THE STRUCTURE AND ARITHMETICAL THEORY OF NON-COMMUTATIVE RESIDUATED LATTICES

Thesis

by

Robert P. Dilworth

In Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

California Institute of Technology,

Pasadena, California

1939

Summary

A survey of the field of non-commutative algebra and arithmetic indicates that a great many of the results are simply statements concerning a lattice the elements of which combine under an additional operation of multiplication. This fact suggests that the investigation of the algebraic and arithmetical properties of lattices with a non-commutative multiplication should simplify and correlate to a large extent a number of the important fields of modern algebra. Such an investigation is the subject of this thesis.

In chapter I the formal properties of lattices with a non-commutative multiplication and its associated residuation are treated in detail. It is shown that under certain general conditions each of these operations may be defined in terms of the other. This fact gives an easy method of extending the domain of definition of the operations and the properties of such extensions are discussed. Multiplications and residuations which are unchanged by the extension have particularly simple properties and are discussed in considerable detail. Finally, various special multiplications and residuations are investigated.

Chapter II treats lattices in which the multiplication is intimately connected with lattice division. It is shown that each element of a modular lattice in which suitable chain conditions hold, may be represented as a product of irreducibles; and if there are two such decompositions, the number of irreducibles is the same and they are similar in pairs. Applying these results to non-commutative semi-groups gives the following fundamental theorem:

The following three conditions are necessary and sufficient that a

semi-group S *with* G.C.D. *and* L.C.M. *operations have an arithmetic*:

(i) *ascending chain condition in* S

(ii) *descending chain condition for the factors of any element of* S

(iii) *modular condition in* S.

Chapter III has three main divisions. In the first part the structure of ideal lattices in the vicinity of the unit element is characterized in terms of arithmetical and semi-arithmetical lattices. In the second division decompositions into primary and semi-primary elements are discussed. And finally in the third part, the structure of archimedean residuated lattices is investigated. In particular structure theorems are proved which are analogous to the structure theorems of hypercomplex systems.

This investigation was undertaken at the suggestion of Professor Morgan Ward to whom I am indebted for constant encouragement and many timely suggestions.

TABLE OF CONTENTS

Chapter I

Multiplication and Residuation

Chapter II

Non-commutative Arithmetic

Chapter III

Algebraic Properties of Non-commutative Residuated Lattices

Section Page

CHAPTER I

Multiplication and Residuation

1. Introduction. In this work we shall investigate lattices* over which auxillary operations of multiplication and residuation are defined. The study of such systems was begun by Dedekind at the turn of the century. In spite of the importance of his work, it was almost completely overlooked until 1927-28 when Krull (Krull [1]) and Grell (Grell [1]) used Dedekind's ideas in treating the ideal theory of commutative and non-commutative rings. After Krull's 1928 paper no further work appears to have been done on this subject until the recent papers of Professor Morgan Ward and the writer on lattices with a commutative multiplication and residuation.

We shall assume that the reader is familiar with elementary lattice theory and also with the basic results of the commutative theory as developed in Ward [3] , Ward-Dilworth [1,2], and Dilworth [1]. We confine ourselves here entirely to the non-commutative case.

2. Notation and terminology. The fixed lattice of elements $a, b, c, \ldots$ will be denoted by $\mathcal{L}$. $(,)$, $[,]$, $\supset$ will

* Equivalent terms used by other authors are: structure (Ore); dualgroup (Dedekind), Verband (Klein). For a connected account of lattice theory up to 1937 cf. Koethe [1] . A complete bibliography of papers on lattice theory up to the present has been compiled by H. A. Arnold, Thesis, C. I. T. (1939).

denote union, cross-cut, and lattice division respectively. If $a \supset b$ and $b \supset a$, we say that a is equal to b and write $a = b$. Sublattices of $\mathcal{L}$ will be denoted by German capitals and subsets of $\mathcal{L}$ which are not necessarily sublattices will be denoted by latin capitals. The *direct product* of the lattices $\mathcal{L}_1, \dots, \mathcal{L}_n$ is defined to be the set of vectors $a = \{a_1, \dots, a_n\}$ where $a_i \in \mathcal{L}_i$ and union, cross-cut, and division are defined by $(a,b) = \{(a_1,b_1), \dots, (a_n,b_n)\}$, $[a,b] = \{[a_1,b_1], \dots, [a_n,b_n]\}$, $a \supset b$ if and only if $a_i \supset b_i$ $(i = 1, \dots, n)$. If $\mathcal{L}$ contains a unit element if will be denoted by u. Similarly the null element if it exists will be denoted by z. If $(a,b) = u$, a and b are said to be co-prime. A set of elements of $\mathcal{L}$ is said to be co-prime if the elements of the set are co-prime in pairs. If $a \supset x \supset b$ and $a \neq b$ implies $x = a$ or b, then a is said to cover b and we write $a > b$.

If S and T are subsets of $\mathcal{L}$, the set-theoretic sum and intersection will be denoted by $S + T$ and $S \wedge T$ respectively.

A set S of elements of $\mathcal{L}$ is said to satisfy the ascending chain condition if every chain $a_1 \subset a_2 \subset a_3 \subset \cdots$ $a_i \in \mathcal{L}$ has only a finite number of distinct elements. Similarly, if every chain $a_1 \supset a_2 \supset a_3 \supset \cdots$ $a_i \in \mathcal{L}$ has only a finite number of distinct elements, $\mathcal{L}$ is said to satisfy the descending chain condition. Ore [1] has shown that a set S closed with respect to union (cross-cut) in which the ascending (descending) chain condition holds always contains a unit (null) element. If both the ascending and descending chain conditions hold in $\mathcal{L}$, $\mathcal{L}$ is said to be *archimedean*.

If every subset S of $\mathcal{L}$ has a union $u(S)$ with the properties $u(S) \supset a$ every $a \in \mathcal{L}$ and $x \supset a$ every $a \in \mathcal{L}$ implies $x \supset u(S)$

then $\mathfrak{S}$ is said to be *completely closed with respect to union*. Similarly if every subset of $\mathfrak{S}$ has a cross-cut $k(S)$, $\mathfrak{S}$ is said to be *completely closed with respect to cross-cut*. If $\mathfrak{S}$ is completely closed with respect to both union and cross-cut, we shall simply say that $\mathfrak{S}$ is *completely closed*.

3. *Formal properties of multiplication and residuation*. Let xy be a one-valued operation which orders to certain pairs of elements x, y of $\mathfrak{S}$ a unique element xy. Such an operation is called a *right multiplication* if the following postulates are satisfied:

P1. *If the products* ac *and* bc *exist, then* $(a,b)c$ *and* $[a,b]c$ *exist**

P2. $a = b \longrightarrow ac = bc, \ ca = cb$.**

P3. $(a,b)c = (ac, bc)$.

From P1-P3 we have

M1. $a \supset b \longrightarrow ac \supset bc$.

For $a \supset b \longrightarrow (a,b) = a \longrightarrow (a,b)c = ac \longrightarrow (ac,bc) = ac \longrightarrow ac \supset bc$.

M2. $[ac, bc] \supset [a,b]c$.

For $ac \supset [a,b]c$ and $bc \supset [a,b]c$ by M1. Hence $[ac,bc] \supset [a,b]c$.

A one-valued operation $x \cdot y^{-1}$ which orders to certain pairs of elements x, y of $\mathfrak{S}$ a unique element $x \cdot y^{-1}$ is called a *right residuation* if the following postulates are satisfied:

* If $\mathfrak{S}$ is completely closed we assume that $u(S)c$ and $k(S)c$ exist if ac exists for all $a \in S$.

** In this and succeeding formulas the relations are assumed to hold if and only if the indicated products exist. The symbol $\longrightarrow$ denotes formal implication.

Q1. *If* $a\cdot c^{-1}$ *and* $b\cdot c^{-1}$ *exist, then* $[a,b]\cdot c^{-1}$ *and* $(a,b)\cdot c^{-1}$ *exist.*

Q2. $a = b \longrightarrow a\cdot c^{-1} = b\cdot c^{-1},\ c\cdot a^{-1} = c\cdot b^{-1}$

Q3. $[a,b]\cdot c^{-1} = [a\cdot c^{-1}, b\cdot c^{-1}]$.

From Q1-Q3 we have

R1. $a \supset b \longrightarrow a\cdot c^{-1} \supset b\cdot c^{-1}$.

For $a \supset b \longrightarrow [a,b] = b \longrightarrow [a,b]\cdot c^{-1} = b\cdot c^{-1} \longrightarrow [a\cdot c^{-1}, b\cdot c^{-1}] = b\cdot c^{-1} \longrightarrow a\cdot c^{-1} \supset b\cdot c^{-1}$.

R2. $(a,b)\cdot c^{-1} \supset (a\cdot c^{-1}, b\cdot c^{-1})$.

For $(a,b)\cdot c^{-1} \supset a\cdot c^{-1}$ and $(a,b)\cdot c^{-1} \supset b\cdot c^{-1}$ by R1. Hence R_2.

In a similar manner left multiplication $x\circ y$ and left residuation $x^{-1} y$ may be defined with the properties

P1'. *If* $a\circ b$ *and* $a\circ c$ *exist, then* $a\circ(b,c)$ *and* $a\circ[b,c]$ *exist.*

P2'. $a = b \longrightarrow a\circ c = b\circ c,\ c\circ a = c\circ b$.

P3'. $a\circ(b,c) = (a\circ b, a\circ c)$.

M1'. $b \supset c \longrightarrow a\circ b \supset a\circ c$.

M2'. $[a\circ b, a\circ c] \supset a\circ[b,c]$,

Q1! *If* $a^{-1}b$ *and* $a^{-1}c$ *exist, then* $a^{-1}(b,c)$ *and* $a^{-1}[b,c]$ *exist.*

Q2'. $a = b \longrightarrow c^{-1}a = c^{-1}b,\ a^{-1}c = b^{-1}c$.

Q3'. $a^{-1}[b,c] = [a^{-1}b, a^{-1}c]$.

R1'. $b \supset c \longrightarrow a^{-1}b \supset a^{-1}c$.

R2'. $a^{-1}(b,c) \supset (a^{-1}b, a^{-1}c)$

We shall now show that under certain general conditions the existence of a right multiplication implies the existence of a right residuation and conversely.

THEOREM 3.1. *If* $\mathcal{M}$ *is completely closed with respect to union and a right multiplication exists satisfying P1-P3 and such that* $u(S)a = u(Sa)$ *

* If S and T are two subsets of $\mathcal{M}$ such that the product of each element of S with each element of T exists, then ST will denote the set of these products. If T consists of one member a we write Sa.

then $\mathcal{M}$ *has a right residuation with the properties:*

R'. $a \supset (a \cdot b^{-1})b$.

R". $a \supset xb \longrightarrow a \cdot b^{-1} \supset x$.

PROOF. If a and b are such that there exists an element x with $a \supset xb$, let X denote the set of all such elements x. Let $a \cdot b^{-1} = u(X)$. Then since $a \supset xb$ all $x \in X$, $a \supset u(Xb) = u(X)b = (a \cdot b^{-1})b$. Also if $a \supset xb$, then $x \in X$ and hence $a \cdot b^{-1} \supset x$. R' and R" are thus satisfied.

Q1 *is satisfied*. For let $a \supset xc$, $b \supset yc$, then $(a,b) \supset (xc, yc) = (x,y)c$ and $[a,b] \supset [xc, yc] \supset [x,y]c$. Hence the residuals $(a,b) \cdot c^{-1}$ and $[a,b] \cdot c^{-1}$ exist.

Q2 *is satisfied*. For let $a = b$. Then $a \supset b \supset (b \cdot c^{-1})c$. Hence $a \cdot c^{-1} \supset b \cdot c^{-1}$. Also $b \supset a \supset (a \cdot c^{-1})c \longrightarrow b \cdot c^{-1} \supset a \cdot c^{-1}$. Hence $a \cdot c^{-1} = b \cdot c^{-1}$. Similarly $c \supset (c \cdot a^{-1})a = (c \cdot a^{-1})b \longrightarrow c \cdot b^{-1} \supset c \cdot a^{-1}$ and $c \supset (c \cdot b^{-1})b = (c \cdot b^{-1})a \longrightarrow c \cdot a^{-1} \supset c \cdot b^{-1}$. Hence $c \cdot a^{-1} = c \cdot b^{-1}$

Q3 *is satisfied*. $a \supset [a,b] \supset ([a,b] \cdot c^{-1})c \longrightarrow a \cdot c^{-1} \supset [a,b] \cdot c^{-1}$. Similarly $b \cdot c^{-1} \supset [a,b] \cdot c^{-1}$ and hence $[a \cdot c^{-1}, b \cdot c^{-1}] \supset [a,b] \cdot c^{-1}$. Now $[a,b] \supset [(a \cdot c^{-1})c, (b \cdot c^{-1})c] \supset [a \cdot c^{-1}, b \cdot c^{-1}]c \longrightarrow [a,b] \cdot c^{-1} \supset [a \cdot c^{-1}, b \cdot c^{-1}]$ by M2, R". Hence $[a,b] \cdot c^{-1} = [a \cdot c^{-1}, b \cdot c^{-1}]$.

THEOREM 3.2. *If* $\mathcal{M}$ *is completely closed with respect to cross-cut and a right residuation exists satisfying* Q1-Q3 *and such that* $k(S) \cdot a^{-1} = k(S \cdot a^{-1})$, *then* $\mathcal{M}$ *has a right multiplication with the properties:*

M'. $(ab) \cdot b^{-1} \supset a$

M". $x \cdot b^{-1} \supset a \longrightarrow x \supset ab$.

PROOF. If a and b are such that there exists an element x with $x \cdot b^{-1} \supset a$, let X denote the set of all such elements x. Let $ab = k(X)$.

Then $(ab)\cdot b^{-1} = k(\mathcal{X})\cdot b^{-1} = k(\mathcal{X}\cdot b^{-1}) \supset a$ since $x\cdot b^{-1}\supset a$ all $x \in \mathcal{X}$. Also if $x\cdot b^{-1} \supset a$ then $x \in \mathcal{X}$ and $x \supset ab$. M' and M" are thus satisfied.

P1 __is satisfied__. For let $x\cdot c^{-1}\supset a$, $y\cdot c^{-1}\supset b$. Then $(x,y)\cdot c^{-1}\supset(x\cdot c^{-1}, y\cdot c^{-1}) \supset (a,b)$ and $[x,y]\cdot c^{-1} = [x\cdot c^{-1}, y\cdot c^{-1}] \supset [a,b]$. Hence $(a,b)c$ and $[a,b]c$ exist.

P2 __is satisfied__. For let $a = b$. Then $(ac)\cdot c^{-1} \supset a \supset b \longrightarrow ac \supset bc$ by M" and $(bc)\cdot c^{-1} \supset b \supset a \longrightarrow bc \supset ac$. Hence $ac = bc$. Similarly $(ca)\cdot a^{-1} = (ca)\cdot b^{-1} \supset c \longrightarrow ca \supset cb$ and $(cb)\cdot a^{-1} = (cb)\cdot b^{-1} \supset c \longrightarrow cb \supset ca$. Hence $ca = cb$.

P3 __is satisfied__. For $((a,b)c)\cdot c^{-1} \supset (a,b) \supset a \longrightarrow (a,b)c \supset ac$ and $((a,b)c)\cdot c^{-1} \supset (a,b) \supset b \longrightarrow (a,b)c \supset bc$ by M". Hence $(a,b)c \supset (ac, bc)$. Also by R2 $(ac, bc)\cdot c^{-1} \supset ((ac)\cdot c^{-1}, (bc)\cdot c^{-1}) \supset (a,b)$. Hence $(ac, bc) \supset (a,b)c$, $(a,b)c = (ac, bc)$.

We clearly have similar theorems for left multiplication and residuation.

LEMMA 3.1. __Let__ $\mathcal{M}$ __have a right multiplication and let a right residuation be defined in terms of the multiplication as in theorem__ 3.1. __Then__ M' __and__ M" __hold for the multiplication and residuation.__

PROOF. Let the product ab exist. Then $ab \supset ab$. Hence $(ab)\cdot b^{-1} \supset a$ by R". If $x\cdot b^{-1} \supset a$, then $x \supset (x\cdot b^{-1})b \supset ab$ by R', R1. Hence M' and M" are satisfied.

LEMMA 3.2. __Let__ $\mathcal{M}$ __have a__ *__right__* __residuation and let a right multiplication be defined in terms of the residuation by theorem__ 3.2. __Then__ R' __and__ R" __hold for the residuation and multiplication.__

PROOF. Let $a\cdot b^{-1}$ exist. Then $a\cdot b^{-1} \supset a\cdot b^{-1}$ and $a \supset (a\cdot b^{-1})b$ by M". If $a \supset xb$, then $a\cdot b^{-1} \supset (xb)\cdot b^{-1} \supset x$ so that R' and R" are satisfied.

As a consequence of lemmas 3.1 and 3.2 we have the following two theorems:

THEOREM 3.3. *Let* $\mathcal{L}$ *be a completely closed lattice with a right multiplication which is completely distributive with respect to union. Let a residuation be defined over* $\mathcal{L}$ *as in theorem* 3.1 *and let a multiplication* $x \circ y$ *be defined in terms of the residuation as in theorem* 3.2. *Then if the product* ab *exists, the product* $a \circ b$ *exists and* $a \circ b = ab$.

PROOF. To prove the theorem we shall need the following lemma:

LEMMA 3.3. *Let* $\mathcal{L}$ *be a completely closed lattice with a right multiplication which is completely destributive with respect to union. Then the right residuation defined as in theorem* 3.1 *is completely distributive with respect to cross-cut.*

Let S be a set of elements a of $\mathcal{L}$. Then since $a \supset \kappa(S)$, $a \cdot b^{-1} \supset \kappa(S) \cdot b^{-1}$. Hence $\kappa(S \cdot b^{-1}) \supset \kappa(S) \cdot b^{-1}$. On the other hand since $a \supset (a \cdot b^{-1})b$, $\kappa(S) \supset \kappa((S \cdot b^{-1})b) \supset (\kappa(S \cdot b^{-1}))b$. And hence $\kappa(S) \cdot b^{-1} \supset \kappa(S \cdot b^{-1})$. Thus $\kappa(S \cdot b^{-1}) = \kappa(S) \cdot b^{-1}$.

Continuing with the proof of the theorem we see from lemma 3.3 that the residual $x \cdot y^{-1}$ satisfies the conditions of theorem 3.2 and hence the multiplication exists. Now suppose that xy exists. Then by lemma 3.1 $(xy) \cdot y^{-1} \supset x$. Hence $x \circ y$ exists by theorem 3.2 and $xy \supset x \circ y$. Furthermore $z \cdot y^{-1} \supset x \longrightarrow z \supset xy$ and $(x \circ y) \cdot y^{-1} \supset x$. Hence $x \circ y \supset xy$. Thus $x \circ y = xy$.

THEOREM 3.4. *Let* $\mathcal{L}$ *be a completely closed lattice with a right residuation which is completely distributive with respect to cross-cut. Let a multiplication be defined over* $\mathcal{L}$ *as in theorem* 3.2 *and let a residuation* $x \circ y^{-1}$ *be defined in terms of the multiplication as in theorem* 3.1. *Then if the residual* $x \cdot y^{-1}$ *exists, the residual* $x \circ y^{-1}$

exists and $x\circ y^{-1} = x\cdot y^{-1}$.

PROOF. As in the previous case we need the following lemma:

LEMMA 3.4. *Let* $\mathfrak{L}$ *be a completely closed lattice with a right residuation which is completely distributive with respect to cross-cut. Then the right multiplication defined as in theorem* 3.2 *is completely distributive with respect to union.*

Let S be a set of elements a of $\mathfrak{L}$. Then since $u(S) \supset a$, $u(S)b \supset ab$. Hence $u(S)b \supset u(Sb)$. On the other hand since $(ab)\cdot b^{-1} \supset a$, $u(Sb)\cdot b^{-1} \supset u((Sb)\cdot b^{-1}) \supset u(S)$. Hence $u(Sb) \supset u(S)b$ and thus $u(S)b = u(Sb)$.

