Séminaire Dubreil.
Algèbre et théorie
des nombres

Garrett Birkhoff

Lattice-ordered demigroups

Séminaire Dubreil. Algèbre et théorie des nombres, tome 14, n° 2 (1960-1961), exp. n° 19, p. 1-26

<http://www.numdam.org/item?id=SD_1960-1961__14_2_A3_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
14e année, 1960/61, n° 19

17 avril 1961
(texte revu et corrigé
le 23 juin 1961)

LATTICE-ORDERED DEMIGROUPS

by Garrett BIRKHOFF

The following discussion is essentially a preliminary draft of the third edition of my book, "Lattice theory", which should appear in print around 1965. Repeated references will be made to :

[DLC] DUBREIL-JACOTIN (M.-L.), LESIEUR (L.) and CROISOT (R.). - Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques. - Paris, Gauthier-Villars, 1953 (Cahiers scientifiques, 21).

[LT2] BIRKHOFF (Garrett). - Lattice theory, revised edition. - New York, American mathematical Society, 1948 (Amer. math. Soc. Coll. Publ., 25).

References such as to : "Ch. V, § 3", refer to the mimeographed "Notes on lattice theory" made by my students in 1960/61.

1. Multiplicative posets.

Lattice-ordered demigroups and their generalizations play a central role in such diverse subjects as algebraic number theory, algebraic geometry, the Wedderburn theory of semisimple algebras, the algebra of binary relations, Brouwerian Logic, and general topology. The theory of lattice-ordered semi-groups attempts to give a synthesis of certain aspects of these subjects, by suitably generalizing the concept of lattice-ordered group.

The logical starting point for the theory of lattice-ordered demigroups consists in the following definition.

DEFINITION. - A multiplicative poset or m-poset ([1]) is a poset M with a binary multiplication which satisfies the isotonicity condition

$$(1) \qquad a \leqslant b \text{ implies } xa \leqslant xb \text{ and } ax \leqslant bx \quad ,$$

for all a , b , $x \in M$. When multiplication is commutative or associative, M is called a commutative or associative m-poset, respectively. An m-demigroup is an associative m-poset.

([1]) "Groupoïde ordonné" in the terminology of [DLC].

EXAMPLE 1. - Any po-group is an m-poset which is a group under multiplication. Conversely, any m-poset which is a group under multiplication is a po-group.

EXAMPLE 2. - Let B be any binary system, that is, any set with a binary multiplication (or "groupoïde"). Then the subsets of B form an m-poset M(B), if ST is the set of all products st with $s \in S$, $t \in T$.

Clearly, M(B) is a Boolean algebra ; and if B is commutative or associative, then so is M(B).

There are many important concepts which are applicable to m-posets generally. Among these are the following.

DEFINITION. - A zero of an m-poset M is an element 0 of M such that

(2) $$0 \leqslant x \text{ and } x0 = 0x = 0 \text{ for all } x \in M .$$

A unity of M is an element 1 such that

(3) $$1x = x1 = x \text{ for all } x \in M .$$

An element a of an m-poset M with unity is integral if and only if $a \leqslant 1$. If all elements of M are integral elements, then M is called an integral m-poset.

An m-poset can have at most one unity. For if 1 and 1' satisfy (3), then $1 = 11' = 1'$. Likewise, a poset can have at most one zero. Any po-group has a unity, the group identity. If a po-group has a 0, it can have no other element.

EXAMPLE 3. - Any distributive lattice L is a commutative and associative m-poset if ab is defined as $a \cap b$. If L has an I, then I is a unity for this m-poset, which is an integral m-poset.

DEFINITION. - In an m-poset M, an element a is called subidempotent if $aa \leqslant a$; it is called a left-ideal element if $xa \leqslant a$ for all $x \in M$, and a right-ideal element if $ax \leqslant a$ for all $x \in M$. An element which is both a left and a right-ideal element is called an ideal element.

In example 2, the subidempotent elements of M(B) correspond to the subalgebras of B. In example 3, and in integral m-posets generally, every element is an ideal element. Clearly any left or right-ideal element is subidempotent. The concept of an ideal element is suggested by the following extension of example 2.

EXAMPLE 4. - Let R be any ring, and let $M(R)$ be defined as in example 2, from the multiplication in R. Then $M(R)$ is an m-poset. The modules (nonvoid additive subgroups) of R form a subset $M_1(R)$ of $M(R)$ which is closed under intersection. If ST is defined as the set of all finite sums $\sum s_i t_i$, $s_i \in S$ and $t_i \in T$, then $M_1(R)$ is also an m-poset, which is a modular lattice as a poset though not a Boolean algebra unless the additive group of R is cyclic of prime order.

In example 4, the 0 of R is a zero of $M_1(R)$. Moreover the subidempotent elements of $M_1(R)$ correspond to the subrings of R; and the right, left, and two-sided ideal elements of $M_1(R)$ to the corresponding ideals in R. If R has a unity, then R itself is a unity for the lattice $M_2(R)$ of all two-sided ideals of R. Hence $M_2(R)$ is an integral m-poset.

EXAMPLE 4'. - Let D be any demigroup, and form $M(D)$ as in example 2. Then the subidempotent elements of $M(D)$ correspond to the subdemigroups of D; and the right, left, and two-sided ideal elements of $M(D)$ to the corresponding sets of ideals in D. If D has a unity, then the two-sided ideals of D form an integral m-poset, as before.

2. Lattice-ordered demigroups.

One of the most important questions in the theory of ordered demigroups is the following. Can one develop a unified theory of ideal elements in m-posets which will yield the theory of ideals in rings and demigroups as special cases ? Such a unified theory should also, of course, have other interesting applications.

To lay the foundations for such a unified theory, we first define some further properties of m-posets of ideals.

DEFINITION. - A multiplicative semilattice, or m-semilattice [2] is a binary system M which is a semilattice under $\cup$, and satisfies

$$a(b \cup c) = ab \cup ac \quad \text{and} \quad (a \cup b)\, c = ac \cup bc \,, \tag{4}$$

for all a, b, $c \in M$. If M is a lattice under $\cup$, then it is called a multiplicative lattice or m-lattice. If the multiplication in M is associative and with a 1, then M is called an ℓ-demigroup.

---

[2] Called a "gerbier" in [DLC], where an m-lattice is called a "groupoïde réticulé".

One shows trivially that any m-semilattice is an m-poset. One verifies easily that the subsets of any binary system B (example 2) form a complemented, distributive m-lattice M(B) . Also, any distributive lattice (example 3) is an m-lattice if $xy = x \cap y$. Again, the modules of any ring form a complemented, modular m-lattice (example 4). Finally, any po-group which is a lattice satisfies (4) and its dual

(4') $$a(b \cap c) = ab \cap ac \quad \text{and} \quad (a \cap b)\, c = ac \cap bc \quad .$$

EXAMPLE 5. - The join-endomorphisms α , β , γ , ... of any semilattice S form an m-semilattice, under the definitions

(5) $$a(\alpha\beta) = (a\alpha)\,\beta \quad \text{and} \quad a(\alpha \cup \beta) = a\alpha \cup a\beta \quad .$$

Observe that the class of m-lattices is <u>equationally definable</u> in the sense of chapter V. Hence the general algebraic concepts of subalgebra, homomorphic image, and direct union apply to m-lattices. In particular, any m-sublattice, homomorphic image, or direct union of m-lattices is itself an m-lattice. A similar remark applies to ℓ-semilattices and to ℓ-demigroups, but not to ℓ-semigroups since the cancellation law is not preserved under all homomorphisms.

The preceding remark permits one to construct various interesting m-semilattices of <u>real functions</u>, under addition and l. u. b. The <u>upper-semicontinuous</u> functions and <u>subharmonic</u> functions of n variables form commutative ℓ-semigroups.

