we mean bare symbols which are distinguishable from one another, but which have no direct connotation. By an "object" we mean something which can be denoted by a "mark." The distinction between "mark" and "object" is somewhat vague; to state it intelligibly would be to solve one of the major problems of epistemology.

Our ultimate aim is to lay the foundations for a precise definition of an "arithmetic" analogous to the postulational definition of an abstract group. For the present, by an "arithmetic" we mean any system wherein

1. All operations possible can be carried out in a finite number of steps.

2. Division is not always a possible operation.

3. Unique factorization into primes is always a possible operation.

SECTION 2: ONE TO ONE CORRESPONDENCE.

PRELIMINARY: In this section, we describe one of the most fundamental ideas of logic, that of the one to one correspondence between two classes.

NOTATION: Consider two collections of entities C_1 and C_2 which have the same cardinal number, so that they can be put into one to one correspondence with each other. We shall denote the fact that C_1 and C_2 are in one to one correspondence by writing

(2.1) $C_1 \overleftrightarrow{\smile} C_2$

which is read " C_1 corresponds to C_2 ."

Let x_1 denote the particular general element of C_1 and x_2 the particular general element of C_2 ; then

(2.2) $x_1 \smile x_2$

is a propositional function. If m_1 , m_2 ; n_1 , n_2 denote corresponding entities in the two collections, then the class of true propositions

$$m_1 \smile m_2 \ , \ n_1 \smile n_2 , \ \ldots$$

are the values of the propositional function (2.2).

THEOREM 2.1: Fundamental Properties of $\smile$.

The relation $\smile$ is symmetric, reflexive, and transitive.

PROOF: Clear from formal logic.

THEOREM 2.2: The Five Types of Correspondence.

All correspondences (2.1) can be separated into five types according as C_1 and C_2 contain marks or objects, and are the same or different.

These types are given by the following table:

Type	Elements of	Elements of	Relation between C_1 and C_2
1.	objects	objects	same
2.	objects	objects	different
3.	objects	marks	different
4.	marks	marks	same
5.	marks	marks	different

PROOF: Clear from formal logic.

DEFINITION 2.1: Labelling.

A correspondence of type 3 is called "labelling," or "naming," and the marks are called the "labels" or "names" of their corresponding objects. Each mark is said to denote its corresponding object.

SECTION 3: FUNCTIONS.

PRELIMINARY: We here describe two kinds of propositional function which we shall need subsequently.

DEFINITION 3.1: Functions of One Variable.

Let x denote the particular general element of a collection of entities, C. Suppose we have a rule which assigns to each "value" of x; that is, to each entity of C, a unique second entity of C denoted by y. We then say y is a one-valued function of x defined over C; briefly, a function of x.

NOTATION:

(3.1) $$y = F(x)$$

In particular, if the rule assigns to the ~~object~~ entity h the ~~object~~ entity g, we write

(3.2) $$g = F(h)$$

x is called the independent, and y the dependent variable of the function. h is said to be the value of y determined by the value g of x. It need not be distinct from h.

DEFINITION 3.2: Functions of Two Variables.

Let u and v denote particular general elements of a collection of entities C. Suppose we have a rule which assigns to each pair of "values" of u and v; that is, to each pair of entities of C, a unique third entity of C denoted by w.

We then say w is a one-valued function of u and v defined over C, briefly a function of u and v.

NOTATION:

(3.3) $W = F(u, v)$

In particular, if the rule assigns to the ~~objects~~ entities g and h of C the ~~object~~ entity fr, we write

(3.4) $fr = F(g, h)$

u and v are called the independent, and W the dependent variables of the function. fr is said to be the value of W determined by the values g and h of u and v. These values need not be distinct, but in general $F(g, h)$ and $F(h, g)$ are distinct.

REMARK: (1.1) and (1.3) are propositional functions, (1.2) and (1.4) values of these propositional functions.

REMARK: These two types of function are extremely general. The following particular kind of function is highly important in what follows.

THEOREM 3.1: Connection between Operations and Functions.

Suppose C is a collection of objects denoted by $m, n, \ldots$ and o an operation by which we can combine any two objects and which satisfies the following condition, called the postulate of closure:

"If m, n denote any two elements of C, then the result of combining the objects denoted by m and n by means of o is a unique object of C denoted by fr."

Then the object denoted by fr is a function of the objects denoted by m and n.

PROOF: Clear.

REMARK: We may express the hypotheses of Theorem 3.1 in the following form:

$m, n \in C$

(3.5) $C/m, n$ *

(3.6) $m \circ n = p$

(3.7) C/p

(3.8) p is unique.

The conclusion then reads, "the conditions (3.5) - (3.8) imply $p = F(m, n)$."

DEFINITION 3.3: Equality of Two Functions.

Two functions are said to be equal when and only when they have the same number of independent variables and are identical for all values of these variables.

NOTATION: $F(x) \equiv G(x), \quad F(u, v) \equiv G(u, v)$

---

* C/m is read " C contains m ," or more accurately, " C contains the entity denoted by m ."

SECTION 4: TRANSFORMATIONS.

PRELIMINARY: We here develop another fundamental idea of formal logic which we shall constantly employ.

THEOREM 4.1: Isomorphism.

Let C_1 and C_2 be two collections of entities between which there exists a definite one to one correspondence symbolized by

(4.1) $C_1 \backsim C_2$

and assume that there exists a function

$z_1 = F(x_1, y_1)$ defined over C_1 as in Df. 3.2.

Then we may define a function $z_2 = G(x_2, y_2)$ over C_2 by means of

(4.2) $z_1 = F(x_1, y_1)$

and the relations

$$z_2 \backsim z_1, \quad y_2 \backsim y_1, \quad x_2 \backsim x_1$$

implied by (4.1) in accordance with Df. 3.2.

PROOF: Clear from formal logic.

THEOREM 4.2: The function $G(x_2, y_2)$ of Th. 4.1 depends upon two factors

(i) the function $F(x_1, y_1)$ in C_1

(ii) the way in which the correspondence (4.1) has been set up; that is, the values of the propositional function $x_2 \backsim x_1$.

PROOF: Clear from formal logic.

DEFINITION 4.1: System.

The collection C_1 and the function $F(x_1, y_1)$ are said to form a system.

NOTATION: $[C_1, F(x_1, y_1)]$

DEFINITION 4.2: Isomorphic Systems.

The systems $[C_1, F(x_1, y_1)]$ and $[C_2, G(x_2, y_2)]$ are said to be isomorphic.

NOTATION: $[C_1, F(x_1, y_1)] \backsim [C_2, G(x_2, y_2)]$

This is read "$[C_1, F(x_1, y_1)]$ is isomorphic with $[C_2, G(x_2, y_2)]$."

THEOREM 4.3: Chief Properties of Isomorphism.

The relation of isomorphism between systems defined in Df. 4.2 is reflexive, symmetric, and transitive.

PROOF: Clear from formal logic.

REMARK 1 : We now introduce a concept of great importance in all that is to follow.

DEFINITION 4.3: Formal Transformation.

The correspondence (3.1) is said to define a formal transformation T of the system $[C_1, F(x_1, y_1)]$ into $[C_2, G(x_2, y_2)]$.

NOTATION: $T(C_1) \longrightarrow C_2 \qquad T(x_1) \longrightarrow x_2$

$T(F(x_1, y_1)) \longrightarrow G(x_2, y_2)$

The class of all possible correspondences (3.1) between C_1 and C_2 is said to define the class $\{T\}$ of all formal transformations T.

REMARK 2 : The general aim of this paper may now be concisely formulated. It is to discover and study the invariants of the class $\{T\}$ of formal transformations; that is, to investigate those properties of $F(x_1, y_1)$ and $G(x_2, y_2)$ which are independent of the factor (ii) in Theorem 4.2.

In view of Theorem 2.2, we may say that our aim is to study those properties of a system $[C, F(x,y)]$ which are independent of the names we give the entities of C.

REMARK 3: We shall now give three examples of such properties.

DEFINITION 4.4: Symmetry.

Let $[C, F(x,y)]$ be any system. If

$$F(x,y) = F(y,x)$$

for all values of x and y, $F(x,y)$ is said to be symmetric in x and y, or briefly, to have symmetry, and the system is said to be commutative.

THEOREM 4.4: Symmetry is an invariant of the class $\{T\}$ of formal transformations.

PROOF: If $C_2 \backsim C_1$, then by (2.2)

$$x_2 \backsim x_1, \quad y_2 \backsim y_1, \quad z_2 \backsim z_1$$

Since $F(x_1, y_1) = F(y_1, x_1) = z_1$, $T(z_1) = z_2$,

and $T(F(x_1, y_1)) \longrightarrow G(x_2, y_2) = z_2$

$$T(F(y_1, x_1)) \longrightarrow G(y_2, x_2) = z_2$$

$G(x_2, y_2) = G(y_2, x_2)$, so that $G(x_2, y_2)$ is also symmetric.

DEFINITION 4.4: Primitivity.

Let $[C, F(x,y)]$ be any system, and let k and ℓ be two values of y. Then if the functions of the single variable x are equal (see Df. 3.3) when and only when $k = \ell$ for every pair of values k, ℓ of y, the function $F(x,y)$

is said to be primitive with respect to y .

Primitivity with respect to x is similarly defined. A function which is primitive with respect to both independent variables is said to be "primitive" without any qualifying phrase.

THEOREM 4.5: Primitivity is an invariant of the class $\{T\}$ of formal transformations.

PROOF: Clear from proof of Th. 4.4.

DEFINITION 4.5: Associativity.

Let $[\, C,\ F(x,y)\,]$ be any system, and let h , l , n denote any entities of C . Suppose

$$F(h,l) = m, \quad F(l,n) = r$$

where m and r denote known entities of C .

The function $F(x,y)$ is said to be <u>associative</u> if

$$F(m,n) = F(h,r)$$

for all sets of three entities h , l , n in C .

THEOREM 4.6: Associativity is an invariant of the class $\{T\}$ of formal transformations.

