POSTULATE SETS FOR CERTAIN MATHEMATICAL SYSTEMS AND THEIR COMPLETE EXISTENTIAL THEORY

Thesis by

Robert J. Levit

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

California Institute of Technology

Pasadena, California

1939

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

The purpose of this paper is to construct postulate sets for certain mathematical systems, establish their complete independence, and, in cases where other postulate sets are already known, to show their equivalence to ours.

In Part I groups and Abelian groups are defined in terms of a triadic relation. The existence of an equivalence relation is not assumed, as is the usual method, but proved by actual construction. The complete independence of the postulates and their equivalence to conventional group postulates is established.

In Part II a completely independent set of postulates for rings is exhibited differing from the usual sets (for example, see Van Der Waerden, Moderne Algebra, page 35) only in that the closure of addition is not explicitly assumed, since it can be deduced from the other postulates. With this definition of the containing ring a completely independent set of postulates for an ideal can then be given.

Part III contains the most novel results of the paper. A definition of divisibility was sought, with properties entirely analagous to arithmetic divisibility but not depending on the existence of a multiplication operation. The postulates for a Division System as defined in this section give the properties of certain classes called principal ideals, which are functions of elements of the system. By means of these classes an equivalence relation and a relation of divisibility are defined, the latter having all the important characteristics of arithmetic divisibility. Most important, the existence of an L.C.M. of any finite set and the G.C.D. of any set whatever in the system is established.

I wish to thank Prof. E. T. Bell for the suggestions which led to the writing of this paper.

THE NOTION OF COMPLETE INDEPENDENCE

The notion of complete independence was first introduced into mathematics by E. H. Moore in 1915. ("Introduction to a Form of General Analysis," by E. H. Moore, New Haven Mathematical Colloquium, 1915, page 82.) A thorough discussion of its significance is given in the article by E. V. Huntington, Transactions of the American Mathematical Society, Volume 20, page 277. We might briefly mention that complete independence carries with it both consistency and ordinary independence. It further demands that no relations of implication whatever exist among the postulates.

The proof of complete independence is established by an extension of the method used for ordinary independence. Examples are exhibited in which all the postulates are true, examples in which they are contradicted one at a time, two at a time, and so on until finally an example is produced for which all are false. It takes 2^n examples to establish the complete independence of n postulates.

The notation used is best explained by an illustration. The character (+ - - + -) is used to designate an example in which the first and fourth postulate of a given set hold, while the second, third and fifth do not.

PART I

GROUPS DEFINED BY A TRIADIC RELATION*

0.1 Definition. We consider a class K of undefined elements a, b, ... and an undefined binary triadic relation R such that for any ordered triple (a,b,c) of elements of K we can either say R(abc) (a, b, and c stand, in that order, in the relation R) or $\not{R}$(abc) (a, b, c do not, in that order, stand in the relation R). The class K and relation R form together a system G when they are subject to the postulates below.

0.2 Definition. Two elements a, a' of K are said to be equivalent ($a ⊜ a'$) if and only if all the following conditions are simultaneously satisfied:

(1) R(axy) implies R(a'xy) and conversely for every $x,y \in$ K.

(2) R(xay) implies R(xa'y) and conversely for every $x,y \in$ K.

(3) R(xya) implies R(xya') and conversely for every $x,y \in$ K.

0.3 Postulate I. $\exists$ x in K for each $b,c \in$ K such that R(xbc).

0.4 Postulate II. $\exists$ y in K for each $a,d \in$ K such that R(ayd).

*The first definition of a group by means of a triadic relation is that of E. V. Huntington (Transactions of American Mathematical Society, Vol. 6, 1905, p. 192), though the idea was suggested earlier by M. Bocher. Huntington's first set of postulates is similar to ours and formed the basis for it. Huntington's postulates are not independent, however, as theorem 2.1 shows. Moreover, they neglect the consideration of the equivalence relation.

0.5 Postulate III. $R(\alpha\beta\delta)$, $R(\delta\gamma\mu)$, $R(\beta\gamma\epsilon)$, and $R(\alpha\epsilon\nu)$ simultaneously holding imply $\mu \circledequal \nu$ provided $\alpha, \beta, \delta, \gamma, \mu, \epsilon, \nu$ are in K.

0.6 Notation. Since the only elements considered are in K, the phrase,"for every a of K,"will usually be omitted.

1.1 Theorem. $a \circledequal a$ for every a in K.

Proof: Obvious from 0.2.

1.2 Theorem. $a \circledequal b$ implies $b \circledequal a$ and conversely for every a,b in K.

Proof: Obvious from 0.2.

1.3 Theorem. If $a \circledequal b$ and $b \circledequal c$, $a \circledequal c$.

Proof: Since $a \circledequal b$, R(axy) implies R(bxy) for all x and y by 0.2. Since $b \circledequal c$, (R(bxy) implies R(cxy) for all x and y.

(1) R(axy) implies R(cxy) for all x and y. Since $c \circledequal b$ by 1.2, R(cxy) implies R(bxy) and since $b \circledequal a$ R(bxy) implies R(axy) for all x and y, then

(2) R(cxy) implies R(axy) for all x and y.

(1) and (2) of this proof together satisfy condition (1) of Definition 0.2. Conditions (2) and (3) can be shown to be fulfilled by exactly analagous proof so that 1.3 follows.

1.4 Remark. The relation $\circledequal$ is an equivalence relation.

2.1 Theorem*. For each pair a,b of elements of K there exists an element of K such that R(abc).

Proof:

(1) For each a, $\exists$ i_a such that $R(i_a aa)$ by 0.3.

(2) For each a, $\exists$ a^{-1} such that $R(a^{-1}ai_a)$ by Postulate I.

(3) For each b, $\exists$ x such that $R(a^{-1}xb)$ by Postulate II.