By lemma 3.4 the conditions of theorem 3.1 are satisfied and the residuation $x\circ y^{-1}$ exists. Let $x\cdot y^{-1}$ exist. Then $x \supset (x\cdot y^{-1})y$ by lemma 3.2. Hence $x\circ y^{-1}$ exists and $x\circ y^{-1} \supset x\cdot y^{-1}$. But $x \supset zy$ $\longrightarrow$ $x\cdot y^{-1} \supset z$ by lemma 3.2. Hence $x\cdot y^{-1} \supset x\circ y^{-1}$ since $x \supset (x\circ y^{-1})y$. Thus $x\circ y^{-1} = x\cdot y^{-1}$.

Theorems 3.3 and 3.4 show that if we start with a given multiplication (residuation) and successively define a residuation (multiplication) and multiplication (residuation), the domain of the original operation is in general extended. This process thus affords an easy method of building up a multiplication table for the given operation. For we have only to take a given set of products satisfying P1-P3 and apply the process described above. In general we will obtain an extension of the original multiplication.

The question naturally arises as to whether we can carry out the above process of extension indefinitely. The answer is that the second application of the process gives nothing new.

THEOREM 3.5. *Let* $\mathfrak{L}$ *be a completely closed lattice in which multiplication is completely distributive with respect to union. Let* $x\cdot y^{-1}$, $x\circ y$, $y\circ y^{-1}$

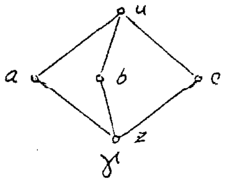
denote the successive multiplications and residuations defined by theorems 3.1 *and* 3.2. *Then* $x \circ y^{-1}$ *exists if and only if* $x \cdot y^{-1}$ *exists and* $x \circ y^{-1} = x \cdot y^{-1}$.

PROOF. From theorem 3.4, the existence of $x \circ y^{-1}$ follows from the existence of $x \cdot y^{-1}$ and $x \circ y^{-1} = x \cdot y^{-1}$. Hence it is sufficient to show that the existence of $x \cdot y^{-1}$ follows from the existence of $x \circ y^{-1}$. Let $x \circ y^{-1}$ exist. Then $x \supset (x \circ y^{-1}) \circ y$. But since the product $(x \circ y^{-1}) \circ y$ exists, $((x \circ y^{-1}) \circ y) \cdot y^{-1} \supset x \circ y^{-1}$ and hence $((x \circ y^{-1}) \circ y] \cdot y^{-1}$ exists. Thus $(x \circ y^{-1}) \circ y \supset [((x \circ y^{-1}) \circ y) \cdot y^{-1}] y$. But then $x \supset (x \circ y^{-1}) \circ y \supset [((x \circ y^{-1}) \circ y) \cdot y^{-1}] y$. And hence the residual $x \cdot y^{-1}$ exists.

THEOREM 3.6. *Let* γ *be a completely closed lattice in which residuation is completely distributive with respect to cross-cut. Let* xy, $x \circ y^{-1}$, $x \circ y$ *denote the successive multiplications and residuations defined by theorems* 3.1 *and* 3.2. *Then* $x \circ y$ *exists if and only if* xy *exists and* $x \circ y = xy$.

PROOF. By theorem 3.3 the existence of $x \circ y$ follows from the existence of xy and $x \circ y = xy$. Hence it is sufficient to show that the existence of xy follows from the existence of $x \circ y$. Let $x \circ y$ exist. Then $(x \circ y) \circ y^{-1} \supset x$ and $(x \circ y) \circ y^{-1}$ exists. Hence $x \circ y \supset ((x \circ y) \circ y^{-1}) y$ and $((x \circ y) \circ y^{-1}) y$ exists. But then $[((x \circ y) \circ y^{-1}) y] \cdot y^{-1} \supset (x \circ y) \circ y^{-1} \supset x$ and $[((x \circ y) \circ y^{-1}) y] \cdot y^{-1}$ exists. Hence xy exists by theorem 3.2.

As an example, consider the lattice diagramed below:



Let us start with the multiplication given by

	u	a	b	c	z
u	u	a	b	c	z
a	a	a			
b	b		b		
c	c			c	
z	z			z	z

The corresponding residuation is

	u	a	b	c	z
u	u	u	u	u	u
a	a	u		z	z
b	b	z	u	z	z
c	c	z		u	z
z	z	z		z	z

The multiplication defined in terms of this residuation is

	u	a	b	c	z
u	u	a	b	c	z
a	a	a	b	c	z
b	b	a	b	c	z
c	c	a	b	c	z
z	z	z	b	z	z

It will be noted that this multiplication is defined for every pair of elements of $\mathfrak{M}$.

It is obvious that a multiplication may be extended in a number of different ways and the question arises as to the relation between the extension we have just obtained and the various possible extensions. The following two theorems characterize the multiplication and residuation extensions of theorems 3.5 and 3.6 among all possible extensions.

THEOREM 3.7. *Let $\mathfrak{M}$ be a lattice with right multiplication and let xy denote its extension according to theorem* 3.5. *Now let $x \circ y$ be an arbitrary extension of the original multiplication.* *Then $xy \supset x \circ y$ whenever the two products exist.*

PROOF. Let $x \cdot y^{-1}$ denote the residual corresponding to the original multiplication and let $x \circ y^{-1}$ be the residuation corresponding to the multiplication $x \circ y$. Now $x \supset (x \cdot y^{-1}) \circ y$ since $x \circ y$ is an extension of the original multiplication. Hence $x \circ y^{-1} \supset x \cdot y^{-1}$ and $x \circ y^{-1}$ exists if $x \cdot y^{-1}$ exists. Now $(xy) \cdot y^{-1} \supset x$. Hence $(xy) \circ y^{-1}$ exists and $(xy) \circ y^{-1} \supset (xy) \cdot y^{-1} \supset x$. But then $xy \supset x \circ y$ by lemma 3.1.

In view of theorem 3.7 we may speak of the extension of the multiplication by residuation as the maximal extension. In a similar manner we find that the extension of residuation by multiplication is the minimal extension . For we have

THEOREM 3.8. *Let γ be a lattice with right residuation and let $x \cdot y^{-1}$ denote its extension according to theorem* 3.6. *Now let $x \circ y^{-1}$ be an arbitrary extension of the original residuation. Then $x \circ y^{-1} \supset x \cdot y^{-1}$ whenever the two residuals exist.*

PROOF. Let xy denote the multiplication corresponding to the original residuation and let $x \circ y$ be the multiplication corresponding to the residuation $x \circ y^{-1}$. Now $(xy) \circ y^{-1} \supset x$ since $x \circ y^{-1}$ is an extension of the original residuation. Hence $xy \supset x \circ y$ and $x \circ y$ exists if xy exists. Now $x \supset (x \cdot y^{-1})\, y$. Hence $(x \cdot y^{-1}) \circ y$ exists and $x \supset (x \cdot y^{-1})\, y \supset (x \cdot y^{-1}) \circ y$. But then $x \circ y^{-1} \supset x \cdot y^{-1}$ by lemma 3.2.

We next prove a sort of converse to theorems 3.1 and 3.2.

THEOREM 3.9. *Let γ be a lattice completely closed with respect to union, over which a right multiplication is defined. Then the existence of a right residual is necessary and sufficient that the right multiplication be completely distributive with respect to union.*

PROOF. The necessity follows from theorem 3.1. To prove the sufficiency, let S be any set of elements of γ and let $u = u(S)$, $v = u(Sa)$ where a is an arbitrary element of γ . Then $ua \supset v$ by M1. Now $v \cdot a^{-1} = u(Sa) \cdot a^{-1} \supset u\left((Sa) \cdot a^{-1}\right) \supset u(S) = u$ and $v \cdot a^{-1}$ exists since $v \supset sa$ for any element $s \in S$. But then $v \supset (v \cdot a^{-1})a \supset ua$ by M1. Hence $v = ua$.

THEOREM 3.10. *Let γ be a lattice completely closed with respect to cross-cut, over which a right residuation is defined. Then the existence ~~of~~ a right multiplication is necessary and sufficient that the right* *residual be completely distributive with respect to cross-cut.*

PROOF. The necessity follows from theorem 3.2. To prove the sufficiency, let S be any set of elements of γ and let $u = \kappa(S)$, $v = K(S \cdot a^{-1})$ where a is an arbitrary element of γ. Then $v \supset u \cdot a^{-1}$ by R1. Now $u = \kappa(S) \supset \kappa((S \cdot a^{-1})a) \supset K(S \cdot a^{-1})a \supset va$, and va exists since $sa \supset v$ any s in S. But then $u \cdot a^{-1} \supset (va) \cdot a^{-1} \supset v$ by R1. Hence $v = u \cdot a^{-1}$.

Closely connected with the notion of residuation is the notion of a quotient.

DEFINITION 3.1. b is said to divide a on the right (left) if there exists an element x (y) such that $a = xb$ $(a = by)$. x is called a *right* quotient and y a *left* quotient.

Consider the union a/b of all quotients x such that $a = xb$. Then if multiplication is completely distributive on the right with respect to union we have $a = u(xb) = u(x)\,b = a/b\,b$. $\frac{a}{b}$ is called *the* quotient of a and b and clearly has the properties:

D1. $a = a/b\,b$

D2. $a = xb \longrightarrow a/b \supset x.$

We have then the following theorem which relates the residual to the quotient;

THEOREM 3.11. *If the right (left) quotient a/b $(b\backslash a)$ exists, then the right (left) residual $a \cdot b^{-1}$ $(b^{-1} \cdot a)$ exists and $a/b = a \cdot b^{-1}$ $(b\backslash a = b^{-1} \cdot a)$*

PROOF. Since $a \supset a/b\,b$, the right residual $a \cdot b^{-1}$ exists and $a \cdot b^{-1} \supset a/b$ by R'. But $a \supset (a \cdot b^{-1})b$. Hence $a = a/b\,b = (a/b\,b, (a \cdot b^{-1})b) = (a/b, a \cdot b^{-1})b$. Then $a/b \supset (a/b, a \cdot b^{-1})$ by D2. But $(a/b, a \cdot b^{-1}) \supset a/b$. Thus $a/b = (a/b, a \cdot b^{-1})$ and hence $a/b \supset a \cdot b^{-1}$. Therefore $a/b = a \cdot b^{-1}$. Similarly $b\backslash a = b^{-1} \cdot a$.

It follows as a corollary that if $a = (a \cdot b^{-1})b$, then $a \cdot b^{-1}$ is the quotient a/b.

4. Special multiplications. In this section we shall study the dual character of multiplication and residuation under various stronger conditions.

We impose first the following restriction:

P4. $a \supset ba$ if the product ba exists.

THEOREM 4.1. P4 implies the following condition on the residual

Q4. $a \cdot a^{-1}$ exists if $x \cdot a^{-1}$ exists for any x and $a \cdot a^{-1} \supset x \cdot a^{-1}$.

Conversely Q4 implies P4 for multiplication.

PROOF. Let $x \cdot a^{-1}$ exist. Then $(x \cdot a^{-1})a$ exists and hence $a \supset (x \cdot a^{-1})a$ by P4. Hence $a \cdot a^{-1} \supset x \cdot a^{-1}$. Conversely let Q4 hold and suppose that ba exists. Then $(ba) \cdot a^{-1}$ exists. Hence by Q4, $a \cdot a^{-1}$ exists and $a \cdot a^{-1} \supset (ba) \cdot a^{-1} \supset b$. Thus $a \supset ba$.

As a consequence of P4 if a divides b on the right, then $a \supset b$.

We note that if $\mathcal{H}$ is closed with respect to multiplication condition Q4 becomes $a \cdot a^{-1} = u$ where u is the unit element of $\mathcal{H}$.

Consider now the condition

P5. $a = ua$ where u is the unit element of $\mathcal{H}$.

THEOREM 4.2. P5 implies the following condition on the residual

Q5. $a \supset b \Longleftrightarrow a \cdot b^{-1} = u$.

Conversely, Q5 implies P5 for the multiplication.

PROOF. Let $a \supset b$. Then $a \supset ub$ and the residual $a \cdot b^{-1}$ exists. Furthermore $a \cdot b^{-1} \supset u$ and hence $a \cdot b^{-1} = u$. If $a \cdot b^{-1} = u$, then $a \supset (a \cdot b^{-1})b = ub = b$. Whence Q5 is satisfied. Assume P5. Then $a \supset a \longrightarrow a \cdot a^{-1} = u$. Hence ua exists and $(ua) \cdot a^{-1} \supset u$. But then $(ua) \cdot a^{-1} = u$ and hence $ua \supset a$. Now $a \supset (a \cdot a^{-1})a = ua$.

Hence $a = ua$ and P5 is satisfied.

We note that P5 → P4. For $P5 \rightarrow a = ua = (u,b)a = (ua, ba) = (a, ba) \rightarrow a \supset ba \rightarrow P4.$

Let us now consider the case where the multiplication is both a right and left multiplication. If γ' is completely closed with respect to union and multiplication is completely distributive with respect to union, then clearly both the left and right residuations exist.

DEFINITION 4.1. A right multiplication (residuation) is said to be normal if it is equal to its maximal (minimal) extension.

A similar definition holds for left multiplication (residuation) and for a multiplication (residuation) which is both a left and right multiplication (residuation). In particular, if γ' is closed with respect to the multiplication (residuation), the multiplication (residuation) is always normal. Moreover the residuation (multiplication) defined in terms of a normal multiplication (residuation) is again normal by theorem 3.4 (3.5).

THEOREM 4.3. The condition that a normal multiplication over γ' be both a left and right multiplication implies the following condition on the residuals:

Q6. $a \cdot b^{-1} \supset c \leftrightarrows c^{-1} \cdot a \supset b.$

Conversely, Q6 implies the equality of the multiplication defined in terms of the two residuals.

PROOF. Let $a \cdot b^{-1} \supset c$. Then cb exists since the multiplication is normal and hence $a \supset (a \cdot b^{-1}) b \supset cb$ by M1. Hence $c^{-1} a$ exists and $c^{-1} a \supset b$. If $c^{-1} a \supset b$, then $a \supset c(c^{-1} a) \supset cb$ by M1' and hence $a \cdot b^{-1} \supset c$.

On the other hand let ab exist. Then $(ab)\cdot b^{-1} \supset a$ and hence $a^{-1}\cdot(ab) \supset b$ by Q6. But then $a \circ b$ exists and $ab \supset a\cdot b$ In a similar manner $a^{-1}\cdot(a\circ b) \supset b \longrightarrow (a\cdot b)\cdot b^{-1} \supset a \longrightarrow a\circ b \supset ab$ and hence $ab = a\circ b$.

LEMMA 4.1. Let γ have a normal right (left) multiplication. Then if ab exists and $a \supset c$ $(b \supset c)$, then cb (ac) exists.

PROOF. Since ab exists $(ab)\cdot b^{-1} \supset a$ $(a^{-1}(ab) \supset b)$ by lemma 3.3. But then $(ab)\cdot b^{-1} \supset c$ $(a^{-1}(ab) \supset c)$ and cb (ac) exists since the multiplication is normal.

THEOREM 4.4. Let γ have a normal left and right multiplication. Then the residuals have the following properties:

R3. $a\cdot(b,c)^{-1} = [a\cdot b^{-1}, a\cdot c^{-1}]$ if $a\cdot b^{-1}$ and $a\cdot c^{-1}$ exist.

R3'. $(a,b)^{-1}\cdot c = [a^{-1}c, b^{-1}\cdot c]$ if $a^{-1}c$ and $b^{-1}\cdot c$ exist.

PROOF. Let $X = [a\cdot b^{-1}, a\cdot c^{-1}]$. Then $a\cdot b^{-1} \supset X$ and $a\cdot c^{-1} \supset x$. Hence by Q6 and theorem 4.3 $X^{-1}a$ exists and $X^{-1}a \supset b$, $x^{-1}a \supset c$. Hence $X^{-1}\cdot a \supset (b,c)$. Again by Q6 and theorem 4.3 $a\cdot(b,c)^{-1}$ exists and $a\cdot(b,c)^{-1} \supset X$. Now $a \supset (a\cdot(b,c)^{-1})(b,c) \supset (a\cdot(b,c)^{-1})b$ by lemma 4.1 and M1'. Hence $a\cdot b^{-1} \supset a\cdot(b,c)^{-1}$. Similarly $a\cdot c^{-1} \supset a\cdot(b,c)^{-1}$. Thus $x = [a\cdot b^{-1}, a\cdot c^{-1}] \supset a\cdot(b,c)^{-1}$. Hence $X = a\cdot(b,c)^{-1}$ which proves R3. A similar proof gives R3'.

LEMMA 4.2. Let γ have a normal right (left) multiplication. Then if $a\cdot b^{-1}$ $(b^{-1}\cdot a)$ exists and $b \supset c$, $a\cdot c^{-1}$ $(c^{-1}\cdot a)$ exists.

PROOF. Since $a\cdot b^{-1}$ $(b^{-1}\cdot a)$ exists, $a \supset (a\cdot b^{-1})b$ $(a \supset b(b^{-1}\cdot a))$ Hence by lemma 4.1 $(a\cdot b^{-1})c$ $(c(b^{-1}\cdot a))$ exists. But then by M1 and M1' $a \supset (a\cdot b^{-1})c$ $(a \supset c(b^{-1}\cdot a))$. Hence $a\cdot c^{-1}$ $(c^{-1}\cdot a)$ exists.

From theorem 4.4 and lemma 4.2 we have immediately

R4 $a\cdot[b,c]^{-1} \supset (a\cdot b^{-1}, a\cdot c^{-1})$ if $a\cdot b^{-1}$ and $a\cdot c^{-1}$ exist.

R4'. $[a,b]^{-1}\cdot c \supset (a^{-1}\cdot c,\ b^{-1}\cdot c)$ if $a^{-1}\cdot c$ and $b^{-1}\cdot c$ exist.

The existence of a multiplication which is both a left and right multiplication implies the following useful relations between the two residuals:

R5. $(a\cdot b^{-1})^{-1}\cdot a \supset b$ if $a\cdot b^{-1}$ exists.

For the existence of $a\cdot b^{-1}$ implies $a \supset (a\cdot b^{-1})b$. Hence $(a\cdot b^{-1})^{-1}\cdot a$ exists and $(a\cdot b^{-1})^{-1}\cdot a \supset b$.

R5'. $a\cdot(b^{-1}\cdot a)^{-1} \supset b$ if $b^{-1}\cdot a$ exists.

From R5 and R5' we get

R6. $a\cdot((a\cdot b^{-1})^{-1}\cdot a)^{-1} = a\cdot b^{-1}$.

R6'. $(a\cdot(b^{-1}\cdot a)^{-1})^{-1}\cdot a = b^{-1}\cdot a$.

For $R5 \longrightarrow (a\cdot b^{-1})^{-1}\cdot a \supset b \longrightarrow a\cdot b^{-1} \supset a\cdot((a\cdot b^{-1})^{-1}\cdot a)^{-1}$ by $R3$. But $a\cdot((a\cdot b^{-1})^{-1}\cdot a)^{-1} \supset a\cdot b^{-1}$ by R5'. Hence $R6$ holds. In a similar manner we get $R6'$.

We note that if the notion of mutual residuation is generalized to mean: b and c are mutually residual with respect to a if either $a\cdot b^{-1} = c$ and $c^{-1}\cdot a = b$ or $b^{-1}\cdot a = c,\ a\cdot c^{-1} = b$; then $a\cdot b^{-1}$ and $(a\cdot b^{-1})^{-1}\cdot a$ are mutually residual with respect to a . Similarly $b^{-1}\cdot a$ and $a\cdot(b^{-1}\cdot a)^{-1}$ are mutually residual with respect to a.