THEOREM 1. - In any m-lattice M ,

(6) $$(a \cap b)(a \cup b) \leqslant ba \cap ab \quad \text{for all} \quad a\,,\ b \quad .$$

If M is an integral m-lattice, then

(7) $$a \cup b = 1 \quad \text{implies} \quad a \cap b = ba \cup ab \quad ,$$

and

(8) $$a \cup b = a \cup c = 1 \quad \text{implies} \quad a \cup bc = a \cup (b \cap c) = 1 \quad .$$

If M has an element $z \leqslant 1$ satisfying $zx = xz = z$ for all $x \in M$, then this z is a zero.

This is theorem 1 of [LT2] (p. 201), where a proof will be found. It applies to ideals in associative rings, in view of the following result.

THEOREM 2. - Let L be any ℓ-demigroup. Then the right-ideal elements of L , the left-ideal elements of L , and the (two-sided)-ideal elements of L are

m-sublattices.

PROOF. - The case of right-ideal elements is typical. If a and b are right-ideal elements, then by (1)

$$(a \cap b)\ x \leqslant ax \leqslant a \quad \text{and} \quad (a \cap b)\ x \leqslant bx \leqslant b$$

for all $x \in L$; hence

$$(a \cap b)\ x \leqslant a \cap b\ .$$

Also, by (4),

$$(a \cup b)\ x = ax \cup bx \leqslant a \cup b\ .$$

Finally, by associativity,

$$(ab)\ x = a(bx) \leqslant ab\ .$$

3. Divisibility in semigroups.

The most deeply studied m-posets are the commutative and associative semigroups associated with multiplication in certain classical integral domains. The fundamental ideas involved can be stated very simply ([3]) ; but the m-posets in question are not generally lattices.

Let G be any commutative semigroup with unity 1 . Define $a|b$ to mean that $ax = b$ for some $x \in G$; this relation is a quasi-ordering of G . Now define $a \wr b$ (read " a and b are associated") to mean that $a|b$ and $b|a$; $a \wr b$ if and only if $b = au$, where u is a "unit", or divisor of 1 . The relation $\wr$ is an equivalence relation, whose equivalence classes form a partly ordered set $P(G)$ (as in Ch. II, § 2). Moreover $a \wr b$ is a congruence relation for multiplication. For if $ax = b$, then $(ac)\ x = (ax)\ c = bc$ for all $c \in G$; hence $a|b$ implies $ac|bc$. Likewise, $b|a$ implies $bc|ac$, and so $a \wr b$ implies $ac \wr bc$ for all $c \in G$, as asserted. Finally, $1|a$ for all $a \in G$. This proves that $P(G)$ is an integral m-poset ; it is evidently a commutative po-demigroup as well. One can prove more.

THEOREM 3. - In any commutative semigroup G with unity, the relation $a|b$ defines an integral po-semigroup $P(G)$ on the sets of associated elements. For each $a \in P(G)$, the mapping $x \to ax$ is an order-isomorphism of $P(G)$ onto the

([3]) See : BIRKHOFF (G.) and MACLANE (S.). - Survey of modern algebra, rev. ed. - New York, MacMillan Company, 1954 ; Ch. III, § 7.

See also : DUBREIL (P.) et DUBREIL-JACOTIN (M.-L.). - Leçons d'algèbre moderne. - Paris, Dunod, 1961 (Collection universitaire de Mathématiques, 6) ; Ch. IV, § 6.

lattice ideal A of elements $c \leqslant a$.

To prove that the po-demigroup $P(G)$ is a po-semigroup is to show that $ax \backsim ay$ implies $x \backsim y$. But $ax|ay$ implies $ay = ya = xaz = axz$ for some $z \in G$, whence $y = xz$ by the cancellation law in G ; therefore $ax|ay$ implies $x|y$. Likewise, $ay|ax$ implies $y|x$, from which the cancellation law in $P(G)$ follows. To summarize the preceding results, we make the

DEFINITION. - A commutative integral po-semigroup in which $a \geqslant b$ if and only if $a|b$ is called a <u>divisibility po-semigroup</u>. If it is a lattice under $a|b$, it is called a <u>divisibility ℓ-semigroup</u>.

The po-semigroup $P(G)$ in theorem 1 is a divisibility po-semigroup ; considered as a semigroup alone, $P(P(G)) \overset{\sim}{=} P(G)$.

Now let G be the multiplicative semigroup of the nonzero elements of an <u>integral domain</u> D . Then $a \backsim b$ is equivalent to the statement that a and b generate the same nonzero principal ideal $(a) = (b)$ of D . We have the

COROLLARY. - The nonzero principal ideals of any integral domain D form a divisibility semigroup $S(D)$.

Referring back to theorem 1, we see that if $S(D)$ is a lattice (i. e., if any two elements, a , $b \in D$ have a g. c. d. and l. c. m. in D), then the correspondence $x \to ax$ preserves joins and meets (which are necessarily in A for any ax and ay). This proves

THEOREM 4. - If a divisibility po-semigroup is a lattice under the relation $a|b$, then for all a , b , c :

$$a(b \cup c) = ab \cup ac \quad \text{and} \quad a(b \cap c) = ab \cap ac \qquad (9)$$

4. <u>Prime factorization</u>.

In classical algebra, attention is focussed on two particular families of integral domains, and specifically on proving that the elements of these domains admit of <u>unique factorization into primes</u>. The integral domains E in question are the following.

EXAMPLE 6. - Let $F = R(\theta)$ be an algebraic extension of the rational field R of finite degree, and let E be the domain of all algebraic integers of F .

EXAMPLE 7. - Let $F = K(x_1, \cdots, x_r)$ be the field of all rational forms in r variables x_i with coefficients in a given base field K, and let $E = K[x_1, \cdots, x_r]$ be the domain (subring) of all polynomial forms in the $x_i \cdots$.

We now define generally three closely related concepts, which are effectively equivalent when unique factorization into primes is possible.

DEFINITION. - Let M be any integral m-poset. An element $m \in M$ is called maximal if it is covered by 1; an element $p < 1$ such that $ab \leqslant p$ implies $a \leqslant p$ or $b \leqslant p$ is called prime; an element $p < 1$ such that $ab = p$ implies $a = p$ or $b = p$ is called indecomposable.

COROLLARY. - In a divisibility po-semigroup, p is a prime if and only if $p|ab$ implies $p|a$ or $p|b$.

LEMMA 1. - In a divisibility po-semigroup, any prime element is maximal; an element is maximal if and only if it is indecomposable.

PROOF. - Let m be maximal in any integral m-poset, and that $xy = m$. Then $x = m$ or $x = 1$ since $m = xy \leqslant x1 = x$ and m is maximal; likewise, $y = m$ or $y = 1$. Since $x = y = 1$ would imply $xy = 1$, either $x = m$ or $y = m$, and so m is indecomposable.

Conversely, unless p is maximal, $1 > q > p$ for some q. Since $q > p$ implies $q|p$, $p = qr$ where (evidently) $r < 1$. Moreover $r \not\leqslant p$ since (by theorem 1) $q < 1$ and $r \leqslant p$ would together imply $qr < p$. Hence p cannot be prime unless it is maximal. Since $r \neq p$ and $q \neq p$, it cannot be indecomposable either.

The classical divisibility semigroups defined by the nonzero elements of examples 6 and 7 satisfy the ascending chain condition. This follows from the corollary of theorem 1, since (i) the ideals of the corresponding integral domains satisfy the ascending chain condition (Ch. VII), and (ii) hence so does the subset of principal ideals a fortiori.