PROOF: Clear from proof of Th. 4.4.

DEFINITION 4.6: Semi-group.

A system consisting of a collection C of entities and a primitive associative function $P(x,y)$ defined over C is said to form a semi-group. If the entities of C are marks, the semi-group is said to be abstract.

NOTATION: $[\, C, P(x,y)\,]$.

REMARK: A large part of this paper is devoted to developing the properties

of abstract semi-groups. (See the remark at the beginning of Part III.)

SECTION 5. COUNTING.

PRELIMINARIES: In view of the remarks under Df. 4.3, and Th. 2.2, it is sufficient to confine our attention to collections of marks.

We assume henceforth that the marks in any collection C are all distinct and denumerable. We shall continue to refer to such special collections of marks as "collections" in accordance with the following definition.

DEFINITION 5.1: Collection of Marks.

A class whose elements consist of marks which are all distinct and denumerable is called a collection of marks.

NOTATION: We shall now restrict C to denote such a class. We shall use other letters as the occasion arises for collections of objects.

If S, S' denote marks of C, then we write $S = S'$ if S and S' denote the same mark, and $S \neq S'$ if S and S' denote different marks.

DEFINITION 5.2: Set of Marks.

If we count the marks of a collection C, we obtain a set of marks, $\mathfrak{C}$.

NOTATION: We shall denote the set of marks $\mathfrak{C}$ by

$$\mathfrak{C}: S_1, S_2, S_3, \ldots$$

It follows from Df. 5.1, and the definition of counting, that if we regard $S_1, S_2, S_3, \ldots$ as denoting marks,

$S_i = S_j$ when and only when $i = j$.

Of course $S_1, S_2, S_3, \ldots$ qua marks are distinguishable.

DEFINITION 5.3: Order of a Set.

There is a last mark S_N of $\mathcal{C}$ or no last mark according as the cardinal number of C is the positive integer N or α_0.

We shall say in these two cases $\mathcal{C}$ is of order N or order ω.

REMARK: The word "type" is usually used instead of the word "order" in Df. 5.3, but we wish to reserve "type" for more important purposes.

THEOREM 5.1: Counting is a special type of formal transformation.

PROOF: In Df. 4.1, 2 take for C_1 the collection of marks C and for C_2 the collection of objects consisting of the numbers $1, 2, 3, \ldots$. The theorem is now clear from the definition of counting.

REMARK: Before we can take advantage of this extremely important theorem, it will be necessary to develop the properties of functions of positive integral variables. This development cannot be done by specializing section 3, because the functions of section 3 do not correspond to the most general type of positive integral function.

PART II. FUNCTIONS OF INTEGERS.

SECTION 1. INTEGRAL FUNCTIONS.

DEFINITION 1.1: Range.

The set of N numbers

$1, 2, 3, \ldots, N$

is called a finite range of order N .

The set of all the numbers

$1, 2, 3, \ldots$ etc.

is called an infinite range of order ω .

NOTATION: A range whose order is unspecified is denoted by

$1, 2, 3, \ldots$

DEFINITION 1.2: Equality of Ranges.

Two ranges are said to be equal when and only when they have the same order.

REMARK: There is only one range of order ω .

DEFINITION 1.3: The Positive Integral Variable.

The particular general member x of the range

$1, 2, 3, \ldots$

is said to be a positive integral variable.

DEFINITION 1.4: Integral Function.

Suppose we have a rule whereby we can associate with each value of the positive integral variable x a definite integer $y = y(x)$. Then $y(x)$ is said to be an integral function of x .

x is called the independent, and y the dependent variable of the function.

REMARK: The various values of y need not be distinct.

NOTATION: We shall denote $y(x)$ by y_x . We shall use thruout the paper

$$a_x, b_x, \ldots, i_n, j_k, \ldots$$

to denote integral functions.

DEFINITION 1.4: Order of a Function.

The order of a function is defined as the order of the range of its independent variable.

DEFINITION 1.5: Matrix of a Function.

The ordered set of integers

$$y_1, y_2, y_3, \ldots$$

is called the matrix of the function y .

NOTATION: $\| y_i \|$ $\quad (i = 1, 2, 3, \ldots)$

DEFINITION 1.6: Equality of Functions.

Two integral functions $y = y(x)$, $Z = Z(x)$ are said to be equal when and only when they are of the same order and their matrices are equal.

THEOREM 1.1: Derived Functions.

Let $y(x)$ be a given integral function. We can define a unique function y' of the positive integral variable w by the following rule:

$$y_1 = y_1'$$

$$y_2 = y_1' \quad \text{if} \quad y_2 = y_1$$

$$y_2 = y_2' \quad \text{if} \quad y_2 \neq y_1$$

$y_3 = y_1'$ if $y_3 = y_2 = y_1$

$y_3 = y_2'$ if $y_3 = y_2 \neq y_1$ or $y_3 \neq y_2 = y_1$

$= y_3'$ if $y_3 \neq y_2 \neq y_1$ and $y_3 \neq y_1$

$= y_1'$ if $y_3 \neq y_2 \neq y_1$ and $y_3 = y_1$

and so on.

Moreover the numbers $y_1', y_2', y_3', \ldots$ are all distinct.

PROOF: Clear from Df. 1.4, and rule.

DEFINITION 1.7: Derived Function.

The function y_w' which is known as soon as y_x is known is called the derived function of y_x. Note that the ranges of w and x need not be equal.

THEOREM 1.2: Types of Integral Functions.

All functions y_x fall into three distinct types given in the table below according as the ranges of x and w are finite or infinite.

Table

Type	Range	
	x	w
1	F	F
2	I	F
3	I	I

PROOF: Clear.

DEFINITION 1.8: Range of Dependent Variable.

The set of numbers

$y_1', y_2', y_3', \ldots$

is called the range of the dependent variable y .

DEFINITION 1.9: Primitive Function.

The function $y = y(x)$ is said to be primitive if $y_i = y_j$ when and only when $i = j$ for all numbers i, j , belonging to the range of x .

THEOREM 1.3: The necessary and sufficient condition that a function be primitive is that it should be equal to its derivative.

PROOF: Clear.

SECTION 2. INTEGRAL FUNCTIONS OF TWO VARIABLES.

DEFINITION 2.1: Integral Function.

Let u , v denote two independent positive integral variables.

Suppose we have a rule which assigns to each pair of values of u and v a definite integer $Z = Z(u, v)$. Then Z is called an integral function of u and v .

NOTATION: We denote $Z(u, v)$ by Z_{uv} .

DEFINITION 2.2: Matrix of a Function.

The array of integers

$$\begin{array}{lllll} Z_{11}, & Z_{12}, & Z_{13}, & \cdots \\ Z_{21}, & Z_{22}, & Z_{23}, & \cdots \\ Z_{31}, & Z_{32}, & Z_{33}, & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdots \end{array}$$

is called the <u>matrix</u> of the function Z .

NOTATION: $\| Z_{ij} \|$ $\qquad (i, j = 1, 2, 3, \ldots)$

DEFINITION 2.3: Equality of Functions.

Two functions are said to be equal when and only when their matrices are equal.

THEOREM 2.1: Derived Function.

By reading the matrix $\| Z_{ij} \|$ by diagonals, we can define a function $Z(W)$ of the positive integral variable W . The first few values of this function are

$$Z_1 = Z_{11}, \quad Z_2 = Z_{12}, \quad Z_3 = Z_{21}, \quad Z_4 = Z_{13}, \quad Z_5 = Z_{22}, \ldots$$

page missing.

PROOF: Clear.

DEFINITION 2.4: The derivative $Z'(w)$ of $Z(u)$ is called the derived function of $Z(u,v)$.

THEOREM 2.2: Types of Integral Functions.

All functions $Z(u,v)$ fall into seven types given by the table below according as the ranges of u, v and w are finite or infinite.

Table

Type	Range		
	u	v	w
1	F	F	F
2	I	F	F
3	I	F	I
4	F	I	F
5	F	I	I
6	I	I	F
7	I	I	I

PROOF: Clear.

DEFINITION 2.5: Range of Dependent Variable.

The numbers

$$Z_1', Z_2', Z_3', \ldots$$

are called the range of the dependent variable Z.

DEFINITION 2.6: Primitive Function.

It is apparent that $Z_{k\,v}$ where k is a fixed value of the range of u, is an integral function of the variable v.

If $z_{k,v}$ is a primitive function of v for all values of k in the range of u, the function $z(u,v)$ is said to be primitive with respect to v.

Similarly, if $z_{u,l}$ is a primitive function of u for all values of l in the range of l, $z(u,v)$ is said to be primitive with respect to u.

A function $z(u,v)$ which is primitive with respect to both its independent variables is said to be primitive, without any qualifying phrase.

REMARK: It should be carefully noted that the values of a primitive function of two variables are not necessarily all distinct; for example, let the ranges of u and v be of order 3 and z_{uv} given by

$$\| z_{ij} \| \quad (i,j = 1,2,3) = \begin{matrix} 1, & 2, & 3 \\ 2, & 4, & 7 \\ 3, & 5, & 2 \end{matrix}$$

Then $z_{12} = z_{21} = z_{33}$, but nevertheless $z(u,v)$ is primitive.

THEOREM 2.3: Types of Primitive Functions.

All primitive functions $z(u,v)$ fall into four types according as the ranges of u, v and w are finite or infinite, where w is the range of the independent variable of the derived function $z'(w)$. These types are given by the following table.

Table

Type	Range		
	u	v	w
1	I	F	I
2	F	I	I
3	I	I	I
4	F	F	F

DEFINITION 2.7: Symmetric Function.

If $Z(i,j) = Z(j,i)$

for all values of i and j in the ranges of u and v,

then Z is said to be a symmetric function.

SECTION 3. OPERATIONAL FUNCTIONS.

DEFINITION 3.1: Operational Function.

The integral function $Z(u, v)$ is said to be an operational function provided

1. The ranges of u and v are identical.

2. The range of u and v contains the range of the derived function Z'.

THEOREM 3.1: Types of Operational Functions.