Consider now an arbitrary fixed pair of elements a,b of K. We will show that the element x of step (3) is the c demanded by the theorem such that R(abc).

(4) $\exists$ p such that R(apx) by Postulate II.

(5) $\exists$ q such that $R(i_a qp)$ by Postulate II.

(6) $\exists$ r such that R(arq) by Postulate II.

(7) p ⊜ q. This follows from Postulate III by putting $\alpha \equiv i_a$, $\beta \equiv \delta \equiv a$, $\gamma \equiv r$, $\epsilon \equiv \mu \equiv q$, $\nu \equiv p$ in steps (1), (6), (6) and (5).

(8) $R(i_a pp)$ by steps (5) and (7) and def. 0.2.

(9) p ⊜ b by Post. III with $\alpha \equiv a^{-1}$, $\beta \equiv a$, $\delta \equiv i_a$, $\gamma \equiv \mu \equiv p$, $\epsilon = x$, and $\nu = b$ in steps (2), (8), (4), and (3).

(10) R(abx) by steps (4) and (9) and def. 0.2.

Q.E.D.

*The method used in this proof was suggested by R. Garver's work on group postulates. (Bulletin of the American Mathematical Society, Vol. 40, 1934, p. 698.)

2.2 Theorem. If $R(abc)$ and $R(abc')$, $c ⊜ c'$.

Proof:

(1) $R(abc)$

by hypothesis

(2) $R(abc')$

(3) $\exists x$ in K such that $R(xab)$ by Post. I.

(4) $\exists y$ in K such that $R(axy)$ by Th. 2.1.

(5) $\exists z$ in K such that $R(yax)$ by Th. 2.1.

(6) $z ⊜ c$ by Post. III, putting $\alpha \equiv \gamma \equiv a$, $\beta \equiv x$, $\delta \equiv y$, $\mu \equiv z$, $\epsilon \equiv b$, and $\nu \equiv c$ in steps (4), (5), (3), and (1).

(7) Similarly, by symmetry, repeating steps (3) to (6) and using (2) in place of (1),

$$z ⊜ c'$$

(8) $c ⊜ c'$ by Th. 1.2 and 1.3.

Q.E.D.

2.3 Remark. To every ordered pair of elements a,b, there corresponds an element c, unique up to equivalence such that $R(abc)$ (from 2.1 and 2.2).

3.0 Definition. By an abstract group we mean the well-known mathematical system consisting of a class G(a,b,...) subject to the following postulates:

3.1 Postulate. There exists an equivalence relation, binary, reflexive, symmetric, and transitive throughout G. This relation holding between a and b is symbolized, a ⊜ b.

3.2 Postulate. To each pair of elements $a,b \in G$ there corresponds a unique element $ab \in G$.

3.3 Postulate. For every $a,b,c \in G$

$$(ab)c = a(bc)$$

3.4 Postulate. For each a and $b \in G$ there exists a corresponding $x \in G$ such that

$$ax = b$$

3.5 Postulate. For each $a,b \in G$ there exists a corresponding $y \in G$ such that

$$ya = b$$

3.6 Theorem. The class K(0.1 - 0.5) is an abstract group. Proof: For our equivalence relation we choose that defined in 0.2, i.e., $a = b$ if and only if a ⊜ b. Then by 1.1 to 1.4, 2.1 is satisfied. By 2.1 for each $a,b \in K$ there will exist a corresponding $z \in K$ such that R(abc). Designate z by ab. Let c be such that R(abc). Then by 2.2

$$ab ⊜ c \text{ or } ab = c$$

The element ab may be regarded as a representative of the class of equivalent elements z for which R(abz). The element c = ab is thus uniquely specified (up to equivalence) by a and b, so 3.2 holds. Take α, β, γ any elements of K and let

(1) $\delta = \alpha\beta$, $\mu = \delta\gamma$, $\epsilon = \beta\gamma$, and $\nu = \alpha\epsilon$

Then

(2) $R(\alpha\beta\delta)$, $R(\delta\gamma\mu)$, $R(\beta\gamma\epsilon)$, and $R(\alpha\epsilon\nu)$.

Therefore by 0.5

(3) $\mu ⊜ \nu$ or $\mu = \nu$.

Substituting from (1) in accordance with Th. 1.3

(4) $(\alpha\beta)\gamma = (\beta\gamma)$.

By postulates 0.3 and 0.4 we can find an x such that R(axb) and a y such that R(yab) corresponding to each a,b ϵ K. Then

(5) ax = b and ya = b

are solvable and all the postulates are satisfied.

Q.E.D.

3.7 <u>Theorem</u>. Every abstract group G satisfies the postulates 0.3, 0.4, 0.5 for K.

<u>Proof</u>: We shall say that R(abc) if and only if ab = c. R so defined satisfies 0.3, 0.4 since by 3.4 and 3.5 we can always find an x and y such that ax = b and ya = b and consequently such that R(axb) and

R(yab). Let $a = a'$. Then $ax = y$ implies $ax' = y$, $xa = y$ implies $xa' = y$, and $xy = a$ implies $xy = a'$ and conversely for all $x, y \in G$. Therefore $a = a'$ implies $a \textcircled{=} a'$. Finally, letting $\delta \equiv \alpha\beta$, $\mu \equiv \delta\gamma$, $\epsilon \equiv \beta\gamma$, $\nu \equiv \alpha\epsilon$, we have $\mu = \nu$ by 3.3. Then $\mu \underset{\sim}{\equiv} \nu$ and Post. 0.5 holds.

3.8 Remark. The postulate set 0.3, 0.4, and 0.5 is equivalent to the set 3.1, 3.2, 3.3, 3.4, and 3.5, since each implies the other by the preceding theorems. Consequently the former set will serve as well as the latter for the definition of an abstract group.