Thus far we have made no assumption of the associative law for the multiplication. In formulating the associative law there is a certain freedom of choice in the existence conditions. However, the following formulation seems to be the only one which preserves the duality between multiplication and residuation.

P6. $a(bc) = (ab)c$ *

* In this postulate it is assumed that the existence of the products on either side of the equality implies the existence of the products on the other side.

THEOREM 4.5. Let $\mathcal{L}$ be a lattice with a right and left normal multiplication for which $P6$ holds. Then the residuals satisfy the following condition:

$Q7.$ $$(a^{-1}b)\cdot c^{-1} = a^{-1}(b\cdot c^{-1})\ ^*$$

Conversely, if $Q7$ is satisfied by the reisudals, then $P6$ holds for the multiplication.

PROOF. Let $a^{-1}b$ and $(a^{-1}b)\cdot c^{-1}$ exist. Then $a^{-1}b \supset ((a^{-1}b)\cdot c^{-1})c$, and $b \supset a(a^{-1}b) \supset a[((a^{-1}b)\cdot c^{-1})c]$ by lemma 4.1. Hence $b \supset [a((a^{-1}b)\cdot c^{-1})]c$ by $P6$. But then $b\cdot c^{-1}$ exists and $b\cdot c^{-1} \supset a((a^{-1}b\cdot c^{-1})$. Hence $a^{-1}(b\cdot c^{-1})$ exists and $a^{-1}(b\cdot c^{-1}) \supset (a^{-1}\cdot b)\cdot c^{-1}$ Similarly $(a^{-1}b)\cdot c^{-1} \supset a^{-1}(b\cdot c^{-1})$. and $Q7$ follows.

Now suppose that $Q7$ holds and let bc and $a(bc)$ exist. Then $a^{-1}(a(bc)) \supset bc$ and $(a^{-1}(a(bc))\cdot c^{-1}) \supset (bc)\cdot c^{-1} \supset b$ by lemma 4.2. But then $a^{-1}((a(bc))\cdot c^{-1}) \supset b$ by $Q7$. Hence $(a(bc))\cdot c^{-1} \supset ab$ Thus $(ab)c$ exists and $a(bc) \supset (ab)c$. Similarly $(ab)c \supset a(bc)$ and $P6$ follows.

As a consequence of $P6$ we have

$R7$ $$a\cdot(bc)^{-1} = (a\cdot c^{-1})\cdot b^{-1}.$$

For $a \supset (a\cdot(bc)^{-1})(bc) = ((a\cdot(bc)^{-1})b)c$ by $P6$. Hence $a\cdot c^{-1} \supset (a\cdot(bc)^{-1})b \longrightarrow (a\cdot c^{-1})\cdot b^{-1} \supset a\cdot(bc)^{-1}$. Conversely $a\cdot c^{-1} \supset ((a\cdot c^{-1})\cdot b^{-1})b \longrightarrow a \supset (a\cdot c^{-1})c \supset (((a\cdot c^{-1})\cdot b^{-1})b)c$ by lemma 4.1. But then $a \supset ((a\cdot c^{-1})\cdot b^{-1})(bc)$ by $P6$. Hence $a\cdot(bc)^{-1} \supset (a\cdot c^{-1})\cdot b^{-1}$. Thus $a\cdot(bc)^{-1}$ $= (a\cdot c^{-1})\cdot b^{-1}$

* In this condition the existence of the residuals on either side of the equality implies the existence of the residuals on the other side.

In a similar manner we have

R7'. $(ab)^{-1}c = b^{-1}(a^{-1}c)$.

In concluding this section we treat the case where we have a left and right multiplication for which the unit element of the lattice is the unit of multiplication.

P5, P5'. $ua = au = a$ all $a \in \gamma$.

We have already seen that this implies

P4, P4'. $a \supset ba, \quad a \supset ab$.

Q5, Q5'. $a \supset b \Longleftrightarrow a \cdot b^{-1} = u \Longleftrightarrow b^{-1} a = u$.

We furthermore have

R8, R8'. $a \cdot u^{-1} = u^{-1} \cdot a = a$

For $a \supset au \longrightarrow a \cdot u^{-1} \supset a$ and $a \supset (a \cdot u^{-1})u \longrightarrow a \supset a \cdot u^{-1}$. Hence $a = a \cdot u^{-1}$ and similarly $u^{-1} a = a$.

R9, R9'. $a \cdot b^{-1} \supset a, \quad b^{-1} a \supset a$ if the multiplication is normal.

For $a \supset ab \longrightarrow a \cdot b^{-1} \supset a$ and $a \supset ba \longrightarrow b^{-1} a \supset a$.

If multiplication is defined in terms of residuation, then R8 implies P5 for the multiplication. For $au = (au) \cdot u^{-1} \supset a$ and $a \cdot u^{-1} \supset a \longrightarrow a \supset au$. Hence $au = a$. Similarly $R8' \longrightarrow P5'$. Also $R9 \longrightarrow P4$ and $R9' \longrightarrow P4'$ if the mesiduation is normal. Hence we may state

THEOREM 4.6. *Let* γ *be a lattice with right (left) multiplication and residuation. Then* $P5 \Longleftrightarrow Q5 \Longleftrightarrow R8$ $(P5' \Longleftrightarrow Q5' \Longleftrightarrow R8')$ *and if the residuation and multiplication are normal, then*

$P4 \Longleftrightarrow Q4 \Longleftrightarrow R9$ $(P4' \Longleftrightarrow Q4' \Longleftrightarrow R9')$.

5. Examples. We list in this section a few examples of systems having the properties discussed in this chapter.

1. Let R be a ring in which multiplication is distributive only on the right with respect to addition. Let $\mathfrak{M}$ be lattice of modules of The product $\mathfrak{a}\mathfrak{b}$ of two modules is defined to be the set of elements $a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$ where $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. $\mathfrak{a}\mathfrak{b}$ is clearly a module of $\mathfrak{M}$. With this definition of multiplication $\mathfrak{M}$ is a lattice with right multiplication.

2. If R is a ring in which multiplication is distributive only on the left with respect to addition, then as in (1) the lattice $\mathfrak{M}$ of modules of R has a left multiplication.

3. The lattice of modules of an arbitrary ring has a multiplication which is both a left and right multiplication.

4. The examples 1, 2, and 3 all give lattices in which the associative law is satisfied. If we start with a non-associative ring then the lattice of modules has a multiplication which is no longer associative.

5. Let R be a non-associative ring in which multiplication is distributive only on the right with respect to addition. A module $\mathfrak{a}$ of R is called a left ideal if $ra \in \mathfrak{a}$ all $a \in \mathfrak{a}$, $r \in R$. The set of all left ideals of R is a lattice with right multiplication in which $P4$ holds.

6. The right ideals of R in 5 give a lattice with right multiplication in which $P4'$ holds.

7. The two-sided ideals of R in 5 form a lattice with right multiplication in which both $P4$ and $P4'$ are satisfied.

8. Let R be a non-associative ring with a left unit element.

Then the lattice of left ideals has a left and right multiplication in which $P5$ holds.

9. As in (8) a non-associative ring with right unit element gives a lattice of right ideals with multiplication for which $P5'$ holds.

10. The two-sided ideals of an arbitrary non-commutative ring yield a lattice with right and left multiplication in which $P4$, $P4'$ and $P6$ hold.

11. If the ring of example 10 has a unit element then the lattice of two-sided ideals satisfies $P5$ and $P5'$.

Finally in sections 4, 5, and 6 of Chapter II several additional examples of lattices with a non-commutative multiplication are treated in detail.

CHAPTER II

Non-commutative Arithmetic

1. Introduction. The subject of the present chapter is the fundamental problem of obtaining decompositions which are in some sense unique for the elements of a multiplicative domain. Conditions that a system with a commutative and associative multiplication have unique factorization into irreducibles have been studied by Clifford [1], Konig [1], and Ward [2]. M. Ward [1] has also treated the non-commutative case. However the requirement that the decompostions be unique is too stringent since in the instances of non-commutative polynomial theory and quotient lattices the decompositions, while not unique are connected by a simple relationship. Moreover in both of these instances instead of a single operation of multiplication the additional operations G. C. D. and L. C. M. are involved. This fact suggests that starting with a lattice over which a multiplication is defined would be the most fruitful way to build a non-commutative arithmetical theory. Furthermore the formal relations between the multiplication and lattice operations have already been developed in considerable detail in chapter I and we are now ready to treat the arithmetical questions.

Before proceeding further let us note that we have already imposed certain existence conditions on the multiplication. If we write $a \rightleftarrows b$ when the product ab exists, then P1 states

(1) $\quad a \rightleftarrows c,\ b \rightleftarrows c \longrightarrow (a,b) \rightleftarrows c,\ [a,b] \rightleftarrows c.$

Furthermore P6 gives

(2) $b \rightleftharpoons c,\ a \rightleftharpoons bc \longrightarrow a \rightleftharpoons b,\ ab \rightleftharpoons c.$

The properties (1) and (2) along with an obvious transitive relation will be taken as the fundamental properties of the existence relation.

2. The multiplication. Let γ be a lattice in which the ascending chain condition holds and let u denote its unit element. Consider in γ a relation $\rightleftharpoons$ having the properties:

T1. For each $a \in \gamma$ there are elements $a', a'' \in \gamma$ such that $a \rightleftharpoons a',\ a'' \rightleftharpoons a.$

T2. $a \rightleftharpoons b,\ a = c$ and $b = d \longrightarrow c \rightleftharpoons d.$

T3. $a \rightleftharpoons c,\ b \rightleftharpoons c \longrightarrow (a,b) \rightleftharpoons c,\ [a,b] \rightleftharpoons c.$

T4. If $a \rightleftharpoons b,\ c \rightleftharpoons d$, then $c \rightleftharpoons b \longrightarrow a \rightleftharpoons d.$

DEFINITION 2.1. Let L_a denote the set of elements x such that $x \rightleftharpoons a.$

By T1 and T3, L_a is non-empty and closed with respect to union and cross-cut. Hence L_a is a sublattice of γ. Thus with each element $a \in \gamma$ we associate a sublattice L_a.

THEOREM 2.1. The sublattices L_a and L_b are either disjoint or they are identical.

PROOF. If L_a and L_b are not disjoint they have an element c in common. Let x be an arbitrary element of L_a. Then $x \rightleftharpoons a,\ c \rightleftharpoons a,$ $c \rightleftharpoons b$, and hence $x \rightleftharpoons b$ by T3. Similarly each elemtnt $y \in L_b$ belongs to L_a.

DEFINITION 2.2. We write $a \sim b$ if a and b belong to the same L-lattice.

$\sim$ is clearly an equivalence relation in γ with the L-lattices as equivalence classes.

Consider now a right multiplication xy over γ for which P4 and P6 hold and in addition the following postulates are satisfied:

P00. ab **exists if and only if** $a \rightleftharpoons b$.

P0. **With each** $a \in \gamma$ **there exists an element** $U_a \rightleftharpoons a$ **such that** $U_a a = a$.

P7. $ac = bc \longrightarrow a = b$.

By P6 we have

2.1. $a \rightleftharpoons b,\ c \rightleftharpoons ab \longrightarrow c \rightleftharpoons a$.

$a \rightleftharpoons b,\ ab \rightleftharpoons c \longrightarrow b \rightleftharpoons c$.

For $c(ab)$ exists. Hence ca exists and $c \rightleftharpoons a$ by P00.

2.2. $a \rightleftharpoons b,\ b \rightleftharpoons c \longrightarrow a \rightleftharpoons bc,\ ab \rightleftharpoons c$.

For $U_{bc} \rightleftharpoons bc \longrightarrow U_{bc} \rightleftharpoons b$ by 2.1. But then $a \rightleftharpoons b$, $U_{bc} \rightleftharpoons bc$ and $U_{bc} \rightleftharpoons b$. Hence $a \rightleftharpoons bc$ by T4. Similarly $ab \rightleftharpoons c$.

2.3. U_a **is the unit element of** L_a .

For if $x \in L_a$, then $a \supset xa \longrightarrow U_a a = a = (a, xa) = (U_a a, xa)$ $= (U_a, x)a$ by P0, P4, P3. Hence $U_a = (U_a, x)$ by P7.

Let ${}_aL$ denote the L-lattice to which a belongs. Let ${}_aU$ denote its unit element. Then we have

2.4. $a\,{}_aU = a$.

For since $a \rightleftharpoons x$ for some x , ${}_aU \rightleftharpoons x$ and ${}_aU x = x$ by 2.3 and P0. But then $a \rightleftharpoons {}_aU x$, and hence $a \rightleftharpoons {}_aU$ by 2.1. Now $ax = a({}_aU x) = (a\,{}_aU)x \longrightarrow a = a\,{}_aU$ by P6 and P7.

From the results of chapter I since the ascending chain condition holds in γ , there exists a residuation $x \cdot y^{-1}$ satisfying R', R", Q1-Q4.

DEFINITION 2.4. We write $a \ominus b$ if the residual $a \cdot b^{-1}$ exists.

2.5. $a \cdot a^{-1} = U_a$

For $a = U_a a \longrightarrow a \supset U_a a \longrightarrow a \cdot a^{-1} \supset U_a$. But $a \cdot a^{-1} \rightleftharpoons a$. Hence $U_a \supset a \cdot a^{-1}$. Therefore $a \cdot a^{-1} = U_a$.

2.6. $(ab) \cdot b^{-1} = a$.

For $(ab) \cdot b^{-1} \supset a$ by lemma 3.1 ch. 1. But $ab \supset ((ab) \cdot b^{-1})b$

$\longrightarrow a' \supset (ab)\cdot b^{-1}$ by P7. Hence $(ab)\cdot b^{-1} - a$.

2.7. $a \supset b$ <u>if and only if</u> $a\cdot b^{-1} = u_b$

For $a \supset b \longrightarrow a \supset u_b b \longrightarrow a\cdot b^{-1} \supset u_b$. But since $a\cdot b^{-1} \rightleftharpoons b$, $u_b \supset a\cdot b^{-1}$ Hence $a\cdot b^{-1} = u_b$. Conversely if $a\cdot b^{-1} = u_b$, then $a \supset (a\cdot b^{-1})b \supset u_b b = b$.

3. <u>The decomposition theory</u>. Throughout this section we make the following assumptions:

A1. $a \sim b \longrightarrow a \ominus b$.

A2. $b \supset a,\ a \ominus b \longrightarrow a = (a\cdot b^{-1})b$.

A3. $\mathcal{N}$ <u>is modular</u>.

As a consequence of A1 and A2, we have

3.1. $a \ominus c,\ b \ominus c \longrightarrow a\cdot c^{-1} \ominus b\cdot c^{-1}$.

For since $a\cdot c^{-1} \rightleftharpoons c$, $b\cdot c^{-1} \rightleftharpoons c$, we have $a\cdot c^{-1} \ominus b\cdot c^{-1}$ by A1.

3.2. $a \sim b \longrightarrow a \ominus (a, b)$.

For $a \sim b \longrightarrow a \sim (a, b) \longrightarrow a \ominus (a, b)$ by A1.

3.3. $[a, b] = (a\cdot b^{-1})b$ <u>if</u> $a \ominus b$.

For $a \supset [a, b] \longrightarrow [a, b] = ([a, b]\cdot b^{-1})b$ by A2 since $a \ominus b$ $\longrightarrow [a, b] \ominus b$ by Q1. But $[a, b]\cdot b^{-1} = [a\cdot b^{-1}, b\cdot b^{-1}] = [a\cdot b^{-1}, u_b] = a\cdot b^{-1}$ Hence $[a, b] = (a\cdot b^{-1})b$.

LEMMA 3.1. $(ba)\cdot c^{-1} = (b\cdot (c\cdot a^{-1})^{-1})(a\cdot c^{-1})$ <u>if</u> $b \rightleftharpoons a$, $c \ominus a$, $a \ominus c$, $ba \ominus c$.

PROOF. $((ba)\cdot c^{-1})c = [ba, c] = ([ba, c]\cdot a^{-1})a = [(ba)\cdot a^{-1}, c\cdot a^{-1}]a$ $= [b, c\cdot a^{-1}]a$ by Q3, 3.3, 2.6. Now $(ba)\cdot a^{-1} \ominus c\cdot a^{-1}$ by 3.1 and hence $b \ominus c\cdot a^{-1}$ by 2.6. Hence $(ba\cdot c^{-1})c = ((b\cdot (c\cdot a^{-1})^{-1})(c\cdot a^{-1}))a$ $= (b\cdot (c\cdot a^{-1})^{-1})((c\cdot a^{-1})a) = (b\cdot (c\cdot a^{-1})^{-1})[a, c] = (b\cdot (c\cdot a^{-1})^{-1})((a\cdot c^{-1})c) =$ $((b\cdot (c\cdot a^{-1})^{-1})(a\cdot c^{-1}))c$ by P6. Hence $(ba)\cdot c^{-1} = (b\cdot (c\cdot a^{-1})^{-1})(a\cdot c^{-1})$ by P7.

DEFINITION 3.1. If $a' = a\cdot b^{-1}$ where $a \sim b$ and $(a, b) = au$ we say that a' is conjugate to a.

DEFINITION 3.2. a is said to be __similar__ to b if there exists a chain of elements $a = a_0, a_1, \ldots, a_n = b$ such that either a_i is conjugate to a_{i+1} or a_{i+1} is conjugate to a_i. (Ore [1]).

The relation of similarity is clearly reflexive, symetric, and transitive.

DEFINITION 3.3. An element $p \in \mathcal{X}$ is said to be __irreducible__ if $p \neq {}_p\mathcal{U}$, and if $x \supset p,\ x \sim p \longrightarrow x = {}_p\mathcal{U}$ __or__ $x = p$.

LEMMA 3.2. __If__ p __is irreducible, then__ $p \not\supset a$ __and__ $p \sim a \longrightarrow (a, p) = {}_p\mathcal{U}$.

PROOF. $(a, p) \supset p$ and $(a, p) \sim p$ since $p \sim a$. Hence either $(a, p) = {}_p\mathcal{U}$ or $(a, p) = p$. If $(a, p) = p$, then $p \supset a$ which contradicts $p \not\supset a$.

LEMMA 3.3. __If__ p __is irreducible and__ $p \supset ab,\ p \sim b,\ p \not\supset b$, __then__ $p' \supset a$ __where__ p' __is conjugate to__ p.

PROOF. Clearly $p \ominus b$. Hence $p \cdot b^{-1} \supset (ab) \cdot b^{-1} = a$. But $(p, b) = {}_p\mathcal{U}$ by lemma 3.4 and $p \sim b$ by assumption. Hence $p' = p \cdot b^{-1}$ is conjugate to p.