All operational functions $Z(u, v)$ fall into five types according as their orders and ranges are equal or not, given by the following table:

Table

Type	Order of u and v	Order of Z'	Range of u and v	Range of Z'	Relation between ranges
1	N	N	F	F	equal
2	N	$M<N$	F	F	unequal
3	ω	N	I	F	unequal
4	ω	ω	I	I	unequal
5	ω	ω	I	I	equal

PROOF: Clear.

REMARK: Operational functions are an example of the functions of Part I, Section 3, Df. 3.2.

THEOREM 3.2: No function of type 3, Th. 3.1 is primitive.

PROOF: Clear.

THEOREM 3.3: A necessary condition that a function $Z(u, v)$ be symmetric is that u and v have the same range.

All symmetric functions are of types 1, 6 or 7 under Th. 2.2.

PROOF: Clear.

DEFINITION 3.2: Associative Function.

Let $Z(u, v)$ be an operational function, and let k, l, m be any three numbers in the range of u and v.

Let $Z(k, l) = r$, $Z(l, m) = s$.

Then r, s are in the range of u and v, since $Z(u, v)$ is operational (Df. 3.1).

If now

$$Z(r, m) = Z(k, s)$$

for all sets of numbers k, l, m in the range of u and v, $Z(u, v)$ is said to be an associative function.

DEFINITION 3.3: Functional.

A primitive associative operational function will be called a functional and will be said to generate a semi-group.

DEFINITION 3.4: Types of Functionals.

A functional of type 1 or 5 Th. 3.1 will be called orthoid, a functional of type 2 or 4 holoid.

PART III. SEMI-GROUPS.

SECTION 1. INTRODUCTION.

The postulates for a semi-group given by Dickson are as follows.*

"Given a function $a \circ b$ of two arguments, and a set of elements, we say that the elements form a semi-group with respect to $\circ$ when the following postulates hold:

(1) For every two elements a and b of the set, $a \circ b$ is uniquely determined as an element of the set.

(2) $(a \circ b) \circ c = a \circ (b \circ c)$ whenever a, b, c and all the determinations of $a \circ b$, $b \circ c$, $(a \circ b) \circ c$ and $a \circ (b \circ c)$ occur in the set.

(3) If a, x, x' occur in the set, and if there are equal determinations in the set of $a \circ x$, $a \circ x'$, then $x = x'$.

(4) If there are equal determinations of $x \circ a$, $x' \circ a$, then $x = x'$."

THEOREM 1.1: The definition of Dickson and the definition 4.5 of Part I, Section 4 are identical.

PROOF: Clear from Part I.

REMARK: The only advance we have made so far is the following: Since we have shown in Part I, Section 4 that the defining properties of a semi-group are invariant under the set $\{T\}$ of formal transformations, it

---

* "On Semi-groups and the General Isomorphism between Infinite Groups," Transactions, Vol. 6, 1905, pp. 205-208.

follows that if we assume that the elements of our semi-group are denumerable, it is sufficient to study either the ordered set of marks

$$\mathcal{G}: \quad s_1, s_2, s_3, \ldots$$

and an operation $\circ$ satisfying Dickson's postulates, or the range of numbers

$$I: \quad 1, 2, 3, \ldots$$

and a primitive, associative operational function, isomorphic (Df. 4.2) with $\mathcal{G}$ and $\circ$ to deduce all the properties of denumerable semi-groups. Before embarking upon this program, it is convenient to define the term "semi-group" to mean denumerable semi-group, and to restate Dickson's postulates as follows:

DEFINITION 1.1: The Semi-Group.

A set of marks

$$\mathcal{G}: \quad s_1, s_2, s_3, \ldots$$

and a function $s_x \circ s_y$ is said to form a semi-group if the following postulates hold.

POSTULATE I. Closure.

If s_a and s_b are any two elements of $\mathcal{G}$, $s_a \circ s_b$ is a uniquely determined element of $\mathcal{G}$.

POSTULATE II. Associativity.

If s_a, s_b, s_c are any three elements of $\mathcal{G}$,

$$(s_a \circ s_b) \circ s_c = s_a \circ (s_b \circ s_c)$$

POSTULATE III. Cancellativity.

If s_a, s_b, s_c are any three elements of $\mathcal{G}$, then

(a) if $S_a \circ S_b = S_a \circ S_c$, $S_b = S_c$

(b) if $S_b \circ S_a = S_c \circ S_a$, $S_b = S_c$

DEFINITION 1.2: Left and Right Semi-groups.

A system $[G; \circ]$ satisfying Postulates I, II, III(a) is called a left semi-group.

A system $[G; \circ]$ satisfying Postulates I, II, III(b) is called a right semi-group.

DEFINITION 1.3: Closed and Closed Associative Systems.

A system $[G; \circ]$ consisting of a set of marks G and a function $S_x \circ S_y$ which satisfies Pos. I is said to be a <u>closed</u> system.

A system $[G; \circ]$ satisfying both Pos. I and Pos. II is said to be a <u>closed associative</u> system.

NOTATION:

Closed system	$[G; \circ / I]$
Closed associative system	$[G; \circ / I, II]$
Left semi-group	$[G; \circ / I, II, III(a)]$
Right semi-group	$[G; \circ / I, II, III(b)]$
Semi-group	$[G; \circ / I, II, III]$

REMARK: Note that these systems are arranged in order of decreasing generality. It follows that the properties of $[G; \circ / I]$ and $[G; \circ / I, II]$ developed in the next two sections are also properties of semi-groups.

DEFINITION 1.4: Commutativity.

It is necessary to consider later systems which satisfy a fourth

postulate, which we shall call the postulate of commutativity, viz:-

POSTULATE IV. Commutativity.

If S_a , S_b are any two elements of $\mathcal{G}$, then

$$S_a \circ S_b = S_b \circ S_a$$

Any system $[\mathcal{G}, \circ]$ satisfying this postulate is said to be commutative.* The extension of the notation under Df. 1.2 is obvious.

DEFINITION 1.5: Abelian Semi-group.

The system $[\mathcal{G}, \circ / I, II, III, IV]$ is called an Abelian semi-group.

* compare Df. 4.4 of Part I.

SECTION 2. CLOSED SYSTEMS.

PRELIMINARY: Consider the system $[\mathcal{C}, o/I]$ so that we have a set of marks

$$\mathcal{C}: S_1, S_2, S_3, \ldots$$

and a function $S_x o S_y$ satisfying Postulate I.

DEFINITION 2.1: Sequence.

Let J_n denote an integral function of n whose order is not greater than the order of $\mathcal{C}$, and denote the mark S_{J_n} by u_n.

Then the ordered set of marks

$$u_1, u_2, u_3, \ldots$$

is called a sequence of marks of $\mathcal{C}$, or, briefly, a sequence. The range of n is called the range of the sequence.

NOTATION: $(u_n): u_1, u_2, u_3, \ldots, u_n, \ldots$

(2.1) $(u_r): u_1, u_2, u_3, \ldots, u_r, \ldots$

DEFINITION 2.2: Equality of Sequences.

Two sequences

$$(u_r): u_1, u_2, u_3, \ldots, u_r, \ldots$$
$$(v_r): v_1, v_2, v_3, \ldots, v_r, \ldots$$

are said to be equal when and only when they have the same range, and

$u_r = v_r$ for all numbers r in their range.

NOTATION: $(u_r) = (v_r)$

DEFINITION 2.3: The Displacement Symbol.

Let a be a number. Denote the operation of replacing in (2.1) the mark u_r by the mark u_{r+a} by

(2.2) $E^a u_r = u_{r+a}$ $\qquad (a, r \geq 1)$

Then E^a is called a displacement symbol.*

DEFINITION 2.4: The Symbol 1 .

If we allow a to assume the value 0 in (2.2), we have

$$E^0 u_r = u_r$$

so that E^0 leaves any mark of (2.1) unchanged.

We denote E^0 by 1 , so that

$$E^0 u_r = 1 \cdot u_r = u_r$$

DEFINITION 2.5: Multiplication of Displacement Symbols.

Let E^a , E^b be two displacement symbols, where it is understood henceforth that $a, b, \geq 0$. By (2.2)

$$E^a(E^b u_r) = E^a u_{r+b} = u_{r+b+a} = E^{b+a} u_r \quad **$$

E^a , E^b are said to be <u>multiplied</u> to form the <u>product</u> E^{b+a} .

THEOREM 2.1: Multiplication of displacement symbols is associative and commutative.

PROOF: Clear from Dfs. 2.3, 2.5.

DEFINITION 2.6: Powers of a Displacement Symbol.

The displacement symbol E^{na} $(n, a \geq 0)$ is called the n^{th} power of E^a .

THEOREM 2.2: Any displacement symbol E^a is the a^{th} power of the fundamental displacement symbol E defined by

$$E = E^1$$

---

* Stefansson: Interpolation, Chap. 1, Baltimore, 1927.
We tacitly assume is less than or equal to the order of the sequence.

** Again, we assume $r + b + a \leq$ the order of the sequence.

PROOF: Clear from Dfs. 2.3, 2.4, 2.6.

THEOREM 2.3: Assume that the order of $\mathcal{G}$ and of $\mathcal{J}_n$ in Df. 2.1 is ω. If after a certain value r' of r, the set of marks

$$u_1, u_2, u_3, \ldots, u_{r-1}, u_r,$$

in the sequence (u_r) repeats itself indefinitely in the sequence, there will be a least value $r' = \mu$ for which this is the case.

PROOF: Clear.

REMARK: If the order of $\mathcal{J}_n$ is N, we consider the set of marks

$$u_1, u_2, u_3, \ldots$$

where $u_m = \mathcal{S}_{j_n}$ $\qquad m \equiv n \bmod N \quad (1 \leq n \leq N)$

and apply Theorem 2.3 to it.

DEFINITION 2.7: With the hypotheses of Th. 2.3, the μ marks

$$u_1, u_2, u_3, \ldots, u_\mu$$

are said to form a cycle of period μ, and the sequence (u_r) is said to be recurring with period μ.