4.1 Theorem. The postulates 0.3, 0.4, 0.5 form a completely independent set.

The proof is by the usual method of examples, all of which are in this case self-explanatory.

Character	Class, K(a,b...)	Relation, R(abc) if
(+ + +)	All rational integers	a+b = c
(+ + -)	All rational integers	1/2(a+b) = c
(+ - +)	Positive rational integers	a = c
(- + +)	Positive rational integers	b = c
(+ - -)	Positive rational integers	a-b = c
(- + -)	Positive rational integers	b-a = c
(- - +)	Positive rational integers	a+b = c
(- - -)	Positive rational integers	2(a+b) = c

ABELIAN GROUPS

Consider a class K subject to postulates II and III (0.4, 0.5) but with I replaced by the following:

5.1 Postulate IV. If R(abc), then R(bac) for every a,b,c $\in$ K.

5.2 Theorem. Postulates II and IV imply I.

Proof: Let a,b $\in$ K. By II, there exists a y such that R(ayb).

By IV, R(yab)

since a,b were any two elements, there will always be an x $\in$ K such that R(xab) if we take x to be y.

5.3 Theorem. A class K subject to postulates II, III, and IV forms an Abelian group.

Proof: By the preceding theorem and theorem 3.6 it forms a group with ab = c if R(abc). Let R(abc). Then R(bac) by IV and consequently ba = c = ab by 3.1 and K is Abelian.

5.4 Theorem. Every Abelian group G satisfies postulates II, III, and IV.

Proof: By theorem 3.7 G satisfies III and IV. Let ab = c in G. Then R(abc). But ba = c since G is Abelian. Therefore R(bac) and II is satisfied since a and b were arbitrary.

5.5 Remark. II, III, and IV may be taken as the postulates for an Abelian group.

5.6 <u>Theorem</u>. The postulates II, III, and IV are completely independent.

Character	Class K(a,b...)	Relation, R(abc) if
(+ + +)	All rational integers	$a+b = c$
(+ + -)	Positive rational integers	$b = c$
(+ - +)	All rational integers	$1/2(a+b) = c$
(- + +)	Positive rational integers	$a+b = c$
(+ - -)	All rational integers	$2a+b = c$
(- + -)	All rational integers	$a = c$
(- - +)	All rational integers	$2(a+b) = c$
(- - -)	All rational integers	$a+2b = c$

PART II

RINGS AND IDEALS

1.0 Definition. A ring is the well-known mathematical system defined as follows: it consists of

(1) A class K of elements a, b, ...

(2) An equivalence relation written ('='), which is binary, reflexive, symmetric, and transitive throughout K.

(3) An operation, addition (+), defining a one-valued function of two variables. That is to every ordered pair $a,b \in K$ there corresponds an element $(a + b)$ unique up to equivalence.

(4) A second operation, multiplication, indicated by ab. Thus, to every ordered pair $a,b \in K$ there corresponds an element ab unique up to equivalence.

(5) The following postulates hold in K:

1.1 Postulate I. For each a,b K there exists a corresponding $x \in K$ such that

$$a + x = b$$

1.2 Postulate II. If $a, b, a + b, b + a \in K$, then

$$a + b = b + a$$

1.3 Postulate III. If $a, b, c, a + b, b + c, a + (b + c), (a + b) + c \in K$, then

$$a + (b + c) = (a + b) + c$$

1.4 Postulate IV. If $a, b \in K$, then $ab \in K$

1.5 Postulate V. If a, b, c, ab, bc, $(ab)c$, $a(bc) \in K$, then

$$a(bc) = (ab)c$$

1.6 Postulate VI. If a, b, c, $b + c$, $a(b + c)$, ab, ac, $ab + ac \in K$, then

$$a(b + c) = ab + ac$$

1.7 Postulate VII. If a, b, c, $a + b$, $(a + b)c$, ac, bc, $ac + bc \in K$, then

$$(a + b)c = ac + bc$$

2.0 Remark. In the postulates for a ring given in the above section, it was not explicitly assumed that the set closed with respect to addition. A postulate to this effect is ordinarily included in the definition of a ring. This is unnecessary as the following theorem shows, and its inclusion destroys the independence of the postulates.

2.1 Theorem. The elements of a ring form an Abelian group with respect to addition.

Proof: If we take $R(abc)$ if and only if $a + b = c$, the postulates for an Abelian group, 0.4, 0.5, and 5.1 of Part I of this paper are clearly satisfied.

2.2 Corollary. A ring is closed with respect to addition.

3.1 Theorem. The postulates I through VII form a completely independent set.

(The equivalence relation in the following table is taken as ordinary equality for rational or integral examples while (a,b) = (c,d) if a = c and b = d for number couples. In the case of number couples we shall let $a = (a_1, a_2)$, $b = (b_1, b_2)$.)

Character	Class	Operations	
	K(a,b,...)	Addition: $a \oplus b =$	Multiplication: $a \circ b =$
(+ + + + + + +)	Integers	$a + b$	ab
(+ + + + + + -)	Integers	$a + b$	b
(+ + + + + - +)	Integers	$a + b$	a
(+ + + + - + +)	Integer couples	(a_1+b_1, a_2+b_2)	$(a_1b_2+a_2b_2, a_1b_1+a_2b_1)$
(+ + + - + + +)	Rational numbers r such that 2r is an integer	$a + b$	ab
(+ + - + + + +)	Integers	$\frac{a + b}{2}$	ab
(+ - + + + + +)	Integers	b	ab
(- + + + + + +)	Positive integers	$a + b$	ab
(+ + + + + - -)	Integers	$a + b$	$1 + a + b$
(+ + + + - + -)	Integers	$a + b$	$2b$
(+ + + - + + -)	Integers	$a + b$	If b is even: b If b is odd: $b/2$
(+ + - + + + -)	Integers	$\frac{a + b}{2}$	b
+ - + + + + -)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(b_1, b_2)
(- + + + + + -)	Positive integers	$a + b$	b