LEMMA 2. - In any integral po-semigroup satisfying the ascending chain condition, every element $c \neq 1$ is a product of indecomposable (= maximal) factors.

PROOF. - If the conclusion fails, then the nonvoid set of all elements not so decomposable must contain a maximal member c. This c cannot be indecomposable

(i. e., covered by 1), or the conclusion would hold trivially. But if c is decomposable, then $c = ab$ where $a > c$ and $b > c$. Since c was maximal among elements not products of indecomposable factors, we have $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$, whence $c = p_1 \cdots p_r = q_1 \cdots q_s$, giving a contradiction.

The following example shows that one cannot prove more, without making a further assumption.

EXAMPLE 7. - Let G be the additive semigroup of pairs (m, n) of nonpositive integers whose sum $m + n$ is even. Then $(-2, 0) + (0, -2) \leq (-1, -1)$, and so $(-1, -1)$ is maximal but not prime. Also, since $(-2, -2) = (-2, 0) + (0, -2) = (-1, -1) + (-1, -1)$, one need not have a unique factorization theorem.

Actually, the relevant assumption is precisely the lattice hypothesis of § 2, as we now show.

LEMMA 3. - In any integral m-lattice L, every maximal element is prime and indecomposable.

PROOF. - Let m be maximal. Unless $x \leq m$, $x \cup m = 1$. Hence if $xy \leq m$, but $x \not\leq m$, then

$$y = 1y = (x \cup m)\, y \leq xy \cup my = m \cup m1 = m \quad ,$$

so that m is a prime. To prove indecomposability, one proceeds as in lemma 1.

COROLLARY. - In a divisibility ℓ-semigroup, the concepts of prime element, indecomposable element, and maximal element are mutually equivalent.

THEOREM 5. - In any divisibility ℓ-semigroup which satisfies the ascending chain condition, every element $c \neq 1$ can be uniquely factored into prime factors.

PROOF. - By the preceding corollary, the words prime, indecomposable, and maximal are mutually interchangeable. By lemma 2, at least one factorization into prime factors exists. If $c = p_1 \cdots p_r = q_1 \cdots q_s$ are any two such factorizations, then by the first corollary of § 3 and induction, $p | q_j$ for some j. Hence, p and q being maximal, $p_1 = q_j$. Cancelling, one can prove uniqueness by induction on r; we omit the details.

APPLICATION. - Theorem 5 has an immediate application to algebraic number theory. It is known ([5]) that factorization into primes is unique in a domain $E = E(\theta)$ of algebraic integers if and only if every ideal of E is principal. But the set of all ideals of any ring is a lattice ; hence, if the unique factorization theorem holds in $E(\theta)$, its principal ideals form an ℓ-semigroup ; hence the same is true of its divisibility po-semigroup, as in the corollary of theorem 3. By theorem 5, and the remarks preceding it, the converse is also true. In conclusion, we have the following result ([6]).

COROLLARY. - The nonzero integers of an algebraic number field $F = R(\theta)$ satisfy the unique factorization theorem if and only if their divisibility po-semigroup is a lattice.

It is actually sufficient that the divisibility po-semigroup be a semilattice under g. c. d. For a reasonably practical necessary and sufficient test for this, see POLLARD, theorem 9.5.

6. Integral m-lattices.

An integral m-poset which is a lattice with respect to its order relation is called an integral m-lattice. The two-sided ideals of any ring with unity form such a (modular) integral m-lattice. Indeed, the main advantage of considering ideals instead of elements, in algebraic number theory, is to ensure the existence of g. c. d. and l. c. m., that is, that one has a (commutative, modular, integral) m-lattice. In general rings, one sacrifices the cancellation law to gain this advantage.

In any integral m-lattice, one defines two elements a and b to be coprime when $a \cup b = 1$ (this is the dual of disjointness, for positive elements in an ℓ-group). Such coprime elements have a number of interesting general properties, proved in [LT2], (Ch. XIII, § 3). From this source we quote only one isolated result.

THEOREM 6. - Every complemented integral m-lattice is a Boolean algebra, in which $xy = x \cap y$.

([5]) POLLARD (Harry). - The theory of algebraic numbers. - New York, J. Wiley and Sons, 1950 (The Carus mathematical Monographs, 9) ; theorem 9.4. This book will be referred to below simply as POLLARD.

([6]) JAFFARD (Paul). - Les systèmes d'idéaux. - Paris, Dunod, 1960 (Travaux et Recherches mathématiques, 4) ; p. 81, théorème 4).

7. Residuation.

One of the most important concepts in the theory of multiplicative lattices is that of residual, defined as follows.

DEFINITION. - Let L be any m-poset. The right-residual $a \cdot\!\!\cdot b$ of a by b is the largest x (if it exists) such that $bx \leq a$; the left-residual $a \cdot\!\!\cdot b$ of a by b is the largest y such that $yb \leq a$. A residuated lattice is an m-lattice L in which $a \cdot\!\!\cdot b$ and $a \cdot\!\!\cdot b$ exist for any a , $b \in L$; a residuated ℓ-demigroup is an associative residuated lattice.

Any po-group is residuated ; moreover $x \cdot\!\!\cdot y = y^{-1} x$ is the operation written x/y in Ch. V, § 10, and $x \cdot\!\!\cdot y = xy^{-1}$ is the operation written $x\backslash y$ there. Since residuals in ℓ-groups are definable in terms of group multiplication alone, their discussion belongs properly to pure group theory, and will not be given here.

THEOREM 7. - In any residuated lattice, we have

(10) $\qquad (a \cap b) \cdot\!\!\cdot c = (a \cdot\!\!\cdot c) \cap (b \cdot\!\!\cdot c)$ and symmetrically,

(11) $\qquad a \cdot\!\!\cdot (b \cup c) = (a \cdot\!\!\cdot b) \cap (a \cdot\!\!\cdot c)$ and symmetrically,

(12) $\qquad ab \leq c$, $b \leq c \cdot\!\!\cdot a$, and $a \leq c \cdot\!\!\cdot b$ are equivalent,

(13) $\qquad (ab) \cdot\!\!\cdot a \geq b$ and $(ab) \cdot\!\!\cdot b \geq a$.

In any residuated ℓ-demigroup

(14) $\qquad (a \cdot\!\!\cdot b) \cdot\!\!\cdot c = (a \cdot\!\!\cdot c) \cdot\!\!\cdot b$ is the largest x such that $bxc = a$, and

(15) $\qquad a \cdot\!\!\cdot (bc) = (a \cdot\!\!\cdot b) \cdot\!\!\cdot c$ and $a \cdot\!\!\cdot (bc) = (a \cdot\!\!\cdot c) \cdot\!\!\cdot b$.

Proofs of these results are given in [DIC]. In equations (10) and (11), the existence of the left side implies that of the right side.

Almost trivially, we have the following result.

LEMMA 1. - In any m-poset, the functions $a \cdot\!\!\cdot b$ and $a \cdot\!\!\cdot b$ are isotone in a and antitone in b .

This result implies $a \cdot\!\!\cdot (b \cap c) \geq a \cdot\!\!\cdot b$ and $a \cdot\!\!\cdot (b \cap c) \geq a \cdot\!\!\cdot c$. By the definition of $\cup$ as least upper bound, there follows the inequality (16) of

LEMMA 2. - In any residuated lattice, we have

(16) $$a \cdot\!\!\bullet (b \cap c) \geqslant (a \cdot\!\!\bullet b) \cup (a \cdot\!\!\bullet c) \quad \text{and symmetrically} \quad ,$$

(17) $$b \leqslant a \cdot\!\!\bullet (a \bullet\!\!\cdot b) \quad \text{and} \quad b \leqslant a \bullet\!\!\cdot (a \cdot\!\!\bullet b) \quad .$$

The first inequality follows from the definition of $a \cdot\!\!\bullet (a \bullet\!\!\cdot b)$, since $(a \bullet\!\!\cdot b)\, b \leqslant a$ by definition of $a \bullet\!\!\cdot b$.