NOTATION: We write $(u_r)_\mu$ for a recurring sequence of period μ.

THEOREM 2.4: A recurring sequence is completely determined by its cycle, and to every recurring sequence there corresponds a finite ordered set of marks of $\mathcal{G}$.

PROOF: Clear from Df. 2.7.

THEOREM 2.5: If (u_r) recurs for $r = r'$, μ is a divisor of r'.

PROOF: Clear from Df. 2.7.

DEFINITION 2.8: Displacement of a Cycle.

From (2.3) it follows that if $(u_r)_\mu$ is a recurring sequence

of period μ,

$$E^a u_r = E^b u_r = u_c \qquad a \equiv b \equiv c \bmod \mu \quad (1 \leq c \leq \mu)$$

Hence

$$E^a (u_r)_\mu = u_{a+1}, u_{a+2}, \ldots, u_{\mu-1}, u_\mu, u_1, u_2, \ldots u_a$$

NOTATION: $E^a (u_r)_\mu = (u_{r+a})_\mu$

$(u_{r+a})_\mu$ is called a displacement of $(u_r)_\mu$.

THEOREM 2.6: The operations

$$E, E^2, E^3, \ldots, E^\mu$$

associated with the recurring sequence (u_r) of period μ form a cyclic group of which E is the generator and E^μ the identity.

PROOF: Clear from the definition of a cyclic group.

NOTATION: We shall denote a cyclic group of order μ by $[CG]_\mu$.

We note for future reference the following important properties of a cyclic group.

Properties of a Cyclic Group.*

1. Every element of a $[CG]_\mu$ is some power of a single element of period μ, and there is one and only one cyclic group whose order is an arbitrary natural number μ. Furthermore, if μ is a prime π, the only group of order π is the $[CG]_\pi$, and there is one and only one cyclic group of infinite order.

2. The $[CG]_\mu$ contains one and only one sub-group (also cyclic) whose order is a given divisor of μ, so that the determination of all the factors of μ gives all the sub-groups of the $[CG]_\mu$.

---

* Finite Groups, Miller, Blichfeldt and Dickson, pp. 54-57, New York, 1916.

3. If $\mu = K \cdot n$, the sub-group of order K contains $\phi(K)$ generators, and if E^{λ} generates $[CG]_K$, $E^{\lambda\rho}$ generates $[CG]_\mu$ when and only when $\Pi(\rho, K) = 1$.

4. The group of cyclic substitutions on μ letters, the group of least positive residues modulo μ with the operation addition, and the group of the μ^{th} roots of unity with the operation of multiplication are simply isomorphic with the $[CG]_\mu$.

DEFINITION 2.9: The Cyclic Group of a Cycle.

The cyclic group

$$[CG]_\mu : E, E^2, E^3, \ldots, E^\mu$$

is called the cyclic group of displacements associated with the cycle $(u_r)_\mu$.

DEFINITION 2.10: Equivalent Cycles.

Let $(u_r)_\mu$, $(v_r)_\mu$ be two cycles of the same period μ . Then $(v_r)_\mu$ is said to be equivalent to $(u_r)_\mu$ when and only when it is a displacement of $(u_r)_\mu$.

NOTATION: $(v_r)_\mu \backsim (u_r)_\mu$

THEOREM 2.7: The class of all cycles equivalent to $(u_r)_\mu$ forms the set of cyclic substitutions on the μ marks

$$u_1, u_2, u_3, \ldots, u_\mu$$

PROOF: Clear from Dfs. 2.10, 2.8 and properties of the $[CG]_\mu$.

THEOREM 2.8: The relation $\backsim$ of Df. 2.10 is symmetric, transitive and reflexive.

PROOF: Clear from Dfs. 2.8, 2.10.

REMARK: We have developed the section above as the simplest example of the "equivalence relation" which appears continually in general arithmetic.

THEOREM 2.9: Assume $\mathcal{G}$ contains precisely N marks

$$s_1, s_2, s_3, \ldots, s_N$$

and let

$$\mu = \pi_1^{m_1} \cdot \pi_2^{m_2} \cdots \pi_s^{m_s}$$

be the factorization of μ, where $\pi_1, \pi_2, \ldots, \pi_s$ are distinct prime numbers. Then $\mathcal{G}$ contains precisely

$$N(\mu) = N^{\mu} - \sum N^{\frac{\mu}{\pi_1}} + \sum N^{\frac{\mu}{\pi_1 \cdot \pi_2}} \cdots + (-1)^s N^{\frac{\mu}{\pi_1 \cdot \pi_2 \cdots \pi_s}}$$

cycles of period μ.

PROOF: Let $M(x)$ be the number of sequences (u_r) which recur for $r = x$ and $N(x)$ the number which have a period of exactly x. Then by Th. 2.5,

$$M(\mu) = \sum_{\delta/\mu} N(\delta)$$

But clearly if N is the number of marks of $\mathcal{G}$,

$$M(\mu) = N^{\mu}$$

The result stated now follows by Dedekind's inversion theorem*, the summations extending over the combinations $1, 2, \ldots, s$ at a time of the distinct prime factors $\pi_1, \pi_2, \ldots \pi_s$ of μ.

THEOREM 2.10: There are $\frac{N(\mu)}{\mu}$ distinct sets of equivalent cycles of period μ in $\mathcal{G}$.

PROOF: Clear from Th. 2.8, Df. 2.10.

---

* Dickson's History, Vol. 1, p. 441, eq. (2).

DEFINITION 2.11: Product of Recurring Sequences.

Let $(u_r)_\mu$, $(v_r)_\nu$ be two recurring sequences of periods μ and ν respectively. The sequence $(u_r \circ v_r)$ is called the product of the sequences $(u_r)_\mu$ and $(v_r)_\nu$.

NOTATION: $(u_r \circ v_r) = (u_r) \circ (v_r)$

REMARK: It is scarcely necessary to add $u_r \circ v_r$ denotes a definite mark of $\mathcal{C}$ determined by

$$u_r = S_{j_r}, \quad v_r = S_{k_r}$$
$$u_r \circ v_r = S_{j_r} \circ S_{k_r}$$

THEOREM 2.11: With the hypotheses of Df. 2.11, $(u_r \circ v_r)$ is also a recurring sequence, whose order is the least common multiple of μ and ν.

PROOF: Clear.

REMARK: This theorem is fundamental in the general theory of recurring series.

REMARK: Any finite sequence

$$u_1, u_2, u_3, \ldots, u_n, \ldots u_N$$

can be written as a recurring sequence, by letting

$$u_m = S_{j_r} = u_r \qquad m \equiv r \bmod N \quad (1 \leq r \leq N)$$

so that Df. 2.11 gives us a method for defining the product of any two sequences.

SECTION 3. CLOSED ASSOCIATIVE SYSTEMS.

PRELIMINARY: Consider the system $[\mathcal{G}, \circ / \text{I}, \text{II}]$ so that we have a set of marks

$$\mathcal{G} : S_1, S_2, S_3, \ldots$$

and a function $S_x \circ S_y$ satisfying Postulates I and II.

DEFINITION 3.1: Power of an Element.

If S is any element of $\mathcal{G}$, r any positive integer, the symbol S^r defined by

(3.1) $$S^{r+1} = S^r \circ S$$
$$S^1 = S$$

is called the r^{th} power of S.

THEOREM 3.1: $\mathcal{G}$ contains the r^{th} power of any element in it.

PROOF: Clear from Df. 3.1, Pos. I and induction.

THEOREM 3.2: If S is any element of $\mathcal{G}$,

(3.2) $$S^r \circ S^t = S^t \circ S^r = S^{t+r}$$

PROOF: $$S^2 = S^1 \circ S = S \circ S^1 \quad \text{by (3.1)}$$

Assume

$$S^k \circ S = S \circ S^k$$

Then

$$S \circ S^{k+1} = S \circ (S^k \circ S) \quad \text{by Df. 3.1}$$
$$= (S \circ S^k) \circ S \quad \text{by Th. 3.1, Pos. II}$$
$$= (S^k \circ S) \circ S \quad \text{by hyp.}$$
$$= S^{k+1} \circ S \quad \text{by Df. 3.1.}$$

Hence by induction

(A) $$S \circ S^r = S^r \circ S$$

and

$$S^1 \circ S^r = S^r \circ S^1 = S^r \circ S = S^{r+1} \quad \text{by (3.1)}$$

$(r = 1, 2, 3, \ldots)$

Assume

$$S^k \circ S^r = S^r \circ S^k = S^{r+k} \qquad (k \text{ fixed})$$

Then

(B) $S^r \circ S^{k+1} = S^r \circ (S^k \circ S)$ by Df. 3.1

$= S^r \circ (S \circ S^k)$ by (A) for $r = k$

$= (S^r \circ S) \circ S^k$ by Th. 3.1, Pos. II

$= (S \circ S^r) \circ S^k$ by (A)

$= S \circ (S^r \circ S^k)$ by Pos. II

$= S \circ (S^k \circ S^r)$ by hyp.

$= (S \circ S^k) \circ S^r$ by Pos. II

or

(C) $S^r \circ S^{k+1} = S^{k+1} \circ S^r$ by (A) and Df. 3.1

Now

$$S^{r+k} \circ S = S^{r+k+1}$$

by Df. 3.1

and

$S^{r+k} \circ S = (S^r \circ S^k) \circ S$ by hyp.

$= S^r \circ (S^k \circ S)$ by Pos. II

$= S^r \circ S^{k+1}$ by (B)

$= S^{k+1} \circ S^r$ by (C)

or

$$S^{r+k+1} = S^{k+1} \circ S^r = S^r \circ S^{k+1}$$

Hence by induction

$$S^r \circ S^t = S^t \circ S^r = S^{t+r}$$

DEFINITION 3.2: One-dimensional Spread.