Character	Class	Addition: $a \oplus b =$	Multiplication: $a \circ b =$
(+ + + + - - +)	Integers	$a + b$	$2a$
(+ + + - + - +)	Integers	$a + b$	a, if a is even $a/2$, if a is odd
(+ + - + + - +)	Integers	$\frac{a + b}{2}$	a
(+ - + + + - +)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1, a_2)
(- + + + + - +)	Positive integers	$a + h$	a
(+ + + - - + +)	Integer couples	(a_1+b_1, a_2+b_2)	$(\frac{a_1b_2+a_2b_2}{2}, \frac{a_1b_1+a_2b_1}{2})$
(+ + - + - + +)	Rational couples	$(2a_1+2b_1, 2a_2+2b_2)$	$(a_1b_2+a_2b_2, a_1b_1+a_2b_1)$
(+ - + + - + +)	Integers	b	$a - b$
(- + + + - + +)	Positive integer couples	(a_1+b_1, a_2+b_2)	$(a_1b_2+a_2b_2, a_1b_1+a_2b_1)$
(+ + - - + + +)	Rationals r such that 2r is an integer	$\frac{a + b}{2}$	ab
(+ - + - + + +)	Rationals r such that 2r is an integer	b	ab
(- + + - + + +)	Rationals r such that 2r is an integer	$a + b$	ab
(+ - - + + + +)	Integers	$2a + b$	ab
(- + - + + + +)	Positive integers	$\frac{a + b}{2}$	ab
(- - + + + + +)	Integers	a	ab
(+ + + + - - -)	Integers	$a + b$	$a - b$
(+ + + - + - -)	Integers	$a + b$	$\frac{1+a+b}{2}$ if $a+b$ is even $1+a+b$ if $a+b$ is odd
(+ + - + + - -)	Integers	$\frac{a + b}{3}$	$1 + a + b$

Character	Class	Addition: a ⊕ b =	Multiplication: a∘b =
(+ – + + + – –)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1+b_1, a_2+b_2)
(– + + + + – –)	Positive integers	a + b	1 + a + b
(+ + + – – + –)	Integers	a + b	b/2
(+ – + + – + –)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(b_1^2+b_1b_2, b_2^2+b_1b_2)$
(– + + + – + –)	Integers	a + b	2b
(+ + – – + + –)	Integers	$\frac{a+b}{2}$	b, if b is even b/2, if b is odd
(+ – + – + + –)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(b_1,b_2) for b_1 a perfect square $(\sqrt{b_1}, b_2)$ for b_1 not a perfect square
(– + + – + + –)	Positive integers	a + b	b, for b even b/2 for b odd
(+ – – + + + –)	Integers	2a + b	ab
(– + – + + + –)	Positive integers	$\frac{a+b}{2}$	b
(– – + + + + –)	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(b_1, b_2)
(+ + + – – – +)	Integers	a + b	a/2
(+ + – + – – +)	Integers	$\frac{a+b}{2}$	2a
(+ – + + – – +)	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(a_1^2+a_1a_2, a_2^2+a_1a_2)$
(– + + + – – +)	Integers	a + b	2a
(+ + – – + – +)	Integers	$\frac{a+b}{2}$	a, for a even a/2, for a odd
(+ – + – + – +)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1, a_2) for a_1 perfect sq. $(\sqrt{a_1}, a_2)$ for a_1 not a perfect square

Character	Class	Addition: $a \oplus b =$	Multiplication: $a \cdot b =$
(- + + - + - +)	Positive integers	$a + b$	$a/2$ for a odd a, for a even
(+ - - + + - +)	Integers	$2a + b$	a
(- + - + + - +)	Positive integers	$\frac{a + b}{2}$	a
(- - + + + - +)	Positive integer couples	$(a_1b_1+a_2b_1,a_1b_2+a_2b_2)$	(a_1,a_2)
(+ + - - - + +)	Integers	$\frac{a + b}{2}$	$\frac{a - b}{2}$
(+ - + - - + +)	Integers	b	$\frac{a - b}{2}$
(- + + - - + +)	Positive integer couples	(a_1+b_1,a_2+b_2)	$\frac{a_1b_2+a_2b_2}{2},\frac{a_1b_1+a_2b_1}{2}$
(+ - - + - + +)	Integers	$2a - b$	$a - b$
(- + - + - + +)	Positive integers	$\frac{a + b}{2}$	$2a + b$
(- - + + - + +)	Integers	a	$a - b$
(+ - - - + + +)	Integers	$2a + b$	$\frac{ab}{2}$
(- + - - + + +)	Rationals r such that 2r is an integer	$\frac{a + b}{2}$	ab
(- - + - + + +)	Rationals r such that 2r is an integer	a	ab
(- - - + + + +)	Positive integers	$2a + b$	ab
(+ + + - - - -)	Integers	$a + b$	$\frac{a - b}{2}$
(+ + - + - - -)	Integers	$\frac{a + b}{3}$	$a - b$
(+ - + + - - -)	Positive rational couples	$(a_1b_1+a_2b_1,a_1b_2+a_2b_2)$	(a_1-b_1,a_2-b_2)
(- + + + - - -)	Positive integers	$a + b$	$2a + b$