COROLLARY. - Any integral element a of a residuated lattice with unity satisfies

(18) $$a \leqslant 1 \cdot\!\!\bullet (1 \bullet\!\!\cdot a) \leqslant 1 \quad \text{and} \quad a \leqslant 1 \bullet\!\!\cdot (1 \cdot\!\!\bullet a) \leqslant 1 \quad .$$

PROOF. - Since $a \leqslant 1$,

$$1 \bullet\!\!\cdot a \geqslant 1 \bullet\!\!\cdot 1 = 1 \quad ;$$

hence by lemma 1,

$$1 \cdot\!\!\bullet (1 \bullet\!\!\cdot a) \leqslant 1 \cdot\!\!\bullet 1 = 1 \quad .$$

On the other hand, since

$$(1 \bullet\!\!\cdot a)\, a \leqslant 1 \quad , \quad 1 \cdot\!\!\bullet (1 \bullet\!\!\cdot a) \geqslant a \quad ,$$

completing the proof of the first inequality. The second follows by symmetry.

8. Residuation and Galois connections.

The two binary operations of left-and right-residuation define a class of Galois connections with many diverse applications (7). We have

THEOREM 8. - For any fixed element c of any residuated lattice L, the correspondences $x \to c \cdot\!\!\bullet x = x^*$ and $y \to c \bullet\!\!\cdot y = y^\dagger$ define a Galois connection on L.

PROOF. - By definition (Ch. VII, § 7), this means that the correspondences in question are antitone, and that

$$x \leqslant c \cdot\!\!\bullet (c \bullet\!\!\cdot x) \quad \text{and} \quad x \leqslant c \bullet\!\!\cdot (c \cdot\!\!\bullet x) \quad \text{for all } x \quad .$$

These results were proved in the last section.

For applications, the choices $c = 0$ and $c = 1$ are the most interesting.

---

(7) See : DUBREIL (P.) et CROISOT (R.). - Propriétés générales de la résiduation en liaison avec les correspondances de Galois, Collectanea Mathematica, t. 7, 1954, p. 193-203 (Seminario matematico de Barcelona).

Moreover for applications, one wants to pursue the implications of theorem 8 somewhat further.

LEMMA 1. - Under any Galois connection, we have

$$(19) \qquad ((x^*)^\dagger)^* = x \quad \text{and} \quad ((x^\dagger)^*)^\dagger = x^\dagger \quad .$$

The correspondences $x \to (x^*)^\dagger$ and $x \to (x^\dagger)^*$ are closure operations. The closed elements $x = (x^*)^\dagger$ form a lattice, and so do the $x = (x^\dagger)^*$. Joins and meets are defined in this lattice by

$$(20) \qquad x \wedge y = x \cap y \quad \text{and} \quad x \vee y = ((x \cup y)^\dagger)^* \quad \text{resp.} \quad ((x \cup y)^*)^\dagger \quad .$$

We omit the proof, which belongs in Ch. VIII, § 7. The above results have an obvious corollary.

DEFINITION. - For any $c \in L$, L a residuated lattice, an element $x \in L$ is right c-closed if and only if $x = c \cdot\!\!\bullet\ (c \bullet\!\!\cdot\ x)$, and left c-closed if and only if $x = c \bullet\!\!\cdot\ (c \cdot\!\!\bullet\ x)$.

COROLLARY 1. - An element $x \in L$ is right c-closed if and only if $x = c \bullet\!\!\cdot\ y$ for some y, and left c-closed if and only if $x = c \cdot\!\!\bullet\ y$ for some y.

The fact that the meet of any two right c-closed elements is right c-closed follows since $(a \cup b)^* = a^* \cap b^*$. On the other hand, the join of two right c-closed elements need not be right c-closed.

Note also the condition of P. DUBREIL ([8]) : The c-closures of x are defined by the equations $\overline{x}_r = cx \cdot\!\!\bullet\ c$ and $\overline{x}_\ell = cx \bullet\!\!\cdot\ c$, respectively.

The preceding definitions can be applied to the ℓ-demigroup L of all modules $A, B, C, \ldots$ of an associative ring R (example 4 of § 1). In this example, the Galois connection defined by $X \to C \cdot\!\!\bullet\ X$ and $Y \to C \bullet\!\!\cdot\ Y$ can also be derived concretely from the polarity (Ch. VIII, § 6) defined by the binary relation $xy \in C$. If C is a right-ideal, then so is $C \cdot\!\!\bullet\ X$; if C is a left-ideal, then so is $C \bullet\!\!\cdot\ Y$. Hence we have :

([8]) DUBREIL (Paul). - Contribution à la théorie des demi-groupes, III., Bull. Soc. math. France, t. 81, 1953, p. 289-306 ; LESIEUR (Léonce). - Sur les demi-groupes réticulés satisfaisant à une condition de chaîne, Bull. Soc. math. France, t. 83, 1955, p. 161-193.

COROLLARY 2. - If C is a (two-sided)-ideal of an associative ring R, then the right C-closed modules are right-ideals of R, and the left C-closed modules are left-ideals.

The concept of c-closure can also be applied to the lattice of bounded subharmonic functions on a region R. The 0-closed functions $0 ; x$ are just the harmonic functions on R.

9. Brouwerian lattices.

The preceding results can be applied to lattices which are m-lattices with respect to the multiplication $xy = x \cap y$, so-called Brouwerian lattices. Brouwerian lattices are necessarily distributive as lattices and commutative as m-lattices. (See also theorem 6).

In dealing with these, and with the other commutative residuated lattices to be discussed in § 9 - § 14, we will write $a : b$ for $a \cdot^{\cdot} b = a \cdot_{\cdot} b$. We also have $a^{\dagger} = a^{*}$ for all a. Hence we can suppress the notation $a^{\dagger}$. We first extend the result of example 3, by proving

THEOREM 9. - A lattice L is a residuated lattice, when xy is defined as $x \cap y$, if and only if it is a Brouwerian lattice. In this case, L is an integral commutative ℓ-semigroup.

The proof is almost trivial, since if $xy = x \cap y$, the definition of relative pseudo-complement $a * b$ given in Ch. I, § 13, coincides when $b \leqslant a$ with that of $b : a$ given in § 7 above, and that of pseudo-complement a^{*} coincides with that of $0 : a$ given in § 7. For the details, see Ch. X, p. 16.

THEOREM 10 (GLIVENKO). - If L is a Brouwerian lattice, then the correspondence $a \to a^{**}$ is a closure operation on L, and a lattice-homomorphism of L onto the Boolean algebra of "closed" elements. Moreover $a^{**} = b^{**}$ if and only if $a \cap d = b \cap d$ for some "dense" $d \in L$ satisfying $d^{**} = I$.

PROOF. - We first establish, for relative pseudo-complement, that

$$(21) \qquad (c : a) \cap (c : (c : a)) \leqslant c \quad .$$

To prove (21), write $c : a$ as a^{*} and $c : (c : a)$ as a^{**}, as in § 7. If $b = a^{*} \cap a^{**}$, then $b^{*} = a^{**} \cup a^{*} \geqslant b$ since the correspondence $x \to x^{*}$ is a dual automorphism of the lattice of c-closed elements. But this implies $b = b \cap b = bb \leqslant c$, proving (21).