A sequence

(h_r): $h_1, h_2, h_3, \ldots h_r, \ldots$

where

(3.3) $h_r = S_{j_r} = S^r$

and S is an element of $\mathcal{C}$ is called a one-dimensional spread, of which S is a generator.

NOTATION: $[S]$

THEOREM 3.3: Any one-dimensional spread is an instance of a system which is closed, associative, and commutative;

(3.4) $h_r \circ h_s = h_s \circ h_r = h_{s+r}$ $\quad (r, s = 1, 2, 3, \ldots)$

PROOF: Clear from Th. 3.1, 3.2, Df. 3.2.

THEOREM 3.4: If a one-dimensional spread contains an infinite number of different elements, they are all distinct.

PROOF: Let $[S]$ be a one-dimensional spread, so that $S^r = h_r$ in the sequence (h_r).

If the h's are not all distinct, there exist positive integers i and j such that

(3.5) $h_i = h_{i+j}$

Then

$$h_{i+r} = h_{i+r+j} \qquad \left(\begin{array}{c} 0 \leq r \leq j-1 \\ n = 0, 1, 2, \ldots \end{array} \right)$$
$$h_{i+r+nj} = h_{i+r}$$

by (3.2), (3.3), (3.4), (3.5) and induction, so that (h_r) consists of at most $i+j$ different elements

$$h_1, h_2, h_3, \ldots h_{i-2}, h_{i-1}, h_i, h_{i+1}, \ldots h_{i+j-1}, h_{i+j}$$

REMARK: Although the general theory of spreads of any number of dimensions whose generators belong to a closed associative system, a semi-group, or a commutative semi-group, is a subject of extreme interest and importance, it will not be developed here, as it would take us too far from our original aim of defining an arithmetic. Such a definition is, indeed, an indispensible preliminary to the theory of spreads itself. Suffice it to say that in the theory of spreads we have the key to the whole problem of ideals and ideal numbers in any conceivable arithmetic, in the wider sense.

SECTION 4. THE IDENTITY.

DEFINITION 4.1: Identity of a Left Semi-group.

Let $[G, \circ / I, II, III(a)]$ be a left semi-group.

If G contains an element ι such that for at least one element S of G,

(4.1) $S \circ \iota = S, \qquad G / S, \iota$

then ι is called an identity of G.

THEOREM 4.1: If the identity ι in (4.1) exists,

(4.2) $\iota \circ S' = S'$

where S' is any element of G.

PROOF:

$S \circ S' = S \circ S'$

$S \circ \iota = S$ by hyp.

$(S \circ \iota) \circ S' = S \circ S'$ by substitution

$S \circ (\iota \circ S') = S \circ S'$ by Pos. II

$\iota \circ S' = S'$ by Pos. III(a)

THEOREM 4.2: If S' is any element of G commutative with the element S of (4.1), so that

$$S \circ S' = S' \circ S .$$

then

$$S' \circ \iota = S'$$

PROOF:

$S \circ \iota = S$ by Hyp.

$S' \circ (S \circ \iota) = S' \circ S$

$(S' \circ S) \circ \iota = S' \circ S$ by Pos. II

$(S \circ S') \circ \iota = S \circ S'$ by hyp.

$S \circ (S' \circ \iota) = S \circ S'$ by Pos. II

$S' \circ \iota = S'$ by Pos. III(a)

THEOREM 4.3: If the element ι of (4.1) exists, it is unique.

PROOF: Suppose there were a second element j such that

(4.3) $S \circ j = S \qquad \mathcal{G} / S, j$

By hyp., $S \circ \iota = S$; hence $\iota = j$ by Pos. III(a).

REMARK: It seems impossible to infer from (4.1) that $S' \circ \iota = S'$ for every element S' of $\mathcal{G}$ without the use of Pos. III(b). To prove this conjecture it would be necessary to construct an actual example, which I have not yet been able to do.

THEOREM 4.4: Theorems 4.1, 4.2, 4.3 remain true if the S in (4.1) is replaced by the ι of (4.1).

PROOF: Clear.

REMARK: The corresponding theorems and definition for a right semi-group are apparent.

THEOREM 4.5: Let $[\mathcal{G}, \circ / I, II, III]$ be a semi-group. Then if $\mathcal{G}$ contains an element ι such that $\iota \circ \iota = \iota$, then for any element S of $\mathcal{G}$,

$$S \circ \iota = \iota \circ S = S$$

and, moreover, ι is unique.

PROOF: Clear from Th. 4.1 - 4.4 and the remarks above.

DEFINITION 4.2: If the ι of Theorem 4.5 exists, it is called the identity of the semi-group.

THEOREM 4.6: Let $[\mathcal{G}, \circ / I, II, III(a)]$ be a left semi-group. If $\mathcal{G}$ contains an element ι such that (4.1) holds for every element S of $\mathcal{G}$, then for every S

$$S \circ \iota = \iota \circ S = S$$

and ι is unique.

PROOF: Clear from Th. 4.1 - 4.4.

REMARK: The corresponding theorem for a right semi-group is apparent. Hereafter, we shall state all definitions and theorems for left semi-groups alone; the corresponding definitions and theorems for right semi-groups are easily inferred.

REMARK: The substance of these theorems on the identity are given in Dickson's paper, but they are proved only for a semi-group, on much stronger assumptions.

REMARK: Although it is unnecessary to postulate the existence of an identity element in a system in order for it to be an "arithmetic" in the narrow sense of the definition given at the close of Part I, Section 1*, nevertheless instances of systems in which an identity exists are of frequent occurrence, and the abstract theory of such systems is of considerable interest.

We accordingly frame the following postulate:

POSTULATE V. The set $\mathcal{G}$ contains an element ι such that

(a) for every element S in the set,

$$S \circ \iota = S$$

(b) for every element S in the set,

$$\iota \circ S = S$$

(c) $$\iota \circ \iota = \iota$$

THEOREM 4.7: The properties expressed in Pos. V are invariants of the class $\{T\}$ of formal transformations defined in Part I, Section 4.

PROOF: Clear.

---

* For example, the set of all numbers of the form $2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma}$ where α, β, γ run over all the positive integers form an arithmetic in the sense of Part I, Section 1, but the set does not contain an identity.

PART IV. THE OPERATION OF DIVISION.

SECTION 1. INVERSE OPERATIONS.

DEFINITION 1.1: Table of Entry of a System.

Let $[\mathcal{G}; \circ / I]$ be any closed system. The matrix

$\| S_i \circ S_j \|$ $\quad (i, j = 1, 2, 3, \ldots)$

where we write for each $S_i \circ S_j$ its unique determination in $\mathcal{G}$, is called the table of entry of the system.

REMARK: The table of entry is simply isomorphic with the matrix $\| z_{ij} \|$ of the operational function $Z(x, y)$ associated with $S_x \circ S_y$.

DEFINITION 1.2: Inversion Problems.

Let $[\mathcal{G}; \circ / I]$ be any closed system. In the function

(1) $\quad S_z = S_x \circ S_y$

we regard S_z as known when S_x and S_y are given. Let us suppose instead now that S_z is known; there are three conceivable cases.

(i) Given S_z, to find S_x and S_y.

(ii) Given S_z and S_x, to find S_y.

(iii) Given S_z and S_y, to find S_x.

These three cases are said to constitute the inversion problem for the function (1). Obviously (i) includes (ii) and (iii).

THEOREM 1.1: Types of Solution.

There are six types of solution conceivable for an inversion problem, according as we can find an infinite number, a finite number, or no S_x's and S_y's to satisfy (1) for a given S_z. These types are given by the following table:

Table

Type	Number of S_x	Number of S_y
1	I	I
2	I	F
3	F	I
4	F	F
5	none	—
6	—	none

PROOF: Clear.

THEOREM 1.2: The necessary and sufficient condition that all possible solutions of the inverse problem be of type 4 in Th. 1.1, is that any particular element S of $\mathcal{G}$ appear in the table of entry of the system at most a finite number of times.

PROOF: Clear.

THEOREM 1.3: The necessary and sufficient condition that the inverse problem always have a solution is that every element S of $\mathcal{G}$ appear in the table of entry of the system at least once.

PROOF: Clear.

THEOREM 1.4: Solutions of Types 1, 2, 3 can occur only when the set is of order ω.

PROOF: Otherwise the table of entry is finite.

THEOREM 1.5: A sufficient condition that the problem of inversion always be solvable in a finite number of steps is that $\mathcal{G}$ be of finite order.

PROOF: Clear.

THEOREM 1.6: If the inversion problem in $[\mathcal{G}; o/I]$ has the property

that all its solutions are of type 4, Th. 1.2, this property is an invariant of the set $\{T\}$ of formal transformations of $\mathcal{C}$ defined in Part I, Section 4 for $\mathcal{C}$ of order N or order ω .

PROOF: Clear.

THEOREM 1.7: If $\mathcal{C}$ is of order ω , a necessary and sufficient condition that all the solutions of the inversion problem for be of type IV is that in the operational function $z = z(u,v) = F(u,v)$ associated with the system,

(1.1) $z \longrightarrow \infty$ as $u \longrightarrow \infty$

and $z \longrightarrow \infty$ as $v \longrightarrow \infty$

Moreover when this condition is satisfied, the inversion problem can always be solved for any given value k of z in a finite number of steps.

PROOF: Let k be any fixed value of z , and consider the solutions of

(i) $k = F(u,v)$

Assume first $z \not\longrightarrow \infty$ as $u \longrightarrow \infty$.

Then we can find two fixed numbers Z and U such that

(ii) $z < Z$ for all values of $u > U$; i.e., for an infinite number of values of u .

Hence if we consider the solutions of

$$1 = F(u,v), \quad 2 = F(u,v), \quad \ldots, \quad Z = F(u,v)$$

there is at least one value k $(1 \leq k \leq Z)$ such that (i) has an infinite number of solutions u , so that the inversion problem for this k is not of type 4. Similarly, it is necessary that $z \longrightarrow \infty$ as $v \longrightarrow \infty$.