THEOREM 3.1. __An element conjugate to an irreducible element is an irreducible element.__

PROOF. Let p be an irreducible element, and let $p' = p \cdot a^{-1}$ where $p \sim a$ and $(p, a) = {}_p\mathcal{U}$. Let $x \supset p'$ with $x \sim p'$. Then $x \supset p \cdot a^{-1}$ and $xa \supset (p \cdot a^{-1})a = [a, p]$ by 3.3 since $p' \rightleftharpoons a$ and $x \sim p'$. Hence $xa = (xa, [a, p]) = [a, (xa, p)]$ by A3. Thus $x = (xa) \cdot a^{-1} = [a, (xa, p)] \cdot a^{-1} = (xa, p) \cdot a^{-1}$ by 2.6, Q3, 2.7. Now $a \rightleftharpoons d$ for some d by T1 and hence $p'a \rightleftharpoons d$, $xa \rightleftharpoons d$ by 2.2. We thus have $xa \sim p'a = (p \cdot a^{-1})a = [a, p]$. But since $p \sim a$, $[a, p] \sim p$ and hence $xa \sim p$. $(xa, p) \supset p$ gives $(xa, p) = {}_p\mathcal{U}$ or p since p is an irreducible; and henco $x = {}_p\mathcal{U} \cdot a^{-1} = \mathcal{U}a = {}_p\mathcal{U}$ or $x = p \cdot a^{-1} = p'$

THEOREM 3.2. <u>If an irreducible</u> p <u>is conjugate to an element</u> p', <u>then</u> p' <u>is an irreducible.</u>

PROOF. Let $p = p' \cdot a^{-1}$ where $p' \sim a$ and $(p', a) = {}_p u$ and let $x \supset p'$, $x \sim p'$. Then $x \cdot a^{-1} \supset p' \cdot a^{-1}$ by Q3, A1; and thus $x \cdot a^{-1} \supset p$. Also $x \cdot a^{-1} \sim p$ since $x \cdot a^{-1} \cong a$ and $p \cong a$. Hence we have either (i) $x \cdot a^{-1} = {}_p u$ or (ii) $x \cdot a^{-1} = p$. If (i) holds, then $x \cdot a^{-1} = u_a$ since $p \cong a$ and hence $x \supset a$ by 2.7. But $x \supset p'$ by hypothesis, hence $x \supset (a, p') = {}_p u$. And since $x \sim p'$, $x = {}_p u$. If (ii) holds, we have $(x \cdot a^{-1})a = (p' \cdot a^{-1})a$ or $[x, a] = [p', a]$ by 3.3. But then $x \supset p' \supset [x, a]$ and by A3, $p' = [x, (p', a)] = [x, {}_p u] = x$. Hence either $x = {}_p u$ or $x = p'$ and thus p' is irreducible.

THEOREM 3.3. <u>Every element similar to an irreducible element is irreducible.</u>

PROOF. Clear from theorems 3.1 and 3.2 and definition 3.2.

THEOREM 3.4. <u>Let</u> a' <u>be conjugate to</u> $a = a_k a_{k-1} \cdots a_2 a_1$, <u>then</u> $a' = a_k' a_{k-1}' \cdots a_2' a_1'$ <u>where</u> a_i' <u>is conjugate to</u> a_i.

PROOF. Suppose the theorem is true for every product of $k-1$ elements and let $a' = a \cdot b^{-1}$, $a \sim b$, $(a, b) = {}_b u$. Then $a \ominus b$, $a_1 \ominus b$, $b \ominus a$ since $a \sim b$ and $a_1 \sim b$. Thus $a' = ((a_k \cdots a_2) \cdot (b \cdot a_1^{-1})^{-1})(a_1 \cdot b^{-1})$ by lemma 3.1. Now $a_1 \sim b$ and $(a_1, b) \supset (a, b) = {}_b u$ which gives $(a_1, b) = {}_b u$. Hence $a_1' = a_1 \cdot b^{-1}$ is conjugate to a_1. Let $b' = b \cdot a_1^{-1}$ and $s = a_k \cdots a_2$. Then $b' \sim s$ since $b' \cong a_1$, and $s \cong a_1$. Now $(s, b')a_1 = (sa_1, b'a_1) = (a, (b \cdot a_1^{-1})a_1) = (a, [b, a_1])$ $= [a_1, (b, a)] = [a_1, {}_a u] = a_1$ by P3, 313 and A3. Hence $(s, b') = a_1 \cdot a_1^{-1} = {}_{b'} u$. Thus $s \cdot b'^{-1}$ is conjugate to s and hence $s \cdot b'^{-1} = a_k' a_{k-1}' \cdots a_2'$ by hypothesis. Substitution gives $a' = a_k' \cdots a_1'$

We now prove the fundamental

THEOREM 3.4. If an element $a \in \mathcal{K}$ has two representations as a product of irreducibles $a = p_r p_{r-1} \cdots p_2 p_1 = q_s q_{s-1} \cdots q_2 q_1$, then $r = s$ and the p's and q's are similar in pairs.

PROOF*. Let $a = p_r \cdots p_1 = q_s \cdots q_1$ (1)

If $p_1 = q_1$, this factor may be cancelled. If $p_1 \neq q_1$, let k be the first number such that $q_1 \supset p_k p_{k-1} \cdots p_1$; then $q_1 \not\supset p_{k-1} \cdots p_1$ and $p_{k-1} \cdots p_1 \sim q_1$. Hence $(q_1, p_{k-1} \cdots p_1) = q_1\mathcal{U}$ by lemma 3.2. But then $q \cdot (p_{k-1} \cdots p_1)^{-1} \supset p_k$ and $q_1' = q_1 \cdot (p_{k-1} \cdots p_1)^{-1}$ is conjugate to q_1 and thus is an irreducible by theorem 3.1. Hence $q_1' = p_k$. Now $p_k p_{k-1} \cdots p_1 = (q_1 \cdot (p_{k-1} \cdots p_1)^{-1})(p_{k-1} \cdots p_1) = [q_1, p_{k-1} \cdots p_1] = ((p_{k-1} \cdots p_1) \cdot q_1^{-1}) q_1$ by 3.3. Hence $p_k p_{k-1} \cdots p_1 = p_{k-1}' \cdots p_1' q_1$ by theorem 3.4 and p_i' is conjugate to p_i $(i = 1, \cdots, k)$. Substituting this result in (1) and cancelling q_1 we may treat the resulting expression in the same manner. We thus find $r = s$ and the p's and q's similar in pairs.

Concerning the existence of a decomposition into irreducibles we have the following theorem:

THEOREM 3.5. If the descending chain condition holds for the right factors of $a \neq a\mathcal{U}$, then a has a decomposition into irreducible elements.

PROOF. If a is not irreducible, then there is an element $a_1 \neq a\mathcal{U}$ such that $a_1 \supset a$, $a_1 \sim a$ and $a_1 \neq a$. But then $a = (a a_1^{-1}) a_1$ by A2. If a_1 is not an irreducible we have an $a_2 \neq a\mathcal{U}$ such that $a_2 \supset a_1$, $a_2 \sim a_1$ and $a_2 \neq a_1$. Then $a = (a \cdot a_1^{-1})(a_1 \cdot a_2^{-1}) a_2$. We Thus get a chain of elements $a \subset a_1 \subset a_2 \subset \cdots$ which must break

* This proof is essentially that given by Ore [2] for non-commutative polynomials.

off giving an irreducible element P_1 such that $a = bP_1$. But if b if not irreducible $b = b_1 P_2$. Since $P_1 \supset P_2 P_1 \supset \cdots$ is a descending chain for factors of a it must break off giving a decomposition $a = P_k P_{k-1} \cdots P_2 P_1$.

We note that the descending chain condition for the factors of an element of γ does not follow from the ascending chain condition in γ as in the commutative case. However it does follow from the ascending chain condition in γ' where γ' is the lattice of left union and cross-cut if they exist.

4. Examples of non-commutative arithmetic. As a first example of the abstract theory let γ be the set of polynomials $P(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, a_0 \neq 0$ in an indeterminate x with coefficients out of a (not necessarily commutative) field K. The multiplication is defined by $xa = \bar{a}x + a'$ where a, a' are elements of K. n is called the degree of $P(x)$ and we write $n = \delta(P)$. $a_0^{-1}P(x)$ is called the reduced form of $P(x)$. Let $Q(x) = b_0 x^m + \cdots + b_m, b_0 \neq 0$ be a second polynomial of γ and let $n \geq m$. Then $P(x) - a_0(b_0^{[m]})^{-1} Q(x)$ is of degree less than n. Hence for each pair of polynomials $F_1(x)$ and $F_2(x)$ there exist polynomials $q_1(x)$ and $F_3(x)$ such that

$$F_1(x) = Q_1(x) F_2(x) + F_3(x) \qquad \delta(F_3) < \delta(F_2)$$

and similarly.

$$\begin{aligned} F_2(x) &= Q_2(x) F_3(x) + F_4(x) \qquad \delta(F_4) < \delta(F_3) \\ &\vdots \\ F_{n-2}(x) &= Q_{n-2}(x) F_{n-1}(x) + F_n(x) \\ F_{n-1}(x) &= Q_{n-1}(x) F_n(x) \end{aligned}$$

the last remainder being 0 since the degrees of the remainders continually decrease.

Let us define in γ, $A(x) \supset B(x)$ if there exists a polynomial $Q(x)$

such that $B(x) = Q(x)\,A(x)$. The operation $\supset$ is clearly reflexive and transitive and if $A \supset B,\ B \supset A$, then A and B differ only by multiplication by an element of K.

DEFINITION 4.1. The reduced form of $F_n(x)$ is called the right union of $F_1(x)$ and $F_2(x)$ and is denoted by $(F_1(x),\ F_2(x))$.

From the form of the defining equations we have

(1) $(F_1(x),\ F_2(x)) \supset F_1(x)\ ,\quad (F_1(x),\ F_2(x)) \supset F_2(x).$

(2) $P(x) \supset F_1(x)$ and $P(x) \supset F_2(x) \longrightarrow P(x) \supset (F_1(x),\ F_2(x)).$

DEFINITION 4.2. The reduced polynomial $[F_1(x),\ F_2(x)] = a\,F_{n-1}(x)\,F_n^{-1}(x)\,F_{n-2}(x)\,F_{n-1}^{-1}(x)$ $\cdots F_3(x)F_4^{-1}(x)F_2(x)F_3^{-1}(x)F_1(x)$ is called the right cross-cut of $F_1(x)$ and $F_2(x)$.

It can be readily shown (Ore [2] , pp. 485-486) that the right cross-cut $[F_1(x),\ F_2(x)]$ has the fundamental properties

(1)' $F_1(x) \supset [F_1(x),\ F_2(x)]\ ,\quad F_2(x) \supset [F_1(x),\ F_2(x)].$

(2)' $F_1(x) \supset P(x)$ and $F_2(x) \supset P(x) \longrightarrow [F_1(x),\ F_2(x)] \supset P(x).$

Hence $\mathcal{M}$ is a lattice with respect to right union and cross-cut.

Since the product of any two polynomials of $\mathcal{M}$ always exists, T1-T4 are trivially satisfied. P00 and P0 are clearly satisfied since we may take $u_a = 1$. P1 and P2 are obviously satisfied and P3 is readily verified by multiplying the defining equations of on the right by a fixed polynomial $A(x)$. The multiplication is obviously associative so that P6 is satisfied and P4 is satisfied by the definition of division. Also P7 is satisfied. For if $A(x)B(x) = 0$ then $a_0\,b_0^{[n]} = 0$ and hence $b_0^{[n]} = 0$ since $a_0 \neq 0$. But then $x^n b_0 = 0$ and $b_0 = 0$ contrary to the assumption that $b_0 \neq 0$. Since $A(x) \supset B(x)$ implies that the quotient $A(x)/B(x)$ exists, A2 follows from theorem 3.11 ch. I. A1 is obviously satisfied and we have only to show that $\mathcal{M}$ is modular. From definition 4.2 we see that $\delta[A,B] = \delta(A) + \delta(B) - \delta(A,B)$.

Furthermore if A and B are reduced and $A \supset B$, $\delta(A) = \delta(B)$ then $A = B$. For $A \supset B \longrightarrow B = QA \longrightarrow \delta(B) = \delta(QA) = \delta(Q) + \delta(A)$ $= \delta(Q) + \delta(B) \longrightarrow \delta(Q) = 0 \longrightarrow Q \in K \longrightarrow B = A$ since A and B are reduced. Now let $A \supset B$. Then $[A,(B,C)] \supset (B,[A,C])$. But $\delta[A,(B,C)] = \delta A + \delta(B,C) - \delta(A,B,C) = \delta(A) + \delta(B) + \delta(C) - \delta[B,C] - \delta(A,C) = \delta[A,C] + \delta(B) - \delta[A,B,C] = \delta(B,[A,C])$ Hence $[A,(B,C)] = (B,[A,C])$.

The irreducibles of γ are simply those polynomials whose right divisors are either elements of K or associates. Furthermore the ascending chain condition holds in γ and the descending chain condition holds for the right divisors of any element of γ as a consideration of the degrees of the polynomials easily shows. Hence the results of § 3 give:

THEOREM 4.1. _Each non-constant polynomial of a non-commutative polynomial domain has a decomposition into irreducibles. If a polynomial has two such decompositions, then the number of irreducibles in each decomposition is the same and the irreducibles are similar in pairs._

Since linear differential or difference expressions are a special case of non-commutative polynomials, theorem 4.1 gives the decomposition theorem for differential expressions proved by Loewy (Loewy [1]). Moreover the example of non-commutative polynomials may be generalized to any non-commutative domain of integrity with a Euclidean algorithm. (Wedderburn [1]).

As a second example, let γ be the set of all ordered pairs $A = a_1/a_2$ of elements of a lattice $\mathcal{L}$ for which $a_2 \supset a_1$. Union and cross-cut are defined by $(A,B) = \frac{(a_1,b_1)}{(a_2,b_2)}$, $[A,B] = \frac{[a_1,b_1]}{[a_2,b_2]}$. γ is a lattice with respect to these operations and is called the quotient lattice of $\mathcal{L}$. Let us set $A \rightleftharpoons B$ if and only if $a_2 = b_1$, in which case the product AB is defined to be a_1/b_2. a_1/b_2 is clearly an element of $\mathcal{H}$ since $b_2 \supset b_1 = a_2 \supset a_1$. The relation $\rightleftharpoons$ satisfies T1 -T4. For $a_1/a_1 \rightleftharpoons A$, $A \rightleftharpoons a_2/a_2$, hence T1 is satisfied. T2 is trivial. Let $A \rightleftharpoons C$, $B \rightleftharpoons C$. Then $a_2 = c_1$, $b_2 = c_1$ and hence $(A,B) = \frac{(a_1,b_1)}{c_1}$, $[A,B] = \frac{[a_1,b_1]}{c_1}$. Thus $(A,B) \rightleftharpoons C$ $[A,B] \rightleftharpoons C$. Hence T3 is satisfied. Finally let $A \rightleftharpoons B$, $C \rightleftharpoons D$ and $C \rightleftharpoons B$. Then $a_2 = b_1$, $c_2 = d_1$, $c_2 = b_1$, and hence $a_2 = d_1$. Thus $A \rightleftharpoons D$ proving T4.

From the definition of multiplication P00 is satisfied. P0 is satisfied since $a_1/a_1 \rightleftharpoons A$ and $\frac{a_1}{a_1}A = \frac{a_1}{a_1}\cdot\frac{a_1}{a_2} = \frac{a_1}{a_2} = A$. P1 is simply T3 and P2 is obviously satisfied. $(A,B)C = \frac{(a_1,b_1)}{c_1}\cdot\frac{c_1}{c_2} = \frac{(a_1,b_1)}{c_2} = \left(\frac{a_1}{c_2}, \frac{b_1}{c_2}\right) = \left(\frac{a_1}{a_2}\cdot\frac{c_1}{c_2}, \frac{b_1}{b_2}\cdot\frac{c_1}{c_2}\right) = (AC, BC)$. Hence P3 holds. P4 is satisfied since $(A, BA) = \left(\frac{a_1}{a_2}, \frac{b_1}{a_2}\right) = \frac{(a_1,b_1)}{a_2} = \frac{a_1}{a_2} = A$. $(AB)C = \left(\frac{a_1}{a_2}\cdot\frac{a_2}{b_2}\right)\cdot\frac{b_2}{c_2} = \frac{a_1}{c_1} = \frac{a_1}{a_2}\left(\frac{a_2}{b_2}\cdot\frac{b_2}{c_2}\right) = A(BC)$. Hence P6 holds. Let $AC = BC$. Then $\frac{a_1}{c_2} = \frac{b_1}{c_2}$ and hence $a_1 = b_1$. But $a_2 = c_1 = b_2$. Hence $A = B$, proving P7. From the definition of the relation $\sim$ we see that $A \sim B$ if and only if $a_2 = b_2$. Furthermore from chapter I $A \ominus B$ if and only if there exists an X such that $A \supset XB$. But this implies that $a_2 \supset b_2$ Conversely if $a_2 \supset b_2$, then $A \supset \frac{[a_1,b_1]}{b_1}\cdot\frac{b_1}{b_2}$ and $\frac{[a_1,b_1]}{b_1}$ belongs to $\mathcal{H}$ since $b_1 \supset [a_1,b_1]$. Hence $A \ominus B$ is and only if $a_2 \supset b_2$ Hence A1 is satisfied. If $A \supset XB$, then $x_2 = b_1$ and $a_1 \supset x_1$, $b_1 \supset x_1$ Hence $[a_1,b_1] \supset x_1$ and $\frac{[a_1,b_1]}{b_1} \supset X$. Therefore $A\cdot B^{-1} = \frac{[a_1,b_1]}{b_1}$. Let $B \supset A$, $A \ominus B$. Then $b_1 \supset a_1$, $b_2 \supset a_2$, $a_2 \supset b_2$ and hence $b_1 \supset a_1$, $a_2 = b_2$. But then $(A\cdot B^{-1})B = \frac{[a_1,b_1]}{b_1}\cdot\frac{b_1}{b_2} = \frac{a_1}{b_2} = \frac{a_1}{a_2} = A$, proving A2. If $\mathcal{L}$ is modular, then $\mathcal{H}$ is clearly modular from the definition of union and cross-cut. Finally the ascending condition holds in $\mathcal{H}$ if and only if it holds in $\mathcal{L}$ and the descending chain condition for the right divisors of an element of $\mathcal{N}$ holds if and only if it holds in $\mathcal{L}$. Hence from theorems 3.4 and 3.5 we have.

THEOREM 4.2. *Let $\mathcal{L}$ be a modular lattice in which the ascending chain condition and the descending chain condition for the divisors of an element hold. Then each element not equal to a unit of the quotient lattice $\mathcal{N}$ has a decomposition into irreducibles and if a quotient has two such decompositions, the number of irreducibles is the same and they are similar in pairs.*

The irreducibles of theorem 4.2 are those elements A for which $a_2 > a_1$. If a_1/a_2 be interpreted to mean the sublattice of elements X such that $a_2 \supset X \supset a_1$, then theorem 4.2 gives a theorem on the sublattices of a modular lattice $\mathcal{L}$. Furthermore if $\mathcal{L}$ is the lattice of normal subgroups of a group G, and a_1/a_2 is the quotient group of a_1 with respect to a_2, Theorem 4.2 then states that the maximal chains of normal subgroups connecting two normal subgroups, have the same length and the factor groups are isomorphic. That similarity of quotients implies isomorphism of the factor groups may be seen as follows. Let $B \cdot C^{-1}$ be conjugate to B. Then $(B,C) = c^{u}$ and $B \sim C$. Hence $(b_1, c_1) = c_2 = b_2$. This gives $\frac{[b_1, c_1]}{c_1}$ conjugate to $\frac{b_1}{(b_1, c_1)}$. But from group theory the quotient group $\frac{[b_1, c_1]}{c_1}$ is isomorphic to the quotient group $\frac{b_1}{(b_1, c_1)}$. Hence since the relation of isomorphism is symetric and transitive, similar quotient groups are isomorphic.

5. *Example of matrices over a ring.* Let M_R be the set of all finite matrices over a ring (non-commutative) R with unit element e.

DEFINITION 5.1. A set A of matrices of M_R is called a left ideal of M_R if

(1) the matrices of A have the same number of rows and the same

number of columns.

(2) the sum of any two matrices of A is again a matrix of A.

(3) the product on the left of a matrix $\alpha \in A$ by any square matrix of M_R having the same number of rows and columns as α has rows is again a matrix of A.

In a similar manner right ideals of M_R may be defined.

DEFINITION 5.2. A set of elements which is both a right and left ideal is called a <u>two-sided ideal</u> or simply <u>ideal</u> of M_R.

The following theorem characterizes the ideals of M_R.

THEOREM 5.1. <u>Let</u> A <u>be an ideal of</u> M_R <u>whose matrices have</u> m <u>rows and</u> n <u>columns. Then</u> A <u>is the set of all</u> m-<u>rowed</u>, n-<u>columned matrices over an ideal</u> $\mathfrak{a}$ <u>of the ring</u> R.