Character	Class	Addition: $a \oplus b =$	Multiplication: $a \circ b =$
(+ + − − + − −)	Integers	$\frac{a + b}{3}$	$1+a+b$ if $a+b$ is odd $\frac{1+a+b}{2}$ if $a+b$ is even
(+ − + − + − −)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1+b_1, a_2+b_2) if a_1+b_1 is a perfect square $(\sqrt{a_1+b_1}, a_2+b_2)$ if a_1+b_1 is not a perfect sq.
(− + + − + − −)	Positive integers	$a + b$	$\frac{1+a+b}{2}$ if $a+b$ is even $1+a+b$ if $a+b$ is odd
(+ − − + + − −)	Integers	$2a + b$	$1 + a + b$
(− + − + + − −)	Positive integers	$\frac{a + b}{3}$	$1 + a + b$
(− − + + + − −)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1+b_1, a_2+b_2)
(+ + − − − + −)	Integers	$\frac{a + b}{2}$	$b/2$
(+ − + − − + −)	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(\frac{b_1}{2}, b_2)$
(− + + − − + −)	Integers	$a + b$	$b/2$
(+ − − + − + −)	Integers	$2a + b$	$2b$
(− + − + − + −)	Positive integers	$\frac{a + b}{2}$	$2b$
(− − + + − + −)	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(b_1^2+b_1b_2, b_2^2+b_1b_2)$
(+ − − − + + −)	Integers	$2a + b$	$b/2$ for b odd b for b even
(− + − − + + −)	Positive integers	$\frac{a + b}{2}$	$b/2$ for b odd b for b even
(− − + − + + −)	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(b_1, b_2) if b_1 is a perfect square $(\sqrt{b_1}, b_2)$ if b_1 is not a perfect square

Character	Class	Addition: $a \oplus b =$	Multiplication: $a \circ b =$
$(- - - + + + -)$	Positive integers	$2a + b$	b
$(+ + - - - - +)$	Integers	$\frac{a + b}{2}$	$a/2$
$(+ - + - - - +)$	Positive rational couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(\frac{a_1}{2}, a_2)$
$(- + + - - - +)$	Positive integers	$a + b$	$a/2$
$(+ - - + - - +)$	Integers	$2a + b$	$2a$
$(- + - + - - +)$	Positive integers	$\frac{a + b}{2}$	$2a$
$(- - + + - - +)$	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(a_1^2+a_1a_2, a_2^2+a_1a_2)$
$(+ - - - + - +)$	Integers	$2a + b$	$a/2$ for a odd a for a even
$(- + - - + - +)$	Positive integers	$\frac{a + b}{2}$	$a/2$ for a odd a for a even
$(- - + - + - +)$	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1, a_2) if a_1 is a perfect square $(\sqrt{a_1}, a_2)$ if a_1 is not a perfect sq.
$(- - - + + - +)$	Positive integers	$a + b$	a
$(+ - - - - + +)$	Integers	$2a - b$	$\frac{a - b}{2}$
$(- + - - - + +)$	Positive integers	$\frac{a + b}{2}$	$\frac{a - b}{2}$
$(- - + - - + +)$	Integers	a	$\frac{a - b}{2}$
$(- - - + - + +)$	Positive integer couples	$(2a_1+b_1, 2a_2+b_2)$	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$
$(- - - - + + +)$	Positive integers	$2a + b$	$\frac{ab}{2}$
$(+ + - - - - -)$	Integers	$\frac{a + b}{3}$	$\frac{a - b}{2}$
$(+ - + - - - -)$	Positive integer	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(\frac{a_1-b_1}{2}, a_2-b_2)$

Character	Class	Addition: $a \oplus b =$	Multiplication: $a \circ b =$
$(+ - - + - - -)$	Integers	$2a + b$	$a - b$
$(+ - - - + - -)$	Integers	$2a + b$	$\frac{a+b+1}{2}$ if $a+b$ is even $a+b+1$ if $a+b$ is odd
$(+ - - - - + -)$	Integers	$2a + b$	$b/2$
$(+ - - - - - +)$	Integers	$2a + b$	$a/2$
$(- + + - - - -)$	Positive integers	$a + b$	$\frac{a - b}{2}$
$(- + - + - - -)$	Positive integers	$\frac{a + b}{3}$	$2a + b$
$(- + - - + - -)$	Positive integers	$\frac{a + b}{3}$	$\frac{a+b+1}{2}$ if $a+b$ is even $a+b+1$ if $a+b$ is odd
$(- + - - - + -)$	Positive integers	$\frac{a + b}{2}$	$b/2$
$(- + - - - - +)$	Positive integers	$\frac{a + b}{2}$	$a/2$
$(- - + + - - -)$	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1-b_1, a_2-b_2)
$(- - + - + - -)$	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	(a_1+b_1, a_2+b_2) if a_1+b_1 is a perfect square $(\sqrt{a_1+b_1}, a_2+b_2)$ if a_1+b_1 is not a perfect sq.
$(- - + - - + -)$	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(\frac{b_1}{2}, b_2)$
$(- - + - - - +)$	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(\frac{a_1}{2}, a_2)$
$(- - - + + - -)$	Positive integers	$2a + b$	$a + b + 1$
$(- - - + - + -)$	Positive integers	$2a + b$	$2b$
$(- - - + - - +)$	Positive integers	$2a + b$	$2a$

Character	Class	Addition: $a \oplus b =$	Multiplication: $a \circ b =$
(– – – – + + –)	Positive integers	$2a + b$	$b/2$ if b is odd b if b is even
(– – – – + – +)	Positive integers	$2a + b$	$a/2$ if a is odd a if a is even
(– – – – – + +)	Positive integers	$2a - b$	$\frac{a - b}{2}$
(+ – – – – – –)	Integers	$2a + b$	$\frac{a - b}{2}$
(– + – – – – –)	Positive integers	$\frac{a + b}{3}$	$\frac{a - b}{2}$
(– – + – – – –)	Positive integer couples	$(a_1b_1+a_2b_1, a_1b_2+a_2b_2)$	$(\frac{a_1-b_1}{2}, a_2-b_2)$
(– – – + – – –)	Positive integers	$2a + b$	$a - b$
(– – – – + – –)	Positive integers	$2a + b$	$\frac{a+b+1}{2}$ if $a+b$ is even $a+b+1$ if $a+b$ is odd
(– – – – – + –)	Positive integers	$2a + b$	$b/2$
(– – – – – – +)	Positive integers	$2a + b$	$a/2$
(– – – – – – –)	Positive integers	$2a + b$	$\frac{a - b}{2}$

Incidental to the devising of the above examples, a number of interesting elementary theorems were obtained, which greatly reduced the work.