Now assume that the conditions (1.1) are satisfied, and let us consider the solution of the inversion problem (1) for $z = k$, a fixed number.

From (1.1), we can find a fixed number $N = N(k)$ such that when $u > N$, $v > N$, $z > k$.

It follows that all possible solutions of (i) lie in the matrix formed of the first N rows and N columns of $\| z_{uv} \|$, so that they are necessarily finite in number and can be found in a finite number of steps.

EXAMPLE: Consider this instance of $[G, \circ / I]$;- the set of numbers $1, 2, 3, \ldots$ and $\circ$ ordinary multiplication. Then $z = xy$ and the condition (1.1) is fulfilled. It is not difficult to make the extension to algebraic integers and multiplication, unit factors disregarded, by thinking of them ranged in order of increasing norms.

REMARK: It should be carefully noted that if G is of order ω, it is <u>not</u> sufficient that the solutions of the inversion problem be all finite for us to find them in a finite number of steps without the use of Th. 1.7; for if $k = F(u, v)$ has no solutions, we must be able to assign limits to u and v beyond which we need not look for solutions, in order to be able to solve the inversion problem in this special case in a finite number of steps; but this is precisely what (1.1) gives us.

SECTION 2. DIVISION.

PRELIMINARIES: Let $G = [G; \circ / I, II, III(a), IV(a)]$ denote henceforth a left semi-group with elements

$$g_1, g_2, g_3, \ldots$$

and an identity element 1.

We use g, g', ... occasionally for particular general elements of G. The notation $G / g, g', g_h$ means G contains the elements g, g' and g_h.

DEFINITION 2.1: Left Divisors.

If for two particular elements g_h, g_k of G, there exists a g_x in G such that*

(2.1) $g_h \circ g_x = g_k \qquad G / g_x$

we say that g_h is a left divisor of g_k, or that it left divides g_k. g_x is called the "quotient" obtained by left division of g_k by g_h," or when there is no ambiguity possible, the "quotient."

NOTATION: $g_h = \Pi_L(g_k)$, $g_h \mid g_k$

DEFINITION 2.2: Right Divisors.

If for two particular elements g_h, g_k of G, there exists a g_y in G such that

$$g_y \circ g_h = g_k$$

we say that g_h is a right divisor of g_k.

NOTATION: $g_h = \Pi_R(g_k)$

---

* Compare Section 1, Df. 1.2.

DEFINITION 2.3: Divisor.

If at least one of the two statements $g_h = \Pi_L(g_k)$,

$g_h = \Pi_R(g_k)$ is true, we say that g_h is a divisor of g_k ,

or that it divides g_k .

NOTATION: $g_h = \Pi(g_k)$, g_h / g_k .

DEFINITION 2.4: Multiples.

Under the conditions of Df. 2.1, (2.2) g_k is called a right (left) multiple of g_h , and is said to right multiply (left multiply) g_h .

NOTATION: $g_k = M_R(g_h)$ $(= M_L(g_h))$

If at least one of the two statements $g_k = M_L(g_h)$,

$g_k = M_R(g_h)$ is true, we say g_k is a multiple of g_h ;

or that g_k multiplies g_h .

NOTATION: $g_k = M(g_h)$

THEOREM 2.1: The g_x of Df. 2.1 is unique.

PROOF: $G / g_h, g_x, g_k, \quad g_h \circ g_x = g_k$ by hyp.

Assume G / g_x' such that $g_h \circ g_x' = g_k$

Then

$$g_h \circ g_x = g_h \circ g_x'$$

$$g_x = g_x'$$ by Pos. III(a).

SECTION 3. UNITS.

PRELIMINARY: The results of this section are due in the main to Dickson, who, however, proved them for a semi-group only.

THEOREM 3.1: If for any element g_h of G there exists an element g_k such that

(3.1) $g_h \circ g_k = 1$ ($G/1$ by Pos. V(a))

then

$$g_k \circ g_h = 1$$

Furthermore, if such a g_k exists, it is unique.

PROOF: $G / g_h, g_k, \; g_h \circ g_k = 1$ by hyp.

$$g_{h_1} = g_h$$

$$(g_h \circ g_k) \circ g_{h_1} = 1 \circ g_k$$

$$g_{h_1} \circ (g_k \circ g_h) = g_{h_1} \circ 1 \qquad \text{by Pos. II and III, Th.4.6}$$

$$g_k \circ g_{h_1} = 1 \qquad \text{by Pos. III(a)}$$

g_k is unique. For suppose there were a second element g_k' such that $g_h \circ g_k' = 1$. Then

$$g_{h_1} \circ g_k = g_h \circ g_k'$$

$$g_k = g_k' \qquad \text{by Pos. III(a).}$$

DEFINITION 3.1: Inverse.

The element g_k of (3.1) if it exists is called the inverse of g_h .

THEOREM 3.2: (i) If g_k is the inverse of g_h , g_h is the inverse of g_k . (ii) 1 is its own inverse.

PROOF: Clear from Th. 3.1, Df. 3.1, and Th. 4.5, Part III.

THEOREM 3.3: Every left divisor of 1 is a right divisor of 1 and conversely.

PROOF: Let $g_h = \mathfrak{D}_L(1)$, $g_k = \mathfrak{D}_R(1)$

$g_h \circ g_x = 1$ and $g_y \circ g_k = 1$ $G / g_x, g_y$ by Df. 2.1, 2.2

$g_x \circ g_h = 1$ and $g_k \circ g_y = 1$ by Th. 3.1

$g_h = \mathfrak{D}_R(1)$ and $g_k = \mathfrak{D}_L(1)$ by Df. 2.2, 2.1

We may henceforth speak simply of the divisors of 1 without ambiguity.

DEFINITION 3.2: The Units.

The class of divisors of 1 in G is denoted by

$E : \epsilon_1, \epsilon_2, \ldots, \epsilon_r \ldots$

Any member of it, ϵ_r , is called a unit.

THEOREM 3.4: E is not a null-class.

PROOF: $1 \circ 1 = 1$, $1 / 1$, 1 is a unit.

THEOREM 3.5: The class E of units of G form a group with respect to $\circ$.

PROOF: (i) If ϵ_s , ϵ_r are any two elements of E , $\epsilon_s \circ \epsilon_r$ is uniquely determined as an element of E .

For $\epsilon_s \circ \epsilon_r$ is uniquely determined as an element of G , since G / ϵ_r , ϵ_s by Df. 3.2, by Pos. I.

Moreover, $E / \epsilon_r \circ \epsilon_s$, for by Df. 3.2, 2.1, Th. 3.1

$\epsilon_x \circ \epsilon_x = 1$, $\epsilon_y \circ \epsilon_s = 1$ $E / \epsilon_x, \epsilon_y$

$(\epsilon_r \circ \epsilon_x) \circ (\epsilon_y \circ \epsilon_s) = 1 \circ 1 = 1$

$\epsilon_r \circ (\epsilon_x \circ (\epsilon_y \circ \epsilon_s)) = 1$ by Pos. II

$\epsilon_r \circ (\epsilon_x \circ \epsilon_y) \circ \epsilon_s = 1$ by Pos. II

$(\epsilon_r \circ (\epsilon_x \circ \epsilon_y)) \circ \epsilon_s = 1$ by Pos. II

$\epsilon_s \circ (\epsilon_r \circ (\epsilon_x \circ \epsilon_y)) = 1$ by Th. 3.1

$(\epsilon_s \circ \epsilon_r) \circ (\epsilon_x \circ \epsilon_y) = 1$ by Pos. II

$\epsilon_s \circ \epsilon_r / 1$, E, $\epsilon_s \circ \epsilon_r$ by Df. 2.3, 3.2

(ii) If ϵ_r , ϵ_s , ϵ_t are any three elements of E

$(\epsilon_r \circ \epsilon_s) \circ \epsilon_t = \epsilon_r \circ (\epsilon_s \circ \epsilon_t)$

for $G / \epsilon_r, \epsilon_s, \epsilon_t$ and Pos. II holds.

(iii) E contains an element ϵ_i such that for any element ϵ_r,

$\epsilon_i \circ \epsilon_r = \epsilon_r \circ \epsilon_i = \epsilon_r$

for $E / 1$, G / ϵ_r, $1 \circ \epsilon_r = \epsilon_r \circ 1 = \epsilon_r$

by Th. 4.6, Part III.

(iv) For every ϵ_r there is an ϵ_s such that

$\epsilon_r \circ \epsilon_s = \epsilon_s \circ \epsilon_r = \epsilon_i = 1$

from Df. 3.2, 2.3, Th. 3.1.

But (i) - (iv) are the postulates for an abstract group.

THEOREM 3.6: The product of any number of units is a unit.

PROOF: Clear from Th. 3.5.

THEOREM 3.7: If $g_h \circ g_k$ is a unit, g_h and g_k are both units.

PROOF: Let $g_h \circ g_k = \epsilon_1$, and let ϵ_2 be the inverse of ϵ_1 . Then

$(g_h \circ g_k) \circ \epsilon_2 = \epsilon_1 \circ \epsilon_2 = 1$ by Th. 3.5

and $\epsilon_2 \circ (g_h \circ g_k) = \epsilon_2 \circ \epsilon_1 = 1$ by Th. 3.5

or

$g_h \circ (\quad) = 1$

$(\epsilon_2 \circ g_h) \circ (\quad) = 1$

$(\breve{\epsilon}_2 \circ g_h) \circ g_k = 1$
$g_h \circ (g_k \circ \epsilon_2) = 1$ by Pos. II

$g_h = \Box(1), \quad g_k = \Pi(1)$ by Df. 2.3

$E / g_h, g_k$ by Df. 3.2.

THEOREM 3.8: If $g_1 \circ g_2 \circ \cdots \circ g_r$ is a unit,

$g_1, g_2, \ldots g_r$ are all units.

PROOF: Clear from Pos. II and Th. 3.7.

SECTION 4. INTEGRALITY.

PRELIMINARY: Let $G = [\mathcal{G}; \circ / I, II, III(a), IV(a)]$.