PROOF. Let μ be a matrix of M_K with m rows and ncolumns and let $\mu = (c_{ij})$, $i = 1, \ldots, m$; $j = 1, \ldots, n$. We define μ_{rs} to be the mn-rowed matrix with all of its elements zero except the element in the r^{th} row and s^{th} column which is c_{rs}. Furthermore let $e_{rs}^{(k)}$ be the square matrix of order k with all of its elements zero except the element in the r^{th} row and s^{th} column which is e.

Now if $\mathfrak{a}$ is the set of all elements of R which occur as elements in matrices of an ideal A of M_R, we show that $\mathfrak{a}$ <u>is a two-sided ideal of</u> R.

For let $a \in \mathfrak{a}$ and $b \in \mathfrak{a}$. Then $a = a_{rs}$, $b = b_{tu}$ where $\alpha = (a_{ij})$, $i = 1, \ldots, m$; $j = 1, \ldots, n$ and $\beta = (b_{ij})$ $i = 1, \ldots, m$, $j = 1, \ldots, n$; are matrices of A. But then A contains $\alpha' = e_{tr}^{(m)} \alpha e_{su}^{(n)}$ which has $a = a_{rs}$ in the t^{th} row and u^{th} column. Then A contains $\alpha' + \beta$ which has $a + b$ in the t^{th} row and u^{th} column. Hence $a + b \in \mathfrak{a}$. Also if r is an arbitrary element of R, A contains $\alpha\mu_n$ and $\mu_m\alpha$ where $\mu_k = \{\overbrace{r, r, \ldots, r}^{k}\}$ and $\alpha\mu$ has ar

in the r^{th} row and s^{th} column, while $\mu_m\alpha$ has ra in the r^{th} row and s^{th} column. Hence with a, $\mathfrak{a}$ contains ar and ra where r is an arbitrary element of R. Thus $\mathfrak{a}$ is a two-sided ideal of R.

We next show that A contains $a\,e_{rs}$ where a is an arbitrary element of $\mathfrak{a}$. For if $a = a_{tu}$ where $\alpha = (a_{ij})$, then A contains $e^{(m)}_{rt}\,\alpha\,e^{(n)}_{us} = a\,e_{rs}$. Thus A contains the set of all mn-rowed matrices over $\mathfrak{a}$. But the set of all mn-rowed matrices over an ideal of R is clearly an ideal of M_R. Hence A is equal to the set of all mn-rowed matrices over $\mathfrak{a}$. Thus completes the proof of the theorem.

DEFINITION 5.3. The ideal $\mathfrak{a}$ of theorem 5.1 is called the ideal of belonging to A.

In view of (1) definition 5.1 we may speak of mn-rowed ideals of M_R.

DEFINITION 5.4. Let A be an mn-rowed ideal of M_R and B an rs-rowed ideal of M_R. Let $\mathfrak{a}$ and $\mathfrak{b}$ be the belonging ideals of R. We define the union (A, B) of A and B to be the set of all $\min(m,r)$-rowed, $\min(n,s)$-columned matrices over the ideal $(\mathfrak{a},\mathfrak{b})$ of R. In a similar manner the cross-cut $[A, B]$ is defined to be the set of all $\max(m,r)$-rowed, $\max(r,s)$-columned matrices over the ideal $[\mathfrak{a},\mathfrak{b}]$ of R.

Let Γ be the set of all ideals of M_R.

THEOREM 5.2. Γ <u>is a lattice with respect to the union and cross-cut of definition</u> 5.4.

PROOF. The proof is left to the reader.

THEOREM 5.3. $A \supset B$ <u>if and only if</u> $\mathfrak{a} \supset \mathfrak{b},\ m \leq r,\ n \leq s$.

PROOF. $A \supset B \rightleftarrows (A, B) = A \rightleftarrows \min(m,r) = m,\ \min(n,s) = n,$ $(\mathfrak{a},\mathfrak{b}) = \mathfrak{a} \rightleftarrows \mathfrak{a} \supset \mathfrak{b},\ m \leq r,\ n \leq s.$

THEOREM 5.4. Γ <u>is modular</u>.

PROOF. Let $A \supset B \supset [A, C]$. Then $[A, (B, C)] \supset B$ since $\mathfrak{M}$ is a lattice. Now $\mathfrak{a} \supset \mathfrak{b} \supset [\mathfrak{a}, \mathfrak{c}]$ by theorem 5.3, and hence $\mathfrak{b} = [\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})]$ since the lattice of ideals of a ring is modular. But $[A, (B, C)]$ is $\max(m, \min(r, t))$-rowed and $\max(m, \min(r,t)) = \min(\max(m, r), \max(m, t)) = r$ since $m \leq r \leq \max(m, t)$. Hence $[A, (B, C)]$ has r rows and similarly has s columns. Thus $[A, (B, C)] = B$ by theorem 5.3.

We next define a multiplication over $\mathfrak{M}$.

DEFINITION 5.5. We write $A \rightleftharpoons B$ if the number of columns of A is the same as the number of rows of B.

DEFINITION 5.6. If $A \rightleftharpoons B$, the product $A \cdot B$ is defined to be the set of all matrices of the form $\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n$ where $\alpha_i \in A$ and $\beta_i \in B$.

We then have

THEOREM 5.5. $A \cdot B$ is an ideal of M_R.

THEOREM 5.6. Let $A \rightleftharpoons B$, A, rm-rowed and B, ms-rowed. Then $A \cdot B$ is rs-rowed and $\mathfrak{a}\mathfrak{b}$ is the ideal of R belonging to $A \cdot B$.

PROOF. $A \cdot B$ is obviously rs-rowed. Now let $\mathfrak{m}$ be the ideal belonging to $A \cdot B$. Let $m \in \mathfrak{m}$. Then m is an element of the i^{th} row and j^{th} column of $\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n$. Hence $m = \sum_{k=1}^{n}\sum_{l=1}^{m} \alpha_{il}^{(k)}\beta_{lj}^{(k)}$ where $(\alpha_{il}^{(k)}) \in A$ and $(\beta_{lj}^{(k)}) \in B$. Hence $m \in \mathfrak{a}\mathfrak{b}$ and $\mathfrak{m} \subset \mathfrak{a}\mathfrak{b}$. On the other hand let $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Then

$$\alpha = \underbrace{\begin{pmatrix} a & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix}}_{m}\Big\}r \in A \text{ and } \beta = \underbrace{\begin{pmatrix} b & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix}}_{s}\Big\}m \in B$$

Hence $\alpha\beta \in A \cdot B$ and $ab \in \mathfrak{m}$. Thus $\mathfrak{a}\mathfrak{b} \in \mathfrak{m}$. Whence $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$.

We state without proof

THEOREM 5.7. The relation $\rightleftharpoons$ satisfies T1 - T4.

It may also be readily verified that P1, P2, P3, P4, and P6 hold since they hold for the ideals of a non-commutative ring.

The lattice $\mathfrak{M}$ may be simply characterized in terms of the lattice $\mathfrak{M}_R$ of ideals of R and the lattice $\mathfrak{M}_c$ of integers ≥ 1 under the division relation $a \supset b$ if and only if $a \leq b$ as follows:

THEOREM 5.8. $\mathfrak{M}$ <u>is isomorphic to</u> $\mathfrak{M}_R \times \mathfrak{M}_c \times \mathfrak{M}_c$ <u>where</u> $\times$ <u>denotes direct product</u>.

PROOF. Let $A \in \mathfrak{M}$ correspond to $\{\bar{a}, m, n\}$ of $\mathfrak{M}_R \times \mathfrak{M}_c \times \mathfrak{M}_c$ if A is mn-rowed. This correspondence is clearly 1-1. In symbols

$$A \longleftrightarrow \{\bar{a}, m, n\}$$

Let $B \leftrightarrow \{\bar{b}, r, s\}$. Then $(A, B) \longleftrightarrow \{(\bar{a}, \bar{b}), \min(m, r), \min(n, s)\}$, $[A, B] \longleftrightarrow \{[\bar{a}, \bar{b}], \max(m, r), \max(n, s)\}$.

We note that the ascending chain condition and the descending chain condition for divisors of an element hold if and only if they hold in $\mathfrak{M}_R$, since they are always satisfied in $\mathfrak{M}_c$.

All of the conditions imposed in the abstract theory have thus been investigated except P1, P7, A1, and A2. If we consider the set $\mathfrak{M}_1$ of all matrices such that the number of rows is greater than or equal to the number of columns, then $\mathfrak{M}_1$ is clearly closed under union and cross-cut and is also closed with respect to multiplication since if A is rm-rowed $r \geq m$ and B is ns-rowed $n \geq s$, then $A \cdot B$ is rs-rowed with $r \geq s$. Now if A is an mn-rowed ideal of $\mathfrak{M}_1$ let U_A be the ideal corresponding to $\{R, n, n\}$. Then clearly $U_A \cdot A = A$; and hence P1 is satisfied.

Now let R be a domain of integrity in which every two-sided ideal is a left principle ideal*. Then P7 is satisfied. For if $A \cdot C = B \cdot C$,

* At this point we exclude from $\mathfrak{M}$ the null-ideal; that is, the ideal consisting of a single matrix all of whose elements are zero. $\mathfrak{M}$ is still a lattice since the null-ideal is irreducible. For if $[\bar{a}, \bar{b}] = 0$ then $\rho[A, B] = \rho(\bar{a}) + \rho(\bar{b}) - \rho(\bar{a}, \bar{b})$ and hence $\rho[\bar{a}, \bar{b}]$ is finite. But $\rho(0)$ is infinite since

then $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$ and hence $(a)(c) = (b)(c)$. But then $(a) = (b)$ or $\mathfrak{a} = \mathfrak{b}$. Now if $A \sim B$, then A is rm-rowed and B is sm-rowed, say. But then $A \supset X \cdot B$ where $X \longleftrightarrow \{\mathfrak{a}, \min(r,s), s\}$. Hence Al is satisfied. Finally if $\mathfrak{b} \supset \mathfrak{a}$ in R, then $(b) \supset (a)$ or $a = xb$; whence $(a) = (x)(b)$ or $\mathfrak{a} = (\mathfrak{a} \cdot \mathfrak{b}^{-1})\mathfrak{b}$ by theorem 3.11 ch. I. Now let $B \supset A$, $A \neq B$ and let $X \longleftrightarrow \{\mathfrak{a} \cdot \mathfrak{b}^{-1}, m, r\}$, $A \longleftrightarrow \{\mathfrak{a}, m, n\}$, $B \longleftrightarrow \{\mathfrak{b}, r, s\}$ Then $m \geq r$ so that $X \in \mathcal{X}$. $s \leq n$ and $n \leq s$; and hence $n = s$ But then $X \cdot B \longleftrightarrow \{(\mathfrak{a} \cdot \mathfrak{b}^{-1})\mathfrak{b}, m, s\} = \{\mathfrak{a}, m, n\} \leftrightarrow A$. Hence $A = X \cdot B$ and $A = (A \cdot B^{-1})B$ by theorem 3.11 ch. I. All of the postulates of the abstract theory are thus satisfied and theorems 3.4 and 3.5 give

THEOREM 5.9. <u>Let M_R be the set of all matrices over a non-commutative domain of integrity R in which every two-sided ideal is left principal and for which the ascending chain condition and descending chain condition for the factors of an ideal not equal to the null-ideal hold. Then each two-sided ideal of M_R can be represented as a product of irreducible two-sided ideals and if there are two such representations, the irreducible ideals are similar in pairs</u>.

This result may be easily generalized as follows: Let G be any non-commutative semi-group with right G. C. D. and L. C. M. And let be the set of vectors $A = \{a, m, n\}$ where $a \in G$, m and n are integers with $m \geq n$. Let union, cross-cut and multiplication in $\mathcal{X}$ be defined by:

$$(A,B) = \{(a,b), \min(m,r), \min(n,s)\}$$

$$[A,B] = \{[a,b], \max(m,r), \max(n,s)\}$$

$$A \cdot B = \{ab, m, s\} \quad \text{if} \quad r = n.$$

It is easily shows that all of the postulates of § 3 are satisfied and hence the decomposition theorems hold in $\mathcal{X}$.

6. <u>The arithmetic of a semi-group</u>. Let S be a semi-group of

---

$\mathfrak{a} \supset \mathfrak{a}^2 \supset \mathfrak{a}^3 \supset \cdots$ is an infinite descending chain.

elements $a, b, c, \cdots$ and unit element i such that each pair of elements a, b has a G. C. D. (a,b). Then if the ascending chain condition holds in S, a and b have an L. C. M. defined as the G. C. D. of those elements which both a and b divide. It is readily shown that $a \cdot b^{-1} = \frac{[a,b]}{b}$. The definitions of § 3 are somewhat simplified.

DEFINITION 6.1. If $a' = a \cdot b^{-1}$ where $(a,b) = i$, we say that a' is conjugate to a.

DEFINITION 6.1. a is _similar_ to b if there exists a chain of elements $a = a_0, a_1, \cdots, a_n = b$ such that either a_i is conjugate a_{i+1} or a_{i+1} is conjugate to a_i.

We have then the following fundamental theorem:

THEOREM 6.1. _Let_ S _be a semi-group with_ G. C. D. _and_ L. C. M. _operations. Then the following three conditions are necessary and sufficient that each element not equal to_ i _of_ S _be uniquely expressible as a product of irreducibles, unique up to similarity_*:

(i) _the ascending chain condition in_ S;

(ii) _the descending chain condition for the right factors of each element in_ S;

(iii) _The modular condition in_ S.

PROOF. The sufficiency of conditions (i) - (iii) follows from the results of § 3. For since the product of any two elements always exists, T1 - T4 are trivially satisfied. P00 - P7 are readily verified and A1 and A2 are trivially true since $a \theta b$ for every a and b. (iii) gives A3. Hence the existence and uniqueness theorems of § 3 hold.

* By "unique up to similarity" we mean that the irreducibles appearing in the decompositions of similar elements are similar in pairs.

Suppose now that each element not equal to i of S is uniquely (up to similarity) expressible as a product of irreducibles. We define $\rho(i) = 0$, $\rho(a) = s$ if $a = p_s p_{s-1} \cdots p_2 p_1$. Then $\rho(a)=0$ if and only if $a = i$ and $\rho(a)=1$ if and only if a is irreducible. Furthermore $\rho(ab) = \rho(a) + \rho b$ since if $a = p_{\rho(a)} \cdots p_1$ and $b = q_{\rho(b)} \cdots q_1$, then $ab = p_{\rho(a)} \cdots p_1 q_{\rho(b)} \cdots q_1$. Hence $a \supset b$ and $a \neq b$ implies that $\rho(a) < \rho(b)$. It follows that the ascending chain condition holds in S and the descending chain condition holds for the factors of each element in S.

We note that if a' is similar to a, then $\rho(a') = \rho(a)$.

Let a and b be any two elements of S. We have then $a = a_1(a,b)$ $b = b_1(a,b)$ where $(a_1, b_1) = i$. Then $[a,b] = [a_1(a,b), b_1(a,b)] = [a_1, b_1](a,b) = (a \cdot b_1^{-1})b_1(a,b) = a_1' b_1 (a,b)$ where a_1' is similar to a_1. Then $\rho([a,b]) = \rho(a_1') + \rho(b_1) + \rho((a,b)) = \rho(a_1) + \rho(b_1) + \rho((a,b))$. But $\rho(a) = \rho(a') + \rho((a,b))$ so that $\rho(a_1) = \rho(a) - \rho((a,b))$. Similarly $\rho(b_1) = \rho(b) - \rho((a,b))$. Hence $\rho([a,b]) = \rho(a) + \rho(b) - \rho((a,b))$ or $\rho([a,b]) + \rho((a,b)) = \rho(a) + \rho(b)$. Thus ρ is a rank function over S in the sense of Birkhoff (Birkhoff [1] pp. 447) and S is nodular by Birkhoff's result. Hence conditions (i) - (iii) are satisfied.

7. <u>Properties of the L-lattices</u>. Throughout this section postulate T3 will be replaced by the stronger postulate

T3'. $a \rightleftharpoons b$ <u>and</u> $c \rightleftharpoons d \longrightarrow (a,c) \rightleftharpoons (b,d),\ [a,c] \rightleftharpoons [b,d]$.

DEFINITION 7.1. The unit elements of the L-lattices are called the units of $\mathcal{H}$.

Let now $a_1, a_2 \in L$. $a_1', a_2' \in L'$ where L and L' are any two L-lattices. Then if $a_1, a_2 \rightleftharpoons x_1$; $a_1', a_2' \rightleftharpoons x_2$, we have $(a_1, a_1') \rightleftharpoons (x_1, x_2)$ and $(a_2, a_2') \rightleftharpoons (x_1, x_2)$. Hence (a_1, a_1') and (a_2, a_2') belong to the same

L-lattice. We call this L-lattice to which all of the unions of elements from L_1 and L_2 respectively belong the union of L_1 and L_2 and write (L_1, L_2). In a similar manner we define the cross-cut $[L_1, L_2]$ of two L-lattices. Hence we make the L-lattices into a lattice $\mathcal{N}_\ell$. $\mathcal{N}_\ell$ will be modular if $\mathcal{N}$ is modular.

In general the union of the unit elements of L_1 and L_2 will not be the unit element of (L_1, L_2). However we show

THEOREM 7.1. If the sescending chain condition holds in $\mathcal{N}$, then the units of $\mathcal{N}$ are closed under union and cross-cut and form a lattice isomorphic with $\mathcal{N}_\ell$.

PROOF. We prove first a necessary lemma.

LEMMA 7.1. If the descending chain condition holds in $\mathcal{N}$, then the only elements of $\mathcal{N}$ such that $x \rightleftharpoons x$ are the units of $\mathcal{N}$.

PROOF OF LEMMA. First of all we note that $u \rightleftharpoons u$ for every unit u; since if $u \rightleftharpoons u$, then $x = ux$, and hence $u \rightleftharpoons u$ by P4. Now let $a \rightleftharpoons a$ Then the chain $a, a^2, a^3, \ldots$ must break off by the descending condition so that $a^{m+n} = a^n$ or $a^m = u_a$ by P7. But since $a \rightleftharpoons a, u_a = {}_a u$ and hence $a^m = {}_a u$. We have then $a^{m-1} = {}_a u \cdot a^{-1} = {}_a u$, and finally $a = {}_a u$.

We continue with the proof of the theorem. Let u and u' be two units, so that $u \rightleftharpoons u$, $u' \rightleftharpoons u'$. Then $(u, u') \rightleftharpoons (u, u')$ and $[u, u'] = [u, u']$. Whence (u, u') and $[u, u']$ are units by lemma 7.1.

The L-lattices have a number of interesting interrelations. We mention however only one.

THEOREM 7.1. Let L be an arbitrary L-lattice and let $\ell \in L$. Then L has a sublattice isomorplic with L_ℓ and having ℓ as the unit element.

PROOF. Let $x \in L_\ell$ and set up the correspondence $x \leftrightarrow x\ell$ where $x\ell$ is clearly in L . Then $(x,y) \longleftrightarrow (x,y)l = (xl, yl)$ and $[x,y] \longleftrightarrow [x,y]l = [xl, yl]$. Forthermore the correspondence is 1-1 by F7. Hence the theorem follows.

We next characterize the irreducibles of γ' in terms of the lattice properties of the L-lattices.

THEOREM 7.3. <u>The irreducibles of</u> γ' <u>are the divisor-free elements of the L-lattices</u>.

PROOF. Let p be a divisor-free element of an L-lattice, and let $x \supset p,$ $x \sim p$, then clearly $x = pu$ or $x = p$. Conversely, if p is an irreducible, let p' be the divisor-free element of p^L dividing p . Then $p' \supset p$, $p' \sim p$ and $p' \neq pu$, and hence $p' = p$.