Now suppose $x \cap a \cap b \leqslant c$ in L ; define $y = x \cap a^{**} \cap b^{**}$. Clearly $y \leqslant x$, whence $y \cap a \cap b \leqslant c$, which implies $y \cap a \leqslant c : b = b^*$. But $y \cap a \leqslant y \leqslant b^{**}$ by definition of y ; hence $y \cap a \leqslant b^* \cap b^{**} \leqslant c$ by (21). This implies $y \leqslant c : a = a^*$; but $y \leqslant a^{**}$ by its definition ; hence $y \leqslant a^* \cap a^{**} \leqslant c$, by (21). In summary, $x \cap a \cap b \leqslant c$ implies $x \cap a^{**} \cap b^{**} \leqslant c$, or $(a \cap b)^* \leqslant (a^{**} \cap b^{**})^*$. But the reverse inequality is obvious ; hence $(a \cap b)^* = (a^{**} \cap b^{**})^*$.

On the other hand, $(a^* \cup b^*)^* = a^{**} \cap b^{**}$, and so

$$(a \cap b)^* = (a^{**} \cap b^{**})^* = ((a^* \cup b^*)^*)^* = a^* \vee b^* \quad ,$$

where $a^* \vee b^*$ is the join of a^* and b^* in the lattice of all c-closed elements of L . For proofs of the other statements of theorem 10 (see [LT2], p. 149).

10. Complete m-lattices.

The majority of residuated lattices are complete, and they satisfy the infinite distributive laws

$$(22) \qquad a(\bigcup b_\beta) = \bigcup (ab_\beta) \quad \text{and} \quad (\bigcup a_\alpha)\, b = \bigcup (a_\alpha\, b) \quad .$$

This leads us to make the following definitions.

DEFINITION. - A complete m-lattice, or cm-lattice, is a complete lattice with a binary multiplication satisfying (22). A complete m-lattice which is an ℓ-demigroup is called a $c\ell$-demigroup ; if the cancellation law holds, it is called a $c\ell$-semigroup.

Analogs of (15), (16) and (21) hold in any cm-lattice which is residuated (see theorem 10).

The modules of a ring (example 4, § 1) constitute a typical cm-lattice ; we omit the verification of (22), which follows from the fact that the operations involved are finitary (binary). We now show abstractly that cm-lattices are almost always residuated.

THEOREM 11. - In any cm-lattice, $a :\!\cdot b$ exists if $bx \leqslant a$ for some x , and $a \cdot\!: b$ exists if $yb \leqslant a$ for some y .

PROOF. - Let u be the join of all x_α such that $bx_\alpha \leqslant a$. Then

$$bu = b(\bigcup x_\alpha) = \bigcup bx_\alpha \leq a$$

by (22) ; hence

$$u = a \cdot\!\!\cdot b \quad .$$

The existence of $v = b \cdot\!\!\cdot a$ under the stated assumptions can be proved similarly.

COROLLARY 1. - Any cm-lattice with zero is residuated. Using theorem 2, we obtain :

COROLLARY 2. - If R is any associative ring, then the complete m-lattices of all modules of R and of all two-sided ideals of R are residuated.

In fact, if H and K are subrings of R, then $H \cdot\!\!\cdot K$ and $H \cdot\!\!\cdot K$ are the right- and left-quotients of H by K, in the sense of ideal theory. The case $H = 0$ is of especial importance ; $0 \cdot\!\!\cdot K$ is called the right-annihilator of K, and $0 \cdot\!\!\cdot K$ the left-annihilator of K. We will discuss these ideas further in § 14.

Regular open sets. - We will now derive the general properties of regular open sets in Hausdorff spaces, as an application of the theory of residuated lattices. Conversely, the discussion gives some intuitive meaning to theorem 10.

EXAMPLE 9. - Let L be the complete Brouwerian lattice of all open sets of any Hausdorff space I, and let $c = 0$ in the Galois correspondence of § 9. This makes $a^* = 0 : a$.

Then $a^* = I^*$ means that a differs from I on a nowhere dense set ; some of the properties of nowhere dense sets will be established below. Also, sets such that $a^{**} = a$ are called regular open sets. In the Hausdorff space defined by the open interval $(0 , 2)$, the open intervals $(0 , 1)$ and $(1 , 2)$ are regular open sets, but their union is not regular. This illustrates the fact that, even if $a = a^{**}$ and $b = b^{**}$ are closed in theorem 10, the union $a \cup b = a^{**} \cup b^{**}$ can be smaller than $a \vee b = (a \cup b)^{**}$.

LEMMA 1. - If $a^{**} = I$ and $b^{**} = I$, then $(a \cap b)^{**} = I$.

PROOF. - In any integral residuated lattice, $0 : 1 = 0$; hence the hypothesis of lemma 1 is equivalent to $a \cap x = 0$ implies $x = 0$ and $b \cap x = 0$ implies $x = 0$ (i. e., $a^* = I^* = 0$ and $b^* = I^* = 0$). But the above conditions yield

in turn that $(a \cap b) \cap x = 0$ implies $a \cap (b \cap x) = 0$, hence $b \cap x = 0$, and hence $x = 0$. This is $(a \cap b)^* = 0$.

LEMMA 2. - Every $a \in L$ satisfies $a = a^{**} \cap k$, where $k^* = 0$. Conversely, if $k^* = 0$, then $a^* = (a \cap k)^*$.

PROOF. - Set $k = a \cup a^*$. Then $k^* = (a \cup a^*)^* = a^* \cap a^{**} = 0$, by definition of $a^{**} = (a^*)^*$. Also

$$a^{**} \cap k = a^{**} \cap (a \cup a^*) = (a^{**} \cap a) \vee (a^{**} \cap a) = a \cup 0 = a,$$

since $a^{**} \geq a$. Finally, if $k^* = 0$, then $k \cap x = 0$ implies $x = 0$. Hence $(a \cap k) \cap x = 0$ (or $k \cap (a \cap x) = 0$) implies $a \cap x = 0$, and so $(a \cap k)^* \leq a^*$. But $(a \cap k)^* \geq a^*$ trivially; hence $a^* = (a \cap k)^*$, completing the proof.

COROLLARY. - In L, $a^* = b^*$ if and only if $a = c \cap h$ and $b = c \cap k$ for some c, where $h^* = k^* = 0$.

PROOF. - If $a^* = b^*$, then $a^{**} = b^{**} = c$. By lemma 2, $a = c \cap h$ and $b = c \cap k$, where $h^* = k^* = 0$. The converse follows from lemma 2 similarly.

We have shown that two open sets have the same "regular" completion if and only if they differ by a nowhere dense set. Finally, we state without proof:

THEOREM 12. - A Brouwerian lattice L is isomorphic with the lattice of all open sets of a Hausdorff space if and only if it is complete, and every element of L is a meet of maximal elements ("dual points").

The second condition is a transfinite analog of factorization into primes.

11. Fundamental theorem of ideal theory.

Residuals (or "ideal quotients"; see the remark after theorem 11, corollary 2) play an important role in modern proofs of the fundamental theorem of ideal theory. This theorem is concerned specifically with E-modules of an arbitrary algebraic number field $R(\theta)$, where E is the domain (subring) of all integers of F. One can easily generalize theorem 2, to show that the set of all such E-modules is a commutative ℓ-demigroup, and an m-sublattice of the ℓ-demigroup of all modules of F.

Such an E-module A is a Dedekind ideal of F if and only if

(i) A is nonzero ,

and

(ii) $nA \subset E$ for some rational integer n .

(Using the concept of integral basis, it is easy to show that an E-module A is a Dedekind ideal if and only if $E \cup A/E \cap A$ is finite ; the trick is to show that every integral ideal contains a rational integer $\prod f(\theta_i)$.)

One of the main conclusions of algebraic number theory is the result that Dedekind ideals of F form an (atomistic) ℓ-group. The unique factorization theorem for integral ideals follows as a corollary of this group property, as in Ch. XI. However, this group property is not easily established.