It may happen that $\mathcal{E}$ coincides with G. It follows then that G is a group by Th. 3.5. But in a group, the problem of inversion of Section 1 is trivial; for

THEOREM 4.1: If g_a, g_b are any two elements of a group G, then g_a left divides g_b and g_a right divides g_b.

PROOF: Let g_a' be the inverse of g_a. Then

$$(g_a \circ g_a') \circ g_b = 1 \circ g_b = g_b$$

But also

$$(g_a \circ g_a') \circ g_b = g_a \circ (g_a' \circ g_b)$$

Hence

$$g_a = \Pi_L (g_b)$$

and similarly

$$g_a = \Pi_R (g_b)$$

It follows that in a group, every element divides every other element, which violates one of our fundamental conditions for an arithmetic (Part I, Section 1). To insure that our system shall not be a group, we frame the following postulate:

POSTULATE VI. Integrality.

The set $\mathcal{C}$ contains two elements s_h and s_k such that

(a) $s_h \circ s_x = s_k$

is satisfied for no element s_x of $\mathcal{C}$.

(b) $s_y \circ s_h = s_k$

is satisfied for no element s_y of $\mathcal{C}$.

Assuming $\mathcal{C}$ contains the element ι of Postulate V, the system contains an element S_h such that

(c) $S_h \circ S_x = \iota$

is satisfied for no element S_x of $\mathcal{C}$.

(d) $S_y \circ S_h = \iota$

is satisfied for no element S_y of $\mathcal{C}$.

DEFINITION 4.1: Integral Left Semi-Group.

The system $[\mathcal{C}; \circ / I, II, III(a), VI(a)]$ is called an integral left semi-group.

NOTATION: We shall continue to use G and g for this system.

THEOREM 4.2: G contains an infinite number of distinct elements.

PROOF: Consider the element g_h of Pos. VI(a).

If $g_h, g_h^2, g_h^3, \ldots$ are all distinct, the theorem is proved. Assume they are not all distinct. Then there exist integers r and s such that

$$g_h^{\,r} = g_h^{\,r+s} \qquad (r, s \geq 1)$$

Now
$$g_h^{\,r} \circ g_k = g_h^{\,r+s} \circ g_k = g_h^{\,r} \circ g_h \circ (g_h^{\,s-1} \circ g_k)$$
$$g_k = g_h \circ (g_h^{\,s-1} \circ g_k)$$

contradicting Pos. VI(a).

THEOREM 4.3: If Pos. VI(a) is true in a left semi-group, then VI(b), (c), (d) are also all true, if the semi-group contains ι

PROOF: Clear.

THEOREM 4.4: If Pos. VI(a) is false, the left semi-group is a group.

PROOF: Clear.

THEOREM 4.5: If g is not a unit, $g, g^2, g^3, \ldots$ are all distinct.

PROOF: Needless to say, this theorem assumes the system contains at least one unit 1.

If $g^s = g^{s+r}$ $(s, r \geq 1)$.

$$g^s \circ 1 = g^s \circ g^r$$

$$1 = g^r; \quad g = 1 \text{ if } r = 1, \quad g \neq 1, \ r > 1$$

so that g is a unit.

THEOREM 4.6: If $G \neq 1$, G contains no element g_0 such that

$$g \circ g_0 = g_0 \circ g = g_0$$ for any g in $G \neq 1$.

PROOF: If $G \neq g_0, 1$, $g_0 = g_0 \circ 1$

Suppose for some $g \neq 1$

$$g \circ g_0 = g_0 \circ g = g_0$$

Then

$$g \circ g_0 = g_0 \circ g = g_0 \circ 1, \quad g = 1$$

REMARK: If G is the class of positive integers and $\circ$ is multiplication, g_0 is zero.

SECTION 5. TYPES OF SEMI-GROUPS.

PRELIMINARY: We are now in a position to classify the possible types of semi-groups. The first obvious classification is into those which contain an identity element and those which do not. Consider now the system

$$G = [\, G ; \circ \,/\, I, II, III(a), IV(a), VI(a) \,]$$

DEFINITION 5.1: The Three Classes of Elements in G.

CLASS 1. Contains all elements g such that we can find a positive integer r for which

(5.1) $$g^r = 1$$

g is called a root of unity. (This class is not null, since $1^2 = 1$).

CLASS 2. Contains all elements g such that

(5.2) $$g \,/\, x$$

the g of (5.2) is called a unit. Class 1 is a sub-class of Class 2.

CLASS 3. Contains all elements for which neither (5.1) nor (5.2) hold. These elements are called integral elements. (~~This class is not null by Pos. VI(a) and the theorems of Section 4~~).

THEOREM 5.1: Classes 1, 2, 3 are closed under $\circ$ and S^k belongs to the same class as S, and conversely.

PROOF: Clear.

THEOREM 5.2: A sufficient condition for g to belong to Class 1 is that

$$g^{t_1} = g^{t_2} \qquad t_1 \neq t_2$$

PROOF: Clear.

THEOREM 5.3: The powers of an integral element are all distinct.

PROOF: Clear.

DEFINITION 5.2: Unitary (Semi-) Groups.

A semi-group which contains only elements of Class 1, that is, such that the inverse of any element in it may be expressed as positive power of that element, defines a type of group which includes finite discrete groups as a special case. Such groups are called unitary.

THEOREM 5.4: There are an indefinite number of infinite discrete groups which are unitary.

PROOF: Let n run through any infinite sequence of numbers which are all relatively prime to each other; for example,

$$2^{r_1},\ 3^{r_2},\ 5^{r_3},\ 7^{r_4},\ 11^{r_5},\ 13^{r_6}$$

where (r_i) is any sequence of positive numbers whatsoever, so that

$$n = p_i^{r_i} \qquad p_i \text{ the } i^{th} \text{ prime.}$$

Take $$S_n = e^{\frac{2\pi i}{n}}$$

The totality of elements

$$S_1^{j_1} \cdot S_2^{j_2} \cdot S_3^{j_3} \cdots \qquad j_1, j_2, j_3, \ldots \geq 0$$

form just such a group, and moreover, no two groups of this type are simply isomorphic.

DEFINITION 5.3: Rational (Semi-) Groups.

A semi-group which contains no elements of Class 3 and at least one element of Class 2 is called a rational semi-group. A rational group G necessarily includes at least one root of unity; namely, the identity element i. If this is the only unitary element unit, G is called pure; otherwise mixed.

THEOREM 5.5: Every rational group contains an infinite number of elements.

PROOF: Clear.

EXAMPLE: The positive and negative powers of 2, with the operation of ordinary multiplication, form a pure rational group; the positive and negative powers of ± 2 and of -1 with the same operation form a mixed rational group.

DEFINITION 5.4: Integral Semi-group*.

A semi-group G which contains at least one integral element g is called an integral semi-group. If it contains no elements of Class 1 and Class 2, it is called pure. Those elements of Class 1 and Class 2 contained in G are called its units; their detailed study is the subject matter of the theory of discrete groups. The detailed study of integral semi-groups is one of the chief objects of the theory of general arithmetic.

---

* Compare Section 4.

SECTION 6. EQUIVALENCE.

PRELIMINARY: In this section we develop the relations between an integral left semi-group $G = [G; \circ / I, II, III(a), IV(a), VI(a)]$ and its units E. In the proofs, we have omitted the reasons for the simpler steps.

DEFINITION 6.1: The General Equivalence Relation.

Let ϵ_r, ϵ_s be any two units and g_h, g_k any two elements of G. g_h is said to be equivalent to g_k when and only when

(6.1) $$g_h \circ \epsilon_r = \epsilon_s \circ g_k$$

NOTATION: $g_h \backsim g_k$

THEOREM 6.1: The relation $\backsim$ of equivalence is

(i) symmetric, (ii) transitive, (iii) reflexive.

PROOF: (i) Suppose $g_h \backsim g_k$ so that by Df. 6.1,

$$g_h \circ \epsilon_r = \epsilon_s \circ g_k$$

Let ϵ_v and ϵ_w be the inverses of ϵ_r and ϵ_s respectively. Then

$$\epsilon_w \circ (g_h \circ \epsilon_r) \circ \epsilon_v = \epsilon_w \circ (\epsilon_s \circ g_k) \circ \epsilon_v$$

$$(\epsilon_w \circ g_h) \circ 1 = 1 \circ (g_k \circ \epsilon_v)$$

$$\epsilon_w \circ g_h = g_k \circ \epsilon_v$$

$$g_k \circ \epsilon_w = \epsilon_v \circ g_h$$

$g_k \backsim g_h$ by Df. 6.1.

(ii) Suppose $g_h \backsim g_k$, $g_k \backsim g_l$. Then by Df. 6.1,

$$g_h \circ \epsilon_r = \epsilon_s \circ g_k$$
$$g_k \circ \epsilon_t = \epsilon_u \circ g_l$$
$$(g_h \circ \epsilon_r) \circ \epsilon_t = (\epsilon_s \circ g_k) \circ \epsilon_t = \epsilon_s \circ (g_k \circ \epsilon_t)$$
$$= \epsilon_s \circ (\epsilon_u \circ g_l)$$
$$g_h \circ (\epsilon_r \circ \epsilon_t) = (\epsilon_s \circ \epsilon_u) \circ g_l$$

But $\epsilon_r \circ \epsilon_t$, $\epsilon_s \circ \epsilon_u$ are units

Therefore $g_h \backsim g_l$ by Df. 6.1.

(iii) 1 is a unit, $g_h \circ 1 = 1 \circ g_h$

THEOREM 6.2: (i) All units are equivalent. (ii) If an element g of G is equivalent to a unit, it equals a unit.

PROOF: (i) Let ϵ_r, ϵ_s be two units, ϵ_u, ϵ_v their inverses. Then

$$\epsilon_r \circ \epsilon_u = 1 = \epsilon_v \circ \epsilon_s$$

$$\epsilon_r \backsim \epsilon_s$$ by Df. 6.1.