We note that theorem 7.3 may not hold if we weaken postulates A1 and A2. For example, let us replace A1 and A2 by

B1. $a \theta b, a \theta c, b \theta c \longrightarrow a \cdot c^{-1} \theta b \cdot c^{-1}.$

B2. $a \supset b$ <u>and</u> $b \theta c \longrightarrow a \theta c.$

B3. $a \theta b$ <u>and</u> $a \sim b \longrightarrow a \theta (a,b).$

We define conjugate elements and irreducible elements by

DEFINITION 7.1. If $a' = a \cdot b^{-1}$ where $a \sim b, a \theta b, b \theta a$, and $(a,b) = au$, we say that a' is conjugate to a .

DEFINITION 7.2. p is an irreducible if $p \neq pu$ and if $x \supset p, x \sim p$ $p \theta x \longrightarrow x = p$ or $x = pu$

With these definitions the proofs of the existence and uniqueness theorems follow, with some modifigation as in §3. However there may be irreducibles which are not divisor-free elemeñts since we may have $x \supset p, x \neq p, pu;$ $x \sim p$ but $x \not\theta p$.

We conclude this section with the investigation of the special case where θ is an equivalence relation. If θ is an equivalence relation, the equivalence classes are multiplicatively closed sublattices. Let $a = a_s \cdots a_1 = b_r \cdots b_1$, be two decompositions of a. Then $a \rightleftharpoons a_1$ and $a \rightleftharpoons b_1$. But $a_s \cdots a_2 \rightleftharpoons a_1$ and $a_s \cdots a_2 \rightleftharpoons a_3$ Hence $a \rightleftharpoons a_3 \rightleftharpoons \cdots \rightleftharpoons a_1 \rightleftharpoons b_r \rightleftharpoons \cdots \rightleftharpoons b_1$.

Thus this case reduces to that of γ' closed under multiplication.

8. The commutative case. In this section we investigate the consequences of assuming that the multiplication is commutative. Explicity we assume

A4. $a \rightleftharpoons b \longrightarrow b \rightleftharpoons a, \ ab = ba.$

We have then

8.1. $a \rightleftharpoons b, \ b \rightleftharpoons c \longrightarrow a \rightleftharpoons c.$

For since $a \rightleftharpoons b$, ab exists and $ab \rightleftharpoons c$. But $ab = ba \rightleftharpoons c$ Whence $a \rightleftharpoons c$.

8.2. $a \rightleftharpoons a$

Hence $\rightleftharpoons$ is an equivalence relation giving equivalence classes $\{a\}, \{b,\}, \cdots$. The L-lattices and the equivalence classes coincide. Furthermore we note that each equivalence class is closed with respect to union, cross-cut, multiplication, and residuation. We note also that $u_a = {}_a u$.

THEOREM 8.1. a' is conjugate to a if and only if $a' = a$.

PROOF. We prove first a series of lemmas.

LEMMA 8.1. If $a \sim b \sim c$ and $b \supset c$, then $a \cdot c^{-1} \supset a \cdot b^{-1}$.

PROOF. The residuals exist by A1. Furthermore $a \supset (a \cdot b^{-1}) b \supset (a \cdot b^{-1}) c \longrightarrow a \cdot c^{-1} \supset a \cdot b^{-1}$ by R' and R".

LEMMA 8.2. $a \sim b \sim c \longrightarrow a \cdot (b, c)^{-1} = [a \cdot b^{-1}, a \cdot c^{-1}]$

PROOF. $[a \cdot b^{-1}, a \cdot c^{-1}] \supset a \cdot (b, c)^{-1}$ by lemma 8.1. But $a \supset ((a \cdot b^{-1}) b, (a \cdot c^{-1}) c) \supset [a \cdot b^{-1}, a \cdot c^{-1}](b, c)$. Hence $a \cdot (b, c)^{-1} \supset [a \cdot b^{-1}, a \cdot c^{-1}]$

and thus $a \cdot (b,c)^{-1} = [a \cdot b^{-1}, a \cdot c^{-1}]$.

LEMMA 8.3. $a \cdot {}_a\mathcal{U}^{-1} = a \cdot \mathcal{U}_a^{-1} = a.$

PROOF. $a \supset a\mathcal{U}_a \longrightarrow a \cdot \mathcal{U}_a^{-1} \supset a$. But $a = a\mathcal{U}_a \supset (a \cdot \mathcal{U}_a^{-1})a \rightarrow a \supset a \cdot \mathcal{U}_a^{-1}$. Hence $a = a \cdot \mathcal{U}_a^{-1}$. Since $\mathcal{U}_a = {}_a\mathcal{U}$, the lemma follows.

We continue with the proof of the theorem. Let $a' = a \cdot b^{-1}, a \sim b, (a,b) = a\mathcal{U}$. Then $a = a \cdot {}_a\mathcal{U}^{-1} = a \cdot (a,b)^{-1} = [a \cdot a^{-1}, a \cdot b^{-1}] = [a\mathcal{U}, a \cdot b^{-1}] = a \cdot b^{-1} = a'$ by lemmas 8.2 and 8.3.

Now obviously any irreducible factor of an element belongs to the same equivalence class as the element itself. Furthermore since multiplication is commutative, the ascending chain condition implies the descending chain condition for the factors of an element $a \in \mathcal{N}$. Hence by the uniqueness and existence theorems and theorem 8.1 each element not a unit in $\mathcal{N}$ is uniquely expressible as a product of irreducibles, the irreducibles belonging to the same equivalence class. Thus considered as a lattice, each equivalence class is a direct product of chain lattices; i.e., an arithmetical lattice (Ward [4]).

CHAPTER III

Algebraic Properties of Non-commutative Residuated Lattices

1. *Introduction*. In the theory of non-commutative rings certain distinguished subrings, one-sided and two-sided ideals, play the important roles. Ideals combine under cross-cut, union, and multiplication and hence are an instance of a lattice over which a non-commutative multiplication is defined. The investigation of such lattices was begun by W. Krull (Krull [1, 2]) who discussed decompositions into isolated component ideals. Our aim in this chapter differs from that of Krull in that we shall be particularly interested in the lattice structure of these domains although certain related arithmetical questions are discussed.

Throughout this chapter $\mathfrak{S}$ will denote a lattice in which the ascending chain condition holds and over which a closed right and left multiplication is defined satisfying P4, P4' and P6. The theorems of chapter I then show that $\mathfrak{S}$ is closed with respect to a right and left residuation. Hence we shall call $\mathfrak{S}$ a non-commutative residuated lattice or more briefly, an *ideal* lattice. If in addition P5 and P5' hold, then we shall call $\mathfrak{S}$ a non-commutative residuated lattice with *unit* or simply, *ideal* lattice with *unit*. All of the formulas developed in chapter I hold for ideal lattices with unit and all of those formulas independent of P5 or Q5 (P5' ar Q5') hold for ideal lattices.

2. *The structure of ideal lattices with unit*. Let $\mathfrak{S}$ be an ideal

lattice with unit. Then in γ' the following formulas hold:

2.1 $(a,b) = u \longrightarrow a\cdot b^{-1} = a,\ b^{-1}a = a.$

For $(b,a) = u \longrightarrow a\cdot(a,b)^{-1} = a\cdot u^{-1} \longrightarrow$ $[a\cdot a^{-1}, a\cdot b^{-1}] = a \longrightarrow a\cdot b^{-1} = a$. Similarly $b^{-1}a = a$

2.2 $(b,c) = u \longrightarrow (a,[b,c]) = [(a,b),(a,c)].$

For $(a,[b,c])\cdot[(a,b),(a,c)]^{-1} \supset ((a,[b,c])\cdot(a,b)^{-1}, (a,[b,c])\cdot(a,c)^{-1})$ $= ([(a,[b,c])\cdot a^{-1}, (a,[b,c])\cdot b^{-1}], [(a,[b,c])\cdot a^{-1}, (a,[b,c])\cdot c^{-1}]) =$ $((a,[b,c])\cdot b^{-1}, (a,[b,c])\cdot c^{-1}) \supset (a\cdot b^{-1}, [b,c]\cdot b^{-1}, a\cdot c^{-1}, [b,c]\cdot c^{-1}) \supset$ $(a\cdot b^{-1}, c\cdot b^{-1}, a\cdot c^{-1}, b\cdot c^{-1}) \supset (c\cdot b^{-1}, b\cdot c^{-1}) \supset (c,b) = u$ by hypothesis. Hence $(a,[b,c])\cdot[(a,b),(a,c)]^{-1} = u$ and $(a,[b,c]) \supset [(a,b),(a,c)]$ by Q5. But $[(a,b),(a,c)] \supset$ $(a,[b,c])$ by lattice properties. Hence $(a,[b,c]) = [(a,b),(a,c)].$

2.3. $(b,c) = u \longrightarrow a = ([a,b],[a,c])$

For $(b,c) = u \longrightarrow ([a,b],[a,c])\cdot a^{-1} \supset ([a,b]\cdot a^{-1}, [a,c]\cdot a^{-1})$ $\supset (b\cdot a^{-1}, c\cdot a^{-1}) \supset (b,c) = u \longrightarrow ([a,b],[a,c]) = u$ $\longrightarrow ([a,b],[a,c]) \supset a.$ But $a \supset ([a,b],[a,c])$ by lattice properties. Hence $a = ([a,b],[a,c]).$

2.4. $(a,b) = u,\ (a,c) = u \longrightarrow (a,[b,c]) = u.$

For $(a,[b,c]) = (a,[b,c])\cdot u^{-1} = (a,[b,c])\cdot(a,b)^{-1} =$ $(a,[b,c])\cdot b^{-1} \supset (a\cdot b^{-1}, [b,c]\cdot b^{-1}) = (a\cdot b^{-1}, c\cdot b^{-1}) \supset$ $(a,c) = u \longrightarrow (a,[b,c]) = u.$

As a consequence of 2.2 and 2.4 we have

2.5. If $a_1,\dots,a_n$ are co-prime in pairs, then $(c,[a_1,\dots,a_n]) = [(c,a_1),\dots,(c_n,a_n)]$

For by successive application of 2.4, a_1 is co-prime to $[a_2,\dots,a_n].$ Hence $(c,[a_1,\dots,a_n]) = [(c,a_1),(c,[a_2,\dots,a_n])] = [(c,a_1),$ $(c,a_2),(c,[a_3,\dots,a_n])] = \cdots = [(c,a_1),(c,a_2),\dots,(c,a_n)].$

2.5 gives the following fundamental property of direct products of sublattices of an ideal lattice with unit:

LEMMA 2.1. *Let* $\mathfrak{A}$ *be the sublattice generated by the sublattices* $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ *each of which contains* u. *Then* $\mathfrak{A}$ *is the direct product of* $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ *if and only if* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ *are co-prime in pairs.*

PROOF. From the definitions of § 2 ch. I it follows directly that $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ are co-prime in pairs if $\mathfrak{A}_n$ is the direct product of $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$. Let now $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ be co-prime in pairs and let $\mathcal{L}$ denote the set of cross-cuts $[a_1, \ldots, a_n]$ where $a_i \in \mathfrak{A}_i$. We have clearly $[[a_1, \ldots, a_n], [a_1', \ldots, a_n']] = [[a_1, a_1'], \ldots, [a_n, a_n']]$. Furthermore $([a_1, \ldots, a_n], [a_1', \ldots, a_n']) = [(a_1, [a_1', \ldots, a_n']), \ldots, (a_n, [a_1', \ldots, a_n'])]$ $= [(a_1, a_1'), \ldots, (a_n, a_n')]$ by 2.5. Hence $\mathcal{L}$ is a sublattice and is thus equal to $\mathfrak{A}$. If $[a_1, \ldots, a_n] = [a_1', \ldots, a_n']$ then $a_i = (a_i, [a_1', \ldots, a_n']) = [(a_i, a_1'), \ldots, (a_i, a_n')] = (a_i, a_i')$ whence $a_i \supset a_i'$. Similarly $a_i' \supset a_i$ and hence $a_i = a_i'$. This completes the proof.

If the sublattices $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ have minimal elements, the conditions of lemma 2.1 may be simplified.

COROLLARY. *If the sublattices* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ *of lemma* 2.1 *have minimal elements* $m_1, \ldots, m_n$, *then* $\mathfrak{A}$ *is the direct product of* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ *if and only if* $m_1, \ldots, m_n$ *are co-prime in pairs.*

From lemma 2.1 we have immediately

LEMMA 2.2. *Any finite set of divisor-free elements generates a finite Boolean algebra.*

PROOF. A finite Boolean algebra of order 2^n is the direct product of n chains $\{u, a_1\}, \{u, a_2\}, \ldots, \{u, a_n\}$ of length 1. But if $a_1, \ldots, a_n$ are divisor-free elements, $\{u, a_1\}, \ldots, \{u, a_n\}$

obviously satisfy the conditions of lemma 2.1.

If there are only a finite number of divisor-free elements in we may speak of *the* Boolean algebra generated by the divisor-free elements. This is certainly the case when the descending chain condition holds in for we have

LEMMA 2.3. *If the descending chain condition holds in* γ , *then there are only a finite number of divisor-free elements.*

PROOF. Let $p_1, p_2, \cdots, p_n, \cdots$ be an infinite sequence of distinct divisor-free elements and form the descending chain $a_1 \supset a_2 \supset a_3 \supset \cdots$ where $a_i = [p_1, p_2, \ldots, p_i]$. If $a_i = a_{i+1}$ then $[p_1, \cdots, p_i] = [p_i, \cdots, p_{i+1}]$ and hence $p_{i+1} = (p_{i+1}, [p_1, \cdots, p_i]) = [(p_{i+1}, p_i), \cdots, (p_{i+1}, p_i)] = u$ which is impossible. Thus $a_1 \supset a_2 \supset a_3 \supset \cdots$ is an infinite descending chain.

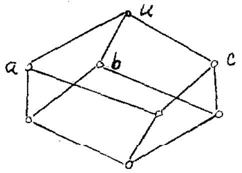
3. *Lattice structure in the vicinity of the unit element.* We turn now to the study of the structure of a residuated lattice in the vicinity of the unit element and prove first the fundamental

THEOREM 3.1. *Let* γ *be a residuated lattice with unit having only a finite number of divisor-free elements* $p_1, \cdots, p_n$. *Moreover let* $\mathcal{L}$ *be the direct product of chain lattices* $\mathcal{L}_1, \cdots, \mathcal{L}_n$ *where* $\mathcal{L}_i$ *is the chain* $u \supset p_i \supset a_i \supset \cdots \supset m_i$. *Then if* $m_k > b$ *and* b *does not belong to* $\mathcal{L}$, *the sublattice generated by the elements of* $\mathcal{L}$ *and the element* b , *is the direct product of the chain lattices* $\mathcal{L}_1, \cdots, \mathcal{L}_k', \cdots, \mathcal{L}_n$, *where* $\mathcal{L}_k'$ *is the chain lattice* $u \supset p_k \supset a_k \supset \cdots \supset m_k \supset b$.

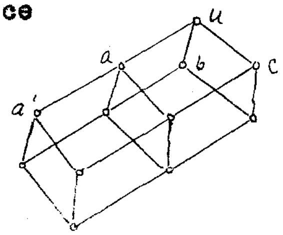
PROOF. In view of the corollary to lemma 2.1, it is sufficient to show that $(b, m_i) = u \quad i \neq k$. If $(b, m_i) \neq k$, there exists a divisor-free element p such that $p \supset (b, m_i)$. Since $p \supset m_i$, we have $p = p_i$. Now $m_K \supset [m_K, p_i] \supset b$ since $p \supset b$. But $m_K \neq [m_K, p_i]$ since otherwise $p_i \supset m_K$ while $(p_i, m_K) = u$. Hence $b = [m_K, p_i]$ and b is contained in $\mathcal{L}$ which is contrary to assumption. Thus $(b, m_i) = u \quad i \neq K$.

This theorem enables us to construct certain characteristic sublattices with very simple properties. For let $\mathcal{L}_0$ be the Boolean algebra generated by the divisor-free elements of $\mathcal{N}$. If a divisor-free element p of $\mathcal{L}_0$ covers an element a_1 not contained in $\mathcal{L}_0$, then $\mathcal{L}_0$ and a_1 generate a sublattice $\mathcal{L}_1$ which is a direct product of chain lattices. If a_1 covers a_2 and a_2 does not belong to $\mathcal{L}_1$, then $\mathcal{L}_1$ and a_2 generate a sublattice $\mathcal{L}_2$ which is again a direct product of chain lattices. We may continue in this manner as long as we obtain elements a_i not contained in $\mathcal{L}_{i-1}$. Having obtained a sublattice $\mathcal{L}_K$ in this manner it may be further extended by building chains from other divisor-free elements. Thus if we call lattices which are direct products of chain lattices, <u>arithmetical</u> (Ward [41]) we see that the structure of a residuated lattice in the vicinity of the unit element is characterized to a large extent in terms of arithmetical lattices.

This principle is very useful in constructing examples of residuated lattices. For example, suppose we wish to construct a residuated lattice containing three divisor-free elements. We start then with the Boolean algebra



Now if we wish to add an element a' covered by a by theorem 3.1 we have immediately the sublattice



The condition of theorem 3.1 that each divisor-free element be a member of one of the chain lattices is essential for the truth of the theorem as may be seen by simple examples. However in general a residuated lattice will have an infinite number of divisor-free elements and theorem 3.1 will no longer apply. It may be generalized as follows:

THEOREM 3.2. *Let* $\mathcal{L}$ *be the direct product of chain lattices* $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$ *of a residuated lattice* $\mathcal{S}$ *and let* $\mathfrak{L}$ *be the lattice generated by* $\mathcal{L}$ *and the set of divisor-free elements* p *which divide at least one element of* $\mathcal{L}$. *Furthermore let* $m_i > b$. *Then either* b *lies in* $\mathcal{L}$ *or the lattice generated by* $\mathcal{L}$ *and* b *is the direct product of the chain lattices* $\mathcal{L}_1, \ldots, \mathcal{L}_i', \ldots, \mathcal{L}_n$ *where* $\mathcal{L}_i' = \{\mathcal{L}_i, b\}$.

PROOF. If $(b, m_k] \neq u$, $k \neq i$, there exists a divisor-free element p such that $p \supset (b, m_k)$. Now $m_i \supset [m_i, p] \supset b$ and $m_i \neq [m_i, p]$ since otherwise $p \supset m_i$ while $(p, m_i) = u$. Hence $b = [m_i, p]$ and $b \in \mathfrak{L}$. Hence if $b \notin \mathfrak{L}$, $(b, m_k) = u$, $k \neq i$ and the theorem follows by lemma 2.1.

The structure of the lattice $\mathfrak{L}$ of theorem 3.2 is comparatively simple. We shall study its properties in terms of the notion of *semi-arithmetical* lattices introduced by Morgan Ward (Ward [41])

DEFINITION 3.1. A distributive lattice $\mathcal{D}$ is said to be semi-arithmetical if the indecomposable elements divisible by a given divisor-free element form a chain lattice.

A semi-arithmetical lattice in which the ascending chain condition holds may be characterised as follows (Ward [41]):

LEMMA 3.1. *A distributive lattice* $\mathcal{D}$ *in which the ascending chain condition holds is semi-arithmetical if and only if the indecomposables occurring in the reduced representation of an element as a cross-cut of* __indecomposables are co-prime in pairs.__

From definition 3.1 it follows trivially that an arithmetical lattice is semi-arithmetical.