3.2 Theorem. Let $x \oplus y \equiv ax + by$ and $x \circ y \equiv mx + ny$ where x and y are any real numbers and a, b, m, and n are fixed real numbers. If $a + b = 1$, then for all x, y, z.

(1) $x \circ (y \oplus z) = x \circ y \oplus x \circ z$ and $(x \oplus y)\ z \equiv x \circ y \oplus x \circ z$

independently of m and n. But, if $a + b \neq 1$, neither of the above equations (1) holds for all x, y, z.

Proof:

(2) $x \circ (y \oplus z) \equiv x \circ (ay + bz) \equiv mx + n(ay + bz) = mx + any + bnz.$

(3) $x \circ y \oplus x \circ z \equiv a(mx + ny) + b(mx + nz) = (a + b)\, mx + any + bnz.$

Thus the first equality of (1) holds identically in x, y, z if and only if $a + b = 1$. The second follows by symmetry.

3.3 Theorem. Let $x \oplus y$ be defined as in 3.2. Then

(4) $$x \oplus (y \oplus z) = (x \oplus y) \oplus z$$

holds for all x, y, z if and only if $a = 0$ or $a = 1$ and $b = 0$ or $b = 1$.

(5) $x \oplus (y \oplus z) = ax + b(ay + bz) = ax + aby + b^2z.$

(6) $(x \oplus y) \oplus z = a(ax + by) + bz = a^2x + aby + bz.$

If (4) is to hold, then $a^2x + aby + bz = ax + aby + b^2z$ and

(7) $a^2 = a,\ b^2 = b; \quad a = 0$ or $a = 1$; $b = 0$ or $b = 1$.

3.4 Corollary. $x \oplus y \equiv x,\ x \oplus y \equiv y,\ x \oplus y \equiv 0,\ x \oplus y \equiv x + y$ are the only linear combinations which make the operation $\oplus$ associative.

3.5 Theorem. Let $K(a,b,\ldots)$ be any abstract set in which an operation $\oplus$ and an operation $(\circ)$ are defined between every pair $a,b \in K$. If

(1) $$a \oplus b = a \quad \text{or} \quad a \oplus b = b$$

for every $a,b \in K$, then

(2) $a \circ (b \oplus c) = a \circ b \oplus a \circ c$ and $(a \oplus b) \circ c = a\ c + a\ b$

for every a,b K no matter how the multiplication, $(\circ)$, is defined.

Proof: Take the first definition in (1)

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

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

If the second definition of (1) is taken instead, the proof follows by symmetry from the above.

3.6 Theorem. In the set K of 3.5 let addition be defined in any other way besides that of equation (1). Let multiplication be defined as follows: either

(3a) $a \circ b = a$ or (3b) $a \circ b = b$.

If definition (3a) is chosen, then for every $a,b,c \quad K$

$$(4a) \qquad (a \oplus b) \circ c = a \circ c \oplus b \circ c\,;$$

while if (3b) is chosen, then

$$(4b) \qquad a \circ (b \oplus c) = a \circ b \oplus a \circ c,$$

but (4a) will not hold for all a,b,c. Also, when (3a) is selected, (4b) is false.

Proof; Choosing (3a), $(a \oplus b) \circ c = a \oplus b = a \circ c \oplus b \circ c$, but $a \circ (b \oplus c) = a \neq a \circ b \oplus a \circ c = a \oplus a$ since addition is not as in (1) of 3.5. The rest follows by symmetry.

3.8 Theorem. In K let multiplication be defined so that $a \cdot x = b$ (or $y \cdot a = b$) is solvable for all $a,b \in K$ and such that

$$(5) \qquad a \cdot (b \circ c) = (a \cdot b) \cdot c$$

Moreover, let $a \circ b = f(b)$ (or $a \cdot b = \varphi(a)$) where $f(b)$ indicates that $a \circ b$ depends only on b. Then $f(b) = b$ ($\Phi(a) = a$) for every b (or a) $\in$ K. $a \cdot (b \cdot c) = f(b \cdot c) = f\,[f(c)]$; $(a \circ b) \circ c = f(c)$. From (5)

$$(6) \qquad f\,[f(c)] = f(c)$$

Let $f(c) = d$; then $f(d) = d$ for every element d such that $d = f(c) = u \circ c$ where u is any element of K. $u \circ c = d$ is solvable in c for any element of K so that for all d

$$f(d) = d$$

The same method will prove $\phi(a) = a$.

IDEALS

4.0 Definition. Let I(a,b,...) be a subset of a ring R. I is called an ideal if and only if the following postulates are satisfied.

4.1 Postulate I. For each $a,b \in I$ there exists an $x \in I$ such that

$$a + x = b \tag{1}$$

4.2 Postulate II. For every $a \in I$ and every $r \in R$, $r\,a \in I$

4.3 Postulate III. For every $a \in I$ and every $r \in R$, $a\,r \in I$

5.1 Theorem. The elements of an ideal form an additive Abelian group.

Proof: Since the elements of the ideal are in a ring the addition is associative and commutative. Solvability, both right and left, follows from the commutativity and Postulate I. The remainder of the proof follows the lines of Theorem 2.1 of this section.

5.2 Remark. An ideal is usually defined by Postulates II and III and by the property that the elements form an Abelian group with respect to addition. Our postulates are equivalent to this as theorem 5.1 shows, and moreover are completely independent as will be shown. Still another definition demands that if a and b are in I, $a - b \in I$ as well as Postulates I and II. This, of course, is also implied by our definition, since it is a property of Abelian groups.