Actually, the fundamental theorem of ideal theory can be best proved using two special properties of the commutative residuated ℓ-demigroup with unity of all nonzero E-modules of F , viz :

I. If A is a nonzero integral E-module, then all chains between A and E have finite length (Finite Chain Condition).

II. If P is a maximal proper integral E-module of F , then $P(1 : P) = 1$.

THEOREM 13. - Let L be any commutative residuated ℓ-demigroup with unity, in which :

(I) $0 < a < 1$ implies that all chains between a and 1 are finite, and

(II) $p(1 : p) = 1$ for every maximal proper integral element p . Then every element $a \in L$ with $0 < a < 1$ has a unique factorization into maximal $p_i < 1$.

We approach the proof through a series of three lemmas.

LEMMA 1. - If $1 > p$ and $p(1 : p) = 1$, then

(23) $\qquad 1 > p > p^2 > p^3 \quad \ldots$ and $1 < (1 : p) < (1 : p)^2 < \ldots$

PROOF. - Since $p < 1$, $p^{r+2} \leqslant p^r$ for $r = 1 , 2 , 3 , \ldots$. If $p^{r+1} = p^r$, then

$$p = p^{r+1}(1 : p)^r = p^r(1 : p)^r = 1 \quad ,$$

giving a contradiction. The proof that $1 < (1 : p) < (1 : p)^2 < \ldots$ is similar.

LEMMA 2. - If $1 > p > a > 0$, then $1 > (1 : p)\, a > a$.

PROOF. - Since $p > a$, $1 = (1 : p)\, p \geqslant (1 : p)\, a$. Moreover $1 = (1 : p)\, a$ would imply $p = p1 = p(1 : p)\, a = 1a = a$, contrary to hypothesis. Likewise, since $(1 : p) > 1$, $(1 : p)\, a \geqslant 1a = a$. Moreover $(1 : p)\, a = a$ would imply $a = 1a = p(1 : p)\, a = pa$, and hence

$$a = pa = p(pa) = p^2 a = p^2(pa) = p^3 a = \cdots \quad .$$

Since $1 \geqslant a$, this would imply $a = p^r a \leqslant p^r 1 = p^r$ for all r . Hence, by (23), we would have an <u>infinite</u> chain of elements $\{p^r\}$ between 1 and a , again contrary to hypothesis.

COROLLARY. - Under the hypotheses of theorem 15, every prime nonzero integral element is maximal.

PROOF. - Let a be any non-zero non-maximal integral element. Then $a < p < 1$ for some maximal $p < 1$. Hence $q = (1 : p)\, a > a$ by lemma 2, so that $p > a$. But $pq = p(1 : p)\, a = a$ since $p(1 : p) = 1$; hence a is nonprime.

LEMMA 3. - If $0 < a < 1$, then a is a product of elements p_i covered by 1 (primes).

PROOF. - By the finite chain condition, either the conclusion holds or there is a maximal element a for which it fails. This maximal element cannot be covered by 1 , because the conclusion holds trivially for elements covered by 1 . Hence, by the corollary of lemma 2, $a = pr$ where $1 > p > a$ and $1 > r > a$. By induction, $p = p_1 \cdots p_r$ and $q = q_1 \cdots q_s$, where the p_i and q_j are covered by 1 . Hence $a = p_1 \cdots p_r\, q_1 \cdots q_s$, which we wanted to prove.

To prove theorem 13, it only remains to prove that the factorization is unique (up to rearrangement of factors). This can be proved by the usual argument. If $a = p_1 \cdots p_r$ and $a = q_1 \cdots q_s$, where the p_i and q_i are covered by 1 , then $p_1 \geqslant a = q_1 \cdots q_s$. Hence, by the corollary of lemma 2 and induction, $p_1 \geqslant q_j$ for some j . Since p_1 and q_j are both maximal, $p_1 = q_j$. Hence

$$p_2 \cdots p_r = (1 : p)\, p_1 p_2 \cdots p_r = (1 : p_1)\, a = (1 : q_j)\, a$$

$$= q_1 q_2 \cdots q_{j-1} (1 : q_j) q_j \cdots q_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s ,$$

whence uniqueness follows by induction on r .

12. Discussion ; Artin equivalence.

Unlike theorem 3, which is much more elegant in appearance, theorem 13 is really useful for algebraic number theory. This is because one can prove that assumptions I and II hold in about five pages (9).

Actually, one can prove much more than assumption I very directly. Since the lattice of E-modules is modular, all connected chains between a and 1 have the same length.

That is, one needs only about five pages of technical reasoning about algebraic numbers per se to establish the fundamental theorem of ideal theory, if one is willing to assume the elements of the theory of ℓ-demigroups. Possibly one can do better, though I doubt if one can replace assumption I by the ascending chain condition.

The identity $p(1 : p) = 1$ for maximal elements was the key assumption made in proving theorem 13. Had we assumed the identity $x(1 : x) = 1$ for all x, then we would have assumed in effect that L was an ℓ-group with $x^{-1} = 1 : x$. For such ℓ-groups, we know by [LT2] (Ch. XIV, § 13), that the ascending chain condition on integral elements does imply unique factorization.

Artin equivalence. - The identity $x(1 : x) = 1$ is related to an interesting congruence relation introduced by ARTIN into commutative residuated ℓ-demigroups with unity 1.

Two elements a, b of such an ℓ-demigroup L are Artin equivalent when $1 : a = 1 : b$. By theorem 8, this is equivalent to saying that $a^{**} = b^{**}$, where we define $x^* = 1 : x$; thus it is analogous to the equivalence relation studied in the theorem of Glivenko. It is related to the identity $x(1 : x) = 1$ since this implies the identity

$$a = a1 = a(1 : a)(1 : (1 : a)) = 1(1 : (1 : a)) : 1 ; (1 : a) .$$

If Artin equivalence were a congruence relation for all operations, so that the analog of the theorem of Glivenko held, then the Artin-equivalent elements would define an ℓ-group. With the ascending chain condition, one could prove unique factorization into primes.

---

(9) One must prove lemmas (8.21)--(8.23) of POLLARD. The proof of these uses his theorem 8.7 ("every prime ideal is maximal"), which must also be proved since to assume the corollary to lemma 2 of § 11 would involve circular reasoning.

By theorem 8, Artin equivalence is a congruence relation for joins. It is also a congruence relation for multiplication, since if $a^* = b^*$, then

$$1 : ax = (1 : a) : x = (1 : b) : x = 1 : bx \quad .$$

For it to be a congruence relation for meets, it is necessary and sufficient that L be integrally closed, in the sense that $a : a = 1$ for all $a \in L$; this is proved in [DLC], p. 243.

13. Applications to algebraic geometry.

The applications of ideal theory to algebraic geometry are very different from its applications to algebraic number theory. Whereas ideals are needed to obtain a general unique factorization theorem for domains of algebraic integers, the opposite is true for polynomial rings.

One therefore expects the application of lattice theory to algebraic geometry to be very different from those to algebraic number theory. Those to algebraic geometry are associated with the complete commutative integral ℓ-demigroup of all ideals of the ring $E = K[x_1 , \dots , x_r]$ of polynomials defined in example 6, § 3.

They stem from the polarity between certain ideals of E and algebraic varieties, defined by the relation $p(x_1 , \dots , x_r) = 0$ between polynomials $p \in E$ and points $x = (x_1 , \dots , x_r)$ in affine r-space $A_r(K)$. The dually isomorphic lattices defined by this polarity have as elements the algebraic varieties of $A_r(K)$, and ideals of E which are their own radicals $\sqrt{E}$, respectively. The former are obviously a distributive lattice, and the latter satisfy the ascending chain condition.