(ii) Suppose $g \backsim \epsilon$. Then by Df. 6.1

$$g \circ \epsilon_r = \epsilon_s \circ \epsilon = \text{a unit.}$$

$\therefore$ g is a unit. by Th. 3.7.

DEFINITION 6.2: Left and Right Equivalence.

If in (6.1), $\epsilon_s = 1$, g_h is said to be left equivalent to g_l .

NOTATION: $g_h \overset{L}{\backsim} g_k$

If in (6.1), $\epsilon_r = 1$, g_k is said to be right equivalent to g_h .

THEOREM 6.3: The relation $\overset{L}{\backsim}$ of left equivalence is symmetric, transitive and reflexive.

PROOF: Clear from proof of Th. 6.1 on taking $\epsilon_s = 1$ in (i) and $\epsilon_s = \epsilon_u = 1$ in (ii).

THEOREM 6.4: (i) All units are left equivalent. (ii) If an element g of G is left equivalent to a unit, it equals a unit.

PROOF: Clear.

THEOREM 6.5: The necessary and sufficient condition that two elements g_h, g_k of G be left equivalent is that they left divide each other.

PROOF: If $g_h \overset{L}{\sim} g_k$, $g_h \circ \epsilon_1 = g_k$. $g_h = \Pi_L(g_k)$

But if $g_h \overset{L}{\sim} g_k$, $g_k \overset{L}{\sim} g_h$ by Th. 6.3.

$\therefore g_k = \Pi_L(g_h)$

If $g_h = \Pi_L(g_k)$ and $g_k = \Pi_L(g_h)$, then

$g_h \circ g_x = g_k$, $g_k \circ g_y = g_h$

$(g_h \circ g_x) \circ g_y = g_k \circ g_y = g_h$

$g_h \circ (g_x \circ g_y) = g_h \circ 1$

$g_x \circ g_y = 1$, g_x, g_y are units,

$g_h \overset{L}{\sim} g_k$ by Df. 6.2.

DEFINITION 6.3: Conjugate Equivalence.

If in Df. 6.1, $\epsilon_s = \epsilon_r$, g_h is said to be conjugate equivalent to g_k in the first sense.

NOTATION: $g_h \overset{\sim}{} g_k$

If in Df. 6.1 $\epsilon_s \circ \epsilon_r = 1$, g_h is said to be conjugate equivalent to g_k in the second sense.

NOTATION: $g_h \overset{\frown}{} g_k$

If in Df. 6.1, $\epsilon_s = \epsilon_r$, and $\epsilon_s \circ \epsilon_r = 1$, g_h is said to be conjugate equivalent to g_k in the third sense.

NOTATION: $g_h \overline{\sim} g_k$

REMARK: Conjugate equivalence in the third sense is the simplest generalization conceivable of ordinary equality. It corresponds to integers having the same absolute value in ordinary arithmetic.

NOTATION: We shall use $g_h \not\sim g_k$ to denote that g_h is conjugate to g_k in at least one of the senses above.

THEOREM 6.6: The relation $\sim$ of conjugate equivalence is symmetric, transitive, and reflexive.

PROOF: Clear.

THEOREM 6.7: ( ) If g is conjugate equivalent to a unit, g is a unit.

PROOF: Clear.

REMARK: There is no analogy with Th. 6.2 (i) in general; it is obvious we are here encroaching upon one of the most important ideas of group theory, that of the transform of one element by another. For if

$$g_h \circ \epsilon_r = \epsilon_r \circ g_k \qquad \text{and} \qquad \epsilon_r' \text{ is the inverse of } \epsilon_r,$$
$$g_h = \epsilon_r \circ g_k \circ \epsilon_r'$$

If
$$g_h \circ \epsilon_r = \epsilon_r' \circ g_k$$
$$g_h = \epsilon_r' \circ g_k \circ \epsilon_r'$$

If
$$g_h \circ \epsilon_r = \epsilon_r \circ g_k \qquad \epsilon_r^2 = 1,$$
$$g_h = \epsilon_r \circ g_k \circ \epsilon_r$$

REMARK: All these relations of equivalence share a remarkable property:

If $g_1 \sim g_2$. $g_1' \sim g_2'$, then we cannot infer $g_1 \circ g_1' \sim g_2 \circ g_2'$ unless the units of G are commutative with all the elements of G .

Again, if g_h / g_k. $g_h \sim g_e$. $g_k \sim g_m$ then we cannot infer g_e / g_m without assuming the units of G are commutative with all the elements of G. We thus have two properties of the integers (and for that matter of the algebraic numbers) which have to be sacrificed if we give up the commutative law.

SECTION 7. DIVISORS AND MULTIPLES.

PRELIMINARY: We are working throughout this section in an integral left semi-group G containing a unit, $G = [G; \circ / I, II, III(a), IV(a), VI(a)]$

THEOREM 7.1: If g is any element of G ; (i) g left divides g . (ii) 1 left divides g . (iii) If g left divides a unit, g is a unit. (iv) If $g \circ g_h$ left divides g , g_h is a unit. (v) Every unit left divides every other unit.

PROOF: Clear.

THEOREM 7.2: If g_h left divides g_k and g_k left divides g_m , g_h left divides g_m .

PROOF: $g_h = \Pi_L(g_k)$. $g_k = \Pi_L(g_m)$ by hyp.

$g_h \circ g_x = g_k$. $g_k \circ g_y = g_m$ $G / g_x, g_y$

$(g_h \circ g_x) \circ g_y = (g_k \circ g_y) = g_m$

$g_{h_1} = \Pi_L(g_m)$

THEOREM 7.3: If g_h left divides g_k , all the left divisors of g_h are left divisors of g_k .

PROOF: Clear from Th. 7.2.

THEOREM 7.4: If g_k has a finite number of left divisors, and g_h left divides g_k , and is not left equivalent to g_k , g_h has fewer left divisors than g_k .

PROOF: $g_k \neq \Pi_L(g_h)$, for if $g_k = \Pi_L(g_h)$ since $g_h = \Pi_L(g_k)$, $g_h \perp g_k$ by Th. 6.5, contrary

to hypothesis. But $g_h = \Pi_L(g_k)$ by Th. 7.1

g_h has one less divisor than g_k, by Th. 7.3.

THEOREM 7.5: If g_h left divides g_k, g_h left divides $g_k \circ g_m$.

PROOF: $g_h = \Pi_L(g_k)$, $g_k = \Pi_L(g_k \circ g_m)$ by hyp. and Df. 2.1

$\therefore g_h = \Pi_L(g_k \circ g_m)$ by Th. 7.2.

THEOREM 7.6: If g_h left divides g_k, $g \circ g_h$ left divides $g \circ g_k$ and conversely.

PROOF: $g_h = \Pi_L(g_k)$ by hyp.

$g_h \circ g_x = g_k$ by Df. 2.1

$g \circ (g_h \circ g_x) = g \circ g_k$

$g \circ g_h = \Pi_L(g \circ g_k)$

by Df. 2.1

Conversely, if $g \circ g_h = \Pi_L(g \circ g_k)$

$g \circ g_h \circ g_z = g \circ g_k \quad G/g_z$ by Df. 2.1

$g_h \circ g_z = g_k$

$g_h = \Pi_L(g_k)$

THEOREM 7.7: If g is any element of G (i) g right multiplies g, (ii) g right multiplies 1, (iii) if a unit right multiplies g, g is a unit, (iv) if g right multiplies $g \circ g_h$, g_h is a unit, (v) every unit right multiplies every other unit.

PROOF: Clear from Df. 2.4.

THEOREM 7.8: If $\mathcal{G}_h$ right multiplies $\mathcal{G}_k$ and $\mathcal{G}_k$ right multiplies $\mathcal{G}_m$, $\mathcal{G}_\ell$ right multiplies $\mathcal{G}_m$.

PROOF: Clear from Df. 2.4, Th. 7.2.

THEOREM 7.9: If $\mathcal{G}_h$ right multiplies $\mathcal{G}_k$, all the right multiples of $\mathcal{G}_k$ are right multiples of $\mathcal{G}_h$.

PROOF: See Th. 7.3.

THEOREM 7.10: If $\mathcal{G}_k$ right multiplies $\mathcal{G}_h$, $\mathcal{G}_k \circ \mathcal{G}_m$ right multiplies $\mathcal{G}_h$.

PROOF: See Th. 7.5.

THEOREM 7.11: If $\mathcal{G}_k$ right multiplies $\mathcal{G}_h$, $\mathcal{G} \circ \mathcal{G}_k$ right multiplies $\mathcal{G} \circ \mathcal{G}_h$ and conversely.

PROOF: See Th. 7.6.

REMARK: Note the strict analogy between the theorems on divisors and multiples.

SECTION 8. CONCLUSION AND SUMMARY.

We have now reached a logical stopping place. In Part I, we have subjected the concept of a class and a binary operation to a careful scrutiny, and shown that for the purposes of general arithmetic, where all classes are denumerable, we can assume the class ordered without any loss of generality, or replaced by the numbers one, two, three, . . . We have thus "arithmetized" general arithmetic in Kronecker's sense. In Part II, we have sketched the theory of arithmetized general arithmetic, without, however, any attempt at a systematic treatment. In Part III, we have developed some of the properties of an abstract semi-group, a concept indispensable both in group theory and arithmetic.

Finally, in Part IV, we have given a fairly complete analysis of the concept of an inverse operation in a semi-group, using the language of ordinary arithmetic. The linking together of the ideas in Part II and Part III remains a desiderata.

Probably the most important consequence of our work is that we now know the problem of defining "arithmetic" in the narrow sense of the introduction has already been solved, provided we assume our "multiplication" is commutative. For in view of the theory of formal transformations developed in Part I, the complete holoid realm of Julius Koenig* is an abstract arithmetic, provided we interpret his "Grösse" as "marks" and his "Verknupfungen" as "functions" in the sense of our paper.

In conclusion, I should like to thank Professor E. T. Bell for criticism and advice in writing this paper.

---

* See Algebraische Grössem, Chap. I