6.1 <u>Theorem</u>. The Postulates I, II, III for an ideal are completely independent.

Character	Ring	Addition: a + b =	Multiplication: a b =	Ideal
(+ + +)	Integers	$a + b$	ab	Even integers
(+ + –)	Linear set of elements $a = a_1i+a_2j$ $b = b_1i+b_2j$ over the rational integers	$(a_1+b_1)i + (a_2+b_2)j$	$(a_1+a_2)b_1i + (a_1+a_2)b_2j$	All elements of form $(a_1i+a_2j)i = (a_1+a_2)i$ $ij = j$ is not in the ideal; so Post.III is false.
(+ – +)	Same as (+ + –)	$(a_1+a_2)i + (b_1+b_2)j$	$a_1(b_1+b_2)i + a_2(b_1+b_2)j$	All elements of form $i(a_1i + a_2j)$
(– + +)	Integers	$a + b$	ab	Zero and all integers n such that $\|n\| > 5$
(– – +)	Same as (+ + –)	Same as (+ – +)	Same as (+ – +)	All elements aj where a is an integer such that $\|a\| > 5$ or $a = 0$
(– + –)	Same as (+ + –)	Same as (+ + –)	Same as (+ + –)	All elements aj where a is an integer such that $\|a\| > 5$ or $a = 0$
(+ – –)	Rationals	$a + b$	ab	Rationals r such that 2r is an integer
(– – –)	Integers	$a + b$	ab	Positive even integers

PART III

DIVISION SYSTEMS

0.0 Definition. Suppose that to each element x of a class K there corresponds a unique subclass $P_x \subseteq K$. K will be called a division system if the Postulates I through V below hold for every element of K.

0.1 Definition. The unique subclass corresponding to x is called the principal ideal of x,

0.2 Definition. If there exists an element i in K such that $P_i = K$, i is called a unit of K.

0.3 Postulate I. $a \in P_a$.

0.4 Postulate II. If $a \in P_b$, then $P_a \leqslant P_b$.

0.5 Postulate III. Every subset $S \subseteq K$ is contained in at least one and at most a finite number of principal ideals.

0.6 Postulate IV. For every $a \in K$ there is an element b not in P_a such that $P_aP_b \neq P_a$.

0.7 Postulate V. The (logical) product of two principal ideals is a principal ideal.

0.8 Theorem. The Postulates I through V are consistent and independent.

Proof: By following examples:

Character	Class K	Principal ideal of x, P_x
(+ + + + +)	Positive integers.	All multiples of x by a positive integer.
(+ + + + -)	Positive integers with 6 omitted.	All multiples of x by a positive integer other than 6. (Eg. P_2P_3 is not a principal ideal.)
(+ + + - +)	Positive integers.	All integers $y \geqslant x$.
(+ + - + +)	Integers > 1	x and all its multiples by an integer > 1. (Eg. no principal ideal contains the pair, (2,3).)
(+ + - + +)*	1 and all fractions with even denominators in lowest terms.	x and all its multiples by a fraction with even denominator in lowest terms. (Every element belongs to an infinite number of ideals.)
(+ - + + +)	Integer couples (a,b) $1 \leqslant a \leqslant 100$; $1 \leqslant b \leqslant 100$.	$x = (x_1,x_2)$; P_x consists of all couples (y_1,y_2) such that either y_1 is a multiple of x_1 or y_2 is a multiple of x_2 where $1 \leqslant y_1 \leqslant 100$; $1 \leqslant y_2 \leqslant 100$.
(- + + + +)	Positive integers.	$P_1 = K$; P_x for $x > 1$ consists of all integers $y > x$.

0.9 Examples of Division Systems. The simplest example is that given under (+ + + + +). Postulate I expresses the fact that divisibility is a reflexive relation and II that it is transitive. III insures the existence of a unit, and moreover adds the restriction

*Two examples are given, one in which a subset S may belong to no principal ideal but at most belongs to a finite number; and a second in which S is contained in at least one and not necessarily in a finite number of principal ideals.

that every integer has at most a finite number of divisors. IV rules out trivial systems such as totally ordered classes, which satisfy all the other postulates. Postulate V states that among the common multiples of a set there is always a least, i.e., one that divides all the rest.

Another example is all the integers positive and negative but not zero. This illustrates the more general situation that equivalent elements, as the equivalence relation will be defined in 1.0, are not equal but merely associate. For instance by the definition of 1.0, 1 ⊜ -1 and in general n ⊜ $-n$, since both n and -n determine the same set of multiples.

The positive Gaussian integers form a division system with the principal ideals defined as usual. Equivalence again means differing only by a unit factor, eg., 2 ⊜ $2i$ since i is a unit. The integers of an algebraic number field in general, however, do not form a division system. Thus in the quadratic integers $a + b\sqrt{-5}$, where a and b are rational integers, the common divisors of 9 and $3 - 6\sqrt{-5}$ are ± 1, ± 3, $\pm(2 - \sqrt{-5})$ no one of which is divisible by all the others; so there exists no G.C.D.

1.0 Definition. We define an equality in K as follows: $a = b$ if and only if $P_a = P_b$

1.1 Remark. The correspondence between classes of equivalent elements and principal ideals is now one to one.

1.2 Theorem. $a = a$.

1.3 Theorem. If $a = b$, $b = a$.

1.4 Theorem. If $a = b$ and $b = c$, then $a = c$.

1.5 Remark. Equality as defined in 1.0 is an equivalence relation.

1.6 Definition. If $b \in P_a$, a is said to divide b, written $a \mid b$.

1.7 Theorem. $a \mid a$ (by Postulate I).

1.8 Theorem. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Since $a \mid b$, $b \in P_a$. By Postulate II, $P_b \leqslant P_a$. Since $b \mid c$, $c \in P_b \leqslant P_a$ so that $c \in P_a$. Therefore $a \mid c$.