These facts have been exploited in [LT2] (Ch. IX, § 8) ; the discussion will not be repeated here ([10]) . It can also be shown, at least if K is the real or complex field, that the dimension of an algebraic variety V is the biggest n such that V contains a chain whose ordinal number is ω^n or more (by the ascending chain condition, every chain of algebraic varieties is well-ordered).

I know of no complete characterization (up to isomorphism) of the lattice of all algebraic varieties in the plane (for $r = 2$), let alone in higher dimensions. To characterize the ℓ-demigroup of all ideals of $K(x_1 , \dots , x_r)$ up to

([10]) For a related discussion, which does not assume the axiom of choice, see: DUBREIL (P.) et DUBREIL-JACOTIN (M.-L.). - Leçons d'algèbre moderne (Footnote ([3])) ; p. 211-223.

isomorhism would seem even more difficult. Offhand, it looks like a major and every interesting problem.

Since any two complex algebraic curves have at least one point in common, while the same is not true for real algebraic curves, the characterization will certainly depend on the base field K.

14. Irreducible and primary elements.

The important concepts of the radical of an ideal, of primary ideal, and of irreducible ideal are easily generalized from ideals in polynomial rings to elements of any commutative, integral ℓ-demigroup which satisfies the ascending chain condition.

Namely, the radical $\sqrt{a}$ of a is defined as the join of all elements $x \in D$ satisfying $x^n \leqslant a$ for some integer $n = n(x)$; $\sqrt{a}$ also satisfies $\sqrt{a}^N \leqslant a$ for some $N = N(a)$. An element q is defined to be primary when $ab \leqslant q$ implies that either $a \leqslant q$ or that $b^r \leqslant q$ for some finite integer $r = r(a, b)$. As in lattices generally, an element a is defined to be (meet-) irreducible when $x \cap y = a$ implies $x = a$ or $y = a$.

Many of the properties of the radical of an ideal, and of primary and irreducible ideals are easily proved abstractly in any ℓ-demigroup having the properties specified. For instance, q is primary if and only if its radical $\sqrt{q}$ is a prime element (i. e.,,if and only if $p \geqslant q \geqslant p^N$ for some prime element p).

However, it is not necessarily true that every irreducible element is primary, even if D is assumed to be a modular lattice ([11]).

This is another serious shortcoming of the theory of ℓ-demigroups, from the point of view of applications.

15. Frobenius condition.

We now turn our attention to applications of the concept of residuation to non-commutative ℓ-demigroups. We begin by considering the full matrix algebra $M_n(D)$ of all $n \times n$ matrices with entries in a given division ring D. The linear associative algebra $M_n(D)$ is isomorphic to the ring of all endomorphisms of the n-dimensional left vector space $V_n(D)$ over D.

([11]) WARD (Morgan) and DILWORTH (R. P.). - Residuated lattices, Trans. Amer. math. Soc., t. 45, 1939, p. 335-354.

It is easy to verify that if a right-ideal A of $M_n(D)$ contains one endomorphism with a given null-space $S \in V_n(D)$, then it contains all endomorphisms of $V_n(D)$ with null-space in S. Further, the set of all such endomorphisms is a right-ideal $J(S)$. Likewise, if a left-ideal contains an endomorphism with range S, then it contains all endomorphisms with range in S; moreover the set of all such endomorphisms is a left-ideal $K(S)$. Finally, $0 \cdot^{\circ} K(S) = J(S)$ and $0 \circ^{\cdot} J(S) = K(S)$. This shows that $M_n(D)$ is a Frobenius ring, in the sense of the following definition :

DEFINITION. - A ring in which $0 \cdot^{\circ} (0 \circ^{\cdot} J) = J$ for all right-ideals J and $0 \circ^{\cdot} (0 \cdot^{\circ} K) = K$ for all left-ideals K is a Frobenius ring. A residuated m-poset in which $0 \cdot^{\circ} (0 \circ^{\cdot} h) = h$ for all right-ideal elements h and $0 \circ^{\cdot} (0 \cdot^{\circ} k) = k$ for all left-ideal elements k is a Frobenius m-poset.

THEOREM 14. - Let A be any semisimple linear associative algebra of finite order over a field F. Then the linear subspaces (F-modules) of A form a Frobenius m-lattice $M(A)$, which is also a projective geometry. The right-ideal elements of M and the left-ideal elements of M are dually isomorphic complemented modular lattices.

The preceding result is a straightforward application of the Wedderburn theory of semisimple algebras, in the light of the remarks of paragraph one above. The Wedderburn theory shows that A is the direct sum of full matrix algebras $A_i = M_{n(i)}(D_i)$, where the D_i are division algebras over F. The right-ideal elements of the m-lattice $M(A)$ form lattices, which are the direct unions of those $H_i = H(A_i)$, for the direct summands A_i. Since each H_i is a complemented modular Frobenius m-lattice, the same is true of their direct union, completing the proof.

It is easy to construct other Frobenius rings. Thus the nilpotent algebra of all polynomials in x, modulo any x^n, is a commutative Frobenius ring. Its ideals are generated by $1, x, x^2, \ldots, x^{n-1}, 0$ respectively ; they form a chain in which $0 : (x^h) = (x^{n-h})$.

But it is harder to construct other Frobenius rings whose right-ideals and left-ideals form complemented (modular) lattices. If A is such a ring, with radical N, then A must contain a right-ideal H complementary to N. Here $HN \leqslant H$ since H is a right-ideal, and $HN \leqslant N$ since N is a (two-sided)-ideal. Hence $HN \leqslant H \cap N = 0$. Likewise, A must contain a complementary left-ideal K such that $NK = 0$.

Regular rings. - In his study of continuous-dimensional geometries, von NEUMANN defined a regular ring as a ring in which every element a has a relative inverse x such that $axa = a$. A finite-dimensional linear associative algebra is regular if and only if it is semisimple ; the equational definition given above has the advantage of being applicable to rings of operators.

In any regular ring R, $aR = axa\,R \leqslant eR$, where $e = ax$ satisfies $e^2 = (ax)(ax) = (axa)\,x = ax = e$. Conversely, $eR = ax\,R \leqslant aR$; hence $aR = eR$. This shows that every principal right-ideal of R is generated by an idempotent. A similar argument works for left-ideals. Conversely, any ring in which every principal right-ideal is generated by an idempotent satisfies $e = ax$ where $e^2 = ax\,ax = eax$. But we cannot cancel x to set $axa = e$.

The lattice of principal right-ideals of any regular ring is complemented, since eR and $(1 - e)\,R$ have in common only elements y for which $(1 - e)\,y = (1 - e)\,ez = 0$ and $ey = e(1 - e)\,z = 0$; hence for which $y = 1y = (1 - e)\,y + ey = 0$. Likewise, the lattice of principal left-ideals of any regular ring is complemented.

I do not know whether the product of two principal right-ideals of a regular ring is itself a principal right-ideal.

16. Algebra of relations.

The algebra of all binary relations on an arbitrary set I of elements α , β , γ , ... provides a final application of the theory of ℓ-demigroups. A binary relation on I may be defined by its relation matrix $||r_{\alpha\beta}||$, by letting $r_{\alpha\beta} = 1$ if the relation holds between α and β , and letting $r_{\alpha\beta} = 0$ if it does not. Relation matrices form a Boolean algebra if $||r_{\alpha\beta}|| \leqslant ||s_{\alpha\beta}||$ is defined to mean $r_{\alpha\beta} \leqslant s_{\alpha\beta}$ for all α. When multiplied by the rule

$$rs = t \text{ means that } t_{\alpha\beta} = \bigcup_{\gamma} r_{\alpha\gamma}\, s_{\gamma\beta} \quad , \tag{24}$$

one gets an ℓ-demigroup D_n , where n is the cardinality of I .