We shall show now that the lattice $\mathcal{L}_a$ of theorem 3.2 is semi-arithmetical and to that end prove the

THEOREM 3.3. __Let__ $\mathcal{L}$ __be a semi-arithmetical sublattice of a residuated lattice__ γ __and let__ $\mathcal{L}$ __contain the unit element__ u __. Then if__ p __is a divisor-free element of__ γ __, the sublattice__ $\mathcal{L}'$ __generated by__ p __and the sublattice__ $\mathcal{L}$ __is semi-arithmetical.__

PROOF. If p is contained in $\mathcal{L}$ the theorem is trivial and we may thus assume that $p \notin \mathcal{L}$. Now let U be the set of all elements of the form a or $[p,a]$ where $a \in \mathcal{L}$. U is clearly closed with respect to cross-cut. We show that U is also closed with respect to union. Let x and y be two members of the set U . If both x and y are contained in $\mathcal{L}$, (x,y) is obviously in U . Let $x = [p,x_1]$, $p \not\supset x_1$ and $y \in \mathcal{L}$. Let $x_1 = [q_1, \dots, q_s]$ where the q_i are indecomposables and $(q_i, q_j) = u \quad i \neq j$. Then since $p \not\supset x_1$, $(p, q_i) = u \quad (i = 1, \dots, s)$ Hence $(x,y) = (y, [p, q_1, \dots, q_s])$ $= [(y,p), (y,q_1), \dots, (y,q_s)]$ by 2.5. But (y,p) is either p or u and hence (x,y) is contained in U . If $x = [p,x_1]$, $p \not\supset x_1$ and $y = [p,y_1]$, $p \not\supset y_1$, then $(x,y) = ([p,q_1, \dots, q_r], [p,q_1', \dots, q_s'])$ $= [p, (q_1,p), \dots, (q_r,p), \dots, (q_s',p), (q_1,q_1'), \dots, (q_r, q_s')] = [p,a]$ where $a \in \mathcal{L}$. Hence U is identical with $\mathcal{L}'$.

Now let a, b, c be contained in U . Then in exactly the same manner as above we find that $(a, [b,c]) = [(a,b), (a,c)]$. For example, if $b = [p,b_1]$, $p \not\supset b_1$ and $c \in \mathcal{L}$, then $(a,[b,c]) =$ $(a, [p, q_1, \dots, q_r, q_1', \dots, q_e'])= [(a,p), (a,q_1), \dots, (a,q_r), (a,q_1'), \dots, (a,q_s')]$ $= [(a,b), (a,c)]$ if $p \not\supset c$; and if $p \supset c$, then $(a, [b,c]) =$

$(a, [q_1, \dots, q_r, q_1', \dots, q_s']) = [(a, q_1), \dots, (a, q_r), (a, q_1'), \dots, (a, q_s')] =$
$[(a, q_1), \dots, (a, q_r), (a, c)] = [(a, p), (a, q_1), \dots, (a, q_r), (a, c)] =$
$[(a, b), (a, c)]$. Hence $\mathcal{L}'$ is distributive.

Finally let $x \in \mathcal{L}'$, then either $x \in \mathcal{L}$ or $x = [p, x_1]$ where $p \not\supset x_1$. If $x \in \mathcal{L}$, then $x = [q_1, \dots, q_r]$ where the q_i are indecomposable and $(q_i, q_j) = u$ $i \neq j$. If $x = [p, x_1]$ then $x = [p, q_1, \dots, q_r]$ where $p, q_1, \dots, q_r$ are indecomposable and $(q_i, q_j) = u$ $i \neq j$, $(p, q_i) = u$ $(i = 1, \dots, r)$. Thus $\mathcal{L}'$ is semi-arithmetical by lemma 3.1 and the proof is complete.

Now since $\mathcal{S}$ is obtained from an arithmetical lattice $\mathcal{L}$ by a successive adjunction of a finite number of divisor-free elements and since at each stage a semi-arithmetical sublattice is obtained, $\mathcal{S}$ itself is semi-arithmetical. We have thus proved

THEOREM 3.4. <u>The lattice</u> $\mathcal{S}$ <u>of theorem</u> 3.2 <u>is a semi-arithmetical sublattice of</u> $\mathcal{H}$.

In forming the sublattice $\mathcal{S}$ from the arithmetical lattice only divisor-free elements which are divisors of some element of are considered. If we adjoin a divisor-free element which does not divide any of the elements of $\mathcal{L}$, the results are even simpler; for we have

THEOREM 3.5. <u>Let</u> $\mathcal{L}$ <u>be a direct product of the chain lattices</u> $\mathcal{L}_1, \dots, \mathcal{L}_n$ <u>and let</u> p <u>denote a divisor-free element not contained in</u> $\mathcal{L}$. <u>Then if</u> p <u>does not divide any of the elements of the sublattice generated by</u> p <u>and</u> $\mathcal{L}$ <u>is the direct product</u> $\mathcal{L}'$ <u>of the chain</u> $\{u, p\}$ <u>and the chain lattices of</u> $\mathcal{L}$. <u>Furthermore if</u> $\mathcal{L}$ <u>is dense in</u> $\mathcal{H}$, <u>then</u> $\mathcal{L}'$ <u>is dense in</u> $\mathcal{H}$.

PROOF. Since p does not divide a_i if $a_i \in \mathcal{L}_i$, $(a_i, p) = u$. Hence the first part of the theorem follows. Let now $X \supset [P, a_1, \ldots, a_n]$. Then $X = [(X,P), (X,a_1), \ldots, (X,a_n)]$. Now (X,P) is clearly in $\mathcal{L}$ and (X,a_i) is in $\mathcal{L}$ by hypothesis. Hence $X \in \mathcal{L}'$

We conclude this section with

THEOREM 3.6. Let $\mathcal{L}$ be the direct product of the chain lattices $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$ of a residuated lattice $\mathcal{H}$ and let $m_i > b$ where b is indecomposable. Then $\mathcal{L}$ and b generate a sublattice $\mathcal{L}'$ which is the direct product of the chain lattices $\mathcal{L}_1, \ldots, \{\mathcal{L}_i, b\}, \ldots, \mathcal{L}_n$. Furthermore if $\mathcal{L}$ is dense in $\mathcal{H}$, then $\mathcal{L}'$ is dense in $\mathcal{H}$.

PROOF. The first part follows directly from theorem 5.2. Let now $X \supset [m_1, m_2, \ldots, b, \ldots m_n]$. Then $X = [(X,m_1) (X,m_2), \ldots, (X,b), \ldots, (X,m_n)]$ Since $\mathcal{L}$ is dense by hypothesis, $(X,m_1), \ldots, (X,m_n)$ are contained in $\mathcal{L}$. Now either $(X,b) = b$ in which case $X \in \mathcal{L}'$ or $(X,b) \supset m_i$ since b is indecomposable. But then $(X,b) \in \mathcal{L}$ and X is contained in $\mathcal{L}'$.

4. Arithmetical properties of ideal lattices. Let $\mathcal{H}$ be an ideal lattice in which the ascending chain condition holds.

DEFINITION 4.1. An element $p \in \mathcal{H}$ is said to be a prime if $p \supset ab$ and $p \not\supset a$ implies $p \supset b$.

DEFINITION 4.2. An element $q \in \mathcal{H}$ is said to be right primary if $q \supset ab$ and $q \not\supset a$, implies $q \supset b^s$ for some whole number s.

In the theory of commutative residuated lattices a residuated lattice in which the ascending chain condition holds is said to be a Noether lattice (Ward-Dilworth [2]) if every irreducible is primary. It is then shown that every element of a Noether lattice may be represented as a simple* cross-cut of a finite number of primaries each of which is

* A cross-cut representation is said to be simple if omitting any one of the terms changes the representation.

associated with a different prime. The primes themselves and the total number of primaries are uniquely determined by the element.

This result also holds for the non-commutative case although there are certain complications due to the non-commutativety of the multiplication. We shall show how these complications may be avoided.

Let $\mathcal{N}$ be a non-commutative Nowther lattice, i.e. every irreducible is right primary. If a and b are elements of $\mathcal{N}$, the product ab then has the form $ab = [q_1, \dots, q_r]$ where the q_i are right primary. Let $q_i \supset a \ (i = 1, \dots, l)$, $q_i \not\supset a \ (i = l+1, \dots, r)$. Then since $q_i \supset ab$ we have $q_i \supset b^{s_i} \ (i = l+1, \dots, r)$. If we then set $s = \max(s_{l+1}, \dots s_r)$ we have

4.1. $$ab \supset [a, b^s] \supset b^s a .$$

Let q be right primary and consider the union p of all elements x such that $q \supset x^s$ for some whole number s. Then $q \supset p^\sigma$ for some whole number σ by the ascending chain condition. Furthermore p is a prime. For if $p \supset ab$, then $q \supset p^\sigma \supset (ab)^\nu \supset a^\tau b^\sigma$ by 6.1 If $q \supset a^\tau$, then $p \supset a$. If $q \not\supset a^\tau$, then $q \supset b^{\sigma s}$ and $p \supset b$ Hence either $p \supset a$ or $p \supset b$. This prime is clearly unique and is called the prime element associated with the right primary q. We have moreover

LEMMA 4.1. The cross-cut of two right primaries associated with the same prime p is also a right primary associated with p.

PROOF. Let $[q, q'] \supset ab$, $[q, q'] \not\supset a$. Then either q or q' say q, does not divide a and hence $q \supset b^s$. But then $p \supset b$ and hence $q' \supset b^t$. Hence $[q, q'] \supset b^{s'}$ where $s' = \max(s, t)$ $[q, q']$ obviously is associated with p.

LEMMA 4.2. Let q and q' be right primaries associated with p and p' respectively. Then if $p \not\supset p'$, $q \cdot q'^{-1} = q$.

PROOF. $q \supset (q \cdot q'^{-1})\, q'$. Hence either $q = q \cdot q'^{-1}$ or $q \supset q'^{s}$. But if $q \supset q'^{s}$, then $p \supset p'^{t}$ and hence $p \supset p'$ contrary to hypothesis.

Note that lemma 4.2 holds only for the right residual. If we were considering left primaries, the left residual would replace the right residual.

The proof from this point on is exactly analogous to the proof in classical ideal theory and will be omitted. We thus obtain

THEOREM 4.1. *Let* γ *be a non-commutative Noether lattice. Then every element of* γ *may be represented as a simple cross-cut of a finite number of right primaries. The primes and the tetal number of right primaries are uniquely determined by the element.*

The following theorem proved in Ward-Dilworth [a] for the commutative case holds also for non-commutative residuated lattices.

THEOREM 4.2. *The following two conditions are sufficient that* γ *be a Noether lattice:*

(i) γ *is modular*

(ii) $ab \supset [a, b^{s}]$ *for some* s.

PROOF. Let a be irreducible and let $a \supset bc$, $a \not\supset b$. Then $a \supset (ac, bc)$ $= (a,b)c \supset [(a,b), c^{s}]$ by (ii). Hence $(a,b) \supset a \supset [(a,b), c^{s}]$ and $a = [(a,b), (a, c^{s})]$ by (i). But $(a,b) \neq a$ and since a is irreducible $a = (a, c^{s})$, $a \supset c^{s}$. Whence a is right primary.

The distinction between left and right primaries may be removed by weakening the condition of definition 4.2. We adopt the name *semi-primaries* for these new elements.

DEFINITION 4.3. An element $a \in \gamma$ is said to be semi-primary if $a \supset b \cdot c$ and $a \not\supset b^{s}$ any s implies $a \supset c^{t}$ for some whole number t .

Let γ be an ideal lattice in which every element may be represented as a cross-cut of a finite number of semi-primaries. Moreover let x and y be any two elements of $\mathfrak{S}$. Then $xy = [a_1, \dots, a_r]$ where the a_i are semi-primary. Let $a_i \supset x^{s_i}$ for $i = 1, \dots, e$ and $a_i \supset y^{t_i}$ $i = e+1, \dots, r$. Then $xy \supset [x^s, y^t]$ where $s = \max(s_1, \dots, s_e)$ and $t = \max(t_{e+1}, \dots, t_r)$. We have proved

THEOREM 4.3. <u>If every element of a residuated lattice $\mathfrak{S}$ is expressible as a cross-cut of a finite number of semi-primaries, then for every x and y in $\mathfrak{S}$, there exist whole numbers s and t such that</u>

4.2. $$xy \supset [x^s, y^t]$$

If 4.2 holds in a residuated lattice, the semi-primary elements may be simply characterized as follows:

THEOREM 4.4. <u>Let $\mathfrak{S}$ be a residuated lattice in which 4.2 holds. Then an element a is semi-primary if and only if a prime p exists such that $p \supset a \supset p^s$ for some whole number s.</u>

PROOF. Let a be semi-primary and let p denote the union of all elements x such that $a \supset x^r$ for some r. Then $a \supset p^\sigma$ for some σ. Now let $p \supset xy$. Then $a \supset (xy)^\sigma \supset x^m y^n$ for some integers m and n by 4.2. Hence $a \supset x^s$ for some s or $a \supset y^t$ for some t. Hence either $p \supset x$ or $p \supset y$. Clearly $p \supset a \supset p^s$ for some s.

Conversely let $p \supset a \supset p^s$ and suppose that $a \supset bc$. Then $p \supset bc$ and hence either $p \supset a$ or $p \supset c$. Hence either $q \supset b^s$ or $q \supset c^s$.

The converse to theorem 4.3 does not hold in general. However under the assumption of the distributive law we have

THEOREM 4.5. <u>The following two conditions are sufficient that every element of a residuated lattice $\mathfrak{S}$ satisfying the ascending chain condition be expressible as a cross-cut of a finite number of semi-</u>

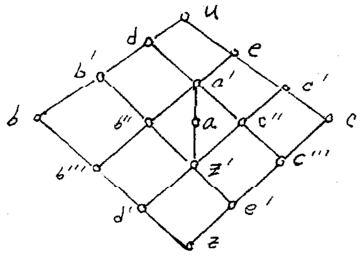
primaries.

(i) γ' is distributive.

(ii) $xy \supset [x^s, y^t]$ for suitable s and t.

PROOF. Every element of γ' is clearly expressible as a cross-cut of a finite number of indecomposables. Hence it is sufficient to show that every indecomposable is semi-primary. Let a be indecomposable and let $a \supset bc$, $a \not\supset b^s$ any s. Then $a \supset [b^s, c^t]$ by (ii) Hence $a = [(a, b^s), (a, c^t)]$ by (i). But $(a, b^s) \neq a$. Hence since is indecomposable $a = (a, c^t)$ and $a \supset c^t$.

The distributive condition is essential in theorem 4.5 as the following example shows:



$\mathcal{L}$

Let $\mathcal{L}_a$ denote the sublattice $\{a', b'', a, c'', b''', z', c''', d', e', z\}$. $\mathcal{L}_b$, the sublattice $\{d, b', b\}$, and $\mathcal{L}_c$ the sublattice $\{e, c', c\}$. We define a multiplication over $\mathcal{L}$ as follows: $u^2 = u$, $ux = b$ if $x \in \mathcal{L}_b$, $ux = c$ if $x \in \mathcal{L}_c$, $ux = z$ if $x \in \mathcal{L}_a$. The product of any two elements in $\mathcal{L}_b$ is b. The product of any two elements in $\mathcal{L}_c$ is c. The product of any element of $\mathcal{L}$ with an element of $\mathcal{L}_a$ is z. The product of an element of $\mathcal{L}_b$ with an element of $\mathcal{L}_c$ is z. It is readily verified that the multiplication so defined satisfies P00 - P4', P6 and is also commutative. $\mathcal{L}$ is clearly not distributive. It can also be verified that $xy \supset [x^s, y^t]$ for suitable s and t. However it is not true that $xy \supset [x, y^s]$ for some s, since $dc \not\supset [d, c^s]$. Furthermore a is indecomposable but *not* semi-primary since $a \supset bc$ but $a \not\supset b^s$ any s and $a \supset c^\sigma$ any σ.

5. *Ideal lattices with unit.* We turn now to the study of the properties of divisor-free elements in an ideal lattice with unit. We prove first the

LEMMA 5.1. *Let* f *be a divisor-free element of* γ *and let* a *be any element not divisible by* f. *Then one and only one of the following formulas hold:*

(i) $fa \supset af$

(ii) $fa = (fa)\cdot f^{-1}$

PROOF. We have $(fa\cdot f^{-1})^{-1}\cdot fa \supset f$ by $R5$. Hence either $(fa\cdot f^{-1})^{-1}\cdot fa = a$ or $(fa\cdot f^{-1})^{-1}\cdot fa = f$. In the first case $fa \supset fa\cdot f^{-1}$. But $fa\cdot f^{-1} \supset fa$ by $R9$. Hence $fa = fa\cdot f^{-1}$. If $(fa\cdot f^{-1})^{-1}\cdot fa = f$, then $f = f\cdot a^{-1} = ((fa\cdot f^{-1})^{-1}\cdot fa)\cdot a^{-1} = (fa\cdot f^{-1})^{-1}(fa\cdot a^{-1}) \supset (fa\cdot f^{-1})^{-1}\cdot f$. But $(fa\cdot f^{-1})^{-1}\cdot f \supset f$. Hence $(fa\cdot f^{-1})^{-1}\cdot f = f$. But then $f^{-1}\cdot(fa\cdot f^{-1}) = fa\cdot f^{-1}$ or $(f^{-1}\cdot fa)\cdot f^{-1} = fa\cdot f^{-1}$. Then $fa\cdot f^{-1} \supset a\cdot f^{-1} \supset a$ Hence $fa \supset (fa\cdot f^{-1})f \supset af$.

If both (i) and (ii) hold, then $fa = fa\cdot f^{-1} \supset af\cdot f^{-1} \supset a$ But then $f = (f, fa) \supset (f, a) = a$ contrary to the assumption that f is a divisor-free element.

We clearly have a similar result for left residuals.

LEMMA 5.2. *Let* f *be a divisor-free element of a residuated lattice in which* 4.2 *holds. Then* f *commutes with every element which it does not divide.*

PROOF. Let $a \in \gamma$ such that $f \not\supset a$. Then by lemma 5.1 either $fa \supset af$ or $fa = fa\cdot f^{-1}$. If $fa = fa\cdot f^{-1}$, then $fa \supset (a^s f^t)\cdot f^{-1}$

$\supset a^s f^{t-1}$ by 4.2. But then $fa \supset (fa) \cdot f^{-1} \supset (a^s f^{t-1}) \cdot f^{-1} \supset a^s f^{t-2}$ continuing in this manner we finally get $fa \supset a^s$. But then $f = (f, fa) \supset (f, a^s) = u$ since $f \not\supset a^s$. hence $f = u$ which is contrary to our assumption that f is a divisor-free element. We thus have $fa \supset af$. In a similar manner using left residuals we get $af \supset fa$. Hence $af = fa$.

As a corollary to lemma 5.2 the divisor-free elements in a residuated lattice for which 4.2 holds always commute. In particular we have from theorem 4.3

LEMMA 5.3. <u>If in a residuated lattice every element is expressible as a cross-cut of semi-primaries, then the divisor-free elements commute</u>.

Let $\mathcal{L}$ be an arbitrary residuated lattice in which the ascending chain condition holds and denote by $\mathcal{L}'$ the set of all elements x which divide a finite product of divisor-free elements. $\mathcal{L}'$ is clearly closed under union, cross-cut, multiplication and residuation and hence is a residuated sublattice of $\mathcal{L}$. We have then

LEMMA 5.4. <u>Every prime in $\mathcal{L}'$ is divisor-free</u>.

PROOF. Let p be a prime in $\mathcal{L}'$. Then by the definition of $\mathcal{L}'$, $p \supset f_1 f_2 \cdots f_r$ where $f_1, f_2, \ldots, f_r$ are divisor-free elements of $\mathcal{L}$. Hence $p = f_i$ for some i .

LEMMA 5.5. <u>Every element of $\mathcal{L}'$ divides a finite product of its divisor-free divisors</u>.

This lemma follows immediately from the following lemma due to Krull (Krull [2]).

LEMMA 5.6. <u>Let $\mathcal{L}$ be a non-commutative residuated lattice in which the ascending chain condition holds. Then each element $a \in \mathcal{L}$ has only a finite number of minimal prime divisors $P_1, \ldots, P_n$ and</u>

divides a power of $p_1 \cdots p_n$ *.

A further consequence of lemma 5.6 is the result that $\mathcal{L}'$ is the maximal residuated sublattice all of whose prime elements are divisor-free.