1.9 Theorem. If $a \mid b$ and $b \mid a$, then $a = b$.

Proof: By Postulate II, since $a \mid b$, $b \in P_a$ and $P_b \leqslant P_a$. Similarly $P_a \leqslant P_b$. By 1.0, then, $a = b$, since $P_a = P_b$.

1.10 Definition. If a b, a is called a divisor of b, and b is called a multiple of a.

1.11 Theorem. There exists a unit in K.

Proof: By Postulate III, K is the principal ideal of some element i, which is then a unit by definition.

1.12 Theorem. There exists only one unit i in K.

Proof: Suppose there were two units i_1 and i_2. Then $K = P_{i_1} = P_{i_2}$ $\therefore i_1 = i_2$ by 1.0.

1.13 Theorem. The unit divides every element of K.

For $a \in K = P_i \therefore i|a$ by 1.6.

1.14 Theorem. Every element of K has a finite number of divisors.

Proof: Let a be any element of K. It has at least one divisor, since a a. It has at most a finite number, since if $x|a$, $a \in P_x$ and by Postulate III a belongs to a finite number of principal ideals P_x.

1.15 Theorem. Let $a \neq i$. Then there exists an element b such that a does not divide b and b does not divide a.

Proof: Direct from Postulate IV.

2.1 Definition. An element which is a multiple of every element of a set S is a common multiple of S.

2.2 Theorem. The product of a finite number of principal ideals is a principal ideal.

Proof: The theorem is trivial for one principal ideal, and for two it is a direct consequence of Postulate V. Assume it true for the n principal ideals. $P_{a_1}, P_{a_2}, \ldots, P_{a_n}$. Then their product $P_a \equiv P_{a_1}P_{a_2} \ldots P_{a_n}$ is a principal ideal. Now consider the $n + 1$ principal ideals $P_{a_1}, \ldots, P_{a_{n+1}}$. Their product is $P_{a_1}P_{a_2} \ldots P_{a_{n+1}} = P_a P_{a_{n+1}}$. This is a principal ideal by Postulate V and the induction is complete.

2.3 Theorem. Every principal ideal contains at least one element. For, if P_x is any principal ideal, $x \in P_x$ by Postulate I.

2.4 Remark. The null class is not a principal ideal.

2.5 Theorem. Every finite set has at least one common multiple. Let S be a set of elements $a_1, a_2, \ldots, a_n$. The product $P = P_{a_1}P_{a_2} \ldots P_{a_n}$ of their principal ideals is a principal ideal by 2.2. It is non-empty by 2.3. Every element of P is a common multiple of S by definitions 1.10 and 2.1.

2.6 Definition. A common multiple of a set S which divides every other common multiple is a least common multiple (L.C.M.) of S.

2.7 Theorem. Every finite set has a least common multiple in K.

Proof: Let $S \subset K$ be any finite set of elements $a_1, a_2, \ldots a_n$. Let $P_m \equiv P_{a_1}P_{a_1} \ldots P_{a_n}$. P_m is a principal ideal by 2.2. Consider the element m of which P_m is the principal ideal. m is a multiple of each of the elements $a_i \in S$, since $m \in P_m$ and P_m is the class of all common multiples of S. Any other common multiple m' is thus also in P_m.

Therefore m' is a multiple of m or m divides m', and is the required L.C.M. by 2.6.

2.8 Theorem. Every finite set has a unique L.C.M.

Proof: It has at least one by the previous theorem. If there were two, say m_1 and m_2, $m_1 \mid m_2$ and $m_2 \mid m_1$. Therefore $m_1 = m_2$ by 1.9.

3.1 Definition. An element which divides every member of a set S is a common divisor of S.

3.2 Theorem. Every set $S \leqslant K$ has at least one and at most a finite number of common divisors.

Proof: By Postulate III S is contained in at least one and at most a finite number of principal ideals $P_{a_1}, P_{a_2}, \ldots, P_{a_n}$. Then the elements $a_1, \ldots, a_n$ are common divisors of S, since each one divides every element of its principal ideal by 1.6. If there were any other common divisor a, $S \leqslant P_a$; so that P_a must be among the P_{a_i} and a among the a_i.

3.3 Definition. A common divisor of a set S which is a multiple of every other common divisor of S is the greatest common divisor (G.C.D.) of S.

3.4 Theorem. Every set $S \leqslant K$ possesses a greatest common divisor in K.

Proof: S possesses at least one common divisor and at most a finite number by 3.2. If D is the class of all common divisors of S, then D is finite and non-empty. Therefore it will possess a unique L.C.M., d, by 2.8. We shall show that d is a G.C.D. of S. Let a_i be an arbitrary element of S. Every element of D divides a_i; so a_i is a common multiple of D by 1.10 and 2.1. Then $d \mid a_i$ since the L.C.M. of a set divides all the other common multiples by 2.6. Since this is true for any a_i, d is a common divisor of S. Let d' be any other common divisor. Then $d' \in D$. But d is a multiple of every element of D by 2.6 and 2.1. $d' \mid d$ by 1.10. Therefore d is a G.C.D. of S from 3.3.

3.5 Theorem. Every set $S \leqslant K$ possesses a unique G.C.D. in K. Proof: It has at least one by the previous theorem. If there were two, d_1 and d_2, $d_1 \mid d_2$ and $d_2 \mid d_1$; so $d_1 = d_2$ by 1.9.

3.6 Theorem. The G.C.D. of a set S is the L.C.M. of the common divisors of S.

(This is a direct consequence of the way the element d was constructed in the proof of theorem 3.4.)

3.7 Remark. It is worthy of note that while only finite sets possess an L.C.M., all sets possess a G.C.D. just as is the case in arithmetic.