This ℓ-demigroup can also be obtained as a special case of example 8, § 4. D_n is isomorphic with the ℓ-demigroup of all join-endomorphisms of the Boolean algebra 2^n . It can also be obtained from example 2, § 1. Let G be the demigroup of elements e_{ij} and 0 , with the multiplication rules for matrix units :

$$e_{ij}\, e_{k\ell} = \begin{cases} e_{i\ell} & \text{if } j = k \\ 0 & \text{if } j \neq k \end{cases} \quad , \tag{25}$$

and $e_{ij}\ 0 = 0e_{ij} = 0$. Then 0_n is isomorphic with the ℓ-demigroup of all subsets of G which contain 0 ; this brings out the analogy with full matrix algebra. Finally, D_n can be defined as the ℓ-demigroup of all ℓ-modules in the ℓ-ring of all real $n \times n$ matrices.

Though the algebra of relations was studied in the nineteenth century, in connection with the logic of relations, the systematic study of postulates for relation algebras dates only from 1945. The first characterization of relation algebras as ℓ-demigroups was given in [LT2] (Ch. XIII, § 5- § 7).

The ℓ-demigroup D_n has a zero $0 = ||0||$ and a unity $e = \delta_{ij}$, as well as an $I = ||1||$. Each $r = ||r_{ij}||$ in D_n has a converse $\breve{r} = ||r_{ji}||$. The operation of conversion can either be considered as a primitive operation peculiar to relation algebra, or it can be defined from the usual ℓ-demigroup operations as follows.

DEFINITION. - A relation algebra is a residuated ℓ-demigroup L with zero 0 and unity e , which is a Boolean algebra when considered as a lattice. Further, it is assumed that

$$e' \cdot^{\circ} r' = e' \circ^{\cdot} r' \quad \text{for all } r \ , \tag{26}$$

$$e' \cdot^{\circ} (rs)' = (e' \cdot^{\circ} s')(e' \cdot^{\circ} r') \quad \text{for all } r, s \ , \tag{27}$$

$$e' \cdot^{\circ} (e' \circ^{\cdot} r) = r \quad \text{for all } r \ . \tag{28}$$

The element $e' : r' = e' \cdot^{\circ} r' = e' \circ^{\cdot} r'$ is in fact the converse $\breve{r}$ of r , and equations (27)-(28) simply reformulate the identities $\breve{r}\breve{s} = \breve{s}\breve{r}$ and $\breve{\breve{r}} = r$.

Note that the definition of a relation algebra is only equational if one admits complementation and residuation as fundamental operations. One can replace the two binary residuation operations by the unary conversion operation, using two identities communicated to the author by DAVIDON :

$$r \cdot^{\circ} s = (\breve{s}r')' \quad \text{and} \quad r \circ^{\cdot} s = (r's)' \ . \tag{29}$$

The identities $\breve{rs} = \breve{s}\breve{r}$ and $\breve{\breve{r}} = r$ imply $\breve{e} = e$; using them and $\breve{r \cup s} = \breve{r} \cup \breve{s}$, which implies $\breve{r \cap s} = \breve{r} \cap \breve{s}$ and $\breve{r'} = \breve{r}'$, one obtains (26)-(28) trivially from the definitions (29). This proves

THEOREM 15. - A relation algebra is an ℓ-demigroup L with unary operations of complementation and conversion such that complementation makes L into a Boolean algebra.

(30) $\breve{rs} = \breve{s}\breve{r}$, $\breve{\breve{r}} = r$, and $\overbrace{r \cup s} = \breve{r} \cup \breve{s}$

in which (29) define residuals.

Since $r \circ^{\circ} s$ can be defined by the identity $[s(r \bullet^{\bullet} s)] \cup r = r$ and the identical implication $sx \cup r = r$ implies $x \cup (r \circ^{\bullet} s) = r \circ^{\bullet} s$, theorem 15 makes possible the application of the concepts of universal algebra.

A simpler, strictly <u>equational</u> definition of a relation algebra has been derived by TARSKI. TARSKI has shown that the equation

(31) $$[\breve{r}(rs)'] \cup s' = s'$$

is sufficient to take care of the properties of residuation. In view of (30), it is equivalent (writing $r = \breve{x}$ and $s = y'$) to $[x(\breve{x}y')'] \cup y = y$, or (using (29)) to $x(y \circ^{\bullet} x) \leqslant y$. Hence we have :

THEOREM 16 (TARSKI). — A relation algebra is an ℓ-demigroup which is a Boolean algebra with a unary conversion operation satisfying (30)-(31).

To apply the concepts of universal algebra (Ch. V) using the above equational definitions, one must require subalgebras to be closed under residuation and conversion, and congruence relations to respect residuation. Thus, one must change the simple concepts of m-sublattice and congruence relation for demigroups used in the earlier sections of this paper.

17. <u>Continuous relation algebras</u>. — The relation algebras considered in § 16 are all atomic Boolean algebras, when considered as lattices. Since many of the most interesting Boolean algebras arising in analysis are continuous, it is natural to try to construct continuous relation algebras. This appears to be difficult, for the following reason.

Considered as Boolean algebras, finite relation algebras obviously correspond to the algebra of all subsets of a <u>product space</u> (the space of all entries of the relation matrix).

Correspondingly, the correspondences $x \to Ix$ and $x \to xI$ <u>project</u> the given relation algebra R onto two isomorphic Boolean subalgebras of R, say A and $\breve{A}$. As a Boolean algebra, then, R is the direct product $A \times \breve{A}$; moreover <u>conversion</u> is an involutory automorphism of R which interchanges A and $\breve{A}$. To reconstruct R as a relation algebra from $A \overset{\sim}{=} \breve{A}$, it suffices to define <u>relation multiplication</u> in $A \times \breve{A}$.

There are various natural ways to define direct products of infinite Boolean algebras. For instance, let $A \cong \tilde{A}$ be the Boolean algebra of all Borel subsets of $[0 , 1]$, modulo subsets of measure zero. Then one naturally defines $A \times \tilde{A}$ as the set of all Borel subsets of the unit square $0 \leqslant x , y \leqslant 1$, that is, of all Borel functions $r(x , y)$ having 0 and 1 for values. The natural definition of the relation product $t(x , y)$ of two such functions $r(x , y)$ and $s(x , y)$ is :

$$(32) \qquad t(x , y) = \begin{cases} 1 & \text{if } \int_0^1 r(x , z)\ s(z , y) > 0 \quad , \\ 0 & \text{if } \int_0^1 r(x , z)\ s(z , y) = 0 \quad . \end{cases}$$

However, this relation algebra, considered as an ℓ-demigroup, does not have a unity 1 in the sense (3). The matrix of the identity function $1 : x = y$ is defined by

$$(33) \qquad r(x , y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \quad . \end{cases}$$

In analysis, such matrices (or integral kernels) are identified with the matrix 0.

The preceding simple discussion indicates a major obstacle to constructing continuous analogs of relation algebras : providing them with a multiplicative unity. If one is willing to forego the existence of a multiplicative unity, one can construct various kinds of relation algebras from appropriate classes of Boolean algebras.

Namely, one can construct an algebraic direct product for any A. If A is a complete Brouwerian lattice, one can construct $A \times \tilde{A}$ as a topological direct product, by analogy with the construction of open sets in a product space from the open sets in the factor. Finally, if A is a measure algebra, one can construct $A \times \tilde{A}$ by analogy with the construction of product measures. We omit the details, noting only that none of the above constructions yields a unity in general.

Some other recent results on the algebra of relations can be found in the Notes alluded to at the beginning.