In certain cases $\mathcal{L}'$ is simply the Boolean algebra $\mathcal{B}$ generated by the divisor-free elements. For example we have

THEOREM 5.7. *Let* $\mathcal{L}$ *be a residuated lattice with only a finite number of divisor-free elements all of which commute among themselves. If the only elements covered by the divisor-free elements are elements of the Boolean algebra* $\mathcal{B}$ *generated by them, then* $\mathcal{L}' = \mathcal{B}$.

PROOF. Under the hypotheses of the theorem $f^2 \subset [f, f']$ or $f^2 = f$ But if $[f, f'] \supset f^2$, then $f' \supset f$ which is impossible. Hence $f^2 = f$. But then $[f_1, f_2, \dots, f_n] = f_1 f_2 \cdots f_n$ and $(f_1 \cdots f_n)^2 = f_1 f_2 \cdots f_n$.

* Krull states this lemma for the more general dase where the ascending chain condition is assumed only for prime elements while a residual chain condition holds for all elements. However his proof seems to be in error as he uses the following rule: If $a \supset a_1' a_2'$, then $a \supset a_1 a_2$ where $a_1 = a \cdot a_2'^{-1}$ and $a_2 = a_1'^{-1} \cdot a$. This rule is in general not correct as the following example shows: Let $\mathcal{L}$ be the lattice defined by the covering relations $u > a > b > c > z$, $b > d > z$. The multiplication is defined by $ux = xu = x$ all $x \in \mathcal{L}$. $a^2 = a$ all other products are equal to z . Then $z \cdot c^{-1} = a$, $d^{-1} z = a$ and $z \supset cd$. However $z \not\supset (z \cdot c^{-1})(d^{-1} z) = a^2 = a$.

The lemma is readily seen to be correct under the assumption of the ascending chain condition since we may take $a_1 = (a, a_1')$ and $a_2 = (a, a_2')$ and the rule stated above holds.

If the divisor-free elements do not commute, the theorem does not hold in general. Consider the lattice $\mathcal{L}$ defined by the covering relations $u > b > c > z$, $u > a > c$ The multiplication is given by $ux = xu = x$ all $x \in \mathcal{L}$, $ab = c$, $ba = z$, $ac = ca = bc = cb = c^2 = z$, $a^2 = a$, $b^2 = b$, $zx = z$ all $x \in \mathcal{L}$ Then $\gamma' = \mathcal{L}$, while $\mathcal{G}$ is the sublattice $\{u, a, b, c\}$.

Applying theorem 5.7 to hypercomplex systems we obtain

THEOREM 5.8. <u>A hypercomplex system in which the prime two-sided ideals are commutative is a direct sum of simple two-sided ideals if and only if each irreducible two-sided ideal which is not a prime has at least two prime ideal divisors</u>.

We conclude this section by giving a variation of a theorem due to Krull*.

THEOREM 5.9. <u>Each element of γ' is expressible as a cross-cut of finite number of semi-primaries if and only if the divisor-free elements commute</u>.

PROOF. The second part follows from lemma 5.3. To prove the first part let $a = [a_1, \dots, a_r]$ be the decomposition of a into co-prime indecomposable elements. Then $a_i \supset p_1^{n_1} \cdots p_r^{n_r} = [p_1^{n_1}, \dots, p_r^{n_r}]$ or $a_i = [(a_i, p_1^{n_1}), \dots, (a_i, p_r^{n_r})]$ whence $a_i = (a_i, p_j^{n_j})$ for some j. We have then $p_j \supset a_i \supset p_j^{n_j}$. Let $a_i \supset bc$, then $p_j \supset bc$ and hence either $p_j \supset b$ or $p_j \supset c$. Hence either $a_i \supset b^{n_j}$ or $a_i \supset c^{n_j}$. Thus if the divisor-free elements of γ' commute, each element of γ' may be uniquely represented as a cross-cut of co-prime semi-primary elements.

6. Archimedean residuated lattices. Throughout this section unless the contrary is explicitly stated it will be assumed that γ is an ideal lattice in which both the ascending and descending chain conditions hold. The unit element of γ need not be the unit of multiplication.

DEFINITION 6.1. An element a of γ is said to be nilpotent if $a^{\sigma}=0$ for some whole number σ.

LEMMA 6.1. The union m of all nilpotent elements of γ is nilpotent. m is called the radical of γ.

PROOF. If $a_1^{\sigma_1}=0$ and $a_2^{\sigma_2}=0$, then $(a_1, a_2)^{\sigma}=0$ where $\sigma=\sigma_1+\sigma_2-1$ The result follows from the ascending chain condition.

DEFINITION 6.2. An element s of γ is said to be simple if $s>z$ where z is the null element of γ.

LEMMA 6.2. A necessary and sufficient condition that the radical be the null element is that each simple element be idempotent.

PROOF. Let $m=z$. If s is a simple element, since $s \supset s^2$, either $s=s^2$ or $s^2=z$. But if $s^2=z$, then $z \supset m \supset s$ contrary to definition 6.2. Suppose now that each simple element is idempotent and let $m \neq z$. Then $m \supset s$ where s is simple. Whence $z=m^{\sigma} \supset s^{\sigma}=s$ which contradicts the definition of s. Hence $m=z$.

DEFINITION 6.3. If the radical is the null element, γ is said to be semi-simple.

LEMMA 6.3. Let γ be semi-simple and s be any simple element of Then

$$a \supset s \Longleftrightarrow as=sa=s$$

$$a \not\supset s \Longleftrightarrow as=sa=z,$$

PROOF. Let $a \supset s$. Then $as \supset s^2 = s$ and hence $as = s$ Similarly $sa = s$. If $a \not\supset s$, then $[a, s] = z$ and hence $as = sa - z$

The position of the radical in the lattice may have important bearing on the arithmetical properties of the lattice. For example, we have the following theorem:

THEOREM 6.1. *Let* $\mathcal{L}$ *be an ar~~c~~himedean residuated lattice whose divisor-free elements generate a Boolean algebra with null element* m. *Then the divisor-free elements are the only primes of* $\mathcal{L}$.

PROOF. Since $\mathcal{L}$ is archimedean there are only a finite number of divisor-free elements. Let p be a prime of $\mathcal{L}$. Then $p \supset m^\sigma = z$ and hence $p \supset m$. But $m = [f_1, \cdots, f_r]$ where $f_1, \ldots, f_r$ are the divisor-free elements of $\mathcal{L}$. Hence $p \supset [f_1, \cdots, f_r]$ and hence $p = f_i$ for some i.

The conclusion of theorem 6.1 may be stated in the form $\mathcal{L} = \mathcal{L}'$.

Let $\mathcal{L}_m$ denote the sublattice of all elements x such $x \supset m$. The study of the structure of $\mathcal{L}_m$ may be reduced to the study of the structure of semi-simple lattices. For since $\mathcal{L}_m$ is dense in $\mathcal{L}$ it is closed with respect to residuation and hence has a multiplication (§ 3 ch. I). We call this multiplication, the multiplication *in* $\mathcal{L}_m$ and denote it by $a \cdot b$.

THEOREM 6.2. *Let* $a, b \in \mathcal{L}_m$. *If* $ab \in \mathcal{L}_m$, *then* $ab = a \cdot b$

PROOF. $a \cdot b$ is defined by (i) $(a \cdot b) \cdot b^{-1} \supset a$ (ii) $x \cdot b^{-1} \supset a$, $x \in \mathcal{L}_m \longrightarrow x \supset a \cdot b$. Similarly ab is defined by (i)' $(ab) \cdot b^{-1} \supset a$. (ii)' $x \cdot b^{-1} \supset a$, $x \in \mathcal{L} \longrightarrow x \supset ab$ Hence if $ab \in \mathcal{L}_m$, then $ab \supset a \cdot b$ by (i)', (ii). On the other hand by (i), (ii)' $a \cdot b \supset ab$. Hence $a \cdot b = ab$

In general we have

LEMMA 6.4. $a \cdot b \supset ab$.

Let now p be a prime element of $\mathcal{L}$. Then $p \supset m^{\sigma} = z$ and hence $p \supset m$. Thus $p \in \mathcal{L}_m$. Now let $p \supset a \cdot b$. Then $p \supset ab$ by lemma 6.4. Hence either $p \supset a$ or $p \supset b$. We thus have

THEOREM 6.3. If p is a prime element of $\mathcal{L}$, then $p \in \mathcal{L}_m$ and p is a prime in $\mathcal{L}_m$ with respect to the multiplication in $\mathcal{L}_m$.

THEOREM 6.4. $\mathcal{L}_m$ is semi-simple.

PROOF. Let s be a simple element of $\mathcal{L}_m$. Then $s > m$. Now $s \supset s\,s$ Hence $s = s \cdot s$ or $s \cdot s = m$. But if $s \cdot s = m$, $m \supset s^2$ by lemma 6.4 and hence $s^{2\sigma} = 0$. This contradicts the definition of m Hence each simple element is idempotent and by lemma 6.1 $\mathcal{L}_m$ is semi-simple

The most important application of archimedean residuated lattices is in the theory of hypercomplex systems. More generally, let $\mathcal{L}$ be the set of two-sided ideals of a non-commutative ring R in which the ascending and descending chain conditions hold for left ideals. Then m is the radical of R. Now the quotient ring R/m is isomorphic to $\mathcal{L}_m$ and hence is semi-simple by theorem 6.4. However from a well known structure theorem, a semi-simple ring is a direct sum of simple two-sided ideals. Its lattice of two-sided ideals is thus a Boolean algebra and theorem 6.1 gives

THEOREM 6.5. The only prime two-sided ideals in a hypercomplex system are the divisor-free ideals.

7. Semi-simple lattices. In this section we shall be particularly interested in the sublattices generated by the simple elements of a semi-simple lattice $\mathcal{L}$.

LEMMA 7.1. There are only a finite number of simple elements in a semi-simple lattice $\mathcal{L}$.

PROOF. Let $s_1, s_2, s_3, \dots$ be an infinite sequence of simple elements. Consider the chain $a_1 \subset a_2 \subset a_3 \subset \cdots$ where $a_i = (s_1, s_2, \dots, s_i)$. The members of this chain are distinct. For suppose that $a_i = a_{i+1}$, then $(s_1, \dots, s_i) = (s_1, s_2, \dots, s_{i+1})$ Hence $s_{i+1} = s_{i+1}^2 = (s_1 s_{i+1}, s_2 s_{i+1}, \dots s_{i+1}^2) = (s_1, \dots, s_{i+1}) s_{i+1} = (s_1, \dots, s_i) s_{i+1} = (s_1 s_{i+1}, \dots, s_i s_{i+1}) = z$. This contradicts definition 6.2. Hence $a_1 \subset a_2 \subset \cdots$ is an infinite ascending chain contradicting the ascending chain condition.

THEOREM 7.1. *Let γ be a semi-simple lattice. Then if each element of γ can be expressed as a union of simple elements, γ is a Boolean algebra.*

PROOF. Let $a \in \gamma$ have the representation

7.1. $$a = (s_1, \dots, s_k)$$

where $s_1, \dots, s_k$ are distinct simple elements. The representation 7.1 is unique and $s_1, \dots, s_k$ are the only simple elements which a divides. For let $a = (s_1, \dots, s_k) = (s_1', \dots, s_\ell')$. Multiplying by s_i' we have $s_i' = (s_1 s_i', \dots, s_k s_i')$. Hence all of the products are null except one, say $s_i s_i'$. Then $s_i s_i' = s_i'$ and hence $s_i \supset s_i'$ by lemma 6.3. Thus $s_i = s_i'$ and $k = \ell$. If $a \supset s$ where s is simple and not equal to any of $s_1, \dots, s_k$, then $(s_1, s_2, \dots, s_k) = (s_1, \dots, s_k, s)$ contrary to the result we have just obtained.

We show now that the product of any two elements is equal to their cross-cut.

We clearly have $[a,b] \supset ab$. Let $[a,b] = (s_1, \dots, s_k)$ Then since $a, b \supset [a,b]$, $a = (s_1, \dots, s_k, a')$ and $b = (s_1, \dots, s_k, b')$ Hence $ab = (s_1, \dots, s_k, a')(s_1, \dots, s_k, b') = (s_1, \dots, s_k, a'b') \supset [a,b]$. Thus $[a,b] = ab$.

Since the product is distributive with respect to union, the cross-cut must be distributive and hence $\mathcal{N}$ is distributive. Furthermore is complemented. For let $a = (s_1, \dots, s_k)$, $u = (s_1, \dots, s_n)$ and define $a' = (s_{k+1}, \dots, s_n)$. Then $(a, a') = u$ and $[a, a'] = aa' = (s_1, \dots, s_k)(s_{k+1}, \dots, s_n) = z$. Hence $\mathcal{N}$ is a Boolean algebra.

In an arbitrary semi-simple lattice, the set of elements which can be represented as a union of simple elements need not be closed with reppect to cross-cut as we shall show by an example. However, if we assume the modular axiom we have the following theorem:

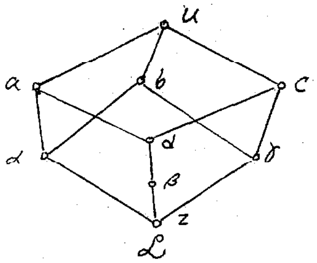
THEOREM 7.2. Let $\mathcal{N}$ be a modular, semi-simple lattice. Then the simple elements of $\mathcal{N}$ generate a Boolean algebra $\mathcal{N}_B$. Moreover $\mathcal{N}_B$ is dense in $\mathcal{N}$.

PROOF. Let $\mathcal{U}$ be the set of all elements of $\mathcal{N}$ which can be expressed as a union of simple elements of $\mathcal{N}$. $\mathcal{U}$ is obviously closed with respect to union. We shall show that $\mathcal{U}$ is dense in $\mathcal{N}$ and hence closed with respect to cross-cut. Let $(s_1, \dots, s_n) \supset x$ and let $x \supset s_1, \dots, s_e$; $x \not\supset s_{e+1}, \dots, s_n$. Then $x = [x, (s_1, \dots, s_n)]$ $= (s_1, \dots, s_e, [x, (s_{e+1}, \dots, s_n)])$ by the modular condition. If $[x, (s_{e+1}, \dots, s_n)] \neq z$, then there is a simple element s such that $[x, (s_{e+1}, \dots, s_n)] \supset s$. But then $x \supset s$ and $(s_{e+1}, \dots, s_n) \supset s$. Hence $s = s(s_{e+1}, \dots, s_n)$ $= (s_{e+1}s, \dots, s_n s) = s_i s$ by lemma 6.3. Thus $s = s_i$ and $x \supset s_i$ contrary to assumption. Hence $[x, (s_{e+1}, \dots, s_n)] = z$ and $x = (s_1, \dots, s_e)$.

Since $\mathcal{U}$ is dense in $\mathcal{N}$, it is closed with respect to multiplication and is clearly semi-simple. Moreover every element of $\mathcal{U}$ can be expressed as a union of simple elements. Hence by theorem 7.1

$\mathcal{U} = \mathcal{M}_\beta$ is a Boolean algebra.

To show the significance of the modular condition in the previous theorem we give an example of a non-modular semi-simple lattice



If $\mathcal{U}$ denotes the set of elements of $\mathcal{L}$ which can be expressed as a union of simple elements, we define a multiplication over $\mathcal{L}$ as follows: If $x, y \in \mathcal{U}, x \neq a, x \neq c$, then $xy = [x, y]$, $ac = \beta$, $dx = \beta$ or z according as $x \supset d$ or $x \not\supset d$. It can be readily verified that all of the multiplication postulates are satisfied. Also $\mathcal{L}$ is non-modular since it contains the non-modular sublattice $\{a, \alpha, d, \beta, z\}$. The simple elements α, β, γ do not generate a Boolean algebra. In fact, $\mathcal{U}$ is not closed with respect to cross-cut since $d = [(\alpha, \beta), (\beta, \gamma)]$.

THEOREM 7.3. *Let* $\mathcal{M}$ *be a modular semi-simple lattice. Then if for each simple element* S *there exists an element* $S' \neq u$ *such that* $(s, s') = u$, $\mathcal{M}$ *is a Boolean algebra.*

PROOF. We may take the S's to be divisor-free elements since if S_i' is not divisor-free, there exists a divisor-free element f_i such that $f_i \supset S_i'$ But then $(S_i, f_i) \supset (S_i, S_i') = u$. Let $v = (S_1, \dots, S_n)$. Then the length of chain from v to z is n. But now $[S_1', S_2', \dots, S_n'] = z$ since if $[S_1', \dots, S_n'] \neq z$, there exists an S_i such that $[S_1', \dots, S_n'] \supset S_i$. But then $S_i' \supset S_i$ which is impossible. Since $[S_1', \dots, S_n'] = z$ the length of chain from u to z is equal to or less than n. But $u \supset v$. Hence $u = v$.

Theorem 7.3 gives immediately

THEOREM 7.4. *A complemented, modular, semi-simple lattice is a Boolean algebra.*

We conclude with the statement of theorem 7.3 in terms of the two-sided ideals of a non-commutative ring.

THEOREM 7.5. *Let* R *be a ring without radical in which the ascending and descending chain conditions hold for two-sided ideals. Then if for each two-sided ideal* $\mathfrak{A}$ *there exists an ideal* $\mathfrak{A}' \neq R$ *such that* $(\mathfrak{A}, \mathfrak{A}') = R$, R *is a direct sum of two-sided simple ideals.*

Such an ideal $\mathfrak{A}'$ always exists if $\mathfrak{A}$ has a principle unit. For in that case we may take $\mathfrak{A}'$ to be the set of all elements x such that $\mathfrak{A}x = (0)$.

REFERENCES

G. Birkhoff

1. On combination of subalgebras, Cambridge Phil. Proc., vol. 29 (1933) pp. 441-464.

A. H. Clifford

1. Arithmetic and ideal theory of commutative semigroups, Annals of Math. vol. 39 (1938) pp. 594-610.

R. Dedekind

1. Dirichlet, Vorlesungen uber Zahlentheorie.

R. P. Dilworth

1. Abstract residuation over lattices, Bulletin of the American Math. Soc., vol. 44 (1938) pp. 262-268.

H. Grell

1. Beziehungen zwischen den Idealen verschiedener Ringe, Math. Annalen, vol. 97 (1927) pp. 490-523.

G. Kothe

1. Die Theorie der Verbande . . . , Jahresbericht der deutschen Mathematiker-Vereinigung, vol. 47 (1937) pp. 125-142.

J. Konig

1. Algebraischen Grossen, ch. I. Leipzig 1903.

W. Krull

1. Axiomatische Begrundung der Allgemeinen Idealtheorie, Sitzungsberichte der Phys.-Med. Soc. der Erlangen, vol. 56 (1924) pp. 47-63.

2. Zur Theorie der zweiseitigen Ideale in nichtkommutative Bereichen, Mathematische Zeit., vol. 28 (1928) pp. 481-503.

A. Loewy

1. Uber reduzible lineare homogene Differentialgleichungen, Math. Annalen, vol. 56 (1903) pp. 549-584.

O. Ore

1. Abstract algebra I, Annals of Math., vol. 36 (1935) pp. 406-437.

2. Theory of non-commutative polynomials, Annals of Math., vol. 34 (1933) pp. 480-508.

M. Ward

1. Postulates for an abstract arithmetic, Proc. Natl. Acad. Sci., vol. 14 (1928) pp. 907-911.

2. Conditions for factorization in a set closed under a single operation, Annals of Math., vol. 36 (1933) pp. 36-39.

3. Residuation in structures over which a multiplication is defined, Duke Math. Journal, vol. 3 (1937) pp. 627-636.

4. Structure residuation, Annals of Math., vol. 39 (1938) pp. 558-568.

M. Ward and R. P. Dilworth

1. Residuated lattices, Proc. Natl. Acad. Sci., vol. 24 (1938) pp. 162-165.

2. Residuated lattices, Transactions of the American Math. Soc., vol. 45 (1939) pp.

J. H. M. Wedderburn

1. Non-commutative domains of integrity, J. fur Math., vol. 167 (1931) pp. 129-141.